Workshop i nettverkssniffing

Martin Vonheim Larsen og Ståle Zerener Haugnæss

28. august 2014

Generell informasjon

Oppgavene skal løses på nettverket `BlackBox` som bruker `wpa2`-kryptering med passord `2co0l4sch00l`. Ved å gå inn på dette nettverket godtar du at andre ev. lytter på trafikken sendt til og fra din datamaskin. Det er med andre ord en god idé å stenge ned Facebook, Altinn, mailklient etc.

Målet med hver oppgave er å få navnet ditt på scoreboardlisten, som du finner på `http://scoreboard.no`. Alle oppgavene (unntatt oppgave 3a og 3b) baserer seg på at du skal komme fram til en kode, som du bruker for å registrere navnet ditt på `http://scoreboard.no`. Navnet ditt kommer da automatisk opp på tavlen.

Oppgave 1: Basic ARP-spoofing

Du har nettopp kjøpt ny PC, og etter å ha lagt inn Linux skal du teste at den mest elementære funksjonaliteten er på plass; nemlig at du klarer å ARP-spoofe andre datamaskiner på nettverket. Du har satt opp den gamle PCen din - `mean_machine` - til å kontinuerlig sende pakker til ruteren. Målet er å ARP-spoofe denne, slik at du mottar pakkene som blir forsøkt sendt til ruteren.

Pakkene som sendes til ruteren inneholder et sitat fra en film, som du skal registrere sammen med navnet ditt på `http://scoreboard.no`, ved hjelp av en vanlig nettleser.

	IP	MAC
ruter	10.0.1.1	D8:30:62:48:AF:50
mean_machine	10.0.1.3	08:00:27:FC:89:86

mean_machine sender pakker til ruteren. Disse inneholder en kode som du skal registrere på scoreboard.

Du vil få bruk for programmet `arp_reply` som du kan laste ned via `http://software.no`. Dersom du kjører Ubuntu eller Mac OS anbefales du å bruke hhv. `arp_reply_ubuntu` eller `arp_reply_osx`. Hvis ingen av disse programmene fungerer kan du kompilere din egen versjon fra `arp_reply.c` (se mer info i `README`). Spør om hjelp hvis det er noe du ikke får til!

Eksempel på bruk av `arp_reply`:

```
sudo ./arp_reply <device> <IP_A> <MAC_A> <IP_B> <MAC_B>
```

Dette vil sende en ARP-pakke til maskinen som har IP-adresse `IP_B` og MAC-adresse `MAC_B` med følgende innhold:

```
arp reply <IP_A> is-at <MAC_A>
```

Du vil også trenge et program som viser trafikken du mottar. Gode alternativer er Wireshark (GUI) eller `tcpdump` (i terminalen). Hvis du ikke har noen av disse programmene installert må du gå på `uio`-nettet og laste ned en av dem.

Eksempel på bruk av `tcpdump`:

```
sudo tcpdump -A -i <device> ip src 10.0.1.3
```

Dette vil skrive ut all mottatt trafikk fra `10.0.1.3` i terminalen.

Du finner typisk `<device>` og din egen MAC-adresse (som vanligvis skal brukes som `MAC_A`) med kommandoen `ifconfig`.

Oppgave 2: Sniffing

I disse oppgavene er du avhengig av at videresending (IP-forwarding) fungerer på PCen din.

På Ubuntu kan du aktivere IP-forwarding slik:

```
sudo sysctl -w net.ipv4.ip_forward=1
```

På Mac OS krever det litt mer innsats første gang. Først må du redigere filen `/Library/Preferences/SystemConfiguration/com.apple.Boot.plist`:

```
sudo nano /Library/Preferences/SystemConfiguration/com.apple.Boot.↩
    plist
```

Endre filen til følgende:

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN" "http://www.↩
    apple.com/DTDs/PropertyList-1.0.dtd">
<plist version="1.0">
<dict>
    <key>Kernel Flags</key>
    <string>net.inet.ip.scopedroute=0</string>
</dict>
</plist>
```

Lagre med `CTRL-x` etterfulgt av `y` og `ENTER`. Når dette er gjort må du restarte maskinen. Når maskinen har startet igjen kan IP-forwarding aktiveres med følgende to kommandoer.

