Kyberturvallisuus

&&

Turvallinen lab

Oppilas: Ariful Islam

Tieto- ja tietoliikennetekniikan perustutkinto

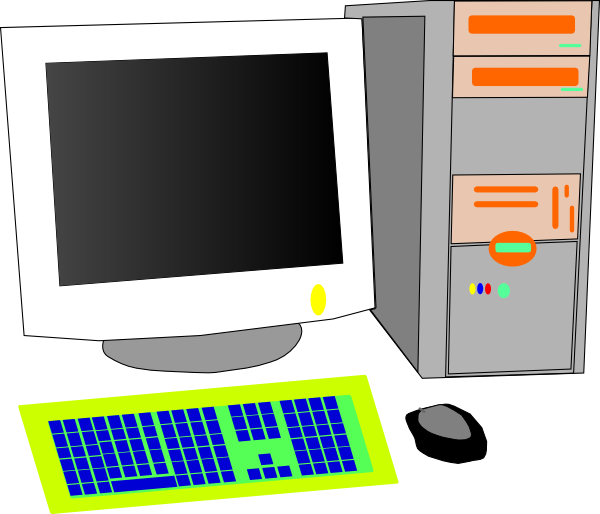
ict-asentaja

Opettaja: Timo Nostolahti

Tietoliikennelaiteasennukset ja kaapelointi

1. Rakennetaan lab





Fyysisen isäntä kone

Virtualbox asennetaan



Natnetwork: lab









Wireshark

IIS

FTP-Server

Apache

Chrome

ADDS

RDP-Client

FTP-client

Metasploit

NMAP

bettercap

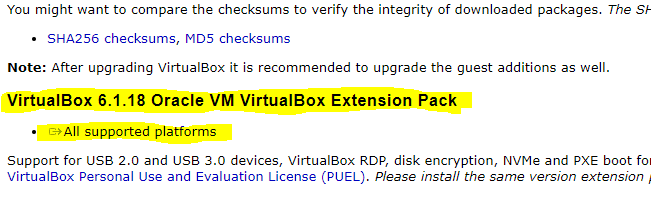
Seth

Kuvio: Virtualbox ja Virtuallikoneet

1. Virtualbox asennus ja konfigurointi
2. Haetaan Virtualbox sovellus ja extension pack nettisivulta https://www.virtualbox.org/



Kuva 1: Ladatan virtualbox



Kuva 2: Ladataan extensions pack

b) Aloitetaan asentaa klikkaamalla ladattu VirtualBox-6.1.18-142142-Win.exe tiedostolla. Seurataan oletuksen vaihtoehtoja. Huoma myös seuravasta kuvasta (bridge networking).



Kuva 3: Asennuksen aloitus

c) Kaikki asennetaan oletuksena loppuasti, paitsi poistetaan ”Virtualbox bridge networking ” optio kun asennetaan Virtualbox. Virtual koneet eivät voi hakea IP-osoite 10.17.242.0/24 verkosta (Koulun verkko).

