Cybersecurity

Activity File

Activity File: Zenmap & NSE Scripts

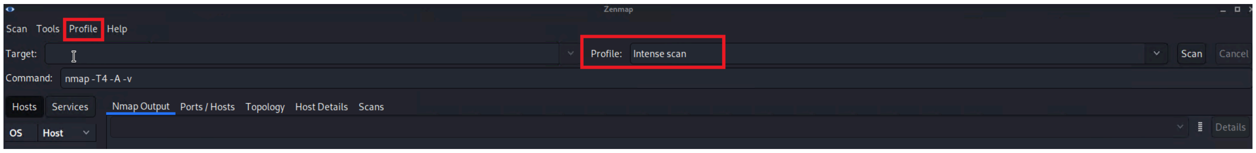
- In this activity, you will continue to play the role of a pen tester conducting an engagement on MegaCorpOne.
- Now that you are on the internal network, you'll get "the lay of the land" by performing scanning.
- You will use Zenmap and NSE scripts to build out a profile and perform a scan on a certain machine on the network.

⚠️ **Reminder:** Don't forget to save your findings, as you will add them to your report on Day 4!

Instructions

1. In Kali, launch Zenmap by typing `zenmap` in the terminal.

2. Ensure that "Intense scan" is selected next to "Profile," as the following image shows:

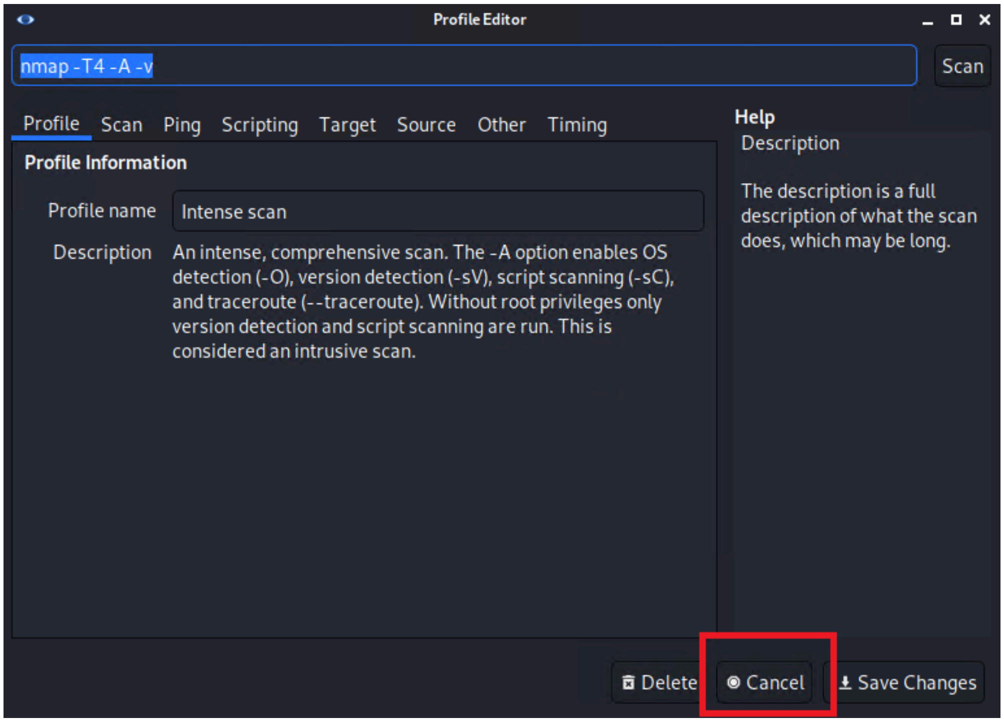


Profile: Intense scan

Command: nmap -T4 -A -v

```
Unset
1. Navigate to "Profile" > "Edit Selected Profile" to read
   about the intense scan profile.
```

