Hackerglede

Program

Intro

Gjennomgang av nyttige verktøy

Demo av oppgave 1

Oppgaveløsing

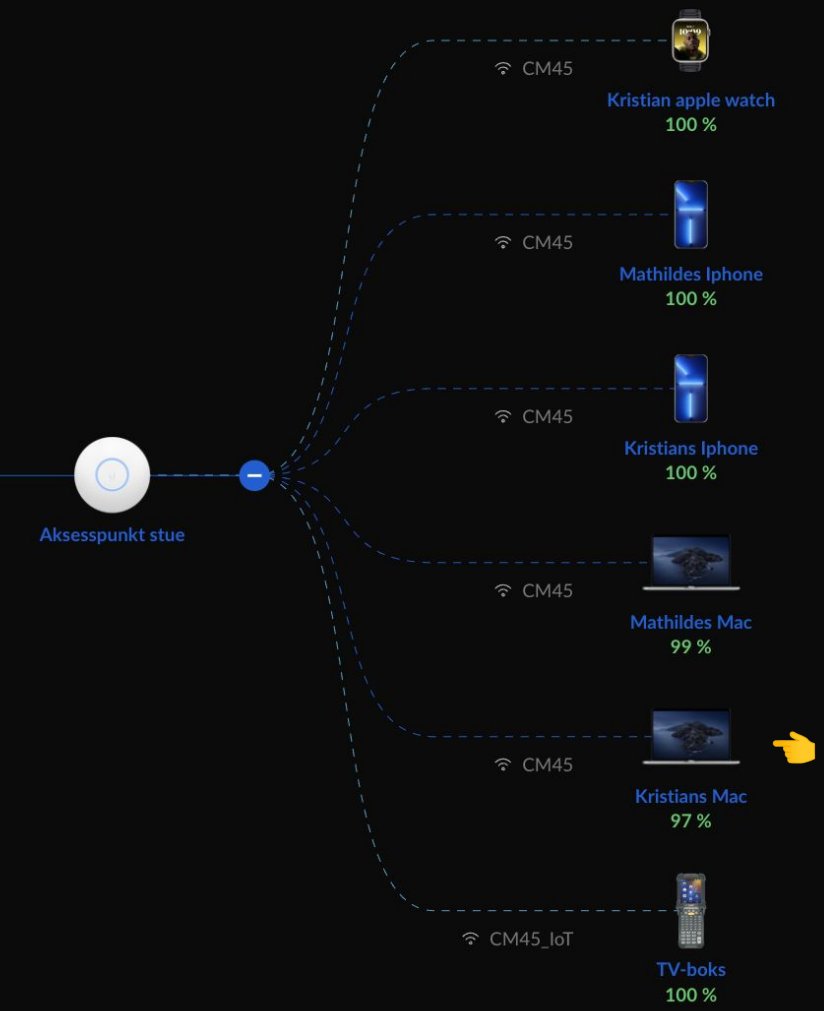
Nmap

Et “must-have” i verktøykassen!

