Rozdział 2.
Hakowanie systemu

Najczęściej hakerzy zyskują nieupoważniony dostęp do danych znajdujących się na dyskach twardych komputerów pracujących pod kontrolą systemu operacyjnego Unix. Przyczyna takiego stanu rzeczy jest prosta — system ten (lub jego odmiany) jest zainstalowany na większości „głównych komputerów", serwerów odległych sieci lokalnych, które są dostępne przez modem lub sieć. Fakt, że Unix jest tak rozpowszechniony stał się zarazem powodem rozlicznych problemów związanych z bezpieczeństwem (czy też jego brakiem) systemu. Z Uniksa korzysta wielu użytkowników komputerów, stąd wiedza na jego temat jest bardzo rozpowszechniona. Przejęcie kontroli nad systemem nie stanowi już trudności dla hakerów. Z dnia na dzień odkrywają oni coraz to nowsze metody i sposoby umożliwiające włamanie się do systemu. Równolegle z tym wzrasta wiedza o funkcjonowaniu systemu i ujawniane są luki tkwiące w jego systemie zabezpieczeń.

Rodzaje hakerskich ataków

Wiedza na temat luk w zabezpieczeniach systemów, którą posiadają hakerzy, daje im możliwość penetrowania odległych systemów i jedyną barierę stanowi dla nich wyłączony komputer. Zatem każda osoba wędrująca po Sieci powinna się liczyć z tym, że jej dysk zostanie splądrowany. Specjaliści-włamywacze w ciągu sekundy mogą zniszczyć wszystkie dokumenty. Zdają sobie z tego sprawę internauci, ale i tak nie podejrzewają nawet, jak wielkie szkody mogą ponieść. Beztroska i niewiedza użytkowników ułatwiają 99% włamań.

Biorąc pod uwagę wcześniejsze rozróżnienia, śmiało można stwierdzić, że zniszczeń tych nie dokonują prawdziwi hakerzy, ale raczej nazywający siebie tak ich „gorsi bracia", zdegenerowani naśladowcy — cyberanarchiści, młodzi ludzie mający za dużo wolnego czasu. Niektórym z nich się wydaje, że mogą się stać dzięki temu sławni. Intruzi dołączają na przykład do e-maili wirusy (w rodzaju „I love you") „oczyszczające" dysk twardy z wszelkich znajdujących się na nim danych. W ten sam sposób — za pomocą poczty elektronicznej — podrzucają oni konie trojańskie, czyli zainfekowane pliki. Można temu łatwo zapobiec — wystarczy trzymać się zasady

nieotwierania podejrzanych załączników z rozszerzeniami typu .exe, .doc lub .xls czy też wcześniejszego ich przetestowania programem antywirusowym. Często sami użytkownicy ułatwiają zadanie włamywaczom komputerowym nieumiejętnie wybierając hasło umożliwiające korzystanie z konta poczty elektronicznej. Wyrazy krótkie, proste i znajdujące się w słowniku są zazwyczaj łatwe do odgadnięcia.

Najtrudniejsze do złamania są hasła składające się z liter i cyfr. O wirusa prosimy się sami, ściągając oprogramowanie, gry czy wygaszacze ekranu z nieznanych stron lub na przykład witryn pornograficznych. Internauci korzystający z systemu Windows w chwili, gdy pobierają pliki z tego serwisu, muszą się liczyć z tym, ze mogą one zmienić konfigurację modemu. W efekcie zamiast z TPS-a zaczniemy się łączyć na przykład z Filipinami. Bywa, że ktoś sugeruje zainstalowanie określonego programu, by dzięki temu zyskać kontrolę nad naszym dyskiem twardym. Trzeba bowiem mieć na uwadze fakt, że taki program może na przykład infiltrować nasze prywatne życie. Anonimowość Internetu usypia przecież czujność. Tymczasem wiele firm wywiadowczych zbiera informacje o preferencjach i zainteresowaniach bywalców przestrzeni wirtualnej. Dane te następnie sprzedawane są producentom i dystrybutorom. Zabawne oprogramowanie firmy Comet Systems, które podczas buszowania w Internecie zmieniało kursor w postacie z kreskówek, przesyłało jednocześnie producentowi informacje o stronach odwiedzanych przez daną osobę. W krótkim czasie przedsiębiorstwo uzyskało dane prawie siedemnastu milionów osób. Trzeba zatem bronić się przed takimi atakami i jeśli nawet kupimy odpowiednie oprogramowanie zabezpieczające, nie możemy spoczywać na laurach.

Jedynym z podstawowych błędów jest zapominanie o aktualizacji programu. Aby uniknąć ataków intruzów, trzeba niemal zbudować twierdzę. Ochrona danych powinna polegać przede wszystkim na profilaktyce, stosowaniu oprogramowania zaporowego (typu *firewall*) i haseł kontroli dostępu do sprzętu, szyfrowaniu ważnych plików oraz przechowywaniu ich kopii na zewnętrznych nośnikach. Bardzo ciężko jest w sposób jednoznaczny i skończony sklasyfikować metody, którymi posługują się komputerowi włamywacze w celu przejęcia kontroli nad innymi systemami. Niektóre z nich powtarzają się dla poszczególnych systemów operacyjnych, inne są ściśle uzależnione od tego, z jakim systemem haker ma do czynienia.

Ogólnie metody włamań możemy podzielić na:

- ataki z zewnątrz sieci lokalnej;
- ataki z wnętrza sieci lokalnej;
- ataki pośrednie.

Ataki z zewnątrz — ***to*** ataki, których najczęstszą formą są zakłócenia stabilnej pracy. Przejmowanie kontroli nad systemami odbywa się z zewnątrz sieci lokalnej — na przykład z Internetu. Można w tym celu wykorzystać lukę w systemie zabezpieczeń, błąd serwisu sieciowego lub po prostu słaby poziom zabezpieczeń firmy. Do najczęstszych tego typu ataków należą :

Ataki na poszczególne komputery bądź serwer główny (DoS,wirusy) — to jeden z najczęstszych typów ataków. Konsekwencjami są zwykle przerwy w pracy sieci lokalnej, uszkodzenie poszczególnych (bądź wszystkich) końcówek serwera, a co za tym idzie — całej sieci, co powoduje wielogodzinne przerwy w pracy. Skutki mogą być niewinne i skończyć się na zawieszeniu poszczególnych komputerów czy nawet całej sieci, ale może to także prowadzić do fizycznego uszkodzenia sprzętu, wymazania BIOS-u na płycie głównej lub uszkodzenia twardych dysków.

Ataki na serwer http — to ataki, których efektem jest utrata danych witryny internetowej lub uzupełnienie jej treściami kompromitującymi firmę.

Do ataków z zewnątrz sieci hakerzy często wykorzystują metodę zwaną DoS.

DoS (Denial of Service — blokowanie serwisów) — jest to atak mający na celu zablokowanie konkretnego serwisu sieciowego (na przykład strony WWW) lub zawieszenie komputera. Możliwe jest przesterowanie ataków DoS do bardziej skomplikowanych metod, co może doprowadzić nawet do awarii całej sieci. Niejednokrotnie hakerzy, którzy włamują się do systemów za pomocą tzw. techniki **spoofingu** lub redyrekcji, ukrywają swój prawdziwy adres internetowy, więc ich zlokalizowanie często staje się niemożliwe. Anonimowość ułatwia więc zdecydowanie atakowanie systemów metodą **Denial of Service**, co powoduje uniemożliwienie wykonania przez serwer jakiejkolwiek usługi. Jednak obecnie ataki te są już rzadko stosowane, gdyż większość administratorów odpowiednio się przed nią zabezpieczyła, co wcale nie było trudne, ale konieczne, gdyż programy umożliwiające ten typ hakowania (jest ich co najmniej kilkanaście) powodują zapchanie serwera, spowolnienie jego pracy aż do konieczności uruchomienia restartu. W przeszłości znane były przypadki zablokowania kilku tysięcy serwerów jednocześnie. Teraz oczywiście jest to niemożliwe!

Ataki typu **DoS** można wymierzyć przeciwko wszystkim platformom systemowym, gdyż wykorzystują one właściwości protokołu IP, czyli protokołu używanego między innymi w Internecie. Programów takich jest bardzo dużo, gdyż kod jest pokazywany publicznie, jak to w prawdziwym światku hakerskim bywa. Tak wiec co 2-3 tygodnie opracowywany jest nowy sposób ataku. Przeważnie programy tego typu przeznaczone są do uruchomienia na jednej platformie (np. Linuksie), a ich celem również jest jedna platforma systemowa (np. Windows NT). Istnieją jednak programy, których cel stanowi atak na kilka systemów jednocześnie.

Dobrym przykładem jest tu LAND. Programy tego typu są dość proste w użyciu i bardzo łatwo dostępne w Internecie. Wystarczy wpisać **Denial of Service i hak** w wyszukiwarce i się wszystko stanie się jasne. Warto jeszcze dodać, że, programy te udostępniane są w postaci kodów źródłowych, co wydaje się zrozumiałe.

Poniżej zamieszczona została tabelka grupująca niektóre tylko nazwy popularnych programów umożliwiających ataki typu DOS:

Nazwa	*System, na którym haker uruchamia program*	*System, który podlega atakowi*	*Efekty*
bonk, boink	Unix	Windows NT i Windows 95	Program powoduje zawieszenie dowolnego komputera systemem Windows NT lub Window 95
hanson	Unix	Windows z klientem mirc	Powoduje odłączenie mirc'a od sieci
Jolt	Unix	Windows 95	Wywoływanie zbyt dużych pakietów powoduje zawieszenie systemu operacyjnego Windows 95
Land	Unix	Dużo systemów sieciowych	Wysyłane pakiety powodują zablokowanie systemu docelowego
Pong	Linux	Window 95	Cel ataku zasypywany jest pakietami ICMP, czyli ping, co powoduje jego zawieszenie

Do bardziej znanych należą natomiast programy zgrupowane poniżej:

Nazwa	*System, na którym haker uruchamia program*	*System, który podlega atakowi*	*Efekty*
Teardrop	Unix	Windows NT i Windows 95	Zablokowanie systemu Windows NT i Windows 95
Winnuke	Linux	Windows NT i Windows 95	Powoduje wyświetlenie niebieskiego ekranu

Podsumowując warto jeszcze raz zaznaczyć, że ataki typu DoS są dość łatwe do przeprowadzenia. Ostatnie ataki na serwery najpoważniejszych firm internetowych przeprowadzone były za pomocą stosunkowo nowej metody opracowanej przez hakerów w celu zablokowania transferu jakichkolwiek danych drogą elektroniczną. Polegało to na wysłaniu do serwera internetowego bardzo dużej liczby zapytań lub poleceń rozpoczęcia transmisji. Było ich tak dużo, że po chwili serwer zostawał przeciążony i przestawał obsługiwać użytkowników. Sposób ten znany jest już od dawna pod nazwą „Denial of Service Attack" i doczekał się „mutacji" w postaci „SYN Flood Attack" czy „Smurf Attack" — działających na bardzo zbliżonych do siebie zasadach.

Hakerzy, którzy zaatakowali między innymi Yahoo3 i CNN twórczo rozwinęli wcześniejszy pomysł. Zamiast wysyłać sygnały ze swojego komputera, wykorzystali do tego całą armię „przejętych" maszyn, znajdujących się na przykład w sieciach uniwersyteckich. Taka „armia" komputerów jest kierowana z jednego miejsca

i jej celem jest wykonanie jednego tylko zadania, którym jest „zasypanie" wybranego obiektu jak największą liczbą połączeń. Wykorzystywany jest do tego program Tribal Flood Network oraz inne, które są do niego podobne — Stacheldraht i Trinoo. Bardzo często hakerzy wykorzystują do ataków z Internetu metodę zwaną spoofingiem.

Spoofing (maskarada) — metoda ta stosowana jest zwykle przez doświadczonych i wyrafinowanych włamywaczy. Polega na podszyciu się włamywacza pod jednego użytkowników systemu, który posiada własny numer IP (numer identyfikujący użytkownika). Technika ta ma na celu omijanie wszelkich zabezpieczeń, jakie zastosował administrator w sieci wewnętrznej. Jest bardzo skuteczna nawet, gdy bywa wykorzystywana przeciwko markowym *firewallom*, *switchom* i ruterom. Dzięki niej możliwe jest „udawanie" dowolnego użytkownika, a co za tym idzie — „podszywanie" się i wysyłanie sfałszowanych informacji.

Ze swego komputera haker może dokonać przekierowania źródłowego adresu IP i „podszyć się" pod komputer sieciowy. Robi to po to, by określić jego bezpośrednią drogę do miejsca przeznaczenia oraz trasę powrotną. W ten sposób może przechwytywać lub modyfikować transmisje bez zliczania pakietów przeznaczonych dla komputera głównego. W przeciwieństwie do ataków polegających na rozsynchronizowaniu, „podszywanie się" pod adresy IP jest trudne do wykrycia. Jeśli serwer internetowy ma możliwość monitorowania ruchu w Sieci w zewnętrznym ruterze internetowym, to należy kontrolować przechodzące przez niego dane. Do Sieci nie powinny być włączane pakiety zawierające adresy komputera źródłowego i docelowego, które mieszczą się w obrębie lokalnej domeny. Najlepszą obroną przed podszywaniem się jest filtrowanie pakietów wchodzących przez ruter z Internetu i blokowanie tych, których dane wskazują na to, że powstały w obrębie lokalnej domeny.

Wirusy — to bardzo przydatne do ataków z zewnątrz Sieci programy. Mogą one zostać podrzucone zwykłą drogą, np. jako program ściągnięty z Internetu, dyskietka z najnowszym upgradem do jakiegoś programu lub też mogą być dołączone do pliku tekstowego czy e-maila. Niekonsekwencja w przypadku takiego postępowania może wiele kosztować. Wirus przenika bowiem do komputera i może być przenoszony w sieci wewnętrznej wraz z nowszymi wersjami programów. Może on tkwić uśpiony długie miesiące, a po okresie uśpienia — zaatakować.

Atak na serwer poczty — to kolejny rodzaj hakerskiej działalności. Jego konsekwencją jest utrata kontroli nad przepływającą korespondencją (e-maile kierowane do konkretnej osoby mogą zostać odczytane i dostać się w posiadanie niepowołanych osób, możliwe jest także fałszowanie korespondencji i wprowadzenie w firmie dezorganizacji pracy). Ulubionymi przez hakerów sposobami atakowania są *ataki na serwer główny*, które prowadzą do utraty kontroli nad całą siecią, wiążą się z utratą wszystkich danych, z zakłóceniami pracy dowolnych usług sieciowych w całej firmie. Po przejęciu kontroli nad głównym serwerem możliwe jest przechwytywanie danych wędrujących wewnątrz sieci, a co za tym idzie — poznanie struktury wewnętrznej firmy. Możliwe jest fałszowanie danych przesyłanych siecią, blokowanie wiadomości przesyłanych między szefem a współpracownikami.

Seeking vulnerabilities (szukanie luk) — jest to podstawa ataku każdego włamywacza. Luki takie są wynikiem błędów w oprogramowaniu.

Każdy szanujący się haker posługuje się w swoich zmaganiach metodą, która wymaga sporej inteligencji. Jest to ***s**ocial engineering* (socjotechnika), metoda, która polega na manipulowaniu ludźmi w taki sposób, aby ujawnili poufne informacje, mogące pomóc we włamaniu się do systemu. Haker bardzo często przeprowadza wstępny wywiad. Zbiera informacje o firmie, pracownikach, systemach, hasłach itp. Może też zadzwonić do administratora sieci i podając się za inną osobę poprosić o zmianę hasła lub też podając się za pracownika serwisu przeszukać biuro w celu odnalezienia haseł, które pracownicy bardzo często zapisują na kartkach i przechowują na biurku. W tym przypadku haker nie cofnie się nawet przed przeszukiwaniem śmieci firmy *trashing*. Jest to inna droga, kolejny sposób zbierania wartościowych informacji, zdobywania potęgi i siły oraz prestiżu.

Hijacking — to metoda polegająca na przechwytywaniu transmisji odbywającej się między dwoma systemami. Dzięki niej możliwe jest przechwycenie dostępu do szczególnie chronionych programów. Ze względu na wysoki stopień skomplikowania jest specjalnością elity hakerskiej.

Do bardzo groźnych ataków należą te, które określane są ogólnie a*takami z wnętrza sieci*. Włamanie następuje z wnętrza sieci lokalnej poprzez wykorzystanie konta jakiegoś użytkownika czy też luki w zabezpieczeniach systemu autoryzacji użytkowników. Najczęściej włamania tego typu są udziałem pracowników firmy, a nie użytkowników komputerów spoza jej obrębu, gdyż dostęp do końcówki Sieci takiej osoby rzadko pozostaje zauważony. Nadal istnieje możliwość dokonania wszystkich wyżej wymienionych ataków.

Innym rodzajem ataków są ataki pośrednie. Hakerzy stosują tu dość wyrafinowane metody, czego najlepszym przykładem są *konie trojańskie*. To grupa ataków najtrudniejszych do wykrycia. „Podłożenie" konia trojańskiego otwierającego dostęp do całej sieci może odbyć się za pośrednictwem poczty elektronicznej czy też podczas ściągania atrakcyjnego programu, który pochodzi z niepewnego źródła. Użytkownik prawie nigdy nie jest świadom tego, że ściągając na przykład najnowszą wersję odtwarzacza plików mp3 faktycznie otwiera dostęp do swojego komputera, a potem — całej Sieci osobom niepowołanym.

PACKET SNIFFING (podsłuchiwanie pakietów) — jest to metoda zdobywania systemu polegająca na przechowywaniu przesyłanych przez sieć niezaszyfrowanych informacji. Można w ten sposób zdobyć hasło użytkownika i uzyskać dostęp do danego konta. Ataki polegające na „biernym węszeniu" stały się powszechne w Internecie. Stanowią one zazwyczaj wstęp do aktywnego przechwytywania cudzych plików. Aby rozpocząć tego rodzaju atak, haker musi zdobyć identyfikator i hasło legalnego użytkownika, a następnie zalogować się do Sieci. Kiedy wykona już te posunięcia, może bezkarnie podglądać i kopiować transmisje pakietów, zdobywając jednocześnie informacje o funkcjonowaniu danej sieci lokalnej. Aby temu zapobiec, administratorzy systemów rozproszonych zazwyczaj zakładają programy identyfikujące, takie jak system jednorazowego sprawdzania hasła czy system uwiarygodniania przepustek (na przykład Kerberos).

Aktywne rozsynchronizowanie — jest to atak polegający na aktywnym rozsynchronizowaniu. Polega na tym, że haker wymusza siłą lub podstępem rozsynchronizowanie dwóch końców połączenia TCP, w efekcie czego komputery nie mogą wymieniać danych. Następnie, używając trzeciego komputera głównego (przyłączonego do fizycznego łącza przesyłającego pakiety TCP), włamywacz przechwytuje rzeczywiste pakiety i tworzy ich zamienniki, akceptowane przez oba połączone ze sobą komputery. Pakiety wygenerowane przez trzeci komputer zastępują pakiety oryginalne, które byłyby wymienione przez połączone systemy.

Ataki korzystające z autoryzowanego dostępu — są to ataki często stosowane przez osoby próbujące się włamać do sieci opartych na systemie operacyjnym (takim jak UNIX, VMS i Windows NT), korzystającym z mechanizmu autoryzowanego dostępu. Duże niebezpieczeństwo niesie ze sobą tworzenie plików zawierających nazwy serwerów, do których można uzyskać dostęp bez podawania hasła.

Podsyłanie numerów sekwencji protokołu TCP/IP — to atak, który wykorzystuje inny nieco mechanizm. Wiadomo, że komputer przyłączony do sieci dołącza do każdego transmitowanego pakietu adres IP komputera docelowego oraz unikatową liczbę, zwaną *numerem sekwencji*. Atak zwany *podsyłaniem numerów sekwencji TCP/IP* polega więc na uzyskiwaniu dostępu do sieci przy wykorzystaniu adresowania komputerów i wymiany pakietu sekwencji. Haker zwykle symuluje numer adresu IP, który następnie umożliwia mu przejście przez ruter i uzyskanie dostępu do systemu (jako wewnętrznemu użytkownikowi). Potem przegląda on numery sekwencji pakietów przesyłanych pomiędzy komputerami w sieci i stara się przewidzieć, jaki będzie następny numer sekwencji wygenerowany przez serwer, podszywa się pod ten numer, zajmując jednocześnie miejsce — o ile można posłużyć się takim wyrażeniem w kontekście przestrzeni wirtualnej — pomiędzy serwerem a użytkownikiem. Najłatwiejszym i najbardziej efektywnym sposobem obrony systemu przed podsyłaniem numerów sekwencji jest upewnienie się, że ruter, firewall i każdy serwer w sieci ma ustawioną pełną ochronę rewizyjną. Za pomocą rewizji można zaobserwować próby przejścia i zajęcia serwera.

Przechwycenie sesji — to rodzaj ataku, który prawdopodobnie jest największym zagrożeniem dla serwerów przyłączonych do Internetu. Czasem bywa on nazywany „aktywnym węszeniem” (w odróżnieniu od omawianego wcześniej „węszenia biernego”). Chociaż sposób ten przypomina nieco podsyłanie numerów sekwencji TCP, jest groźniejszy, gdyż w tym wypadku haker zamiast odszyfrowywać adresy IP, uzyskuje dostęp do sieci i wymusza akceptację swojego adresu IP jako adresu sieciowego. Idea polega na tym, że włamywacz przejmuje kontrolę nad komputerem łączącym go z siecią, a następnie odłącza ten komputer i „oszukuje” serwer, podając się za legalnego użytkownika. Przechwytywanie w protokole TCP stanowi większe niebezpieczeństwo niż podszywanie się pod IP, ponieważ po udanym przechwyceniu haker ma na ogół dużo większy dostęp do systemu.

Szukanie słabych punktów systemu — do tego typu należą między innymi ataki, które wykorzystują zarówno autoryzowany dostęp, jak i inne sposoby włamywania się do sieci. Prawdopodobieństwo tego, że haker przypadkowo odkryje jeden ze słabych punktów danego systemu, jest jednak bardzo małe.

Ataki wykorzystujące współużytkowane biblioteki — to ataki, które polegają skupiają się na zasadach działania współużytkowanych bibliotek stosowanych w systemie UNIX. Biblioteka taka zawiera zestaw funkcji, które system operacyjny wczytuje z pliku do pamięci RAM. Hakerzy mogą zastąpić niektóre programy biblioteki, funkcjami wykonującymi inne operacje, które umożliwią na przykład uzyskanie dostępu do sieci. Zabezpieczenie przed takimi atakami jest łatwe — należy regularnie sprawdzać spójność współużytkowanych bibliotek.

Ataki za pomocą apletów — stanowią jeden z najczęstszych sposobów atakowania systemu. Jego specyfika polega na przeprowadzeniu ataku typu „odmowa obsługi". Polega to na utworzeniu apletu, którego uruchomienie przez przeglądarkę będzie powodowało częste zatrzymania systemu, jak np.: Aplet InfiniteThreads.java i Klasa TripleTheat.java.

Ataki korzystające z haseł (PASWORD GUESSING) — są to najchętniej stosowane przez hakerów metody, które polegają na próbie włamania się do systemu przez podanie identyfikatora użytkownika i hasła. Programy takie używają słów zgromadzonych w słowniku i dlatego właśnie są znane pod nazwą *ataków słownikowych*. System Unix jest szczególnie na nie podatny, ponieważ — w odróżnieniu od innych systemów — zezwala użytkownikom na wielokrotne podawanie hasła.

Aby uzyskać dostęp do systemu, hakerzy często próbują rozszyfrować hasła z pliku „passwd" (w tym właśnie pliku, znajdującym się w katalogu [etc] przechowywane są hasła użytkowników). W nowoczesnych wersjach systemów Unix, jak również w jego odmianach, są one „zaciemniane", co oznacza, że hasło używane mieści się gdzie indziej. Ale fakt ten może być tylko problemem hakera-nowicjusza.

Zdarza się nieraz, że włamywacze zdobywają pliki z hasłami wysyłając pocztę kierowaną do portu 25. serwera uniksowego. Nie posiada on bowiem żadnych zabezpieczeń, ponieważ jest używany do rozsyłania poczty elektronicznej w najróżniejsze miejsca. Korzystając z możliwości danych przez ten właśnie port, haker zdobywa zwykle poszukiwany plik z „zaciemnionymi" hasłami (shadowpsswd). Jednak w „surowym" stanie te pliki są bezużyteczne. Znajdujące się w nich hasła są zaszyfrowane w tak skomplikowany sposób, że często okazują się niemożliwe do odczytania za pomocą konwencjonalnych metod. Zatem rozszyfrowanie hasła lub całego pliku z hasłami stanowi cos w rodzaju supergry. Trzeba użyć w tym celu specjalnie napisanych programów, takich jak: *CRACK*, *CRACKERJACK* czy *JOHN THE RIPPER*. Programy te za pomocą specjalnie wygenerowanych tekstowych słowników wyrazowych próbują „odgadnąć" indywidualne hasła użytkowników. Haker-profesjonalista może poszczycić się przynajmniej kilku megabajtowym plikiem słownika. Zaczerpnięte z niego słowa są przez program porównywane z zaszyfrowanymi w pliku z hasłami.

Programy do łamania haseł uniksowych

Poniższe programy są aplikacjami DOS, które bywają wykorzystywane do łamania haseł systemu Unix. Metoda kompilacji, działania i ich uruchamiania oparta jest na podobnym algorytmie: nazwa programu, plik z hasłami (w systemie Unix jest to pliki etc/shadow lub etc/passwd), słownik i — w niektórych przypadkach — docelowe miejsce umieszczania wyników.

- Program FBRUTE

  FBRUTE <password-filename single-password|@password-list-file|*>

FBRUTE single-passwd passlist.txt, gdzie:

- password-filename — plik z hasłami;
- single-password — konkretne hasło do złamania.

Hasło, które ma być złamane nie może być nazwą słownika, czyli: „single-passwd" — „passlist.txt". Zasada ta obowiązuje również w odwrotnej sytuacji. Inny sposób wywołania programu to:

FBRUTE password-filename @passlist.txt, gdzie:

- password-filename — konkretny plik zawierający zakodowane hasła;
- passlist.txt — nazwa słownika;
- znak @ — informacja o tym, że używany jest plik z listą haseł.

Złamane hasła wraz z ich opisem zapisywane są w pliku „pwd_hits.dat" wraz z informacjami nazw użytkowników i haseł. Są to jedyne parametry, gdyż nie ma możliwości podania czasu działania aplikacji, ani ilości przetworzonych haseł.

- Program GUESS

  GUESS [password_file] [[option] [dictionary]]

Opcje:

- a — wykonuje algorytmiczną kontrolę hasła pliku;
- cWORD — odnajduje wyszczególniony wyraz w słowniku;
- sWORD — sprawdza hasło pliku tylko w odniesieniu do wyspecyfikowanego słowa;
- uNAME — ogranicza sprawdzanie słownika do nazwy użytkownika;
- w — pozwala na sprawdzanie za pomocą słownika wszystkich użytkowników.

Po prawidłowym uruchomieniu programu na ekranie pojawiają następujące informacje: nazwa użytkownika, jego hasło, ilość haseł sprawdzanych i czas łamania.

- Program KILLER

  KC
  PWfile: password_file
  Wordfile: dictionary
  Validfile: write_file

Opcje:

- ?, HELP — wyświetla menu;
- INACTIVE — wyświetla i zapisuje nieaktywne sprawozdanie;
- Pwfile:<file> — składa hasła pliku do <pliku> ;
- Quiet — zakazuje każdego wyjścia z stdout;
- Restore: <file> — przywraca sesję używanemu <plikowi> jako zwracanemu plikowi;
- SIngle — czyta plik w formacie „pojednyczy-crack”;
  - STdin — czyta słowa z standardostdin zamiast z „wordfile”;
  - Validfile:<file> — pobiera hasła ze wskazanego pliku;
- Wordfile:<file> — umieszcza wynik w pliku.

W trakcie uruchamiania KILLER-a trzeba wprowadzić nazwę pliku, który zawiera hasła, słownik i nazwę pliku, w jakim później umieszczony będzie wynik. (Wynikiem działania „łamacza” jest plik tekstowy z informacjami na temat ilości przeszukanych haseł, czasie wykonania operacji i oczywiście nazwy właścicieli plików wraz z hasłami).

- JOHN

  JOHN [options][password-files]

Opcje:

- single — włącza tryb „single crack” korzystając z możliwości, które daje [List.Rules:Single];
- wordfile:FILE -stdin — tryb słownikowy, za pomocą którego odczytywane są słowa z pliku lub stdin;
- incremental[:MODE] — włącza tyb incremental używając wyszczególnionej w pliku ~/john.ini definicji (sekcja [Incremental:MODE] lub domyślnie [Incremental:All]);
- external:MODE — tryb external lub filtr słów; włącza tryb external, używając funkcji zdefiniowanych w pliku ~/john.ini’s sekcja [List.External:MODE],
- restore[:FILE] — przywraca przerwaną sesję; kontynuuje przerwaną sesję łamania haseł, odczytuje informacje o punkcie z wyszczególnionego pliku (domyślnie ~/restore);
- session:FILE — ustawia nazwę pliku sesji na określony plik; pozwala określić inny punkt informacyjny nazwy pliku odpowiedni do używania w tej sesji. Jest to użyteczne dla przypadków wielokrotnego użycia programu w podobnych przypadkach lub odzyskiwania starej sesji w późniejszym czasie;
- show — pokazuje rozszyfrowane hasła;

- users:[-]LOGIN|UID[,..] — załadowuje tylko wybranych użytkowników;
- groups:[-]GID[,..] — załadowuje tylko daną powłokę; opcja ta jest użyteczna w przypadku załadowywania konta z ważną powłoką; można pominąć ścieżkę przed powłoką: '-shells:csh' będzie oznaczać'/bin/csh' i '/usr/bin/csh', natomiast: '-shells:/bin/csh' będzie oznaczać tylko powłokę '/bin/csh';
- format:NAME — wymusza format nazwy szyfrowanego tekstu (DES, BSDI, MD5, BF);
- savemem:LEVEL — umożliwia zapisywanie pamięci, na poziomach 1 do 3.

Tryby wywoływane przez opcje:

- Tryb „Listy"

  Jest to najprostszy typ rozszyfrowywania haseł używany przez program: lista słów (plik z jednym słowem w linii) i plik z zaszyfrowanymi hasłami. Program ten nie sortuje listy, by nie zużywać zbyt wiele pamięci, więc sortowanie trzeba wykonać ręcznie (wtedy program pracuje szybciej). Słowa na liście nie powinny być dłuższe niż osiem znaków. Zalecaną drogą sortowania listy jest:

  ```
  tr A-Z a-z < SOURCE | sort -u > TARGET
  ```

- Tryb "Single Crack"

  Jest to tryb, od którego należałoby zacząć pracę nad rozszyfrowywaniem haseł. Używa informacji login/GECOS jako hasła. Tryb „single crack" jest szybszy niż tryb listy. Używa haseł domyślnych, kierując się zasadą, że większość użytkowników ma te same hasła.

- Tryb incremental

  To jest najefektywniejszy sposób łamania haseł. Używa wszystkich możliwych kombinacji znaków jako hasła. Jednak takie rozszyfrowywanie może długo trwać, ponieważ liczba kombinacji jest zbyt duża. Dlatego też używa się okrojonych definicji, które ograniczają liczbę kombinacji.

  Aby wykorzystać ten tryb, potrzeba specjalnych definicji parametrów (parametry są zdefiniowane w pliku ~/john.ini sekcja [Incremental:MODE]). Można używać predefiniowanych definicji trybów inkrementacji ('All', 'Alpha', or 'Digits') lub zdefiniować własną.

