Administratorens Hacker værktøjer. Del 1

Denne artikel er IKKE for begyndere, men for den øvede administrator eller den der ønsker at blive det. Artiklen er første del i en serie der gerne skulle sætte dig igang med disse helt nødvendige administrator værk

Skrevet den **07. Feb 2009** af **bufferzone** I kategorien **Sikkerhed / Generelt** | ★★☆☆☆

Administratorens hacker værktøjer. Del 1.

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.

En administrator der ønsker at beskytte sit netværk, er nødt til at vide en del om hvordan en hacker arbejder og kunne bruge mange af de værktøjer der anvendes af hackerne. Han anvender dem ikke nødvendigvis på samme måde som en hacker ville, da han ikke behøver at skjule hvad han har gang i. Herunder gennemgås et lille udsnit af de vigtigste værktøjer samt lidt om hvordan de anvendes og andre tips der skulle kunne hjælpe administratoren i hans kamp.

Religion og den løftede pegefinger.
Lad mig starte med at slå den religiøse diskussion ihjel før den starter. Jeg kender godt de orginale betydninger af både hacker og cracker. I dag hedder en ondsindet person der bryder ind i computer systemer en hacker. Om det er rigtigt eller ej er du velkommen til at diskutere til hudløshed, forvent ikke at jeg deltager.

Det skal også siges at hacking er strengt forbudt og straffes. Du må ALDRIG anvende nedenstående værktøjer over Internettet mod andre, heller ikke selv om du har fået lov eller er blevet bedt om det på f.eks.Eksperten. Er du sikker på at den person der beder dig hacke hans net virkelig ejer nettet? Eller har han lige sat dig i gang med at ødelægge konkurrentens systemer. Hvis du nu ender med at ødelægge noget der koster penge, er du så helt sikker på at manden der bad dig hacke ham, også kan huske det når han skal betale regningen? LAD VÆRE MED AT FORSØGE DEN SLAGS på andet end lukkede netværk, du selv ejer og har fuld kontrol med.

Test maskinen.
Du kan lige så godt først som sidst installere en Linux maskine, du kan ikke klare dig med Windows alene, da der er værktøjer der ikke findes til Windows, er urealistisk dyre til Windows eller simpelthen fungere dårligt på Windows, så det er bare at gå i gang. Hvilken distribution du vælger er ikke så vigtig, jeg kører selv Fedore, Debian eller PHLAK alt efter hvilken af mine maskiner jeg lige sidder ved eller hvad jeg laver, og jeg har da også en KNOPPIX CD distribution eller 2 liggende til døde systemer der skal vækkes.

TCPDump. eller **WINDump** til windows.
Download: http://www.tcpdump.org
Manual: http://windump.polito.it/docs/manual.htm (windump)

TCPDump er en uundværlig netværks sniffer, du er nødt til at være dus med. At give en uddybende forklaring og beskrivelse her ville ikke være muligt, men jeg kan sætte dig i gang og så må du arbejde med den seriøst for at lærer den at kende. Du kan ikke klare dig uden en sniffer, da det er den eneste måde at finde ud af hvad der virkelig foregår helt nede på bit niveau. (mail mig hvis du har spørgsmål eller stil dem på eksperten). TCPDump bruges til et hav af ting, lige fra almindelig sniffning af trafik, over validering af værktøjer, firewalls og andre programmer samt kontrol af alle mulige forskellige ting.

Her er først et eksempel på hvordan en sniffning ser ud med mine kommentarer i []

```
[s&aring;dan starter jeg sniffningen fra/p&aring; min egen maskine]
E:\Download\tcpDump>tcpdump -X host 80.63.242.176
tcpdump: listening on \Device\NPF_{9DC5D0F0-E248-4277-BD9F-901DAD2D49BD}

[jeg har klippet en af de opfangede pakker ud, en indkommende SYN pakke]

|22:24:29.136279| IP |0x503ff2dd.boanxx10.adsl-dhcp.tele.dk.4310 >||
bufferzone.opasi
a.dk.2745|:| S| 3398479460:3398479460(0) win 64240 <mss 1460,nop,nop,sackOK>
(DF)
0x0000   4500 0030 1f77 4000 7f06 5644 503f f2dd        E..0.w@...VDP?..
0x0010   503f f2b0 10d6 0ab9 ca90 ae64 0000 0000        P?.........d....
0x0020   7002 faf0 6d9d 0000 0204 05b4 0101 0402        p...m...........
```

