Trådløs Hacking - Administratorens Hacker værktøjer. Del 4

Her er så del 4 i serien om administratorens hacker værktøjer. Denne artikel kan sagtens læses alene, men du får et langt bedre overblik hvis du læser dem i den tiltænkte rækkefølge.

Skrevet den **04. Feb 2009** af **bufferzone** I kategorien **Sikkerhed / Generelt** | ★★★☆☆

Administratorens Hacker værktøjer. Del 4 (trådløs Hacking).

Denne artikel er fjerde del af serien om værktøjer der bruges af hackerne og som den seriøse administrator er nødt til at kende. I denne del kikker vi på værktøjer til trådløs hacking

Andre artikler i serien
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. (Trådløs hacking)

Reglerne fra de tre foregående dele gælder stadig. Hack aldrig andre, hverken for sjov eller når de beder dig om det, og brug kun disse værktøjer i et sikkert test miljø der ikke har forbindelse med andre "skarpe" miljøer hvor du kan gøre skade.

Når vi taler om værktøjer til trådløs hacking, er der en ting der er meget vigtigt at vide. For at værktøjerne kan virke, kræver det ofte at de understøtter dit trådløse netkort. Du er derfor nødt til at vide hvilket netkort du har og om det understøttes at de værktøjer du ønsker at bruge, ofte er værktøjerne Linux baserede, hvorfor det også er vigtigt at vide om dit netkort understøttes i Linux. Trådløse maskiner er jo oftest bærbare og det kan give lidt udfordringer når du skal installere Linux, det kan dog oftest sagtens lade sig gøre hvis du forbereder dig ordentlig og får lidt hjælp.

Wardriving er et fænomen der hører til miljøet omkring trådløs hacking. Sammen med dette findes Warchalking der faktisk kan betragtes som en tillægs disciplin. Wardriving går ud på at hackeren kører rundt med en bærbar computer med trådløst netkort og forsøger at fange, hacke og udnytte alle de trådløse net han kan finde. Warchalking går ud på at markere alle de bygninger der indeholder trådløse net med oplysninger så andre hackere der kommer forbi kan se at her er et trådløst net og hvilke oplysninger de skal anvende for at kunne udnytte det.

Network Stumbler.
http://www.netstumbler.com

Network Stumbler er et Windows baseret værktøj der aktivt kan lytte og forespørge efter alle accesspoints der er åbne for broadcast probes for standarderne 802.11 a, b og g. Net Stumbler vil ofte kunne give oplysninger om MAC adresse, SSID, accesspoint navn, fabrikat og om der anvendes WEP kryptering. Net stumbler kan samarbejde med GPS udstyr, så man kan visualiserer de net der findes på et kort. Net Stumbler findes også i en udgave, der kan kører på en pocket PC.

Da Net Stumbler er et Windows program og man ikke kan indsætte screen dumps i artiklerne, er det vanskeligt at vise hvordan programmer virker. Der er dog ingen tvivl om at enhver ejer af et trådløst

netværk, som også interessere sig for sikkerheden bør bruge Net stumbler eller tilsvarende program.

Do some WarWalking.
Først og fremmest bør du anvende NetStumbler til at finde ud af hvor stort det område hvor dit net kan tilgås fra er. Du bør også eksperimentere med placeringen af dit accesspoint og med hvordan dine antenner peget. Det drejer sig om at placere sit accesspoint og antenner således at signalstyrken er bedst inden for "egne mure" og ikke stråler ret meget ud uden for disse. Du kan også eksperimentere med andre antenner, eller med afskærmning i forhold til dit accesspoint for at forbedre dine sendeforhold.
Det at vide hvilke andre net der er operative i dit område er også væsentligt for din sikkerhed, det at naboen har et trådløst accesspoint, betyder jo også at han har mindst en PC med trådløst netkort, der bevidst eller ubevidst kan tilkobles dit net, hvis du ikke har gjort dit arbejde ordentligt.
Network Stumbler er afgjort et hacker værktøj, men det har bestemt også plads i den seriøse trådløse administrators værktøjskasse.

