VAASAN AMMATTIKORKEAKOULU
VASA YRKESHÖGSKOLA
UNIVERSITY OF APPLIED SCIENCES

Jan Åkerholm

TIETOTURVATYÖN SUUNNITTELU

Tekniikka ja liikenne

2012

VAASAN AMMATTIKORKEAKOULU
Tietotekniikan koulutusohjelma

TIIVISTELMÄ

Tekijä	Jan Åkerholm
Opinnäytetyön nimi	Tietoturvatyön suunnittelu
Vuosi	2012
Kieli	suomi
Sivumäärä	45
Ohjaaja	Antti Virtanen

Tämän opinnäytetyön tarkoituksena on tietoturvaharjoitustyön suunnittelu Vaasan ammattikorkeakoululle. Työn tutkimuskohteena on tietoliikenteen tietoturva. Sitä tutkitaan tarkastelemalla Iptables-palomuurin käyttöä sekä analysoimalla verkkoskannerin, haavoittuvuuksien analysointityökalun ja tunkeutumisen havaitsemisjärjestelmän tuloksia.

Tietoturvan tutkimiseksi luodaan verkkoympäristö, joka koostuu sisäisestä, ulkoisesta ja DMZ-verkosta. Laitteisto koostuu kolmesta tietokoneesta ja kytkimestä. Työssä käytetään myös neljättä tietokonetta, johon on asennettu verkkoskanneriohjelma ja verkkoliikenteen analysointityökaluja. Työn suoritukseen vaaditut ohjelmat toteutetaan avoimen lähdekoodin ohjelmistoilla.

Tietoturvaharjoitustyön tavoitteina on opettaa Iptables-palomuuritekniikan käyttöä ja tutkia turvaamatonta verkkoympäristöä. Siinä konfiguroidaan palomuuri ja tutkitaan verkkoympäristöä avoimeen lähdekoodiin pohjautuvien ohjelmien avulla.

Avainsanat	tietoliikenteen tietoturva, Iptables-palomuuri, avoin lähdekoodi

VAASAN AMMATTIKORKEAKOULU
UNIVERSITY OF APPLIED SCIENCES
Information Technology

ABSTRACT

Author	Jan Åkerholm
Title	Planning of Data Security Exercise
Year	2012
Language	Finnish
Pages	45
Name of Supervisor	Antti Virtanen

The purpose of this thesis is to create a data security exercise for Vaasa University of Applied Sciences. The research topic of the thesis is data security in network traffic. It is studied by examining the use of Iptables firewall and by analysing results given by a network scanner, a vulnerability scanner and an intrusion detection system.

In order to study data security, the hardware using internal, external and DMZ networks is created and it consists of three computers and a switch. Also a fourth computer is used, and it has a network scanner program and network analysing tools installed. The programs and tools required to complete the work are based on open source.

The goals of the data security exercise are to teach the use of Iptables firewall technique and to examine unsecured network environment. In the exercise, a firewall is created and network environment is examined with the help of open source programs and tools.

Keywords data security, Iptables-Firewall, open source

SISÄLLYSLUETTELO

LIITELUETTELO

LYHENNELUETTELO

CUPS = Common Unix Printing System	Tulostusohjelmisto Unix-yhteensopiviin järjestelmiin
DHCP = Dynamic Host Configuration Protocol	IP-osoitteiden jako lähiverkon laitteille
DMZ = Demilitarized Zone	Ulkoisen verkon ja sisäisen verkon välissä oleva vyöhyke
DNS = Domain Name System	Nimipalvelujärjestelmä, joka muuntaa verkkotunnuksia IP-osoitteiksi
FTP = File Transfer Protocol	TCP-protokollaa käyttävä tiedonsiirtomenetelmä
ICMP = Internet Control Message Protocol	Tietokoneesta toiseen nopeasti lähetettävä TCP/IP-pinon kontrolliprotokollan viesti
IDS = Intrusion Detection System	Tunkeutumisen havaitsemisjärjestelmä
IP = Internet Protocol	TCP/IP-mallin internet-protokolla
LTS = Long Term Support	Pitkäaikainen päivitystuki ohjelmistoille
NAT = Network Address Translation	IP-osoitteenmuunnos
NIDS= Network Intrusion Detection System	Snort-ohjelman tunkeutujan havaitsemistila
SMTP = Simple Mail Transfer Protocol	Sähköpostipalvelu
SSH = Secure Shell	Salatun tietoliikenteen protokolla
TCP = Transmission Control Protocol	Tietokoneiden yhteyksien tietoliikenneprotokolla

VPN = Virtual Private Network	Julkisen verkon yli muodostettava näennäinen yksityinen verkko

1 JOHDANTO

Tämän opinnäytetyön toimeksiantajana on Vaasan ammattikorkeakoulu ja sen tarkoituksena on suunnitella ja toteuttaa tietoturvaharjoitustyö tietotekniikan opiskelijoille. Harjoitus perehdyttää opiskelijat Iptables-palomuurin toimintaperiaatteisiin, Linux-käyttöjärjestelmän hallintaan ja Opensource-ohjelmiin eli avoimeen lähdekoodiin pohjautuviin ohjelmiin.

Tietoturvaharjoitustyön suunnittelemiseksi tässä opinnäytetyössä tutkitaan tietoliikenteen tietoturvaa ja palomuurin merkitystä verkkoympäristön tietoturvallisuuden kannalta. Työn toiminnallisiin ominaisuuksiin kuuluvat Iptables-palomuurin konfiguroiminen, skannaus, haavoittuvuuksien analysointi ja tunkeutumisyritysten havaitsemisjärjestelmän luominen. Työssä konfiguroidaan Linux-pohjaista palomuuria Iptables-työkalulla ja luodaan turvallinen verkkoympäristö ulkoisen verkon, sisäisen verkon ja DMZ-verkon välille. Palomuurikoneena toimivaa tietokonetta skannataan Nmap-verkkoskannerilla ja selvitetään kaikki sen verkon sisältämät mahdolliset laitteet ja palvelut. Verkon haavoittuvuuksia analysoidaan Nessus-työkalulla ja selvitetään mitä palveluja laitteissa on päällä ja mitä varoituksia ohjelma niistä antaa. Palomuurina toimivalle tietokoneelle asennetaan Snort-niminen IDS-järjestelmä, jolla havaitaan tunkeutumisyritykset.

Tämän opinnäytetyön pohjalta toteutettu tietoturvaharjoitustyö koostuu esitehtävistä, kysymyksistä Iptables-palomuurin tekniikasta, Iptables-työkalun komentojen hallitsemisesta ja tietoliikenteen tietoturvan tutkimisesta.

2 TIETOTURVATEKNIIKKA TIETOLIIKENTEESSÄ

Tietoturva on laaja käsite. Yleisesti ottaen tietoturvan tarkoituksena on suojella tiedon luottamuksellisuutta, eheyttä ja käytettävyyttä. Suojeltava tieto voi sisältää esimerkiksi salaisia yksityisten ihmisten tai yritysten tietoja. Tällaisten tietojen halutaan pysyvän halutussa muodossaan eikä niihin tulisi päästä käsiksi luvattomasti. Tällaista tietoa säilytetään tietokannoissa, verkkopalvelimilla ja tietokoneilla. (Viestintävirasto 2012.)

Tietoturva voidaan toteuttaa joko teknisillä tai hallinnollisilla toimenpiteillä. Teknisiin toimenpiteisiin lukeutuvat palomuurit, virustentorjuntaohjelmat, salausmenetelmät ja tunkeutumisen havaitsemisjärjestelmät. Hallinnollisiin toimenpiteisiin lukeutuvat tietoturvan koulutus ja päivittäisten toimintatapojen ohjeistaminen. (Viestintävirasto 2012.)

Tässä työssä tietoturvaa käsitellään tietoliikenteen näkökulmasta. Tällöin tärkein osa tietoturvaa on palomuuri ja sen käyttö tiedon suojelemiseksi. Palomuuri voi olla ohjelmisto tai erillinen laitteisto, joka valvoo verkkoliikennettä. Sen toiminta perustuu siihen, että se analysoi verkkoliikennettä ja päästää läpi vain halutun liikenteen. (Viestintävirasto 2007.) Palomuurin avulla voidaan estää ulkopuoliset tunkeutujat, kun taas tietokonevirus- ja vakoiluohjelmaskannereiden avulla voidaan estää haittaohjelmien toimintaa. Tehokkain tietoturva saadaan aikaiseksi käyttämällä sekä palomuuria että tietokonevirus- ja vakoiluohjelmaskannereita. (Spamlaw 2012.)

3 OHJELMISTOT

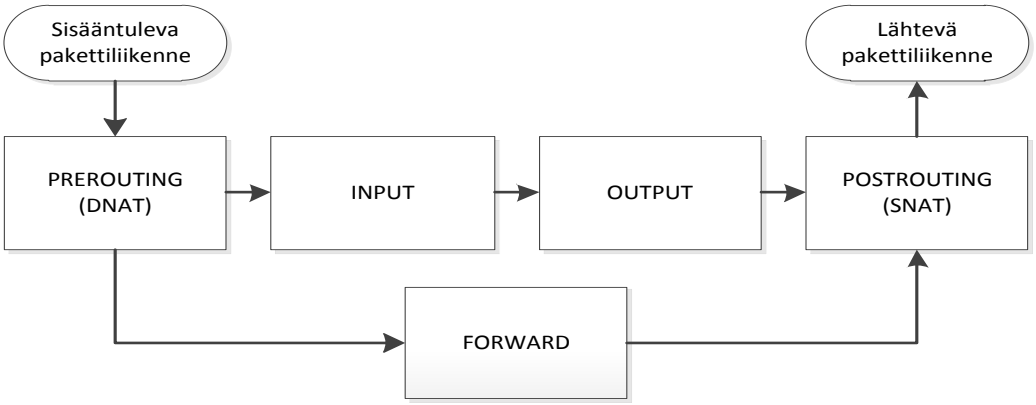
3.1 Iptables

Työssä käytetään Iptables-palomuuria suojaamaan verkkoympäristöä. Oletusarvoisesti Ubuntu-käyttöjärjestelmän Iptables-palomuuri on avoin kaikelle, mutta portit ovat suljettuja, jos mikään ohjelma ei käytä niitä.