Alle disse tal, der for den uindviede ser ud som volapyk, har betydning og kan fortælle dig masser hvis du kan læse dette. De fircifrede tal par under de første to linier i hver pakke er faktisk hexadecimale tal par der hver repræsentere en bite. Hvis du f.eks. kikker på første pakke. Kan du se byte 0 er 45 (første bite tælles altid 0) dette viser at der er tale om IP version 4 pakke med en header længde på 5 4 bite's segmenter, i alt 20 bite. Den 9. bite har værdien 06, her kan vi læse at der er tale om TCP protokollen der har nummer 6.
De første to linier fortæller dig alt om source og destination IP adresser, porte, offset hvis der er tale om fragmenterede pakker, sekvens nummer, flag og meget mere.

Således kan du uddrage alt den information der findes i alle pakker hvis du taler det rigtige sprog, og der er kun en måde at lærer det på, det er at tale og tale.

Her et par eksempler på hvordan du får tcpdump til at sniffe forskellige ting

tcpdump -X host 80.63.242.176 and ip[9]=17 [her fanges DNS trafik (protocol 17, hex 11)]

tcpdump -X host 80.63.242.176 and ip[9]=1 [her fanges ICMP pakker (protocol 1, hex 01) dette vil f.eks. fange en loki bagdør]

tcpdump -Xe host 80.63.242.176 [e switchen medtager MAC addresser, her kan du se om der skulle være netkort du ikke kender på dit net]

tcpdump -nnX -w prove_class.cap [her dumpes sniff resultatet til filer prove_class.cap til efterfølgende behandling]

tcpdump -nnr perimeter_class.cap tcp port 25 |more [her finder du alle mailservere i nettet]

tcpdump -nnr perimeter_class.cap src net 12.33 and tcp port 25 |more [her finder du alle mailservere i subnettet 12.33]

tcpdump -nnr perimeter_class.cap tcp[0:02]=0x19 and src net 12.33 and not src host 12.33.247.3 |more [her søges i filer perimeter_class.cap, i TCP headeren med et offset på 0 bytes og en længde på 2 bytes for alle poster med værdien 25 (hex 0x19) i subnettet 12.33, dog ikke hosten 12.33.247.3. Det er port 25 vi søger efter og vi udelukker en kendt mailserver. Her kan du f.eks. se om der skulle være sat servere op i dit netværk du ikke kender til]

TCPDump kan meget meget mere men den kræver viden og kunden. Det kan du ikke læse dig til i en artikel. Du må arbejde med programmet og have et indgående kendskab til TCP/IP protokollen og alle andre afledte protokoller.

Nmap.
http//:www.insecure.org/
Nmap er **port scanneren**. Det er den Triniti brugte i en af Matrix filmene og det er den alle hackere med respekt for sig selv bruger. Glem alle andre port scannere hvis du vil tage alvorligt. Der findes et grafisk interface til Windows versionen (måske også til linux, men sådan noget har en ordentlig hacker ikke forstand på og kunne aldrig drømme om at bruge).

Lige som TCPDump kan Nmap konfigureres meget fint og scanne på et hav af måder. Hackeren vil bruge tid på at konfigurere Nmap så den ikke opdages af Intrution Detection systemer og så scanningerne skjules i loggen. Det behøver vi ikke.

Her har du et eksempel på et Nmap scanningsresultat. Mine Kommentare i []

```
[s&aring;dan startes Nmap. sS betyder at der foretages en s&aring;kaldt TCP SYN
stealth port scan. Half scan/incomplete handshake. PO betyder Don't ping hosts
og p betyder scan portene mellem 0 og 65535]

nmap -sS -P0 80.63.242.176 -p 1-65535


Starting nmap V. 2.53 by fyodor@insecure.org ( http://www.insecure.org/nmap/ )
Interesting ports on (80.63.242.176):
(The 55 ports scanned but not shown below are in state: filtered)
Port       State       Service
22/tcp     open        smtp
25/tcp     open        smtp
80/tcp     open        http
443/tcp    open        https

Nmap run completed -- 1 IP address (1 host up) scanned in 63 seconds
```