- Tryb External

  Tryb ten jest zdefiniowany w pliku ~/john.ini sekcja [List.External:MODE]. Sekcja zawiera pewne funkcje, których program używa do generacji słów.

Podstawowym narzędziem potrzebnym do uruchomienia programu jest plik z hasłami, który trzeba skopiować:

```
unshadow /etc/passwd /etc/shadow > passwd.1
cp /etc/passwd passwd.1
```

Później można rozpocząć łamanie zawartych w nim haseł. Dobrym posunięciem jest rozpoczęcie pracy z trybem „single crack":

```
john -single passwd.1
```

Jeśli istnieje więcej plików, które trzeba rozszyfrować, dobrze jest załadować je w tym samym czasie. Gdy mamy do czynienia ze złożonymi hasłami, lepiej jest użyć silniejszych trybów łamania. Najpierw należy jednak rozszyfrować hasła za pomocą słownika.

```
john -w:words.lst passwd.1
```

lub z włączonymi regułami (metoda wolniejsza lecz bardziej efektywna):

```
john -w:words.lst -rules passwd.1
```

Gdy nie przyniesie to oczekiwanego efektu, warto skorzystać z najsilniejszego trybu łamania, czyli „incremental". Uruchamia się go następująco:

```
john -i passwd.1
```

To wywołanie używa domyślnych parametrów, które są zdefiniowane w pliku ~/john.ini's sekcja [Incremental:All]. W pliku konfiguracyjnym dostarczonym z programem te parametry używają pełnego ustawienia 95-znakowego i próbują złamać wszystkie hasła o długości od 0 do 8. W pewnych przypadkach dobrze jest użyć innych predefiniowanych typów incremental i tylko rozszyfrowywać prostsze hasła o ograniczonej liczbie znaków. Poniższa komenda służyć będzie do łamania haseł składających się najwyżej z dwudziestu sześciu znaków (od „a" do „zzzzzzzz"):

```
john -i:alpha passwd.1
```

Jeśli istnieje plik z hasłami, a większość z nich jest już znana, wtedy można wygenerować nowy plik haseł, bazujący na znakach występujących tylko w tym pliku haseł:

```
john -makechars:custom.chr passwd.1
```

W efekcie tego postępowania część haseł zostaje złamana. Zapisywane są następnie w pliku ~/john.pot, który można wywołać komendą:

```
john -show passwd.1
```

Korzystając z opcji programu możemy:

- sprawdzić, czy hasło roota (uid 0) zostało złamane:

  ```
  john -show -users:0 passwd.1
  ```

- w przypadku, gdy rzecz dotyczyła więcej niż jednego plik z hasłami, stosujemy komendę:

  ```
  john -show -users:0 passwd.*
  ```

- wyświetlić listę roota:

  ```
  john -show -users:root passwd.1
  ```

- sprawdzić, czy hasło roota uprzywilejowanych grup zostało złamane:

  ```
  john -show -groups:0,1 passwd.1
  ```

Roger Safian — ekspert od spraw bezpieczeństwa na Northwestern University — sprawdzał w taki sposób hasła we własnym systemie i osiągał niezłe wyniki. Potrafił ujawnić około 2000 haseł, kont użytkowników w jeden weekend. Wszystko to mógł zrobić dzięki dobrze napisanemu oprogramowaniu i dużemu słownikowi. Często hakerzy wykorzystują słowniki napisane w różnych językach. Dobry program po podłączeniu do niego słownika będzie pracował tak długo, aż zbada wszystkie dostępne związki międzywyrazowe. Użytkownik może mieć tylko nadzieję, że wymyślił takie hasło, które nie zostanie złamane. Aby tak się stało powinien je często zmieniać.

Tworzenie słownika

Użytkownik ma możliwość zdefiniowania słownika za pomocą odpowiedniego programu. Przykładem takiej aplikacji jest program *JILL*. Ogólna zasada działania opiera się na wybraniu jednej pozycji z listy parametrów, po czym podaje się nazwę pliku z zapisanymi wyrażeniami do modyfikacji, a później miejsce docelowego zapisu. Omawiany program pozwala w sposób szybki utworzyć potrzebny zasób słów poprzez zastosowanie permutacji, podstawień, zmian wielkości liter. Tym samym użytkownik oszczędza czas, pozostawiając programowi tworzenie kombinacji i wariacji wyrazów.

Opcje:

- List Conversion — konwertuje słowo, czyli zamienia litery na duże, małe, o mieszanej wielkości, przestawia szyk wyrazu;
- Character Addition — nadaje różny charakter słowom z listy (dodaje znaki, tworzy krótkie słowa będące kombinacją innymi znajdującymi się na liście);
- Number Compiler — liczba kompilacji tworzy listę numerów składającą się z wyszczególnionych początkowych i końcowych numerów;
- Delete Deactivated Accounts — usuwa wszystkie sprawozdania (rachunki, rozliczenia) z listy wyszczególnionych słów;
- Eliminate Short Words — usuwa krótkie słowa z listy, które nie spełniają określonej długości;
- Extract Username — wydobywa odpowiednie nazwy z wyszczególnionej listy słów;
- Deleted Duplicate Words — usuwa powtarzające się wyrazy na podstawie ośmiu porównanych liter (odróżnia małe i duże litery);
- Complite Random List — opracowywuje listę z przypadkowych ciągów znaków i haseł dla wyszczególnionego pliku; opcje dla przypadkowej listy powinny być konfigurowane z odpowiednimi ustawieniami;
- Setup Random List — wykaz opcji, konfiguracji dla skompilowanej dowolnie wygenerowanej listy;
- Exit — wyjście z progaramu.

Reasumując — sieci komputerowe niosą ze sobą ogromną ilość zagrożeń. Walka z nimi nie może sprowadzać się do biernej administracji systemu. Musi to być zorganizowany proces monitoringu ważnych procesów na serwerze, a także regularne konfigurowanie systemu wykonywane pod kątem nowo odkrytych dziur w zabezpieczeniach, instalowanie gotowych lub stworzenie na potrzeby sytuacji odpowiednich programów monitorujących pojawienie się w sieci koni trojańskich czy procesów zakłócających stabilność systemu.

Rodzaje hakowania

Hakerzy — co wielokrotnie już było podkreślane — mogą atakować systemy operacyjne komputerów na wiele sposobów. Mogą oni przechwytywać dowolne transmisje dokonywane przez Internet lub sieć lokalną czy miejską, do której mają dostęp. W dalszej części tego rozdziału przedstawione zostaną specyficzne, tzw. „aktywne" ataki hakerów:

- Najprostszy atak, czyli podsyłanie numerów sekwencji protokołu TCP/IP (Transport Control Protocol/Internet Protocol);
- Największe zagrożenie dla bezpieczeństwa systemów, czyli przechwytywanie sesji TCP (aktywny *sniffing*);
- Węszenie (*sniffing*), czyli obserwacja sposobu, w jaki pakietu „przechodzi" przez sieć, co zwykle poprzedza przechwytywanie danych lub podszywanie się pod innego użytkownika;
- Podszywanie się (*spoofing*), czyli fałszowanie adresów IP, mające na celu udawanie serwera w istniejącym połączeniu sieciowym;
- Kontrola poczty elektronicznej;
- Atak na sesję telnetu;
- Wykrywanie ataków hakerskich;
- Podszywanie się pod hiperłącza w celu zaatakowania instalacji serwera SSL (Secure Socket Layer).

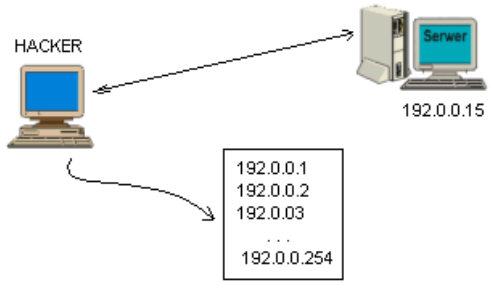
Najprostszy atak hakerski

Kto ma styczność z jakimkolwiek rodzajem sieci wie, że użytkownik, który się do niej zaloguje ma własny adres IP, gdyż do każdego pakietu transmitowanego z komputera podłączonego do sieci automatycznie zostaje dopisany adres IP komputera docelowego oraz unikatowa liczba zwana *numerem sekwencji*. W połączeniu TCP komputer odbierający przyjmuje tylko pakiety z poprawnymi adresami IP i numerami sekwencji. Wiele urządzeń zabezpieczających (w tym rutery) przepuszcza

przez sieć tylko transmisje kierowane do (albo z) komputerów o określonych adresach IP. Atak zwany *podsyłaniem numerów sekwencji TCP/IP* polega na uzyskiwaniu dostępu do Sieci za pomocą reguł określających sposoby adresowania i wymiany pakietu sekwencji.

Haker dokonujący ataku przesyła numer sekwencji TCP/IP ma do wyboru dwie możliwości. Najpierw usiłuje określić adres serwera IP, więc najczęściej analizuje pakiety, które można znaleźć w Internecie, eksperymentuje kolejno z numerami komputerów głównych, łączy się z serwerem poprzez przeglądarkę WWW i szuka adresu IP na pasku stanu. Zwykle wie o tym, że inne komputery w Sieci będą miały adresy IP o częściowo takich samych numerach jak w adresie serwera, dlatego też próbuje symulować numer adresu IP, który umożliwi mu przejście przez ruter i uzyskanie dostępu do systemu tak, jak się to dzieje w przypadku wewnętrznego użytkownika. Jeśli system na przykład ma adres IP 192.0.0.15, to haker, który wie, że do sieci klasy C może być przyłączonych najwyżej 256 komputerów, może próbować odgadnąć wszystkie numery adresów, jakie są określone przez ostatni bajt w serii. Adres IP definiuje również liczbę komputerów przyłączonych do Sieci. W tym wypadku ustawienia dwóch najbardziej znaczących bitów (128+64=192) w pierwszym bajcie oznaczają, że sieć jest klasy C.

Na rysunku przedstawiony jest sposób, w jaki haker może przewidzieć numery wewnątrz sieci klasy C.



Po rozpoczęciu prób z adresami sieciowymi haker przegląda numery sekwencji pakietów przesyłanych pomiędzy komputerami podłączonymi do Sieci. Następnie stara się przewidzieć, jaki będzie następny numer sekwencji wygenerowany przez serwer, a później podszywa się pod ten numer i stara się zająć miejsce pomiędzy serwerem a użytkownikiem. Dysponując również adresem IP serwera, haker może utworzyć pakiety z poprawnymi numerami sekwencji i adresami IP, co pozwala mu na przechwytywanie transmisji użytkownika.

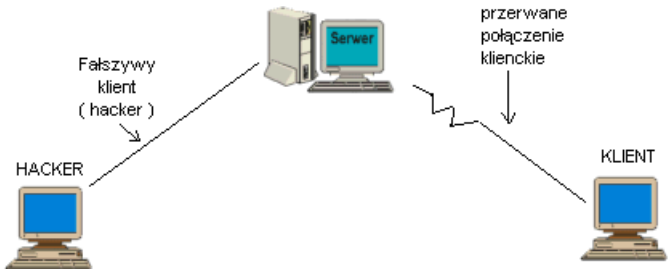
Przechwycenie w protokole TCP

Wielu specjalistów do spraw zabezpieczeń twierdzi, że największym zagrożeniem dla serwerów przyłączonych do Internetu jest przechwytywanie danych w protokole TCP (zwane również *aktywnym węszeniem*).

Chociaż atak ten jest bardzo podobny do podsyłania numerów sekwencji TCP, w tym wypadku haker, zamiast odgadywać adresy IP, uzyskuje dostęp do Sieci wymuszając zaakceptowanie swojego adresu IP jako adresu sieciowego. Idea, na której opiera się przechwycenie w protokole TCP, polega na tym, że haker przejmuje kontrolę nad komputerem łączącym go z Siecią, a następnie go odłącza i „oszukuje" serwer, podając się za użytkownika prawdziwego komputera głównego.

Na rysunku przedstawiony jest sposób, w jaki haker dokonuje przechwycenia w protokole TCP.

Po skutecznym opanowaniu komputera administratora haker zastępuje w każdym pakiecie adres IP komputera docelowego swoim adresem IP, a później podsyła numery sekwencji. Specjaliści do spraw zabezpieczeń nazywają to właśnie symulowanie numeru sekwencji „podszywaniem się pod IP". Robiąc to haker imituje adres IP komputera administratora na swoim własnym komputerze. Po „podszyciu się" pod adres użytkownika komputera docelowego w sprytny sposób podsyła numery sekwencji i staje się celem serwera.



Przechwycenie w protokole TCP jest dla hakera dużo łatwiejsze niż „podszycie się" pod IP. Co więcej — umożliwia mu to ominięcie jednorazowego sprawdzenia hasła (na przykład w systemach korzystających ze wspólnego tajnego hasła), a w efekcie — przejście do komputera głównego, który może mieć lepsze zabezpieczenia. Ominięcie hasła daje hakerowi ponadto sposobność do penetracji systemu operacyjnego innego niż jego bieżący system.

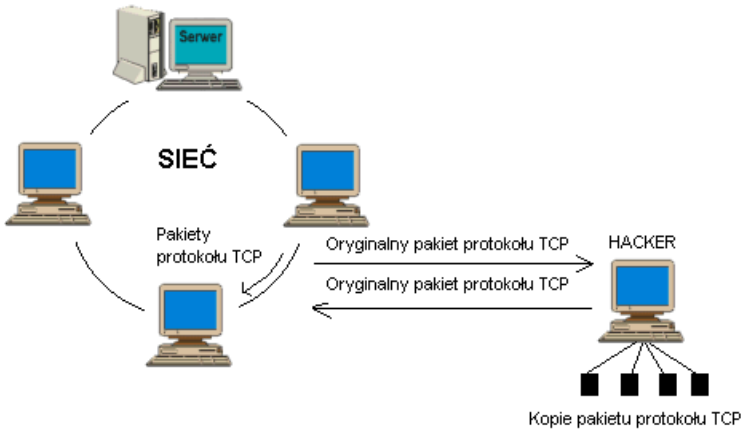
Przechwytywanie w protokole TCP stanowi większe niebezpieczeństwo niż podszywanie się pod IP, ponieważ po udanym ataku haker ma tu na ogół dużo większy dostęp do systemu. Dzieje się tak dlatego, że przechwytuje on odbywające się już transakcje, zamiast rozpoczynać je dopiero po zasymulowaniu komputera.

Węszenie (sniffing)

Ataki polegające na *biernym węszeniu* stały się obecnie bardzo powszechne w Internecie. Są one zazwyczaj wstępem do aktywnego przechwytywania lub podszywania się. Aby rozpocząć „węszenie", włamywacz musi zdobyć identyfikator i hasło legalnego użytkownika i zalogować się do sieci rozproszonej. Następnie zaczyna „węszyć", czyli podglądać i kopiować transmisje pakietów, a tym samym — zdobywać coraz to nowsze informacje.

Aby temu zapobiec, administratorzy systemów rozproszonych zazwyczaj zakładają programy identyfikujące, takie jak system jednorazowego sprawdzania hasła czy system uwiarygodniania biletów (na przykład Kerberos). Mogą oni używać różnych systemów jednorazowego sprawdzania hasła. Niektóre z nich podczas każdego wylogowywania się użytkownika z systemu podają mu na przykład hasło potrzebne do następnego zalogowania się. Chociaż systemy jednorazowego sprawdzania hasła, jak i Kerberos mogą znacznie utrudniać hakerowi „węszenie" w niezabezpieczonej sieci, to jednak metody te nie likwidują zagrożenia aktywnymi atakami, jeśli nie szyfrują ani nie podpisują danych.

Na rysunku przedstawiony jest sposób, w jaki haker może dokonać biernego węszenia.



Po przekierowaniu strumienia danych TCP haker może ominąć zabezpieczenia systemu w postaci jednorazowego sprawdzania hasła lub uwiarygodniania biletów. Połączenie TCP jest praktycznie pozbawione jakiejkolwiek ochrony, gdy haker dysponuje kopią pakietu i generatorem pakietów umieszczonym na linii połączenia. Innymi słowy — dobrze umieszczony podsłuch i generator umożliwia zdobycie wielu pakietów, wśród których mogą się znajdować pakiety przesyłane przez Internet.

Do czego może przydać się sniffer?

Początkowo *sniffery* wykorzystywane były bardzo często przez administratorów poszczególnych sieci w celu wynajdywania usterek. Analizując trasę pakietów można było stwierdzić, na jakie problemy one napotykały, gdzie ginęły itp. Nie

trzeba było długo czekać, by znalazł się ktoś, kto znalazł sposób, by wykorzystać je do własnych potrzeb (np. podglądania cudzej poczty). Obecnie dobry sniffer stanowi bardzo wygodne narzędzie dla hakera. Umieszczony w newralgicznym punkcie Sieci potrafi on zebrać ogromną ilość danych.

Warto podkreślić, że dobry sniffer to taki, który poza samą swą niezawodnością, stabilnością i możliwością konfiguracji posiada także zestaw filtrów, odrzucających wybrane pakiety, a przyjmujących tylko te, na które są istotne. Filtrowanie jest rzeczą bardzo ważną, gdyż ilość danych przepływająca nawet w najmniejszej sieci lokalnej może wynosić (w zależności od aktywności) od kilkuset kb do kilkudziesięciu MB w ciągu minuty (gdy kilka komputerów ściąga jednocześnie dużo danych). Pozostawienie na kilka godzin takiego sniffera, zapewne zapchałoby dysk twardy komputera zupełnie niepotrzebnymi pakietami. Jest wiele takich programów. Jednym z nich jest Sniff ICMP, najprostszy sniffer, który funkcjonuje w systemie operacyjnym Windows 95/98. W zasadzie program przyda się bardziej do analizowania przychodzących sygnałów ICMP, gdyż nie wyłapuje on sygnałów spoza konkretnego komputera. Należy pamiętać o tym, że protokół ICMP odpowiada za przesyłanie komunikatów o działaniu sieci (są to zarówno komunikaty PING, jak i informacje o niedostępności danych hostów). Tak więc ilość zebranych danych siłą rzeczy ograniczy się tylko do tych informacji.

To program prosty w obsłudze. Po uruchomieniu mamy do dyspozycji niewiele opcji:

- *Sur ecoute* — włączenie nasłuchiwania;
- *Signaler une eventuelle attaque* — sygnalizowanie ewentualnych ataków;
- *Enregistrer le log* — włączenie zapisywania logów do pliku *icmp_log.txt* w katalogu, w którym został uruchomiony program;
- *Voir le log* — pokaz zapisanego logu;
- *Reinitialiser* — wyczyszczenie okna z logami;
- *Minimiser* — minimalizowanie okna.

Dobrze jest również zapoznać się z wartościami znajdującymi się w najważniejszych kolumnach okna z logami:

- *Nbre* — ilość identycznych komunikatów wysłanych kolejno (zwykle jest ich kilka, więc kilkaset może oznaczać atak, np. Ping Flood);
- *IP (distant)* — adres IP z jakiego został wysłany komunikat;
- *Port (distant)* — port na zdalnym komputerze, z jakiego został wysłany komunikat;
- *IP (local)* — adres IP odbierającego komputera;
- *Port (local)* — port komputera, na który został wysłany komunikat;
- *Message* — jest to „przetłumaczony” przez program komunikat, jaki trafił (nie przetłumaczony znajduje się w kolumnie *Code*) do odbierającego komputera.

Aktywne rozsynchronizowanie

Połączenie TCP wymaga zsynchronizowanej wymiany pakietów. Jeśli z jakiegoś powodu numery sekwencji pakietu nie zgadzają się z wartościami oczekiwanymi przez komputer, to zostaną one odrzucone i ponownie nastąpi faza oczekiwania na poprawnie numerowany pakiet. Haker może wykorzystać wymagania dotyczące numerów sekwencji protokołów TCP i przechwycić połączenie.

Reasumując — atak polegający na aktywnym rozsynchronizowaniu charakteryzuje się tym, że haker wymusza siłą lub podstępem rozsynchronizowanie dwóch końców połączenia TCP w taki sposób, że komputery te nie mogą wymieniać danych. Następnie haker — używając trzeciego komputera głównego (przyłączonego do fizycznego łącza przesyłającego pakiety TCP) — przechwytuje rzeczywiste pakiety i tworzy ich zamienniki, akceptowane przez oba połączone komputery. Pakiety wygenerowane przez trzeci komputer naśladują pakiety oryginalne, które byłyby wymienione przez połączone systemy.

Przechwycenie po rozsynchronizowaniu

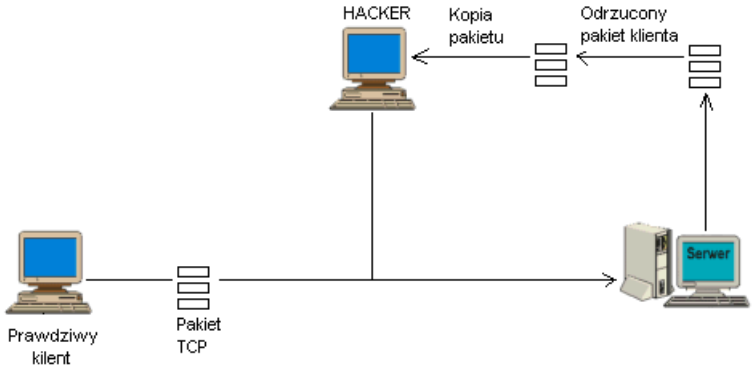
Jeśli założymy, że haker może podejrzeć każdy pakiet wymieniany pomiędzy dwoma komputerami połączonymi protokołem TCP, musimy przyjąć i to, że po przechwyceniu może on podrobić dowolny pakiet IP i zastąpić nim oryginalny. Podrobiony pakiet umożliwia włamywaczowi „udawanie" klienta lub serwera (a wiele podrobionych pakietów umożliwia nawet „udawanie" klienta przed serwerem i na odwrót). Jeśli haker byłby w stanie to zrobić, to mógłby sprawić, że wszystkie transmisje między klientem a serwerem będą się odbywały za jego pośrednictwem.

Przyjmijmy więc, że hakerowi udało się rozsynchronizować sesję TCP i klient wysyła pakiet zawierający w nagłówku następujący kod:

```
SEG_SEQ  =  CLT_SEQ
SEG_ACK  =  CLT_ACK
```

Pierwszy wiersz nagłówka pakietu — `SEG_SEQ = CLT_SEQ` — oznacza, że numer sekwencji pakietu (SEG oznacza segment danych) jest następny w serii klienta. Drugi wiersz — `SEG_ACK = CLT_ACK` — przypisuje wartość potwierdzenia do następnej wartości potwierdzenia. Ponieważ haker rozsynchronizował połączenie TCP, numer sekwencji pakietu klienta (`CLT_SEQ`) nigdy nie będzie równy poprzednio wysłanemu przez serwer potwierdzeniu (`SVR_ACK`) oczekiwanego numeru sekwencji i dlatego serwer nie zaakceptuje danych i odrzuci pakiet. Haker natomiast skopiuje ów pakiet odrzucony przez serwer.

Na rysunku przedstawiona jest sytuacja, w której serwer odrzuca pakiet, a haker go kopiuje.

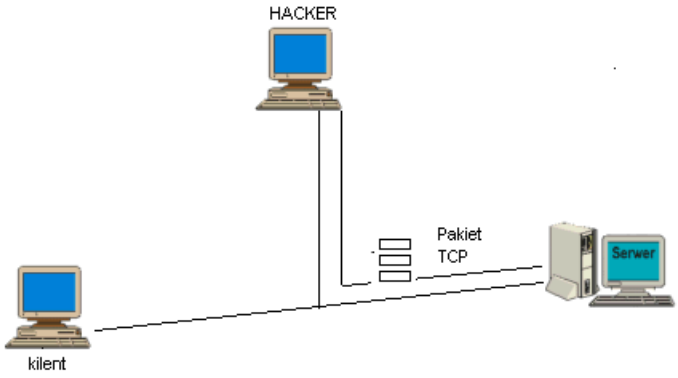


Po niewielkim opóźnieniu, dającym serwerowi czas na odrzucenie pakietu, haker wysyła do niego ponownie ten sam pakiet, co klient, ale ze zmienionymi już poleceniami `SEG_SEQ` i `SEG_ACK` (i zmienioną wartością sumy kontrolnej pakietu). Nagłówek wygląda wtedy następująco:

```
SEG_SEQ = SVR_ACK
SEG _ACK = SVR _SEQ
```

Ponieważ numer sekwencji w nagłówku pakietu jest poprawny (`SVR_ACK` jest równe `SEG_SEQ`), serwer akceptuje nagłówek i pakiet, a następnie przetwarza dane. W tym czasie (zależnie jednak od tego, jak wielu przesłanych pakietów serwer nie zaakceptował) prawdziwy klient może ciągle wysyłać dodatkowe pakiety albo transmitować pakiety `ACK`.

Na poniższym rysunku przedstawiony jest sposób przechwycenia połączenia po wysłaniu przez hakera zmodyfikowanego pakietu TCP.



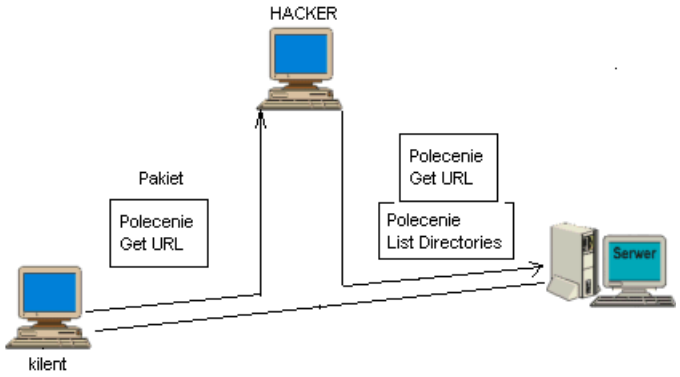
Jeżeli wartość zmiennej `CLT _TO_SVR_OFFSET` zostanie określona jako równa różnicy zmiennych `SVR_ACK` i `CLT_SEQ` (czyli różnicy pomiędzy numerem sekwencji *oczekiwanym* przez serwer i *rzeczywistym* numerem sekwencji klienta), a zmienna `SVR_ TO_CLT_OFFSET` przyjmie wartość równą różnicy zmiennych `CLT_ACK` i `SVR_SEQ` (czyli różnicy pomiędzy numerem sekwencji *oczekiwanym* przez klienta i *rzeczywistym*

numerem sekwencji serwera), to haker musi przepisać pakiet TCP wysłany przez klienta do serwera tak, aby pakiet ten reprezentował wartości `SEG_SEQ` i `SEG_ACK` w następujący sposób:

```
SEG_SEQ = (SEG_SEQ + CLT_TO_SVR_OFFSET) SEG_ACK = (SEG_ACK -
SVR_TO_CLT_OFFSET)
```

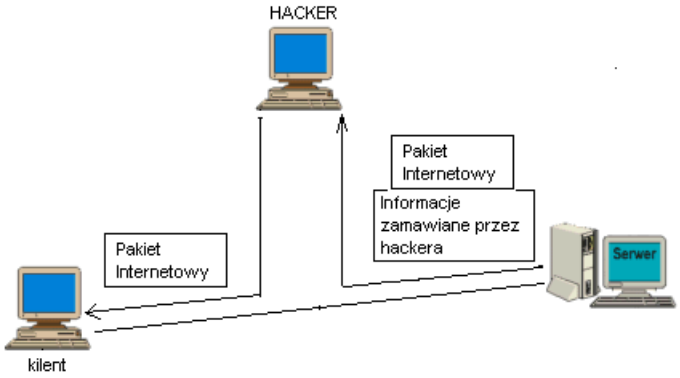
Ponieważ wszystkie transmisje przechodzą przez komputer hakera, może on dodać lub usunąć dowolne dane ze strumienia. Jeśli na przykład połączenie polega na zdalnym zalogowaniu się przy użyciu programu Telnet, haker może wpisać dowolne polecenie w imieniu użytkownika.

Na rysunku przedstawiony jest sposób, w jaki haker dodaje polecenia do strumienia danych przesyłanych od klienta do serwera.



Serwer po otrzymaniu pakietu odpowiada zarówno na polecenia wydane przez hakera, jak i na polecenia wydane przez prawdziwego klienta. Przed przekazaniem odpowiedzi serwera do klienta haker może wyodrębnić i usunąć odpowiedzi na swoje polecenia tak, aby użytkownik nie spostrzegł obecności intruza.

Na rysunku przedstawiony jest sposób, w jaki haker przechwytuje transmisję i usuwa z niej zamawiane wcześniej informacje.

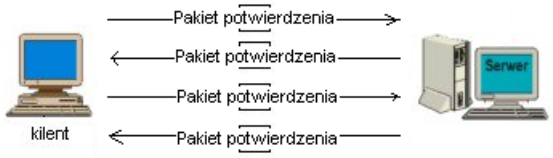


Nawałnica potwierdzeń TCP

Atak sieciowego intruza polegający na rozsynchronizowaniu i przechwytywaniu ma jedną podstawową wadę. Chodzi o to, że produkuje on pakiety TCP ACK w ogromnie dużych ilościach. Specjaliści do spraw bezpieczeństwa Sieci nazywają taką sytuację *nawałnicą potwierdzeń TCP*. Kiedy komputer główny (klient albo serwer) otrzyma pakiet, którego nie może zaakceptować, wówczas potwierdzi jego otrzymanie, gdy wyśle oczekiwany numer sekwencji do nadawcy pakietu.

W wypadku aktywnego ataku hakera, pierwszy pakiet potwierdzenia zawiera własny numer sekwencji serwera. Klient nie akceptuje tego potwierdzenia, ponieważ poprzednio nie wysłał pakietu ze zmodyfikowanym zamówieniem, dlatego tworzy własny pakiet potwierdzenia. To z kolei zmusza serwer do wysłania kolejnego pakietu potwierdzenia i tak dalej. Dla każdego wysyłanego pakietu z danymi powstaje — przynajmniej teoretycznie — nieskończona pętla.

Na poniższym rysunku przedstawiony został proces tworzenia pętli potwierdzeń TCP.



Jako że pakiety potwierdzenia nie zawierają danych, ich nadawca nie wysyła pakietu powtórnie, jeśli odbiorca go utraci. Innymi słowy — pętla kończy się, gdy komputer utraci jeden z pakietów nawałnicy. Na szczęście w zawodnej warstwie sieciowej protokół TCP używa IP. Jeśli tracone są pakiety z danymi, to warstwa sieciowa szybko kończy pętlę. Ponadto im więcej pakietów zostaje utraconych, tym krócej trwa nawałnica potwierdzeń (pętla). Poza tym pętle potwierdzeń są samoregulujące się, co oznacza, że im więcej pętli tworzy haker, tym większy jest natłok pakietów odbieranych przez serwer i klienta, przez co więcej pakietów jest traconych i więcej pętli się przerywa.

Połączenie TCP tworzy pętlę za każdym razem, gdy klient lub serwer wysyła dane. Jeśli ani klient, ani serwer nie wysyła danych, to pętla nie powstanie. Gdy natomiast klient albo serwer wysyła dane, a zabraknie hakera, który by je potwierdzał, nadawca będzie wysyłał dane powtórnie. Następnie połączenie TCP będzie tworzyć nawałnicę dla każdej retransmisji, a w końcu obie strony utracą połączenie, ponieważ ani klient, ani serwer nie wyśle pakietu potwierdzenia. Jeśli haker potwierdza transmisję danych, to połączenie TCP produkuje tylko jedną nawałnicę. W praktyce haker często traci pakiet z danymi z powodu zatłoczenia Sieci i dlatego potwierdza pierwszą z kolejnych retransmisji, co oznacza, że za każdym razem, gdy coś wysyła, atak powoduje utworzenie co najmniej jednej nawałnicy potwierdzeń.