Iptables-työkalun avulla käsitellään Netfilter-pakettisuodatinta. Iptablesin kaltainen palomuuri perustuu siihen, että tiettyjä paketteja joko päästetään sääntöketjuissa (**Kuva 1.)** läpi tai estetään. (Hakala & Vainio & Vuorinen 2006, 205-206.) Iptables-työkalun sääntöketjuja hallitaan lukuisilla komennoilla, parametreilla ja moduuleilla. (Hakala ym. 2006, 208-210.)

Paketit jaetaan viiteen eri luokkaan:

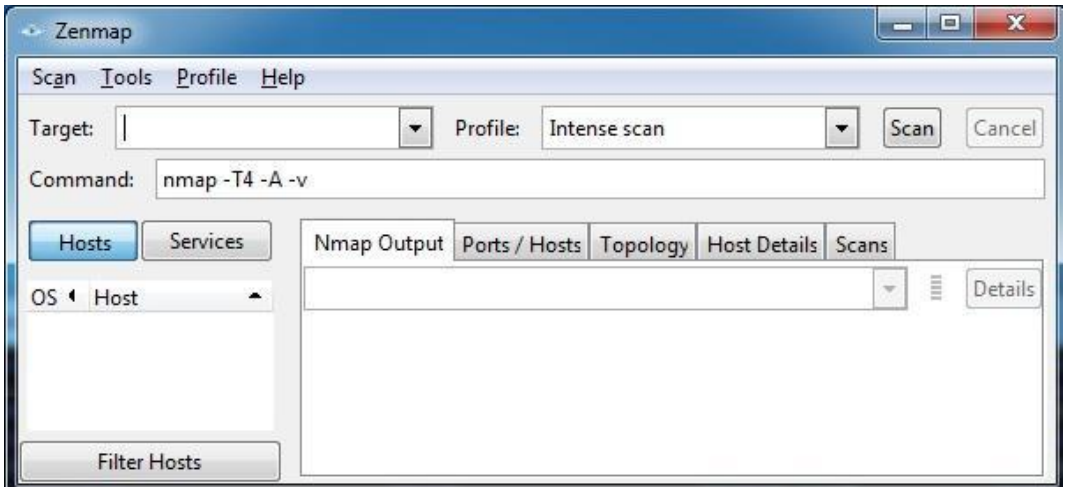
- INPUT = tietokoneelle saapuvan pakettiliikenteen sääntöketju
- FORWARD = tietokoneen kautta kulkeva pakettiliikenteen sääntöketju
- OUTPUT = tietokoneelta lähtevän pakettiliikenteen sääntöketju
- PREROUTING = tietokoneelle saapuvan pakettiliikenteen uudelleenohjaus
- POSTROUTING = tietokoneelta lähtevän pakettiliikenteen jälkikäsittely.



Kuva 1. Pakettiliikenteen kulku Iptablesin sääntöketjuissa

3.2 Nmap

Verkkoskanneriohjelmana tässä työssä käytetään Nmapia (**Kuva 2.**), jonka avulla voidaan arvioida tietokoneen tai verkkoympäristön turvallisuutta. IP-osoitteella pystytään selvittämään kohteesta esimerkiksi käyttöjärjestelmä, palvelut ja portit. Nmap hyökkää kohteeseensa skannaamalla tunnettuja portteja ja lähettämällä Ping-pyyntöjä. (Nmap.org 2012.)

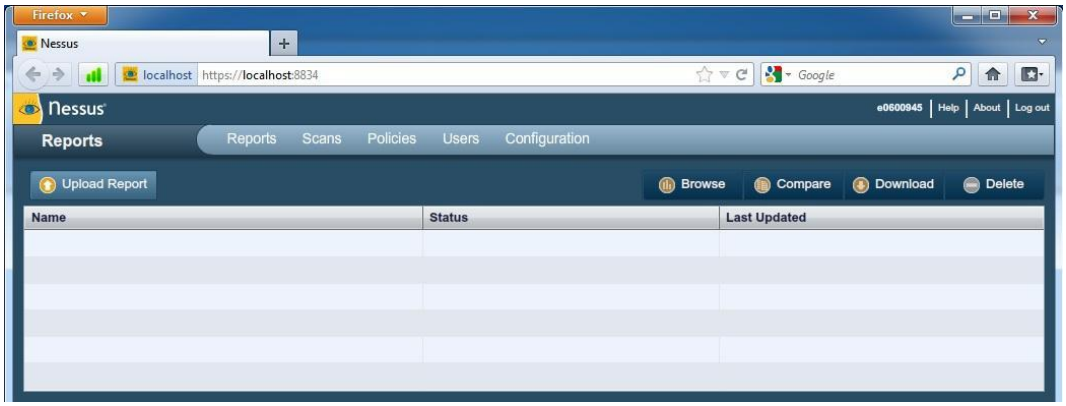


Kuva 2. Nmapin graafinen käyttöliittymä

3.3 Nessus

Haavoittuvuuksien analysointityökaluna tässä työssä käytetään Tenables Nessus-ohjelmaa (**Kuva 3.**), jolla voidaan suorittaa etäselauksia ja tarkastaa verkon infrastruktuuri. Nessus löytää verkkolaitteet ja tunnistaa käyttöjärjestelmät, sovellukset ja tietokannat sekä kaikki palvelut, jotka niissä toimivat. Nessus skannaa kaikki mahdolliset portit jokaisessa laitteessa ja ehdottaa verkon turvallisuutta parantavia keinoja tarpeen mukaan. Se tunnistaa myös vertaisverkot, vakooja- ja haittaohjelmat. (Tenable Network Security 2012.)

Raportit analysoiduista kohteista ovat muokattavissa ja niistä voidaan luoda tiettyyn osa-alueeseen keskittyviä selostuksia. Raportin tulokset voidaan rajata näyttämään esimerkiksi jotain tiettyä turvariskiä. (Tenable Network Security 2012.)



Kuva 3. Nessuksen selainpohjainen käyttöliittymä

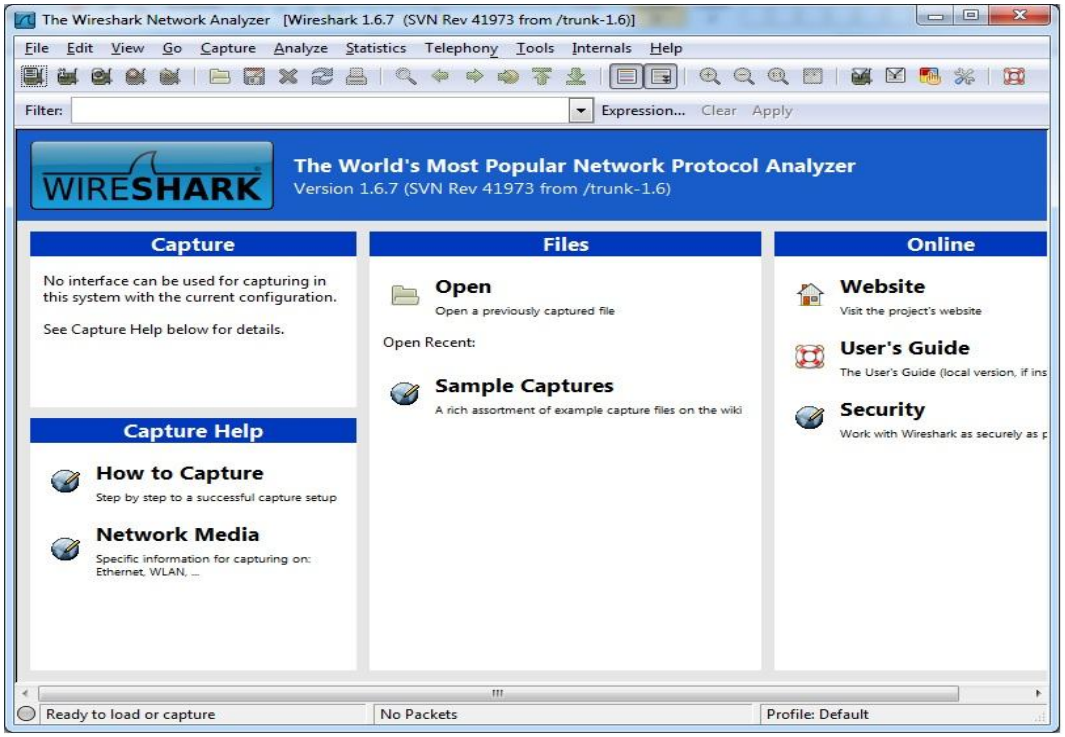
3.4 Snort

Tässä työssä käytetään Sourcefiren kehittämää Snortia. Se on verkon tunkeutumisyrityksien havaitsemisjärjestelmä, joka pohjautuu avoimeen lähdekoodiin. Järjestelmä kykenee reaaliaikaiseen pakettiliikenteen tietojen analysointiin ja tallentamiseen. Snortin tärkeimmät ominaisuudet ovat Network Intrusion Detection System Mode, Sniffer Mode ja Packet Logger Mode. Tämän työn kannalta tärkein

näistä on Network Intrusion Detection System Mode, jota käytetään erilaisten tunkeutumiskeinojen havaitsemiseen. (Sourcefire, Inc 2010.)

