Denne guide er oprindeligt
udgivet på Eksperten.dk

COMPUTERWORLD

Administratorens Hacker værktøjer. Del 2

Dette er anden del af en serie om hackerværktøjer og viden for administratore. Læs første del først
http://www.eksperten.dk/artikler/387

Skrevet den **10. feb 2009** af **bufferzone** I kategorien **Sikkerhed / Generelt** | ★★★☆☆

Administratorens Hacker værktøjer. Del 2

Denne artikel er anden del af en serie om værktøjer der bruges af hackerne og som den seriøse administrator er nødt til at kende.

Del 1:http://www.eksperten.dk/artikler/387.
Del 2:http://www.eksperten.dk/artikler/400.
Del 3:http://www.eksperten.dk/artikler/426.
Del 4:http://www.eksperten.dk/artikler/445.

Som altid når man bevæger sig ind på dette område, skal det siges at hacking er strengt forbudt og straffes. Disse værktøjer bør kun anvendes af øvede brugere på "rigtige" net med adgang til Internettet. Alle andre bør kun bruge dem i test netværk, det ikke har forbindelse til andre. Jeg selv kunne aldrig finde på, at teste værktøjer jeg ikke er 100% dus med på et "skarpt" miljø.

I del 2 vil jeg kikke på nogle af de områder, der danner forudsætning for at du kan få maksimal udbytte af de værktøjer jeg gennemgik i del 1. De ting der her gennemgås er områder du er nødt til at vide noget om som administrator da det er områder hackerne mestre.

Perl.
http://www.perl.org/
Perl er et programmerings/script sprog, der er meget populært i Linux verdenen og dermed også blandt hackere. Som administrator vil du opdage at perl er utroligt stærkt til at scripte administrations opgaver og andre rutine opgaver. Som administrator og interesseret i IT sikkerhed kan du ikke komme uden om perl af følgende grunde.
Mange exploits er skrevet i perl. Som du har læst i del 1 bør du validere de sårbarheder som f.eks. programmet Nessus finder til dig. Når nessus præsenterer resultatet af sin scanning kunne det f.eks. se således ud:

```
Vulnerability found on port http (80/tcp)
The web server is probably susceptible to a common IIS vulnerability discovered
by
'Rain Forest Puppy'. This vulnerability enables an attacker to execute arbitrary
commands on the server with Administrator Privileges.

*** Nessus solely relied on the presence of the file /msadc/msadcs.dll
*** so this might be a false positive

See Microsoft security bulletin (MS99-025) for patch information.
Also, BUGTRAQ ID 529 on www.securityfocus.com (
http://www.securityfocus.com/bid/529 )
```

```
Risk factor : High
CVE : CVE-1999-1011 (http://cgi.nessus.org/cve.php3?cve=CVE-1999-1011 )
BID : 529 ( http://www.securityfocus.com/bid/529 )

Nessus ID : 10357 (http://cgi.nessus.org/nessus_id.php3?id=10357)
```

Læg her især mærke til de 3 links I bunden af rapporten.
CVE er en forkortelse for "Common Vulnerabilities and Exposures" her kan du finde yderligere oplysninger om sårbarheden.

BID er en forkortelse for Bugtraq ID og hvis du følger dette link kommer du frem til en side der bl.a. giver dig mulighed for at se nogle af de exploits der findes (tryk på linket exploit og scroll ned i bunden af siden) her ser du linket /data/vulnerabilities/exploits/msadc.pl der giver dig en perl fil med et exploit til denne sårbarhed. Hvis du ikke har kendsskab til perl kan du ikke gennemskue scriptet og hvis din maskine ikke understøtter perl kan du ikke eksekvere scriptet og dermed ikke se hvordan det virker.

Nessus ID er et link til den side hos Nessus der beskriver sårbarheden, på denne side (dog ikke i dette tilfælde) kan du ofte klikke på et link der viser dig source koden til det plugin, nessus bruger til at teste sårbarheden. Dette plugin er skrevet i nessus egen udgave af perl, der selvfølgelige ligner perl meget. Hvis du ikke kan finde en exploit på securityfocus.org eller andet sted på nettet, kan du, hvis du kan læse perl, se hvordan nessus ville teste sårbarheden og dermed validere sårbarheden manuelt.

