

Opiskelija
Lauri Partinen
Kyberturvallisuus
ktkt23sp

Tehtävän nimi

17.11.2025

Penetraatiotestaus
Marko Oras

Viikkotehtävä 8

Raportin aiheena on tunnistaa oman kotiverkon haavoittuvuuksia. Raportissa on käytössä hotspot verkko mobiililaitteesta, joka jakaa yhteyttä muihin laitteisiin. Asun kerrostalossa, jossa on monia eri Wifi verkkoja, joita voi skannata.

Kotiverkon turvallisuus on henkilökohtaisten tietojen, yksityisyyden turvaamisen ja talouden toiminnan kannalta kriittistä. Käytän itse puhelimen hotspot yhteyttä, koska en ole kokenut tarvitsevani erillistä Wifi verkkoa.

Hotspotin yleisiä haavoittuvuuksia ovat. Heikko salasana helpottaa hyökkääjän käyttämään yhteyttä. Salauksen puute tai heikkous. Vanhentuneet suojausprotokollat esimerkiksi Wep, joka on harvinainen nykypuhelimissa enää. Nykyisin laitteet käyttävät WPA2 tai WPA3. Hotspotin jatkuva päällä olo mahdollistaa verkon ulkopuolisen tarkkailun. Mac-osoite on jatkuvasti nähtävillä.

Toimenpiteet netin turvallisuuden kannalta

- salasanan vahvistaminen
- salausprotokollien päivittäminen WPA2->WPA3
- SSID: Poista oma nimi hotspot verkon nimestä
- Pidä käyttöjärjestelmä ajan tasalla
- Poista tuntemattomat laitteet pois

Kuvakaappaus windows network asetuksista. Antaa hotspotin ip-osoitteen, mac-osoitteen

```

SSID:                               Lauri's Galaxy S23
Protocol:                           Wi-Fi 4 (802.11n)
Security type:                       WPA2-Personal
Manufacturer:                       Intel Corporation
Description:                         Intel(R) Wi-Fi 6E AX211 160MHz
Driver version:                      23.120.0.3

Network band (channel):              2.4 GHz (1)
Aggregated link speed (Receive/
Transmit):                           144/144 (Mbps)
IPv6 address:                        2001:14bb:11e:4555:5221:52a3:eb0b:5493
Link-local IPv6 address:              fe80::344:f062:371b:4ead%5
IPv6 default gateway:                 fe80::ccb9:45ff:fe69:666d%5
IPv6 DNS servers:                     2001:14bb:11e:4555::dd (Unencrypted)
IPv4 address:                        10.245.240.183
IPv4 DNS servers:                     10.245.240.147 (Unencrypted)
Physical address (MAC):                D4:F3:2D:20:4E:55

```

netsh wlan show networks mode=bssid saadan lisätietoa verkosta esimerkiksi signaalin laatu.

```

SSID 9 : Lauri's Galaxy S23
  Network type           : Infrastructure
  Authentication         : WPA2-Personal
  Encryption             : CCMP
  BSSID 1                : ce:b9:45:69:66:6d
    Signal               : 99%
    Radio type           : 802.11ac
    Band                  : 2.4 GHz
    Channel               : 1
    QoS MSCS Supported   : 0
    QoS Map Supported     : 0
    Basic rates (Mbps)   : 1 2 5.5 11
    Other rates (Mbps)   : 6 9 12 18 24 36 48 54

```

Lisäsin mielenkiinnosta arp-välimuistista kuvakaappauksen. Arp yhdistää ip-osoitteet mac-osoitteisiin. Tulosteesta näkyy hotspot verkko. Verkossa on vain

yksi dynamic-laite 10.254.240.147. Jos olisi monta dynamic-osoitettta, se voisi tarkoittaa joku muu on verkossa kiinni.

```
C:\Users\35845>arp -a
```

```
Interface: 10.245.240.183 --- 0x5
```

Internet Address	Physical Address	Type
10.245.240.147	ce-b9-45-69-66-6d	dynamic
10.245.240.255	ff-ff-ff-ff-ff-ff	static
224.0.0.22	01-00-5e-00-00-16	static
224.0.0.251	01-00-5e-00-00-fb	static
224.0.0.252	01-00-5e-00-00-fc	static
239.255.255.250	01-00-5e-7f-ff-fa	static
255.255.255.255	ff-ff-ff-ff-ff-ff	static

```
Interface: 192.168.137.1 --- 0x10
```