3.5 Wireshark

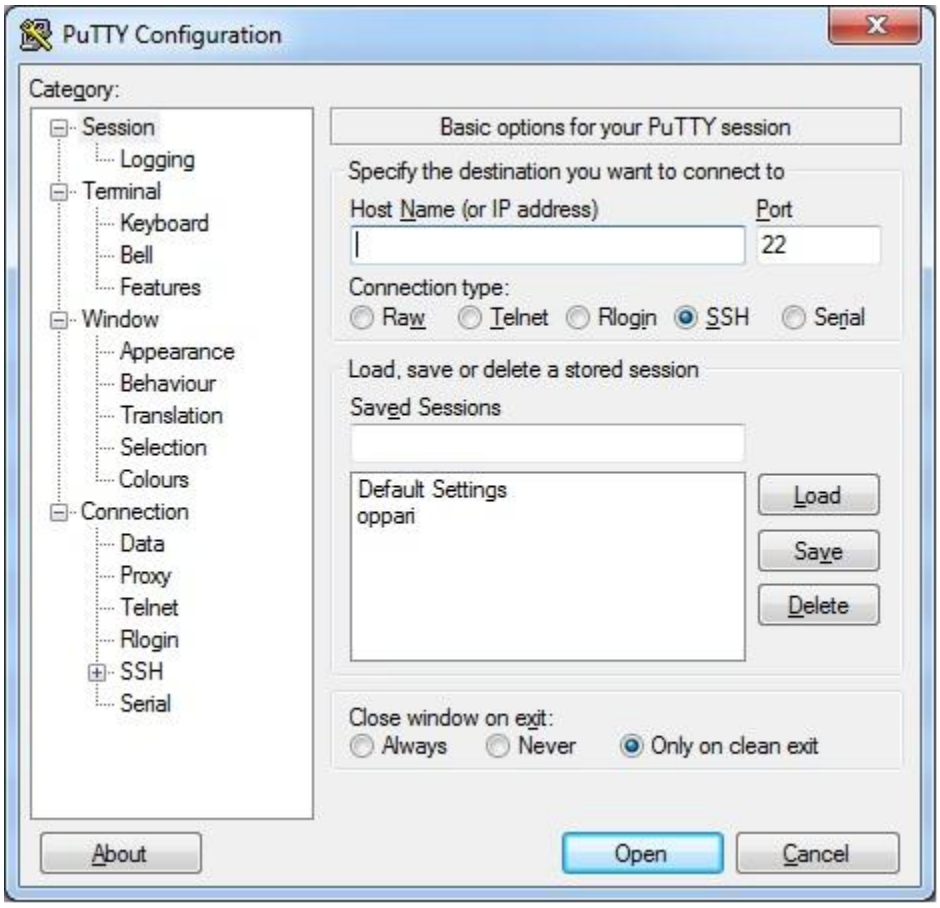
Verkkoliikenteen analysointiin tässä työssä käytetään avoimeen lähdekoodiin pohjautuvaa Wiresharkia (**Kuva 4.**). Sen avulla voidaan tutkia interaktiivisesti tietokoneen verkkoliikennettä. Wireshark toimii useilla käyttöjärjestelmillä, kuten Windows, OS X, Linux ja UNIX. (Wireshark 2006.)



Kuva 4. Wiresharkin käyttöliittymä

3.6 Putty

SSH-yhteyden muodostamista varten tässä työssä käytetään Putty-ohjelmaa (**Kuva 5.**). Se on tarkoitettu SSH-, Telnet- ja Rlogin-verkkoprotokollia varten ja niiden avulla muodostetaan etäyhteys toiseen tietokoneeseen. (PuTTY 2012.)

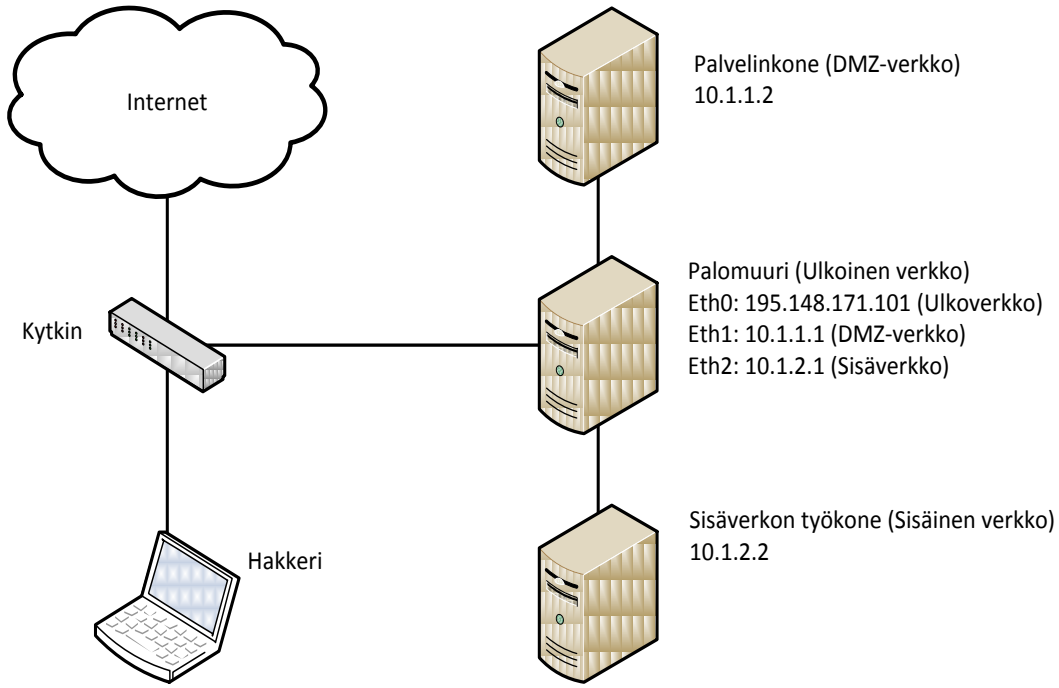


Kuva 5. Puttyn käyttöliittymä

4 VERKKOYMPÄRISTÖN SUUNNITTELU

4.1 Verkon rakenne

Työssä luodaan verkkoympäristö, joka koostuu sisäisestä verkosta, ulkoisesta verkosta ja DMZ-verkosta (**Kuva 6.**). Sisä- ja DMZ-verkon tietokoneet sekä palomuurina toimiva tietokone yhdistetään RJ-45 -verkkokaapelilla kytkimeen. Palomuurikoneen eth0-verkkokortti toimii ulkoisena verkkona, eth1-verkkortti DMZ-verkkona ja eth2-verkkortti taas sisäisenä verkkona.



Kuva 6. Verkon rakenne

4.2 Verkko-osoitteiden konfigurointi

Työssä käytetään julkista staattista IP-osoitetta 195.148.171.101, jota käytetään palomuurikoneen ulkoverkkona toimivalla eth0-verkkokortilla. Eth1- ja eth2-ver-

korteilla käytetään yksityisiä staattisia IP-osoitteita. Palomuurina toimivalle tietokoneelle, DMZ-verkon palvelin tietokoneelle ja sisäverkon tietokoneelle asetetaan /etc/resolv.conf-tiedostossa Google.fi:n nimipalvelimien osoitteet 8.8.8.8 ja 8.8.4.4 (**Kehys 1.**).

```
search google.com
nameserver 8.8.8.8
nameserver 8.8.4.4
```

Kehys 1. Google.fi:n nimipalvelut

4.2.1 Palomuurina toimiva tietokone

Palomuurina toimivalle tietokoneelle ja sen kolmelle verkkokortille luodaan jokaiselle oma verkko-osoite. IP-osoitteet ovat staattisia osoitteita. Muutokset ja lisäykset tehdään /etc/network/interfaces-tiedostoon (**Kehys 2.**). Tarvittavat lisämääritelmät ovat address, netmask, network, broadcast ja gateway. Viimeinen määritelmä eli gateway tulee lisätä vain ulkoverkkona toimivalle verkkokortille.

```
auto lo
iface lo inet loopback
auto eth0 #Ulkoverkkona toimiva eth0-verkkokortti
iface eth0 inet static #IP-osoitteen staattinen mene-
telmä asetettuna
address 195.148.171.101   #Julkinen staattinen IP-
osoite
netmask 255.255.255.192
network 195.148.171.0/26
broadcast 195.148.171.255
gateway 195.148.171.126 #Gateway-osoite vain ulkoverk-
kona toimivalle verkkokortille

auto eth1 #DMZ-verkkona toimiva eth1-verkkokortti
iface eth1 inet static   #IP-osoitteen staattinen mene-
telmä asetettuna
address 10.1.1.1 #Yksityinen staattinen IP-osoite
netmask 255.255.255.0
network 10.1.1.0/24
broadcast 10.1.1.255

auto eth2 #Sisäverkkona toimiva eth2-verkkokortti
iface eth2 inet static #IP-osoitteen staattinen mene-
telmä asetettuna
address 10.1.2.1 #Yksityinen staattinen IP-osoite
netmask 255.255.255.0
network 10.1.2.0/24
broadcast 10.1.2.255
```

Kehys 2. Palomuurina toimivan tietokoneen Interfaces-tiedosto

4.2.2 DMZ-verkon tietokone

Palvelinkoneena toimivalle tietokoneelle lisätään /etc/network/interfaces-tiedostoon IP-osoitteet, jotka kuuluvat samaan aliverkkoon palomuurikoneen eth1-verkkokortin kanssa (**Kehys 3.**).

```
auto lo
iface lo inet loopback
auto eth0
iface eth0 inet static   #IP-osoitteen staattinen mene-
telmä asetettuna
address 10.1.1.2 #Yksityinen staattinen IP-osoite
netmask 255.255.255.0
network 10.1.1.0/24
broadcast 10.1.1.255
gateway 10.1.1.1 #Gateway-osoitteena palomuurina toi-
mivan tietokoneen DMZ-verkon Eth1-verkkokortin IP-
osoite
```

Kehys 3. DMZ-verkon tietokoneen Interfaces-tiedosto

4.2.3 Sisäverkon tietokone

Sisäverkon työkoneena toimivalle tietokoneelle lisätään /etc/network/interfaces-tiedostoon IP-osoitteet, jotka kuuluvat samaan aliverkkoon palomuurikoneen eth2-verkkokortin kanssa (**Kehys 4.**).

```
auto lo
iface lo inet loopback
auto eth0
iface eth0 inet static   #IP-osoitteen staattinen mene-
telmä asetettuna
address 10.1.2.2 #Yksityinen staattinen IP-osoite
netmask 255.255.255.0
network 10.1.2.0/24
broadcast 10.1.2.255
gateway 10.1.2.1 #Gateway-osoitteena palomuurina toi-
mivan tietokoneen sisäverkon Eth2-verkkokortin IP-
osoite
```

Kehys 4. Sisäverkon tietokoneen Interfaces-tiedosto

4.3 Ipv4-pakettien uudelleenohjaus

Jotta ipv4-pakettien uudelleenohjaus palomuurikoneelta muualle verkkoympäristöön olisi mahdollista, tulee /etc/sysctl.conf-tiedostoon tehdä muutos. Sysctl.conf-tiedostossa olevan net.ipv4.ip_forward=0 -rivin arvo 0 muutetaan arvoksi 1 (**Kehys 5.**).

```
net.ipv4.ip_forward=1
```

Kehys 5. Ipv4-pakettien uudelleenohjaus

5 VERKKOLAITTEIDEN JA OHJELMISTOJEN TOTEUTUS

5.1 Laitteisto

Opinnäytetyössä käytetään neljää tietokonetta verkkoympäristön luomiseen. Kolme tietokoneista on pöytätietokonemallisia ja yksi on kannettava tietokone.