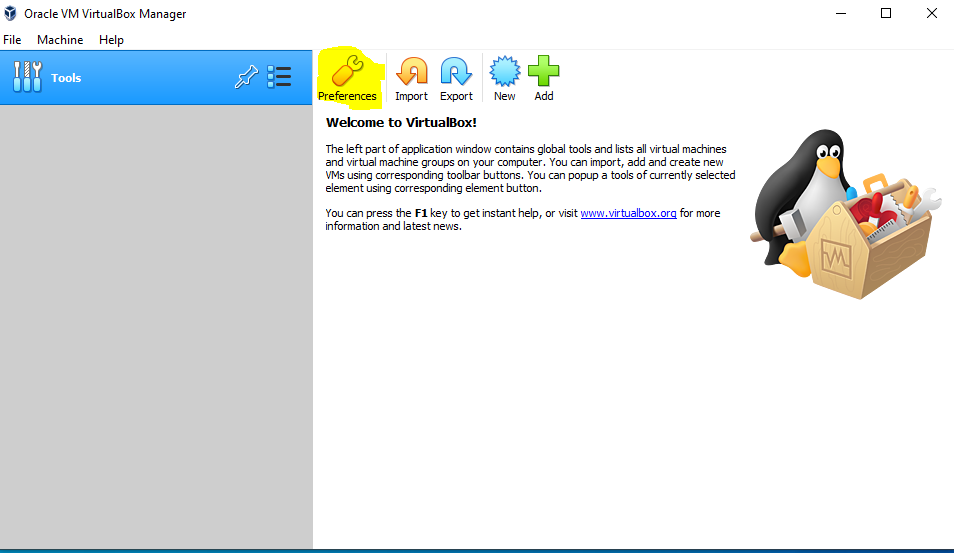
Graphical user interface, application

Description automatically generated

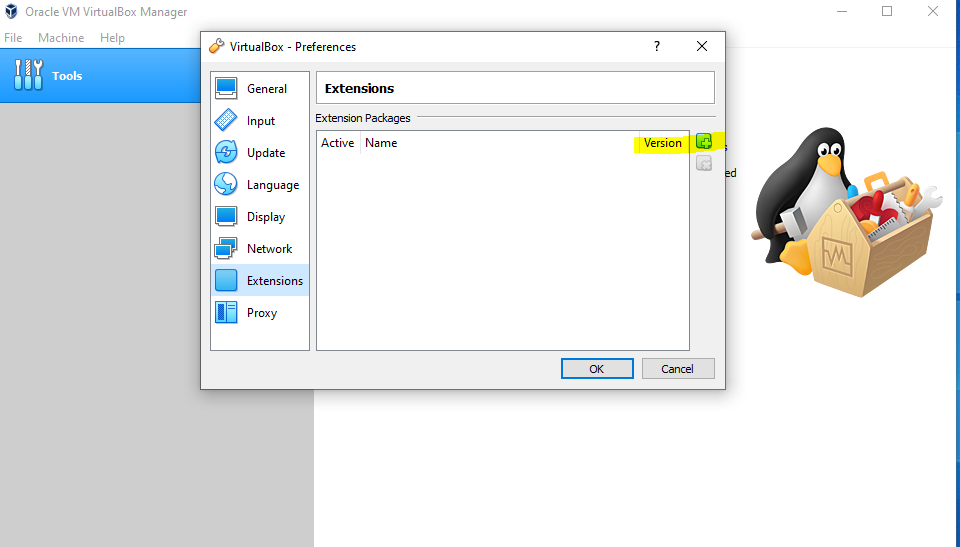
Kuva 4: Bridge networking poistaminen

Virtualboxin on valmit asennus . Nyt liitän aikaisin haettu VirtualBox\_Extension\_Pack.

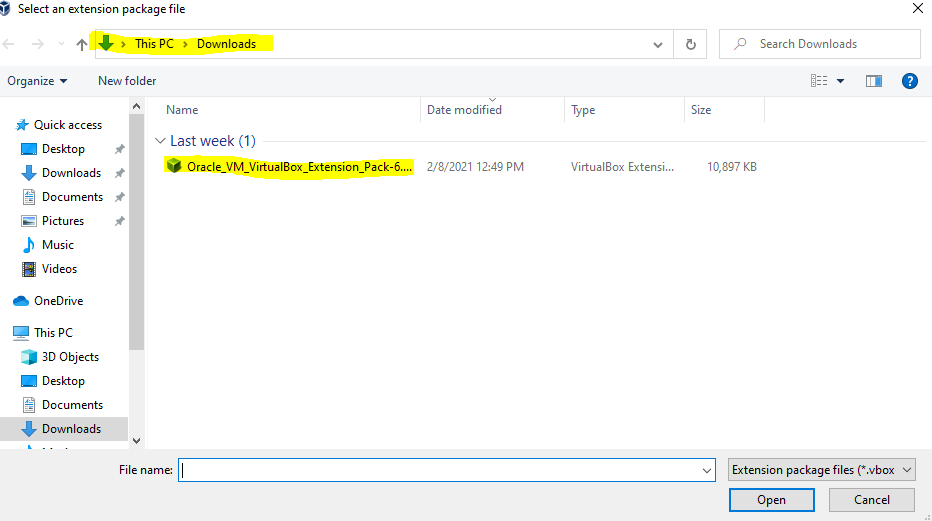
d) Avataan asennettu virtualbox sovellus ja menen Preferences>Extensions ikkuna. Siella ikonilla  klikkaamalla haetaan ladattu Oracle\_VM\_VirtualBox\_Extension\_Pack-6.1.18.vbox-extpack ja se liitan.



