x.

Herrasmieshakkerit, Työkaluvelho, vieraana Joona Hoikkala:

- Käytä aina salasanalompakkoa ja erityisesti passkeytä, koska avainta ei voi vahingossa syöttää väärään paikkaan
- Let's Encrypt muuttanut Internetin salauksia tekemällä siitä helppoa ja ilmaista kaikille
- Certainly työkalu voi kaapata dataa https-pyynnöstä muuttamalla vain yhtä bittiä
- Confused työkalu on tehty tarkastamaan riippuvuuksia, joka on käytännössä ”niin hyvä kuin käyttäjä”. Paljastaa paketinhallintatyökalujen haavoittuvuuksia.

Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains:

- Indikaattori on tiedonpalanen, joka paljastaa tunkeutumisen
    - Atomic, indikaattori, jota ei voi pilkkoa pienempiin palasiin
    - Computed, datasta johdettu indikaattori
    - Behavioral, käyttäytymiseen pohjautuvat indikaattori
- Kill chain vaiheet:
    - Reconnaissance
    - Weaponization
    - Delivery
    - Exploitation
    - Installation
    - Command and Control
    - Actions on Objectives

The Art of Hacking

- Active reconnaissance on vaihe, jossa aletaan lähettää paketteja kohteeseen eli aktiivisesti ”skannamaan” kohdetta
- Tarkkailu on tärkeää, koska siten selvitetään kohteet ja niihin liittyvät mahdolliset heikkoudet
- Metodologia:
    - Port scanning
    - Web service review
    - Vulnerability scanning
- Työkaluja
    - Nmap, port scanning
    - EyeWitness, web servicce review
    - Qualys, network vulnerability scanning
    - Burp Suite, web vulnerability scanning

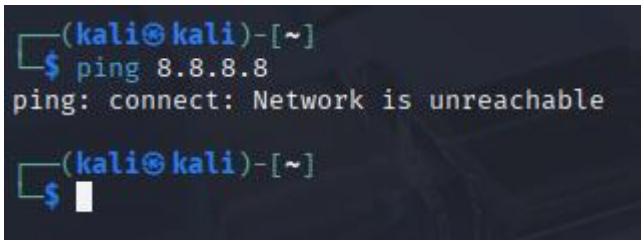
KKO:2003:36

- Tehty porttiskannaus Osuuspankin järjestelmiä vastaan, tuloksia ei ollut tullut
- OP vaati palkkakustannuksia korvauksena tietomurron yrittäjältä
- Poliisi tutkinassa todennut, että IP-osoite kuului tekijälle, jolta oli löydetty porttiskannaukseen käytettävä ohjelma

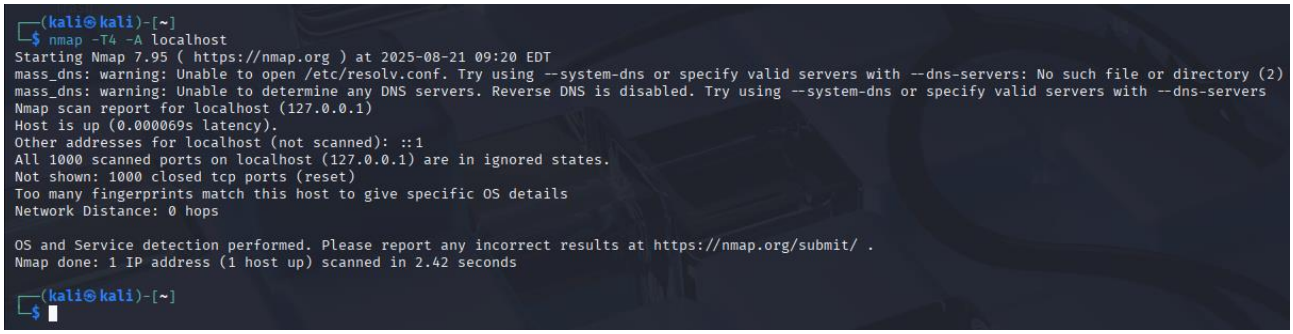
- Hovioikeus muutti käräjäoikeuden päätöksen ja tuomitsi tekijän maksamaan korvauksia
- Korkeinoikeus ei muuttanut hovioikeuden tuomiota, joten porttiskannaus on laiton toimenpide, josta maksetaan vahingonkorvauksia

a. Kali linux versio 2025.2 ja ladattu kali.org nettisivulta.