Jokaisen pöytäkoneen laitteisto sisältää

- Intelin Pentium 4 3.00GHz tuplaydinprosessorin
- 3,4 GB muistin
- 70 GB:n ST380819AS- kiintolevyn
- HL-DT-ST DVD+-RW GWA4164B -levyaseman
- Intelin 82945G/GZ -integroidun näytönohjaimen.

Kannettavana koneena käytetään Dell Precisionin M4400 -mallia, joka sisältää

- Intel:in P8400 2.26GHz tuplaydinprosessorin
- 4 GB muistin
- 186 GB:n ST9200423ASG -kiintolevyn
- TSST corp DVD +- RW TS-U633A -levyaseman
- Nvidian Quadro FX 770M –näytönohjaimen.

Tietokoneiden yhteydet toisiinsa ja ulkoiseen verkkoon varmistetaan SMC-EZ6508TX-mallisella 10/100 Mbps-kytkimellä. Verkkokaapeleina käytetään seitsemää suoraankytkettyä RJ-45 -kaapelia.

5.2 Käyttöjärjestelmät

Tässä työssä rakennettavan verkkoympäristön käyttöjärjestelminä ovat Ubuntu Desktop 10.04 LTS ja Ubuntu Server 10.04 LTS. Kannettavan tietokoneen käyttöjärjestelmänä on 32-bittinen Windows 7 Enterprise.

5.3 Ubuntu-käyttöjärjestelmän ohjelmat

Työssä asennetaan ohjelmat Ubuntu-käyttöjärjestelmän tietokoneille Synaptic Package Manager ja Advanced Packaging Tool -työkalujen avulla. Nämä Ubuntun työkalut hakevat ja asentavat tarvittavat ohjelmistopaketit oikeassa järjestyksessä. Ubuntu 10.04 LTS -käyttöjärjestelmän tietokoneilla on työssä käytettävä SSH-palvelin valmiiksi asennettuna, mutta Ubuntu Server 10.04.1 LTS -käyttöjärjestelmän tietokoneelle se asennetaan Advanced Packaging Toolin avulla.

Palomuurina toimivalle tietokoneelle asennetaan Synaptic Package Manager -työkalun avulla Snort, OpenVPN Server ja Vsftpd. Snort asennetaan Synaptic Package Managerin avulla, jolloin myös muut tarvittavat ohjelmistopaketit liitetään asennukseen mukaan. OpenVPN asentamiseen tarvittavia lisäohjelmistopaketteja ovat liblzo2-2, libpkcs11-helper1, openssl-blacklist ja openvpn-blacklist. Vsftpd-palvelimen asentamiseen tarvitaan vain vsftpd-ohjelmistopaketti.

DMZ-verkon tietokoneelle asennetaan Advanced Packaging Tool -työkalun avulla Apache2, Bind, OpenSSH ja Cups. Apache2-palvelimen asentamiseen tarvittavia lisäohjelmistopaketteja ovat apache2-mpm-worker, apache2-utils, apache2.2-bin, apache2.2-common, libapr1 libaprutil1, libaprutil1-dbd-sqlite3 ja libaprutil1-ldap. Bind-palvelimen asentamiseen tarvittava lisäohjelmistopaketti on bind9utils. OpenSSH-palvelimen asentamiseen tarvitaan openssh-server-lisäohjelmistopaketti.

CUPS-palvelimen asentamiseen tarvittavia lisäohjelmistopaketteja ovat cups-driver-gutenprint ja ghostscript-cups.

5.4 Windows-käyttöjärjestelmän ohjelmat

Windows-käyttöjärjestelmän tietokoneelle tarvittavat ohjelmat ladataan niiden kotisivuilta ja asennetaan Windowsin omien asennustyökalujen avulla. Palomuuria ja sen verkkoympäristöä tutkivalle kannettavalle tietokoneelle asennetaan Nmap, Nessus, Wireshark ja Putty. Verkkoympäristöä kartoittavana ohjelmana käytetään Nmap-nimistä Opensource-ohjelmaa. Tietoturvariskien analysoimiseen käytetään Nessus-nimistä Opensource-ohjelmaa. Pakettiliikennettä kaappaavana ohjelmana käytetään Wireshark-nimistä ohjelmaa. SSH-yhteyden luomiseen käytetään Windows-pohjaiselle käyttöjärjestelmälle tarkoitettua Putty-ohjelmaa.

Nmap 5.51-version asennustiedosto ladataan osoitteesta http://nmap.org/download.html. Ladattu tiedosto puretaan ja asennetaan tietokoneelle Windowsin asennustyökalujen avulla. Nmap asennetaan Dell Precisionin M4400 -tietokoneelle, jotta palomuuria ja verkkoympäristöä voidaan skannata ulkoverkosta.

Nessus 5.0 ladataan osoitteesta http://downloads.nessus.org. Installshield Wizard -asennustyökalu purkaa ja asentaa ladatun Windows Installer Package -tiedoston tietokoneelle. Nessus 5.0 käyttöä varten tarvitaan rekisteröintiavain, jonka voi tilata Tenablen kotisivuilta sähköpostiin. Rekisteröintiavaimia on maksulliseen yrityskäyttöön ja ilmaiseen kotikäyttöön. Nessus asennetaan Dell Precisionin M4400 -tietokoneelle, jotta palomuurin ja verkkoympäristön tietoturvallisuutta voidaan tutkia.

Wireshark ladataan osoitteesta http:// www.wireshark.org/download.html. Ladattu tiedosto puretaan ja asennetaan Wiresharkin tietokoneelle. Wireshark asennetaan Dell Precisionin M4400 -tietokoneelle, jotta palomuurina toimivalta tietokoneelta tulevaa pakettiliikennettä voidaan kaapata ja tutkia.

Putty ladataan osoitteesta http:// www.chiark.greenend.org.uk/ ~sgtatham/ putty/ download.html. Ladattu tiedosto on client-pohjainen sovellus, jota ei erikseen tarvitse purkaa ja asentaa tietokoneelle. Putty ladataan Dell Precisionin M4400 -tietokoneelle, jotta palomuurikoneena toimivaan tietokoneeseen voidaan ottaa SSH-yhteys ulkoverkosta.

5.5 Iptables-määritelmät

Tässä kappaleessa käsitellään tietoturvaharjoitustyössä tarvittavia Iptablesin sääntöjä. Kaikki säännöt luodaan palomuurina toimivalle tietokoneelle. Työssä tarvittavat komennot, parametrit ja moduulit on esitelty liitteessä 1. Iptables-työkalun käyttöä voi tarkastella liitteestä 2.

5.5.1 Liikenteen esto sääntöketjuissa

Kun halutaan estää kaikki muu pakettiliikenne, asetetaan sääntöketju DROP-tilaan. Sääntöketjuun täytyy tässä tilanteessa lisätä kaikki halutut pakettiliikenteet. Tätä työtä varten INPUT- ja FORWARD-sääntöketjut asetetaan DROP-tilaan (**Kehys 6.**).

```
iptables -P INPUT DROP
iptables -P FORWARD DROP
```

Kehys 6. DROP-tilan komennot

5.5.2 ICMP-viestit

Yhteyden toiminnan testaamista varten sallitaan ICMP-viestit INPUT-ketjussa (**Kehys 7.**).

```
iptables -A INPUT -p icmp –icmp-type echo-reply -j ACCEPT
iptables -A INPUT -p icmp –icmp-type echo-request -j ACCEPT
```

Kehys 7. ICMP-viestien salliminen

5.5.3 Loopbackin asettaminen

Kun sääntöketjuihin tehdään tiloja, jotka poistavat kaikki sisääntulevat tai ulosmenevät paketit, täytyy niihin asettaa Loopback-liikenne omalle koneelle. Loopbackia tarvitaan, jotta ohjelmille tai laitteille ei aiheutuisi vahinkoja. Tietoturvallisuuden suunnittelutyötä varten Loopbackia tarvitaan INPUT-ketjussa (**Kehys 8.**).

```
iptables -A INPUT -i lo -j ACCEPT
```

Kehys 8. Loopback-liikenteen salliminen

Jos sääntö halutaan asettaa sääntöketjussa jollekin tietylle sijalle, täytyy Append-komennon sijaan käyttää Insert-komentoa. Tässä työssä Loopback-liikenteen salliva sääntö sijoitetaan INPUT-ketjun ensimmäiseksi säännöksi (**Kehys 9.**).

```
iptables -I INPUT 1 -i lo -j ACCEPT
```

Kehys 9. Insert-komento

5.5.4 FORWARD-ketjun sääntöjä

FORWARD-kejussa sallitaan pakettiliikenteen kulku sisäverkosta ulkoverkkoon ja DMZ-verkkoon. Samassa ketjussa sallitaan myös yhteys ulkoverkosta DMZ-verkkoon. (**Kehys 10.**)

```
iptables -A FORWARD -i eth2 -o eth0 -j ACCEPT
iptables -A FORWARD -i eth2 -o eth1 -j ACCEPT
iptables -A FORWARD -i eth0 -o eth1 -j ACCEPT
```