Wczesne rozsynchronizowanie

W przeciwieństwie do ataku przechwytywania, atak wczesnego rozsynchronizowania powoduje przerwanie połączenia między klientem a serwerem we wczesnej (konfiguracyjnej) fazie, a nie dopiero wtedy, gdy połączenie będzie można uznać za zakończone. Rozsynchronizowanie odbywa się po stronie serwera. Tuż po nim haker tworzy nowe połączenie, które posługuje się innym numerem sekwencji. Atak polegający na wczesnym rozsynchronizowaniu przebiega z zachowaniem zasad, które zostały przedstawione poniżej.

1. Haker oczekuje na pakiet potwierdzenia zsynchronizowanego połączenia (`SYN/ACK`), który podczas drugiej fazy transmisji jest zwykle wysyłany do klienta przez serwer.
2. Po wykryciu tego pakietu „intruz" wysyła do serwera pakiet żądania wyzerowania (`RST`), a później — pakiet zsynchronizowanej odpowiedzi (`SYN`) z dokładnie takimi samymi parametrami, które pojawiły się w pakiecie `SYN/ACK` serwera (a przede wszystkim z takim samym portem TCP, przez który ma być synchronizowane połączenie). Jednak pakiet hakera będzie miał inny numer sekwencji. Można go więc uważać za pakiet zerowy potwierdzenia ataku (`ATK_ACK_0`).
3. Po otrzymaniu pakietu `RST` serwer zamyka połączenie, a następnie — po otrzymaniu pakietu `SYN` — otwiera nowe połączenie kontynuowane przez ten sam port, ale już z innym numerem sekwencji (`SVR_SEQ_0`). Do prawdziwego klienta serwer wysyła z powrotem pakiet `SYN/ACK`.
4. Haker przechwytuje tenże pakiet `SYN/ACK` i wysyła do serwera swój własny pakiet `ACK`. Serwer przełącza się w tryb połączenia zsynchronizowanego ESTABLISHED.
5. W momencie gdy klient otrzyma od serwera pierwszy pakiet `SYN/ACK`, jest już przełączony w tryb ESTABLISHED. Powodzenie ataku zależy od tego,
   czy haker wybierze odpowiednią wartość zmiennej `CLT_TO_SVR OFFSET`. Wybranie złej wartości spowoduje odrzucenie obu pakietów — klienta i hakera — oraz wywoła niepożądane efekty, takie jak zawieszenie połączenia.

Rozsynchronizowanie pustymi danymi

Aby rozsynchronizować połączenie TCP, haker może również użyć pustych danych. Terminem *puste dane* określa się dane, które nie będą miały żadnego wpływu na działanie serwera poza tym, że zmienią numer potwierdzenia TCP. Haker wykonuje atak rozsynchronizowania pustymi danymi poprzez równoczesne wysłanie ich dużej ilości do serwera i do komputera-klienta.

Tak przesyłane dane nie są widoczne dla klienta. Powodują jednak przełączenie obu komputerów — które są połączone w trakcie sesji TCP — do stanu rozsynchronizowanego, ponieważ niweczą możliwość utrzymywania połączenia TCP.

Atak na sesję Telnetu

Omówione wcześniej sposoby atakowania nie wyczerpują jednak wszystkich możliwości. Hakerzy mogą psuć dowolne rodzaje połączeń sieciowych. Znają na przykład świetny sposób na przechwytywanie sesji Telnetu. Dzieje się to zgodnie z przytoczonymi poniżej metodami.

1. Przed rozpoczęciem ataku na sesję Telnetu haker biernie przygląda się transmisjom, ale ich nie przerywa.
2. W odpowiednim momencie kieruje jednak do serwera dużą ilość pustych danych. W przechwyconej sesji Telnetu wysyła zmienną `ATK_SVR_OFFSET`, zawierającą rozszerzoną sekwencję bajtów `IAC NOP IAC NOP`. Polecenie `NOP` jest zdefiniowane w protokole Telnet jako „brak operacji". Innymi słowy — zadaniem odbiornika jest ignorowanie bajtów w tej parze. Polecenie to powoduje, że zarządca Telnetu na serwerze interpretuje każdą parę bajtów (`IAC NOP` jest pojedynczą parą bajtów) jako pustą wartość.
3. Kolejnym krokiem zarządcy jest usunięcie ze strumienia każdej parę, którą uważa za pustą. Przyjęcie przez serwer rozszerzonej pustej transmisji powoduje przerwanie sesji Telnetu. Po wykonaniu tej czynności serwer otrzymuje następujące polecenie:
4. SVR_ACK = CLT_SEQ + ATK_SVB_OFFSET
5. Wykonanie przez serwer tego poleceniia powoduje rozsynchronizowanie połączenia w sesji Telnetu.

(Aby rozsynchronizować klienta, haker wykonuje taką samą procedurę jak w wypadku serwera).

Hakerzy przechwytujący sesje Telnetu mogą używać opisanej metody tylko wtedy, gdy sesja zezwala na przenoszenie pustych danych. Ale nawet gdy jest możliwe przenoszenie pustych danych, haker będzie miał trudności z określeniem odpowiedniego do tego momentu. Jeżeli wyśle puste dane w nieodpowiedniej chwili, to taka próba ataku może po prostu przerwać sesję Telnetu lub uszkodzić ją, uniemożliwiając kontrolę nad przekazywaniem danych.

Więcej o nawałnicy potwierdzeń

Podczas połączenia TCP prawie wszystkie pakiety z ustawioną flagą `ACK` — lecz bez dołączonych danych — stanowią potwierdzenia niezaakceptowania. W każdej sieci, a w szczególności w połączeniach internetowych, pojawia się znaczna liczba retransmisji. Jeszcze większa ich ilość występuje w sieci, która została zaatakowana przez hakera jedną z poprzednio opisanych metod. Dodatkowa liczba retransmisji powstaje z powodu zatłoczenia sieci i komputera głównego hakera nawałnicą potwierdzeń.

Raport serwera, który mierzy liczbę pakietów transmisji (w tym wszystkich pakietów ACK), może podczas nawałnicy wywołanej przez pojedynczą próbę ataku, zawierać ponad 3000 pustych pakietów potwierdzeń. Tylko jeden pakiet z danymi, jaki jest wysłany podczas aktywnego ataku, może utworzyć od 10 do 300 pustych pakietów ACK.

Wykrywanie ataków oraz ich efekty uboczne

Wykrywanie stanu rozsynchronizowanego

Numery sekwencji na obu końcach połączenia można odczytać za pomocą czytnika pakietów TCP, czyli specjalnego programu lub urządzenia zliczającego pakiety TCP i wyświetlającego ich zawartość. W zależności od numerów sekwencji można określić, czy połączenie jest w stanie rozsynchronizowanym. Jednak pakiety na obu końcach połączenia można czytać tylko przy założeniu, że numery sekwencji nie są zmieniane przez hakera podczas przesyłania.

Wykrywanie nawałnicy potwierdzeń

Niektóre ustalenia dotyczące ruchu w lokalnym odcinku sieci w połączeniu TCP podają, że przed atakiem średnia liczba pakietów potwierdzeń bez danych stanowi około połowy wszystkich pakietów Telnetu. Bardziej zatłoczona sieć Fast Ethernet ma średnio trzy pakiety Telnetu na każdy pusty pakiet potwierdzenia. Natomiast podczas ataku hakerskiego liczba pakietów potwierdzeń może wzrosnąć nawet do trzystu.

Obliczanie procentu pakietów

Stan połączenia można sprawdzać poprzez obliczanie procentu pakietów. Przez porównanie procentu pakietów podczas ataku z normalnym stosunkiem pakietów zawierających dane przeznaczone dla pakietów potwierdzeń można wykryć atak rozsynchronizowania sieci. W poniższej tabeli przedstawione zostały liczby pakietów zawierających dane i pakietów potwierdzeń transmitowanych w ciągu minuty zwykłego połączenia.

Tabela 1.
Liczba pakietów zawierających dane i pakietów potwierdzeń transmitowanych w ciągu minuty zwykłego połączenia

Typ pakietu	Transmisja w sieci Ethernet	Transmisja Fast Ethernet
Wszystkie pakiety TCP	80-100	1400
Wszystkie pakiety potwierdzeń	25-75	500
Wszystkie pakiety Telnetu	10-20	140
Wszystkie pakiety potwierdzeń Telnetu	5-10	45

Całkowita liczba pakietów TCP (podobnie jak całkowita liczba pakietów potwierdzeń) zmienia się znacznie w sieci lokalnej. Tabela prezentuje więc możliwe zakresy liczby pakietów TCP i pakietów potwierdzeń w sieci lokalnej. Odwrotnie jednak przedstawia się sytuacja w przypadku procentu pakietów potwierdzeń Telnetu, który w normalnym połączeniu jest stały i wynosi około 45%. Fakt, że sesja jest tutaj interakcyjna i serwer musi wywoływać i potwierdzać każdy znak wpisywany przez użytkownika, wyjaśnia stabilność liczby pakietów Telnetu. Objętość wymienianych danych jest mała, ponieważ każdy pakiet zawiera zazwyczaj jeden znak lub jeden wiersz tekstu, co powoduje zmniejszenie objętości traconych pakietów. Analogicznie wygląda przepływ danych w sieci Fast Ethernet. Jest on bardzo stabilny, ponieważ danych jest bardzo dużo, odbierający je komputer główny może utracić kilka pakietów.

Opóźnienie RTD (*Round Trip Delay*) w sesji komunikacyjnej wynosi około 3 milisekundy. Na przykład sesja komunikacyjna pomiędzy klientem a komputerem głównym może przechodzić najwyżej przez cztery serwery, które powinny znajdować się w pobliżu. Jak wynika z podanego zestawienia, zmiana liczby pakietów podczas ataku hakera jest wyraźna. Nawet jeśli różni się ona nieznacznie od całkowitej liczby pakietów, to liczba pakietów potwierdzeń jest prawie równa całkowitej liczbie pakietów. Warto dodać, że prawie cały ruch w sieci odbywa się za sprawą pakietów potwierdzeń, co oznacza, że w efekcie ataku nie przepływają prawie żadne pakiety z danymi.

Zapobieganie przechwyceniu po rozsynchronizowaniu

Program do szyfrowania transmisji Kerberos (znajdujący się w warstwie aplikacji sieciowych) lub kryptograficzna implementacja protokołu TCP (znajdująca się w warstwie transportowej sieci) zapewniają obecnie jedyny możliwy sposób zapobiegania aktywnym atakom wymierzonym w sesje Telnetu. Szyfrowanie strumienia danych wprawdzie nie uniemożliwia podglądania ani modyfikowania zawartości, ale może poważnie ograniczyć zdolność hakera do manipulowania nimi.

Maskarada

Atak o intrygującej nazwie — maskarada, stanowi rodzaj aktywnego węszenia. Polega na tym, że haker, który rozpoczyna sesję, wysyła do serwera zsynchronizowany pakiet (`SYN`) i wykorzystuje adres IP klienta jako adres źródłowy (adres transmitowany przez hakera musi być rozpoznany przez komputer główny). Serwer potwierdza odbiór pakietu SYN za pomocą pakietu potwierdzenia synchronizacji (`SYN/ACK`), zawierającego następujący wiersz:

```
SEG_SEQ = SVR_SEQ_0
```

Następnie haker potwierdza odbiór pakietu serwera `SYN/ACK`, wysyłając swój własny pakiet, który zawiera „odgadniętą” wartość numeru sekwencji (`SVR_SEQ_0`).

Aby odnieść sukces, włamywacz nie musi podglądać pakietów klienta, bo jeśli umie przewidzieć wartość `SVR_SEQ_0`, może potwierdzić ją w ten sposób. Atak typu maskarada ma dwie zasadnicze wady.

Komputer-klient, za który „podaje się" haker, otrzymuje od serwera pakiet SYN/ACK, a następnie tworzy pakiet wyzerowania (RST) i wysyła go do serwera, ponieważ z jego punktu widzenia nie istnieje żadna sesja. Teoretycznie haker mógłby powstrzymać utworzenie pakietu RST przez klienta, wykonując atak wtedy, gdy komputer-klient nie jest przyłączony do sieci lub przepełniając kolejkę jego TCP (poprzez atak podobny do rozsynchronizowania pustymi danymi) tak, aby prawdziwy klient utracił pakiet SYN/ACK wysłany przez serwer.

Haker nie może otrzymać danych od serwera. Jednak ma możliwość wysłania danych, co czasami wystarcza do „zaspokojenia" komputera głównego. Atak typu maskarada różni się zdecydowanie od opisanego wcześniej ataku przechwycenia po rozsynchronizowaniu. Przypomnijmy, że umożliwia on hakerowi przeprowadzenie i kontrolę fazy identyfikacji połączenia, podczas gdy atak typu maskarada opiera się na procedurze identyfikacyjnej przeprowadzonej przez komputer główny. Kolejna różnica polega na tym, że atak przechwycenia po rozsynchronizowaniu daje hakerowi dostęp do dwukierunkowego strumienia TCP, co oznacza, że może on zarówno wysyłać, jak i otrzymywać dane, natomiast w ataku typu maskarada możliwe jest tylko wysyłanie. Ponadto pierwszy z analizowanych ataków sprowadza się do „węszenia" w sieci Ethernet, które umożliwia „zgadnięcie" lub zdobycie wartości `SVR_SEQ_0`. Haker może więc stosować atak przechwycenia po rozsynchronizowaniu względem komputera głównego dowolnego typu. Atak typu maskarada działa tylko w sieciach uniksowych.

Gdy jednak komputer-klient jest rozłączony lub nie ma możliwości odbierania i wysyłania pakietów zerujących (RST), haker może zastosować atak typu maskarada w celu ustanowienia dwukierunkowego połączenia TCP z serwerem. Pozwala mu to na wysyłanie i otrzymywanie danych w imieniu klienta. Oczywiście musi pokonać barierę identyfikacji. Jeżeli w systemie jest używana procedura identyfikacji oparta na zaufaniu (tak jak w sieciowym systemie plików NFS lub jak w wypadku polecenia rlogin w systemie Unix), haker będzie miał pełny dostęp do usług komputera głównego.

Atak przechwycenia po rozsynchronizowaniu jest bardzo łatwy do wykrycia przez administratora systemu wtedy, gdy haker zaatakuje sieć lokalną, ale przeprowadzona na dużą odległość i skierowany w stronę sieci o niskiej szerokości pasma i dużym opóźnieniu (na przykład w sieciach rozległych) okazuje się niebezpieczny. Co więcej — haker może go przeprowadzić za pomocą takich samych zasobów, jakich używa do biernego węszenia. Zarówno przechwycenie po rozsynchronizowaniu, jak i atak typu maskarada są dla hakera bardzo wygodne, ponieważ bywają niewidoczne dla użytkownika.

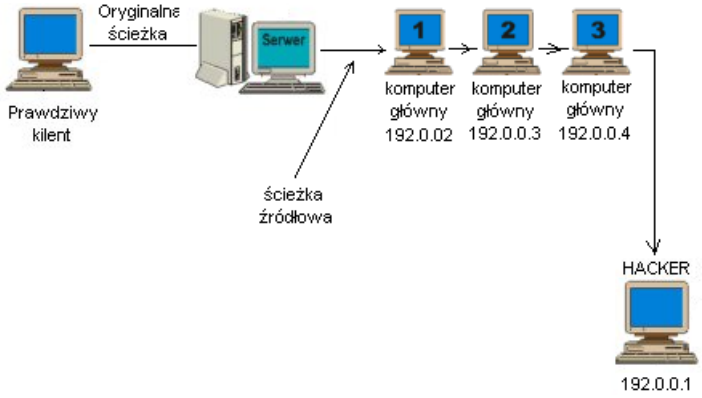
Atak metodą podszywania się (spoofing)

Protokoły TCP (*Transport Control Protocol*) i UDP (*Uniform Datagram Protocol*) działają przy założeniu, że adres protokołu IP (*Internet Protocol*) komputera głównego jest ważny. Jednak haker może przekierować źródłowy adres IP i „podszyć się" pod użytkownika sieci i w ten sposób określić bezpośrednią drogę do miejsca przeznaczenia oraz trasę powrotną. Intruz może więc przechwytywać lub modyfikować transmisje bez zliczania pakietów przeznaczonych dla prawdziwego komputera głównego.

Aby haker mógł podszyć się pod prawdziwego klienta jakiegoś serwera, powinien wykonać następujące polecenia.

1. Haker musi zmienić adres IP atakowanego komputera głównego, aby był zgodny z adresem prawdziwego komputera-klienta.
2. Następnie należy utworzyć ścieżkę źródłową, podającą bezpośrednią trasę, którą pakiety IP powinny przechodzić do serwera i z powrotem do komputera hakera. Jako ostatniego etapu na drodze do serwera trzeba użyć prawdziwego klienta.
3. Później, korzystając ze ścieżki źródłowej, haker powinien wysłać żądanie komputera-klienta do serwera.
4. Serwer zwykle akceptuje żądanie, a następnie wysyła odpowiedź.
5. Prawdziwy klient, korzystając ze ścieżki źródłowej, przesyła pakiet do hakera.
6. Zazwyczaj komputery z systemem operacyjnym Unix akceptują pakiety skierowane do źródła i przesyłają je tam, gdzie wskazuje ścieżka źródłowa. Podobnie zachowuje się wiele ruterów i tylko niektóre z nich można skonfigurować tak, aby blokowały pakiety skierowane do źródła.

Na rysunku przedstawiony został schemat podszywania się hakera pod adres IP.



Łatwiej jednak podszyć się pod klienta w inny sposób. Wystarczy poczekać, aż jego system będzie zamykany i „podszyć" się pod niego. W wielu firmach pracownicy

używają komputerów osobistych i oprogramowania sieciowego TCP/IP do łączenia się i używania komputerów posługujących się systemem Unix jak z serwerów sieci lokalnych. Komputery typu PC często bowiem korzystają z uniksowego sieciowego systemu plików (NFS) do uzyskania dostępu do plików i katalogów serwera (system NFS używa adresów IP tylko do uwiarygodnienia klientów). Haker może podszyć się pod prawdziwego klienta i skonfigurować komputer typu PC tak, aby miał taką samą nazwę i adres IP jak inny komputer, a następnie zainicjować połączenie z uniksowym komputerem głównym. Jest to bardzo łatwe. Co więcej — atak ten będzie prawdopodobnie atakiem „od wewnątrz", ponieważ tylko będąc wewnątrz chronionej sieci można wiedzieć, które komputery są wyłączone.

Poczta elektroniczna — rodzaje hakerskich ataków

Poczta elektroniczna, z której usług skorzystać można w Internecie nie jest dla hakerów trudnym do zdobycia celem. Na ogół nie można ufać wiadomościom, które nie są opatrzone podpisem cyfrowym. Jako przykład wystarczy przeanalizować wymianę e-maili, która odbywa się przy użyciu nieskomplikowanego protokołu, korzystającego z poleceń znakowych zapisanych w systemie ASCII. Napastnik łatwo je może ręcznie zmodyfikować, używając Telnetu do bezpośredniego połączenia z portem protokołu SMTP (*Simple Mail Transfer Protocol*). Odbierający komputer główny „wierzy", że tożsamość nadawcy jest prawdziwa, dzięki czemu haker może łatwo podszyć się pod niego, wpisując adres inny od swojego. W rezultacie każdy użytkownik może sfałszować listy wysyłane pocztą elektroniczną.

Ataki z pochodzące z wewnątrz programu pocztowego

Większość ludzi, którzy korzystają z usług poczty elektronicznej albo nigdy nie widzi rzeczywistego adresu wysłanego e-maila, albo nie wie, jak go odczytać, więc podszywanie się jest tutaj jednym z łatwiejszych ataków hakerskich. Można — a nawet trzeba — stosować odpowiednią profilaktykę. Zatem aby ustawić odpowiednio przeglądarkę Netscape Navigator i sprawdzać podszywanie się w poczcie elektronicznej, należy wykonać poniższe czynności.

1. W oknie Navigatora trzeba wybrać z menu *Options* polecenie *Mail and News/Preferences*. W efekcie Navigator wyświetli okno dialogowe *Preferences*.
2. Następnie należy w oknie dialogowym *Preferences* wyświetlić kartę *Identyfi*, na której powinna znajdować się informacja o pochodzeniu bieżącej wiadomości. Aby zmienić zawartość wiersza *who* w wiadomości, trzeba

przejść do pola *Your Name*, a następnie do pola *E-Mail Address* i wpisać tam coś innego.

3. Później należy wyświetlić kartę *Servers*. Navigator wyświetli okno dialogowe z listą serwerów pocztowych. Podszywając się trzeba usunąć adres serwera poczty przychodzącej (POP3), aby nikt nie mógł wyśledzić adresu nadawcy. Następnie trzeba usunąć zawartość pola *Mail server user name* (pozostanie wtedy tylko pozycja serwera poczty wychodzącej).
4. Teraz wystarczy już tylko nacisnąć przycisk *OK*, aby zamknąć okno dialogowe. Wiadomość jest przygotowana do sfałszowania.

Jedynym sposobem upewnienia się, że wiadomość pochodzi od prawdziwego nadawcy, jest sprawdzenie podpisu cyfrowego. Gdy użytkownik otrzymuje dużą liczbę sfałszowanych wiadomości, często może wyśledzić fałszerza przeglądając informacje zawarte w nagłówku wiadomości, gdyż wskazują one zazwyczaj prawdziwy serwer nadawcy. Znając serwer nadawcy można porozmawiać z administratorem systemu tego serwera i sprawdzić, czy można jakoś powstrzymać nieprzyjaciela przed dalszymi atakami.

Jak wykryć atak metodą podszywania się?

W przeciwieństwie do ataków polegających na rozsynchronizowaniu, podszywanie się pod adresy IP jest trudne do wykrycia. Jeśli serwer internetowy ma możliwość monitorowania ruchu w sieci w zewnętrznym ruterze internetowym, to należy kontrolować przychodzące przez niego dane. Podczas kontrolowania ruchu zapis rutera jest przechowywany w rejestrze systemowym. Korzystając z niego należy sprawdzać, czy wśród przychodzących danych są pakiety zawierające adresy komputera źródłowego i docelowego mieszczące się w obrębie lokalnej domeny. Do sieci nie powinny przychodzić z Internetu pakiety zawierające adresy dwóch komputerów — źródłowego i docelowego. Jeśli znalezione zostaną pakiety zawierające obydwa adresy, to oznacza, że prawdopodobnie jest dokonywany atak polegający na podszywaniu się pod adres IP.

Programy tcdump i netlog

Dwa bezpłatne programy narzędziowe — tcdump i netlog — mogą być pomocne w kontrolowaniu przepływu pakietów w systemie Unix. Pakiet tcdump można pobrać w postaci archiwum */tcdump.tar*, korzystając z protokołu FTP (*File Transfer Protocol*) i logując się jako użytkownik „anonymous" pod adresem – dajmy na to — *ftp.ee.lbl.gov*. Po wczytaniu i zainstalowaniu programu tcdump należy wydrukować wszystkie pakiety znalezione przez tcdump, które mają dwa adresy IP komputerów (źródłowego i docelowego) i są zlokalizowane w sieci domain.name. Można to zrobić wpisując w wierszu poleceń następujące instrukcje:

```
# tcdump src net domain.name <Enter>
# tcdump dst net domain. name <Enter>
```

Oprócz tego można również pobrać pakiet netlog, który został opracowany na uniwersytecie w Teksasie. W tym celu należy za pomocą FTP zalogować się jako użytkownik „anonymous" (np. pod adresem *coast.cs.pnrdue.edu)* i pobrać plik */pub/ools/unix//TAMU/netlog-1.2.tar.gz*. Po wczytaniu i zainstalowaniu programu netlog należy go wywołać następującym poleceniem:

```
# tcplogger -b | extract -U -e 'srcnet=X.Y.O.O && dstnet=X.Y.0.0
{print}' <Enter>
```

Polecenie tcplogger nakazuje programowi netlog wyszukiwanie pakietów z adresami komputera źródłowego i docelowego, które znajdują się w tej samej sieci.

Zapobieganie podszywaniu się

Najlepszą obroną przed podszywaniem się jest filtrowanie pakietów wchodzących przez ruter z Internetu i blokowanie tych, których dane wskazują na to, że powstały w obrębie lokalnej domeny. Cecha filtrowania pakietów (zwana *filtrem wejścia*) jest obsługiwana przez kilka typów ruterów. Są to — między innymi — rutery następujących marek:

- Bay Networks/Wellfleet — wersja 5 oraz nowsze;
- Cabletron z modułem LAN Secure;
- Cisco z oprogramowaniem RIS w wersji 9.21 i nowszym;
- Livingston.

Jeśli obecny ruter nie umożliwia filtrowania wchodzących pakietów, to można zainstalować drugi, który będzie się mieścił pomiędzy już istniejącym ruterem a przyłączeniem do Internetu. Będzie wtedy służył jako filtr sfałszowanych pakietów IP.

Ataki z przechwyceniem sesji

Niektórzy hakerzy przejmują kontrolę nad istniejącymi sesjami systemu za pomocą programu narzędziowego o nazwie *tap*. Narzędzie to umożliwia włamywaczowi, który zdobył uprawnienia użytkownika root (czyli dostęp do systemu na poziomie administratora), przejęcie kontroli nad każdą aktywną sesją w systemie i wykonywanie poleceń tak, jakby były wpisane przez właściciela sesji. Jeżeli użytkownik wykonywał w sesji przejście do innego komputera za pomocą Telnetu lub polecenia `rlogin`, haker może również zdobyć zdalny dostęp do tego komputera, omijając zazwyczaj konieczną do tego procedurę uwiarygodniania. Program *tap* działa obecnie tylko na komputerach z zainstalowanym systemem SunOS.

Wykrywanie przechwyconych sesji

Właściciel przechwyconej sesji (ofiara przechwycenia) zwykle zauważa niezwykłą aktywność komputera (w tym pojawianie się poleceń wpisywanych przez hakera), a czasami także utratę połączenia. Administrator powinien powiadomić użytkowników systemu o niebezpieczeństwie przechwytywania, a także zachęcić ich do zgłaszania uwag związanych z podejrzanym działaniem komputera.

Zapobieganie przechwytywaniu sesji

Główną metodą obrony przed przechwytywaniem sesji jest odpowiedzialne zarządzanie systemem, które często sprowadza się do instalowania rozmaitych zabezpieczeń w programach, a także systemów kontroli dostępu do sieci, takich jak *zapory ogniowe (firewall)*. Obecnie używane narzędzie tap ma cechę wspomagającą moduły ładowalne SunOS, która umożliwia dynamiczne modyfikowanie kolejnych operacji systemu Unix. Departament CIAC (*U.S. Department of Energy's Computer Incident Advisory Capability*) zaleca, aby sieci, które nie wymagają modułów ładowalnych, nie uaktywniały tej cechy w swoich systemach SunOS. Jeśli użytkownicy nie potrzebują modułów ładowalnych, mogą łatwo wyłączyć tę cechę.

Podszywanie się pod hiperłącza — atak na weryfikację serwera SSL

Innym sposobem zdobycia kontroli nad zdalnym systemem jest podszywanie się pod hiperłącza. Stanowi to powszechnie stosowany przez hakerów rodzaj ataku wymierzonego w komputery komunikujące się przy użyciu protokołu HTTP. Hakerzy mogą atakować protokół weryfikacji serwera SSL (*Secure Socket Layer*), który jest używany przy tworzeniu bezpiecznych przeglądarek internetowych i serwerów (produkowanych na przykład przez firmy Microsoft lub Netscape). W tym przypadku haker może spowodować połączenie przeglądarki z fałszywym serwerem. Następnie „zmusza" on użytkownika do przesłania do fałszywego serwera danych (np. numerów kart kredytowych, numerów identyfikacyjnych, szczegółów dotyczących ubezpieczeń i bankowości lub innych prywatnych informacji).

Innym ryzykiem związanym z podszywaniem się pod hiperłącza jest to, że użytkownik (na przykład klient banku lub bazy danych) może pobrać z fałszywego serwera i uruchomić złe aplikacje napisane w języku Java, sądząc, że pochodzą one z prawdziwego serwera i są bezpieczne.

Należy zauważyć, że podszywanie się pod hiperłącza wykorzystuje to, że większość przeglądarek zabezpiecza sesje internetowe za pomocą certyfikatów cyfrowych. Podszywanie się pod hiperłącza nie dotyczy kryptografii niskiego poziomu ani działania

samego protokołu SSL. W konsekwencji atak może być również skierowany przeciw innym aplikacjom zabezpieczonym certyfikatami, w zależności od tego, w jaki sposób certyfikaty te są używane.

Przeglądarki Internet Explorer 3.0x Microsoftu, Netscape Navigator 3.0 i Netscape Navigator 4.0 są bardzo podatne na ataki podszywania się pod hiperłącza. Możliwe też, że atak taki może mieć wpływ na inne przeglądarki oraz na typowe protokoły zastępujące SSL. Podszywanie się pod hiperłącza nie dotyczy jednak takich technik, jak „podpisywanie kodów" lub „podpisywanie apletów", które również korzystają z certyfikatów.

Haker może podszywać się pod dowolny serwer oznaczony jako SSL, spełniając zwykłe procedury certyfikacyjne lub uzyskując dostęp do wymienionych wcześniej przeglądarek. Co więcej — niektóre certyfikaty serwerów (np. Verisign lub Thawte) są podatne na ataki podszywania się pod hiperłącza, jeśli używana jest przeglądarka Netscape Navigator lub Internet Explorer. Szansa powodzenia ataku może być ograniczona przez pewne modyfikacje dokonane w oprogramowaniu serwera. Jednak najlepszym i długotrwałym rozwiązaniem jest prawdopodobnie modyfikacja zarówno zawartości certyfikatu, jak i przeglądarki internetowej. Podszywanie się pod hiperłącza nie ma wpływu na certyfikaty komputerów-klientów, na certyfikaty używane przez serwery do kodowania (takie jak formanty ActiveX) ani na podpisywanie aplikacji w języku Java.

Źródła ataku

Podczas połączenia SSL przeglądarka i serwer wspólnie korzystają z protokołu, dokonując weryfikacji serwera i (opcjonalnie) klienta. Haker, który atak podszywając się pod hiperłącze, koncentruje się jednak na weryfikacji serwera. Podczas pierwszej wymiany protokołu SSL serwer podaje przeglądarce swój certyfikat. Jest to podpisana cyfrowo struktura, przypisująca klucz publiczny serwera do pewnych atrybutów.

Obecnie w certyfikacie protokołu SSL używana jest nazwa serwera DNS (*Domain Name Server*). Zamiast pełnej nazwy DNS certyfikat może też zawierać wieloznaczniki (może na przykład czytać nazwę *www.brd.ie* albo **.brd.ie)*. Poprzez poprawne przetransportowanie protokołu i przedstawienie komputerowi-klientowi ważnego certyfikatu, serwer „przekonuje" przeglądarkę, że ma odpowiedni klucz prywatny (znany tylko serwerowi). Przeglądarka akceptuje ten dowód i jest przekonana, że serwer naprawdę ma podaną nazwę DNS lub prawo do używania jej. Należy zauważyć, że dla ataku podszywania się pod hiperłącze protokół SSL nie stanowi problemu. Zasadniczą kwestią jest natomiast zawartość certyfikatu oraz interfejs użytkownika przeglądarki.

Przebieg

Atak podszywania się pod hiperłącze udaje się zwykle, ponieważ większość użytkowników nie zamawia połączenia poprzez serwer DNS lub adres URL, ale korzysta głównie z hiperłączy. Obecne zastosowanie SSL weryfikuje tylko część adresu URL serwera, a nie hiperłącze.