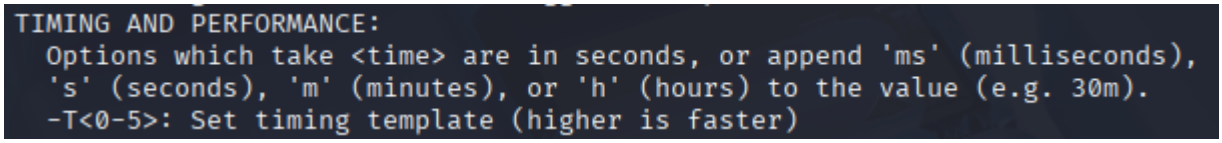
b. Kali kone ei ole verkossa.



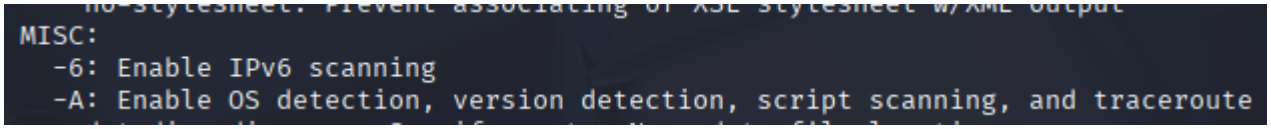
c. Tein porttiskannauksen ja kaikki 1000 porttia ovat kiinni. Komento yritti löytää DNS serverin, ei löytänyt, joten skannasi localhostin IP-osoitteesta 127.0.0.1.



T on timing ja performance:



A parametrillä yritetäänn tunnistaa käyttöjärjestelmän versio.



d. Käynnistetty ssh ja http daemonit tehty uusi porttiskannaus. Nmap löytää ssh portista 22 ja http portista 80.

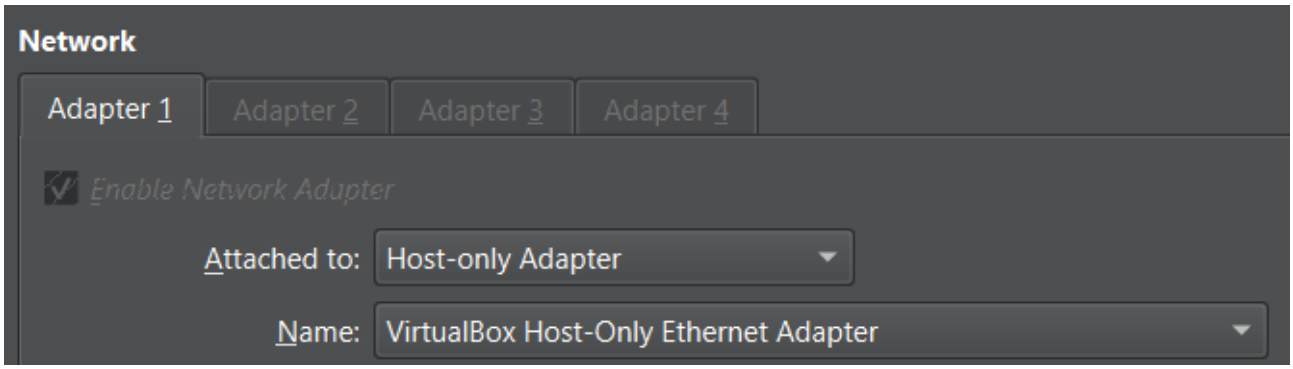
```
┌──(kali㉿kali)-[~]
└─$ nmap -T4 -A localhost
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-21 09:32 EDT
mass_dns: warning: Unable to open /etc/resolv.conf. Try using --system-dns or specify valid servers with --dns-servers: No such file or directory (2)
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for localhost (127.0.0.1)
Host is up (0.000055s latency).
Other addresses for localhost (not scanned): ::1
Not shown: 998 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 10.0p2 Debian 5 (protocol 2.0)
80/tcp open  http    Apache httpd 2.4.63 ((Debian))
|_http-server-header: Apache/2.4.63 (Debian)
|_http-title: Apache2 Debian Default Page: It works
Device type: general purpose
Running: Linux 5.X|6.X
OS CPE: cpe:/o:linux:linux_kernel:5 cpe:/o:linux:linux_kernel:6
OS details: Linux 5.0 - 6.2
Network Distance: 0 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 8.25 seconds

┌──(kali㉿kali)-[~]
└─$
```