Kehys 10. FORWARD-ketjun pakettiliikenteen sallitut säännöt

5.5.5 Itseluodun yhteyden salliminen

Sääntöketjuihin voidaan asettaa säännöt, jotka sallivat itseluodut yhteydet muun liikenteen ollessa kielletty. Tällaisten sääntöjen luomiseen tarvitaan State-moduulia. Tätä työtä varten itseluotujen yhteyksien säännöt tarvitaan INPUT- ja FORWARD-ketjuihin. INPUT-ketjussa tällä säännöllä sallitaan palomuurikoneelle palaava itseluotu pakettiliikenne (**Kehys 11.**). FORWARD-ketjussa sallitaan ulkoverkosta ja DMZ-verkosta vain takaisin palaava pakettiliikenne sisäverkkoon (**Kehys 12.**). FORWARD-ketjuun asetetaan myös sääntö, joka sallii DMZ-verkosta vain takaisin palaavan pakettiliikenteen ulkoverkkoon (**Kehys 12.**).

```
iptables -A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
```

Kehys 11. Takaisin palaavan liikenteen salliva sääntö INPUT-ketjussa

```
iptables -A FORWARD -i eth0 -o eth2 -m state --state
ESTABLISHED,RELATED -j ACCEPT
iptables -A FORWARD -i eth1 -o eth2 -m state --state
ESTABLISHED,RELATED -j ACCEPT
iptables -A FORWARD -i eth1 -o eth0 -m state --state
ESTABLISHED,RELATED -j ACCEPT
```

Kehys 12. Takaisin palaavan liikenteen sallivat säännöt FORWARD-ketjussa

5.5.6 Sisääntuleva TCP-pakettiliikenne palomuurikoneen portteihin

Eri laitteita ja palveluja varten sääntöketjuihin voidaan lisätä ehto, joka joko sallii tai estää TCP-pohjaisen pakettiliikenteen tietyssä portissa. Tätä työtä varten palomuurikoneelle sallitaan pakettiliikenne SSH-palvelinta varten portissa 22, FTP-palvelinta varten portissa 21 ja OpenVPN-palvelinta varten portissa 1194 (**Kehys 13.**).

```
iptables -A INPUT -p tcp --dport 22 -j ACCEPT
iptables -A INPUT -p tcp --dport 21 -j ACCEPT
iptables -A INPUT -p tcp --dport 1194 -j ACCEPT
```

Kehys 13. Sallitut TCP-portit

5.5.7 NAT

Tietokoneet, joilla on yksityinen IP-osoite, tarvitsevat osoitteenmuunnoksen, jotta ne pystyvät luomaan yhteyden internettiin. Tässä työssä sisäverkon tietokoneelle ja DMZ-verkon tietokoneelle tehdään osoitteenmuunnokset. Palomuurina toimivan tietokoneen Iptablesin POSTROUTING-ketjuun asetetaan nämä uudet lähdeosoitteet käyttäen SNAT-moduulia (**Kehys 14.**).

```
iptables -t nat -A POSTROUTING -s 10.1.1.0/24 -j SNAT --to 195.148.171.101
iptables -t nat -A POSTROUTING -s 10.1.2.0/24 -j SNAT --to 195.148.171.101
```

Kehys 14. Osoitteenmuunnokset

5.5.8 Sisääntulevan TCP-pakettiliikenteen uudelleenohjaus

PREROUTING-ketjuun lisätään säännöt, kun halutaan ohjata tiettyä pakettiliikennettä johonkin toiseen osoitteeseen. Tässä työssä palomuurikoneen portteihin 22, 80, 53, 443 ja 631 saapuva TCP-pakettiliikenne halutaan uudelleenohjata DMZ-verkossa oleville palvelimille (**Kehys 15.**). Uudelleenohjaussäännöt aiheuttavat sen, että kaikki sisään tuleva TCP-pakettiliikenne ei enää saavu palomuurina toimivalle tietokoneelle. Jos esimerkiksi palomuurina toimivan tietokoneen IP-osoitteeseen 195.148.171.101 luodaan SSH-yhteys, ohjautuu tämä yhteys DMZ-verkossa olevalle tietokoneelle.

```
iptables -t nat -A PREROUTING -p tcp -d 195.148.171.101 --dport 22 -j DNAT
--to 10.1.1.2
iptables -t nat -A PREROUTING -p tcp -d 195.148.171.101 --dport 80 -j DNAT
--to 10.1.1.2
iptables -t nat -A PREROUTING -p tcp -d 195.148.171.101 --dport 53 -j DNAT
--to 10.1.1.2
iptables -t nat -A PREROUTING -p tcp -d 195.148.171.101 --dport 443 -j DNAT
--to 10.1.1.2
iptables -t nat -A PREROUTING -p tcp -d 195.148.171.101 --dport 631 -j DNAT
 --to 10.1.1.2
```

Kehys 15. TCP-pakettiliikenteen uudelleenohjaus

5.6 Iptables-restore

Iptables-säännöt eivät oletusarvoisesti säily tai tule voimaan automaattisesti tietokoneen uudelleenkäynnistyksen yhteydessä. Luodut säännöt voidaan manuaalisesti tallentaa iptables-save -komennolla ja palauttaa tietokoneen uudelleenkäynnistyksen jälkeen iptables-restore -komennolla.

Iptables-save -komento tallentaa säännöt tiedostoon, josta iptables-restore lukee ne. Säännöt voidaan myös tallentaa toiseen tiedostoon, joka nimetään itse (**Kehys 16.**). Tällä tavalla voidaan luoda monia erilaisia ja valmiiksi laadittuja sääntöjä käytettäväksi.

```
Sudo sh -c “iptables-save > /etc/iptables.rules”
```

Kehys 16. Sääntöjen tallennus omaan tiedostoon

Iptables-palomuurin säännöt saadaan myös automaattisesti asettumaan. Palomuurikoneen ulkoverkkoa käyttävän eth0-verkkokortin /etc/network/inter-faces-tiedoston asetusten jälkeisille riveille lisätään Iptables-restore -toiminto ja määri-

tellään sille tiedosto, josta Iptables automaattisesti tietokoneen uudelleen-käynnistymisen jälkeen hakee sääntöketjujen asetukset (**Kehys 17.**).

```
pre-up iptables-restore < /etc/iptables.rules
```

Kehys 17. Iptables-restore komento

5.7 Nmap – verkkoskanneri

Tässä työssä palomuurikoneena toimivaa tietokonetta skannataan Nmap-verkkos-kannerilla kahden eri skannaustekniikan avulla. Regular-skannaustekniikalla suoritetaan pikainen porttien selaus ja Ping-pyyhkäisy kohteeseen. Perusteellisemmalla ja agressiivisemmalla Intense-skannaustekniikalla selvitetään kohteen kaikki mahdolliset avoimet portit, käyttöjärjestelmä ja ohjelmien versiot. Iptables-palomuurilla ei tässä työn vaiheessa ole sääntöjä eikä pakettien uudelleenohjausta tai osoitteenmuunnosta ole. Skannauskomentoon lisätään Regular-skannaustekniikkaan verrattuna neljä lisäparametriä (**Kehys 18.**).

```
-p 1-65535 #Skannataan kaikki 65535 TCP-porttia
-T4 #Agressiivisempi ja nopempi skannaus
-A #Käyttöjärjestelmän ja pakettiliikenteen reitin skannaus
-v #Tulostaa tarkempaa tietoa skannauksesta
```

Kehys 18. Perusteellisemman skannauksen parametrit

5.8 Nessus – haavoittuvuuksien analysointityökalu

Tässä työssä Nessus-analysointityökalulla skannataan palomuurina toimivaa tie-tokonetta. Tämän tietokoneen palomuurin on tarkoitus tässä vaiheessa työtä olla poissa päältä, jotta Nessus voisi löytää mahdollisimman paljon palveluja ja avoi-mia portteja. Nessus luokittelee näiden palvelujen ja porttien turvallisuusriskin, ilmoittaa niistä mahdollisia tarkempia tietoja ja ehdottaa turvallisuutta parantavia keinoja.

5.9 Snort – tunkeutumisyrityksien havaitsemisjärjestelmä

Tässä työssä Snort-ohjelmaa käytetään ilman Iptables-palomuurin sääntöjä. Iptables-palomuurin sääntöketjut asetetaan sallimaan kaikki liikenne, Snort käynnistetään Network Intrusion Detection System Mode (NIDS)-tilassa ja kannettavalla tietokoneella skannataan Nmap-verkkoskannerilla palomuurina toimivaa tietokonetta. Skannaminen aiheuttaa varoitustietojen syntymisen Snortin Alertlog-tiedostoon. Tätä tiedostoa voidaan lukea nano-työkalulla ja varoitustiedoista pystytään lukemaan aikaleima, protokolla ja hyökkääjän sekä kohteen IP-osoitteet.

NIDS-tilassa ollessaan Snort kirjaa ylös log-tiedostoon ne paketit, jotka aiheuttavat hälytyksen. Tällaiset paketit määritellään snort.conf -tiedostossa. (Sourcefire, Inc 2010, 9-11.) Snort.conf -ja rules-tiedostostot löytyvät /etc/snort -polusta ja alert -tiedostot /var/log/snort -polusta.

Tätä työtä varten Snort.conf tiedoston Output plugins -asetuksissa on vaihdettu pakettien tallennus log_tcpdump: tcpdum.log -muodosta output full_alert: alertlog –muotoon.

Snortin käynnistäminen komentorivillä NIDS-tilassa vaatii Snort-komennon (**Kehys 19.**) ja snort.conf-tiedoston polun määrittelemisen (**Kehys 20.**).

```
snort -c /etc/snort/snort.conf
```

Kehys 19. Snortin käynnistyskomento

```
-c /etc/snort/snort.conf
```

Kehys 20. Snort.conf-tiedoston sijainnin määrittely

6 TULOKSET

6.1 Iptablesin säännöt

Tässä opinnäytetyössä tarvitut Iptables-säännöt asetettiin INPUT-, FORWARD-, PREROUTING- ja POSTROUTING-sääntöketjuihin. Iptables-palomuuriin asetetut säännöt kokonaisuudessaan voidaan tarkistaa komennoilla iptables –L -v ja iptables –t nat –L –v (**Kuva 7.**).

