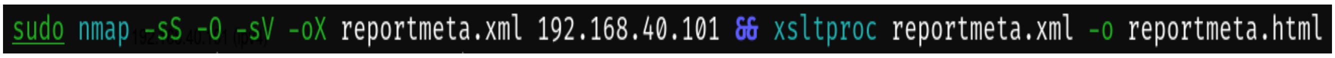
Scansione dei servizi con **nmap**

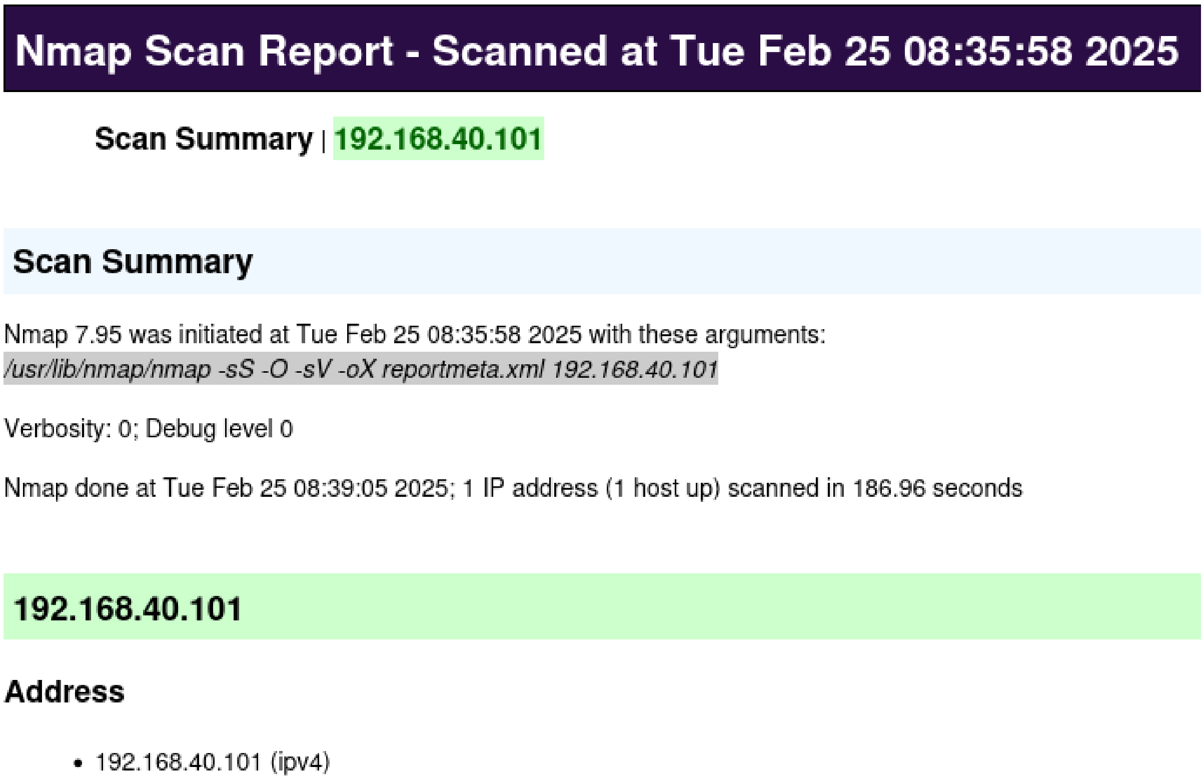
Dal terminale di kali linux eseguiamo il seguente comando per creare un report grazie a nmap e effettuiamo le seguenti scansioni sul target Metasploitable:

- OS fingerprint.
- Syn Scan.
- Version detection.



```
sudo nmap -sS -O -sV -oX reportmeta.xml 192.168.40.101 && xsltproc reportmeta.xml -o reportmeta.html
```

Aprendo il file html avremo il report completo:



Nmap Scan Report - Scanned at Tue Feb 25 08:35:58 2025

Scan Summary | 192.168.40.101

Scan Summary

Nmap 7.95 was initiated at Tue Feb 25 08:35:58 2025 with these arguments:
/usr/lib/nmap/nmap -sS -O -sV -oX reportmeta.xml 192.168.40.101