e. Asennettu metasploitable geeks for geeks nettisivun ohjeiden mukaan.

f. Aluksi metasploitablen käynnistys ei onnistunut, mutta tajuttuani vaihtaa storage olemassa olevaan metasploitable.vdmk, kone suostui käynnistymään.

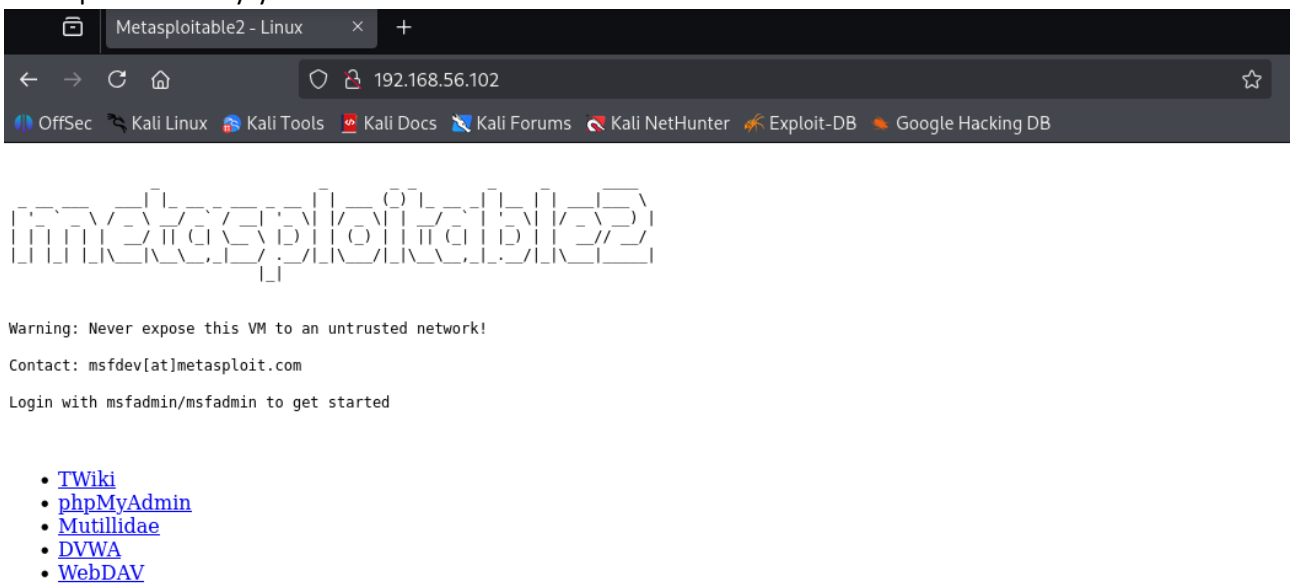


Molemmat koneet ovat host-only adapter tilassa ja löytävät toisensa.

g. Nmap skanni löysi kolme IP-osoitetta 1, 100, 101 ja 102

```
┌──(kali㉿kali)-[~]
└─$ nmap -sn 192.168.56.0/24
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-21 10:48 EDT
mass_dns: warning: Unable to open /etc/resolv.conf. Try using --system-dns or
 specify valid servers with --dns-servers: No such file or directory (2)
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabl
ed. Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 192.168.56.1
Host is up (0.00037s latency).
MAC Address: 0A:00:27:00:00:0F (Unknown)
Nmap scan report for 192.168.56.100
Host is up (0.00017s latency).
MAC Address: 08:00:27:71:AE:E4 (PCS Systemtechnik/Oracle VirtualBox virtual N
IC)
Nmap scan report for 192.168.56.102
Host is up (0.00061s latency).
MAC Address: 08:00:27:09:82:56 (PCS Systemtechnik/Oracle VirtualBox virtual N
IC)
Nmap scan report for 192.168.56.101
Host is up.
Nmap done: 256 IP addresses (4 hosts up) scanned in 1.88 seconds
```

