Lauri Partinen ktkt23sp

Aloitusprojekti

Raportti

Aloitusprojekti

2024



SISÄLLYS

[1 P1 3](#_Toc183902608)

[2 P2 6](#_Toc183902609)

[3 P6 7](#_Toc183902610)

[4 P9 10](#_Toc183902611)

[5 Kyberturvallisuustyökalu powerpoint 13](#_Toc183902612)

# P1

Projektin tavoite on tarkistaa ja tutustua oman tietokoneen tietoturva-asetuksiin käytännössä. Uutena asiana opin. Palomuuri estää oletuksena ICMP liikenteen, joten ping-komento ei toimi. Sain lopulta ping toimimaan kuva alhaalla.

1. Koneiden välillä ei eroja kaikki Windows pohjaisia.
2. Tarkistin virustorjunnan asetukset. Firewall on päällä. Tietokone on ajan tasalla.

* Kuva, joka sisältää kohteen teksti, kuvakaappaus, Fontti

  Kuvaus luotu automaattisesti

1. Mahdollistin pingaamisen palomuurin läpi komennoilla ja kokeilin, toimiiko ping.

Kuva, joka sisältää kohteen teksti, kuvakaappaus, Fontti

Kuvaus luotu automaattisesti

1. Loin kaksi uutta sääntöä yksi ICMPv4 requesteille ja yksi ICMPv6 requesteille

Kuva, joka sisältää kohteen teksti, kuvakaappaus, Fontti

Kuvaus luotu automaattisesti

Kuva, joka sisältää kohteen teksti, kuvakaappaus, Fontti, numero

Kuvaus luotu automaattisesti

**Kuva, joka sisältää kohteen teksti, kuvakaappaus, Fontti, numero

Kuvaus luotu automaattisesti**

1. Kolmansien osapuolien vpn tai palomuuri ohjelmat voivat vaikuttaa Windowsin oletusasetuksiin. Tietoturvaan liittyviä asetuksia voi joutua muuttamaan, jos palomuuri estää sovellukseen pääsyn. Palomuuri asetuksissa tulee sallia sovellus.

# P2

Selvittää ja määrittää www-selaamiseen tarkoitetun virtuaalikoneen palomuurisäännöt hyödyntäen IP-tables palomuurisääntöjä. Projektin aikana opin paljon uutta. Miten iptables toimii, miten tehdä erilaisia komentoja ja testata toiminta. Projektin aikana ei ilmennyt suurempia ongelmia.

Linuxin perusasennus ja konfigurointi tehty.

Kuva, joka sisältää kohteen teksti, kuvakaappaus, Multimediaohjelmisto, ohjelmisto

Kuvaus luotu automaattisesti

Iptables asennus.

Kuva, joka sisältää kohteen teksti, elektroniikka, kuvakaappaus, ohjelmisto

Kuvaus luotu automaattisesti

Ensimmäinen sääntö sallii TCP-liikenteen porttiin 80 (HTTP).

Toinen sääntö sallii TCP-liikenteen porttiin 443 (HTTPS).

****

Testasin iptablesin toimintaa avamaalla nettisivun.

**Kuva, joka sisältää kohteen teksti, kuvakaappaus, Fontti, numero

Kuvaus luotu automaattisesti**

# P6

Projektin tavoite on tutustua Man-in-the-middle-hyökkäyksen toteuttamiseen langattomassa ja langallisessa verkossa. Projektin aikana esiintyi useita ongelmia. Wireshark ei jostain syystä halunnut toimia, joka vaikeutti man in the middle hyökkäyksen tarkkailua. Projektin aikana opin, miten Ettercap käytetään ja miten man in the middle hyökkäys toteutetaan käytännössä.

Latasin Ettercap man in the middle hyökkäystä varten

Kuva, joka sisältää kohteen teksti, selkärangaton, hyönteinen, kuvakaappaus

Kuvaus luotu automaattisesti

Skannataa, jonka avulla saadaa hostit selville, jotka on kiinni tietokoneessa.

**Kuva, joka sisältää kohteen teksti, kuvakaappaus, ohjelmisto, numero

Kuvaus luotu automaattisesti**

Lisätään kohteen ip osoite hostille.

**Kuva, joka sisältää kohteen teksti, kuvakaappaus, ohjelmisto, numero

Kuvaus luotu automaattisesti**

Tehdään Arp hyökkäys kohteeseen.

**Kuva, joka sisältää kohteen teksti, kuvakaappaus, ohjelmisto, Verkkosivusto

Kuvaus luotu automaattisesti**

2. Miten MITM-hyökkäys voidaan estää langattomassa verkossa ?

Käytetään vahvaa salasanaa, vpn-yhteys, huolellisuus julkisissa verkoissa toimiessa, palomuuri ja HTTPS-protokollan käyttö.

# P9

Projektin tavoite on asentaa www-palvelin palvelimelle ja miettiä palvelulle riittävät tietotuvan määritykset. Projekti oli tosi opettava, koska en ole aiemmin linux:in tieturvaa tutustunut tarkemmin. Opin minkälaisia eri tietoturvan parannuskeinoja linuxilla on mahdollista toteuttaa.

Asennetaan apache palvelin



Käynnistetään apache ja varmistetaan toiminta

Kuva, joka sisältää kohteen teksti, kuvakaappaus, Fontti

Kuvaus luotu automaattisesti

Avataan tarvittavat palomuurin portit

Kuva, joka sisältää kohteen teksti, kuvakaappaus, Fontti

Kuvaus luotu automaattisesti

WWW-sivun määrittäminen



Lisätään html koodi palvelimen toiminnan testausta varten

Kuva, joka sisältää kohteen teksti, kuvakaappaus, ohjelmisto, Fontti

Kuvaus luotu automaattisesti

Www-sivu näkyy selaimessa

Kuva, joka sisältää kohteen teksti, kuvakaappaus, ohjelmisto, näyttö

Kuvaus luotu automaattisesti

Asennetaan certbot ja apache-liitäntä



Luodaan SSL-varmenne



Poistetaan ylimääräiset Apache-moduulit

Kuva, joka sisältää kohteen teksti, kuvakaappaus, Fontti

Kuvaus luotu automaattisesti

Muokataa security.conf



ServerTokens Prod: Asetus määrittää, kuinka paljon tietoa palvelimesta paljastetaan HTTP-vastauksissa.

ServerSignature Off: Asetus poistaa palvelimen allekirjoituksen HTTP-vastauksista.

TraceEnable Off: Asetus poistaa HTTP-jäljityksen käytöstä.

Kuva, joka sisältää kohteen teksti, kuvakaappaus, ohjelmisto, Multimediaohjelmisto

Kuvaus luotu automaattisesti

Käytetään palomuuria ja estetään tarpettoomat portit

Kuva, joka sisältää kohteen teksti, Fontti, kuvakaappaus

Kuvaus luotu automaattisesti

Kuva, joka sisältää kohteen teksti, kuvakaappaus, Fontti

Kuvaus luotu automaattisesti

Otetaan käyttöön HTTP Strict Transport Security

Asennetaan ModSecurity, joka estää verkkohyökkäyksiä



# Kyberturvallisuustyökalu powerpoint

Tein esitelmän kaksivaiheisesta tunnistautumisesta

[MFA](https://ksamk-my.sharepoint.com/personal/flapa010_edu_xamk_fi/Documents/MFA.potx?web=1)

