Lamer FAQ

Vložil/a cm3l1k1 [1], 10 Prosinec, 2004 - 19:21

- Free Mind [2]
- Fun [3]

Tento dokument byl vytvořen pro "začínající" rádoby hackery, kteří zaplavují fóra a IRC channely pořád stejnými naivními otázkami. Jsou v něm odpovědi na nejčastější otázky lamerů.

Naučíte mě hackovat ??

Lameři si to představují jak Hurvínek válku. Hacking není otázkou minut ale několika let. Čím starší člověk je, tím méně má volného času a určitě ho nevyužije tak, že by vás něco učil. Učte se sami. Čtěte co se dá - např. knihy o počítačových sítí, bezdrátových sítí, firewallech a proxy serverech, směrování, šifrování, metody útoků, databázích, GNU/Linuxu či *BSD systémech. Snažte se dopodrobna pochopit používanou terminologii, fungování operačních systémů, protokolů a vůbec není na škodu programování, bez kterého se nehnete. Hlavně si uvědomte význam slova hacker. To není člověk který shazuje servery, maže je, nebo bezdůvodně pozměňuje webové stránky. Pravý význam slova hacker naleznete v našem článku [4].

Jak mám začít s hackováním ??

Něco jsem popsal již výše. Čtěte vše co se vám dostane do ruky a hlavně si to vyzkoušejte. Nejlépe na svém systému. Snažte se pochopit jak věci fungují a ověřte si to v praxi. Čtěte články na serverech věnující se bezpečnosti, počítačovým sítím, GNU/Linuxu atd. Na IRC channely choďte jen s konkrétními dotazy nad kterými jste se opravdu předtím zamysleli. Pokud nemáte dostatečné znalosti tak se o žádný hack nepokoušejte! Nejdříve se učte - člověk který chce létat se taky musí nejdřív naučit chodit.

Poradíte mi jak hacknout email ??

S touto otázkou je bohužel nenávratně spojen název programu wwwhack. Na internetu se vyskytují i návody jak ho ovládat, což už je opravdu absurdní. Zkoušet se dostat do mailového účtu na serveru přes webové rozhraní nebo POP3 server pomocí slovníkového útoku je hloupost. Pokud totiž nejste skryti za proxy či SOCKS serverem, tak po sobě zanecháte tisíce stop (logů). V podstatě už samotná otázka je hloupost. Nehackuje se mailový účet, ale POP3 server kde jsou mailové účty vedeny a odkud se lze dostat ke zprávám. Pokud si někdo za heslo zvolí běžné slovo vyskytující se ve slovníku (Lucka, zlatíčko, sex, prosinec, KoRn, lampa...) tak lze heslo cracknout rychle a jednoduše, ale mě připadá užití podobných technik "neúčinné" a použil bych je až jako úplně poslední možnost. Metod jak se dostat k mailovým účtům je nespočet. Od webových útoků (sql, script, cookies injection) až po napadení jiných serverů v síti ISP za účelem další infiltrace do systému.

Jak zjistím svoji IP adresu ??

Svoji IP adresu zjistíte snadno. Nepředpokládám, že tuto otázku položí někdo kdo při bootování viděl na svém monitoru něco jiného než logo Windows. Takže ve windozích zjistíme IPnu takto: start -> spustit -> cmd -> ipconfig. Pokud jste připojený k lokalní síti a na internet přistupujete přes NAT nebo proxy, tak budete mít veřejnou IPnu proxy serveru. Tu zjistíte např. na testovacích stránkách anonymity proxyn http://anoncheck.security-portal.cz/ [5]

Jak zjistím IP adresu někoho jiného na Internetu ??

Je spousta možností, ale uvedu jen ty nejběžnější.
1) Podle hlavičky emailu - pokud vám dotyčný napsal email, tak se jeho IP adresu či adresu jeho proxy serveru můžete dočíst z hlavičky emailu. Postupu jak toho dosáhnout je na internetu spousta, tak nebuďte líní a naučte se používat google.
2) Z některých IM klinetů - např. pokud si nezakáže jednu z voleb v nastavení ICQ, tak se v jeho profilu zobrazí IP adresa.
3) Z webových stránek - pokud umíte základy psaní webových stránek, tak můžete vytvořit stránku s logováním IP adres a dotyčnému poslat odkaz ať se na to podívá. Při troše štěstí na to klikne.
+ i když zjistíte něčí IP adresu, tak není 100% dáno že ji bude mít pořád. Pokud se např. připojuje na internet přes modem, tak má pokaždé jinou - záleží na konkrétním připojení.

Jak mám hackovat pomocí telnetu ??