Kuva 5: Preferences tai Asetukset työkalu



Kuva 6: Klikka Extensions + nappi



Kuva 7: paikanna paketti ja valitsen

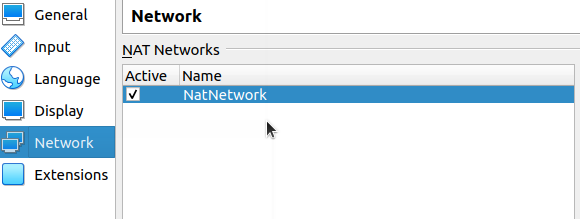
Virtulbox on valmiina, nyt tässä projektissa luodaan omaverkko seuravaksi.

1. Luodaan verkko Virtualbox: ssa
2. File-->Preferences ja Network--> ikonilla lisätään verkko.

Graphical user interface, text, application

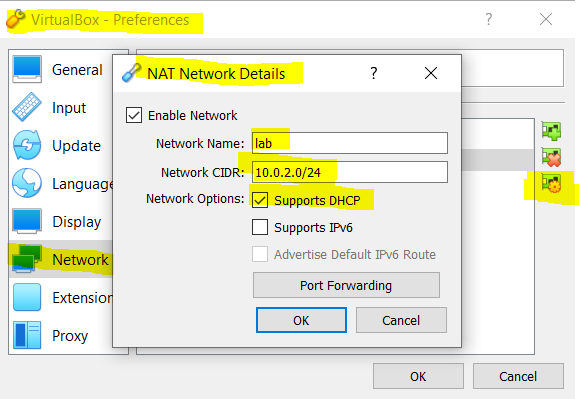
Description automatically generated

Kuva 8: Valitsen Network eli verkko asetukset



Kuva 9: NatNetwork nimeinnen verkko synty oletuksesti.

1. Nyt oikealla (hiiri) klikkaamalla ”NatNetwork” pällä saada uuden ikkuna sitten vaihdetaan nimi lab:ikisen ja Network CIDR laitan haluttu verkko osoiteetta. Olen jaanyt oletuksena.



Kuva 10: haluttu verkon luonti



Kuva 11: Virtual boxissa mahtua verkkoa ja niiden reittiä.

Verkko on luotu. Luotu verkko on sellainen, että se toimi virtuaalikoneiden joukossa.

Liitetty tietokoneita tässä verkossa voi kommunikoida, ihan normallisti kuten fyysinen kytkimilla tehdän. Virtulabox sovellus voi sisältää virtuaaliverkkokytkin ja monet käyttöjärjestelmät.

1. Haetaan netista ne alla oleva käyttöjärjestelmän .iso tiedosto ja niiden asennuksen jälkeen jossa koneessa asennetaan sovellukset.

* Windows 10 (Virtualbox:ssa)

1. Haetaan and asennetaan Chrome, wirshark, FileZilla-client.

* Ubuntu (Virtualbox:ssa)

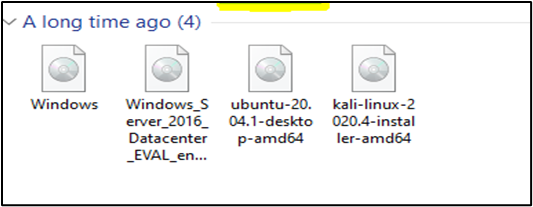
1. asennetaan apache2
2. asennetaan wordpress

