

Cyber practicum 1

```
IP-address Kali Linux: 10.0.2.4
```

```
IP-address Metasploitable : 10.0.2.5
```

- Na het invoeren van

```
nmap -sn 10.0.2.0/24
```

1.1

1.3 Applicatie-, OS-herkenning met nmap

- Appllicatie en versie-identificatie

```
nmap -sV 10.0.2.5
```

PORT	STATE	SERVICE	VERSION
21/tcp	open	ftp	vsftpd 2.3.4
22/tcp	open	ssh	OpenSSH 4.7 p 1 Debian 8 ubuntu 1 (protocol 2.0)
23/tcp	open	telnet	Linux telnetd
25/tcp	open	smtp	Postfix smtpd
53/tcp	open	domain	ISC BIND 9.4.2
80/tcp	open	http	Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp	open	rpcbind	2 (RPC #100000)
139/tcp	open	netbios-ssn	Samba smbd 3. X - 4. X (workgroup: WORKGROUP)
445/tcp	open	netbios-ssn	Samba smbd 3. X - 4. X (workgroup: WORKGROUP)
512/tcp	open	exec	netkit-rsh rexecd
513/tcp	open	login	OpenBSD or Solaris rlogind
514/tcp	open	shell?	
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 5.0.51 a-3 ubuntu 5
5432/tcp	open	postgresql	PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp	open	vnc	VNC (protocol 3.3)
6000/tcp	open	X 11	(access denied)
6667/tcp	open	irc	UnrealIRCd
8009/tcp	open	ajp 13	Apache Jserv (Protocol v 1.3)
8180/tcp	open	http	Apache Tomcat/Coyote JSP engine 1.1

- OS-herkenning

```
sudo nmap -O -v 10.0.2.5
```

Door het gebruik van sudo krijg je meer gebruiksrechten

1.3 Vulnerability-scanning met nmap

```
locate .nse werkt nog niet
```

```
Starting Nmap 7.93 ( https://nmap.org ) at 2023-02-17 03:16 EST
Nmap scan report for 10.0.2.5
Host is up (0.00054 s latency).

PORT      STATE SERVICE VERSION
6667/tcp  open  irc      UnrealIRCd
|_irc-unrealircd-backdoor: Looks like trojaned version of unrealircd. See
http://seclists.org/fulldisclosure/2010/Jun/277
Service Info: Host: irc. Metasploitable. LAN

Service detection performed. Please report any incorrect results at https://nmap.org/submit/
.
Nmap done: 1 IP address (1 host up) scanned in 9.47 seconds
```

Omdat je met sC de scripts vind deze waren eerst nog niet nodig

1.5 Beschermen tegen scannen

1.5.1 uitzetten van services

De http server mist

1.5.2 Afschermen van poorten met een firewall

Alle poorten worden gesloten behalve poort 20 en 80

Er zijn geen poorten zichtbaar behalve poort 20 en 80

1.6 Verdieping (optioneel)