3. Click "Cancel," as the following image shows:



nmap -T4 -A -v

Profile Information

Profile name: Intense scan

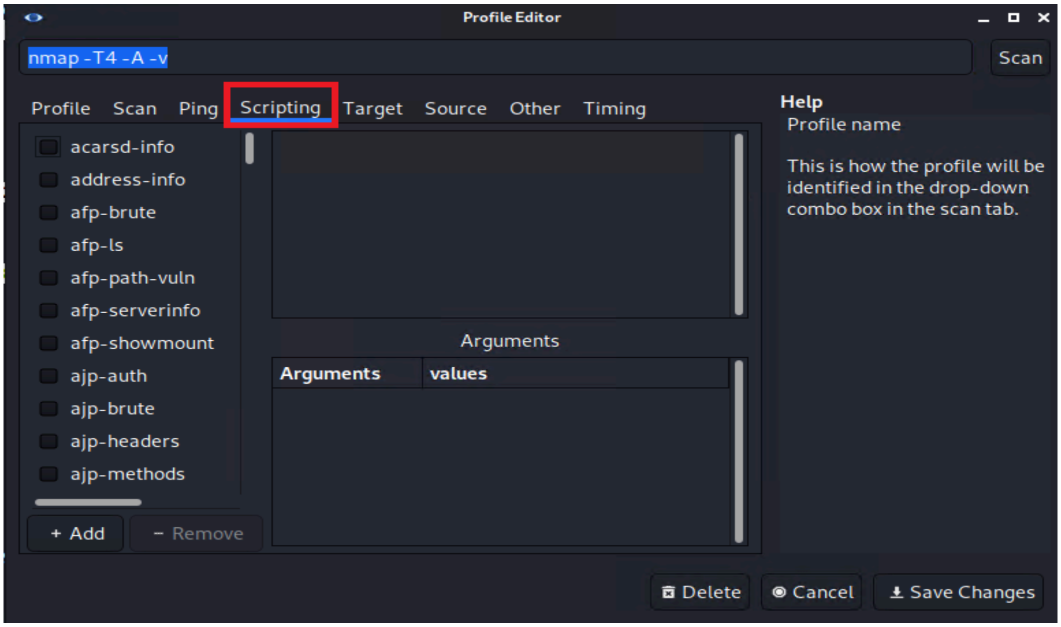
Description: An intense, comprehensive scan. The -A option enables OS detection (-O), version detection (-sV), script scanning (-sC), and traceroute (--traceroute). Without root privileges only version detection and script scanning are run. This is considered an intrusive scan.

Help
Description

The description is a full description of what the scan does, which may be long.

4. Type in your subnet's IP range using CIDR notation (e.g., /24), and click "Scan." Wait for the scan to finish, and view the results. There is a machine of interest that has port 21 open; take note of its IP address.

- Intense scan automatically uses certain NSE scripts based on the services discovered via the `-sC` flag. To add additional scripts, go to "Profile" > "Edit profile" > "Scripting," as the following image shows:



nmap -T4 -A -v

□ acarsd-info
□ address-info
□ afp-brute
□ afp-ls
□ afp-path-vuln
□ afp-serverinfo
□ afp-showmount
□ ajp-auth
□ ajp-brute
□ ajp-headers
□ ajp-methods