* Kali (Virtualbox:ssa)

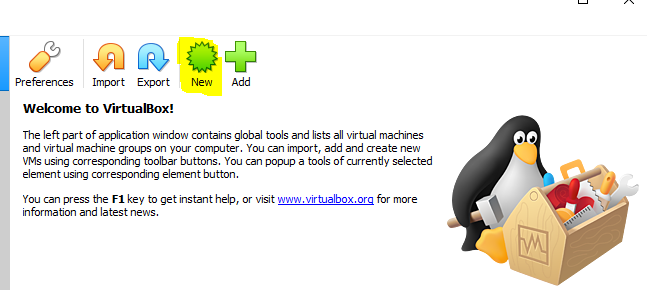
1. Kali: ssa on sisällä rakennettu tarvitseva työkalua NMAP
2. Lisäksi asennetaan bettercap
3. Seth työkalu haetaan github:lta
4. Wireshark

* Windows 2016 (Virtualbox: ssa)

1. FTP-Server/Filezilla server
2. RDP - etäyhteys käytössä
3. ADDS, DHCP jne.
4. Asennan nyt yhden järjestelmän viitteitä varten. Esimerkiksi, asennan Windows 10: n. Olen haettu ja ladattu kaiket tarvitseva järjestelmät .iso tiedostona.