Efterhånden som du bliver dus med perl vil du også opdage at du kan bruge perl til at gennemse dine log filer. Du kan skrive perl scripts der gennemlæser logfiler, henter de relevante posts ud og præsentere dem på en mere sigende måde. Jeg taler her om alle former for logfiler, både firewall logs og Snort logs. Mere herom senere.

Snort og Snortsnaf.
http://www.snort.org
Snort er et "Network based Intrution Detection System (NIDS eller bare IDS)" der kan kører på både Linux og Windows. Det er et open source projekt og som sådan gratis. Snort følger med i mange linux distributioner og de fleste firewall løsninger der bygger oven på linux netfilter firewall indeholder også Snort (se f.eks. shorewall og Smoothwall)

Som du sikkert kan regne ud, så kikker Snort på netværkstrafik og lige som en virusscanner, skal den kende signaturen for trafikken for at kunne genkende den. Snort laver Real-Time trafik analyse og logger IP trafik. Den kan lave protokol analyse, kikke på dataindhold og matche dette op mod sin signatur database for at genkende f.eks. buffer overflows og CGI angreb. Den kan genkende hele trafikmønstre som f.eks. portscanninger og stealth portscanninger, SMB prober, OS fingerprinting og meget mere.
Ud over at genkende signaturer og at logge trafikken, kan Snort også alarmere en administrator. Alarmeringen kan ske på mange forskellige måder, alt efter hvilke teknologi man har til rådighed. Du kan få popup vinduer, e-mails og sms beskeder til din mobiltelefon.

Hvis du ikke er vant til Linux kommandolinie administration og aldrig har sat en netfilter firewall op, så vil Snort virke gammeldags og uoverskuelig for dig. Alt foregår via kommandolinien eller gennem konfigurations filer. Mit råd til dig er at tage det roligt og arbejde dig frem stille og roligt med små succeser ad gangen. Start med at installere Snort og få den til at logge. Prøv så at portscanne dig selv, eller brug en af de programmer jeg nævner herunder, se om du kan genkende trafikken i Snort's log. Snort kan utroligt meget og hvis du vil det hele med det samme, så ender du med at brække nakken. Start i det små, så skal du nok blive god, men du er nødt til at gøre det i praksis, du kan ikke læse dig til det.

Snortsnarf er faktisk skrevet i perl, og kræver at du har perl installeret på din maskine for at kunne kører. Snortsnarf bruges til at nedbryde Snort alart filer og præsentere den i html format på en sådan måde at

man kan overskue hvilke problemer og trusler der er logget, Hvor Snort logger og alarmere ud fra en signaturdatabase, samler Snortsnarf hændelserne "statistisk" og behandler dem visuelt. Under normale forhold vil du bruge et såkaldt Cron Job eller tilsvarende til at producere regelmæssige, d.v.s. f.eks. sige daglige eller ugentlige filer af Snort alarmer, der så behandles af Snortsnarf.

Igen skal du bruge både Snort og Snortsnarf for at blive rigtig god til det. Da der her er tale om IDS og plugin til IDS vil det være naturligt at arbejde på begge sider af firewallen. Brug programmer som Nmap, nessus, netwox mod firewallen, Brug TCPDump til at validere hvad der faktisk sendes af pakker fra disse programmer. Brug så snort og Snortsnarf på selve firewallen og på den anden side for at se hvordan disse angreb og prober ser ud for en administrator, det vil hjælpe dig til dels at genkende hvad der sker og også give dig en større forståelse for hvad der skal gøres som forsvar.

Tripwire.
http://www.tripwire.org/
Tripwire er et "Host based Intrution Detection System (HIDS eller bare IDS)", der kikker på filer og ikke på trafik. Lidt forenklet, så virker tripwire ved at tage en checksum/Hashværdi af alle filer og så holde øje med hvilke filer der ændres hvornår og af hvem. Tripwire er gratis til Linux og koster til Windows. Der findes andre produkter, der baserer sig på samme teknik, de fleste er kommercielle og enkelte gratis.
I praksis er det selvfølgelig ikke alle filer tripwire holder øje med. Det ville ikke være praktisk da mange filer faktisk ændres løbende ved lovlig brug af din PC. Tripwire holder øje med key attributter på filer der ikke burde ændres, herunder binære signaturer og filstørrelse. Det der giver kvaliteten i et program af denne type, er balancen. Programmet skal alarmere når der sker noget grimt, men ikke når ændringerne er naturlige.
Tripwire, der er et gratis open source program, er fuldt på højde med dyre kommercielle produkter,

Du kan her finde både beskrivelse samt installations vejledning og andet på dansk

http://www.linuxbog.dk/sikkerhed/sikkerhed/tripwire.html

I professionelle net, hvor sikkerheden sættes i top kan man gøre brug af Snort på f.eks. firewall, specielle IDS prober der indsættes til at sniffe kritisk trafik og på SYSLOG serveren hvor alle logfiler samles. Kritiske systemer som f.eks. firewallen og SYSLOG serveren beskyttes så af Tripwire.