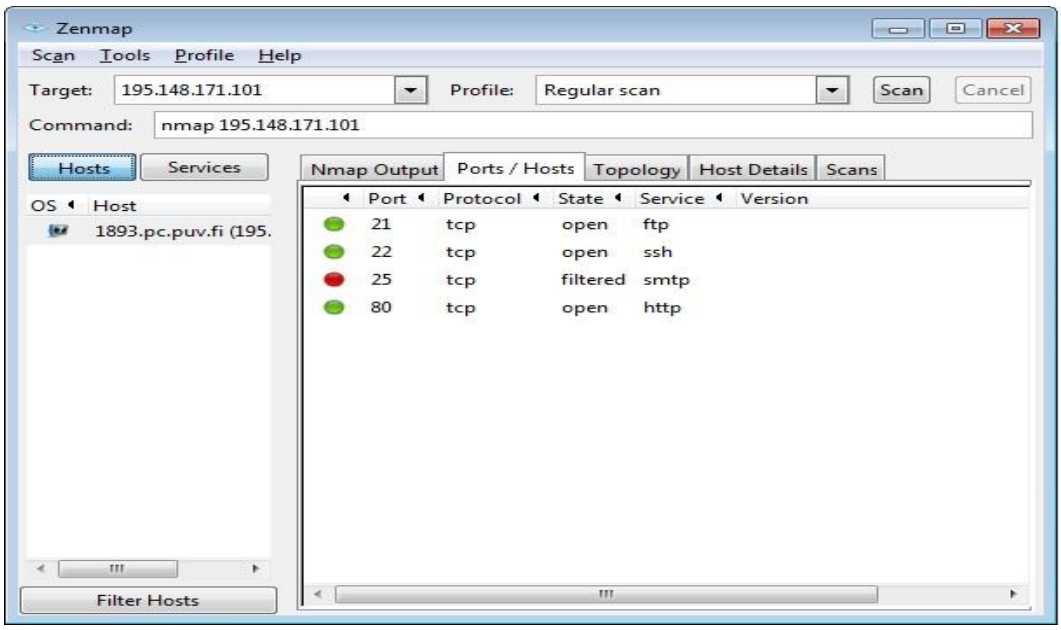
```
Chain INPUT (policy DROP 61558 packets, 3218K bytes)
 pkts bytes target     prot opt in     out     source       destination
   91  7390 ACCEPT     all  --  lo     any     anywhere     anywhere
    5   284 ACCEPT     icmp --  any    any     anywhere     anywhere           icmp echo-reply
   88  6437 ACCEPT     icmp --  any    any     anywhere     anywhere           icmp echo-request
  489 36712 ACCEPT     all  --  any    any     anywhere     anywhere           state RELATED,ESTABLISHED
 1756  166K ACCEPT     tcp  --  any    any     anywhere     anywhere           tcp dpt:ssh
    0     0 ACCEPT     tcp  --  any    any     anywhere     anywhere           tcp dpt:ftp
    0     0 ACCEPT     tcp  --  any    any     anywhere     anywhere           tcp dpt:openvpn

Chain FORWARD (policy DROP 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source       destination
    0     0 ACCEPT     all  --  eth2   eth0    anywhere     anywhere
    0     0 ACCEPT     all  --  eth2   eth1    anywhere     anywhere
    0     0 ACCEPT     all  --  eth0   eth1    anywhere     anywhere
    0     0 ACCEPT     all  --  eth0   eth2    anywhere     anywhere           state RELATED,ESTABLISHED
    0     0 ACCEPT     all  --  eth1   eth2    anywhere     anywhere           state RELATED,ESTABLISHED
    0     0 ACCEPT     all  --  eth1   eth0    anywhere     anywhere           state RELATED,ESTABLISHED

Chain OUTPUT (policy ACCEPT 534K packets, 28M bytes)
 pkts bytes target     prot opt in     out     source       destination

Chain PREROUTING (policy ACCEPT 561K packets, 26M bytes)
 pkts bytes target     prot opt in     out     source       destination
   73  3884 DNAT       tcp  --  any    any     anywhere     1893.pc.puv.fi     tcp dpt:www to:10.1.1.2
    0     0 DNAT       tcp  --  any    any     anywhere     1893.pc.puv.fi     tcp dpt:ssh to:10.1.1.2
    0     0 DNAT       tcp  --  any    any     anywhere     1893.pc.puv.fi     tcp dpt:www to:10.1.1.2
    0     0 DNAT       tcp  --  any    any     anywhere     1893.pc.puv.fi     tcp dpt:domain to:10.1.1.2
    0     0 DNAT       tcp  --  any    any     anywhere     1893.pc.puv.fi     tcp dpt:https to:10.1.1.2
    0     0 DNAT       tcp  --  any    any     anywhere     1893.pc.puv.fi     tcp dpt:ipp to:10.1.1.2

Chain POSTROUTING (policy ACCEPT 9948 packets, 705K bytes)
 pkts bytes target     prot opt in     out     source       destination
    1    67 SNAT       all  --  any    any     10.1.1.0/24  anywhere           to:195.148.171.101
    1    67 SNAT       all  --  any    any     10.1.2.0/24  anywhere           to:195.148.171.101
```

Kuva 7. Iptables-sääntöketjujen säännöt

6.2 Nmap-skannaus

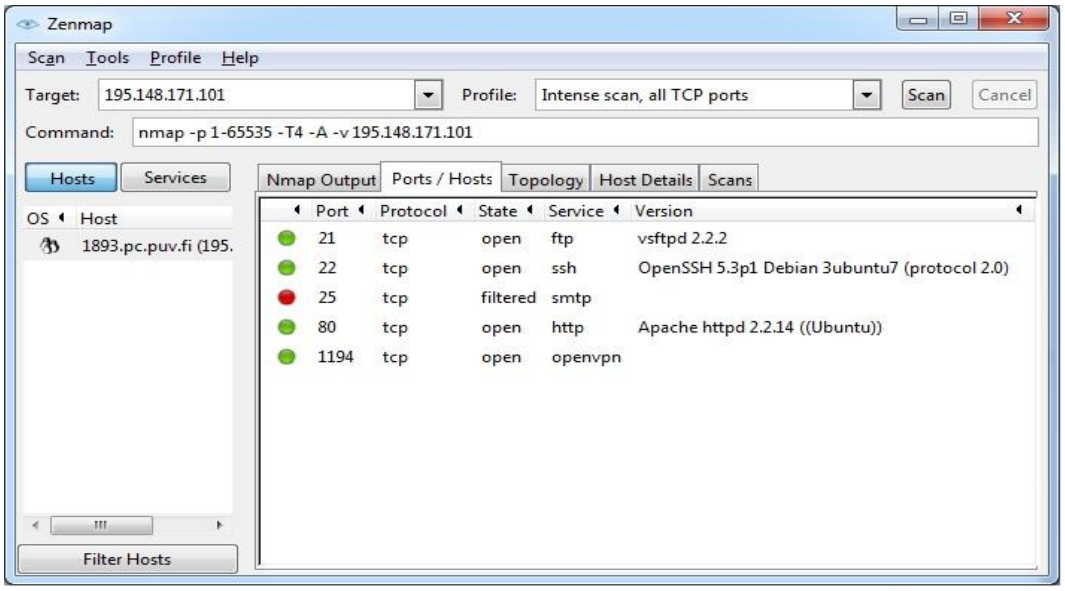
Nmap-ohjelmalla skannattiin palomuurina toimivaa Linux-tietokonetta Regular-skannauksella (**Kuva 8.**). Palomuuri oli asetettu pois päältä ja tietokoneen TCP-

portit 21, 22 ja 80 havaittiin avoimiksi. Näitä portteja käyttävät FTP-, SSH- ja Web-palvelut. Portin 25 tila on Filtered ja se on SMTP-palvelun käytössä.



Kuva 8. Nmapin tulos tavallisella skannauksella

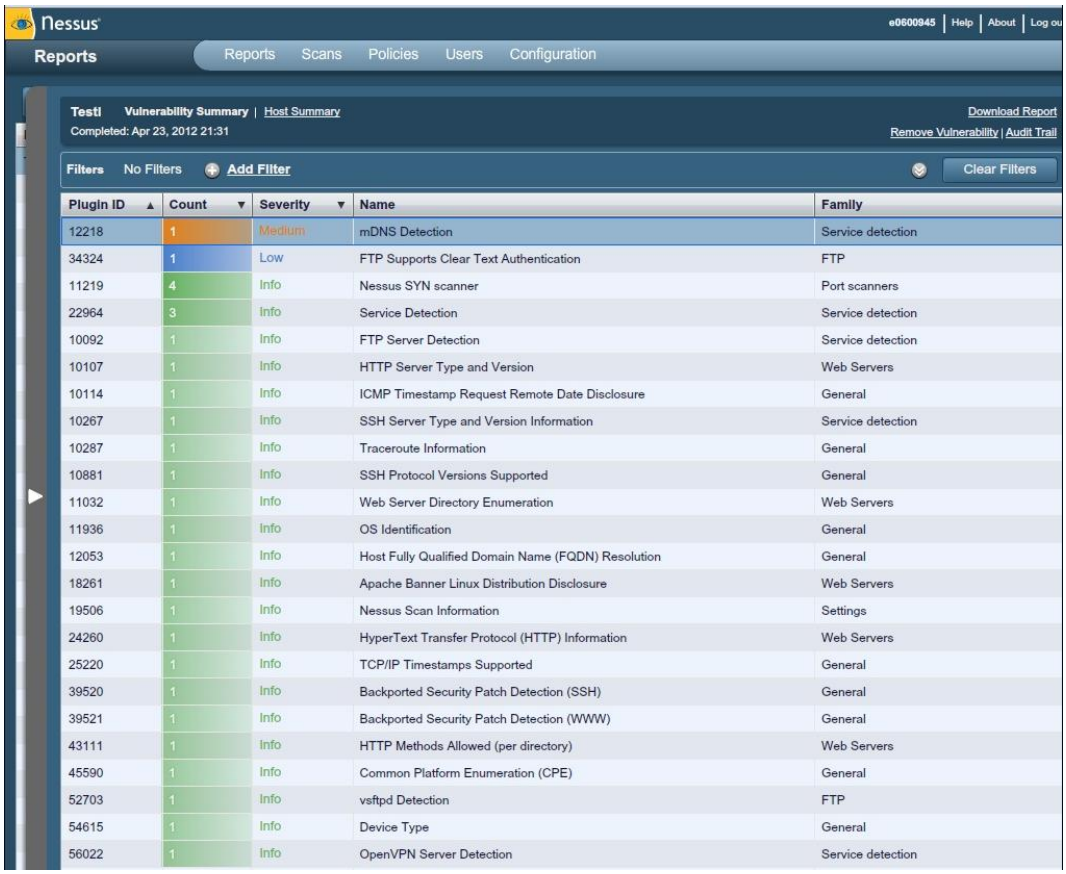
Regular-skannaus ei tosin tutki kaikkia mahdollisia porttinumeroita, jolloin esimerkiksi OpenVPN-porttia ei näy tuloksessa. Perusteellisemmalla ja agressiivisemmalla Intense-skannaustekniikalla selvitettiin kohteen kaikki mahdolliset avoimet portit, käyttöjärjestelmä ja ohjelmien versiot (**Kuva 9.**).