Podobnie jak nazwa DNS jest przedmiotem ataków „podszywania się pod DNS" (serwer DNS podaje fałszywe informacje na temat adresu internetowego), adresy URL są celem podszywania się pod hiperłącza, polegającego na tym, że strona podaje fałszywe informacje na temat nazwy DNS adresu URL. Obie formy podszywania się powodują przejście użytkownika na złą stronę internetową. Jednak podszywanie się pod hiperłącza technicznie jest dużo łatwiejsze od podszywania się pod DNS. Na przykład haker może podać przeglądarce następujący kod w języku HTML:

```
<A HREF=https://www.haker.com/infogather/>This way to a free
books!</A>
```

Użytkownik zobaczy stronę z odsyłaczem, który wyświetla tekst: „*This way to a free books*!". Ale jeśli kliknie w tym miejscu, przeniesie się do innego bezpiecznego serwera (w domenie *haker.com*), do katalogu o nazwie *infogatherer*. Dzisiejsze przeglądarki sprawdzają, czy połączenie jest bezpieczne, pokazują nawet stałe klucze, niemniej jednak haker po prostu się podszywa. Korzysta on z pewnych sztuczek polecając przeglądarce, aby pokazywała użytkownikowi prywatne połączenie z żądanym serwerem.

Jest to prywatne połączenie z niewłaściwym serwerem. Na stronie infogatherer nie będzie żadnych darmowych książek, ale w prawdziwym ataku haker mógłby tę stronę imitować i sprawić, że będzie wyglądała tak, jak autentyczna strona internetowa. Jednak gdyby użytkownik przeszukał dokładniej menu swojej przeglądarki i obejrzał źródła dokumentów lub informacje o nich, to zauważyłby, że zweryfikowana tożsamość serwera różni się od tej, której się spodziewał.

W miarę jak używanie certyfikatów rozpowszechnia się, pokonywanie weryfikacji serwera staje się coraz łatwiejsze, a nie trudniejsze. Gdy coraz więcej serwerów ma certyfikaty, hakerzy mają większy wybór stron, do których mogą przekierowywać nieostrożnych podróżników po Internecie. Jeśli każde połączenie i dokument jest bezpieczny, to wiedza, że zamówiło się bezpieczny dokument, nie jest szczególnie pomocna, gdyż weryfikowanie połączenia serwera staje się bez znaczenia.

Pomimo skomplikowanej weryfikacji, nie istnieje żaden ślad kontrolny, który wskazałby użytkownikowi, co się dzieje podczas podszywania się pod hiperłącza. W najlepszym razie rejestr przeglądarki może pokazać, że wpisane było polecenie `HTTP` (lub `HTTPS`) `GET` (dla prawdziwego serwera), a następnie polecenie `HTTPS GET` (dla fałszywego serwera). W szczęśliwym wypadku w lokalnej pamięci podręcznej może być przechowywana odwiedzona strona (haker może ją stamtąd wydobyć za pomocą polecenia `PRAGMA`). Podczas ataku podszywania się drugie pole-

cenie GET pojawia się, ponieważ pierwsze zwraca niepoprawny lub zmieniony wynik.

Niestety nie można udowodnić (nawet z najlepszymi rejestrami), że drugie polecenie GET zostało zainicjowane przez zdalnie połączoną stronę. Użytkownik mógł przechodzić na ulubione strony lub do innego okna i podać polecenie GET. Nawet w sytuacji, gdy użytkownik udowodni, że tego nie robił, oszukańcza strona może zniknąć z pamięci podręcznej (włącznie z sąsiednimi pamięciami ISP) lub z pierwszego polecenia GET. Można podejrzewać, że fałszywa strona należy do hakera, ale nie da się tego udowodnić.

Haker nie zamierza jednak wysyłać użytkownika na swoją bezpieczną stronę, gdyż tym samym dałby mu swój certyfikat i trop do zidentyfikowania tożsamości. Może więc wysłać użytkownika do czyjejś skrzynki SSL, do jakiej się włamał, lub do innego miejsca w bezpiecznej domenie, do której użytkownik chciał się dostać. Innymi słowy — adres URL może mieć postać */attackpage* zamiast */securepage.* Ten rodzaj przekierowania może pojawić się na wirtualnie zarządzanych stronach internetowych lub na stronach, których adresy URL reprezentują skrypty CGI (*Common Gateway Interface*) lub Javy, z których część haker legalnie kontroluje.

Kolejno przedstawiane informacje zostały zaczerpnięte z następujących stron internetowych :

- Podszywanie się pod DNS i Java*:* http://java.sun.com/sfaq/dns.html;
- Podszywanie się pod IP: *http://sunshine.nextra.ro/route-conf.html*;
- Przykład podszywania się pod hiperłącze: *http://www.brd.ie/papers/sslpaper/hyperlin.html*;
- Archiwum BugTraq: http://www.geekgirl.com/bugtraq/1995_1/0128.html;
- Strona podszywania się EMV: *http://www.coast.net/~emv/tubed/spoofing.html*;
- CIAC*: http://ciac.llnl.gov/ciac/bulletins/g-48.shtml*;
- Podszywanie się w WWW: *http://www.cs.princeton.edu/sip/pub/spoofing.html*;
- Podglądanie IP: *http://www.engarde.com/software/ipwatcher/risks/overview.html*;
- Podszywanie się i „węszenie”: *http://ori.careerexpo.com/pub/docsoft197/spoof.soft.html*;
- „Węszenie” haseł: *http://gradeswww.acns.nwu.edu/ist/snap/doc/Sniffing.html.*

Inżynieria społeczna — Social Enginering

Inżynieria społeczna wykorzystywana przez hakerów sprowadza się do stosowania rozmaitych metod kierowania ludźmi. Przeważnie manipulowanie odbywa się w ten sposób, aby haker mógł uzyskać informacje lub jakiś rodzaj dostępu do systemu. To jest wielka umiejętność wśród hakerów i bardzo dla nich użyteczna. Zamiast wyprawiać rozliczne „sztuczki" z Unixem, pyta on ludzi o ich hasła, a robi to oczywiście w odpowiedni sposób. To zdumiewające, jak wielka ilość różnych informacji może się pojawić w trakcie konwersacji.

Istnieją dwie drogi uzyskania nieuprawnionego dostępu do serwera. Pierwsza z nich — tradycyjna — osiąga cel przez programowe złamanie kodów lub przechwycenie haseł użytkowników. Druga natomiast ważna staje się wtedy, gdy nasze możliwości są zbyt małe. Cóż robimy w takiej sytuacji? Otóż możemy spróbować zrobić to, co chcemy, ale startując „z innej strony". Podstawowe założenia metody określanej jako inżynieria społeczna opierają się na tym, że na każdym serwerze znajdują się użytkownicy, którzy nie zdają sobie do końca sprawy z tego, jak trudno się na taki serwer dostać. Słowem — nie ma serwerów stuprocentowo bezpiecznych.

Inżynierią społeczną nazywa się wszystkie metody wykorzystywanie nieświadomości, niewiedzy czy po prostu niekompetencji osób posiadających bezpośredni dostęp do informacji o charakterze zastrzeżonym. Uzasadnienie znajduje w postawionym niegdyś pytaniu retorycznym:

„Po co marnować całe godziny na zgadywanie hasła otwierającego system komputerowy jakiejś korporacji, skoro można zadzwonić do jednego z administratorów, podać się za szefa jego szefa i zmusić go, by podał to hasło?"

Haker i Samuraj, Jeff Goodell, s. 29.

Najważniejszą z zaliczanych tu metod jest próba odgadnięcia hasła. Wymaga ona najmniej wiedzy, ale za to trzeba mieć dużo czasu i cierpliwości. Wbrew pozorom nie polega ona nie beznadziejnym wpisywaniu kolejnych kombinacji cyfrowych, lecz na wybraniu jednego konkretnego administratora lub użytkownika, na poznaniu jego upodobań i uporządkowaniu ich na podstawie zdobytej wiedzy. Dopiero wtedy można podjąć próbę odgadnięcia jego hasła. Jest to możliwe.

*Wady — c*zas trwania procesu, niepewność, zrywanie połączenia po kilkakrotnej nieudanej próbie (nowe wersje niektórych systemów operacyjnych mają wbudowane mechanizmy blokujące konto po kilku następujących po sobie nieudanych procesach logowania).

Zalety — duża, praktycznie stuprocentowa, anonimowość i możliwość szybkiego rozwiązania.

Zabezpieczenia — posługiwanie się hasłami generowanymi przez system lub takimi, które trudno powiązać z właścicielem konta pocztowego.

Uwagi — przed podjęciem decyzji dotyczącej ataku haker musi zorientować się, na jaki serwer zamierza się włamać, z jakim systemem operacyjnym przyjdzie mu się zmierzyć i trafnie dobrać użytkownika, którego będzie musiał rozpracować.

„Oczywiście, żeby się to udało, musi być naprawdę dobry. Władczy, niecierpliwy i kompetentny. Musi znać imię asystenta szefa. Musi znać język wewnętrzny przedsiębiorstwa. Musi znać procedury. Musi mieć umiejętności gryftera, oszusta."

Haker i Samuraj, Jeff Goodell, s. 29.

Najbardziej typowy i najczęściej stosowany sposób, jest ciągle pociągający. Często w celu uzyskania hasła haker wykorzystuje swoich znajomych.

Zalety — anonimowość, szybkość działania, niska wykrywalność przecieku, gdyż pracownik nigdy się nie przyzna, że zdradził tajemnicę firmy.

Wady — trzeba stosować odpowiednie, czasem wyrafinowane sposoby, bo inaczej metoda się nie powiedzie.

Uwagi — jeżeli haker chce mieć pewność, że metoda zadziała, powinien wykorzystywać wszelkie metody zdobywania informacji, nie gardząc nawet przeszukiwaniem śmieci, których pozbywa się firma, gdyż i tam mogą się znaleźć niezbędne dokumenty, które pozwolą mu lepiej zrozumieć sytuację.

„Kiedyś na przykład Kevin Mitnick próbował dostać się do komputera marki Digital Equipment. Był to mały interes na dwie, trzy osoby. (...)Wraz z kolegami zainstalowali oprogramowanie wyglądające jak rutynowy upgrade stosowanego wówczas przez Digital programu, ale zawierające tajny kod pozwalający na wejście do komputera „tylnymi drzwiami". Starannie opakowali swój program w pudełko Digitala, dołączyli autentyczną metkę pakowacza z Digitala, oprawioną w plastyk, i dostarczyli do przedsiębiorstwa."

Haker i Samuraj, Jeff Goodell, s. 29.

Jak widać rożne są metody hakerskich ataków. Może to być nawet dobry trojan, niekoniecznie przez siebie napisany, firmowe pudełko po oryginalnym produkcie i etykietka w stylu — „do Internet Explorera w prezencie od firmy Microsoft". Można to dostarczyć pocztą i system należy już do hakera.

Zalety — duże prawdopodobieństwo powodzenia.

Wady — długi czas oczekiwania na efekty, wysoka odpowiedzialność za oszustwa pocztowe.

Uwagi — konieczna jest to, by zadbać o szczegóły.

Jeżeli haker chce zdobyć zaufanie nieświadomego tego użytkownika, postępuje według pewnych zasad:

- *Jest cierpliwy* — udaje, że mu nie zależy i nawet gdy uda się przesłać plik, nie każe mu od razu go uruchamiać;
- *Jest miły* — nawet gdy rozmówca myśli, że jest wielkim hakerem, to albo udaje on lamera, albo — jeszcze lepiej — innego hakera; prowadzi rozmowę skomplikowanym, elitarnym językiem, a kiedy interlokutor powie, że nie jest zainteresowany nową ofertą, haker proponuje mu np. exploita albo NetBusa „na odległość, bez przesyłania pliku";
- Stara się trafić w upodobania ofiary;
- Nie jest nachalny;
- Gdy ofiara wygląda na uległą, wręcz narzuca się z rozmaitymi propozycjami;
- Nie próbuje przekupstwa;
- Udaje, że jest mniej więcej na tym samym poziomie co ofiara;
- Stara się pozyskać wdzięczność ofiary;
- Pamięta o tym, że nawet gdy otrzyma już to, czego chciał, nie jest to ostatni kontakt z ofiarą.

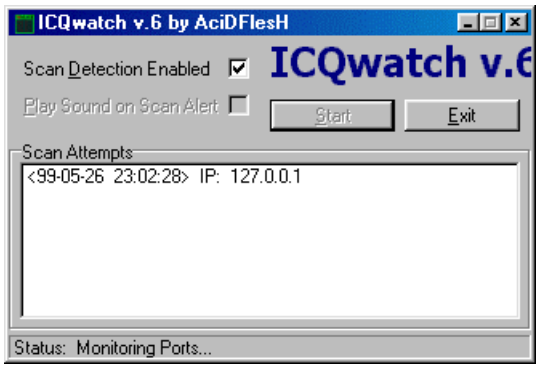
Nowsze i starsze sposoby hakerskich ataków

Równolegle z nowymi technikami w dziedzinie komunikacji powstają nowe sposoby i formy ataków. Odpowiedzią na to są powstające kolejno systemy zabezpieczeń, które — nie dajmy się oszukać — tylko na pewien czas prawidłowo spełniają swoją funkcję. Gdyby jedna z dziedzin — czy to atak, czy ochrona — nieco przeważyła szalę, prawdopodobnie zaraz potem wyeliminowałaby drugą. Obie te rzeczy niczym tryby w wielkim mechanizmie napędzają same siebie, stosując coraz to bardziej wyrafinowane rozwiązania. Łatwo to sobie wyobrazić — gdyby powstał tak idealny atak, który łamałby wszystkie systemy, to system zabezpieczeń wypadłby z gry. Ale powstanie sprawnego system przeciwko włamywaczom równie łatwo wyeliminowałoby każdy atak i hakerstwo — z braku skuteczności — odeszłoby w zapomnienie. Przedstawione niżej programy wprawdzie nie mają takich ambicji, jednak zmniejszają zdecydowanie podatność na atak.

ICQWatch 0.6

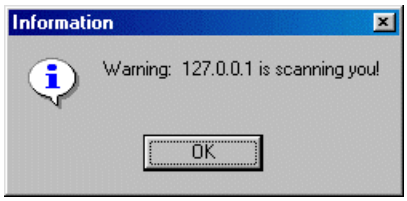
Mimo kilku zasadniczych wad jest to ciekawy program utrudniający programom skanującym znalezienie niektórych ważnych portów.

A oto jego interface:



Jak działa ów program?

Jego głównym założeniem jest ochrona programu ICQ 98 przed atakami prowadzonymi przez otwarty port. Wystarczy kliknąć *Start* i program zaczyna „nasłuchiwać". W tym celu otwiera on kilka lub kilkanaście podobnych portów, by zmniejszyć ryzyko, że ktoś zaatakuje ten właściwy. Oczywiście jeśli ktoś się uprze to zaatakuje każdy otwarty port i koniec końców atak dojdzie tam, gdzie ma dojść. Jednak można zaoszczędzić na tym trochę czasu, a o ile skaner natrafi na jeden z otwartych przez program portów (gdy będzie włączona opcja Scan Detection Enabled) pojawi się komunikat:



Wskazuje on IP, spod którego nastąpiło skanowanie. Ta informacja, o ile adres IP skanującego nie został sfałszowany, będzie informacją o tym, kto przygotowuje się do ewentualnego ataku. Mając świadomość tego, że coś nie jest dokładnie tak, jak powinno być, można wyłączyć ICQ lub ustawić tryb OFFLINE. W tym przypadku zamknięty zostanie prawdziwy port ICQ i nikt nie będzie miał dostepu do tego kanału. Można również zignorować całą tę sytuację, wiedząc, że jest to na przykład adres naszego dobrego kumpla albo odwrócić role i zamienić się w atakującego. W tym celu należy uruchomić skaner i zeskanować podany adres.

Nie jest wykluczone, że włamywacz także korzysta z ICQ 98 i efektem może być wysłanie tysiąca kopii z informacją: „Sorry kolego, musisz się jeszcze poduczyć".

Zalety programu

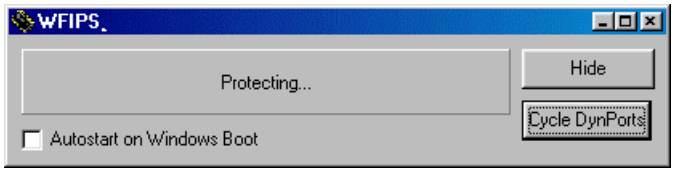
W przeciwieństwie do wielu innych programów tego typu, program nie zamyka momentalnie zeskanowanego wirtualnego portu, dzięki czemu (np. podczas skanowania programem 7th Sphere Port Scan) trudniej jest rozróżnić, który port jest tym

prawdziwym, jakim posługuje się ICQ. Jest to ciekawa właściwość i zapewne dawałoby to dosyć dobre zabezpieczenie, gdyby nie fakt, że otwierane porty są często zlokalizowane „za nisko". Praktycznie znaleźć je można na wysokości od 1024 do około 1215, z czego ICQ pracuje na wysokości mniej więcej od 1024 do 10000. I jeżeli nawet ktoś znajdzie wirtualne porty, przy czym jeden na znacznie wyższej wysokości, to od razu zrozumie, który jest prawdziwy. Gdy pojawi się więc okienko z komunikatem o skanowaniu naszego komputera, trzeba jak najszybciej wcisnąć OK, gdyż dopiero wtedy zostanie pobrane IP intruza. Jeżeli proces skanowania zakończy się wcześniej i intruz „wyjdzie" z portów — otrzymamy jedynie komunikat:

```
<99-05-27 22:22:22> IP: error
```

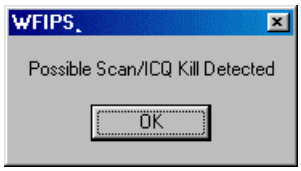
WFIPS

To kolejny program do zabezpieczania portów w ICQ. O ile sama idea ochrony jest taka sama (otwieranie wirtualnych portów), o tyle jest ona zrealizowana w nieco inny sposób. Inny jest także wygląd:



Program jest o tyle wygodniejszy, że można włączyć opcję *Hide*, dzięki której nie trzeba ciągle oglądać tego samego okienka, a przy włączonej dodatkowej opcji *Autostart on Windows Boot*, program będzie się uruchamiał automatycznie przy każdym uruchomieniu Windows.

Program ten — podobnie jak ICQWatch — otwiera kilkanaście losowych portów, ale robi to w nieco większym zakresie: od 1024 do mniej więcej 2200. W przypadku skanowania pojawia się komunikat:



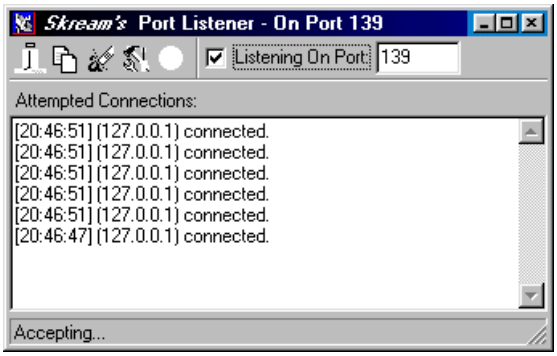
Jak widać, program nie ujawnia adresu IP skanującego, ale w przypadku jednoczesnego korzystania z ICQWatch nie będzie to miało większego znaczenia. pojedynczo nie zapewnia aż tak dobrej ochrony, chyba że ktoś użyje kiepskiego skanera lub programu, który „próbuje się włamać" do pierwszego napotkanego otwartego portu. Ciekawym rozwiązaniem programu jest także to, że za pomocą kliknięcia *Cycle DynPorts*, można poprzestawiać nowo otwarte porty, co uniemożliwia namierzenie nawet portów wirtualnych.

Program posiada pewne wady, ale mimo to z powodzeniem utrudni atak niejednego lamera.

Skream's Port Listener 2.3

Działania hakerów mogą przyjmować rozmaite formy. Jedną z nich jest analiza zainstalowanych na twardych dyskach systemów przyłączonych do Sieci komputerów, która sprowadza się do ujawnienia połączeń z serwerami FTP, Fingera, Telnetu itp. Jako że używają one tych samych portów, obrona przed penetracją niepożądanych gości jest bardzo łatwa.

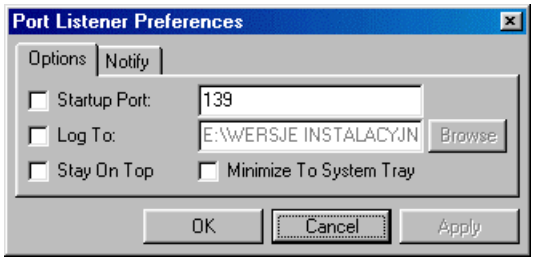
Nie trzeba wystawiać wielu — by posłużyć się kolokwializmem — „czujek", lecz wystarczy skupić się na ochronie jednego punktu. Do tego właśnie służy program Skream's Port Listener:



Aby zabezpieczyć port, wystarczy wpisać jego numer do okienka widocznego na pasku zadań i kliknąć *Listening On Port*. Od tej pory wszelkie odwołania się do wpisanego portu będą rejestrowane wraz z numerem IP i godziną ataku. Jest to bardzo przydatna opcja.

Program dysponuje jeszcze kilkoma opcjami (w oknie reprezentują je odpowiednie ikony), które umożliwiają wyjście, kopiowanie zawartości okna do bufora, konfigurację oraz wyświetlenie niezbędnych informacji o programie.

Przyjrzyjmy się dokładniej opcjom konfiguracji. Znajdziemy tu:



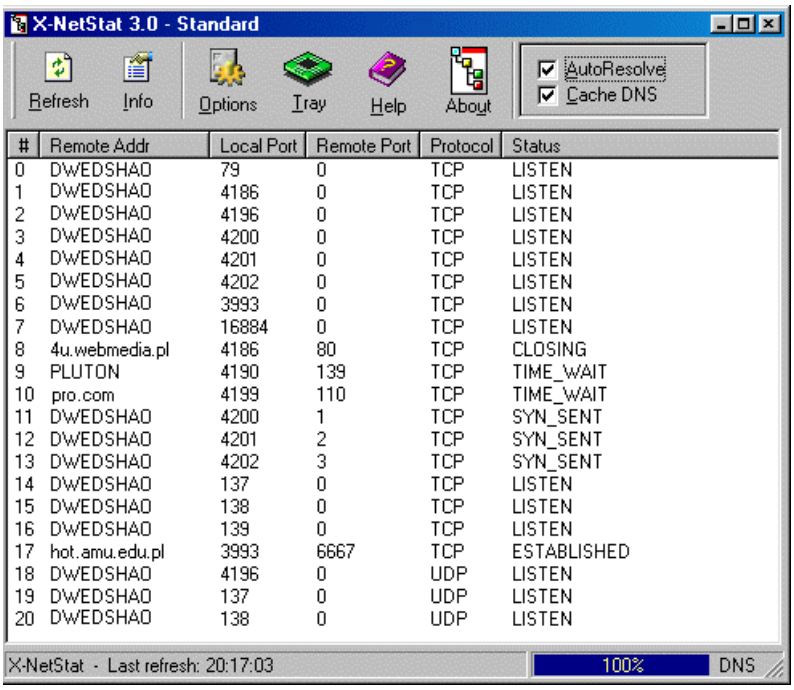
- *Startup port* — numer portu, który ma być „sprawdzany” po uruchomieniu programu;
- *Log To* — nazwa i ścieżki dostępu pliku, w którym będą rejestrowane odwołania do portu;
- *Stay On Top* — zaznaczenie tej opcji zapewnia, że okno będzie zawsze na wierzchu;
- *Minimize To System Tray* — zaznaczenie tej opcji zapewnia minimalizację (okno programu w postaci ikonki pojawi w prawym dolnym rogu ekranu monitora).

Druga zakładka — *Notify* umożliwia skonfigurowanie dźwięków, które mogą sygnalizować zaistnienie określonych sytuacji — np. próby sforsowania portu.

Jeżeli sprawdzimy, na jakim porcie działa aktualnie ICQ, możemy wpisać w oknie programu odpowiedni numer portu, dzięki czemu będziemy mieli dodatkową informację o tym, czy ktoś skanuje zasoby naszego dysku twardego. Jeśli zdarzy się, że ktoś będzie na przykład będzie znał numer naszego otwartego portu, ale będzie go penetrował bez stosowania skanowania (jest przecież taka możliwość) i wyśle nam spam, okaże się, że jest to jedyny sposób namierzenia intruza.

X-Netstat 3.0

Ten program bez wątpienia przyda się każdemu, kto lubi wiedzieć, gdzie „znajduje się” jego komputer. Jest on odpowiednikiem okienkowej wersji komendy `netstat`, znanej z DOS-a lub Linuksa, której zadaniem było pokazanie wszystkich aktualnych połączeń komputera z siecią i hostów, z jakimi nastąpiło połączenie. Okienkowa wersja jest łatwiejsza w obsłudze, a ponadto ma kilka opcji, których próżno byłoby szukać w jej prototypach.

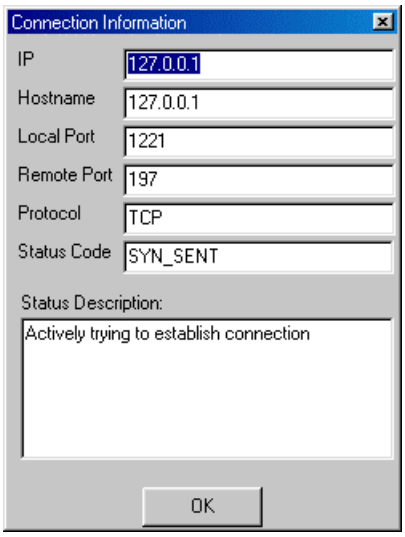


#	Remote Addr	Local Port	Remote Port	Protocol	Status
0	DWEDSHAO	79	0	TCP	LISTEN
1	DWEDSHAO	4186	0	TCP	LISTEN
2	DWEDSHAO	4196	0	TCP	LISTEN
3	DWEDSHAO	4200	0	TCP	LISTEN
4	DWEDSHAO	4201	0	TCP	LISTEN
5	DWEDSHAO	4202	0	TCP	LISTEN
6	DWEDSHAO	3993	0	TCP	LISTEN
7	DWEDSHAO	16884	0	TCP	LISTEN
8	4u.webmedia.pl	4186	80	TCP	CLOSING
9	PLUTON	4190	139	TCP	TIME_WAIT
10	pro.com	4199	110	TCP	TIME_WAIT
11	DWEDSHAO	4200	1	TCP	SYN_SENT
12	DWEDSHAO	4201	2	TCP	SYN_SENT
13	DWEDSHAO	4202	3	TCP	SYN_SENT
14	DWEDSHAO	137	0	TCP	LISTEN
15	DWEDSHAO	138	0	TCP	LISTEN
16	DWEDSHAO	139	0	TCP	LISTEN
17	hot.amu.edu.pl	3993	6667	TCP	ESTABLISHED
18	DWEDSHAO	4196	0	UDP	LISTEN
19	DWEDSHAO	137	0	UDP	LISTEN
20	DWEDSHAO	138	0	UDP	LISTEN

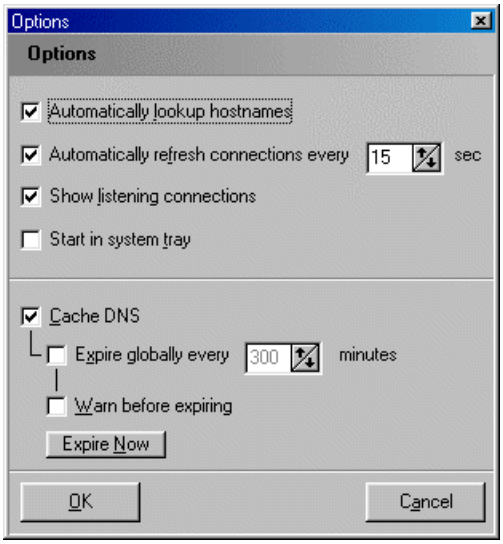
Główny ekran programu podzielony został na dwie części, z których jedna zawiera opcje, a w druga pokazuje listę połączeń.

Opcje dostępne w głównym oknie:

- *Refresh* — odświeża i wyświetla listę połączeń;
- *Info* — wyświetla dodatkowe informacje na temat wybranego połączenia, co może wyglądać tak, jak przedstawiono na poniższym rysunku:



- *Options* — za pomocą tej opcji można dopasować funkcje do aktualnych wymagań; poniżej przedstawione zostało okno konfiguracji:



- *Automatically lookup hostnames* — automatyczne sprawdzanie nazwy serwera DNS odpowiadającego adresowi IP, który został „złapany” na gorącym uczynku, czyli połączeniu;
- *Automatically refresh connections every* — automatyczne odświeżanie listy, które odbywa się co wybraną ilość sekund,
- *Show listening connections* — pokazuje porty, które są „otwierane na świat”;
- *Start in system tray* — rozpoczyna działanie programu w zminimalizowanej wersji;

- *Cache DNS* — włączenie tej opcji powoduje zapamiętywanie nazwy DNS dla podanego IP, co znacznie przyśpiesza proces odświeżania listy połączeń;
- *Expire globally every* — wskazuje czas, po upływie którego ma zostać wyczyszczony bufor, w jakim przechowywane są nazwy DNS;
- *Warn before expiring* — „ostrzega" przed wyczyszczeniem bufora;
- *Expire Now* — „czyści" bufor z nazwami DNS;
- *Tray* — minimalizuje program do ikony umieszczonej po prawej stronie paska zadań; wcześniej znaleźć można jeszcze opcję *Help* (pomoc) i *About* (informacje), a na końcu — opcje *AuroResolve* i *Cache DNS*, które dublują się z opcjami z okna konfiguracji.

Aby przeanalizować otrzymane informacje o połączeniach, trzeba skorzystać z pomocy włączonej opcji *Show listening connections*, gdyż daje ona dużo możliwości zastosowania (standardowo jest wyłączona). W oknie tym znajduje się kilka tabel, w których pojawiają się następujące dane:

- # — numer połączenia (tylko dla użytku programu; nie ma on nic wspólnego w właściwymi danymi);
- *Remote Addr* — adres IP (lub nazwa DNS) komputera, z którym nastąpiło połączenie (lub jego próba);
- *Local Port* — port na naszym komputerze, poprzez który nastąpiło połączenie; dzięki temu można dowiedzieć się, jaki ma ono charakter;
- *Remote Port* — zdalny port komputera, z którym połączył się nasz komputer;
- *Protocol* — typ protokołu, przez który nastąpiło połączenie;
- *Status* — status aktualnego połączenia.

Możliwe są następujące statusy:

- *Listen* — nasz komputer otwiera port i czeka na połączenie; dzięki tej opcji można bardzo skutecznie sprawdzić, czy komputer nie został „zarażony" jednym z koni trojańskich typu klient-serwer (np. jeśli znajdziemy na naszym komputerze nasłuchujący port 12345, to mamy 98% pewności, że nasz komputer ma aktywnego Netbusa, o ile nie uruchomiliśmy Netbustera;
- *Established* — oznacza, że połączenie zostało nawiązane i jest aktualnie używane;
- *Time_Wait* — jest to czas, jaki — po udanym połączeniu z innym komputerem, który nie wysłał sygnału o jego zakończeniu — nasz komputer daje (tak zwany czas życia połączenia) na rozłączenie;
- *Closing* — połączenie jest zamykane,
- *Syn_Sent* — próba połączenia.

Program ten ma wiele zastosowań. Za jego pomocą można na przykład sprawdzić, na jakim porcie rozmawia z nami kolega z ICQ. Z kolei analizując logi, dowiemy się, czy inni nas nie skanują, o ile używają prostych technik.

Na koniec jeszcze jedna, tym razem zła wiadomość. Program jest w wersji demo i pozwala na użytkowanie tylko przez niedługi okres czasu. Trzeba go albo zarejestrować u autora, albo scrackować.

Skanowanie portów

Skanery stosowane do hakowania są to programy, za których pomocą możemy „wyciągnąć" informacje z interesującego nas komputera podłączonego do Sieci. Rodzaj informacji, które można podejrzeć, zależy od rodzaju skanera. Wcześniej należy jednak poznać zasady funkcjonowania skanera portów.