```
sudo sysctl -w net.inet.ip.forwarding=1
sudo sysctl -w net.inet.ip.fw.enable=1
```

IP-forwarding deaktiveres når du restarter PCen, så det eneste du trenger å gjøre for å resette dette etter workshopen er å restarte.

Oppgave 2a: FTP-innlogging

Alice er hovedgruppelærer i EST1000 - Introduksjon til estetikk, og skal se over en eksamen som foreleser Bob har laget. Bob har lagt ut eksamenssettet på en FTP-server, og Alice har fått brukernavn og passord til serveren. Du er meldt opp i kurset pga. et tapt veddemål, men er ikke særlig interessert i å gjøre en innsats i faget. Alice er hipster, så hun sitter på en kafé og jobber. Men Alice driter seg ut, for hun bruker et åpent nettverk, og der sitter du også.

Din oppgave er å sniffe trafikken til Alice når hun logger seg på FTP-serveren, slik at du kan fange opp brukernavn og passord. Til dette trenger du, som i stad, programmet `arp_reply`. For at FTP-tilkoblingen ikke skal bli brutt, slik at Alice blir mistenksom, må du i tillegg videresende trafikken. Dette gjør du ved å aktivere IP-forwarding (se over).

Når du har sniffet brukernavn og passord må du logge deg på FTP-serveren (f.eks. med kommandoen `ftp 10.0.1.2`). Så finner du fram til eksamenssettet, og registrerer filnavnet (**MED** filendelse) på scoreboard.

	IP	MAC
FTP-server	10.0.1.2	08:00:27:3E:D2:3F
Alice	10.0.1.4	08:00:27:C0:06:E1

Alice logger seg stadig på FTP-serveren. Din oppgave er å sniffe brukernavn og passord. Bruk disse til å logge på FTP-serveren, finn eksamenssettet og bruk filnavnet til dette settet (med filendelse) som kode til scoreboard.

Oppgave 2b: Mail-utveksling

Du møter foreleser i EST1000 i heisen, og slår av en prat om dine medstudenter. Samtalen glir raskt over på Kassandra, en av de mindre lovende som tar kurset. Etter et par geniale spydigheter fra din side om de faglige prestasjonene til Kassandra, sier den litt naive professoren at han 'kan vedde på' at hun i hvertfall møter på eksamen. Som ung entreprenør aner du her en mulighet til å tjene raske penger.

Du bestemmer deg for å finne ut om du bør slå til på tilbudet om veddemål med foreleser, ved å overvåke mailtrafikken mellom Kassandra og studieadmin. Som alle andre estetikkstudenter, har også Kassandra sitert et dikt hun liker i mailsignaturen sin. Koden til scoreboard består av den første bokstaven i hvert ord i sitatet til Kassandra.

Kassandra sitter på sin maskin som er tilkoblet mailserveren, og kontinuerlig laster opp mailen du er interessert i. Du vil derfor sniffe på trafikken fra Kassandra til mailserveren. For at dette skal fungere må du i tillegg videresende trafikken.

	IP	MAC
mailserver	10.0.1.2	08:00:27:3E:D2:3F
Kassandra	10.0.1.5	08:00:27:BA:4C:80

Kassandra logger seg stadig på mailserveren. Din oppgave er å sniffe mailen hun sender til mailserveren. Denne mailen inneholder et dikt, og koden til scoreboard består av første bokstav i hvert ord i dette diktet (alt i lowercase).

Oppgave 2c: Webtrafikk

Du sliter med en kamerat som liker å kalle seg for Hunter, og som til stadighet misligholder penger han skylder deg fra et veddemål. Han lover stadig at du

skal få pengene, men etter dager med utsettelser har du nå sett deg lei, og bestemmer deg for å inndrive pengene selv. For å få til det er du avhengig av å vite hvilken bank han bruker, så du setter av en ledig fredagskveld til å stikke bortom huset hans for å sniffe litt på nettverket hans.

Du vet at Hunter surfer rundt på litt forskjellige nettsider, men du er altså interessert i å finne ut hvilken bank han bruker. Dette betyr at du vil lytte på trafikken som sendes fra Hunters PC til ruteren, for å se hvilke nettsider han besøker. For at han ikke skal oppdage at noe er galt må du også passe på å videresende trafikken hans.

	IP	MAC
ruter	10.0.1.2	08:00:27:3E:D2:3F
Hunter	10.0.1.6	08:00:27:0E:DB:B8

Hunter surfer rundt på en rekke nettsider. Én av disse er nettsiden til en vanlig norsk bank. Koden til scoreboard er webadressen til denne banken (uten 'www')

Oppgave 3: Manipulering av data

Denne oppgaven er en nøtt for viderekomne, spør om hjelp hvis det er noe du ikke skjønner!

Alice (en annen Alice) er daglig leder på arbeidsplassen din, og skal utbetale en bonus til månedens beste ansatt. Du har innsett at du ikke er typen til å bli månedens ansatt, men har kommet frem til at du likevel kunn tenkt deg bonusen. Du vet at Alice hver måned sender en datapakke til økonomiansvarlig, Bob, med navnet på månedens ansatt, og har bestemt deg for å bruke dine leet-skills til å manipulere pakken fra Alice slik at du får månedens bonusutbetaling.

Etter å ha overvåket trafikken mellom Alice og Bob i noen måneder, har du kommet frem til at pakken er på følgende format:

- et tilsynelatende tilfeldig tall med åtte siffer
- kolon
- navn på månedens ansatt

Din oppgave er å lage en løsning som manipulerer pakken slik at navnet til månedens ansatt byttes ut med ditt.

Oppgave 3a: Manipulering av UDP-pakker

I denne deloppgaven sendes oppgavene fra Alice som UDP-pakker.

	IP	MAC
Bob	10.0.1.2	08:00:27:3E:D2:3F
Alice	10.0.1.7	08:00:27:2C:86:5B

Alice sender UDP-pakker (port 1234) som inneholder en (tilsynelatende) tilfeldig nøkkel, og navnet på månedens ansatt. Du må sørge for å få trafikken til din maskin, bytte ut navnet med ditt eget, og sende pakken videre til Bob. Du blir da automatisk registrert i scoreboard.

Oppgave 3b: Manipulering av TCP-pakker

I denne deloppgaven sendes oppgavene fra Alice som TCP-pakker (som gjør ting mer komplisert).

	IP	MAC
Bob	10.0.1.2	08:00:27:3E:D2:3F
Alice	10.0.1.8	08:00:27:F9:62:21

Alice sender TCP-pakker (port 6789) som inneholder en (tilsynelatende) tilfeldig nøkkel, og navnet på månedens ansatt. Du må sørge for å få trafikken til din maskin, manipulere pakken så den inneholder ditt navn og sende meldingen videre til Bob. Du blir da automatisk registrert i scoreboard.