Kuva 9. Nmapin tulos perusteellisemmalla skannauksella

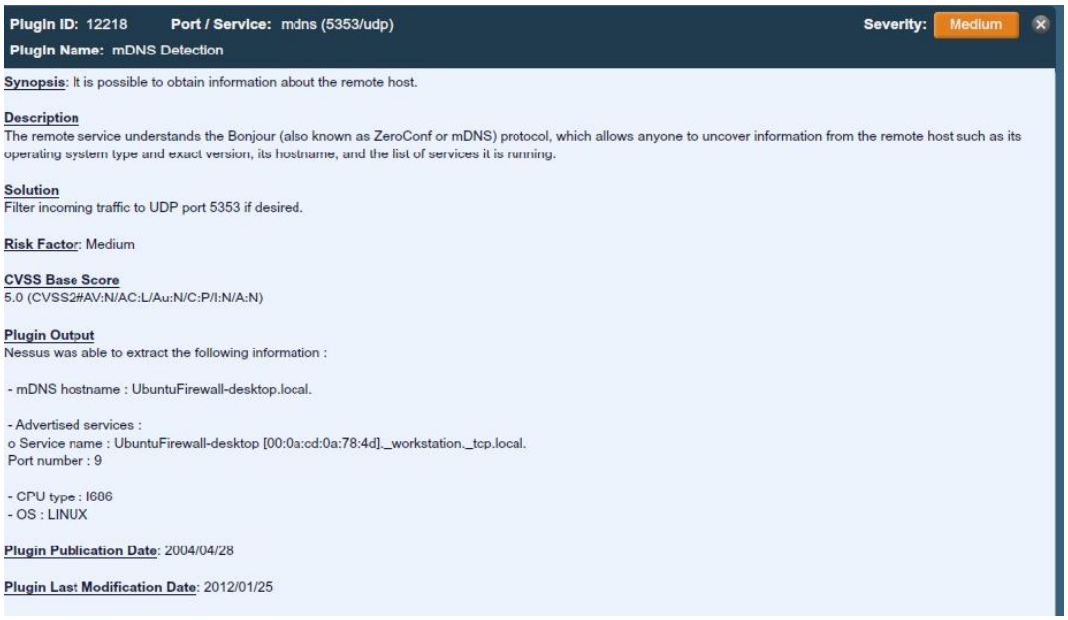
6.3 Nessus-skannaus

Nessus-ohjelmalla skannattiin palomuurina toimivaa Linux-tietokonetta, jonka Iptables-palomuuri ei ole päällä. Skannauksen tuloksena saatiin tietoa lukuisista palveluista ja kohteen järjestelmästä (**Kuva 10.**). Työn kannalta merkittävimpiä tuloksia olivat Medium-turvaluokituksen saanut mDNS-palvelu (**Kuva 11.**) ja Low-turvaluokituksen saanut FTP-palvelu (**Kuva 12.**). Nessuksen skannaustiedoista selviää, että kohteesta on saatu mDNS-protokollan avulla tietoa käyttöjärjestelmästä ja palveluista. FTP-palvelun skannaustiedot paljastavat, että sen käyttäjänimissä ja salasanoissa ei käytetä salausta.



Plugin ID	Count	Severity	Name	Family
12218	1	Medium	mDNS Detection	Service detection
34324	1	Low	FTP Supports Clear Text Authentication	FTP
11219	4	Info	Nessus SYN scanner	Port scanners
22964	3	Info	Service Detection	Service detection
10092	1	Info	FTP Server Detection	Service detection
10107	1	Info	HTTP Server Type and Version	Web Servers
10114	1	Info	ICMP Timestamp Request Remote Date Disclosure	General
10267	1	Info	SSH Server Type and Version Information	Service detection
10287	1	Info	Traceroute Information	General
10881	1	Info	SSH Protocol Versions Supported	General
11032	1	Info	Web Server Directory Enumeration	Web Servers
11936	1	Info	OS Identification	General
12053	1	Info	Host Fully Qualified Domain Name (FQDN) Resolution	General
18261	1	Info	Apache Banner Linux Distribution Disclosure	Web Servers
19506	1	Info	Nessus Scan Information	Settings
24260	1	Info	HyperText Transfer Protocol (HTTP) Information	Web Servers
25220	1	Info	TCP/IP Timestamps Supported	General
39520	1	Info	Backported Security Patch Detection (SSH)	General
39521	1	Info	Backported Security Patch Detection (WWW)	General
43111	1	Info	HTTP Methods Allowed (per directory)	Web Servers
45590	1	Info	Common Platform Enumeration (CPE)	General
52703	1	Info	vsftpd Detection	FTP
54615	1	Info	Device Type	General
56022	1	Info	OpenVPN Server Detection	Service detection

Kuva 10. Nessus-skannaus palomuurista



Kuva 11. Medium-luokituksen saanut palvelu

Kuva 12. Low-luokituksen saanut palvelu

6.4 Snortin Alertlog-tiedosto

Nmap-ohjelmalla skannattiin tietokonetta, jossa Snort-ohjelma oli käynnissä. Snortin /var/log/snort/alertlog-tiedostoon (**Kehys 21.**) tulostui tietoja skannauksesta. Tiedostosta selviää, että tietokoneeseen on kohdistunut TCP-porttiskannaus, suuri pakettiliikenne yhdestä lähteestä ja Web-palvelimen tiedustelu.

```
[**] [122:1:1] (portscan) TCP Portscan [**]  #Porttiskannauksen tunniste
[Priority 3] #Turvataso
04/30-10:36:22.026246 94.22.122.29->195.148.171.101 #Aikaleima sekä
hyökkääjän ja kohteen IP-osoite

[**] [1:100000160:2] COMMUNITY SIP TCP/IP message flooding directed to
SIP proxy [**] #Suuren pakettiliikenteen havaitsemistunniste
[Classification: Attempted Denial of Service] #Palvelunestohyökkäysluokitus
04/30-10:36:22.026246 94.22.122.29 ->195.148.171.101 #Aikaleima sekä
hyökkääjän ja kohteen IP-osoite

[**] [119:18:1] (http_inspect) WEBROOT DIRECTORY TRAVERSAL [**]
#Web-palvelimen tiedustelutunniste
[Priority 3] #Turvataso
04/30-10:37:22.671353 94.22.122.29 ->195.148.171.101 #Aikaleima sekä
hyökkääjän ja kohteen IP-osoite
```

Kehys 21. Alertlog-tiedosto

6.5 Tietoturvaharjoitustyö

Palomuurin avulla suojataan ja valvotaan tietoliikenneverkkoja. Tässä laboratoriotyössä konfiguroidaan Iptables-työkalun avulla Linux-pohjainen palomuuri. Työstä kirjoitetaan työselostus, jossa vastataan esitettyihin kysymyksiin, listataan ja kommentoidaan tehtävän suorittamiseen vaadittavat komennot.

6.5.1 Esitehtävät

Ennen harjoitustyötä tulee tehdä esitehtävät. Tutustu Iptablesiin esimerkiksi osoitteissa: http://linux.fi/index.php/Iptables, https://help.ubuntu.com/community/IptablesHowTo ja http://linux.die.net/man/8/iptables.

a) Mikä on DMZ-alue ja miksi sitä käytetään?

b) Mitkä ovat oletuksena Ubuntu 10.04 LTS:n Iptablesin pakettien käsittelysäännöt ja politiikka?

c) Millä tavalla INPUT- ja FORWARD-sääntöketjujen pakettien käsittely eroavat toisistaan? Entä miten PREROUTING- ja POSTROUTING-sääntöketjut käsittelevät pakettiliikennettä?

d) Mitä tapahtuu seuraavilla säännöillä?

Iptables -L

iptables -t nat -L

iptables –t nat -F

iptables –P INPUT DROP

iptables –A FORWARD –i eth0 –o eth2 –j ACCEPT

Tehtävissä tarvittavia komentoa

man <komento>	Näyttää kyseisen komennon manuaalisivut
ifconfig	Verkkoliityntöjen konfigurointi
service --status-all	Näyttää tietoja päällä olevista palveluista
nano	Yksinkertainen tekstieditori
/etc/init.d/<palvelu>	Palveluiden käynnistäminen ja sammuttaminen

6.5.2 Tehtävä 1. Palomuurin valmistelu

Varmista, että Iptablesin sääntöketjuissa ei ole mitään sääntöjä. Sen jälkeen tarkista, että Iptablesin kaikki Policy-asetukset ovat Accept-tilassa.