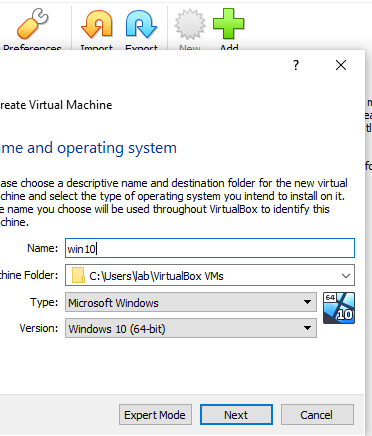


Kuva 12: .iso tiedosto ladattu netista

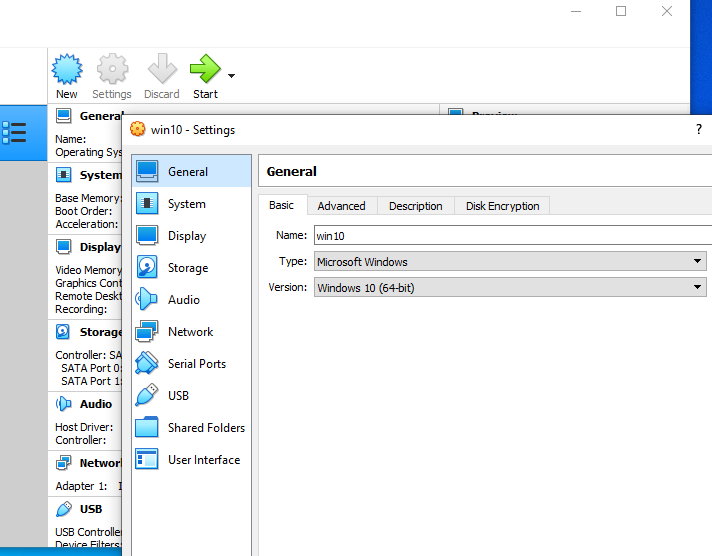
1.  klikkaus New ikoni lla

Kuva 13: Uusi virtuaali kone

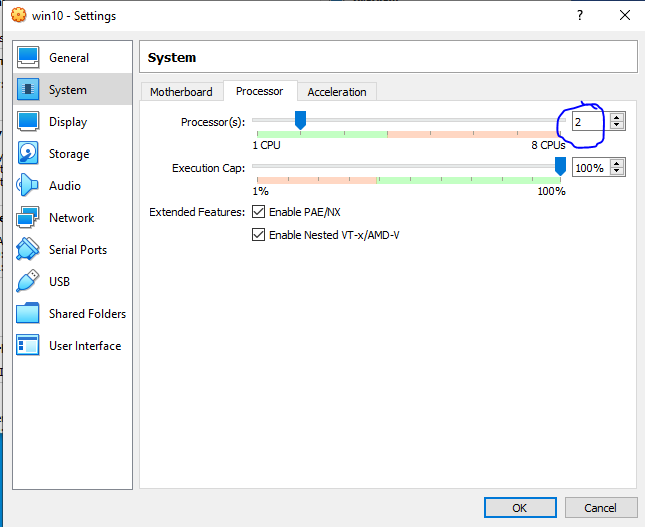
1. Virtuaali konen Kuvausta



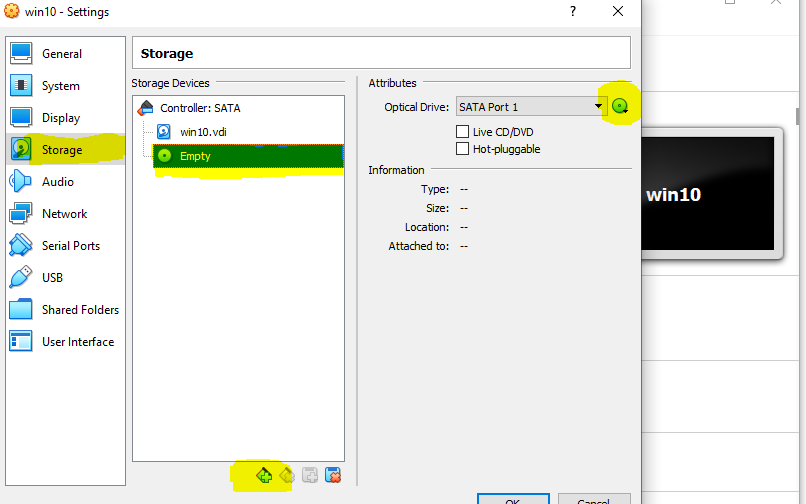
Kuva 14: Laitan konen nimi ja valitsen Type (linux tai windows) ja versio

1. Luotu virtuaalikoneen asetukset

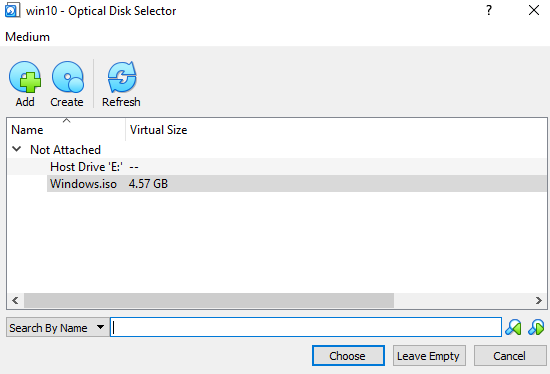
Kuva 15: Virtuaali konen asetukset

1. Tästä voi vaihtaa RAM-muistin määrä ja suoritimen määrä.

Kuva 16: valitsen 2 prosessori

1. Tässä näyttää storage ja konen tarvitse bootable disk eli windows.iso tiedosto.

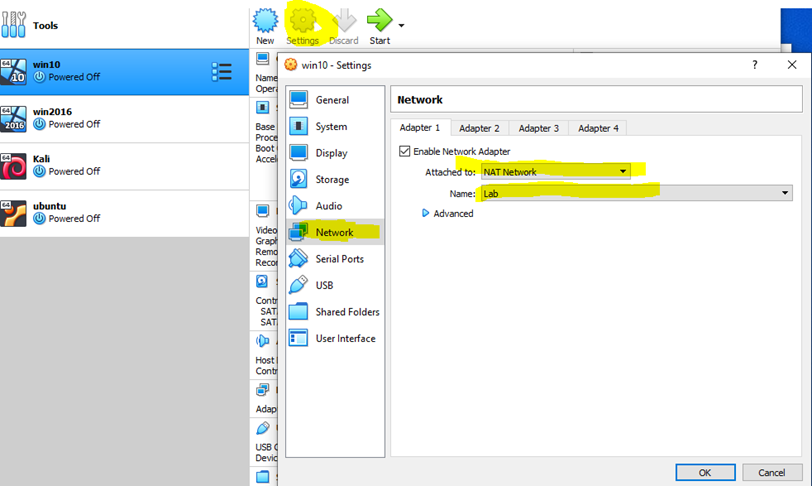
Kuva 17: Tyhjä toinen levy eli ei ole bootable disk tai lähde.

