

Hackování ženských

Vložil/a [cm3l1k1](#) [1], 21 Prosinec, 2004 - 19:37

- [Free Mind](#) [2]
- [Fun](#) [3]

velmi zajímavá a vtipná úvaha o biologickém hackování - převzata ze serveru hysteria.sk, zveřejněna v Prielomu 11
autori: puf a muf

ako preniknut do systemu zena... ...alebo zakladne informacie o biologickom hackovani

+ [0] +-----+ [UVOD] +-----

Tato príručka mladého zaletníka vzniká v pondelok niekedy doobeda den potom čo sa muf vrátil s hysteria session, kde tieto techniky konzultoval s naslovovzatými odborníkmi na vysokej komunikačnej úrovni a vo vysoko kultúrnom prostredí...

Autori neručia za prípadne morálne, fyzické, materiálne, psychicke, hardverové, softferové, genetické ani žiadne ine škody, negatívne, pozitívne, neutronové, kozmické, konfrontačné ani ine následky spôsobené nesprávnym použitím nižšie uvedených informácií...

+ [1] +-----+ [DISTRIBUCIE, JADRA] +-----

Medzi základne, verejnosti najznámejšie distribúcie, môžeme zaradiť nasledujúce:

Blondian - jadra triedy Public - nie príliš bezpečne a stabilne preto sú často preinštalovávajú, takže dlhodobšie využívanie systému neprichádza do úvahy

BrunetWare - jadra typu Romantic - stabilne a jedny z najbezpečnejších (ja osobne tiež fachcím na klony BrunetWaru a som veľmi spokojný, pozn. muf, puf prikyvkáva hlavou na znak súhlasu)

Red Head - jadra sadistic a príbuzné - táto distribúcia je veľmi variabilná a závisí od administrátora na ake použítie bude nakonfigurovaná, preto aj bezpečnosť je relatívna

FreeBLACK - jadra Free - slúžia predovšetkým ako školské alebo firemne servery, takže získať konto nie je problém

+ [2] +-----+ [ZISKAVANIE INFORMACII O SYSTEME] +-----

Pomocou programov typu womanMAP obeť dôkladne preskenujeme a snažíme sa zistiť distribúciu, triedu jadra (jadro nie je podmienené distribúciou pozn. muf), a následne aj porty na ktorých masína počuva. Dôkladnejšie by sme sa potom mali pozrieť na porty 22, 23, 69, 79, 99, 110. Avšak najdôležitejšie, čo nás zaujíma je, či už náhodou stroj nie je zdieľaný inými používateľmi!

Následovne sa snažíme o odchytenie hesiel užívateľov (sniff), získanie ich ID, real name, a práv pre danú masínu. Vhodné je tiež získať informácie o serveri od masín v tej istej sieti, prípadne od ostatných strojov v DOMene...

+ [3] +-----+ [UTOK] +-----

Ak uznáme že stroj je pre nás výhodný a vhodný pre útok, mali by sme prejsť k ofenzíve. Postup by mohol vyzeráť nasledovne:

- otestujeme vulnerability serveru na bežné exploity, napr. exploit triedy pozvanie.* (pozvanie.kino, pozvanie.prechádzka, pozvanie.bar) niekedy a len u niektorých jadier, je možné ochromiť bezpečnosť pomocou c2h5oh utility (snooping), ktorú môžeme zamaskovať v nejakom bežnom programe, napr. juice (tzv. trojan)

pozor! tieto techniky nie je možné používať ak je pripojený ROOT! S utilitou c2h5oh nie je vhodné si

zahravat ak sme neskuseny lameri, kedze moze lahko sposobit DoS nielen na cielovom stroji ale aj u nas

- snazime sa ziskat poziciu TRUSTED HOST, pripadne naburame iny system, o ktorom vieme, ze je v .rhosts, pripadne sa inymi technikami sami snazime dostat do .rhosts

- ako nasledujuci krok by malo nasledovat rusenie .rhostov, obmezovanie procesov, pamate a nastavenie quoty ostatnym uzivatelom, ako aj co najviac zaneprazdnit administratorov daneho stroja.

Na skodu nie je ani kontrolovanie posty a monitorovanie komunikacie a procesov...

- po ziskani accountu na danej masinke je vhodne pre ziskanie UID 0 pouzit multisystemovy a multipaltformovy exploit KWETY, ktory je uspesny v 90% (skoro ako ten exploit na SUNy v prielome #9 :), pozn. puf). Aj ked obrana proti tomuto zakernemu utoku je velmi tazka, odporuca muf pouzivat aspon verziu RUZE 3.0 a vyssie. V pripade neuspechu sa pokuste utok zopakovat...

- ak nedosiahneme superpouzivatelske prava, mozeme sa pokusit zautocit aj na sluzbu KISS, ktoru riadi USTAd, a to pomocou kombinacie standardne implementovanych klientov PERY a JAZYK. Musime vsak byt opatrní, pretoze v pripade neuspechu je velka pravdepodobnost ze nam bude vytvoreny nemily, avsak dufajme ze len docasny zaznam v subore /etc/host.deny, ale moze nastat aj situacia, ze budu pouzite aj prikazy ako delluser, ci rm -rf v kombinacii s vasim LOGINom, apod.

- niektore drsnejšie povahy preferuju utoky typu BRUTE FORCE, ktore su vhodne hlavne na jadra triedy sadistic a pribuzne. Cielom je ziskanie pristupu k sluzbam finger (port 79), suck (port 69) a fuck (port 99).

