Tvorime honeypoty

Vložil/a clusk [1], 13 Prosinec, 2004 - 04:03

- Hacking [2]
- Recenze [3]
- Security [4]

Prakticky navod na tvorbu honeypotu pomoci aplikace honeyd.

Uvod

Na uvod by bylo dobre si rici, co ze to vlastne honeypot je. V prekladu do cestiny to znamena "medovy hrnec" a jedna se o aplikaci, ktera simuluje virtualni prvek (pocitac, router, ...) v siti se vsemi jeho vlastnostmi - tzn. operacni system, otevrene/zavrene porty, bezici sluzby, bannery techto sluzeb, veskere prvky dane sluzby a mnoho dalsiho. Na tvorbu honeypotu se da na internetu najit nekolik komercnich i nekomercnich programu. My si ukazeme praci s nekomercnim programem honeyd. Rekl bych, ze ten je jeden z nejznamejsich a nejpouzivanejsich.

A na co vlastne honeypot? Tuto otazku jsem si polozil take, kdyz jsem zacal honeypoty studovat. Vzapeti jsem si odpovedel - uz podle nazvu, slouzi jako lakadlo na hackery (sladky med, ale lepkavy;)). Hacker v siti vzdy vyhledava ten nejmene zabezpeceny stroj (retez je vzdy jen tak silny, jak je jeho nejslabsi clanek), takze muzeme vytvorit "deravy" server a odlakat tak hackera mimo nase dulezite servery. Ve spojeni s IDS (intrusion detection system) pak muzeme zkoumat, co vsechno hacker zkousi. Timto zpusobem je odhalovano spoustu 0-day exploitu (exploity, jenze nejsou oficialne vydany, ale funguji:)). V neposledni rade bojuji honeypoty i proti virum a cervum - zachytavaji a analyzuji.

Dukladne jsem prostudoval veskere materialy, ktere jsem nasel - google po zadani "honeyd pdf" vysype ohromne mnozstvi pdf dokumentu. Tyto dokumenty zanedlouho naleznete i v nasi pripravovane knihovne e-booku, na ktere pracujeme. Ale zpet k veci. Vse jsem zkousel v praxi a mohu vam tedy predat k precteni muj navod...

Instalace

Na oficialni strance - http://www.honeyd.org [5] - muzeme stahnout zdrojove soubory a vse si sami zkompilovat. V tom pripade ale budeme potrebovat i nasledujici knihovny, na nichz je honeyd zavisly: libevent, libdnet a libpcap. Vetsina distribuci ma ale honeyd jiz v balickovacim systemu, takze staci nainstalovat. Nazev balicku je logicky honeyd. Dale potrebujeme aplikaci arpd.

Nastaveni

Pozor! Predtim nez se pustime do samotneho nastavovani honeyd, musime spustit zminovany arpd, ktery se bude starat o "zivot" IP adresy pridelene nasim virtualnim strojum. Rekneme, ze chceme vytvorit 3 virtualni stroje s IP 10.0.0.2-10.0.0.4, spustime arpd takto: arpd -i eth0 10.0.0.2-10.0.0.4. V praxi to pak funguje tak, ze pokud se nekdo bude chtit spojit napriklad s pocitacem s IP 10.0.0.2, vysle se pozadavek a na nej odpovi pocitac 10.0.0.1, ale s IP adresou 10.0.0.2 (protoze jedna mac adresa patri obema IP).

Ted uz k samotnemu nastaveni honeyd. Zkusime si vytvorit dva virtualni stroje s operacnim systemem MS Windows XP a jeden z nich bude mit otevreny port 21, na kterem budeme emulovat

FTP sluzbu. Nejprve vytvorime prvni, jednodussi stroj. Vytvorime si soubor honeyd.conf s timto obsahem:

```
create windowsxp
set windows personality "Microsoft Windows XP Professional"
add windowsxp tcp port 135 open
add windowsxp tcp port 139 open
add windowsxp tcp port 137 open
add windowsxp tcp port 445 open
add windowsxp udp port 137 open
add windowsxp udp port 138 open
set windowsxp default tcp action block
set windowsxp default udp action block
set windowsxp default icmp action open
bind 10.0.0.2 windowsxp
```

Timto mame hotovy prvni stroj. Na vysvetleni zde popisi vyznam jednotlivych prikazu:

```
create windowsxp
```

Vytvoreni stroje s nazvem windowsxp. Nazev slouzi pouze jako identifikator pro honeyd, utocnikum se nikde nezobrazi.

```
set windows personality "Microsoft Windows XP Professional"
```

Nastaveni "charakteru" systemu, neboli jak se ma dany system tvarit. Podle toho honeyd pozna, jaky otisk (fingerprint) ma na zadost poslat utocnikovi. Jestlize nevite, jak presne ma byt tento retezec zapsan, podivejte se do souboru nmap.assoc.

```
add windowsxp tcp port 135 open
```

Otevre TCP port 135. Stejne i pro UDP, jen se zameni slovicka tcp a udp.

```
set windowsxp default tcp action block
```

Nastavi standardni (default) akci pri skenovani nedefinovanych portu. V tomto pripade budou ostatni (nenastavene) porty blokovany. Analogicke pro udp i icmp. Jestlize toto zapomenete nastavit, budou se vsechny porty hlasit jako otevrene!

```
bind 10.0.0.2 windowsxp
```

Prideleni IP adresy k virtualnimu stroji. V tomto pripade davame nasemu virtualnimu stroji s nazvem "windowsxp" IP adresu 10.0.0.2.