Metasploitable 2 löytyi osoitteesta 192.168.56.102:



Mielenkiintoiset portit:

- 21, FTP portti, käytössä vsftpd 2.3.4, jossa on backdoor command execution haavoittuvuus, jolla hyökkääjä pystyy avaamaan remote shell portissa 6200
- 3306, mySQL 5.0.51, haavoittuvuus, jossa pystyy ohittamaan privilege checki:n
- 8180, apache 5.5, useampia remote code execution haavoittuvuuksia

└─$ nmap -A -T4 -p- 192.168.56.102
Starting Nmap 7.95 (https://nmap.org) at 2025-08-21 10:54 EDT
mass_dns: warning: Unable to open /etc/resolv.conf. Try using --system-dns or specify valid servers with --dns-servers: No such file or directory (2)
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 192.168.56.102
Host is up (0.0034s latency).
Not shown: 65505 closed tcp ports (reset)
PORT STATE SERVICE VERSION
21/tcp open ftp vsftpd 2.3.4
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
| ftp-syst:
| STAT:
| FTP server status:
| Connected to 192.168.56.101
| Logged in as ftp
| TYPE: ASCII
| No session bandwidth limit
| Session timeout in seconds is 300
| Control connection is plain text
| Data connections will be plain text
| vsFTPd 2.3.4 - secure, fast, stable
|_End of status

```
22/tcp    open  ssh        OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
| ssh-hostkey:
|   1024 60:0f:cf:e1:c0:5f:6a:74:d6:90:24:fa:c4:d5:6c:cd (DSA)
|_  2048 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3 (RSA)
23/tcp    open  telnet     Linux telnetd
25/tcp    open  smtp       Postfix smtpd
|_ssl-date: 2025-08-21T14:39:41+00:00; -17m09s from scanner time.
| sslv2:
|   SSLv2 supported
|   ciphers:
|     SSL2_RC2_128_CBC_WITH_MD5
|     SSL2_DES_192_EDE3_CBC_WITH_MD5
|     SSL2_RC4_128_EXPORT40_WITH_MD5
|     SSL2_RC4_128_WITH_MD5
|     SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
|_    SSL2_DES_64_CBC_WITH_MD5
| ssl-cert: Subject: commonName=ubuntu804-
base.localdomain/organizationName=OCOSA/stateOrProvinceName=There is no such thing outside
US/countryName=XX
| Not valid before: 2010-03-17T14:07:45
|_Not valid after:  2010-04-16T14:07:45
|_smtp-commands: metasploitable.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS,
ENHANCEDSTATUSCODES, 8BITMIME, DSN
53/tcp    open  domain     ISC BIND 9.4.2
| dns-nsid:
|_  bind.version: 9.4.2
80/tcp    open  http       Apache httpd 2.2.8 ((Ubuntu) DAV/2)
|_http-server-header: Apache/2.2.8 (Ubuntu) DAV/2
|_http-title: Metasploitable2 - Linux
111/tcp   open  rpcbind    2 (RPC #100000)
| rpcinfo:
|   program version    port/proto  service
|   100000  2          111/tcp   rpcbind
|   100000  2          111/udp   rpcbind
|   100003  2,3,4      2049/tcp   nfs
|   100003  2,3,4      2049/udp   nfs
|   100005  1,2,3      40226/udp   mountd
|   100005  1,2,3      48713/tcp   mountd
|   100021  1,3,4      40397/tcp   nlockmgr
|   100021  1,3,4      49054/udp   nlockmgr
|   100024  1          42148/udp   status
|_  100024  1          57866/tcp   status
139/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn Samba smbd 3.0.20-Debian (workgroup: WORKGROUP)
512/tcp   open  exec       netkit-rsh rexecd
513/tcp   open  login
514/tcp   open  shell      Netkit rshd
1099/tcp  open  java-rmi    GNU Classpath grmiregistry
```