Kismet.
http://www.kismetwireless.net/

Kismet er et gratis Linux værktøj der kan mange af de samme ting som NetWork Stumbler. Det er dog min opfattelse, at den kan konfigureres finere og har mere funktionalitet. Frem for alt så er den kompatibel med en del andre uundværlige Linux værktøjer. Funktionalitet og features er blandt andet:

- Ethereal/Tcpdump kompatibel data logning. Meget væsentligt da TDPDump kan filtrerer utroligt fint. Læs del 1 af denne serie,
- Airsnort kompatibel weak-iv pakke logning. Også vigtigt, se herunder
- Network IP range detection
- Indbygget channel hopping og multicard split channel hopping. Meget avanceret teknik der anvendes til at skjule signalkanaler
- Hidden network SSID decloaking. Her er intet helligt.
- Grafisk mapping af netværk, herunder understøttelse for samarbejde med GPS
- Client/Server arkitektur, der gør det muligt for flere klienter at anvende en Kismet server
- Mærke og model identifikation af accesspoints og klienter
- Detektion af kendte default accesspoint konfigurationer
- Runtime decoding af WEP pakker for kendte netværk
- Named pipe output for og dermed fuld integration med andre værktøjer f.eks layer 3 IDS, f.eks. Snort (Se del 2)
- Multiplexing af mange simultane capture sources fra samme Kismet instance
- Distribueret remote drone snifning
- XML output
- Support for mere end 20 forskellige trådløse netkort

Kismet kan bruges "som den er" men der kan installeres ekstra funktionalitet, ønsker du f.eks. understøttelse for anvendelse af GPS og grafiske kort, skal der installeres en del ekstra klasse biblioteker og andre moduler, se den udmærkede dokumentation

Udover at bruge kismet som et aktivt værktøj til at finde andres trådløse net og til at teste eget net, kan du også bruge Kismet som intrusion detection og alarmeringssystem på dit eget trådløse netværk. Kismet kan bl.a. Give alarmer baseret på forskellige fingerprints, f.eks. netstumbler signatur og andre specifikke angreb og prober. Kismet håndtere 802.11 kommunikation og tilbyder integration med layer 3+ IDS som f.eks. Snort via named pipes

En alarm kunne f.eks. se således ud

```
Alert name:       NETSTUMBLER
Alert type:       Fingerprint
Alert on:         Netstumbler probe requests
Alert message:    "Netstumbler ($version) probe detected from ($macsource)"
Tool-specific:    Yes (Netstumbler 3.22, 3.23, 3.30)
References:       http://www.netstumber.com
Details:          In an attempt to disclose the SSID of a network,
                  Netstumbler sends out unique packets.  This is not done
                  in all situations, but when it is detected the potential
                  for false positives is very low.
```

AirSnort.
http://airsnort.shmoo.com/
AirSnort er en passiv trådløs forbindelses monitor til både Windows og Linux, der opsamler pakker, og når nok pakker er indsamlet udregnes WEP krypteringsnøglerne.
WEP er baseret på RSA's rc4 stream cpiher og der anvendes en 24 bits initialiseringsvektor (iv). Denne sammenkædes med en 40-bits eller en 104 bits secret shared key for at danne en 64-bits eller 128-bits nøgle der så bruges til at kryptere resten med. Den komplette krypteringsmetode og den måde den anvendes på hver enkelt pakke indeholder en række svagheder der gør at WEP krypteringen kan brydes relativt enkelt hvis trafikmængden er stor nok således vil AirSnort med sikkerhed kunne gætte nøglen efter opsamling af 5-10 millioner datapakker og ofte skal der bare 20.000 stk. Til før det kan gøres.
AirSnort kører med et grafisk interface, hvorfor det er vanskeligt at beskrive yderligere her, men det er relativt enkelt at anvende, når man først har fået det til at køre. Et tip er at kontrollere at det trådløse netkort man har er supporteret af AirSnort inden man starter med at installerer, dette lille åbenlyse tip, kunne have sparet mig for mindst 3 timers arbejde.