Pozornie nie daje on zbyt wielu informacji, ale analizując część z nich możemy się dowiedzieć, w jaki sposób interesujący nas komputer jest „otwarty" na świat. Skanowanie jest procesem, który często poprzedza włamanie i służy jako pewnego rodzaju sprawdzenie, z czym mamy do czynienia po drugiej stronie kabla.

7th Sphere Port Scan 1.1

Skaner ten jest z całą pewnością jednym z ciekawszych i użyteczniejszych do skanowania portów. Jest szybki, niemal niezawodny oraz ma kilka dosyć ciekawych rozwiązań. Poniżej zostało przedstawione jego główne okno.

Do ważniejszych funkcji programu należą:

- *Scan* — rubryka, w której wpisać należy adres IP komputera, który ma być skanowany; w przypadku, gdy chcemy sprawdzić własny komputer, należy wpisać jedną z podanych niżej możliwości:
  - nazwę komputera;
  - stały adres IP 127.0.0.1, który odnosi się zawsze do komputera, na którym właśnie pracujemy;
  - słowo „localhost", które działa analogicznie do 127.0.0.1;
  - przydzielony nam adres IP czy adres wewnętrzny typu 10.0.0.123;
- *Send port* — rubryka, w której wpisać należy port, od jakiego chcemy zacząć skanowanie;
- *Delay (ms)* — oznacza opóźnienie (w milisekundach), po jakim program ma zacząć skanowanie kolejnego portu (w przypadku, gdy istotny jest pośpiech należy wpisać zero);
- *Filename* — rubryka, w której wpisać należy pełną ścieżkę dostępu, jeżeli chcemy efekt naszej pracy (czyli spis otwartych portów wraz z niewielkim opisem) zapisać do pliku; do wyboru są dwie opcje zapisu:
  - w dowolnym momencie (*Save*);
  - automatyczne nagrywanie pliku (*Save on halt*) w przypadku zatrzymania skanowania przyciskiem *Halt*.

Skoro zasady posługiwania się programem są jasne, nadszedł czas na analizę tego, co udało się zeskanować. Przypuśćmy, że w okienku zobaczymy następujący zapis:

```
0 :PORTSCAN READY.
0 :SCANNING HOST:127.0.0.1
0 :SCAN BEGUN ON PORT:1
0 :IP:127.0.0.1
```

Jako pierwsze pojawiają się dane dotyczące samego procesu skanowania, a potem kolejno: komunikat gotowości do skanowania, wpisana nazwa hosta (lub IP) do skanowania, port, od którego skanowanie się rozpoczęło, oraz IP skanowanego właśnie hosta. Czasem można znaleźć otwarte porty. Na przykład:

```
139: CONNECT
```

Oznacza to, że znaleziony został pierwszy otwarty port. Jeżeli znajduje się on na komputerze, na którym pracujemy, to istnieje ryzyko, że ktoś, może zdalnie zawiesić system owego komputer za pomocą programów typu NUKE.

Czasami niektóre porty zaraz po przeskanowaniu, natychmiast się zamykają, co na ekranie powoduje wyświetlenie dodatkowego komunikatu:

```
868 :CONNECT
868 :CLOSED
```

Oznaczać to może, że właściciel skanowanego komputera uruchomił program zabezpieczający przeciwko atakom za pomocą portów.

Program ten ma jeszcze jedną bardzo przydatną funkcję — niektóre porty zaraz po ich otworzeniu wysyłają pewne informacje, czego przykładem może być port `13`, pokazujący aktualny czas na zdalnym komputerze:

```
13 :CONNECT
13 :Time 22:06:04
```

I następny przykład:

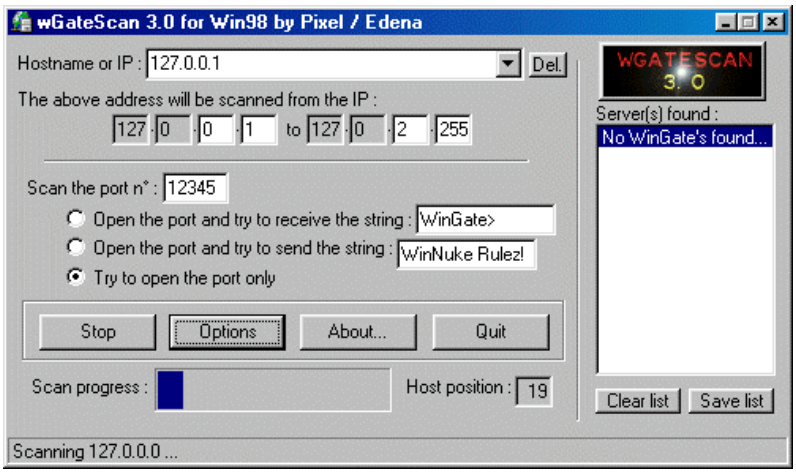
```
21 :CONNECT
21 :FTP Server, Hello lost user! Please enter Your name and
password!
```

Taki lub podobny komunikat można ujrzeć, gdy na komputerze ofiary został udostępniony serwer FTP. Informacja jest niejednokrotnie bardzo istotna w przypadku włamań.

Pytaniem, które teraz może się nasunąć jest to, czy skanowanie umyka uwadze naszej ofiary. Z reguły jest tak, że czym większy i ważniejszy serwer, tym posiada on więcej zabezpieczeń i systemów wykrywania intruzów. O ile na zwykłych niezabezpieczonych komputerach scanning przejdzie bez echa, to istnieją serwery, które nasłuchują własnych portów i połączenie z nimi jest natychmiast odnotowywane wraz z informacją o IP atakującego. Jednocześnie (w zależności od czułości systemu) może zostać podniesiony alarm o wstępnych objawach potencjalnego ataku. Warto jednak wiedzieć o tym, że skanowanie jest legalne (a dokładniej: nie jest zabronione przez prawo), jeśli nie czyni szkód na skanowanym komputerze.

Win Gate Scan 3.0 for Windows

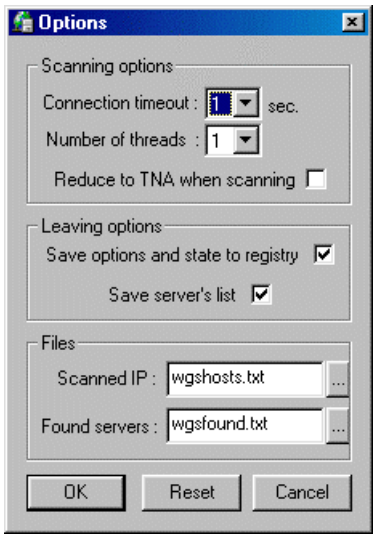
Program Win Gate Scan 3.0 for Windows — pomimo swojej nazwy — nie ogranicza swych możliwości do znalezienia otwartego portu Win Gate'a i można za jego pomocą przeskanować każdy dowolny port. Zasada działania jest prosta: należy wskazać interesujący nas port, a program automatycznie sprawdzi wszystkie komputery z domeny i wyświetli komunikat ze wskazaniem adresów, pod którymi ów port jest otwarty. A tak wygląda okno programu:



Opis funkcji:

- *Hostname or IP* — w tym miejscu należy wpisać interesującą nas domenę; ostatnia (ewentualnie — przedostatnia) liczba symbolizująca dane pojedynczego komputera może być dowolna, gdyż i tak zostaje przeskanowany każdy element podanego zakresu;
- *The above address will be scanned from the IP* — to rubryka, w której trzeba podać zakres (od którego i do którego komputera) planowanego skanowania (domyślnie ustawiona jest opcja zakładająca wykonanie działania na wszystkich komputerach o IP w klasie C, czyli xxx.xxx.xxx.1-255); możliwe jest także skanowanie adresów w klasie B (xxx.xxx.1-255.1-255);
- *Scan the port* — miejsce, w którym należy zapisać port, jaki będziemy skanowany;
- *Open the port and try to receive the string* — opcja ta zezwala na „wyłowienie" podanego ciągu znaków w przypadku, gdy znajdziemy otwarty port;
- *Open the port and try to send the string* — opcja ta działa podobnie jak ta opisana wyżej z tą jednak różnicą, że to my wysyłamy podany ciąg znaków;
- *Try to open the port only* — opcja, której zadaniem jest sprawdzenie tego, czy port jest otwarty.

Pod przyciskiem *Options* kryją się następujące możliwości:



- *Connection timeout* — czas połączenia; w przypadku, gdy dwukrotnie otwieramy program w celu przeskanowania różnych IP, należy zwiększyć wartość do 2, gdyż może się zdarzyć, że obydwa programy otworzą zbyt dużą ilość portów jednocześnie i w efekcie skanowania nie będzie prawidłowy;
- *Number of threads* — jest to liczba określająca ilość komputerów pominiętych przy skanowaniu danych, czyli tak zwany „skok" (jeśli na przykład wpiszemy wartości 2, skanowanie obejmie dane znajdujące się na co drugim dysku twardym komputerów przyłączonych do Sieci);
- *Reduce to TNA when scanning* — opcja, która reguluje widokiem okna programu podczas skanowania (jej zaznaczenie powoduje redukcję obrazu przedstawiającego działanie programu do ikony);
- *Save options and state to registry* — opcja, za pomocą której można włączyć lub wyłączyć zapamiętywanie ustawień w rejestrach;
- *Save server's list* — opcja decydująca o tym, czy wynik skanowania ma być zapisany na twardym dysku;
- *Scanned IP* — to rubryka, w której należy wpisać nazwę, pod jaką zapisane będą przeskanowane porty;
- *Found servers* — to rubryka, w której należy wpisać adresy, pod jakimi znaleźliśmy nasz otwarty port.

Po kliknięciu *Scan* aktualna pozycja skanowanego komputera będzie widoczna w okienku *Host Position*, a efekt — w oknie *Server(s) Found*. I właśnie ta lista zawierać będzie informacje o komputerach, na których znalezione zostały otwarte porty. Wskazane jest zatem jej zapamiętanie za pomocą przycisku *Save list* (w nazwie należy wskazać port, jaki był skanowany, gdyż informacja ta nie pojawia się w pliku), a następnie „wyczyścić" okno (*Clear list*), co zabezpieczy nas przed pomyłką, gdy

zaczniemy skanować inny port. Jak widać, program nie jest specjalnie trudny w obsłudze, a możliwości, jakie oferuje, są naprawdę spore.

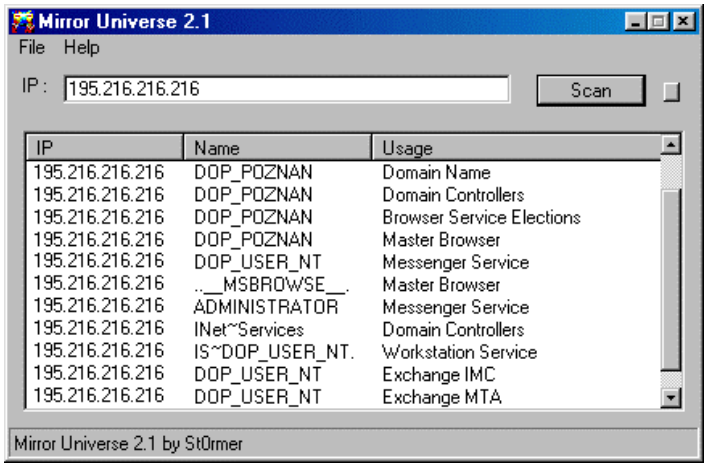
Mirror Universe 2.1

Kolejnym ciekawym skanerem jest skaner NetBiosu. Różni się od poprzednich skanerów przede wszystkim zasadą działania. Jego zadaniem jest bowiem pobieranie danych dotyczących domeny czy zalogowanego użytkownika z interesującego nas adresu IP. Nie każdy komputer udostępnia tę usługę, więc nie zawsze ten zabieg się udaje. Tak czy inaczej warto próbować, gdyż zdobytych informacji może być znacznie więcej (w zależności od tego, ile udostępnia ich docelowy komputer).

Ilość danych może być naprawdę imponująca, ale zdarza się również że zamiast nich zobaczymy tylko krótką wiadomość:

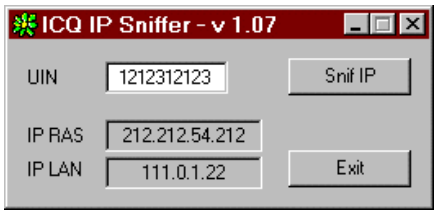
```
No NetBIOS on IP
```

Sam program jest banalny w obsłudze. Wystarczy podać w okienku IP ofiary i klinąć *Scan*, by po chwili zobaczyć całą masę informacji, co zostało przedstawione na poniższym obrazku.



ICQ IP Sniffer 1.07

Miło sobie od czasu do czasu „posiedzieć” na ICQ, pogadać z przyjaciółmi, poznać nowych ludzi... No tak, ale nasza ciekawość nie zna granic i jeszcze zanim przedstawi nam się nowa osoba, chcemy już znać jej imię, nazwisko, adres zamieszkania, telefony, kontakty, kolor oczu. Kolejny program tych wymogów nie spełnia, lecz i tak jest on bardzo przydatny. Najogólniej mówiąc podaje nam na podstawie numeru UIN adres IP komputera, pod jakim znajduje się aktualnie jego właściciel. Jest łatwy w obsłudze, co widać na załączonym obrazku:



Wystarczy jedynie wpisać UIN, czyli numer osoby z ICQ i kliknąć *Snif IP*. Po chwili, o ile interesująca nas osoba będzie w trybie on-line, ujrzymy w okienku dwa adresy IP. Dlaczego dwa? Wbrew pozorom nie jest to błąd. Ujawnione informacje dotyczą nieco odmiennych sfer. Pierwsza z nich *IP RAS* wskazuje adres, z jakim bezpośrednio nastąpił kontakt przy połączeniu. Czasem jest to adres zapory firewall lub serwera, a nie komputera, z którego interesująca nas osoba korzysta faktycznie. Nieraz zdarza się także, że program pokazuje adresy, które niewiele mogą nam pomóc lub są po prostu niezrozumiałe. Jednak na ogół wyświetlony adres będzie adresem serwera lub adresem wewnętrznym, który kryje się w programie pod nazwą *IP LAN* (na niewiele nam się zda, jeśli nie jesteśmy bezpośrednio do niej podłączeni). Ale w tym właśnie tkwi przewaga tego programu nad zwykłym wyświetlaniem adresu IP w informacjach o użytkowniku (opcja w ICQ), gdyż tam bowiem widzimy jedynie adres zewnętrzny, który często nam nie wystarcza.

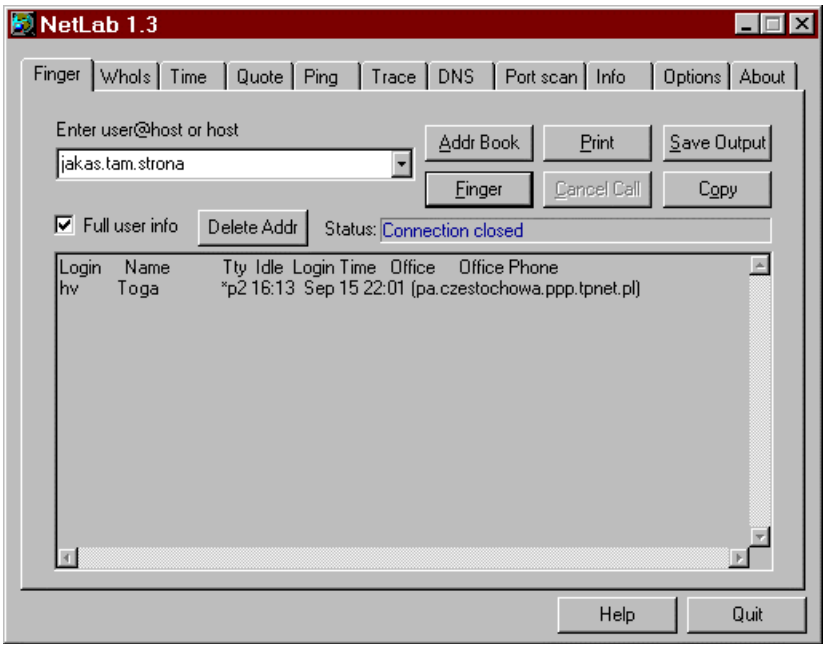
Do czego może w praktyce przydać się ten program? Przy odrobinie szczęścia i w połączeniu z innymi programami poznamy dzięki niemu następujące informacje:

- Używając Mirror Universe można uzyskać dodatkowe wiadomości na temat użytkownika;
- Można przeskanować konkretny adres i sprawdzić, czy nie występuje zagrożenie w postaci uaktywnienia koni trojańskich;
- Zamienić adres IP na adres DNS, dzięki czemu można poznać rodzaj domeny (ustalić czy jest to firma, kawiarenka internetowa);
- Sprawdzić, czy osoba o podanym numerze jest w trybie on-line czy off-line. Można również dowiedzieć się, czy dana osoba nie dodała naszego adresu do listy Invisible.

Istnieje bardzo dużo programów hakerskich, których istota działania jest oparta na zasadach funkcjonujących w Sieci i wymagane jest wówczas podanie adresu IP jako sprecyzowania komputera, którego ma on się tyczyć.

Netlab 1.3

Kolejnym programem godnym przedstawienia jest znakomity „kombajn” łączący w sobie kilka standardowych dla sieci funkcji — Netlab. Nie zawiera on typowo hakerskich funkcji, lecz mimo to każdy, kto ma do czynienia z Siecią, mieć go powinien. Jego okno wygląda tak, jak przedstawiono na poniższej ilustracji.



Przedstawiony zrzut nie ukazuje całej gamy opcji, gdyż każda z nich kryje się pod oddzielną zakładką. Poniżej zostanie więc przedstawiony ich skrócony opis.

- *Finger* — dosłownie oznacza on „palec". Finger to — ogólnie rzecz ujmując — usługa, która na danym komputerze (częściej na serwerze niż na prywatnej jednostce) udostępnia różne informacje tekstowe (często jest to spis aktualnie zalogowanych użytkowników wraz z czasem zalogowania, adresem sieciowym czy informacją o czekającej na odbiór poczcie). Innym razem możemy przejąć informację o właścicielu (np. o profilu komputera, firmy itp.). Aby uzyskać możliwie najwięcej danych, dobrze jest włączyć opcję *Full user info*.

Finger jest ulubionym narzędziem dla hakerów, czyli tych, którzy potrafią wykorzystać „dziury" znajdujące się w atakowanym systemie, tych, którzy mogą podłączyć do niego różne pliki, co w efekcie kończy się zwykle udostępnieniem aktualnych haseł.

Załóżmy więc, że mamy pewną interesującą nas domenę klasy C. Przypuszczalnie na jednym z komputerów znajduje się serwer, który udostępnia informacje o użytkownikach. Jako że usługa finger rezyduje na porcie 79, wystarczy przeskanować domenę w jego poszukiwaniu (np. opisanym programem WinGateScann). Do znalezionego adresu IP możemy teraz dopasować fingera, a wówczas zobaczymy listę użytkowników wraz z ich adresami IP.

Jest to tylko jedna opcja z wielu możliwych, ale pokazuje ona, jak może zostać wykorzystana do uzyskania pożądanych rezultatów. Należy jednak pamiętać, że w większości przypadków *finger* rejestruje na sprawdzanym komputerze, z jakiego IP zostało on uaktywniony, więc jest to pewna poszlaka...

Kolejnymi opcjami, które pojawią się niemal przy każdej zakładce w NetLabie, są:

- *Delete Addr* (lub *Server, Host*) — dodanie wpisanego adresu do listy;
- *Print* — drukowanie danych wynikowych;
- *Cancel All* — zatrzymanie działania funkcji;
- *Save Output* — nagrywanie danych wynikowych do pliku;
- *Copy* — kopiowanie danych wynikowych do clipboardu;
- *Whois* jest kolejną przydatną funkcją. Jest serwerem przechowującym dane o użytkownikach, firmach itp. Wpisując posiadane informacje możemy dowiedzieć się czegoś więcej o interesujących nas użytkownikach. Szukaną nazwę należy wpisać w pole *Query String*, a w *Whois* wystarczy wybrać jeden z wprowadzonych wcześniej serwerów lub dopisać nowy.
- *Time* — zastosowanie tej funkcji niewiele ma wspólnego ze skanowaniem, ale na pewno jest przydatne. Dzięki temu możliwe będzie dosyć dokładne zsynchronizowanie daty, a przede wszystkim godziny z serwerami, które tych informacji udzielają. Tak więc w pierwszym przypadku (*Day Time*) wpisać trzeba adres (lub wybrać jeden z listy) serwera udostępniającego tę funkcję i kliknąć przycisk *Day Time*. Po chwili komputer połączy się, a data zostanie na naszym komputerze automatycznie ustawiona (uwzględniając naszą strefę czasową). Na podobnej zasadzie działa ustawianie czasu — *Clock synchronization*. Wystarczy wpisać nazwę hosta i kliknąć *Synchronize*. Tu jednak jest więcej funkcji do wyboru: można włączyć okresowe, automatyczne łączenie się z podanym serwerem co określony przedział czasu (od minuty do 24 godzin). Aby funkcja działała od razu po włączeniu programu, należy ustawić funkcję *Connect At Startup*. Można także ustalić, jaką techniką mają być przesyłane dane — TCP/UDP czy SNTP. Jeżeli okaże się że serwer źle zinterpretuje strefę czasową i ustawi na przykład czas Zimbabwe, to klikając *Offest* można ręcznie ustawić różnicę czasu odpowiedniej strefy czasowej (względem GMT), a komputer „weźmie to pod uwagę" podczas następnej synchronizacji.
- *Quote* — jest chyba najrzadziej używaną funkcją w programie. Niektóre serwery otwierają port 17, przez który podają hasło dnia (nie należy tego mylić z hasłami systemowymi).
- *Ping* jest funkcją, która wysyła sygnał w stylu „żyjesz" pod określony adres, a jeśli tamten jest włączony powinien odesłać komunikat w stylu „no jasne, że tak", dodatkowo pokazując czas, jaki minął. Oczywiście nie jest to dosłowne tłumaczenie, lecz prymitywne uproszczenie. Oto dodatkowe funkcje, jakie towarzyszą pingowi:
  - *Resolve IP Adress* — działanie jego jest banalne: jeśli wpisaliśmy jako skanowany host adres IP, to otrzymamy także jego adres DNS;
  - *Don't fragment* — zabrania fragmentowania wysyłanych pakietów;
  - *Number of Pings* — zawiera ilość „zapytań", jaką chcemy wysłać pod wskazany adres;

- *Delay* — opóźnienie, jakie ma nastąpić pomiędzy kolejnymi „zapytaniami”;
- *Base Packet Size* — określa wielkość pojedynczego „zapytania”;
- *Timeout* — czas oczekiwania na rezultat „zapytania”.

Wynik procesu można zobaczyć w okienku. A przedstawia się on mniej więcej tak:

- # — numer „zapytania”;
- *IP Adress* — adres IP „pytanego” komputera;
- *Host Name* — nazwa hosta;
- *Packet Round Trip Time* — czas, jaki upłynął na połączeniu.

Do czego może się to przydać? Przede wszystkim do sprawdzania, czy interesujący nas komputer jest podłączony do Sieci i czy jest w stanie nawiązać połączenie. Innym przykładem może być atak — wysyłając znaczną ilość dużych pingów — na dodatek nieposortowanymi pakietami — do jakiegokolwiek użytkownika modemu, możemy znacznie spowolnić jego pracę, gdyż atakowany komputer będzie miał zbyt wiele „roboty” z odpowiadaniem na nasze pingi.

- *Trace* jest kolejną, ciekawą funkcją, którz bez wątpienie pomoże w uzyskaniu pewnych informacji na temat innego komputera. Teoretycznie sprawdza ona, przez jakie komputery, hosty czy serwery przechodzi nasz sygnał zanim trafi do odbiorcy. Można ją skonfigurować używając następujących opcji:
- *Maximum Hops* — określa maksymalną ilość pokazanych hostów, przez jakie ma przejść pakiet;
- *Start from Hop* — zaznaczenie tej opcji inicjuje proces „śledzenia”, począwszy od wybranego hosta;
- *Delay* — określa opóźnienie, jakie ma nastąpić pomiędzy sprawdzaniem kolejnych hostów;
- *Data Size* — określa wielkość wysyłanego pakietu;
- *Timeout* — określa maksymalny czas oczekiwania na odpowiedź od hosta.

Pozostaje jeszcze opcja *DNS* , której działanie jest równie proste, co przydatne. Wystarczy po prostu wpisać w rubrykę IP lub DNS, a program połączy się z odpowiednim serwerem DNS i pokaże nam jego obydwie formy. Oznacza to, że jeśli wiemy, że interesujący nas komputer ma adres 195.123.123.123, to możemy sprawdzić, czy ma również alternatywną nazwę hosta (adres DNS) np. *franek. mojaszkola.edu.pl.* Od razu można się wtedy zorientować, skąd „pochodzi” komputer. Adres DNS może w sobie kryć także miasta, w jakich „znajduje się” komputer, providera (można np. sprawdzić, czy użytkownik korzysta z modemu poprzez TPSA) czy jej charakter *(*.edu, *.mil, *.gov, *.com* itp.). Z drugiej strony niektóre programy wymagają docelowego adresu w postaci IP, więc tutaj możemy zamienić go na ten wymagany. Dodatkowo mamy także funkcję Local IP pokazującą nasz

adres w obydwu formach, pod jakimi widnieje on w Sieci. Jeśli jednak będziemy w trybie off-line, prawdopodobnie zobaczymy tylko adres 127.0.0.1.

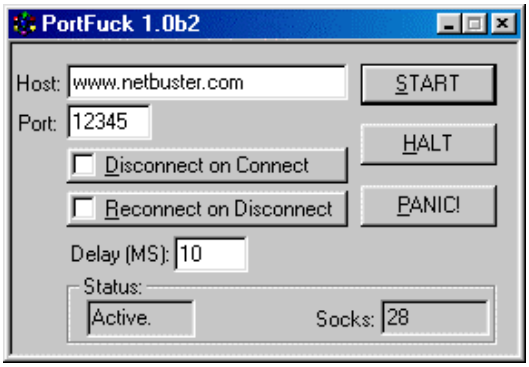
- *Port Scan* — nie jest kolejnym skanerem podobnym opisanych wcześniej. Ta funkcja pokazuje jedynie, jakie usługi kryją się pod danymi portami na naszym komputerze. Niestety poza przypomnieniem *Well Know Ports* (standardowych usług na danych portach) nie przyniesie żadnych korzyści.

Na koniec zostały jeszcze trzy zakładki:

- Info — prezentuje informacje dotyczące naszego komputera (czasem — nieprawidłowe dane);
- Options — opcje służące do konfiguracji programu; za pomocą Choose Font można wybrać czcionkę do wyświetlania poszczególnych danych; Use Firewall pozwala skonfigurować program tak, by działał także przez zaporę firewall; natomiast pozostałe opcje zawierają standardowe funkcje, takie jak Minimize Tray (po zminimalizowaniu programu pokaże się tylko jego ikonka na pasku zadań);
- About — wyświetla informacje o autorze.

Port Fuck

Program ten, mimo że dokładnie wiadomo, co robi, nie ma jasno określonego zastosowania i w zasadzie trudno jest się domyślić, do czego służy. Jego główne okno prezentuje się tak, jak to przedstawiono na poniższej ilustracji.



Idea programu jest niezwykle prosta. Program łączy się podanym adresem (*Host*) w określonym wcześniej porcie (*Port*) i „stara się" ustanowić jak najwięcej połączeń jednocześnie. Trzeba oczywiście dodać że port, który chcemy atakować musi być otwarty. Warto zaznaczyć, że istnieje możliwość ingerencji w przebieg tego procesu. Służy do tego opcja *Disconnect on Connect.* Po jej zastosowaniu każde pojedyncze połączenie z portem (pamiętajmy, że może być ich wiele w jednym czasie) będzie zrywane. Dodatkową pomocą jest opcja *Reconnect on Disconnect*, która powoduje, że po rozłączeniu się będzie następowała próba ponownego połą-

czenia. Na koniec możemy jeszcze ustalić, jak szybko ma cały proces przebiegać (opcja *Delay)*.

Aby zainicjowac działanie programu, wystarczy kliknąć *START* i obserwować okienko *Socks*, gdzie zobaczymy ilość nawiązanych połączeń w tym samym czasie. Naciśnięcie *HALT* zatrzymuje proces podłączania się (jednak już ustalone połączenia będę powoli się odłączać), a wybór *PANIC*! — resetuje wszelkie podłączenia w ciągu jednej chwili do 0.

Zastosowanie programu jest proste. Otóż wszelkie połączenia TCP/IP w Sieci nawiązywane są poprzez porty. Zwykle program ustanawia sobie jakieś jedno „gniazdko" i na nim następuje proces wymiany danych. A jeśli nagle połączymy się z nim dziesiątki razy? Wtedy można naprawdę narozrabiać. Czasem program nic nie zdziała, czasem kompletnie zawiesi system... Wszystko zależy od „odporności" oprogramowania po „drugiej stronie kabla". Oto reprezentatywny, a zarazem sprawdzony przykład: NetBuster.

Mówiąc w skrócie jest to symulator serwera NetBusa. Można się z nim połączyć i „wydawać" mu rozkazy za pomocą klienta NetBusa. mimo że wszystko wygląda jak najbardziej prawdziwe, faktycznie jednak program nie wykonuje żadnych zlecanych przez nas działań, lecz zapisuje nasze nieudolne próby *hakowania* zapisując dodatkowo nasze namiary. Najprościej mówiąc jest dowodem naszej nieautoryzowanej działalności poprzez NetBusa. Tak to już jest, że ci, którzy mieli zainstalowany serwer NetBusa prędzej czy później dowiadują się o wszelkich próbach ingerencji i zamieniają go na NetBustera. I tu nas mają. Ale czy na pewno? NetBuster, podobnie jak NetBus, oczekuje na połączenia na ustalonym porcie (standardowo 12345 — czyli taki sam jak dla NetBusa). Gdyby teraz spróbować użyć PortFucka? Faktycznie NetBuster „pokaże" próbę połączenia lub po prostu się zawiesi.

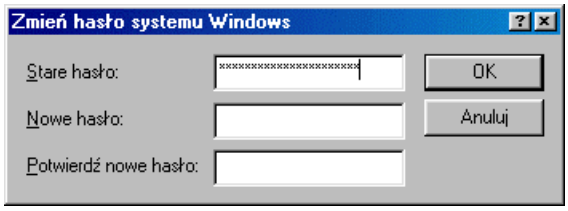
Łamacze

Skłonność do odgadywania haseł nie jest niczym nowym ani rzadko spotykanym. Przyświeca naszym zamiarom nawet wtedy, gdy pozbawieni złych zamiarów, dyskretnie sprawdzamy kilka najbardziej oczywistych kombinacji, które mogą ułatwić dostęp do konta naszego znajomego. Takie sytuacje znamy też ze starych filmów, w których złamanie odpowiedniego hasła do systemów NASA było jedynie kwestią nieprzespanej nocy. Nad ranem okazywało się, że jest to piękny slogan — „NASA is the best". Ale to tylko komercyjna fikcja. Nie ma więc nic wspólnego z prawdziwym hakowaniem. Obecnie hasła są naprawdę trudne do odgadnięcia ze względu na ilość kombinacji. Dlatego stosuje się wiele technik łamania, które znacznie ułatwiają ten czasochłonny proces. Czasem okazuje się jednak, że hasło sobie po prostu „leży" i czeka, aż ktoś je weźmie... Powstało zatem wiele programów napisanych przez hakerów, które są bardzo pomocne w procesie zdobywania haseł użytkowników systemów.