Podobne si vytvorime i druhy stroj, ale s FTP sluzbou. V nasem pripade pouzijeme jiz hotovy skript ftp.sh, ktery je k honeyd prilozen. Konfiguracni soubor upravime tak, ze cely odstavec zkopirujeme jeste jednou pod sebe a zmenime vsechna slova "windowsxp" treba na "ftpserver". Mezi prikazy na otevreni portu pridame tento:

```
add ftpserver tcp port 21 "sh ftp.sh"
```

CC-BY-SA Security-Portal.cz | secured by paranoid sense | we hack to learn

Tim docilime toho, ze po pripojeni na port 21 se spusti soubor ftp.sh, bude reagovat na prikazy a vypisovat svuj vystup primo na port. Nesmime zapomenout zmenit i posledni radku na:

```
bind 10.0.0.3 ftpserver
```

Jako treti a posledni stroj si zkusime udelat postovni server bezici na operacnim systemu linux. Dva potrebne soubory stahneme z http://www.honeyd.org/contrib.php [6]. Jmenuji se smtp.sh a pop3.sh. Po stahnuti z nich musime udelat spustitelne soubory (chmod +x smtp.sh). Cast tykajici se naseho virtualniho linuxu bude v konfiguracnim souboru vypadat nejak takto:

```
create mailserver
set mailserver personality "Linux 2.4.16 - 2.4.18"
add mailserver tcp port 25 "sh smtp.sh"
add mailserver tcp port 110 "sh pop3.sh"
set mailserver default tcp action block
set mailserver default udp action block
set mailserver default icmp action open
bind 10.0.0.4 mailserver
```

Spusteni

Dostali jsme se k samotnemu spusteni nasi medove misky. Provedeme to timto jednoduchym prikazem:

```
honeyd -f honeyd.conf 10.0.0.2-10.0.0.4
```

Po spusteni honey daemona by mely zacit virtualni pocitace reagovat na ping (pokud jste nastavili spravne "set windowsxp default icmp action open") a na dalsi zadosti. Zkuste si nektery z honeypotu oskenovat nmapem.

Detaily

Skripty, jako jsou zde pouzite ftp.sh, smtp.sh a pop3.sh jsou psany v bashi. Skripty si muzete napsat sami, se svymy funkcemi a to i v perlu nebo pythonu. Prilozene skripty doporucuji upravit dle sveho. Napriklad smtp.sh se tvari jako smtp na SuSe linuxu, coz v nekterych pripadech nemusi byt spravne (na windows stroji urcite ne:)). Dale doporucuji procist manualovou stranku k programu (man honeyd). Snazil jsem se zde popsat zaklady a napsat prakticky navod, ale honeyd toho umi daleko vic - napriklad umi simulovat router, jak jsem se na zacatku zminil. Nebo umi vytvorit cele site propojene GRE tunnelem, ci simulovat zpozdeni, ztratavost nebo sirku pasma. Vsimnete si ale vlastnosti pri trasovani virtualniho pocitace (napr. tracert 10.0.0.2). Paket putuje pres 10.0.0.1, coz je logicke, ale v nasem pripade nezadouci. Proto se doporucuje spustit honeyd na vasi dobre zabezpecene brane.

Závěrem

Jestliže najdete nejakou nepresnost ci chybu, informujte me prosim v diskuzi, opravim to. Pokud mate nejake otazky, zkuste opet diskuzi, vynasnazim se vam poradit:) A uplne nakonec - toto je pouze seznameni se zakladni syntaxi a popis toho, jak to vlastne funguje. Kdyby byl zajem, napisi klidne druhy dil, kde si vyzkousime tvorbu routeru, nastavovani ztratavosti atd...

CC-BY-SA Security-Portal.cz | secured by paranoid sense | we hack to learn

URL článku: https://security-portal.cz/clanky/tvorime-honeypoty

Odkazy:
[1] https://security-portal.cz/users/clusk
[2] https://security-portal.cz/category/tagy/hacking
[3] https://security-portal.cz/category/tagy/recenze
[4] https://security-portal.cz/category/tagy/security
[5] http://www.honeyd.org
[6] http://www.honeyd.org/contrib.php

CC-BY-SA Security-Portal.cz | secured by paranoid sense | we hack to learn