1. Etsin ja valitsen verkosta ladattu windows.iso tiedosto.

Kuva 18: Valitsen windows.iso

Samalla tavalla asennetaan muita virtuaalikoneita. Seuravaksi pitää vaihtaa koneiden verkkon asetkuset. Jokanen kone pitää olla lab verkossa.

1. Yhdistetään kaiket virtuallikoneet lab verkokseen.

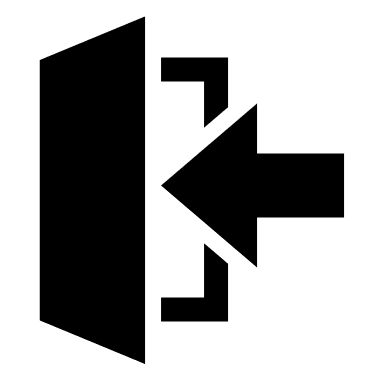


Virtualit koneiden IP osoitteet, kytketty Natnetwork labiseen.

|  |  |  |  |
| --- | --- | --- | --- |
| Hosts | IP-Osoite | Gateway | MAC-osoite |
| Kali | 10.0.2.6/24 | 10.0.2.1 | 08-00-27-ab-08-1c |
| Ubuntu | 10.0.2.15/24 | 10.0.2.1 | 08-00-27-ab-08-3d |
| Win 2016 | 10.0.2.4/24 | 10.0.2.1 | 50-16-d8-b1-fe-10 |
| win 10 | 10.0.2.5/24 | 10.0.2.1 | 98-22-cf-19-6b-55 |

Fyysisen isäntä kone>> Käyttöjärjestelmä: Windows 10 >> IP: 10.17.242.163/24 >> Gateway: 10.17.242.1

Käytännöllinen laboratorio on valmiina.



1. Tässä vaiheessa tutkitaan, että luotu laboratorio on toimiva.

Seuravaksi suoritan MITM-hyökkäyksen. Etätyöpöytäyhteys-RDP:n kirjautumistiedot hakemisia.

1. Käytettävä työkalua Seth, se haetaan GitHubilta.
2. Kalissa avataan konsoli ja annetaan ala oleva kommenttia
3. git clone <https://github.com/SySS-Research/Seth.git>
4. cd Seth
5. win10 koneella komento rivillä(cmd) laitan ”arp -a” kommentti.

|  |  |  |
| --- | --- | --- |
| IP | Mac-osoite | Kone |
| 10.0.2.4 | 50-16-d8-b1-fe-10 | Palvelin |
| 10.0.2.6 | 08-00-27-ab-08-1c | Kali |

Table

Description automatically generatedJos nyt win10 kone (10.0.2.5 ja 98-22-cf-19-6b-55) lähettää datapaketti palvelin (10.0.2.4 ja 50-16-d8-b1-fe-10) suuntaan. Ethernet Frame

Kuva 19: Ethernet Frame oikea suuntaan

1. Kali-Konsolilla sudo ./seth.sh eth0 10.0.2.6 10.0.2.5 10.0.2.4

Text

Description automatically generated

Kuva 20: Mac on muutettu, hyödynnetty arp-cache ja odottele SYN-pakettia

1. Nyt uudelleen tarkistan arp-a taulukko win10 koneella. Se näytä eri, kuin viimeisen.

|  |  |  |
| --- | --- | --- |
| IP | Mac-osoite | Kone |
| 10.0.2.4 | 08-00-27-ab-08-1c | Palvelin |
| 10.0.2.6 | 08-00-27-ab-08-1c | Kali |

Kali ja palvelimen Mac osoitteetta ovat samaa eli win10 koneen arp-cache on muutettu.