NetFilter.
http://www.netfilter.org
Enhver seriøs hacker er nødt til at have et indgående kendskab til hvordan en firewall fungerer og sættes op. Mange administratorer holder meget af at købe en dyr boks, med et dyrt navn uden på og et fancy interface med farver og grafik som de så kan pege på og sige at de selvfølgelig har en Firewall-1 fra checkpoint og så kan det jo ikke gøres bedre.

Dette er en sandhed med kraftige modifikationer, selv en dyr firewall kan fejlkonfigureres hvis man ikke ved hvad man gør og også dyre firewalls har sårbarheder. (Når man bevæger sig i miljøet er det faktisk relativt sjældent at man finder en firewall der slet ikke har fejlkonfigurationer der kan udnyttes)

Netfilter er indbygget i Linux kernel og følger således med i alle Linux distributioner (kernel 2.4 og op). Fordelen (og ulempen) er, at det kræver viden at sætte den op og at Netfilter nærmest kan udbygges i det uendelige. Netfilter er et rigtig godt valg hvis du vil lære at konfigurere firewalls og et helt naturligt valg til dit testmiljø.

Netfilter's regelsæt kan laves forholdsvis enkelt eller meget kompliceret hvis du ønsker. Du kan starte med at lave en simpel pakkefiltrerings router, derefter udbygge med stateful inspection og ende ud med proxy funktionalitet på applikations niveauet hvis du ønsker det. (læs mere om de forskellige firewall typer her http://www.eksperten.dk/artikler/158)

Du kan bruge Netfilter som den er eller du kan anvende færdige produkter der bygger oven på Netfilter

som f.eks. Smoothwall eller Shorewall.

Netfilter kan lave port forwarding, også kaldet masquerading. Den kan lave Network Address Translation kaldet NAT i flere forskellige former.

Der findes udbygninger til Netfilter som Squid der er en http, FTP og Gopher proxy der giver performance forbedringer via ram caching af filer og DNS opslag, indholdssikkerhed gennem filtrering af URL og http data. Du kan booste sikkerheden yderligere ved at implementere Jeanne oven på Squid der så giver dig den ultimative kontrol med den http trafik du tillader at passere.

Det var så anden del i serien. I denne del har jeg ikke været hel så konkret som i del 1. Dette skyldes at der her er tale om emner der danner forudsætning for den dybere forståelse af virket som administrator. Hvor del 1 kunne tages i anvendelse direkte, du kunne installere programmerne og prøve eksemplerne, er der hel tale om emneområder der kræver væsentligt mere arbejde at mestre. Dette gør dem faktisk ikke mindre væsentlige, men dem der havde regnet med at det ultimative hacker kursus max tog en weekend er nu sat af.

Skulle du have spørgsmål, kommentarer eller rettelsen (herunder især stavefejl) er du velkommen til at kontakte mig på kim@bufferzone.dk, ligesom jeg ofte er at finde på Eksperten. Jeg hjælper selvfølgelig også gerne med de forskellige værktøjer. Undlad venligst at stille spørgsmål i kommentarerne, dem kan jeg jo ikke svare på.

Kommentar af cybermike d. 04. dec 2004 | 1

Læs min kommentar på http://www.eksperten.dk/artikler/426 før du køber artiklen.

Kommentar af steen_hansen d. 25. aug 2004 | 2

Stærkt, bufferzone - igen :o)

Kommentar af webmasterdk d. 24. aug 2004 | 3

Atter en fin artikel!
Synes du ikke snart du har fået nok af vores point? ;)

Kommentar af the_email d. 24. aug 2004 | 4

Endnu en kanon artikel fra bufferzone. Keep up the good work :-)

Kommentar af mortency d. 18. nov 2004 | 5

Veldig bra.

Kommentar af dustie d. 09. aug 2005 | 6

Kommentar af ttj d. 24. aug 2004 | 7

Fin artikel

Kommentar af sorenbs d. 24. aug 2004 | 8