Denne guide er oprindeligt
udgivet på Eksperten.dk

COMPUTERWORLD

The Hacking Dojo 3 - Sådan hacker du - Sniff bare, det lugter ikke

Vi skal nu i gang med at arbejde med noget af det der lugter ganske lidt af hacking og vi er kun begyndt at kradse i overfladen. Dette er nok den vigtigste artikel i serien, mis den og du vil ikke kunne følge med senere på passende niveau

Skrevet den **13. Nov 2010** af **bufferzone** I kategorien **Sikkerhed / Generelt** | ★★★☆☆

At starte med snifferen er egentlig ganske naturligt når man tænker over det, der er masser af gode grunde til det og dem vil jeg så komme ind på her. Denne lektion er nok den vigtigste du kommer ud for og det er væsentligt at du formår at uddrage alt det du kan af lektionen.

Den første og i denne sammenhæng vigtigste grund til at du skal i gang med en sniffer er at den giver dig mulighed for at opnå den nødvendige protokol og netværks kommunikations forståelse. En sniffer giver dig dels mulighed for at kikke ned i den enkelte data pakke og se hvad den indeholder og hvordan den er opbygget og så giver den dig mulighed for at se sammenhængen og samspillet mellem de enkelte pakker i en kommunikation.

Den anden grund er at du senere skal bruge snifferen til at forstå hvordan andre værktøjer og teknikker virker og arbejder. Uden snifferen vil du ikke kunne gennemskue portscannere, pakke crafters, sårbarheds scannere og andre aktive værktøjer.

Den tredje grund er at du skal kunne bruge snifferen som værktøj til at hacke med. En sniffer er et passivt værktøj, der ikke sætter nogen mærker og spor. Et mål kan ikke mærke at der bliver sniffet, hvorfor det er en relativ sikker teknik, lidt afhængig af hvordan du gør.

Snifferen.

Vi bruger TCPDump i disse lektioner og det er der, som med alt andet jeg vælger, en god grund til. Der findes masser af andre gode sniffere som f.eks. Wireshark, der tidligere hed ethereal og f.eks. Windows Server versioner har indbygget værktøjer der kan sniffe.

Der er to primære grunde til at vi anvender TCPDump, dels er den fuldstændig rå. Den gør kun det den får besked på og lægger ingen intelligens eller præsentation oven på pakkerne, vi ser dem som de er og det har vi brug for i denne sammenhæng hvor vi arbejder med forståelse for hvad der sker. Den anden grund er at der er tale om en kommandolinie sniffer der startes og konfigureres med kommandoer og det er ofte eneste mulighed når vi hacker. Du vil senere komme til at arbejde med Wireshark, da den også giver nogle fordele til specifikke opgaver, det vil vi vende tilbage til.

Lab opsætning.

Det er klart at jeg selvfølgelig forventer at du på nuværende tidspunkt har et opsat lab med et bund OS og et antal virtuelle maskiner klar og at du nu kan arbejde forholdsvis smertefrit med en Linux, så du kan sniffe fra denne med TCPDump. Skulle du ikke være helt klar er det dog ikke nødvendigt at ligge artiklen til side, du kan faktisk starte nu, dels fordi du kun har brug for en Linux maskine og dels fordi (og her sænker vi lige stemmen og taler sagte så alle ikke høre det) så kan du faktisk bruge en Windows maskine til denne øvelse med programmet WINDump der er en TCPDump til Windows. Og selvom du er klar med Linux bø'r du også prøve WINDump da du jo kan bruge den nå vi skal til at hacke Windows bokse.

Øvelser:

1. Igen starter vi med google. Læs alt hvad du kan finde om snifning, TCPDump (især TCPDump man page, prøv også at skrive kommandoen man tcpdump på din Linux box), WINDump.

2. Vi skal nu i geng med at kigge på TCP/IP protokol suiten. Snif et TCP tree way handshake, Snif en IP pakke, en TCP pakke, en UDP pakke og en ICMP pakke. Brug google igen og find oversigts skemaer over hvad de enkelte pakker indeholder og hvordan de ser ud. Brug -x switchen til at sniffe header informationer og sammenlign det du sniffer med skemaerne og sørg for at du kan uddrage de forskellige informationer der er til rådighed i headerne.

3. Snif en Windows ping pakke hvor du sætter en -l 4000 på. Sørg for at du identificerer pakkefragmenteringen og læser de enkelte offsets. Prøv at installerer forskellige personlige firewalls, (zonealarm, sygate og XP's indbyggede) og se hvordan de håndterer fragmentering og hvis du er heldig og en af dem ikke kan det, så forklar hvad der er galt. (jeg har en gammel version af sygate der ikke kan håndterer fragmenterede pakker, så mail mig hvis du ikke kan finde en)

4. Læs om Teardrop og Ping of Death og se om du på nettet kan finde værktøjer der kan lave disse angreb og snif så resultatet (kræver at du sniffer fra en anden maskine end du angriber, for den går måske død. Kig f.eks. på pakkecrafteren Netwox)

5. Vi skal nu lidt op i OSI modellen og kigge lidt på de elementer der findes i TCP/IP suiten. Snif en FTP session og se at du faktisk kan læse både password og brugernavn i klart sprog, Snif hentning og sending af mail med SMTP og POP3, hvor du også kan se både brugernavne og passwords. Snif SSL, SSH og IPSec forbindelser og se at data faktisk er krypteret. Snif et HTTP get request og se hvad sådan en indeholder, prøv at lave dit eget skema over hvad pakken indeholder.

6. Igen afslutter vi med google for de ovennævnte opgaver skal betragtes som et absolut minimum. Mens du sniffer vil du forhåbentlig undre dig over andre pakker du fanger. Hvad er f.eks. arp, hvorfor ser du trafik på port 53 osv. osv. alt hvad du ser bør du undre dig over, du bør lede efter små bider du ikke forstår og så borde dig ned der. Prøv selv at finde på andre interessante ting at sniffe, prøv at sniffe til en fil over tid og så efterfølgende sniffe ned i filen for at se om der er sket noget interessant. Søg på nettet og se om du ikke kan finde nogle capture filer til TCPDump som du kan undersøge. Disse filer findes der ude.

Hints

Kig særligt på -n, -v og -x og se hvad de giver dig.

Husk også at snifning opbygges langsomt et skridt af gangen, forstået sådan, at det er sjældent at du første gang kan sniffe dig frem til det resultat du søger. Snif og se hvad du fanger og gør så din snifning mere specifik eller snif og find det kendte, sorter derefter det fra og se hvad du ender med.

Skriv til mig hvis du har spørgsmål på kim@bufferzone.dk

Kommentar af denjoer d. 07. Nov 2008 | 1

Kommentar af enza d. 24. Nov 2008 | 2

må indrømme, jeg kan ikke se hvad man skal bruge sniffing til udover at holde øje med sin egen computer :S du kan jo ikke sniffe fks google.dk, for at se alt trafik google laver ud

Kommentar af Alcz d. 10. Apr 2013 | 3

Fed fed feeee artikel, den vil jeg læse lidt på engang imellem ;)