6.5.3 Tehtävä 2. Verkon skannaaminen

a) Skannaa palomuurina toimivaa tietokonetta ulkoverkossa olevalla kannettavalla tietokoneella. Mitä palveluja on käynnissä ja mitkä portit ovat auki?

b) Millä eri tekniikoilla verkkoja voidaan skannata ja miten nämä tekniikat eroavat toisistaan?

c) Tallenna tulokset.

6.5.4 Tehtävä 3. Haavoittuvuuksien analysointi

Nessus-työkalulla voidaan analysoida kohteen haavoittuvuuksia. Skannaa palomuurina toimivaa tietokonetta. Mitä palveluja Nessus löytää ja mitä varoituksia se niistä antaa?

6.5.5 Tehtävä 4. Iptables

Iptables on Linux-ympäristössä tehokas työkalu, jonka avulla voidaan toteuttaa tehokas ja monipuolinen palomuuri. Iptablesin avulla voidaan suoraan antaa oh-

jeita miten Netfilter-pakettisuodatin käsittelee pakettiliikennettä. Iptables-työkalu vaatii rootin oikeuksia.

a) Muuta INPUT-ketjun politiikkaa siten, että kaikki sisään tuleva pakettiliikenne estetään. Varmista pingaamalla joko ulkoverkossa olevaa kohdetta tai sisäverkon tietokoneita. Käytä Wiresharkia ICMP-viestien tutkimiseen.

b) Luo säännöt, joiden avulla sallitaan Ping-request- ja Ping-reply -viestit. Tarkista pingaamalla.

c) Luo sääntö, joka sallii Loopback-liikenteen INPUT-ketjussa. Tämä sääntö täytyy olla sääntöketjussa ensimmäisenä.

d) Muuta FORWARD-ketjun poliitiikka estämään uudelleenohjattava pakettiliikenne. Luo sen jälkeen säännöt seuraavat säännöt:

- salli yhteydet sisäverkosta ulkoverkkoon ja DMZ-verkkoon
- salli vain takaisin palaava pakettiliikenne ulkoverkosta ja DMZ-verkosta sisäverkkoon
- salli yhteys ulkoverkosta DMZ-verkkoon, mutta DMZ-verkosta ulkoverkoon saa vain takaisin palaava pakettiliikenne kulkea.

e) Luo lisäksi sääntö, jonka avulla sallitaan SSH-protokolla ulkoverkosta palomuuriin. Varmista ottamalla yhteyttä ulkoverkon kannettavan tietokoneen Putty-ohjelmalla.

6.5.6 Tehtävä 5. Nat

a) Konfiguroi NAT sisä- ja DMZ-verkosta ulkoverkkoon. Varmista toiminta pingaamalla ulkoverkossa olevaa kannettavaa tietokonetta ja tarkista Wireshark-pakettikaapparilla, että pakettiliikenne tulee palomuurin IP-osoitteesta.

b) Konfiguroi palomuuri uudelleenohjaamaan palomuurin porttiin 80 tulevaa pakettiliikennettä DMZ-verkon palvelimelle. Uudelleenohjaa pakettiliikenne myös SSH-, DNS-, HTTPS- ja CUPS-palvelimille. Varmista toiminta ottamalla yhteys palomuurina toimivan tietokoneen SSH-porttiin.

6.5.7 Tehtävä 6. Iptables-restore

Tietokoneen uudelleenkäynnistyksen yhteydessä Iptablesin säännöt katoavat ja palomuuri palaa oletustilaansa. Selvitä, miten luodut Iptablesin säännöt saadaan pysymään.

6.5.8 Tehtävä 7. IDS

IDS-järjestelmän tarkoitus on havaita tunkeutumisyrityksiä. Palomuurina toimivalle tietokoneelle on asennettu Snort-niminen ohjelma. Aseta Iptables-työkalulla sääntöketjut ACCEPT-tilaan ja poista kaikki aikasemmin asetetut säännöt komennoilla iptabales -F ja iptables -t nat -F. Käynnistä Snort komentorivillä komennolla snort -c /etc/snort/snort.conf. Snortin ollessa päällä, skannaa palomuurina toimivaa tietokonetta ulkoverkon kannettavan tietokoneen Nmap-ohjelmalla. Skannaus aiheuttaa Snortin kirjaamaan ylös alert-tiedostoonsa hälyttävät pakettiliikenteet. Alert-tiedostoa, joka sijaitsee polussa /var/log/snort, voi lukea nano-työkalulla. Kopioi yksi varoitus työselostukseen.

7 YHTEENVETO

Tietoturvatyön suunnittelu onnistui hyvin. Työtä varten saatiin tarpeellinen ja riittävän tehokas laitteisto. Käyttöjärjestelmät ja ohjelmat toteutettiin Opensource-vaatimusten mukaisesti.

Työtä varten luodussa verkkoympäristössä ilmenee palomuuri, DMZ-verkko ja sisäinen verkko. Sisäisessä verkossa on vain yksi tietokone työkoneena. DMZ-verkossa on myös vain yksi tietokone, jossa sijaitsevat palvelut. Web-, DNS- ja CUPS-palveluja ei ole konfiguroitu toimimaan oikeina palveluina, mutta tämän työn tuloksen osalta pelkästään niiden asennetut oletusversiot ovat riittävät.

Tätä työtä voisi jatkaa kehittämällä täysin toimivan verkkoympäristön. DHCP-, Web-, DNS- ja CUPS-palvelut voisivat olla konfiguroituna, jolloin verkkoympäristöstä voisi ilmetä uusia riskejä tietoliikenteen turvallisuudesta.

LÄHTEET

Hakala, Mika & Vainio, Mika & Vuorinen, Olli. 2006. Tietoturvallisuuden käsikirja. 205-206, 208-210. 1. painos. Jyväskylä. Docendo.

Nmap.org. 2012. Introduction. Viitattu 10.2.2012. http://nmap.org/

PuTTY. 2012. What is PuTTY. Viitattu 21.3.2012. http://www.chiark.greenend.org.uk/ ~sgtatham/putty/ faq.html#faq-what.

Sourcefire, Inc. 2010. About Snort. Viitattu 15.2.2012. http://www.snort.org/ snort.

Sourcefire, Inc. 2010. Snort Manual. Viitattu 15.2.2012. http://www.snort.org/ assets/ 166/ snort_manual.pdf. 9-11.

Spamlaw. 2012. Data Protection. Viitattu 6.5.2012. http://www.spamlaws.com/protect-data-on-internet.html

Tenable Network Security. 2012. Customized Reporting. Viitattu 10.2.2012. http://www.tenable.com/products/nessus/nessus-product-overview/nessus-features/ customized-reporting.

Tenable Network Security. 2012. In-Depth Assessments. Viitattu 10.2.2012. http://www.tenable.com/products/nessus/nessus-product-overview/nessus-features/ in-depth-assessments.

Viestintävirasto. 2007. Palomuuri. Viitattu 6.5.2012. http://www.ficora.fi/index/palvelut/palvelutaiheittain/tietoturva/palomuuri.html

Viestintävirasto. 2012. Tietoturva ja -suoja. Viitattu 6.5.2012. http://www.ficora.fi/index/palvelut/palvelutaiheittain/tietoturva.html

Wireshark. 2006. About Wireshark. Viitattu21.3.2012. http://www.wireshark.org/ about.html.

LIITE 1: Iptablesin peruskomennot, parametrit ja moduulit

Iptablesin peruskomennot

- A = append, sääntöketjuun lisääminen
- D = delete, sääntöketjusta poistaminen
- I = insert, sääntöketjun tietylle sijalle lisääminen
- L = list, sääntöketjun listaus
- F = flush, koko sääntöketjun tyhjennys
- P = policy, sääntöketjun tila

Iptablesin parametrit

- p = protocol, protokollan määrittely
- m = match, sovitusmoduulin valinta
- s = source, lähteen määrittely
- d = destination, kohteen määrittely
- j = jump, määrittelee säännön toimintaa paketin ja säännön vastatessa toisiaan
- i = in-interface, vastaanotettujen pakettien rajapinta
- o = out-interface, lähetettyjen pakettien rajapinta
- v = verbose, yksityiskohtaisempi tiedon listaus

Työssä tarvittavat pakettien sovitusmoduulit (Match Extensions)

- State = moduuli, joka sallii yhteyden tilan seurannan

Moduulin mahdolliset tilat:

- NEW, paketti aloittaa täysin uuden yhteyden

- ESTABLISHED, paketit ovat jo liikkuneet molempiin suuntiin
- RELATED, yhteys valmiiksi olemassa olevaan pakettiliikenteeseen

Työssä tarvittavat kohdemoduulit (Target Extensions)

- DNAT - -to = destination nat - -to, määrittelee kohteen IP-osoitteen
- SNAT - -to = source nat - -to, määrittelee lähteen IP-osoitteen

LIITE 2: Iptablesin käyttö

Sääntöjen lisäys sääntöketjuun

Iptables -A (SÄÄNTÖKETJU, esim. INPUT) (LISÄTTÄVÄ SÄÄNTÖ, esim. -p tcp –dport 22) -j ACCEPT

Sääntöjen lisäys sääntöketjuun tietylle sijalle

Iptables -I (SÄÄNTÖKETJU) (SIJA, esim. 3) (LISÄTTÄVÄ SÄÄNTÖ) -j ACCEPT

Sääntöjen poisto sääntöketjusta

Iptables -D (SÄÄNTÖKETJU) (POISTETTAVA SÄÄNTÖ) -j ACCEPT/DROP

Sääntöketjun tilan vaihto

Iptables -P INPUT/OUTPUT/FORWARD ACCEPT/DROP

Iptables-sääntöketjujen tarkastus

INPUT-, FORWARD- ja OUTPUT -sääntöketjujen tarkastelu -L (list) komennolla:

- iptables -L

PREROUTING- ja POSTROUTING -sääntöketjujen tarkastelu -t (table) nat -komennolla:

- iptables -t nat -L

Lisäämällä komentoon -v (verbose) saadaan sääntöketjuista tarkempaa tietoa:

- iptables -L -v
- iptables -t nat -L –v