1524/tcp open bindshell   Metasploitable root shell
2049/tcp open nfs   2-4 (RPC #100003)
2121/tcp open ftp   ProFTPD 1.3.1
3306/tcp open mysql   MySQL 5.0.51a-3ubuntu5
| mysql-info:
| Protocol: 10
| Version: 5.0.51a-3ubuntu5
| Thread ID: 10
| Capabilities flags: 43564
| Some Capabilities: LongColumnFlag, Support41Auth, SupportsTransactions,
SwitchToSSLAfterHandshake, SupportsCompression, Speaks41ProtocolNew, ConnectWithDatabase
| Status: Autocommit
|_ Salt: #;>c\"1o_J6j8uh*4e!
3632/tcp open distccd   distccd v1 ((GNU) 4.2.4 (Ubuntu 4.2.4-1ubuntu4))
5432/tcp open postgresql PostgreSQL DB 8.3.0 - 8.3.7
|_ssl-date: 2025-08-21T14:39:41+00:00; -17m09s from scanner time.
| ssl-cert: Subject: commonName=ubuntu804-
base.localdomain/organizationName=OCOSA/stateOrProvinceName=There is no such thing outside
US/countryName=XX
| Not valid before: 2010-03-17T14:07:45
|_Not valid after: 2010-04-16T14:07:45
5900/tcp open vnc   VNC (protocol 3.3)
| vnc-info:
| Protocol version: 3.3
| Security types:
|_   VNC Authentication (2)
6000/tcp open X11   (access denied)
6667/tcp open irc   UnrealIRCd
6697/tcp open irc   UnrealIRCd
8009/tcp open ajp13   Apache Jserv (Protocol v1.3)
|_ajp-methods: Failed to get a valid response for the OPTION request
8180/tcp open http   Apache Tomcat/Coyote JSP engine 1.1
|_http-favicon: Apache Tomcat
|_http-title: Apache Tomcat/5.5
|_http-server-header: Apache-Coyote/1.1
8787/tcp open drb   Ruby DRb RMI (Ruby 1.8; path /usr/lib/ruby/1.8/drb)
40231/tcp open java-rmi   GNU Classpath grmiregistry
40397/tcp open nlockmgr   1-4 (RPC #100021)
48713/tcp open mountd   1-3 (RPC #100005)
57866/tcp open status   1 (RPC #100024)
MAC Address: 08:00:27:09:82:56 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.33
Network Distance: 1 hop
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE:
cpe:/o:linux:linux_kernel

Host script results:
|_smb2-time: Protocol negotiation failed (SMB2)
| smb-os-discovery:
| OS: Unix (Samba 3.0.20-Debian)
| Computer name: metasploitable
| NetBIOS computer name:
| Domain name: localdomain
| FQDN: metasploitable.localdomain
|_ System time: 2025-08-21T10:39:37-04:00
|_clock-skew: mean: 42m54s, deviation: 2h00m02s, median: -17m09s
| smb-security-mode:
| account_used: guest
| authentication_level: user
| challenge_response: supported
|_ message_signing: disabled (dangerous, but default)
|_nbstat: NetBIOS name: METASPLOITABLE, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)

TRACEROUTE
HOP RTT   ADDRESS
1   3.42 ms 192.168.56.102

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 168.78 seconds

Lähteet:

https://www.geeksforgeeks.org/linux-unix/how-to-enable-and-start-ssh-on-kali-linux/

https://linuxconfig.org/kali-http-server-setup

https://www.geeksforgeeks.org/linux-unix/how-to-install-metasploitable-2-in-virtualbox/

https://terokarvinen.com/tunkeutumistestaus/#h1-kybertappoketju

https://www.makeuseof.com/vulnerable-ports-check-when-pentesting/

https://en.wikipedia.org/wiki/DROWN_attack

https://ubuntu.com/security/notices/USN-671-1

https://www.cvedetails.com/cve/CVE-2011-2523