Nettverksscanner

Brukes til å kartlegge et nettverk

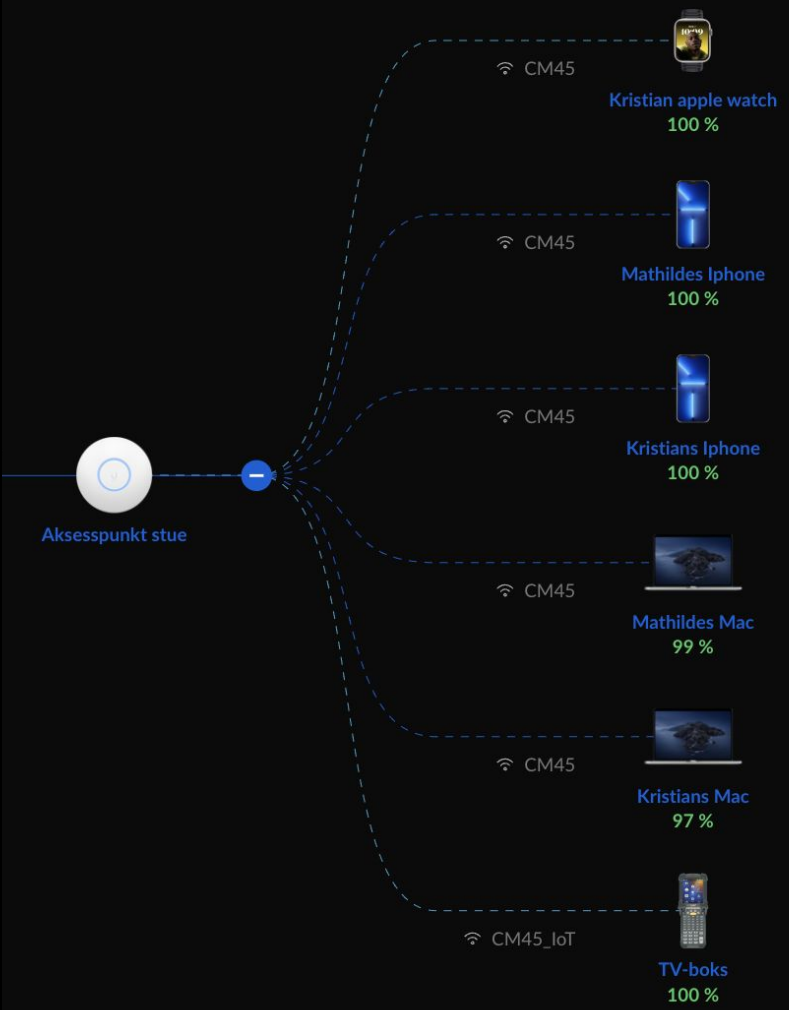
- Hvilke andre enheter finnes på nettverket?
- Hvilke porter svarer de på?
- Hvilket operativsystem kjører de?
- Hvilke sårbarheter har de?




```
~ ifconfig -L en0
en0: flags=8863<UP,BROADCAST,SMART,RUNNING,SIMPLEX,MULTICAST> mtu 1500
        options=6463<RXCSUM,TXCSUM,TSO4,TSO6,CHANNEL_IO,PARTIAL_CSUM,ZEROINVERT_C
        ether f8:ff:c2:36:17:e3
        inet6 fe80::18a7:dbd4:50df:a3b3%en0 prefixlen 64 secured scopeid 0x6
        inet 192.168.1.146 netmask 0xffffff00 broadcast 192.168.1.255
        nd6 options=201<PERFORMNUD,DAD>
        media: autoselect

~ sudo nmap -sn 192.168.1.1-255

Starting Nmap 7.93 ( https://nmap.org ) at 2022-10-20 21:55 CEST
Nmap scan report for unifi.localdomain (192.168.1.1)
Host is up (0.0057s latency).
MAC Address: 70:A7:41:A7:5B:A7 (Ubiquiti Networks)
Nmap scan report for 192.168.1.2
Host is up (0.0036s latency).
MAC Address: 70:A7:41:A7:5B:A7 (Ubiquiti Networks)
Nmap scan report for Kristian-iPhone.localdomain (192.168.1.16)
Host is up (0.42s latency).
MAC Address: AC:49:DB:34:E9:CC (Apple)
Nmap scan report for Aksesspunktstue.localdomain (192.168.1.54)
Host is up (0.0047s latency).
MAC Address: 70:A7:41:CE:E9:90 (Ubiquiti Networks)
Nmap scan report for bekk-mac-02456.localdomain (192.168.1.109)
Host is up (0.27s latency).
MAC Address: 14:7D:DA:D4:C4:BA (Apple)
Nmap scan report for Aksesspunktsoverom.localdomain (192.168.1.186)
Host is up (0.0053s latency).
MAC Address: 70:A7:41:CC:88:34 (Ubiquiti Networks)
Nmap scan report for XBOX.localdomain (192.168.1.204)
Host is up (0.0037s latency).
MAC Address: 4C:3B:DF:36:A4:5C (Microsoft)
Nmap scan report for bekk-mac-2095.localdomain (192.168.1.146)
Host is up.
Nmap done: 255 IP addresses (8 hosts up) scanned in 3.53 seconds
```




```
~ nmap 192.168.1.2
  Starting Nmap 7.93 ( https://nmap.org ) at 2022-10-20 22:10 CEST
  Nmap scan report for 192.168.1.2
  Host is up (0.0029s latency).
  Not shown: 990 filtered tcp ports (no-response)
  PORT     STATE SERVICE
  21/tcp   open  ftp
  22/tcp   open  ssh
  23/tcp   open  telnet
  25/tcp   open  smtp
  80/tcp   open  http
  110/tcp  open  pop3
  445/tcp  open  microsoft-ds
  1433/tcp open  ms-sql-s
  2222/tcp open  EtherNetIP-1
  8000/tcp open  http-alt
```

```
~ nmap 192.168.1.*
~ nmap 192.168.20.2/24
~ nmap -p 22 192.168.20.128
~ nmap -A 192.168.20.128
~ nmap -p- 192.168.20.128
~ nmap -F google.com
```

Gobuster

Verktøy for å «brute force» mapper og filer på en nettside

Leser en ordliste og skriver ut hvilke sider som fins

gobuster dir -u <url> -w <ordliste>

Metasploit

Metasploit framework er et rammeverk med flere tusen exploits man kan bruke ut av boksen

Kan også brukes som et oppslagsverk for kjente svakheter

Startes opp ved å kjøre `msfconsole`

Metasploit - finne en exploit

Man kan slå opp i kjente exploits med

`search <keywords i exploiten>` (alternativt `grep`)

og så bruke en exploit med

`use <nummer på exploit>`

`info <nummer på exploit>` viser info om selve exploiten

Metasploit - bruke en exploit

Når man har valgt exploiten man vil bruke (via `use`) er man i exploit-mode

For å se hvilke parametere man må / kan sette kan man kjøre `show options`

Typisk må man sette info om målet, og kanskje noe om din maskin for å få opprettet en sesjon tilbake

Etter å ha satt nødvendige verdier med `set` (f.eks. `set RHOST 10.0.0.1`) kan man kjøre exploiten med `exploit`

meterpreter

Den typiske payloaden for en RCE-exploit setter opp en terminal-lignende sesjon til den andre maskinen (en meterpreter-sesjon)

Du kan få kjøre programmer på den lokale maskinen (f.eks. et shell / cmd-prompt avhengig av plattform), kikke rundt i mappestruktur, laste ned filer og ta bilder med evt. tilkoblede web-kamera (!)

WPS

Knapp eller PIN-kode istedenfor passord

PIN-kode er 8 siffer

1,5 år hvis autentisering tar 1 sek (10^8 / 2 / 60 / 60 / 24)

WPS - svakhet i protokollen

PIN-kode sjekkes i to deler

Siste siffer er en sjekksum

Det gir 4 + 3 siffer, altså bare 11000 varianter å sjekke

Da er vi nede i 1,5 time i snitt (11000 / 2 / 60 / 60)

WPS - svakhet i implementasjonen

Klienten mottar bevis på at ruteren også vet PIN-koden

Bevis = HMAC-SHA-256(nonce | pin | PKE | PKR)

Hvis vi vet hva nonce er kan vi brute force pin lokalt (offline)

Svakheter i noen rutere i genereringen av nonce

Offline brute force tar noen sekunder