Her er lidt forskellige gode muligheder
-sS TCP SYN stealth port scan. Half scan/incomplete handshake
-sT TCP connect port scan. Full 3-way handshake
-sU UDP port scan
-sP ping scan (Find any reachable machines)
-sF,-sX,-sN Stealth FIN, Xmas, or Null scan (experts only) *
-sV Version scan probes open ports determining service & app names/versions
-sR/-I RPC/Identd scan (use with other scan types)

Her er nogle optioner der normalt også bruges. F.eks. -O der gætter operativ systemet ganske godt under de fleste forhold.

-O Use TCP/IP fingerprinting gætter operativ systemet
-p <range> ports to scan. Example range: '1-1024, 1080, 6666, 31337'
-v Verbose. Giver dig flere oplysninger. Du kan sætte to V'er for at få endnu flere oplysninger.
-P0 Don't ping hosts

Lige som TCP dump kan du ikke lærer at bruge Nmap ved at læse en artikel, brug den, øv dig og spørg hvis der er noget du ikke kan finde ud af. Nmap bruges i øvrigt at flere andre værktøjer f.eks. nessus og Netwox

Nessus.
http://www.nessus.org/
Nessus er en sårbarhedsscanner og også et uundværligt værktøj for både hackere og administratorer. Nessus er et af de værktøjer der faktisk kun findes til Linux. Det vil sige, du kan få den til Windows, hvis du har rigtig mange penge. Sidst jeg kikkede kostede en Windows Nessus server 30.000 Dollars og du skal bruge en server. Linux versionen er ganske gratis.
Selve installationen af nessus er meget enkel. Der findes en enkel shell fil (.sh) du kører fra din linux maskine, den henter alle nødvendige filer, pakker dem ud, kompilere de binære filer og installere dem. Herefter skal du køre en række filer, f.eks. nessus-adduser for at lave den bruger konto nessus kører under (du kan her vælge root), nessus-mkcert for at lave server certifikater, nessus-update-plugins for at opdatere de sårbarheder nessus scanner for. Denne bør køres ofte. Endelig startes Nessus demonen (det hedder en service i linux verdenen) ved at give kommandoen nessusd.
Nessus har en grafisk flade, som selv hackerne bruger. Selve det at lave en sårbarhedsscanning er ikke det svære, men der er selvfølgelig noget man er nødt til at vide. Inden du begynder at scanne skal du slå "enable all but dangerous plugins" TIL. Hvis du ikke gør dette, vil Nessus også scanne for de sårbarheder der giver Denial of service, og dermed lukke den server du scanner ned. Dette er jo ikke en fordel, da Nessus så kun kan scanne til og med den første DOS sårbarhed, herefter vil serveren ikke virke og dermed ikke vise de sårbarheder den måske har.
Omvendt vil "enable all but dangerous plugins" betyde at Nessus giver dig mange falske positive, (fortæller dig at din server er sårbar over for et angreb, der ikke er sårbar overfor i virkeligheden). Og det betyder at du er nødt til at validere de fundne sårbarheder manuelt for at vide med sikkerhed hvad der er falske positiver og hvad der er reelle sårbarheder.
Da alle sårbarheder og også exploits er forskellige, skal de selvfølgelig valideres forskellige og det vil være umuligt at beskrive dem alle her. Det kunne der måske komme en fremtidig artikel ud af.
Læs mere om Nessus i del 2. Under afsnittet om Perl

Netwox.
http://www.laurentconstantin.com/en/netw/netwox/
Netvox er et hacker værktøj der anvendes til at crafte pakker og meget meget andet. Netvox indeholder mere end 212 forskellige værktøjer og du kan sammensætte alle mulige forskellige pakker til at teste din firewall opsætning og også til at validere nogle af de sårbarheder Nessus har fundet.
Netwox kan bl.a. Spoofe alle slags pakker, Sniffe og svare på forskellige pakker f.eks. DNS og dermed lave DNS poisoning, agere klient og server for et hav af forskellige protokoller, snakke telnet, ICMP, arp og meget mere.
Du er nødt til at være lidt opmærksom når du installere Netwox. Dels kræver den, at den rigtige version af Nmap er installeret (i virkeligheden er det ikke selve Nmap den anvender, men Nmap's object og klasse bibliotek) og så kræver den et antal andre object og klasse biblioteker installeret først. Læse vejledningen grundigt før du går i gang og

læs README filerne for hver enkelt fil samling (hedder en tarball i linux verdenen) grundigt inden du gør noget. Er du omhyggelig så kører det uden problemer, jabber du igennem vil du få problemer med afhængigheder og i yderste konsekvens fuc.... Dit system op,