Snad Boy's Revelation 1.1

Istnieje wiele programów funkcjonujących w systemie operacyjnym Windows, które „pamiętają" wprowadzone hasła. Zwykle przedstawiają je w postaci ciągu gwiazdek (*******), z których każda oznacza jedną literę prawdziwego hasła.

A oto przykład:



Jeśli nie znamy hasła uruchamiającego działanie systemu — nawet skopiowanie ciągu znaków i próba wklejenia go do dokumentu spełza na niczym — musimy spróbować złamać hasło za pomocą tradycyjnych metod. Ale tak było kiedyś, bo dzisiaj posłużyć się możemy stworzonym w tym celu programem. Potrafi on niejako „wejrzeć" w zaszyfrowane gwiazdkami hasło i pokazać je w wersji literowej. Jest to oczywiście SnadBoy's Revelation v1.1

Gdyby ktoś nie wiedział, jak się nim posługiwać (instrukcja właściwie zawiera się w oknie programu), to może posłużyć się następującymi wskazówkami. Wystarczy kliknąć w celownik podpisany *Password Field Selector* i nie puszczając przycisku myszy, przenieść go do pola z gwiazdkami. W tej samej chwili w rubryce *Password* ukaże się literowa zawartość pola. Działanie programu jest proste i skuteczne, więc wystarczy tylko znalezienie odpowiednich pól z gwiazdkami...

Oto spis programów (nie wszystkich), które bez problemu poddają się tej metodzie odgadywania haseł :

- M$ Outlook Express;

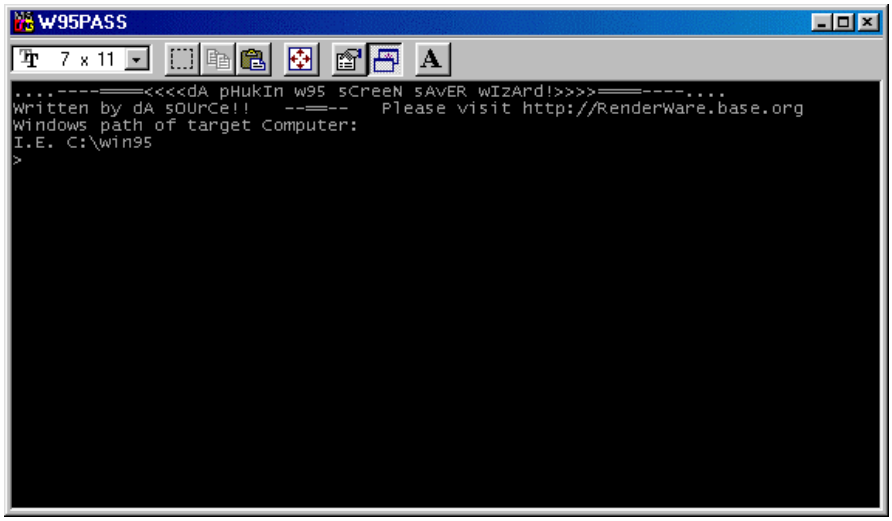
- Windows Commander (hasła do kont FTP);
- Cute FTP;
- Ustawienia Dial-Up;
- Netscape (i ile będzie włączona opcja zapamiętywania hasła).

Warto pamiętać — to uwaga skierowana do osób, które pragną zabezpieczyć się przed hakerami — aby nie pozostawiać haseł w programach. Lepiej wpisywać je za każdym razem od nowa, bo inaczej można się wystawić na banalny atak.

Da Phukin W95 Screen Saver Wizard

To kolejny program, który umożliwia przechwycenie haseł programów działających w systemie Windows. Za jego pomocą zdobyte hasło ma mniejsze znaczenie niż to, które można poznać posługując się poprzednim programem, jednak każde z nich jest na wagę złota. Znając kilka zaszyfrowanych „kluczy"można rozpoznać technikę, jaką stosuje ofiara w wymyślaniu haseł — np. nazwy własne, imiona ulubionych bohaterów kreskówek czy tendencyjne przedrostki przed zwykłymi hasłami. Czas jednak powrócić do programu. Jego zadaniem jest „wyciąganie" hasła ze standardowego wygaszacza ekranu.

Program działa pod DOS-em i po uruchomieniu wygląda tak:



W chwili, gdy pojawi się komunikat inicjujący jego działanie, trzeba wpisać ścieżkę dostępu do katalogu w którym znajdują się nasze profile. W przypadku, gdy jest tylko jeden profil użytkownika lub nie zalogujemy się w Windows, najprawdopodobniej ścieżką katalogu będzie:

C:\Windows

Gdy użytkowników jest wielu — a każdy z nich ma oddzielny profil (więc ustawienia wygaszacza ekranu są oddzielne) — konieczne jest wpisanie indywidualnej do użytkownika ścieżki. Np. dla użytkownika, jakim jest lamer, ścieżka wyglądać będzie prawdopodobnie tak:

C:\Windows\Profiles\Lamer

W obu przypadkach, o ile oczywiście ofiara posiada hasło, na ekranie powinny pojawić się następujące informacje:

```
Searching.....Found!
Decoding.....Finished!
```

A na końcu —

```
DECODED String: [lamer1]
```

To oznacza, że hasłem do wygaszacza ofiary jest „lamer1". Należy dodać jeszcze tylko jedną uwagę. Jeżeli w wybranym katalogu nie zostało wpisane żadne hasło, program (bez dodatkowej informacji) zatrzyma się po komunikacie:

```
Searching.....Found!
Decoding...
```

i nie będzie to wina powolnego procesu dekodowania hasła (trwa nie więcej niż kilka sekund), lecz błędu programu. Program — wbrew nazwie — działa w kolejnych wersjach systemów operacyjnych Windows (95-98).

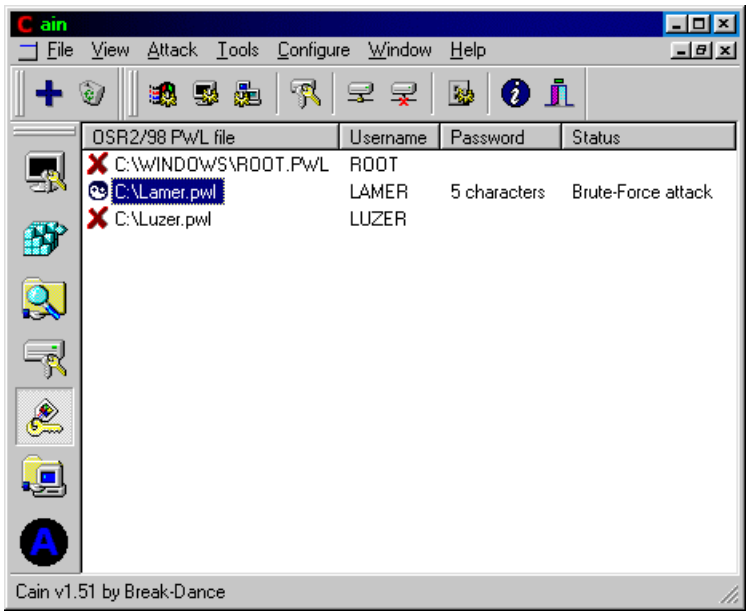
Cain 1.51

Następnym programem, który wart jest opisu, będzie cracker do haseł. To oznacza, że hasła nie tyle można „wyciągnąć, ale naprawdę je złamać. Program jest naprawdę bardzo dobry, a w przeciwieństwie do większości jemu podobnych jest zupełnie darmowy... Można go nazwać „prawdziwym kombajnem", gdyż za jego pomocą udaje się „wyciągnąć" hasła z kilku całkiem niebanalnych źródeł.

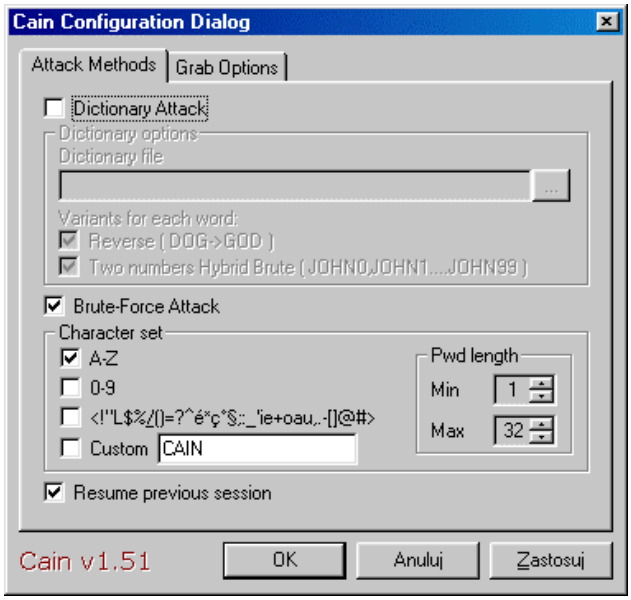
Oto one:

- Hasła do wygaszacza ekranu;
- Hasła do wygaszacza ekranu, ale z cudzych ustawień;
- Sharing lokalny (zdobycie pełnej kontroli nad katalogami, które udostępniamy „na zewnątrz");
- Hasła mieszczące się w CACHE (np. z Dial-Up-u), hasła do systemu Windows (pliki **.PWL*);
- Hasła do katalogów znajdujących się na cudzych komputerach,

A oto jak się prezentuje okno programu:



Najpierw trzeba omówić konfigurację programu (patrz: menu), gdyż ma to zasadniczy wpływ na działanie opcji. Na rysunku poniżej znajdziesz okno, w którym można ustawić kilka opcji.



To właśnie tu należy ustalić, w jaki sposób będzie przebiegał proces łamania haseł. Pierwsza z opcji *Dictionary Attack* służy do łamania w oparciu o gotowy spis haseł. Metoda ta sprawdza się głównie wtedy, gdy hasło składa się z jakiegoś oczywistego wyrazu jak imię, miejsce i inne słowa występujące w potocznej mowie. Oczywiście

słownik taki musimy posiadać na dysku jako plik ASCII (im większy, tym lepszy). Jego ścieżkę dostępu wybieramy w *Dictionary File*. Aby zwiększyć skuteczność takiego rodzaju *łamania*, autorzy programu pomyśleli o dodatkowych opcjach, które modyfikują hasło wejściowe ze słownika i sprawdzają je na dwa dodatkowe sposoby. Pierwszy z nich — *Reverse,* odwraca słowo, a drugi — *Two numbers Hybrid Brute,* dodaje na końcu do każdego hasła ciąg dwucyfrowy z zakresu od 0-99. Jest to konsekwencją często stosowanej konwencji ujawniającej się przy wymyślaniu haseł. Ludzie, którzy chcą być sprytni, często najzwyczajniej odwracają prosty wyraz lub dopisują na końcu jakąś cyfrę — owszem to komplikuje proces łamania hasła, ale powinno się stosować inne, bardziej skuteczne reguły przy dobieraniu dobrych haseł.

Drugim rodzajem ataku jest *Brute Force Attack*. Różni się od poprzedniego tym, że sprawdzane są wszystkie możliwe kombinacje wyrazowe z danego zakresu znaków, a nie tylko ze słownika. Z tego też powodu cały proces jest znacznie dłuższy, jednak przy krótkich hasłach, udaje się poznać je w ciągu jednego dnia. Jak w każdym poważniejszym programie łamiącym metodą brute-force, mamy i tu do dyspozycji szereg opcji pozwalających na dokładne określenie zakresu i kombinacji sprawdzanego hasła. Standardowo ustawiona jest opcja *A-Z*, która służy do analizy liter. Następnie za pomocą opcji *0-9* możemy sprawdzić cyfry, a korzystając z *<!@L#...>* — także znaki specjalne. Jednak opcją, która powinna nas zainteresować najbardziej jest *Custom*. Pozwala ona na samodzielne wpisanie znaków, jakie mają brać udział w łamaniu. Bardzo wygodne byłoby włączenie wszystkich kombinacji liter, cyfr oraz znaków, ale w praktyce to rozwiązanie się nie sprawdzaak nie jest bowiem czas na znalezienie powiedzmy 9 znakowego hasła we wszystkich kombinacjach znakowych nie trwało by godzinę, dzień, tydzień... ale miesiące, lata... Dlatego dobrze jest ograniczyć ilość znaków do niezbędnego minimum. Przykładowo dla haseł wymyślanych przez Polaków można spróbować wpisać w *Custom alfabet*, jednak pomijając litery X czy Q (są rzadziej stosowane) — przy 3-4 literach w haśle niewiele to da, ale już przy pięciu czy sześciu zauważymy znaczącą różnicę. Na koniec możemy ustalić długość sprawdzanych haseł (mamy liczbę minimalnych znaków — *Min* oraz maksymalną *Max*.

Ostatnią bardzo przydatną opcją (dotyczącą obydwu rodzajów łamania) jest możliwość przerwania łamania z zapamiętaniem miejsca, w którym zatrzymał się program. Przy włączonej opcji *Resume Previous Sesion* można dokończyć proces następnym razem, gdy będziemy mieli dostęp do komputera.

Drugą zakładką w opcjach konfiguracji jest *Grab Options*, ale nie ma ona większego znaczenia dla ogólnego działania programu.

Po prawej stronie okna zauważyć można rozmaite ikonki. Za ich pomocą wybieramy, jakimi hasłami chcemy się „zająć". *Screen Saver Password* — pozwala uzyskać w niezwykle prosty sposób hasło do wygaszacza ekranu. O ile takowe będzie ustawione, pokaże się w okienku *External Screen Saver Passwords*. Wystarczy nacisnąć + na górnym pasku lub wybrać go z menu i określić plik z danymi **.dat*. Mieszczą się one w katalogu systemowym *Windows/Profiles*, do którego dopisujemy nazwę użytkownika. Kolejana opcja to *Local Shares.* Pozwala ona na ustalenie

tego, jakie katalogi udostępnia nasz komputer innym komputerom. *Cached Passwords* — wskazuje hasła, które zostały umieszczone w pamięci CACHE. Znajdziemy tu np. hasło do Dial-Up, które jest szczególnie przydatne wtedy, gdy używamy komputera w kawiarence internetowej (lub innego miejsca. które pozwala na uzyskanie połączenia za pomocą ze zwykłego modemu). Wtedy wpisujemy numer telefonu providera, z jakim się on łączy (z wyjątkiem TPSA), hasło i w ten sposób możmy dzwonić na cudzy koszt). Następna opcja to *PWL Files*. Dzięki niej możliwe jest odnalezienie hasła, które wprowadzamy podczas logowania się do systemu. Jednak nie należy go mylić z hasłami logowania do Sieci, które przechowywane są gdzie indziej i działają na nieco innych zasadach. Tak czy inaczej — także i to hasło może nam się przydać w różnych okolicznościach, gdyż zyskujemy na przykład bezpośredni dostęp do cudzych ustawień, konfiguracji, a tam mieszczą się czasem hasła do programów (np. Outlook — dostosowuje się do aktualnego użytkownika i automatycznie wybiera nasze konto pocztowe). *Remote Shares* — sprawdza się w tych wypadkach, gdy w trakcie szperania po zasobach lokalnej sieci odnajdujemy katalog, którego udostępnienie wymaga wpisania odpowiedniego hasła. Aby je znaleźć, wystarczy kliknąć + i wybrać nazwę interesującego nas katalogu.

Abel Client

Trudno byłoby nazwać ten program „koniem trojańskim", ale na trochę podobnej zasadzie on działa. Do pakietu dołączony jest program *Abel.exe*, który pełni rolę serwera i umożliwia pobranie za pomocą Caina (w tym przypadku klienta) wszystkich wcześniej wymienionych haseł na cudzym komputerze. Serwer ten jest jawny i po uruchomieniu informuje o jego działaniu, więc nie można użyć go bez wiedzy drugiej strony. Ale wystarczy użyć dowolnego programu do edycji HEX i zmienić komunikat ostrzegający. Wtedy ofiara będzie myślała, że uruchomiony został jakiś nieznany bliżej program, a haker ma w tym czasie sposobność do tego, by przechwycić jej dane. Program po uruchomieniu nie „chowa się" w systemie, więc po zamknięciu, nie może uruchomić się samoistnie, jak to robią konie trojańskie.

Niektóre omawiane opcje programu (ikony z lewej strony) wskazują od razu jedno lub więcej haseł, lecz w przypadku takich opcji jak *PWL* aby je ujrzeć musimy, je sami złamać. W tym celu wybieramy interesującą nas pozycję i naciskamy prawy klawisz myszki. W tej chwili dostępnych mamy kilka opcji:

- *Start Attack* — rozpoczyna proces łamania (jeśli atak na daną pozycję wcześniej został przerwany, program automatycznie zaczyna sprawdzać od miejsca, na którym skończył, to znaczy od chwili, kiedy została użyta opcja *Stop Attack*);
- *Remove from list* — usuwa pozycję z listy (nie usuwa jej z dysku!);
- *Delete sesion file* — wskazuje pozycję, w której powstrzymany został poprzedni atak (zwykle jest ona zapisywana w oddzielnym pliku, który po uruchomieniu opcji zostaje skasowany);
- *Test password* — pozwala sprawdzić „ręcznie" czy znamy prawdziwe hasło;

- *Try another username* — pozwala zmienić nazwę posiadacza (użytkownika) danego pliku **.pwl*

Opis kolejnych funkcji programu kryjących się pod odpowiednimi ikonami można pominąć, gdyż pokrywają się one w całości z rozwijanym menu, w którym jest możemy znaleźć jeszcze więcej rozwiązań. Przede wszystkim znajdziemy tam:

- *File*:
  - *Add to list* — dodaje do listy plik (ewentualnie katalog czy sharing), który chcemy łamać;
  - *Remove from list* — działa podobnie do wyżej opisanej opcji, z tą wszakże różnicą, że działa — by tak rzec — negatywnie i służy do kasowania;
  - *Exit* — można nazwać największym (ale nie jedynym przecież) potknięciem Autora tej książki, gdyż mój brak kompetencji (widoczny na każdej poprzedniej stronie), który z różnym skutkiem próbuję zneutralizować zapałem, do tej pory nie pozwolił mi jednak ogarnąć zasad działania tej funkcji, więc pozostaje wiara w to, że Czytelnicy okażą się bardziej inteligentni;
- *View*:
  - *Minimize to tray* — „chowa" program do ikony umieszczonej na pasku zadań;
  - *Hide* — „chowa" program całkowicie i, aby ponownie go zobaczyć, należy wcisnąć *ALT+PAGE UP*;
- *Attack*:
  - Jako że kryją się tu dokładnie takie same możliwości jak te zamknięte w ikonach, można pozwolić sobie na brak komentarza;
- *Tools*:
  - *Show current Windows user* — wskazuje użytkownika aktualnie zalogowanego doWindows;
  - *Show current Microsoft Network user* — wskazuje użytkownika aktualnie zalogowanego do Sieci;
  - *Change Windows password* — zmienia hasło dostępu do Windows;
  - *Change Screen Saver password* — zmienia hasło wygaszacza ekranu;
  - *Change Microsoft Network Password* — zmienia hasło dostępu do Sieci;
  - *Toggle password caching* — włącza lub wyłącza buforowanie hasła;

Jeżeli je wyłączymy, nie będzie możliwe zalogowanie się do Windows! Co ciekawe — próba sprawdzenia lub zmiany hasła przebiegnie bez zarzutu, lecz zalogowanie się będzie niemożliwe. Aby powrócić do poprzedniego stanu należy z dowolnego konta uruchomić Caina i ponownie włączyć *cache*.

- *Map network drive* — pozwala „podłączyć" katalog jako dodatkowe urządzenie;
- *Disconnect network drive* — pozwala na jego odłączenie;
- *Windows Logoff* — wylogowanie z Windows.

Nie wiem — to wspomniany wcześniej brak umiejętności, który z takim szacunkiem każe mi odnosić się do inteligencji i wiedzy hakerów — jak to się dzieje, że wylogowanie się za pomocą tej opcji nie zamyka programu Cain! Jednak jestem w stanie zauważyć skutki, a te zdają się — potrafię ocenić — zadowalające. Dają niepowtarzalną możliwość ciągłego łamania haseł, które może się odbywać pod naszą nieobecność. Ale miałem „drobne" problemy z tą opcją — teraz już już chyba wiadomo dlaczego, więc nie będę sypał głowy popiołem — i odrobinkę „zmodyfikowała" mi ona porządek na pulpicie. Nie zauważyłam mimo to żadnych większych wad — pytanie o przyczynę jest czysto retoryczne — i wciąż wydaje mi się, że warto z nią trochę poeksperymentować (oczywiście na własną odpowiedzialność, bo ze względu na brak wiedzy nie jestem w stanie niczego zagwarantować).

- *Windows restart* — restartowanie Windows;
- *Windows shutdown* — wyłączenie komputera.

Dobór skutecznego hasła

Kiedy omawia się szczegółowo sposoby łamania haseł, nie sposób nie powiedzieć jak można się przed tym ustrzec, to znaczy — jak wybrać hasło, aby było bezpieczne. Wbrew pozorom nie liczy się tylko jego długość, ale przede wszystkim — jego znaczenie, czyli wykorzystane nazwy, imiona, charakterystyczne słowa. Zostało stwierdzone, że w wielu przypadkach włamania się do systemu, wina nie leżała po stronie oprogramowania, lecz jej przyczyną było źle dobrane hasło. Poniżej znaleźć można kilka fundamentalnych porad, z których można skorzystać przy wymyślaniu i stosowaniu haseł.

Czego nie należy robić...	Przyczyna	Login	Przykład błędnego hasła
Stosować takiej samej nazwy dla login i hasła	Brak utrudnienia przy łamaniu hasła odgadnięcia	ziutek	ziutek
Stosować jako hasła odwróconego *Loginu*	Niektóre „łamacze" uwzględniają odwrócone hasła	ziutek	ketuiz
Dodawać cyfr po lub przed takim samym l:/p:	Podobnie jak poprzednio — „łamacze" to często uwzględniają	ziutek	ziutek1; 12ziutek
Stosować jako hasła podwojonego loginu	Niektóre łamacze to uwzględniają	ziutek	ziutekziutek
Stosować kojarzących się z osobą wyrazów	Łatwe do skojarzenia	ziutek	kowalski; ziootek; metalica

(nazwiska, pseudonimy, ulubione zespoły itp.)			
Używać nawet długich, ale popularnych słów z dowolnej dziedziny	Łatwe do złamania metodą słownikową	ziutek	helikopter; samochodowy1; hobbit
Stosować tendencyjnych haseł wymyślanych na podstawie rozłożenia klawiszy na klawiaturze	Łatwe do złamania metodą słownikową	ziutek	123456789; qwerty; qazwsx
Używać zbyt któtkich haseł (mniej niż sześć znaków)	Łatwe do złamania	ziutek	abc; aaa; c64
Używać takich samych, podobnych lub tendencyjnych haseł dla różnych kont	Odgadnięcie jednego może spowodować złamanie reszty haseł	zuitek	ziutekpoczta; ziutekftp
Zapisywania haseł w plikach na dysku, na kartkach, naklejania na monitorze itp.	Niepowołane osoby mogą je poznać	—	—
Podawania haseł innym	Nawet zaprzyjaźnieni ludzie mogą je wykorzystać	—	—

Skoro wiadomo, jakich haseł stosować nie należy, warto zapytać o poprawne metody zabezpieczenia kont. Najskuteczniejsze są tu hasła, które są długie i jako jeden ciąg nie mają żadnego znaczenia. Pomimo trudności z ich zapamiętaniem, spełniają swoje zadanie. Dodatkowo można wprowadzić znaki specjalne oraz cyfry. Przede wszystkim jednak, trzeba się zdać na własną inwencję.

Ograniczanie ryzyka

Przyjmując, że do zapisania hasła możemy użyć około stu dwudziestu znaków (w zależności od implementacji Uniksa niektóre znaki sterujące nie mogą być używane w hasłach), otrzymujemy 42 998 169 599 999 999 możliwych kombinacji.

Nawet ograniczając zestaw znaków stosowanych tylko do małych i dużych liter, cyfr, oraz około osiemnastu znaków specjalnych (!@#$%^&*()_+—={}[]<>), liczba wszystkich możliwych ich kombinacji 1— 2— 3— 4— 5— 6— 7— 8— znakowych wynosi 1 677 721 599 999 999.

Porównanie tej liczby z liczbą wszystkich możliwych słów w najważniejszych językach świata prowadzi do wniosku, że szansę, aby czyjeś hasło znajdowało się w słowniku używanym przez hakera są rzędu 1/100 000 000. Niemniej, aby ta wielkość była tak niska, trzeba przestrzegać kilku zasad, które zamieszczone zostały poniżej.

Dobre hasło: **Złe hasło:**

- Powinno zawierać duże i małe litery.
- Powinno zawierać cyfry i znaki przestankowe.
- Może zawierać spacje.
- Powinno być łatwe do zapamiętania.
- Powinno mieć co najmniej siedem liter.
- Imię własne, dziecka, zwierzęcia, współpracownika, przyjaciela lub też nazwisko, pseudonim.
- Nazwa systemu operacyjnego.
- Numer telefonu użytkownika.
- Data urodzenia.
- Informacje łatwo dostępne.
- Kombinacja klawiszy.
- Postacie z literatury, filmu
- Popularne słowa.
- Wszystkie poprzednie możliwości zapisane od tyłu.
- Wszystkie poprzednie możliwości z dopisanym z przodu lub z tyłu pojedynczym znakiem.

Najważniejsze techniki ochrony

Najczęściej pliki z hasłami stają się obiektem hakerskich ataków. Istnieje jednak wiele sposobów ochrony. W przypadku sporadycznego łączenia się z odległymi komputerami, często stosowaną techniką jest ustalenie ważności hasła tylko dla jednego połączenia. Może się zdarzyć, że przy nawiązaniu połączenia hasło zostanie podsłuchane i dlatego przed „opuszczeniem" systemu, należy je zmienić.

Wiele systemów operacyjnych ma możliwość narzucenia użytkownikom odpowiedniej „polityki" wprowadzania haseł (co jakiś czas ulegają one przedawnieniu i użytkownik zmuszony jest do wprowadzenia nowego hasła). System może również wymagać od użytkownika odpowiedniej konstrukcji hasła, która jest kombinacją liter i znaków specjalnych. Czasem administrator ma także możliwość przedawnienia ważności kont użytkowników (czyli ich haseł).

Bardzo bezpiecznym mechanizmem służącym do ochrony haseł są karty magnetyczne weryfikujące dostęp. Wygenerowane hasło charakteryzuje bowiem bardzo trudna do złamania kombinacja i odpowiednia długość. Jako że użytkownik nie musi pamiętać hasła, rozwiązania te wygodne, ale i są bardzo drogie, więc mogą sobie na nie pozwolić tylko bogate firmy.

Systemy jednokrotnych haseł często są stosowane w systemach o hierarchicznej, protegowanej strukturze dostępu. Użytkownik jest wówczas zmuszony do ustalenia dużej ilości haseł w zależności od typu danych i aplikacji.

Systemy haseł jednakowego użycia należą do jednych z najbardziej zaawansowanych technologicznie rozwiązań. Hasło zawarte jest na specjalnej karcie, która je generuje. Następnie hasło jest weryfikowane przez dedykowany serwer na podstawie PIN-u. Hasło tego typu ważne jest około minuty.

Konie trojańskie

Podstawowe informacje o tzw. *koniach trojańskich* przedstawione zostały już wcześniej, jednak mimo to watro przybliżyć sposób ich działania.

Koń trojański to krótko mówiąc program „udający" nieszkodliwą aplikację, która po uruchomieniu oprócz spodziewanej funkcji (zwykle jednak działanie to kończy się komunikatem o błędzie) dokonuje spustoszenia w systemie operacyjnym.

W wielu przypadkach koń trojański automatycznie instaluje się w katalogu *Windows* lub w folderze systemowym, przybierając nazwę jednej z aplikacji systemu Windows lub sterownika. Dokonuje również wpisu w rejestrze (sekcja „Run"; dzięki temu jest uruchamiany wraz ze startem systemu), nadając sobie atrybut „ukryty". Opis ten dotyczy jednak programu zwanego serwerem (działającego na komputerze ofiary), który drogą sieciową odbiera polecenia od programu klienta (działającego na komputerze hakera). Starsze trojany wykorzystywały do komunikacji program Telnet, jednak został on zastąpiony specjalnymi aplikacjami posiadającymi szereg funkcji.

Powiadamianie o obecności ofiary w Sieci można osiągnąć na kilka sposobów. Najprostszy polega na wysłaniu odpowiedniego listu. Ale może się zdarzyć, że trojan nie posiada takiej funkcji i wtedy pozostaje wykorzystanie skanera portów. Włamywacz może skorzystać z zewnętrznego lub wewnętrznego skanera konia trojańskiego (taką opcję posiada tylko kilka z nich). W przypadku, gdy atak nie został wymierzony w kierunku konkretnej osoby, włamywacz może skorzystać z komputerów udostępnionych przez innych włamywaczy. Jednak nie nad każdym systemem można przejąć kontrolę. Włamywacz może założyć hasło na serwerze, uniemożliwiając innym dostęp do danej maszyny.

Koni trojańskich można pozbywać się „ręcznie" za pomocą programów antywirusowych lub przy użyciu „specjalnych" aplikacji. Pierwsza metoda nie należy do najwygodniejszych, ale czasami okazuje się jedyna. Na początku należy przy użyciu skanera sprawdzić otwarte porty. Jednak z uwagi na ich dużą liczbę praca ta zajęłaby sporo czasu, warto więc sprawdzić najpierw te porty, które są najczęściej wykorzystywane przez konie trojańskie. Będą to:

- Backdoor 2 — 1999;
- BO — 31337;
- Bowl — 1981;
- GateCrasher — 6969;
- GirlFriend — 21554;

- Master's Paradise — 31, 40421, 40426;
- NetBus — 12345, 12346;
- NetSpy — 1025;
- phAse — 555;
- Prosiak — 44444, 33333;
- Sockets de Troie — 5000;
- StealthSpy — 555;
- T5Port — 31337;
- Web EX — 1001;
- StealthSpy, phase — 31.

Trojany umieszczają odpowiednie wstawki w rejestrze, więc należy sprawdzić zawartość klucza:

HKEY_LOCAL_MACHINE/Software/Microsoft/Windows/CurrentVersion.

Szczególną uwagę trzeba zwrócić na następujące klucze: *Run*, *RunOnce*, *RunOnceEx*, *RunServicesOnce*. Jeżeli uda nam się znaleźć podejrzany klucz należy go usunąć, co spowoduje unieruchomienie trojana, a po wykonaniu tej operacji można usunąć go z dysku.

Poniżej znajduje się opis kilkunastu najbardziej pospolitych koni trojańskich (wraz z różnymi ich wersjami).

Należy jednak pamiętać o tym, że nie są to wszystkie backdoory, jakie się mogą pojawić w sieciach komputerowych, a jedynie najpopularniejsze z nich. Zostały podzielone na dwie kategorie:

- Aplikacje nie mające GUI, a więc takie, których klientem jest program Telnet;
- Aplikacje z własnym GUI, składające się z dwóch części: instalowanym na komputerze ofiary serwerze i kliencie uruchamianym na komputerze włamywacza.