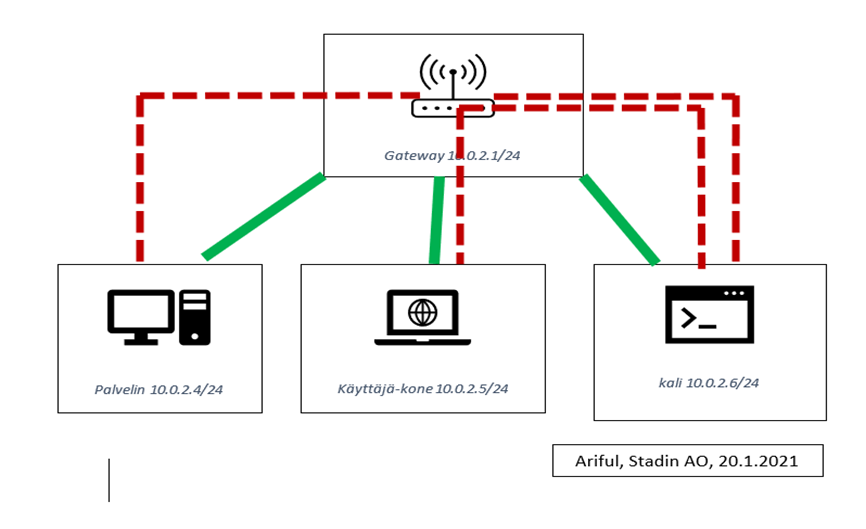
Win10 koneesta lähetettävissä paketin mac-header vaihdettu.

Table

Description automatically generated

Kuva 21: Kuva 8: Ethernet Frame Kali suuntaan

Mies välissä -hyökkäys ([engl.](https://fi.wikipedia.org/wiki/Englannin_kieli) man-in-the-middle attack, lyhenne MITM), [Lisä tietoja Wikipediassa](https://fi.wikipedia.org/wiki/Mies_välissä_-hyökkäys)



Kuva 22: Punaisia pisteviivaa tarkoittaa MITM yhteys.

1. Windows 10 koneella avataan rdp-client ja laitetaan palvelimen

Graphical user interface, text, application, email

Description automatically generated

Kuva 23: Käyttäjänimi ja rdp-isännän IP-osoite.

1. Text

   Description automatically generated with low confidenceSeth on löydetty käyttäjänimi: lk510 ja koneennimi: win-10.

Kuva 24: Käyttäjä ei laittanut salasana.

1. Kun käyttäjä laita salasana. Seurvaksi tulee varoitus ilmoitus . Ei pääse suoran RDP-Palvelimen.

Graphical user interface, application

Description automatically generated

Kuva 12: salasana menossa

1. Graphical user interface, text, application, email

   Description automatically generated Windows näyttää varoitus ilmoitus, mutta yleensä käyttäjä sivuuttaa.

Kuva 25: väärennetty palvelin certificate

1. Seuravaksi Seth löydä salasana: stadin2021 ihan selkeä kielellä (TEXT).

Text

Description automatically generated

Kuva 26: käyttäjä ja Salasana

Verkossa on tonnia työkaluja. Sieltä voi hakea ja joku voi pelata. Jos joku halua olla hakkeri, ei tarvitaan paljon tekniikan taitoa. Joskus se tehdään vain huvin vuoksi. Jonkun hauskaa voi tuoda itkeä muille.

Nykyään tietotekniikka on jotain erittäin tärkeää. Kun kehitämme tekniikkaa, sama aika meidän pitäisi myös kehittää etiikkaa.

Ariful Islam, Opiskelija

Tieto- ja tietoliikennetekniikan perustutkinto.

Stadin ammattiopisto, Sturenkatu.

[islaari@edu.hel.fi](mailto:islaari@edu.hel.fi) [// arif.js@gmail.com](mailto://%20arif.js@gmail.com)

20.1.2021 Helsinki