Verbosity: 0; Debug level 0

Nmap done at Tue Feb 25 08:39:05 2025; 1 IP address (1 host up) scanned in 186.96 seconds

192.168.40.101

Address

- 192.168.40.101 (ipv4)

Ports

The 977 ports scanned but not shown below are in state: **closed**

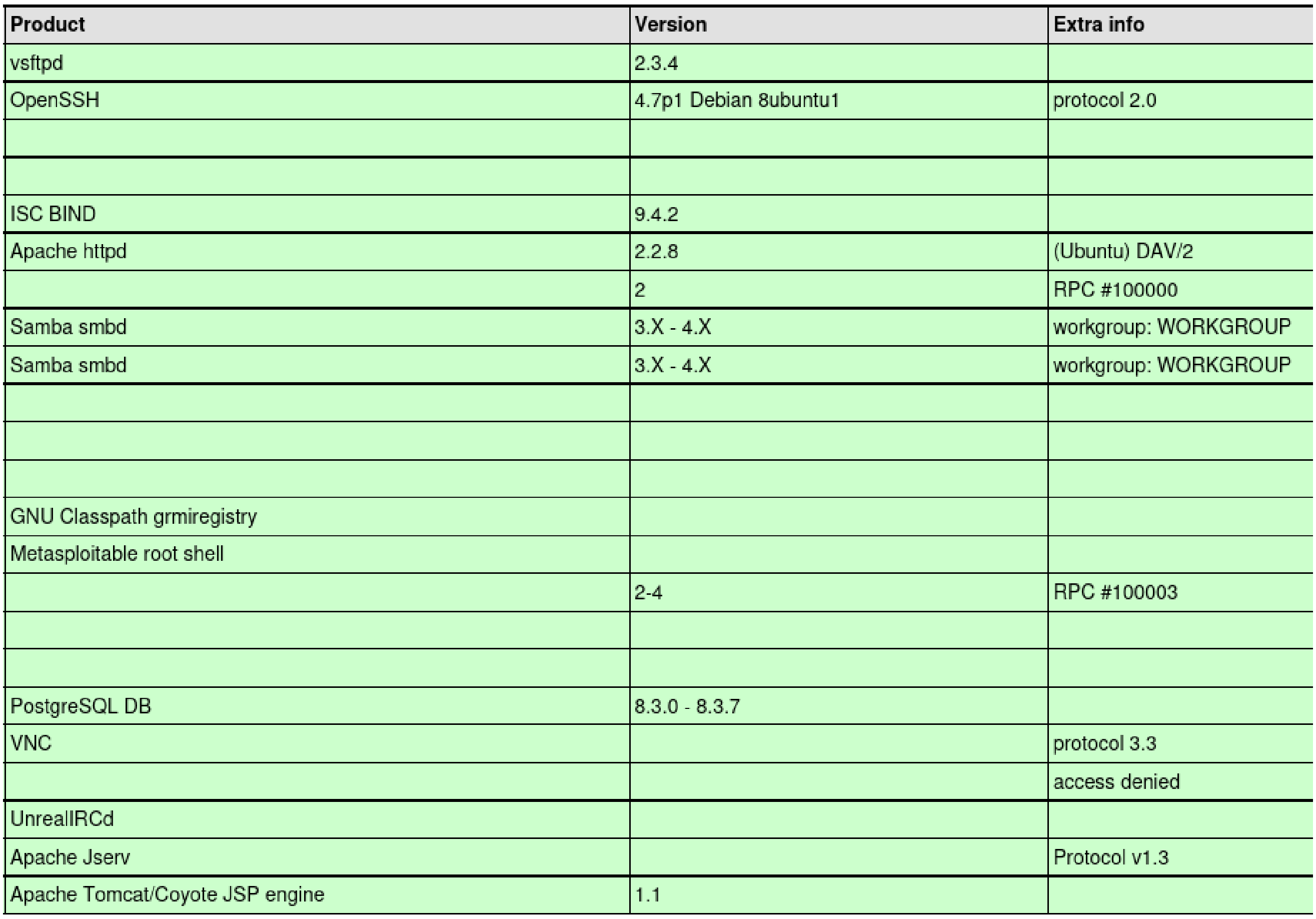
- 977 ports replied with: **reset**

Port		State (toggle closed [0] | filtered [0])	Service
21	tcp	open	ftp
22	tcp	open	ssh
23	tcp	open	telnet
25	tcp	open	smtp
53	tcp	open	domain
80	tcp	open	http
111	tcp	open	rpcbind
139	tcp	open	netbios-ssn
445	tcp	open	netbios-ssn
512	tcp	open	exec
513	tcp	open	login
514	tcp	open	shell
1099	tcp	open	java-rmi
1524	tcp	open	bindshell
2049	tcp	open	nfs
2121	tcp	open	ccproxy-ftp
3306	tcp	open	mysql
5432	tcp	open	postgresql
5900	tcp	open	vnc
6000	tcp	open	X11