APLIKACJE WYKORZYSTUJĄCE TELNET

T5Port 1.0

Jest to niewielki program (18 432 b), najprostszy w swojej kategorii, który pojawił się jako jeden z pierwszych trojanów. Nie ma żadnego programu instalacyjnego czy też konfiguracyjnego. Zajmuje port 31337 na komputerze ofiary. Połączenie odbywa się poprzez program służący do łączenia się z terminalem (np. Telnet). Wystarczy wybrać w menu *Połącz* opcję *System Zdalny* i wpisać w *Nazwie Hosta* adres IP atakowanego komputera, a w *Porcie* wartość — `31337`, aby zaczął działać. Po nawiązaniu łączności należy wpisać domyślne hasło, którego nie można już zmienić. Jest nim znane hakerom słowo „satan". Uruchomiony na komputerze ofiary aktywny jest tylko podczas trwania sesji Windows. Aby się w nim zagnieździć, potrzebny jest „ręczny" wpis do rejestru systemowego. Oznacza to, iż łatwo go dezaktywować, ale znacznie trudniej wykryć w systemie (włamywacz może nadać mu taką nazwę, jaka tylko mu przyjdzie do głowy). Jest on niezbyt rozbudowany, o czym świadczą komendy podobne do tych, które znamy z systemu MS-DOS:

- `exec` — uruchomienie aplikacji na komputerze ofiary;
- `cmd` — uruchomienie komendy systemowej;
- `annoy` — wyświetlenie komunikatu o błędzie;
- `shutdown` — resetujowanie komputera ofiary;
- `exit` — zamknięcie sesji;
- `die` — „zabicie" sesji serwera (usunięcie z pamięci);
- `help` — wyświetlenie tematów pomocy.

Sosób usunięcia z systemu:

T5Port nie jest wykrywany przez programy antywirusowe. Należy usunąć go „ręcznie". W tym celu:

1. Trzeba sprawdzić za pomocą skanera portów, czy jest otwarty port 31337 (uwaga: ten port jest również używany przez Back Orifice'a). Jeśli wynik będzie pozytywny, należy sprawdzić, jakie procesy są uruchomione w obecnej sesji Windows. Trzeba ustalić, jak nazywa się potencjalny trojan (często dokładne ustalenie nazwy nie jest możliwe). Jeśli jednak znana jest nazwa pliku, to wystarczy odnaleźć go na dysku lokalnym i porównać z podanym wyżej rozmiarem. Jeśli będzie pasował – istnieje duża szansa na to, że jest to trojan. Następnie trzeba uruchomić *Edytor Rejestru* (pamiętając o sporządzeniu kopii plików systemowych) i znaleźć klucz o nazwie, takiej jak nazwa pliku (powinien być w : *HKEY_LOCAL_MACHINE/Software/Microsoft/Windows/CurrentVersion/RUN lub ~/RUNONCE,* lub *~/RUNSERVICES* itp.). Kolejnym krokiem jest skasowanie klucza, będącego nazwą ustalonego pliku. Jeśli w katalogach *RUN, RUNONCE, RUNSERVICES* nie ma takiej nazwy, to zadanie jest ułatwione, gdyż oznacza to, że trojan nie jest zapisany w rejestrze i wystarczy zresetować Windows, aby się go pozbyć.
2. Po wykonaniu powyższych poleceń należy zresetować system.
3. Po ponownym uruchomieniu można odszukać backdoora na dysku lokalnym i usunąć go do kosza – jeśli system skasuje go, to oznacza pozbycie się trojana. W przeciwnym wypadku pojawia się informacja o tym, że „podany plik jest używany przez system Windows". Trzeba więc znowu wrócić do pierwszego kroku i zlokalizować trojana (przywracając skasowany plik i pliki rejestru z uprzednio stworzonego katalogu zapasowego).

BOWL 1.0

Program składa się z dwóch plików: głównego o nazwie *bowl.exe* (38 912 b) i pomocniczego służącego do konfiguracji o nazwie *config.exe* (15 360 b). Konfiguracja polega na ustawieniu hasła serwera (domyślnym hasłem jest „allnewbowl") i zainstalowaniu go w systemie. Komunikacja z serwerem odbywa się poprzez program służący do łączenia się z terminalem (np. Telnet).

Należy zatem wybrać w menu *Połącz* opcję *System Zdalny* i wpisać w *Nazwie Hosta* adres IP atakowanego komputera, a w *Porcie* wartość `1981`. Po nawiązaniu łączności trzeba natomiast wpisać skonfigurowane wcześniej hasło. Po tym zabiegu w oknie telnetowym hakera powinien pokazać się serwer Bowla, który podaje konfigurację systemu ofiary. W przypadku błędnego hasła połączenie zostaje zerwane. Komendy wydawane są na wzór MS-DOS. Dostępne polecenia to:

- `beep` — generowanie sygnału dźwiękowego;
- `cat` — wyświetlenie zawartości plików;
- `cd/chdir` — przechodzenie pomiędzy katalogami;
- `clear` — wyczyszczenie ekranu;
- `cmd[v]` — uruchomienie niewidzialnego dla ofiary *command.com* (MS-DOS);
- `cmdr` — uruchomienie programu i wypisanie rezultatu po jego zakończeniu (przerwanie – klawisz ESC);
- `del/rm` — usunięcie jednego lub kilku plików;
- `die` — „zabicie” sesji serwera (usunięcie z pamięci);
- `dir/ls` — wyświetlenie istniejących katalogów;
- `errormsg` — wyświetlenie komunikatu o błędzie;
- `exec[v]` — uruchomienie programu niewidzialnego dla ofiary [widzialny];
- `freeze` — zawieszenie systemu ofiary;
- `get` — ściągnięcie pliku z komputera ofiary (włamywacz zwykle uruchamia przeglądarkę internetową i wpisuje adres: *http://IP.ofiary:1982/nazwa_pliku);*
- `graphoff` — wyłączenie trybu graficznego;
- `kill` — „zabicie” aktywnego procesu;

- `md/mkdir` — utworzenie katalogu;
- `passwd` — wypisanie hasła: MS Internet Mail, Netscape Navigator oraz zasobów sieciowych;
- `ps` — lista aktywnych procesów (nazwa procesu | numer procesu | ścieżka dostępu programu);
- `quit` — zamknięcie klienta;
- `rd/rmdir` — usunięcie pustych katalogów;
- `shutdown` — resetowanie komputera ofiary;
- `swapmouse` — zamiana klawiszy myszki;
- `telnet` — łączenie się Telnetu z innym hostem;
- `vied` — prosty edytor tekstu (do 1024 linii i 256 znaków na każdą)

Sosób usunięcia z systemu:

Bowl nie jest wykrywany przez programy antywirusowe. Należy usunąć go „ręcznie”, a w tym celu trzeba wykonać kolejno poniższe polecenia:

- Usunąć z *Rejestru Systemowego* w kluczu *HKEY_LOCAL_MACHINE/ Software/Microsoft/Windows/currentversion/runservices* wpis: „networkpopup”.
- Zresetować system;
- Usunąć plik *C:/WINDOWS/netpopup.exe;*
- Sprawdzić, czy na dysku nie ma pliku *bowl.exe.*

ACID SHIVER

AS to narzędzie służące nie tylko do przejmowania kontroli nad czyimś komputerem, ale również do generowania konia trojańskiego, który może zostać uruchomiony na komputerze ofiary. Pakiet składa się z dwóch części: aplikacji konfiguracyjnej (domyślnie nazywa się ona *ACiD Setup.exe* i ma 14 336 b) oraz serwera (domyślnie: *AciDShivers.exe* — 186 368 b). .Za pomocą pierwszej z nich włamywacz tworzy dowolnie nazywający się plik, w skład którego wchodzą: serwer oraz serwer SMTP (służący do przesyłania poczty) i adres e-mailowy włamywacza. Aplikacja ma ikonę łudząco przypominającą programy instalacyjne Microsoftu. Backdoor wyróżnia się na tle innych, gdyż aplikacja ta „próbuje" w każdej sesji Windows połączyć się ze skonfigurowanym przez włamywacza serwerem pocztowym i wysłać na podany przez niego adres informację o posiadanym przez ofiarę numerze IP oraz porcie, przez który możliwa będzie komunikacja (port ten zmienia się za każdym razem). Nie przyda się więc w sieci lokalnej nie posiadającej własnego serwera pocztowego. Na dodatek AS to projekt otwarty, który udostępniany jest wraz z kodem źródłowym i każdy użytkownik – programista czy haker — może dodać coś od siebie. AS wykrywany jest przez większość markowych programów antywirusowych. Serwer potrzebuje do działania następujące pliki: *MSvbvm 50.dll* oraz *MSwinsck.ocx.* Główne komendy to:

- `HELP` <komenda> — pomoc;
- `BEEP` <#> — generowanie dźwięku;
- `BOUNCE` <host> <port> — przekierunkowanie połączenia na dany host i port;
- `CAT` <plik> — wyświetlanie zawartości pliku;
- `CD` <katalog> — zmiana katalogu;
- `CLS` — czyszczenie ekranu;
- `CMD` <komenda> — uruchomienie komendy;
- `COPY` <plik1> <plik2> — kopiowanie — plik1 na plik2;
- `DATE` — pokazanie daty;
- `DEL` <plik> — skasowanie pliku;
- `DESK` — zmiana na domyślny katalogu z zawartością pulpitu;
- `DIE` — wyłączenie AS;
- `DIR` — wyświetlenie listy katalogów;
- `DRIVE` <napęd> — podanie informacji o napędzie;
- `DRIVES` — wyświetlenie zawartości dysków, RAM-dysków, CD-ROM-ów;
- `ENV` — wyświetlenie zmiennych systemowych DOS-a;
- `GET` <plik> — ściągnięcie z serwera wskazanego pliku;

- `HIDE` <PID> — ukrycie aplikacji o danym <PID> (identyfikatorze) widocznej w menedżerze programów (lista aplikacji pokazująca się po wciśnięciu kombinacji: CTRL+ALT+DEL);
- `INFO` — ujawnienie informacji o komputerze ofiary i użytkowniku;
- `KILL` — „zabicie" aktywnego procesu;
- `LABEL` <napęd> — zmiana etykiety dysku;
- `LS` — działanie podobne do DIR;
- `MKDIR` <katalog> — zakładanie katalogów;
- `NAME` <nazwa> — zmiana nazwy komputera ofiary;
- `PORT` <#> — zmiana portu AS;
- `PS` — lista aktywnych procesów;
- `RMDIR` <katalog> — przenoszenie katalogów wraz z podkatalogami i plikami;
- `S` — wysyłanie kombinacji klawiszy do aktywnej aplikacji;
- `SH` <komenda> — działanie podobne jak opisane wyżej i ujawnienie rezultatów;
- `SHOWS` <PID> — pokazanie aplikacji;
- `SHUTDOWN` — resetowanie serwera;
- `TIME` — pokazanie czasu;
- `VERSION` — pokazanie numeru wersji AS.

Sposób usunięcia z systemu:

AS jest wykrywany przez markowe programy antywirusowe. Można usunąć go „ręcznie", gdyż AS pozostawia po sobie wpis „Explorer" = „*C:/WINDOWS/ MSG SVR16.EXE*" (serwer przyjmuje stałą nazwę pliku) w *Rejestrze Systemowym* w kluczach: *HKEY_LOCAL_MACHINE/Software/Microsoft/Windows/CurrentVersion/Run; HKEY_LOCAL_MACHINE/Software/Microsoft/Windows/CurrentVersion/RunServices.* Standardowa procedura polega na usunięciu tego wpisu, zresetowaniu komputera i skasowaniu pliku: *C:/WINDOWS/MSGSVR16.EXE.*

Istnieje również zmieniona przez LEENTech Corporation *(Living in an Evolution of Enhanced Networking Technology*) wersja AcidShiver. Różni się nie tylko wielkością serwera (188 416 b), ale również jego nazwą — *tour98.exe oraz* wpisem „*WinTour"=„C:/WINDOWS/WINTOUR.EXE*" w rejestrze (w kluczach: *HKEY_LOCAL _MACHINE/Software/Microsoft/Windows/CurrentVersion/Run* i *HKEY_LOCAL _MACHINE/Software/Microsoft/Windows/CurrentVersion/RunServices*).

Dodano również nowe funkcje:

- `BCAT` <plik> lub `BGET` <plik> – wyświetlenie zawartości pliku binarnego;
- `MACADDR` — ujawnienie statusu połączenia ethernetowego;
- `RECENT` — kasowanie folderu *RECENT* (z ostatnio uruchomionymi dokumentami);
- `STATUS` — ujawnienie statusu wszystkich używanych od początku sesji Windows portów;
- `WSFTP` — ustawienie domyślnego folder *WS_FTP*.

Nowy AS jest już wykrywany przez programy antywirusowe.

Aplikacje wykorzystujące klienta

BACK ORIFICE

Back Orifice jest niezłym narzędziem służącym do administrowania komputerem ofiary. Łączy w sobie cechy wcześniejszych aplikacji (Bowla, T5Porta), udostępnia konsolę tekstową oraz aplikację typu klient-serwer, a ponadto ma ciekawy, niestandardowy interfejs GUI. Działa on tylko na komputerach z zainstalowanym systemem Windows 95 i 98. Jego instalacja przebiega szybko i sprawnie — pakiet składa się bowiem z kilku plików:

- *bo.txt* — dokumentacja BO (15 184b);
- *plugin.txt* — dokumentacja modułu rozszerzającego BO (914b);

- *boserve.exe* — samoinstalujący się serwer BO (124 928b);
- *bogui.exe* — klient graficzny BO (284 160b);
- *boclient.exe* — klient tekstowy BO (57 856b);
- *boconfig.exe* — konfiguracja BO (28 672b);
- *melt.exe* — dekompresor plików spakowanych programem freeze (29 184b);
- *freeze.exe* — kompresor plików (33 280b).

Najważniejszą częścią BO jest serwer o nazwie *boserve.exe*. Wystarczy uruchomić go kliknięciem lub naciśnięciem klawisza *Enter*, aby zainstalował się „bezszelestnie" w katalogu systemowym. Aby go skonfigurować, należy posłużyć się programem *boconfig.exe*, który może również dołączyć się do innych plików wykonywalnych w ten sam sposób, jak to robią wirusy. Dwa kolejne wykonywalne pliki w pakiecie są używane przez konia trojańskiego podczas kompresji (*freeze.exe*) lub dekompresji (*melt.exe*) plików na komputerze ofiary. Uruchomiony po raz pierwszy serwer BO tworzy plik *windll.dll* w katalogu systemowym Windows (plik ten jest zawarty w kodzie konia trojańskiego), a potem wyszukuje aktualnie uruchomione przez poprzednią wersję programu procesy, zakańcza je i uaktualnia uruchamiając własne. Następnie kopiuje sam siebie do katalogu systemowego Windows (pod nazwą „*.exe*" i rejestruje się w rejestrze jako jedna z usług autostartu). Później przydziela sobie port numer 31337 (identyczny do T5Port) i zaczyna nasłuchiwanie. Komendy można wpisywać korzystając z pomocy aplikacji o graficznym GUI lub w konsoli tekstowej. Zależnie od wydanego polecenia trojan może podejmować następujące działania:

- `App add` — uruchomianie tekstowej aplikacji gotowej do „nasłuchu" przez port (dostępnych później przez Telnet);
- `App del` — zatrzymanie działania opisanej wyżej aplikacji;
- `Apps list` — wyświetlenie listy uruchomionych wyżej aplikacji;
- `Directory create` — tworzenie na serwerze katalogu;
- `Directory list` — wyświetlenie listy katalogów na serwerze;
- `Directory remove` — usunięcie katalogów;
- `Export add`;
- `Export delete`;
- `Exports list`;
- `File copy` — kopiowanie jednego lub kilku plików;
- `File delete` — kasowanie jednego lub kilku plików;
- `File find` — szukanie jednego lub kilku plików;
- `File freeze` — kompresowanie jednego lub kilku plików;

- `File melt` — dekompresowanie jednego lub kilku plików;
- `File view` — przegląd pliku tekstowego;
- `HTTP Disable` — wyłączenie serwera http;
- `HTTP Enable` — włączenie serwera http (można uzyskać dostęp do komputera przez przeglądarkę);
- `Keylog begin` — logowanie sekwencji wciskanych przez ofiarę klawiszy;
- `Keylog end` — zakończenie logowania;
- `MM Capture avi` — przechwycenie obrazu video wraz z dźwiękiem z serwera;
- `MM Capture frame` — przechwycenie pojedynczych klatek;
- `MM Capture screen` — przechwycenie obrazu (*screenshot*);
- `MM List capture devices` — lista przechwytujących urządzeń;
- `MM Play sound` — odtworzenie dźwięku na serwerze;
- `Net connections` — lista połączeń sieciowych;
- `Net delete` — odłączenie serwera ofiary od Sieci;
- `Net use` — przyłączenie serwera ofiary do Sieci;
- `Net view` — wyświetlenie wszystkich informacji dotyczących Sieci (serwerów, udostępnionych katalogów lub dysków);
- `Ping host` — pingowanie serwera;
- `Plugin execute` — uruchomienie modułu rozszerzającego BO;
- `Plugin kill` — zakończenie działania modułu rozszerzającego BO;
- `Plugins list` — wyświetlenie listy dostępnych modułów rozszerzających BO;
- `Process kill` — zakończenie procesu;
- `Process list` — wyświetlenie listy dostępnych procesów;
- `Process spawn` — uruchomienie program jako ukrytego lub widocznego na serwerze;
- `Redir add` — przekierunkowanie zasobów TCP/IP (połączenia);
- `Redir del` — usunięcie przekierunkowania zasobów TCP/IP;
- `Redirs list` — wyświetlenie listy dostępnych przekierunkowań zasobów TCP/IP;
- `Reg create key` — utworzenie klucza w *Rejestrze Systemowym*;

- `Reg delete key` — kasowanie klucza;
- `Reg delete value` — kasowanie wartości klucza;
- `Reg list keys` — wyświetlenie listy kluczy rejestru;
- `Reg list values` — wyświetlenie wartości klucza;
- `Reg set value` — ustawienie wartości klucza (binarna, DWORD, string);
- `Resolve host` — zamiana nazwy domeny na adres IP;
- `System dialogbox` — wyświetlenie okienka dialogowego z komunikatem i przyciskiem OK;
- `System info` — wyświetlenie informacji o serwerze;
- `System lockup` — zawieszenie systemu;
- `System passwords` — podanie hasła systemowego serwera;
- `System reboot` — resetowanie serwera;
- `TCP/IP file receive` — łączenie serwera z podanym IP i zapisanie do pliku ściągniętych danych;
- `TCP/IP file send` — łączenie serwera z podanym IP i przesyłanie danych;

Możliwości tego konia trojańskiego skutecznie rozbudowują rozmaite moduły rozszerzające. Mogą one być wysyłane do „serwera" i instalowane.

Sposób usunięcia z systemu:

Back Orifice jest wykrywany przez programy antywirusowe. Jeśli dysponujemy najnowszą sygnaturą wirusów, to problem BO jest rozwiązany. Jeśli nie, musimy ją ściągnąć z Internetu.

Możemy także użyć programów do wykrywania BO. W Sieci znajdziemy ich całą masę. Najbardziej znane to: Bored 0.2 executable i BoDetect v1.0.2. oraz NOBO.

Gdy chcemy to zrobić „ręcznie" musimy najpierw uruchomić *Edytor Rejestru* (*regedit.exe*) i znaleźć klucz (*HKEY_LOCAL_MACHINE/Software/Microsoft/Windows/Current Version/RunServices)*. Później usuwamy wartość o nazwie „*.exe*". Resetujemy system. Z katalogu *C:/WINDOWS/SYSTEM* usuwamy pliki z rozszerzeniem *.exe* i *windll.dll*. Nasz system jest od tej pory bezpieczny.

DEEP THROAT REMOTE 1.0

Program składa się z dwóch plików: serwera *systempatch.exe* (260 971 b) oraz klienta *RemoteControl.exe* (271 959 b). Serwer DTR 1.0 nie jest zabezpieczany ha-

słem, więc dostęp do niego jest możliwy z każdego klienta programu. Aplikacja działa tylko na komputerach z zainstalowanym systemem Windows 95 i 98.

Program wyposażony został w następujące funkcje:

- Otwieranie i zamykanie CD-ROM-u na serwerze;
- Uruchamianie okienka dialogowego z komunikatem;
- Chowanie i przywracanie paska startowego Windows;
- Serwer FTP umożliwiający ściągnięcie dowolnego pliku z komputera ofiary (aby tego dokonać niezbędny jest klient FTP, np. Cute FTP lub WS_FTP);
- Zrzut ekranu serwera (dzięki temu można zobaczyć aktualny ekran na serwerze, np. pulpit ofiary),
- Otwarcie adresu internetowego na serwerze;
- Włączenie trybu oszczędzania energii;
- W wersji późniejszej niż 1.0 — kradzież hasła systemowego;
- Uruchamianie programów na serwerze (widzialne lub nie);
- Resetowanie serwera;
- Skaner obecności serwera DTR na hostach;
- Pingowanie (przesyłanie pakietu informacji) hosta w celu sprawdzenia aktywności serwera DTR;
- Podanie dokładnych informacji o komputerze ofiary.

Sposób usunięcia z systemu:

DTR jest wykrywany przez większość znanych programów antywirusowych.

Jeśli nie mamy takiego programu lub brakuje nam najnowszej sygnatury znanych wirusów, możemy usunąć program „ręcznie".

W tym celu uruchamiamy *Edytor Rejestru* i odnajdujemy klucz o nazwie *HKEY_LOCAL_MACHINE/Software/Microsoft/Windows/CurrentVersion/Run*. W kluczu tym znajdujemy wpis „SystemDLL32" i zapamiętujemy nazwę skojarzonej z nim aplikacji (powinna się nazywać: „*SYSTEMPATCH.EXE*"). Następnie kasujemy wpis.

Resetujemy komputer. Po ponownym uruchomieniu Windows odszukujemy na dysku aplikację i kasujemy ją. Nasz system jest od tej pory bezpieczny.

MASTER'S PARADISE

W przypadku MP twórca programu jest znany. Jest nim niemiecki programista Dan Lehman. MP składa się z dwóch części. Serwer może być dołączony do praktycznie każdej aplikacji. W Internecie upowszechnił się poprzez dołączenie do popularnej gry-parodii — „Pie Bill Gates" (rzucanie ciastkiem w Billa Gatesa), gdzie zagnieździł się w pliku *game.exe*. Uruchomienie tej gry powoduje jednocześnie zarażenie systemu koniem trojańskim (najczęściej poprzez zainstalowanie gry, której nielegalna dystrybucja rozpowszechniona jest w samorozpakowujących się archiwach programu TurboSFX). Aplikacja działa tylko na komputerach z zainstalowanym systemem Windows 95 i 98. Program wyposażono w różne funkcje:

- Otwieranie lub zamykanie CD-ROM-u (pojedyncze lub w określonych odstępach czasu);
- „Podsłuchiwanie" ofiary — przesyłanie ciągu wystukiwanych na serwerze znaków;
- Chowanie, pokazywanie i wyłączanie okien aplikacji na serwerze;
- Generowanie dźwięku wciskanych klawiszy;
- Nagrywanie dźwięku przez mikrofon ofiary;

- Nawigacja myszką ofiary;
- Odtworzenie dźwięku na komputerze ofiary;
- Otwarcie adresu internetowego na serwerze;
- Przesyłanie dowolnych plików na serwer;
- Screenshot — zrzut ekranu ofiary;
- Ściąganie i kasowanie dowolnego pliku na serwerze;
- Uruchomienie aplikacji na serwerze;
- Wyłączenie dowolnego klawisza;
- Wysłanie komunikatu do ofiary.;
- Wysyłanie tekstu do aktywnej aplikacji;
- Wyświetlenie dokładnych informacji o komputerze;
- Wyświetlenie na ekranie ofiary obrazka;
- Zamiana przycisków myszki: prawy na lewy i na odwrót;
- Zmiana głośności dźwięku;
- Zresetowanie, wylogowanie ofiary.

Sposób usunięcia z systemu:

MP jest wykrywany przez większość znanych programów antywirusowych. Usuwa go także aplikacja wykrywająca Back Orifice'a: BOClean 2.01

Jeśli nie mamy programu wykrywającego wirusy lub najnowszej sygnatury znanych wirusów, możemy usunąć program „ręcznie" lub ściągnąć sygnaturę z Internetu.

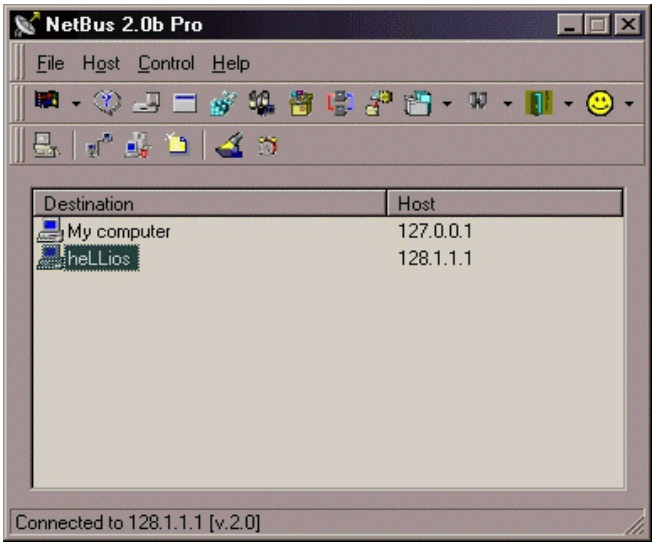
MP instaluje się do systemu poprzez zastąpienie programu *sysedit.exe* swoim serwerem oraz biblioteki *KeyHook.dll* znajdującej się w katalogu Windows lub katalogu systemowym (*C:/WINDOWS* lub *C:/WINDOWS/SYSTEM*). O ile odzyskanie tego pierwszego pliku nie sprawia większych trudności (jest dołączany do każdej dystrybucji programu instalacyjnego systemu), to z przywróceniem drugiego pliku są już większe problemy, gdyż jest on dołączany do niektórych tylko programów. Trzeba więc znaleźć go w ich wersjach instalacyjnych lub w Internecie.

Uruchamiamy *Edytor Rejestru* i odnajdujemy klucz o nazwie: *HKEY_LOCAL_MACHINE/Software/Microsoft/Windows/CurrentVersion/Run*. W kluczu tym znajdujemy wpis i zapamiętujemy nazwę skojarzonej z nim aplikacji (powinna się nazywać: „*SYSEDIT.EXE*"). Kasujemy wpis.

Resetujemy komputer. Po ponownym uruchomieniu Windows odszukujemy na dysku aplikację i kasujemy ją. Kasujemy również bibliotekę *KeyHook.dll* i przy-

wracamy powyższe pliki z oryginalnych wersji instalacyjnych. Nasz system jest od tej pory bezpieczny.

NETBUS 2.0



Podobnie jak w przypadku wcześniejszego Master's Paradise znamy twórcę Netbusa. Jest nim Carl-Fredrik Neikter. Co ciekawe, wersja 2.0 jest programem sharewareu, który należy zarejestrować [istnieją dwa rodzaje licencji: „na użytek domowy" oraz dla firm i organizacji (pojedyncze lub stanowiskowe)]. Opłata jest związana, jak twierdzi autor, nie z komercyjną działalnością, ale ze wsparciem jego działań. Wersja 1.6 składa się z dwóch najważniejszych plików (nie mówiąc o dokumentacji): serwera o nazwie *Patch.exe* (472 576 b) oraz klienta — *NetBus.exe* (567 296 b). Wersja 1.7 to pliki o tej samej nazwie, ale innym rozmiarze: 494 592 b (serwer) i 599 552 b (klient). Obie wersje instalują się domyślnie na portach 12345 lub 12346. Najnowsza wersja rozpowszechniana jest w charakterystycznej dla znanych programów dystrybucji InstallShield(r) Wizard i jej serwer zajmuje domyślnie port 20034.

Ustawienia serwera zmienić można za pomocą programu instalacyjnego lub po połączeniu się z klientem. W wersjach wcześniejszych od 2.0 wystarczy tylko uruchomić serwer (jego nazwa może się dowolnie różnić od *patch.exe*, można też stosować parametry: */noadd,/remove,/pass:xxx,/port:xxx*), aby stał się aktywny podczas każdej sesji Windows.

NetBus ma funkcje podobne do wcześniejszych koni trojańskich. Są to:

- Otwieranie, zamykanie CD-ROM-u (pojedyncze lub w określonych odstępach czasu);

- „Podsłuchiwanie” ofiary — przesyłanie ciągu wystukiwanych na serwerze znaków;
- Chowanie, pokazywanie i wyłączanie okien aplikacji na serwerze;
- Generowanie dźwięku wciskanych klawiszy;
- Nagrywanie dźwięku przez mikrofon ofiary;
- Nawigacja myszką ofiary;
- Odtworzenie dźwięku na komputerze ofiary (format *wav*);
- Otwarcie adresu internetowego na serwerze;
- Powiadamianie e-mailowe o obecności ofiary w Sieci;
- Przesyłanie dowolnych plików na serwer;
- Przekierunkowanie danych ze specyficznego portu na podany host i na odwrót (możliwość sterowania aplikacją ofiary z komputera włamywacza przez konsolę telnetową);
- Screenshot — zrzut ekranu ofiary;
- Skaner serwerów NetBusa w Sieci;
- Ściąganie i kasowanie dowolnego pliku na serwerze;
- Uruchomienie aplikacji na serwerze;
- Wyłączenie dowolnego klawisza;
- Wysłanie komunikatu do ofiary;
- Wysyłanie tekstu do aktywnej aplikacji;
- Wyświetlenie dokładnej informacji o komputerze;
- Wyświetlenie na ekranie ofiary obrazka (w formacie *bmp* i *jpg*);
- Zamiana przycisków myszki: prawy na lewy i na odwrót;
- Zmiana głośności dźwięku;
- Zmiana konfiguracji serwera NetBusa (port, hasło, itp.);
- Zresetowanie, wylogowanie ofiary.

W wersji 2.0 wprowadzono następujące zmiany:

- Zmieniono GUI;
- Zwiększono wydajność;
- Zmieniono menedżera plików;
- Zmieniono menedżera okien;

- Dodano menedżera *Rejestru Systemowego*;
- Dodano menedżera modułów rozszerzających;
- Dodano możliwość ściągnięcia filmu z serwera;
- Dodano możliwość kradzieży haseł systemowych;
- Dodano klienta Chatu z innymi użytkownikami NetBusa (sic!).

Sposób usunięcia z systemu:

NetBus jest wykrywany przez większość znanych programów antywirusowych. Usuwa go także aplikacja NetBus Remover.

Jeśli nie mamy programu wykrywającego wirusy lub najnowszej sygnatury znanych wirusów, możemy usunąć program „ręcznie" lub ściągnąć sygnaturę z Internetu.

Wykrycie NetBusa jest trudne, ponieważ jego serwer może przyjąć każdą nazwę. Na szczęście można go odkryć w *Rejestrze Systemowym*. NetBus pozostawia takie wpisy jak: *HKEY_CURRENT_USER/NETBUS 1.6, HKEY_CURRENT_USER/NETBUS 1.7, HKEY_CURRENT_USER/NetBus, HKEY_CURRENT_USER/NetBus Server* (dwa ostatnie to wersja 2.0, a wtedy wystarczy tylko odszukać klucz *HKEY_CURRENT_USER/NetBus/Transfer*, w którym podana jest ścieżka serwera, usunąć dwa wcześniejsze klucze, zresetować komputer i w następnej sesji Windows usunąć serwer oraz plik *NBHelp.dll*).

Wcześniejsze wersje NetBusa trudniej jest wykryć (chyba że włamywacz nie pofatygował się i nie zmienił nazwy serwera — wówczas jest nim plik o nazwie *Patch.exe*). NetBus w wersji 1.6 i 1.7 zostawia charakterystyczny wpis w rejestrze: *HKEY_CURRENT_USER/nazwa_serwera_w_wersji_1.6_lub_1.7*. Jeśli znamy tę nazwę, możemy usunąć konia trojańskiego kasując w kluczu: *HKEY_LOCAL_MACHINE/Software/Microsoft/Windows/CurrentVersion/Run* wpis o takiej samej nazwie jak nazwa serwera (czyli np. jeśli nasz serwer nazywa się *serwer.exe*, to zostawia takie klucze w rejestrze jak: *HKEY_CURRENT_USER/SERWER*.