Internet Address	Physical Address	Type
192.168.137.255	ff-ff-ff-ff-ff-ff	static
224.0.0.22	01-00-5e-00-00-16	static
224.0.0.251	01-00-5e-00-00-fb	static
224.0.0.252	01-00-5e-00-00-fc	static
239.255.255.250	01-00-5e-7f-ff-fa	static

```
Interface: 192.168.159.1 --- 0x16
```

Internet Address	Physical Address	Type
192.168.159.255	ff-ff-ff-ff-ff-ff	static
224.0.0.22	01-00-5e-00-00-16	static
224.0.0.251	01-00-5e-00-00-fb	static
224.0.0.252	01-00-5e-00-00-fc	static
239.255.255.250	01-00-5e-7f-ff-fa	static

ipconfig, jolla saadaan verkon ip-osoite

```
Wireless LAN adapter Wi-Fi:
```

```

Connection-specific DNS Suffix . : 
IPv6 Address. . . . . : 2001:14bb:11e:4555:5221:52a3:eb0b:5493
Temporary IPv6 Address. . . . . : 2001:14bb:11e:4555:e93c:c051:f6d4:2434
Link-local IPv6 Address . . . . . : fe80::344:f062:371b:4ead%5
IPv4 Address. . . . . : 10.245.240.183
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : fe80::ccb9:45ff:fe69:666d%5
                             10.245.240.147

```

nmap skannaus verkosta. nmap 10.245.240.183.

```

C:\Users\35845>nmap 10.245.240.183
Starting Nmap 7.98 ( https://nmap.org ) at 2025-11-17 20:42 +0200
Nmap scan report for 10.245.240.183
Host is up (0.000020s latency).
Not shown: 995 closed tcp ports (reset)
PORT      STATE SERVICE
135/tcp    open  msrpc
139/tcp    open  netbios-ssn
445/tcp    open  microsoft-ds
902/tcp    open  iss-realsecure
912/tcp    open  apex-mesh

