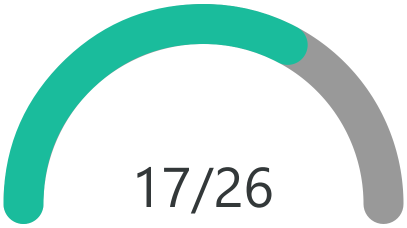
09: APPLIED Lab: Scanning a Vulnerable System

PenTest+ (Exam PT0-002)



Congratulations, you passed!

Duration: 8 minutes, 48 seconds

☑ What is the exact command line for a simple nmap ping sweep for the 10.1.16.x network? *Score: 1*

nmap -sn 10.1.16.0/24

Correct

☑ What is the IP address of the new target? *Score: 1*

10.1.16.9

Correct

☑ How many ports are open on the new target? *Score: 1*

23

Correct

☒ What service is associated with the open port 1099? *Score: 0*

wmisomething

Incorrect, the correct answer is: rmiregistry

☑ What operating system does nmap think is running on the target? *Score: 1*

Linux

Correct

☑ Does the FTP server running on the target support anonymous logins? *Score: 1*

● Yes

○ No

Correct

☑ Which of the following command lines using nmap and the -A and -p options will correctly scan just port 80 on the new target. *Score: 1*

○ nmap -A -p 80 10.1.16.9
○ nmap -A -p80 10.1.16.9
○ nmap -p 80 -A 10.1.16.9
○ nmap -p80 -A 10.1.16.9
● All of the above
○ None of the aboce

Correct

☒ What is the version number of the Apache web server running on the target? *Score: 0*

2.2.28

Incorrect, the correct answer is: 2.2.8

☑ How many items are reported for the target? *Score: 1*

27

Correct

☒ What is the name of the folder that nikto reported as "This might be interesting ..."? *Score: 0*

/dav/

Incorrect, the correct answer is: test

☑ What database administration tool is repeatedly mentioned in the report? *Score: 1*

● phpMyAdmin
○ PHP
○ MySQL
○ XSS

Correct

☒ **CheckNiktoReportOutput** *Score: 0*

Click the Score button to confirm the existence of your report file.

```
/root/Desktop/nikto-results.txt not found
```

☑ How many directories were found by this scan? *Score: 1*

89

Correct

☑ What is the name of the first directory that dirb reported as LISTABLE? *Score: 1*

/dav/

Correct

☑ While nikto and dirb reported many of the same directories, which of the following directories were only reported by dirb? *Score: 1*

○ dvwa
○ twiki
○ multillidae
● All of the above
○ None of the above

Correct

☒ **CheckDirbOutput** *Score: 0*

Select the **Score** button to validate this task:
`/root/Desktop/dirb-results.txt not found`

☑ Which of the following was not listed as a High rated vulnerabilities? *Score: 1*

○ rexec Passwordless / Unencrypted Cleartext login
○ Possible Backdoor: Ingreslock
● Anonymous FTP Login Reporting
○ VNC Brute Force Login

Correct

☑ Which of the following was not listed as a Medium vulnerabilities? *Score: 1*

☐ Anonymous FTP Login Reporting
☐ /doc directory browsable
☑ TCP timestamps
☐ SSL/TLS Report Weak Cipher Suite

Correct

☑ What is the highest score given to a vulnerability? (Note: Do NOT include the decimal) *Score: 1*

10

Correct

☒ How many Low rated vulnerabilities are shown on the results? *Score: 0*

27

Incorrect, the correct answer is: 2

☑ What is the Reference BID number for this vulnerability *Score: 1*

48539

Correct

☒ What nmap option is used to conduct a ping only scan? *Score: 0*

○ -sn
○ -Sn
○ -Pn
● -pn

Incorrect, the correct answer is: -sn

☑ Which nmap output will do OS detection, version detection, script scanning and a traceroute? *Score: 1*

● -A
○ -O
○ -all
○ --options=a;;

Correct

☒ Nikto and dirb are examples of what type of scanner? *Score: 0*

○ Network
○ Web
○ Internet
● All of the above
○ None of the above

Incorrect, the correct answer is: Web

☒ OpenVAS only scans web sites, True or False? *Score: 0*

○ True
● False

Incorrect

☑ What port is being used by the OpenVAS web UI? *Score: 1*

- ● 9392
- ○ 9292
- ○ 10000
- ○ 9300

Correct