WEPCrack.
http://sourceforge.net/projects/wepcrack
WEPCrack er et linux baseret værktøj der, lige som AirSnort bruges til at cracke WEP krypterede nøgler på trådløse 802.11b netværk.

Arpwatch.

Arpwatch er ikke et værktøj der kun kan/bør anvendes I forbindelse med trådløse netværk. Faktisk bør arpwatch anvendes på alle netværk hvor sikkerheden har prioritet. ARP (Address resolution Protocol) håndtere navneopløsning mellem MAC adresser op IP numre, og ligger således under TIP/IP laget i OSI modellen.
Denne navneopløsning sker på alle TPC/IP netværk og derfor er arpwatch relevant på alle TCP/IP netværk, men da trådløse netværk dels giver mulighed for "tilslutning" til netværket overalt hvor nettet kan opfanges og dels ofte filtrere netop på MAC adresser er arpwatch ekstra relevant i et trådløst net.

Arpwatch monitere Ethernet aktivitet og opbygger en database over MAC adressernes tilhørsforhold til IP adresser. Arpwatch alarmere/meddeler via e-mail når IP adresser tildeles via DHCP eller når IP adresser der er statisk tildelt til en computer skifter MAC adresse. Dette betyder at der alarmeres hvis nye maskiner tilkobler sig til vores net, eller hvis "gamle" maskiner ændrer deres IP opsætning.

Arpwatch er et typisk linux kommandolinie værktøj, der startes ved at skrive arpwatch med forskellige switches i kommando linien

Et bogon prefix er en IP adresse der ikke burde kunne forekomme I en Internet routing table. En IP pakke der routes over Internettet (ikke inklusive VPN eller andre tunneler), altså kommer udefra, burde aldrig have en IP adresse der hører til på et internt net (10.0.0.0, 192,168,0,0 eller 172.16.0.0) eller en adresse der ikke er officielt tildelt, se http://www.iana.org/assignments/ipv4-address-space.
Begrebet bogon hører snævert sammen med begreberne ingress og egress filtering, der dækker henholdsvis inbount og outbount filtrering af bogons.
Undersøgelser viser at omkring 60 % af alt det skidt der kommer udefra Internettet, falder inden for begrebet bogons

-a Som standard rapportere arpwatch bogons (undtagen når -N sættes) for IP addresser der ligger i det samme subnet som den første IP adresse på default interfacet. Hvis -a sættes rapportere arpwach alle bogon adresser.
-d flaget enabler debugging. Flaget forhindre at arpwatch afvikles i baggrunden og at rapporter sendes som e-mail. Rapporter sendes i stedet til stderr.
-f flaget bruges til at navngive ethernet/ip adresse databasen. Standard navnet er arp.dat og standard placeringen for daemonen er /var/lib/arpwatch/arp.dat.
-i flaget bruges til at override standard interfacet.
-m optionen specificere hvilken e-mail adresse rapporterne skal sendes til. Som standard sendes til root.
-n flaget specificere yderligere lokale netværk. Dette er meget brugbart når du har mere end et subnet netværk kørende og ikke ønsker bogon advarsler for den trafik der kører her.
-N flaget disabler bogon rapporter.
-p flaget disabler promiscuous operation.
-r flaget bruges til at specificere savefile
-s flaget bruges til at specefisere stein til SendMail. Ethvert program (husk at vi kører linux) der kan bruge -odi og kan hente tekst fra stdin kan bruges I stedet for SendMail.
-u flaget medfører at arpwatch dropper root privileges og ændre user ID til username samt group ID til den primære gruppe for username. Dette er en sikkerhedsmæssig fordel.
Du er nødt til at lave en tom arp.dat fil før du starter arpwach den første gang. Du skal også huske af den bruger arpwatch kører under (root eller andet hvis du bruger -u) skal have skriverettigheder til det bibliotek hvor arp.dat ligger.
Med en fornuftig IP opsætning i dit trådløse netværk, med en grundig undersøgelse af dit nets udbredelsesområde med Net Stumbler, med kismet og med arpwatch installeret og konfigureret ordentligt og med de fysiske forhold omkring dit net som beskrevet i min artikel "Trådløs sikkerhed - hvad bør jeg tænke på (http://www.eksperten.dk/artikler/117)" er du rimeligt godt kørende og jeg kan ikke forestille mig den hacker, der ikke hellere vælger et andet trådløst net at angribe.