6667	tcp	open	irc
8009	tcp	open	ajp13
8180	tcp	open	http

Remote Operating System Detection

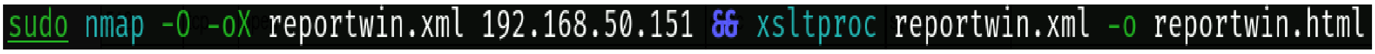
- Used port: **21/tcp** (**open**)
- Used port: **1/tcp** (**closed**)
- Used port: **32785/udp** (**closed**)
- OS match: **Linux 2.6.15 - 2.6.26 (likely embedded)** (**96%**)
- OS match: **Linux 2.6.29** (**96%**)
- OS match: **Linux 2.6.9 - 2.6.27** (**96%**)
- OS match: **Linux 2.4.20** (**95%**)
- OS match: **Linux 2.6.26** (**94%**)
- OS match: **Dell Integrated Remote Access Controller (iDRAC9)** (**94%**)
- OS match: **Linux 2.6.30** (**93%**)
- OS match: **Linux 2.6.16 - 2.6.28** (**93%**)
- OS match: **Linux 2.6.22** (**93%**)
- OS match: **Linux 2.6.24 - 2.6.26** (**92%**)

grazie a **-sV** otteniamo anche i dettagli:

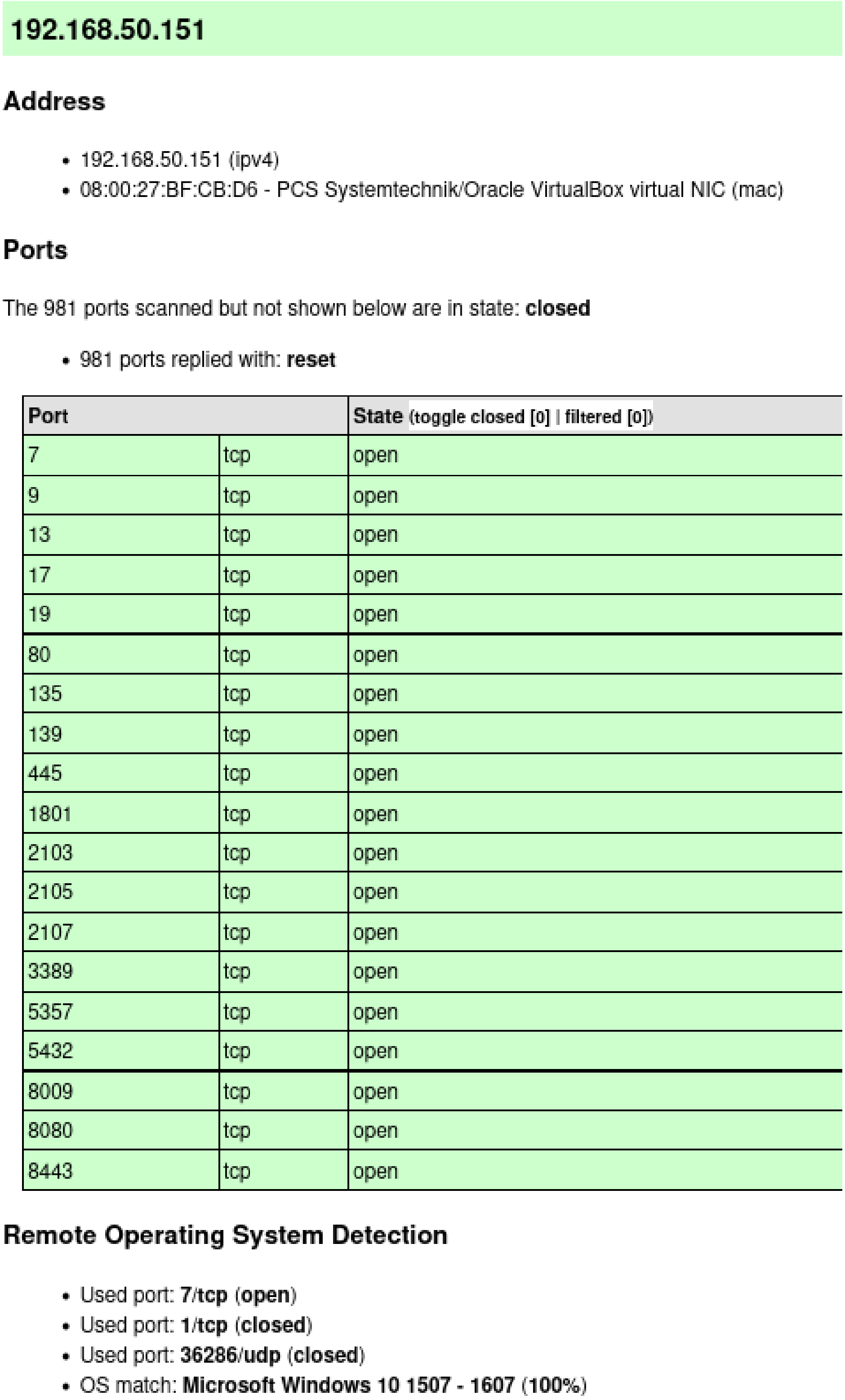


Product	Version	Extra info
vsftpd	2.3.4	
OpenSSH	4.7p1 Debian 8ubuntu1	protocol 2.0
ISC BIND	9.4.2	
Apache httpd	2.2.8	(Ubuntu) DAV/2
	2	RPC #100000
Samba smbd	3.X - 4.X	workgroup: WORKGROUP
Samba smbd	3.X - 4.X	workgroup: WORKGROUP
GNU Classpath grmiregistry		
Metasploitable root shell		
	2-4	RPC #100003
PostgreSQL DB	8.3.0 - 8.3.7	
VNC		protocol 3.3
		access denied
UnrealIRCd		
Apache Jserv		Protocol v1.3
Apache Tomcat/Coyote JSP engine	1.1	

Per **windows** utilizziamo questo comando:



```
sudo nmap -O -oX reportwin.xml 192.168.50.151 && xsltproc reportwin.xml -o reportwin.html
```



192.168.50.151

Address

- 192.168.50.151 (ipv4)
- 08:00:27:BF:CB:D6 - PCS Systemtechnik/Oracle VirtualBox virtual NIC (mac)

Ports

The 981 ports scanned but not shown below are in state: **closed**

- 981 ports replied with: **reset**

Port		**State** (toggle closed [0] | filtered [0])
7	tcp	open
9	tcp	open
13	tcp	open
17	tcp	open
19	tcp	open
80	tcp	open
135	tcp	open
139	tcp	open
445	tcp	open
1801	tcp	open
2103	tcp	open
2105	tcp	open
2107	tcp	open
3389	tcp	open
5357	tcp	open
5432	tcp	open
8009	tcp	open
8080	tcp	open
8443	tcp	open

Remote Operating System Detection

- Used port: **7/tcp** (**open**)
- Used port: **1/tcp** (**closed**)
- Used port: **36286/udp** (**closed**)
- OS match: **Microsoft Windows 10 1507 - 1607** (**100%**)