```

nmap -A 10.245.240.183. Skannaus tarjoaa yksityiskohtaisempaa tietoa. Käyttöjärjestelmän tunnus, palveluversio, skriptien tulokset ja traceroute.

```

TCP/IP fingerprint:
OS: SCAN(V=7.98%E=4%D=11/17%OT=135%CT=1%CU=37302%PV=Y%DS=0%DC=L%G=Y%TM=691B6
OS: D3B%P=i686-pc-windows-windows)SEQ(SP=100%GCD=1%ISR=105%TI=I%CI=I%II=I%SS
OS: =S%TS=A)SEQ(SP=102%GCD=1%ISR=10D%TI=I%CI=I%II=I%SS=S%TS=A)SEQ(SP=106%GCD
OS: =1%ISR=105%TI=I%CI=I%II=I%SS=S%TS=A)SEQ(SP=108%GCD=1%ISR=10A%TI=I%CI=I%I
OS: I=I%SS=S%TS=A)SEQ(SP=FC%GCD=1%ISR=108%TI=I%CI=I%II=I%SS=S%TS=A)OPS(O1=MF
OS: FD7NW8ST11%O2=MFFD7NW8ST11%O3=MFFD7NW8NNT11%O4=MFFD7NW8ST11%O5=MFFD7NW8S
OS: T11%O6=MFFD7ST11)WIN(W1=FFFF%W2=FFFF%W3=FFFF%W4=FFFF%W5=FFFF%W6=FFFF)ECN
OS: (R=Y%DF=Y%T=80%W=FFFF%O=MFFD7NW8NNS%CC=N%Q=)T1(R=Y%DF=Y%T=80%S=0%A=S+F=
OS: AS%RD=0%Q=)T2(R=Y%DF=Y%T=80%W=0%S=Z%A=S+F=AR%O=%RD=0%Q=)T3(R=Y%DF=Y%T=80
OS: %W=0%S=Z%A=0%F=AR%O=%RD=0%Q=)T4(R=Y%DF=Y%T=80%W=0%S=A%A=0%F=R%O=%RD=0%Q=
OS: )T5(R=Y%DF=Y%T=80%W=0%S=Z%A=S+F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=80%W=0%S=A%
OS: A=0%F=R%O=%RD=0%Q=)T7(R=Y%DF=Y%T=80%W=0%S=Z%A=S+F=AR%O=%RD=0%Q=)U1(R=Y%
OS: DF=N%T=80%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=Z%RUCK=G%RUD=G)IE(R=Y%DFI=N%T=
OS: 80%CD=Z)

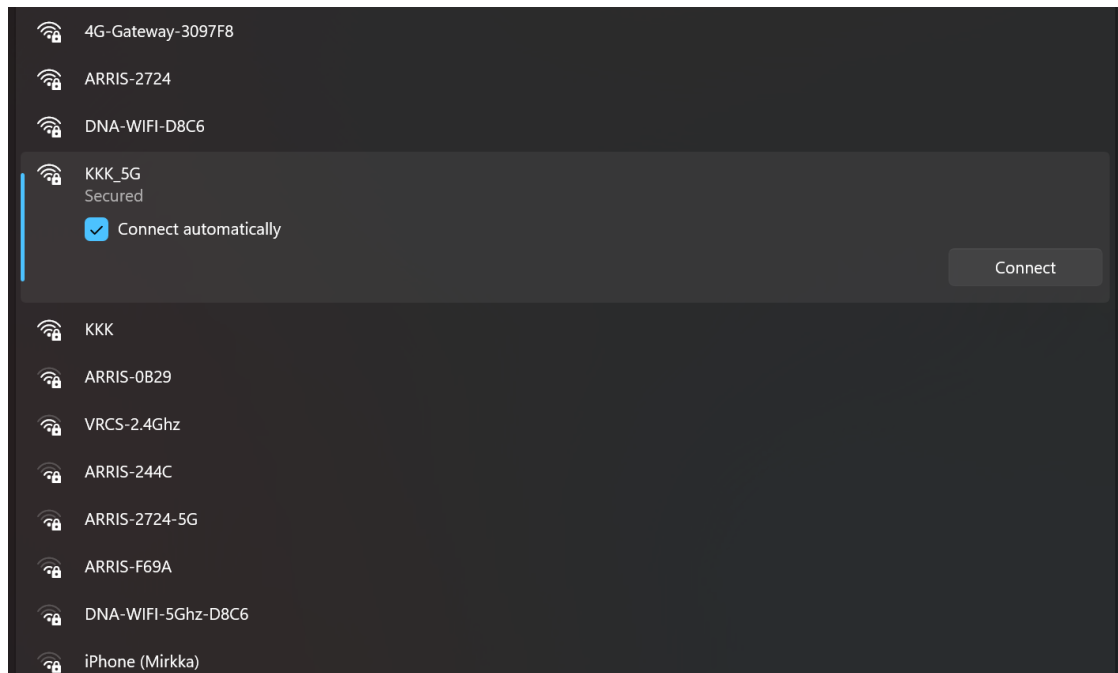
Network Distance: 0 hops
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_ smb2-security-mode:
|   3.1.1:
|_   Message signing enabled but not required
|_ smb2-time:
|   date: 2025-11-17T18:45:04
|_   start_date: N/A

```

Skannauksen perusteella turvallisuutta voisi parantaa tarkistamalla palomuurisäännöt ja rajoittaa pääsyä.

Verkot kerrostalossa, jossa asun.



netsh wlan show networks mode=bssid kommennolla saadaan. SSID eli verkon nimi. BSSID: reitittimen mac-osoite. Todennus WPA2 standardi ja WPA3 uudempi versio. Salaus AES. Signaalin laatu. Channel: kanava, jolla verkko toimii.

```
C:\Users\35845>netsh wlan show networks mode=bssid
```

```
Interface name : Wi-Fi
```

```
There are 10 networks currently visible.
```

```
SSID 1 :
```

```

Network type           : Infrastructure
Authentication         : WPA3-Personal
Encryption             : CCMP
BSSID 1               : 46:95:ce:f6:82:66
    Signal             : 26%
    Radio type         : 802.11ax
    Band               : 2.4 GHz
    Channel            : 6
    Details            : (H2E supported)
    QoS MSCS Supported : 0
    QoS Map Supported  : 0
    Basic rates (Mbps) : 1 2 5.5 6 11 12 24
    Other rates (Mbps) : 9 18 36 48 54

```

```
SSID 2 : DNA-WIFI-D8C6
```

```

Network type           : Infrastructure
Authentication         : WPA3-Personal
Encryption             : CCMP
BSSID 1               : c8:ea:f8:eb:d8:c6
    Signal             : 57%
    Radio type         : 802.11ac
    Band               : 5 GHz
    Channel            : 100
    Details            : (H2E Not supported)
    QoS MSCS Supported : 0
    QoS Map Supported  : 0
    Basic rates (Mbps) : 6 12 24
    Other rates (Mbps) : 9 18 36 48 54