UPOZORNENIE: Na systemoch s jadrom romantic je tento druh utoku vyslovene nevhodny a mnohi zabudaju na to, ze ich cinnost sa loguje a hrozi nielen zmarenie utoku ale aj zamedzenie pristupu a dokonca priama fyzicka konfrontacia s adminmi, trusted hostami, ako aj s policiou a inymi organmi...

- na jadra typu romantic je preto najvhodnejšie vyuzit vyssie spomenute exploity (kino, prechadzka.*, kwety).

- na distribuciu Blondian zabera na 100% exploit na diery v sprave pameti, nazyvany medzi hackermi KARELAB/KALERAB. Tento je mozne "tlacit" cez lubovolny port. Pri tejto distribucii je defaultne povolene pouzivanie sluzieb FINGER a niekedy aj zmienenyh FUCK a SUCK.

+ [4] +-----+ [FIREWALLY] +-----

V minulosti boli na zamedzovanie sluzby FUCK pouzivane HW ochany, prvi predchodcovia firewallu, ktore az do zadania patricneho osobneho kluca blokovali port 99. Nazyvally sa PASCUDY, co je vlastne skratka zo slov PAS a CUDNOST. Dnes sa uz tieto primitivne nastroje nevyuzivaju a v pripade, ze sa najdu nejake podobne zabezpecenia, su tieto tunelovane a obchadzane prevazne portami 69, 79, pripadne redirektormi cez ine volne porty. Ich konfiguracia a spojzdnenie v distribucii BrunetWare je dost otiazne a vyzaduje vela casu a zrucnosti.

+ [5] +-----+ [ZABARIKADOVANIE] +-----

Po dosiahnutí ROOT LEVELU na cielovej masine dochadza casto (hlavne v distribuciach s jadrami romantic) k zavedeniu zdielania diskov a procesov a k zosuladeniu userlistov, trusted hostov a k blokacii vacsiny portov vonkajsiemu svetu. V jadrach romantic je tato podpora priamo zabudovana, avsak u jadier sadistic, free a public je nutne tuto podporu dokompilovat ako zvlastny modul. V distribucii Blondian je spojzdnenie, vyuzivanie a administracia tychto sluzieb priam nemozna. Ak sa to niekomu podarilo, pripadne ma s tymto problemom blizsie skusenosti, ozvite sa prosim na nasu znamu adresu: Slovenska Televizia, Mlynska Dolina, 845 45 Bratislava.

+ [6] +-----+ [LEGISLATIVA] +-----

UPOZORNENIE: Treba si davat pozor, pretoze zakon zakazuje vyuzivanie portov 69, 79 a hlavne 99 (sluzby suck, finger a hlavne fuck = sietovy kombinacno duplikacny protokol, skratka je z ludoveho narecia autora, ktory bol domorodcom z ostrova borneo, s mierne ugrofinskym prizvukom, pozn.

muf) na nestabilných strojoch, tj. strojoch ktorých UPTIME je mensi ako 15 rokov. Niektore stroje sa preto snazia oklamať potencialnych zaujemcov o vyuzitie tychto sluzieb pouzivaním PATCHnutého uptimu, modifikaciou systemoveho casu, prípadne vyuzivaju ine maskovacie techniky a lakaju tak userov/attackerov na vyuzivanie tychto sluzieb.

+ [7] +-----+ [BACKDOORY A NAVRATY SPAT] +-----

Vo vseobecnosti sa neodporuca skusat opakovane navraty pomocou zadnych dvierok, avsak tato moznost existuje. Najpouzivanejsim backdoorom je vytvorenie vlastneho administratorskeho konta a zmenenie rootovskeho hesla. System je potom na nas plne zavisly. Dalsimi, avsak menej vyuzivanimi zadnymi dvierkami je odchytenie a zalohovanie privatneho komunikacneho kluca. Zablockovanie pristupu po odhaleni, je vsak velmi jednoduche, staci tento kluc zamenit za iny a zostaneme navzdy vyvreti zo systemu.

+ [8] +-----+ [VSEOBECNE RADY] +-----

Ak sa rozhodnete system vyuzivat vo vacsej miere, je vhodne masinu raz za cas rebootovat. Poma ha to spravne nacistat vasu konfiguraciju. Niekedy vsak staci len prikaz kill -POHUBE 1. Tieto problemy s implementovaním správnej konfigurácie sa vyskytuju hlavne v distribuciach s jadrami sadistic a najma free a public.

Odporucane su aj upgrady systemu zaveditel'nymi modulmi jadra DETi, ci uz aplikaciou X-Lapec alebo daemonom IEVCAd. Vhodne je instalaciju konzultovat s povodnymi administratormi systemu.

+ [9] +-----+ [DOVERYHODNOST A BEZPECNOST] +-----

Tento navod berte s rezervou a hlavne pri sietovom styku pouzivajte ochranné prostriedky, ci uz HW povodu (tabletky, vyrobky z plastickych hmot, firmu DUREX odporucaju 8 z 10 zuba...gynekologov) alebo SW (wrappery, ...) Uvedene techniky nie je vhodné pouzivat na verejnych, nekryptovanych kanaloach, uliciach alebo inych miestach obvykleho vyskytu, ale doporučujeme vyuzivat kryptovanu komunikaciju na neverejnom okuhu, odpojenom od ostatnych sieti, prípadne pracovat priamo za systemovou konzolou...

puf a muf (pufamuf(at)hysteria.sk, after session, volna hodina & skolsky bufet)

URL článku: <https://security-portal.cz/clanky/hackov%C3%A1n%C3%AD-%C5%BEensk%C3%BDch>

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>