ISEC3002 Penetration Testing and Defence Workshop 2

Part 1: Using Shodan search engine to do the following exercises:

Exercise 1. How many ports are open on the server at IP 37.128.132.7? What type of FTP is running on the server? Specify the version of email (if any) running on the server. Specify the top two issues with the site and explain your reasoning. What database service is running on the server (if any)?

Exercise 2. What is the lowest version of TLS supported by the server at 199.120.167.74? Who issued the security certificate for the server? Comment on the overall security setup.

Exercise 3. What is the lowest type of encryption supported by the server at 62.94.10.134? What type of attacks are applicable (if any) based on the encryption settings for the server? How many ports are open on the server?

Exercise 4. Run Spiderfoot on the bank named Mongol Bank (mongolbank.mn)? How many emails are found when using Google? Compare the results with those obtained by running the same search but this time use Bing.

Exercise 5. How many ports are open on the server at 209.172.128.17? How many vulnerabilities can you find applicable to the service running on the lowest open port on this server? What is the most recent vulnerability?

Exercise 6. Consider the following sites:

a) www.aui.ma
b) www.bubok.com.ar
c) web4.ucn.cl
d) hackinsight.org
e) contactmonkey.com

Which website is running on IIS 5.0?
Which server support RC4 ciphers (if any)?
Which server settings are susceptible to the OpenSSL Padding Oracle vulnerability?
Which server/s has the best settings?

Exercise 7. What operating system is running on the server at 157.250.156.23?

Exercise 8. Which of the following IPs are running FTP, SSH and NTP services: 46.23.184.196, 103.83.106.69, 217.31.246.55? Which port do they all these IP addresses have open? What runs on that particular port (what is the purpose of the service)?

Exercise 9. What is the common service running on the servers at the following IP addresses: 37.130.48.179, 188.150.111.250, 46.97.237.250? Which one of the IPs is running a login page for a company called Alliance?

Exercise 10. Which one of the following IPs is running a service that allows one to check the CPU load on a virtualised host: 46.101.106.205, 20.199.188.68, 184.82.64.28?

Exercise 11. What credentials would you try on the service running at IP 88.213.248.8/

Exercise 12. Which of the following IP addresses run webcams that overlooks a stage: 88.213.248.8, 191.25.51.100, 176.80.10.69?

Part 2: Using the provided Cyber Range to answer the following questions:

Exercise 1.

a) How many IPs are currently live in the 192.168 subnet?

b) How many of the IPs are running Linux OS and how many are running Windows OS?

c) Specify the names of at least 4 of the machines that are live.

d) How many Domain Controllers are currently live in the 192.168 subnet and what are their names?

e) What is/are the name/s of the domain/s currently active in the 192.168 subnet?

f) How many systems currently live in the 192.168 subnet are running FTP services?

g) How many systems currently live in the 192.168 subnet are running TFTP services?

h) Are there more than two systems currently live in the 192.168 subnet that are running database services?

i) How many systems currently live in the 192.168 subnet are running websites? Are there any systems running more than one website?

j) Specify whether there are any systems providing NFS shares and if they do, specify the share.

k) Which machine named Dagol-Fel (specify the IP address)?

l) Which domain is the largest (in terms of live machines)?

Exercise 2.

a) Specify which system has the largest number of ports open.

b) Specify the IPs of the machines running SSH services.

c) Specify whether or not there is machine running XAMPP currently live in the cyber range.

d) Specify whether or not there is machine running MS-SQL2016 currently live inthe cyber range.

e) Specify the IPs of least two machines that allow anonymous FTP. Explain howyou determine whether or not anonymous access is allowed.

f) Specify whether or not there is machine running MySQL in the cyber range.

g) Specify the FQDN name for the domain controllers that live in the cyber range.

h) Which of the live systems in the cyber range could be used as domain controllers?