Dodatek nr 3

Ten tekst jest podzielony na dwie części. W pierwszej zawartych jest piętnaście podstawowych kroków, które należy wykonać, aby stać się uebercrackerem, ale z drugiej można się już dowiedzieć, co należy zrobić, by zostać ueberadminem i powstrzymać uebercrackerów.

Dla uzupełnienia warto dodać, że „uebercracker" to termin stworzony przez Dana Farmera. Nawiązuje on do dokonań niektórych legendarnych już hakerów, którzy nie są w stanie trzymać się z daleka od Sieci.

A oto kilka wskazówek, które mogą pomóc w staniu się uebercrackerem.

KROK 1: Odpręż się i zachowaj spokój. Pamiętaj, że chcesz być uebercrackerem.

KROK 2: Jeśli znasz „Małego Uniksa", masz przed sobą otwartą drogę i możesz pominąć 3 krok.

KROK 3: Powinieneś kupić podręcznik o Uniksie (lub sam program), aby dowiedzieć się, co znaczy: ls. cd. cad.

KROK 4: Śledź rozmowy w następujących grupach dyskusyjnych: *alt.irc*, *alt.security.unix*. Dopisz *Phrack@well.sf.ca.us*., aby otrzymać historię kultury uebercrackera.

KROK 5: Zapytaj w *alt.irc,* jak można otrzymać i skompletować późniejszego klienta IRC i połącz się z nim.

KROK 6: W przyszłości (na IRC) przyłącz się do hakerskiego kanału.

KROK 7: Korzystając z hakerskiego kanału wyślij wiadomość (np. „Hi whatsUp?"). Ale pamiętaj, że staniesz się lamerem, gdy włączysz się do hakerskiego kanału i zapytasz się: „dlaczego nie mogę przyłączyć się do kanału # WAREZ?".

KROK 8: Wyślij do kogokolwiek wiadomość z pytaniem o nowe „pluskwy" lub „dziury". Rozejrzyj się wokół swojego systemu za binarnym programem zainstalowanym w katalogu roota. Jeśli znajdziesz coś takiego (su, chfn, syslog), powiedz ludziom, że masz nową „pluskwę" w tym programie i że napiszesz do tego skrypt. Gdy zapytają, jak to działa, to znaczy (i możesz im to powiedzieć!), że są lamerami. Ale pamiętaj, że sam jesteś uuebercrackerem i swobodnie możesz postawić pytanie o to, czy chcieliby dostać albo przehandlować te skrypty.

KROK 9: Wyślij znajomym dowolne skrypty (albo trochę plików-śmieci) i powiedz, że są odkodowane, bo były „zaśmiecone" i trzeba załadować je jeszcze raz.

KROK 10: Spędź tydzień ściągając wszelkie skrypty, jakie tylko uda ci się znaleźć.

KROK 11: Gdy wykonasz prawidłowo powyższe czynności, będziesz miał skrypty, które pozwolą ci dostać się do roota większości Uniksów. Ograbiaj więc dyski lokalnych maszyn, czytaj pocztę twojego administratora, a nawet innych użytkowników. Nie zapomnij o plikach zapisujących czas i datę różnych działań w danym systemie.

KROK 12: Dobrym testem dla uebercrackerów jest zdolność fałszowania poczty. O to, jak można to zrobić, zapytaj innych uebercrackerów, którzy też przechodzili taki test. Potem wyślij e-maila do administratora. Możesz napisać, że został wykorzystany i wyjaśnić mu, w jaki sposób poznałeś zasoby jego dysku twardego i dlaczego na przykład skasowałeś jego pliki. powinno to ukazać się pod adresem *satan@evil.com.*

KROK 13: Po wykonaniu kolejnych zadań, możesz już myśleć o tym, by skontaktować się z elitą uebercrackerów. Pochwal się swoimi wyczynami na hakerskim kanale.