Help
Profile name

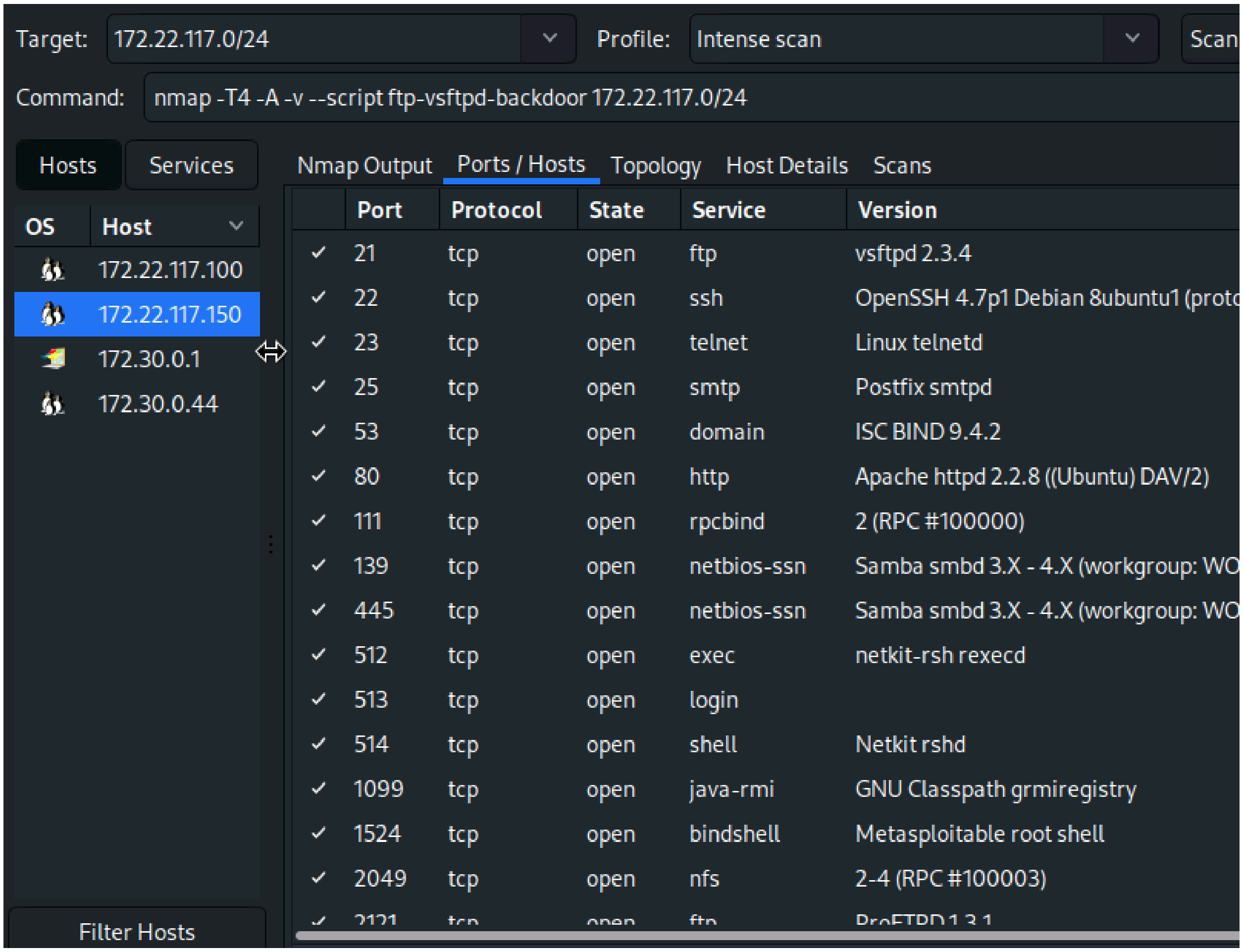
This is how the profile will be identified in the drop-down combo box in the scan tab.

Scroll down to "ftp" and add "ftp-vsftpd-backdoor." Click "Save Changes."

1. Now the intense scan profile has been edited to include these NSE scripts. In the "Target" box, enter the IP address of the machine with port 21 open, and click "Scan" to rerun the scan on that specific host.

2. Notice in the output that port 21 (FTP) is vulnerable to the backdoor exploit.

3. Save this scan by going to "Scan" > "Save Scan."



Target: 172.22.117.0/24

Profile: Intense scan

Command: nmap -T4 -A -v --script ftp-vsftpd-backdoor 172.22.117.0/24

OS	Host
	172.22.117.100
	172.22.117.150
	172.30.0.1
	172.30.0.44

	Port	Protocol	State	Service	Version
✓	21	tcp	open	ftp	vsftpd 2.3.4
✓	22	tcp	open	ssh	OpenSSH 4.7p1 Debian 8ubuntu1 (proto
✓	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: WO
✓	445	tcp	open	netbios-ssn	Samba smbd 3.X - 4.X (workgroup: WO
✓	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