A w *KEY_LOCAL_MACHINE/Software/Microsoft/Windows/CurrentVersion/Run* wpis: nazwa „SERWER" — dane „*ścieżka_dostępu\serwer.exe*". Wystarczy usunąć te dwa wpisy, zresetować komputer i usunąć serwer z dysku, aby pozbyć się ostatecznie NetBusa.

PROSIAK 0.47, 1.2

Program o swojsko brzmiącej nazwie — Prosiak jest ewenementem, jeśli chodzi o twórczość polskich programistów. Jego autorem jest student ukrywający się pod adresem *kwikwi@kki.net.pl*. Trojan składa się z dwóch części: serwera *prosiak.exe* (238 592 b w wersji 0.47, 237 056 b w wersji 1.2) oraz klienta *pro_cli.exe* (211 456 b w wersji 0.47, 258 048 b w wersji 1.2). Serwer instaluje się na porcie 33333 (w wersji 0.47) lub 44444 (w wersji 1.2). Działa w systemach Windows 95 i 98.

Usunąć można go tylko „ręcznie”. W przeciwieństwie do wcześniejszych koni trojańskich, które powielały pomysły, Prosiak ma kilka innowacji.

Dostępne w wersji 0.47 funkcje to:

- Zamknięcie, odinstalowanie, zmiana nazwy serwera;
- Zmiana nazwy sieciowej komputera;
- Zmiana nazwy, chowanie, pokazywanie, minimalizowanie, maksymalizowanie okien oraz „okien — dzieci” (czyli np. menu aplikacji);
- Efekty wizualne: skurczenie, wstrząsanie, migotanie, zamiana kolorów na negatyw, dziurkowanie okien;
- Podstawowe operacje na plikach (kopiowanie, usuwanie, uruchamianie, tworzenie katalogów, ściąganie, przesyłanie na serwer);
- Podstawowe informacje o serwerze (nazwa domeny, IP, ścieżki systemowe);
- Czytanie, usuwanie, przesyłanie tekstu do schowka;
- Uruchamianie na serwerze strony internetowej;
- Uruchamianie na serwerze domyślnego programu pocztowego z zadanym adresem e-mailowym i tematem listu;
- Uruchamianie komend DOS-a;
- Włączenie wygaszacza ekranu, trybu oszczędzania energii, zmiana kolorów w Windows na negatyw (również czasowa);
- Ukrycie lub pokazanie przycisku *START*, paska zadań (*TASKBAR*);
- Zamiana klawiszy myszki;
- Wyświetlenie okienka dialogowego lub wodzenie za kursorem komunikatu;

- Wylogowanie, zresetowanie, zamknięcie systemu;
- Pokazanie na ekranie serwera obrazka;
- Odtworzenie na serwerze pliku muzycznego;
- Zrzut ekranu z serwera;
- Efekty wizualne na ekranie: „skaczące pixelki", „inwazja mrówek", „rozmycie", „znikające kolory"

W wersji 1.2 dodano:

- Dokładniejsze informacje o systemie (czas pracy, rozdzielczość, pamięć fizyczna, długość pinga;
- Skaner Sieci (wykrywanie Prosiaka na innych komputerach podłączonych do Sieci);
- Opcję zawieszenia komputera;
- Możliwość uruchamiania i edycji skryptów;
- Zmiana hasła (domyślnie: prosiak);
- Wystartowanie serwera proxy (przekierunkowanie aplikacji znane z BO czy NetBusa);
- Wystartowanie serwera *httpd;*
- Konsola wykonywanych przez serwer poleceń.

Sposób usunięcia z systemu:

Prosiak nie jest wykrywany przez programy antywirusowe. Mimo to jego wykrycie jest łatwiejsze niż NetBusa, gdyż nie zmienia on nazwy wpisu w rejestrze (*Microsoft DLL Loader*), a pozostawia w kluczu *HKEY_LOCAL_MACHINE/ Software/ Microsoft/Windows/CurrentVersion/RunServices*. Domyślnie wpis ma wartość: *windll32.exe* (w wersji 0.47) lub *vbrun60.exe* (w wersji 1.2). Ponadto w wersji 1.2 Prosiak tworzy klucz: *HKEY_LOCAL_MACHINE/Software/Microsoft/Windows/ CurrentVersion/Rconfig*. Usuwając wpis, resetując komputer i kasując serwer znajdujący się w katalogu *C:/WINDOWS/SYSTEM*, pozbędziemy się go na dobre.

SOCKETS DE TROIE

Jest to drugi (po Prosiaku) program stworzony w języku innym niż angielski, a mianowicie francuskim. Powstał w październiku 1998 roku. Napisany jest w języku Delphi 3, ma rozbudowany (około 443 kB) rdzeń.

Ciekawostką jest to, iż dystrybucja tego konia trojańskiego obejmuje: aplikację klient-serwer, dokumentację oraz kod źródłowy (w przeciwieństwie do innych, „komercyjnych" aplikacji). Istnieją dwa rodzaje instalacji serwera:

Uruchomiony serwer podaje komunikat o brakującej bibliotece (*setup32.dll*) instalując się w katalogu systemowym Windows (jako plik *mschv32.exe*) i modyfikując zarazem *Rejestr Systemowy*, aby rozpocząć działanie wraz z każdą sesją systemu (pierwszy klucz: *HKEY_CURRENT_USER/Software/Microsoft/Windows/CurrentVersion/Run Load* oraz wpis: „MSchv32 Drv = *C:\WINDOWS\SYSTEM\ MSchv32.exe*", drugi klucz: *HKEY_CLASSES_ROOT/DirectSockets* oraz wpis: „DirectSocketsCtrl =$A4D5 #FFF").

Uruchomiony serwer podaje komunikat o brakującej bibliotece (*isapi32.dll*) instalując się trzykrotnie: raz w katalogu Windows (*c:/windows/rsrcload.exe*), dwa razy w katalogu systemowym (*c:/windows/system/mgadeskdll.exe, c:/windows/system/ csmctrl32.exe*) i modyfikując zarazem *Rejestr Systemowy* (pierwszy klucz: *HKEY_ CURRENT_USER/Software/Microsoft/Windows/CurrentVersion/RunLoad* oraz wpis: „Mgadeskdll = *C:\WINDOWS\SYSTEM\Mgadeskdll.exe";*

drugi klucz:
HKEY_LOCAL_MACHINE/Software/Microsoft/Windows/CurrentVersion/RunLoad oraz wpis: „Rsrcload = *C:\WINDOWS\Rsrcload.exe";*

trzeci klucz:
HKEY_LOCAL_MACHINE/Software/Microsoft/Windows/CurrentVersion/RunServi cesLoad oraz wpis: „Csmctrl32 = *C:\WINDOWS\SYSTEM\Csmctrl32.exe").*

Sposób usunięcia z systemu:

Sockets de Troie nie jest wykrywany przez programy antywirusowe. Usuwa go Anti-Sockets de Troie.

Można to również zrobić „ręcznie”. W tym celu trzeba skasować podane wyżej klucze w *Rejestrze Systemowym*. Wcześniej należy zapamiętać ścieżki i nazwy plików, które po ponownym uruchomieniu Windows należy usunąć z systemu. Od tej chwili system jest bezpieczny.

WinCrash 1.03

Kolejny program z dziedziny aplikacji klient-serwer. Stworzony został przez dwóch programistów: M@niac_Teen & Terminal Crasher. Konfiguracja serwera [domyślnie: *Server.exe* (296 448 b), charakterystyczna ikonka Windows — falujące czterokolorowe okienko] na komputerze ofiary odbywa się automatycznie, a sam program nie jest pojawia na pasku zadań czy też liście aktywnych procesów (uruchamianej kombinacją klawiszy: *Ctrl+Alt+Del*). Włamywacz może również dowolnie zmieniać nazwę pliku serwera. Dostępne funkcje programu:

- Otwieranie, zamykanie CD;ROM-u;
- Zapalanie, wygaszanie diod na klawiaturze (Caps Lock i Scroll Lock);
- Zablokowanie, odblokowanie, zdalne sterowanie kursorem;
- Wyłączenie, włączenie monitora;
- „Zapchanie” drukarki sieciowej;
- Zablokowanie klawiszy systemowych (Caps Lock i Scroll Lock);
- Wyłączenie schowka;
- Włączanie, wyłączanie wygaszacza ekranu;
- Ukrycie lub wyłącznie: paska zadań, przycisku *Start;*
- Usunięcie, zmiana tapety;
- Zmiana czasu i daty systemowej;

- Zamknięcie, odinstalowanie serwera;
- Zamknięcie uruchomionych programów;
- Zamknięcie, zawieszenie, zresetowanie Windows;
- Wyświetlenie okienka dialogowego (CHAT) lub tekstu;
- Pobranie informacji o systemie;
- Zdobycie haseł systemowych;
- Wyświetlenie listy aktywnych procesów;
- Uruchomienie dostępu do dysku twardego ofiary poprzez FTP;
- Odtworzenie pliku dźwiękowego (format *wav*);
- Wykonywanie podstawowych operacji dyskowych na komputerze ofiary;
- Modyfikacja pliku *autoexec.bat;*
- Uruchamianie aplikacji na serwerze.

Sposób usunięcia z systemu:

WinCrash jest wykrywany przez markowe programy antywirusowe. Można go również usunąć „ręcznie", gdyż WinCrash instaluje się w katalogu systemowym (może ukrywać się pod różnymi nazwami) i zostawia w kluczu: *HKEY_LOCAL_MACHINE/Software/Microsoft/Windows/CurrentVersion/Run* wpis: „MsManager" = „nazwa pliku serwera". Wystarczy więc usunięcie tego wpisu przez zresetowanie komputera i skasowanie znanego pliku.

Web EX 1.2

Aplikacja składa się z następujących plików: klienta *Web Ex.exe* (96 768 b) i serwera *Task_bar.exe* (115 200 b). Ponadto do uruchomienia potrzebne są następujące pliki:

- *MSVBVM50.dll*;
- *MSWINSCK.ocx*;
- *MSINET.ocx*.

Nie są one domyślnymi plikami systemowymi. Włamywacz musi się więc zatroszczyć o to, aby wraz z serwerem umieścić je na komputerze ofiary. Ponadto do programu dołączany jest komponent o nazwie *Antidote.exe*, który służy do trwałego usunięcia serwera z systemu. Web EX nie jest więc programem przeznaczonym dla „profesjonalnych włamywaczy", ale raczej eksperymentalnym projektem jego twórcy. GUI programu jest łudząco podobne do wcześniejszych wersji NetBusa. Sam program oferuje też niewiele funkcji (głównie mających za zadanie zwrócenie uwagi użytkownika na to, że coś jest nie w porządku z jego systemem). Najciekawszym pomysłem jest zintegrowanie trojana ze stroną internetową jego twórcy (oferuje ona stały, serwis podając listę dostępnych w Sieci zarażonych komputerów). Dostępne funkcje to:

- Wyświetlenie okna dialogowego z komunikatem na serwerze;
- Uruchamianie strony internetowej na serwerze;
- Uruchamianie dowolnej aplikacji;
- Otwieranie, zamykanie CD-ROM-u;
- Wyświetlenie listy aktywnych aplikacji;
- Zapełnienie ekranu ofiary tekstem;
- Rysowanie okręgów wokół kursora;
- Zresetowanie komputera ofiary;
- Zamiana przycisków myszy;
- Wyświetlenie informacji o systemie ofiary;
- Powiadamianie wszystkich chętnych na stronie internetowej autora (*http://www.cates.mcmail.com/webex*) o obecności w Internecie każdego użytkownika z zainstalowanym koniem trojańskim (sic!);
- Powiadamianie włamywacza poprzez e-mail o obecności w Internecie ofiary;
- „Podsłuchiwanie" ofiary — przesyłanie ciągu wystukiwanych na serwerze znaków;
- Wyświetlenie listy adresów IP zarażonych komputerów tworzonej na stronie internetowej autora konia trojańskiego.

Sposób usunięcia z systemu:

Web EX nie jest wykrywany przez programy antywirusowe. Można usunąć go „ręcznie", gdyż WE pozostawia po sobie wpis „RunDl32" = „*C:\windows\system\task_bar*" (serwer przyjmuje stałą nazwę pliku) w *Rejestrze Systemowym* w kluczu: *HKEY_LOCAL_MACHINE/Software/Microsoft/Windows/CurrentVersion/Run*.
Standardowa procedura to usunięcie wpisu, zresetowanie komputera i skasowanie pliku: *C:/WINDOWS/SYSTEM/TASK_BAR.EXE*.

EXECUTER 1

Executer to prosta aplikacja klient-serwer.

Składa się z dwóch części: serwera [domyślnie: *Exec.exe* (249 334 b)] oraz wyglądającego nietypowo (podobnie jak BO) klienta [domyślnie: *Controller.exe* (340 992 b)]. Dużo trudności użytkownikowi sprawić może wykrycie serwera, który przydziela sobie wolne porty, zmieniając ich wartość po każdym połączeniu. W równie niekonwencjonalny sposób odbywa się sterowanie aplikacją — opcje wybiera się przemieszczając je z okienka komend (gdzie wyszczególniono wszystkie) do okienka komend przeznaczonych do uruchomienia (uruchomić można jedną lub kilka komend na raz ustalając odstęp czasu, możliwe jest również „zapętlenie" wykonywanych komend). Na szczęście trojan ma rzucającą się w oczy ikonę: żółto-czerwony napis: „SeEK". Dysponuje on wieloma destrukcyjnymi z założenia funkcjami:

- `//DestroyDblClick` — wyłączenie dwukrotnego kliknięcia;
- `//DestroyDesktopColors` — zmiana kolorów systemowych na żółty;
- `//DestroyDesktopColors2` — zmiana kolorów systemowych na czarny;
- `//DestroyDesktopColors3` — zmiana kolorów systemowych na niebieski;
- `//DestroyDesktopColors4` — zmiana kolorów systemowych na czerwony;

- `//Disconnect` — wyłączenie aplikacji serwera;
- `//DestroyCtrlAltDel` — wyłączenie kombinacji klawiszy: *Ctrl+Alt+Del*;
- `//DestroyCursorPos` — ustawienie kursora w pozycji 0.0;
- `//DestroyTrayWnd` — ukrycie paska zadań;
- `//DestroyWindows` — zresetowanie komputera ofiary;
- `//RestoreDblClick` — włączenie dwukrotnego kliknięcia;
- `//RestoreCtrlAltDel` — włączenie kombinacji klawiszy: *Ctrl+Alt+Del*;
- `//RestoreTrayWnd` — przywrócenie paska zadań;
- `//CopyProgramToWindowsDir` — skopiowanie serwera do katalogu *C:/Windows/*;
- `//AddProgramToStartup` — dodanie serwera do *Autostartu*;
- `//DeleteLogo.Sys` — skasowanie *C:\Logo.sys*;
- `//DeleteWin.Com` — skasowanie *C:\Windows\Win.com*;
- `//DeleteIo.Sys` — skasowanie *C:\IO.sys*;
- `//DeleteSystem.Ini` — skasowanie *C:\Windows\System.ini*;
- `//DeleteWin.Ini` — skasowanie *C:\Windows\Win.ini*;
- `//DeleteConfig.Sys` — skasowanie *C:\Config.sys*;
- `//DeleteAutoexec.Bat` — skasowanie *C:\Autoexec.bat*;
- `//DeleteCommand.Com` — skasowanie *C:\Command.com*;
- `//DeleteRegedit.Exe` — skasowanie *Regedit.exe*;
- `//DeleteTaskman.Exe` — skasowanie *Taskman.exe*;
- `//EnableScreenPaint` — włączenie wyświetlania na ekranie ciągu: DIE!!! DIE!!! DIE!!!;
- `//DisableScreenPaint` — wyłączenie wyświetlania na ekranie ciągu: DIE!!! DIE!!! DIE!!!;
- `//EnableBeeping` — włączenie generowania dźwięków na PC Speakerze;
- `//DisableBeeping` — wyłączenie generowania dźwięków na PC Speakerze.

W rzeczywistości jest to program bardzo powolny i nieudolny. Nie został wyposażony w opcję samodzielnej instalacji na komputerze ofiary. Włamywacz musi dokonać tego „ręcznie”. Musi w tym celu skopiować serwer na komputer ofiary i dodać go do *Autostartu* (ułatwieniem dla niego jest obecność takich funkcji w trojanie) po uruchomieniu na komputerze ofiary serwera.

Sposób usunięcia z systemu:

Executer nie jest wykrywany przez programy antywirusowe. Można go usunąć „ręcznie", ponieważ koń trojański instaluje się w katalogu Windows jako *Sexec.exe* i zostawia w kluczu *HKEY_LOCAL_MACHINE/Software/Microsoft/Windows/ Current Version/Run* wpis: „<<SeEK>> EXECUTOR 1" = „*C:\Windows\ SExec.exe*". Usuwając ten wpis, resetując komputer i kasując znany plik, pozbywamy się go z systemu.

GirlFriend 1.3

Stworzony przez General Failure koń trojański składa się z dwóch nieodłącznych składników: serwera [nazwanego przez twórców GirlFriend domyślnie: *Windll.exe* (331 264 b)] oraz klienta [BoyFriend: *gf.exe* (425 984 b)]. Jego funkcje nie są rozbudowane i służy on głównie do wykradania haseł systemowych i wyświetlania komunikatów. Oprócz zdobywania hasła może je również wykasować (pod tym względem jest niebezpieczny, zwłaszcza jeśli ofiara ma hasła dostępu do Internetu inne niż „ ppp" lub nie pamięta haseł pocztowych w MS OUTLOOK). Ciekawostką jest również kopiowanie odkrytych w systemie haseł do *Rejestru Systemowego* do klucza *HKEY_LOCAL_MACHINE/Software/Microsoft/General*. Program oznacza zdobyte hasła lub pola tekstowe we wpisach kolejnymi liczbami, np.: „1"= „Połączenie Dial-up___ppp". Dostępne opcje to:

- *Show Passes* — wyświetlenie listy haseł dostępnych na komputerze ofiary (np. hasła dostępu do Internetu) oraz wszelkich aktywnych pól tekstowych (w tym również zakodowanych ciągiem gwiazdek: *******);
- *Send Message* — wyświetlenie na ekranie ofiary okienka dialogowego; możliwe jest wybranie jednego spośród pięciu rodzajów komunikatów: ostrzeżenia, informacji, błędu, zapytania, zwykłego oraz przetestowanie komunikatu na komputerze włamywacza;
- *Reset Password List* — kasowanie wszystkich haseł systemowych na serwerze;

- *Custom* — wysłanie jednej z komend do serwera:
  - `TEST?` — wysyła do serwera pytanie: „Are you alive?”; jeśli serwer działa, odpowie: „Server is alive!”;
  - `ver` — wyświetla wersję serwera;
  - `KillHER` — „zabija” serwer (usuwa serwer z rejestru, ale nie kasuje pliku *windll.exe*);
  - `{U}<URL>` — uruchamia na serwerze zadaną stronę internetową (adres zaczyna się od *http://*);
  - `{S}<plik>` — odgrywa plik dźwiękowy (format *wav*);
  - `{P}<plik>` — wyświetla plik graficzny (format *bmp*);
  - `DOWN` — wyłącza szukanie haseł na serwerze;
  - `UP` — włącza szukanie haseł na serwerze;
  - `setport<port>` — ustawia nowy port.

Sposób usunięcia z systemu:

GirlFriend jest wykrywany przez markowe programy antywirusowe. Można go także usunąć „ręcznie”, gdyż instaluje się w Windows jako *windll.exe* i zostawia w kluczu *HKEY_LOCAL_MACHINE/Software/Microsoft/Windows/CurrentVersion/ Run* wpis: „windll.exe” = „*C:\Windows\windll.exe*”. Usuwając ten wpis, resetując komputer i kasując znany plik, usuwamy konia trojańskiego z systemu.

MILLENIUM 1.0

Millenium to program, który składa się z dwóch części: niezwykle małego serwera [o nazwie SPY: domyślnie plik nazywa się *server.exe* (48 128 b)] oraz klienta [*client.exe* (164 352 b)]. Cechą charakterystyczną serwera jest nietypowa ikona (szara dyskietka z czarno-zieloną etykietą). Dostępne funkcje to:

- Zresetowanie, wylogowanie, zamknięcie, uruchomienie w trybie MS-DOS, odłączenie od Sieci;
- Zamknięcie, uruchomienie, usunięcie serwera;
- Otwarcie, zamknięcie CD-ROM-u;
- Włączenie, wyłączenie kombinacji: *Ctrl+Alt+Del*, *Caps Lock*, *Number Lock;*
- Przejęcie kontroli nad myszką i kursorem ofiary;
- Podstawowe operacje dyskowe;
- Przekierunkowanie danych

Sposób usunięcia z systemu:

Millenium nie jest wykrywany przez markowe programy antywirusowe, lecz przez program Millenium Remove

Można go usunąć „ręcznie", gdyż instaluje się w katalogu systemowym Windows jako *reg66.exe* i zostawia w kluczu *HKEY_LOCAL_MACHINE/Software/Microsoft/ Windows/CurrentVersion/Run* wpis: „Millenium" = „*C:\windows\system\reg66. exe*". Jest również jedynym koniem trojańskim, który pozostawia wpis w pliku *C:/WINDOWS/ win.ini* w sekcji [windows]: „run=*C:\windows\system\reg66.exe*". Usuwając te dwa wpisy, resetując komputer i kasując plik usuwamy go z systemu.

SK Silencer 1.01

Silencer to najnowszy produkt The SmithKlan. Jest jednym z najmniejszych koni trojańskich mających własnego klienta. Nazwą domyślną serwera jest *server.exe* (34 304 b), którą można dowolnie zmieniać. Ma on charakterystyczną ikonę — czerwony trójkąt równoboczny z białym wykrzyknikiem wewnątrz. Klient jest dwa razy większy (78 336 b) i ma „radioaktywną" ikonę. Program nie jest zbyt rozbu-

dowany. Jest to również jedyny backdoor ze standardowym GUI, wyglądającym jak większość aplikacji Windows. Współpracuje z Windows 95 i 98. Dysponuje jedynie kilkoma standardowymi opcjami:

- *Chat* — uruchomienie CHATA między serwerem a komputerem włamywacza;
- *Send KeyStrokes* — wysłanie kombinacji klawiszy;
- *ICQPassJack* — zdobycie hasła ICQ;
- *Run Application* — uruchomienie aplikacji na serwerze;
- *Send Msg* — wyświetlenie na serwerze okna dialogowego z dowolną informacją;
- *Hide Taskbar* — ukrycie paska zadań;
- *Disable Ctrl-Alt-Del* — wyłączenie kombinacji *Ctrl+Alt+Del*;
- *Ping Pong Virus* — wyświetlenie na serwerze piłeczki pingpongowej odbijającej się od krawędzi ekranu;
- *Reboot* — resetowanie komputera ofiary;
- *Run Screensaver* — włączenie wygaszacza ekranu;
- *Show Shutdown Menu* — uruchomienie procedury zamknięcia systemu.

Sposób usunięcia z systemu:

SK Silencer jest wykrywany przez markowe programy antywirusowe. Można usunąć go ręcznie, gdyż SK Silencer nie ma opcji pozwalającej na zainstalowanie się w *Rejestrze Systemowym*. Włamywacz musi więc dokonać tego ręcznie (nie istnieje wtedy standardowa procedura i wszystko zależy od jego inwencji). Należy się wystrzegać plików z ikoną i rozmiarem, jaki miały te przedstawione wyżej. Po odkryciu na swoim dysku opisanego serwera należy uruchomić program *regedit.exe* i znaleźć wpis będący ścieżką dostępu do serwera, a następnie usunąć go, zresetować komputer i wykasować z dysku konia trojańskiego.

StealthSpy

W przeciwieństwie do większości koni trojańskich StealthSpy nie jest anonimowy. Jego twórcą jest człowiek nazwisku — Andrei Birjukov. I chociaż programy rosyjskich twórców należą do czołówki najlepszych, to jednak ten pozostawia wiele do życzenia (chociaż sam autor zastrzega, że jest to dopiero wersja BETA 3). Tak się złożyło, że zdobyłem wersję roboczą, w której istnieje wiele „białych plam", a użycie niektórych opcji kończy wykonywanie programu poprzez jego wyłączenie. Nieobce są również komentarze odautorskie pokazywane przez aplikację zamiast oczekiwanych funkcji. Mimo tych niedociągnięć należy spodziewać się kolejnego, ale — na szczęście niezbyt groźnego — konia trojańskiego. W wersji BETA 3 składa się on z następujących plików: serwera o nazwie *telserv.exe* (235 520 b), biblioteki *tserv.dll*, pliku wsadowego *doscmd.bat* odpowiedzialnego za wykonywanie komend dosowych, *klienta telman.exe* (137 216 b), który wymaga biblioteki *MSVBVM50.DLL* oraz pliku *MSWINSCK.OCX*. Koń trojański ma następujące (ubogie) funkcje:

- Screenshot (zrzut ekranu);
- Menedżer plików (kopiowanie plików na i z serwera);
- Uruchamianie komend dosowych;
- Zamykanie aplikacji;
- Wyświetlanie na serwerze okienka dialogowego;
- Zresetowanie komputera ofiary.

Sposób usunięcia z systemu:

StealthSpy nie jest wykrywany przez programy antywirusowe. Usunięcie „ręczne" jest możliwe, ponieważ StealthSpy nie ma opcji pozwalającej na zainstalowanie się do *Rejestru Systemowego*. Włamywacz musi więc dokonać tego ręcznie (nie istnieje wtedy standardowa procedura, wszystko zależy od jego inwencji). Jest to jedyny koń trojański, którego serwer jest widoczny po wciśnięciu kombinacji klawiszy *Ctrl+Alt+Del*. Po odkryciu na swoim dysku opisanego serwera należy uruchomić *regedit.exe* i znaleźć wpis (jeśli takowy istnieje) będący ścieżką do serwera, a następnie usunąć go, zresetować komputer i wykasować z dysku konia trojańskiego.

GateCrasher 1.1

GC jest narzędziem napisanym w całości w języku Visual Basic. Znani są dwaj jego twórcy, którzy ukrywają się pod pseudonimami: KillBoy i ExCon. Program ten jest jedynym koniem trojańskim, który może infekować komputer ofiary na dwa sposoby: klasycznie jako aplikacja lub w sposób bardziej wyrafinowany, gdy dostarczany jest jako dokument MS Word (w wersji 97) z makrem. Będąc podłączonym do Internetu lub pracując w sieci lokalnej użytkownik jest narażony na kontakt z aplikacją, która przejmuje kontrolę nad takimi platformami, jak: Windows 95, 98 i NT. Zarażony dokument można więc otrzymać na wiele sposobów — może on być dołączony do e-maila, może być powszechny na IRC i w CHAT ROOMach, a także zdarza mu się wykorzystywać „dziury" w popularnych przeglądarkach internetowych. Domyślnie instaluje się na porcie 6969, ale może korzystać z każdego innego.

W skład programu wchodzą następujące pliki:

- *TCP.exe* — plik wspomagający TCP/IP;
- *Port.dat* — plik z danymi serwera, który może przybrać nazwę *Port.exe* lub *Port.doc* w zależności od sposobu instalacji na komputerze ofiary;
- *GC.exe* — klient;
- *Cleaner.exe* — program usuwający serwer z systemu;
- *MsWinsck.ocx* — kontrolka Winsock ActiveX używana do komunikacji przez protokół TCP/IP pomiędzy serwerem a klientem;
- *MSVBVM60.DLL* — biblioteka Visual Basic 6.0 Enterprise;
- *Inet.drv* — agent wykrywający połączenie, który „otwiera" serwer.

Dostępne opcje to:

- *Clear Recent Folder* — kasowanie foldera *RECENT* (z ostatnio uruchomionymi dokumentami);
- *Close CD* — zamykanie CD-ROM-u;
- *Close The Server* — zamykanie serwera;
- *Close Windows* — zamykanie sesji Windows;
- *Crazy Mouse Start* — przejęcie kontroli nad myszką użytkownika;
- *Crazy Mouse Stop* — przywrócenie kontroli nad myszką użytkownika;
- *Delete Directory* — kasowanie katalogu;
- *Delete File* — kasowanie pliku;
- *Fill Drive* — zapełnianie dysku (tworzy na nim pliki);
- *Format Drive* — formatowanie dysku;

- *Get Active Windows* — wyświetlanie listy aktywnych aplikacji;
- *Get Computer Name* — wyświetlanie nazwy komputera ofiary;
- *Get Disk Serial #* — wyświetlanie informacji o numerze seryjnym dysku twardego ofiary;
- *Get Free Space* — wyświetlanie informacji o ilości wolnego miejsca na dysku;
- *Get HD Letter* — wyświetlanie litery dysku lokalnego;
- *Get ICQ UIN* — wyświetlanie numeru ICQ;
- *Get Local Time* — wyświetlanie obecnego czasu na serwerze;
- *Get Organization* — wyświetlanie informacji o organizacji właściciela Windows;
- *Get OS* — wyświetlanie informacji o wersji Windows;
- *Get Owner* — wyświetlanie informacji o właścicielu Windows;
- *Get Server Path* — wyświetlanie ścieżki, na której znajduje się serwer;
- *Get System Directory* — wyświetlanie nazwy katalogu systemowego;
- *Get Temp Directory* — wyświetlanie nazwy katalogu tymczasowego;
- *Get User* — wyświetlanie nazwy aktualnego użytkownika;
- *Get Windows Directory* — wyświetlanie nazwy katalogu Windows;
- *Hide Mouse* — ukrywanie kursora;
- *Hide Task Bar* — ukrywanie paska zadań;
- *Kill Window* — zamykanie aplikacji;
- *List File in Directory* — wyświetlanie listy plików w katalogu;
- *Log Off* — wylogowanie ofiary;
- *Make Directory* — tworzenie katalogu na serwerze;
- *Open CD* — otwieranie CD-ROM-u;
- *Open Control Panel* — otwieranie *Panelu Sterowania*;
- *Open Date/Time* — otwieranie *Właściwości Daty/Godziny;*
- *Open FTP Server* — otwieranie na porcie 6970 serwera FTP, co daje włamywaczowi możliwość wyświetlania zawartości katalogu, odczytywania, zapisywania, kasowania plików, tworzenia, kasowania katalogów;
- *Open Webbrowser* — uruchamianie strony internetowej w domyślnej przeglądarce;
- *PING!* — wysłanie pakietu danych na serwer;

- *Read from Drive A*: — odczytanie stacji dysków na serwerze;
- *Reboot Computer* — resetowanie komputera;
- *Search For File* — szukanie pliku na komputerze ofiary;
- *Send Message* — wysłanie komunikatu;
- *Send Text* — wysłanie tekstu do aktywnego na serwerze okienka tekstowego;
- *Set Computer Name* — zmiana nazwy komputera użytkownika;
- *Set VolumeLabel For C* — ustawianie etykiety dysku C;
- *Show Mouse* — pokazanie kursora;
- *Show Task Bar* — pokazanie paska zadań;
- *ShutDown* — resetowanie komputera;
- *Start Program* — uruchomienie programu na komputerze ofiary;
- *Start Screen Saver* — uruchomienie wygaszacza ekranu;
- *Switch Window* — zmiana danych okna na aktywne.

Sposób usunięcia z systemu:

GateCrasher nie jest wykrywany przez programy antywirusowe. Aplikacją wykrywającą jego działanie jest BOClean 2.01 oraz GateCleaner.

Usunięcie „ręczne" też jest możliwoe, gdyż GateCrasher instaluje się jako *C:/ WINDOWS/EXPLORE.EXE*. Pozostawia też po sobie wpis „Explore"=„ *EXPLORE. EXE*" w kluczu: *HKEY_LOCAL_MACHINE/Software/Microsoft/Windows/Current Version Run*. Usuwając wpis, resetując komputer i kasując plik, usuwamy go na trwałe z systemu.