Det var så Del 4. om der kommer en Del 5 ved jeg ikke endnu, har du forslag er du meget velkommen til at maile dem til mig.

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

Kan man få det points tilbage man har betalt for at se artiklen?

Kommentar af fastwrite d. 10. Oct 2004 | 2

Fin artikel - måske du skulle have skrevet at det hovedsageligt er linux værktøjer, men godt formuleret, og som kurtspurt skriver, en helhjertet skriveindsats.

Kommentar af mjense173 d. 19. Sep 2006 | 3

Kommentar af medions d. 04. Oct 2004 | 4

Ginial artikel! Virklig godt læsestor.

Kommentar af zhristian d. 03. Oct 2004 | 5

Dejlig artikel :) Beskriver programmerne hurtigt og godt.

Kommentar af kesh d. 08. Oct 2004 | 6

Godt gået...:-)

Kommentar af kurtspurt d. 09. Oct 2004 | 7

Tak for god og heljertet skriveinsats

Kommentar af human d. 04. Oct 2004 | 8

Rigtig fin artikel må jeg sige. Keep it up!

Kommentar af xodeus d. 07. Oct 2004 | 9

Fed artikel

Kommentar af thorjakobsen d. 08. Oct 2004 | 10

En hel anden ting jeg syntes at han glemmer at fortælle, er at trådløse netværk ikke er sikre, heller ikke hvis du smider et mac filter på, det er meget nemt at omgå

Kommentar af barbarbo d. 05. Oct 2004 | 11

Rigtig fed artikle, jem må nu installere linux og til at lege

Kommentar af xyborx d. 23. Dec 2004 | 12

Mangler lidt en rød tråd, som om den er skrevet fordi nogle andre ønskede det. Men der er da en del relevant information. Som fastwrite siger vil det nok være en god ide at nævne i beskrivelsen, at det hovedsageligt er linux værktøjer der bliver beskrevet.

Kommentar af frewald d. 28. Jul 2005 | 13

Endnu en god artikel i serien. Savner lidt mere windows-software der kan lidt af det som linux værtøjerne kan.
BTW: Network Stumbler fungerer fint på min Win XP

Kommentar af htmlkongen d. 05. Oct 2004 | 14

Der udvidede du min viden en del :) /Htmlkongen

Kommentar af jesper_bn d. 08. Oct 2004 | 15

Fin artikel til mig der lige har fået en bærbar(så ved jeg hvad jeg skal lave i min ferie(Joke)God og spændende

Kommentar af eneq d. 06. Oct 2004 | 16

Super, dog med mange gamle fakta
...men det er rigtigt godt, god beskrivelse af progammer og den tekniske side..

Kommentar af draco999 d. 24. Feb 2005 | 17

Som altid syntes jeg det er en god og spænnende artikel som _Bufferzone skriver

Kommentar af chodeof72 d. 01. Mar 2005 | 18

mangler windows værktøjer.
for Network Stumbler vil ikke virke på windows

Kommentar af evilhoppemis d. 04. Oct 2004 | 19

Det var en rigtig god artikel. Jeg er selv indehaver af et trådløst netværk har jeg har da fået nogle gode fif til hvordan jeg skal sikre mit netværk. Tak.

Kommentar af muvo d. 18. Apr 2005 | 20

Den er sku da god.. er der kommet en femmer?

Kommentar af safebutsorry d. 19. Oct 2004 | 21

Kommentar af wiccaone d. 09. Oct 2004 | 22

Kommentar af weblib d. 15. Oct 2004 | 23

Kommentar af thomaxz d. 14. Dec 2004 | 24

-/-*2--------

Kommentar af phil-profil d. 15. May 2006 | 25

Kommentar af team-temp d. 10. Oct 2006 | 26

Skide go' du får en stort 5 tal :)