Når du nu bruger Netwox til at validere firewall regler eller til at validere sårbarheder med, kan du passende bruge TCPDump både foran og bagved firewallen til at se hvad der kommer ind og ud af denne.

Der findes en grafisk flade til Netwox. Jeg har ikke selv brugt den endnu, men på baggrund af anbefaling fra den programmør der har lavet NetWox går jeg meget snart i gang med at kikke på den og vil opdatere artiklen når jeg ved hvad jeg taler om.
Igen du er nødt til at arbejde med tingene for at mestre dem at læse om dem er ikke nok.

Her er en liste over hvilke forskellige programmer Netwox indeholder.
http://www.laurentconstantin.com/common/netw/netwox/download/v5/toollist.txt

Her er et par pragtiske eksempler du kan bruge:

Fra kommando prompten skrives

netwox [netwox startes i hjælpe mode. Her kan du bl.a. få en forklaring på alle de andre værktøjer samt søge på funktionalitet. Hjælp til de enkelte værktøj fås ved at vælge 4 (når du er i hjælpe mode) og derefter skrive værktøjets nummer. Prøv dig lidt frem start f.eks. med værktøj 87 der er er at de meget brugbare]

Netwox 1 [dette vil vise dig din netværks konfiguration]
netwox 177 -i "195.41.46.251" -p "25" [her kontrollere jeg om TDC's SMTP server eksistere og er oppe]
Command returned 0 (OK) [betyder at den er oppe]
Error 4006 : error in connect()
hint: errno = 111 = Connection refused [betyder at der ikke eksistere en SMTP server på den IP eller at den er nede]

Efterhånden som jeg selv bliver mere dus med netwox kommer flere eksempler

Det var første del
Vi er nu nået side 5 og faktisk allerede over grænsen af hvad folk gider læse. Samtidig hermed kan det jo ikke siges at være let stof der bare glider ned uden fordøjelse. Jeg vil anbefale at du får din maskine op at køre, installere programmerne og lejer lidt med den.

Når du er færdig med at lege, så har jeg måske skrevet del 2, der bl.a. vil kikke på programmeringssproget Perl, programmerne Snort og Snortsnaf, L0phtCrack, Leviathan, N-Stealth, nikto, Whisker, Firewalk, Cheops-NG, Tkined, ProxyHunter, Superscan, Fping, Icmpquery, Dsniff, Ettercap, Hunt, Network Stumbler/MiniStumbler, Kismet, Hping2, Nemesis, Rain, Rafale, FragRouter, HttpTunnel, Stunnel, Fpipe, for lige at nævne nogle få som appetitvækker. (og tro ikke at listen er færdig, der er lige så mange tilbage endnu)

Du kan finde anden del at artikelserien her
http://www.eksperten.dk/artikler/400

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.

Kommentar af a1 d. 18. Aug 2004 | 1

god artikel men både let og svær at forstå f.eks. denne:
tcpdump -nnr perimeter_class.cap tcp[0:02]=0x19 and src net 12.33 and not src host 12.33.247.3 |more
[her søges i filer perimeter_class.cap, i TCP headeren med et offset på 0 bytes og en længde på 2 bytes for alle poster med værdien 25 (hex 0x19) i subnettet 12.33, dog ikke hosten 12.33.247.3. Det er port 25 vi søger efter og vi udelukker en kendt mailserver. Her kan du f.eks. se om der skulle være sat servere op i dit netværk du ikke kender til]? (Habla no Espaniol)
Hvorfor søge med et offset på 0 bytes og en længde på 2 bytes? (port 25, subnet og host siger (næsten) sig selv, selv for en der ikke ved meget)
Hvad er den "man" søger efter og gerne vil finde (eller ikke vil finde)? ;o)
Hvor ligger forskellen fra den ovenover? (bortset fra host)

Kommentar af cybermike d. 04. Dec 2004 | 2

http://www.eksperten.dk/artikler/426 læs mit indlæg der før du køber artiklen.