KROK 14: Powstrzymaj swą działalność, ale po kilku miesiącach zbierz wszystkie swoje notatki. Bądź przygotowany, że w każdej chwili może wkroczyć FBI, Tajny Urząd i inne agencje strzegące prawa, które skonfiskują ci sprzęt. Zadzwoń na EFF.Org., aby poskarżyć się.

KROK 15: Teraz dla końcowego efektu ponownie skontaktuj się z elitą, pochwal się na kanale hakerskim, że zostałeś zatrzymany. W końcu jesteś prawdziwym uebercrackerem!

Następna część tekstu jest wciąż tajna, więc przekazuj ją tylko zaufanym administratorom i przyjaciołom, a nawet niektórym grupom dyskusyjnym etc. Możesz mieć pewność, że nikt, kto nie jest wtajemniczony nie dostał jeszcze tej listy. Warto dodać, że opisuje ona podstawowe przedsięwzięcia, które należy podjąć, zostać ueberadminem i powstrzymać uebercrackerów.

KROK 1: Czytaj podręcznik Uniksa.

KROK 2: Bardzo ważne: chmod 700 rdist; *chmod 644/etc/utmp*. Zainstaluj sendmail 8.6.4, a tym sposobem prawdopodobnie powstrzymasz 60% uebercrackerów. Skrypt rdist należy do najczęściej stosowanych w celu „zdobycia" cudzego dysku, czyli uzyskania nielegalnego wglądu do jego danych.

KROK 3: Jeśli chcesz uaktualnić bezpieczeństwo swojego komputera poprzez elitarnych uebercrackerów, którzy potrafią włamać się w dowolne miejsce w Internecie, wykonaj koniecznie następny krok.

KROK 4: Zainstaluj swojego firewall w bloku *rpc/nfs/ ip-forwarding/src, a* powstrzyma to 90% wszystkich uebercrackerów przed próbą włamania się do twojego komputera.

KROK 5: Przestrzegaj wskazówek CERT i uaktualniaj swoje systemy (tak możesz unieszkodliwić dokładnie 95% uebercrackerów.

KROK 6: Uruchom dobry program do odgadywania haseł, aby znaleźć wszystkie otwarte konta i zamknąć je. Uruchom tripwire po sprawdzeniu, że binaria są nienaruszone. Uruchom tcp_wrapper, aby znalazł ślady uebercrackera, jeśli ten grzebał w twoim systemie.

KROK 7: Jeśli zrobiłeś wszystko, co należy, zatrzymasz 99% uebercrackerów.

K*ROK 8*: Teraz pozostał już tylko 1% hakerów, którzy zyskali wiedzę, dzięki czytaniu poczty ekspertów bezpieczeństwa (prawdopodobnie uzyskali dostęp do poczty via NFS).

KROK 9: Trudnym zadaniem jest próba przekonania ekspertów do spraw bezpieczeństwa, że nie lepsi niż reszta świata. Rozdawanie (wszystkim z wyjątkiem uebercrackerów!) nierozpoznanych przez nich „pluskiew" może więc być tylko przysługą dla użytkowników Internetu. Trzeba pamiętać o tym, że rozsyłanie tego typu wiadomości pomiędzy zaufanymi ludźmi umocni ich wiedzę.

KROK 10: Jeśli zyskałeś już zaufanie, powinieneś dowiedzieć się, jak należy traktować kogoś takiego jak administrator systemu, który jest zdolny powstrzymać najwięcej uebercrackerów. Prawdziwie ostatecznym testem, który pozwala zostać ueberadminem jest kompilowanie klienta IRC, a następnie wejście na kanał hakerski, spisanie wszystkich przechwalających się swoimi umiejętnościami oraz pomoc w złapaniu uebercrackerów. Jeśli uebercracker dostał się do twojego systemu i używał metod, których nie znałeś wcześniej, możesz powiedzieć o tym administratorowi (pewnie

otrzymasz połowiczną odpowiedź w stylu — „ta pluskwa była znana przez lata, nie ma dla niej żadnej właściwej odtrutki” lub „to jest bardzo imponujące, poznałeś wielką lukę w moim kole bezpieczeństwa”).