Oblig 5 - Nettverkssikkerhet

IN2120 - Høst 2023

Introduksjon

I denne obligen skal vi se på nettverkssikkerhet, nettverksskanning, brannmurer og TLS-inspeksjon.

Nmap er et verktøy som blir brukt til å kartlegge datanettverk. Disse blir ofte kalt for *portscannere*. Det nmap gjør er å skanne IP-adresser og porter, og fortelle oss hvilke porter som er åpne og tjenester som er tilgjengelige på de ulike maskinene på nettverket.

Labmaskinen har tilgang til det lokale nettverket. I et reelt dataangrep vil det å få tilgang til en slik maskin på innsiden av nettverket være noe av det som er øverst på ønskelisten til en angriper. Fra en kompromittert maskin vil de kunne utforske resten av nettverket og lete etter sårbare tjenester.

Det anbefales sterkt å søke etter hjelp på internett dersom man står fast på denne obligen.

Oppgave 1

Vi har funnet ut at det kjører en viktig server på det lokale nettverket på ip-adressen 10.2.0.19. Åpne Cygwin, og scan ip-adressen med Nmap.

Denne serveren har noen åpne porter. Viss du legger sammen nummerene til disse portene, hva blir summen?

Oppgave 2

Nå skal vi prøve å kontakte tjenestene vi fant med nmap. **Hva er det tjenesten som kjører på den høyeste åpne porten sier til oss når vi kontakter den?**

Hint: Bruk netcat, slik som i oblig 4.

Oppgave 3

Prøv å komme deg inn på FTP-serveren, ved å bruke Internett Explorer på labmaskinen. Porten som FTP-serveren kjører på er standard-porten for FTP-trafikk. FTP er en protokoll for å overføre filer.

Hva er det hemmelige tallet som fins i en spennende fil?

Hint 1: I steden for å spesifisere for eksempel HTTP://, kan man velge andre protokoller i adressefeltet før adressen man vil besøke. Hint 2: Brukernavnet er "bruker", men på engelsk. Passordet til brukeren har fått et rykte som verdens mest brukte passord. Her må man prøve seg litt frem.

Oppgave 4

For å hindre at denne relativt sårbare FTP-serveren er eksponert mot internett vil nok nettverksadministratoren beskytte den med en brannmur. Mange brannmurer kjører Linux, og her er et vanlig brannmur-program **iptables**.

Iptables styres med kommandolinjer, som grovt sett er utformet på denne måten:

```
iptables (hva du vil) (med hvilken liste av regler) (hvilke pakker du vil ramme) (hva gjøre med dem)
```

Listene med regler kalles "chains" og i utgangspunktet har man tre av dem: **OUTPUT**, **INPUT** og **FORWARD**.

OUTPUT er utgående trafikk, INPUT er innkommende trafikk, og FORWARD er for trafikk som skal blir videresendt til en annen adresse, for eksempel en klient eller tjener bak en brannmur.

Hvilke pakker man vil fange opp kan man for eksempel spesifisere med "**-s**" (source, altså hvilken IP-adresse pakken har som avsender) eller "**-d**" (destination, altså hvilken IP-adresse pakken er adressert til).

Nettverksprotokoll kan spesifikseres med for eksempel **-p udp**. Spesifikke porter innenfor denne protokollen kan skrives rett etter med for eksempel

```
 --dport 53 og --sport 53
```

NB: Legg merke til dobbel strek.

Til slutt skriver man hva man vil gjøre med pakkene. En vanlig ting å gjøre med pakkene er å stanse dem, noe man kan gjøre med "**-j DROP**".

En mer fullstendig og nøyaktig liste med kommandoer kan man finne ved å lese iptables sin manual.

Dersom man vil blokkere all trafikk som går fra maskinen man er på til for eksempel *uio.no*, kan man gjøre det slik:

```
Enten med ip-adressen:
    iptables -A OUTPUT -d 129.240.118.130 -j DROP

Eller med domenenavnet:
    iptables -A OUTPUT -d uio.no -j DROP
```

I datanettverk er det vanlig å gi tilgang til internett gjennom en proxy-gateway. En slik gateway har sin egen ip-adresse, og fungerer ofte også som en brannmur for å sikre og regulere nettverkstrafikken mellom de interne tjenestene på nettverket og det eksterne internettet.

Anta at serveren på 10.2.0.19 er koblet til internett gjennom en proxy-brannmur på ip-adressen 10.1.1.99. Vi ønsker å skrive en brannmurregel med iptables-format som gjør at tilkoblingsforsøk og nettverkstrafikk mot FTP-tjenesten på 10.2.0.19 blir blokkert i brannmuren. Den skal altså passe på at slik trafikk ikke blir sendt videre fra proxyen til serveren.

Hvordan er iptables-regelen som hindrer nettverkstrafikk å bli videresendt fra proxy-brannmuren (og dermed fra internett) til FTP-tjenesten på 10.2.0.19?

Hint 1: Husk at i Linux er det forskjell mellom store og små bokstaver. Hint 2: Rekkefølgen på flaggene er viktig her. Hint 3: Tilkoblinger til en FTP-server gjøres med TCP. Hint 4: Les gjerne litt i manualen til iptables, og søk rundt på internett om du står fast.

Oppgave 5

I denne oppgaven antar vi at proxy-gatewayen driver med TLS-inspeksjon.

Det vil si at all trafikken som i utgangspunktet skal være kryptert mellom for eksempel en nettleser og internett-server, blir dekryptert og kan leses i klartekst der TLS-inspeksjonen finner sted. Dette er noe mange organisasjoner og bedrifter ønsker for å sikre seg mot skjult trafikk fra ondsinnede aktører som har fått fotfeste på innsiden av nettverket. For eksempel kan dette være kommandoer til skadevare installert, eller illegitim data-uthenting.

Hva kaller vi med et begrep aktøren som har generert sertifikatet *klientene* som surfer på internett fra innsiden av nettverket ser?