Kommentar af coder d. 29. Oct 2005 | 3

"Glem alle andre port scannere hvis du vil tage alvorligt"

"Der findes et grafisk interface til Windows versionen (måske også til linux, men sådan noget har en ordentlig hacker ikke forstand på og kunne aldrig drømme om at bruge)."

Hva er det for noget pis at lukke ud? Så du bruger ikke grafiske grænseflader? Du har sgu styr på tingene må man sige!

Kommentar af _darkstar_ d. 28. Aug 2004 | 4

Mangler at skrive at artiklen handler om Windows (før man betaler for at se den).

Kommentar af resten d. 14. Sep 2004 | 5

Super artikel Kim "resten" c",)

Kommentar af x-masman d. 18. Aug 2004 | 6

Udmærket artikel, der giver en introduktion til nogle få værktøjer. Men man må vel vente til næste artikel for at se flere. :o) Beskrivelsen af TCPDump, NMap og nessus er udmærket, mens beskrivelse af Netwox er lidt overfladisk. Det er lidt ærgeligt, da det nok er den, der måske kræver mest af brugeren. En mere fyldig beskrivelse af benyttelse af den, samt måske et par eksempler på praktisk brug havde været godt.

Kommentar af rossonero d. 18. Aug 2004 | 7

Go artikel .. at læse er godt .. men at prøve det i praksis er et must .. da det så giver mere mening.

Kommentar af barbarbo d. 19. Aug 2004 | 8

Rigtig god artikel. Jeg synes ikke den er for avanceret, også en begynder kan få meget ud af den, hvis han er parat til at arbejde lidt med tingene og læse lidt på nettet også

Kommentar af xyborx d. 17. Aug 2004 | 9

Lækker artikel, selvom jeg nu gerne ville have fået demonstreret nogle flere programmer. Det må jeg bare vente med til næste del :)

Kommentar af ebe d. 21. Jan 2007 | 10

De danske tegn er ikke med, så jeg har kun "hakket" mig igennem en del, og har så opgivet :(

Kommentar af slasher_x d. 19. Aug 2004 | 11

God artikel! Selv den lidt uerfarne kan følge med. Det er altid godt at have lidt at starte på, inden man selv går i gang med at eksperimentere..

Kommentar af wanze d. 25. Aug 2004 | 12

Fin artikel!

Kommentar af freehelp d. 24. Aug 2004 | 13

Good job buffer!!

Kommentar af optical d. 24. Aug 2004 | 14

hold da helt fast - jeg ejer rent faktisk mit netværk nu - heh - til Lan bliver der ikke downloadet warez eller noget :D

Kommentar af duronbro d. 24. Aug 2004 | 15

Kommentar af ranglen d. 24. Aug 2004 | 16

Kommentar af herkules69 d. 03. Oct 2004 | 17

Lækker artikel

Kommentar af i865 d. 25. Oct 2004 | 18

Kommentar af innercitydk d. 30. Apr 2006 | 19

Jeg synes det er absolut hul i hovedet at lave sådan en artikel her.

-"Det skal også siges at hacking er strengt forbudt og straffes. Du må ALDRIG anvende nedenstående værktøjer over Internettet mod andre, heller ikke selv om du har fået lov eller er blevet bedt om det på f.eks.Eksperten."

Alle ved at mange vil prøve disse ting fordi de er facineret at begrebet hacking! Der er unge mennesker derude der ikke tænker på konsekvenserne af deres handlinger. Du bidrager til dette formål selvom det ikke er din hensigt. Hvis du ikke havde lavet denne serie ville det være væsentligt sværer/tidskrævende at samle disse informationer..

Kommentar af per1291 d. 31. Jul 2005 | 20

Okay, du har overbevist mig: Jeg skal have installeret Linux på min reservemaskine. - Hilsen Per

Kommentar af arkanis d. 21. Mar 2007 | 21

Hvis man som mig har problemer med at læse artiklen så er her et lille fif.
Kopier teksten ind i et skriveprogram og brug " søg og erstat" funktionen=
æ = æ
ø =ø
å = å