Hackování ženských

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

- Free Mind [2]
- Fun [3]

velmi zajimavá 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 prirucka mladeho zaletnika vznika v pondelok niekedy doobeda den potom co sa muf vratil s hysteria session, kde tieto techniky konzultoval s naslovovzatymi odbornikmi na vysokej komunikacnej urovni a vo vysoko kulturnom prostredi...
Autori nerucia za pripadne moralne, fyzicke, materialne, psychicke, hardverove, softferove, geneticke ani ziadne ine skody, negativne, pozitivne, neutronove, kozmicke, konfrontacne ani ine nasledky sposobene nespravnym pouzitim nizsie uvedenych informacii...

+[1]+----------+[DISTRIBUCIE, JADRA]+----------
Medzi zakladne, verejnosti najznamejsie distribucie, mozeme zaradit nasledujuce:
Blondian - jadra triedy Public - nie prilis bezpecne a stabilne preto su casto preinstalovavane, takze dlhodobejsie vyuzivanie systemu neprichadza do uvahy

BrunetWare - jadra typu Romantic - stabilne a jedny z najbezpecnejsich (ja osobne tiez fachcim na klone BrunetWaru a som velmi spokojny, pozn. muf, puf prikyvkava hlavou na znak suhlasu)

Red Head - jadra sadistic a pribuzne - tato distribucia je velmi variabilna a zavisi od administratora na ake pouzitie bude nakonfigurovana, preto aj bezpecnost je relativna

FreeBLACK - jadra Free - sluzia prevazne ako skolske alebo firemne srvery, takze ziskat konto nie je problem

+[2]+----------+[ZISKAVANIE INFORMACII O SYSTEME]+-----
Pomocou programov typu womaNMAP obet dokladne prescanujeme a snazime sa zistit distribuciu, triedu jadra (jadro nie je podmienene distribuciou pozn. muf), a nasledne aj porty na ktorych masina pocuva. Dokladnejsie by sme sa potom mali pozriet na porty 22, 23, 69, 79, 99, 110. Avsak najdolezitjesie, co nas zaujima je, ci uz nahodou stroj nie je zdielany inymi pouzivatelmi!
Nasledovne sa snazime o odchytenie hesiel uzivatelov (sniff), ziskanie ich ID, real name, a prav pre danu masinu. Vhodne je tiez ziskat informacie o serveri od masin v tej istej sieti, pripadne od ostatnych strojov v DOMEne...

+[3]+----------+[UTOK]+----------
Ak uzname ze stroj je pre nas vyhodny a vhodny pre utok, mali by sme prejst k ofenzive. Postup by mohol vyzerat nasledovne:
- otestujeme vulnerability serveru na bezne exploity, napr. exploity triedy pozvanie.* (pozvanie.kino, pozvanie.prechadzka, pozvanie.bar) niekedy a len u niektorych jadier, je mozne ochromit bezpecnost pomocou c2h5oh utility (snooping), ktoru mozeme zamaskovat v nejakom beznom programe, napr. juice (tzv. trojan)
pozor ! tieto techniky nie je mozne pouzivat ak je pripojeny ROOT ! S utilitou c2h5oh nie je vhodne 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 opatrni, 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 drsnejsie 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 najvhodnejsie vyuzit vyssie spomenute exploity (kino, prechadzka.*, kwety).

- na distribuciu Blondian zabera na 100% exploit na dieru 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 zmienenych 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. Nazyvaly sa PASCUDY, co je vlastne skratka zo slov PAS a CUDNOST. Dnes sa uz tieto primitvne 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 spojazdnenie v distribucii BrunetWare je dost otiazne a vyzaduje vela casu a zrucnosti.

+[5]+----------+[ZABARIKADOVANIE]+----------
Po dosiahnuti 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 spojazdnenie, 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 duplifikacny protokol, skratka je z ludoveho narecia autora, ktory bol domorodcom z ostrova borneo, s mierne ugrofinskym prizvukom, pozn.

muf) na nestabilnych strojoch, tj. strojoch ktorych UPTIME je mensi ako 15 rokov. Niektore stroje sa preto snazia oklamat potencionalnych zaujemcov o vyuzitie tychto sluzieb pouzivanim PATCHnuteho uptimu, modifikaciou systemoveho casu, pripadne 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 vyuzivanymi zadnymi dvierkami je odchytenie a zalohovanie privatneho komunikacneho kluca. Zablokovanie 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 nacitat vasu konfiguraciu. Niekedy vsak staci len prikaz kill -POHUBE 1. Tieto problemy s implementovanim spravnej konfiguracie sa vyskytuju hlavne v distribuciach s jadrami sadistic a najma free a public.
Odporucane su aj upgrady systemu zaveditelnymi modulmi jadra DETi, ci uz aplikaciou X-Lapec alebo daemonom IEVCAd. Vhodne je instalaciu konzultovat s povodnymi administratormi systemu.

+[9]+----------+[DOVERYHODNOST A BEZPECNOST]+----------
Tento navod berte s rezervou a hlavne pri sietovom styku pouzivajte ochranne 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 vhodne pouzivat na verejnych, nekryptovanych kanaloch, uliciach alebo inych miestach obvykleho vyskytu, ale doporucujeme vyuzivat kryptovanu komunikaciu na neverejnom okuhu, odpojenom od ostatnych sieti, pripadne 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