Tuhle otázku nechápu doteď. Kde někdo vzal představu, že se dá hackovat pomocí telnetu ?? Telnet je klient/protokol pro správu systému, který se v dnešní době vůbec nepoužívá, protože přenos dat není šifrovaný a hesla se přenášejí v otevřené podobě (text).[a hlavně to není stavový protokol (myšleno ve vztahu k sekvenčním číslům), takže je náchylný k útokům převzetí spojení]

K čemu je ping a traceroute ??

Ping: odesílá pakety na cílový počítač a ten mu na paket odpoví (pokud pakety neblokuje firewallem). Slouží jen k zjišťování aktivních počítačů.
Traceroute: Vypisuje přes které routery putují data odesílaná od vás k cílovému počítači.
-- tyto příkazy nemají s hackováním nic společného.

Jaký je rozdíl mezi virem a červem ??

Vir (virus): program, který se připojí k jinému programu nebo systémové oblasti a ty pozmění. Může se nekontrolovatelně rozšiřovat, nebo po svém spuštění vykonat destrukční proceduru.
Červ (worm): program, který vytváří své kopie do jiných počítačových systémů (sítí). Do systémů se většinou dostane pomocí využití některé z bezpečnostních chyb.

Co je to Exploit ??

Exploit je program (vetšinou napsaný v programovacím jazyce C nebo Perl), který využívá chybu v systému, siťové aplikaci, webových aplikacích atd. Důsledkem toho je, že se např. dostanete ke vzdalenému příkazovému řádku, shodíte aplikaci, spustíte vzdálený kód a nebo v případě lokálních útoků si také můžete navýšit práva.

Jak můžu sniffovat (odposlouchávat) data a hesla ??

Mno abych to zjednodušil... sniffování je věda. Hlavně tedy na přepínaných (switch) sítích. Funguje to vlastně tak že vy odposloucháváte data jiných uživatelů, která by se vám za normálních okolností neměla dostat do rukou, protože síťová karta je má zahodit pokud nejste označen jako příjemce (cílová IP). Na internetu je několik zajímavých prográmků, které ale pomocí určitých postupů mohou takto data získat a vy tím pádem sledovat komunikaci ostatních uživatelů (kteří jsou ve stejné podsítí jako vy!) a bez problémů odchytávat jejich hesla přes nešifrované protokoly (http, pop3, telnet...). Velice jednoduchým ale občas nefunkčním programem je Cain&Abel a velice profesionálním a konfigurovatelným je ettercap. Sniffování je na celý článek, proto se tomu zde nebudu dále věnovat.

Jak rozšifrovat heslo ??

Tak vaším hlavním cílem bude zjistit v čem je heslo šifrováno, nebo spíš v čem hashováno (což je

mnohem běžnější). Hashování je jednocestný proces, kdy je vytvořen "otisk" hesla a zpětně ho nelze dešifrovat, ale jen zkoušet všechny možné kombinace. Pokud zjistíte v čem je heslo hashováno musíte mimojiné sehnat program, který umí na tento hash bruteforce útok, wordlist atd. Ono občas je težké rozpoznat hash. Zaměřte se na zakladní rysy... kolik ma bitů, jaké jsou použité znaky, jestli se nekteré sekvence neopakuji atd. MD5 má např. 124 bitů, SHA1 160bitů, takže tam to lze rozpoznat dobře, ale takto to neplatí vždycky. Mezi nejznámější louskače hesel jednoznačně patří john the ripper a L0phtCrack (LC).

Jak zjistit heslo administrátora Windows ??

K tomuto tématu je na SP pěkný a jednoduchý článek Hesla ve Windows 2000/XP [6]

Závěr

Všichni lameři se ptají na naprosto primitivní věci, které lze najít během 5-ti sekund na googlu (http://www.google.com [7]). Raději se zeptají na 10-ti fórech, než aby si to našli sami. Přeci není tak težké, když hledám co je to keylogger, tak zadat vyhledávání v češtině a "keylogger je".
Pokud jsem některé z nejčastějších otázek neuvedl, tak mě na to upozorňete v komentáři a článek doplním.

URL článku: https://security-portal.cz/clanky/lamer-faq

Odkazy:
[1] https://security-portal.cz/users/cm3l1k1
[2] https://security-portal.cz/category/tagy/free-mind
[3] https://security-portal.cz/category/tagy/fun
[4] http://www.security-portal.cz/clanky/kdo-je-to-hacker
[5] http://anoncheck.security-portal.cz/
[6] http://www.security-portal.cz/clanky/hesla-ve-windows-2000xp
[7] http://www.google.com