```

```

SSID 3 : 4G-Gateway-3097F8
  HESSID : b8:d4:bc:34:97:f8
  Network type : Infrastructure
  Authentication : WPA3-Personal
  Encryption : CCMP
  BSSID 1 : b8:d4:bc:34:97:f8
    Signal : 70%
    Radio type : 802.11ac
    Band : 5 GHz
    Channel : 52
    Details : (H2E Not supported)
    Bss Load:
      Connected Stations: 0
      Channel Utilization: 1 (0 %)
      Medium Available Capacity: 31250 (1000000 us/s)
    QoS MSCS Supported : 0
    QoS Map Supported : 0
    Basic rates (Mbps) : 6 12 24
    Other rates (Mbps) : 9 18 36 48 54
  BSSID 2 : b8:d4:bc:30:97:f8
    Signal : 83%
    Radio type : 802.11n
    Band : 2.4 GHz
    Channel : 8
    Details : (H2E Not supported)
    QoS MSCS Supported : 0
    QoS Map Supported : 0
    Basic rates (Mbps) : 1 2 5.5 11
    Other rates (Mbps) : 6 9 12 18 24 36 48 54

```

SSID 4 : ARRIS-0B29

```

Network type           : Infrastructure
Authentication         : WPA2-Personal
Encryption             : CCMP
BSSID 1                : 60:d2:48:aa:c9:cc
    Signal             : 67%
    Radio type         : 802.11n
    Band               : 2.4 GHz
    Channel            : 6
    QoS MSCS Supported : 0
    QoS Map Supported  : 0
    Basic rates (Mbps) : 1 2 5.5 6 11 12 24
    Other rates (Mbps) : 9 18 36 48 54

```

SSID 5 : KKK_5G

```

Network type           : Infrastructure
Authentication         : WPA2-Personal
Encryption             : CCMP
BSSID 1                : 2c:99:24:37:6a:77
    Signal             : 83%
    Radio type         : 802.11ac
    Band               : 5 GHz
    Channel            : 36
    QoS MSCS Supported : 0
    QoS Map Supported  : 0
    Basic rates (Mbps) : 6 12 24
    Other rates (Mbps) : 9 18 36 48 54

```

```

SSID 5 : KKK_5G
  Network type      : Infrastructure
  Authentication    : WPA2-Personal
  Encryption        : CCMP
  BSSID 1           : 2c:99:24:37:6a:77
    Signal          : 83%
    Radio type      : 802.11ac
    Band            : 5 GHz
    Channel         : 36
    QoS MSCS Supported : 0
    QoS Map Supported  : 0
    Basic rates (Mbps) : 6 12 24
    Other rates (Mbps) : 9 18 36 48 54

SSID 6 : KKK
  Network type      : Infrastructure
  Authentication    : WPA2-Personal
  Encryption        : CCMP
  BSSID 1           : 2c:99:24:37:6a:71
    Signal          : 83%
    Radio type      : 802.11n
    Band            : 2.4 GHz
    Channel         : 6
    QoS MSCS Supported : 0
    QoS Map Supported  : 0
    Basic rates (Mbps) : 1 2 5.5 11
    Other rates (Mbps) : 6 9 12 18 24 36 48 54

```

```

SSID 7 : ARRIS-2724
  Network type           : Infrastructure
  Authentication         : WPA2-Personal
  Encryption             : CCMP
  BSSID 1                : 50:a5:dc:d5:dc:bc
    Signal                : 83%
    Radio type            : 802.11ac
    Band                  : 2.4 GHz
    Channel               : 1
    QoS MSCS Supported   : 0
    QoS Map Supported    : 0
    Basic rates (Mbps)   : 1 2 5.5 6 11 12 24
    Other rates (Mbps)   : 9 18 36 48 54

SSID 8 : ARRIS-2724-5G
  Network type           : Infrastructure
  Authentication         : WPA2-Personal
  Encryption             : CCMP
  BSSID 1                : 50:a5:dc:d5:dc:bd
    Signal                : 38%
    Radio type            : 802.11ac
    Band                  : 5 GHz
    Channel               : 44
    QoS MSCS Supported   : 0
    QoS Map Supported    : 0
    Basic rates (Mbps)   : 6 12 24
    Other rates (Mbps)   : 9 18 36 48 54

```

Verkoista huomioita. Useimmat verkot käyttävät WPA2 tai WPA3 salausta.
Oletussalasanat ovat vaihdettu pois.