

Lab Report

Your Performance

Your Score: 6 of 6 (100%)

Elapsed Time: 7 minutes 14 seconds

Pass Status: Pass

Required Score: 100%

Task Summary**Required Actions & Questions**

- ✓ Used WhoIs.org to discover name servers
- ✓ Q1 Which of the following Name Servers are being used by CorpNet.xyz?
Your answer: NS1.NETHOST.NET, NS2.NETHOST.NET
Correct answer: NS1.NETHOST.NET, NS2.NETHOST.NET
- ✓ Used nslookup to discover www.corpnet.xyz IP address
- ✓ Q2 What is the IP address for CorpNet.xyz?
Your answer: 198.28.1.1
Correct answer: 198.28.1.1
- ✓ Used nmap to discover open ports for ftp and telnet
- ✓ Q3 Which of the following servers use the potentially vulnerable ftp and telnet ports?
Your answer: 198.28.1.3, 198.28.1.4
Correct answer: 198.28.1.3, 198.28.1.4

Explanation

In this lab, your task is to perform reconnaissance on www.corpnet.xyz and to find potentially vulnerable ports on the servers in the CorpNet networks as follows:

- On Consult-Lap, use the Whois.org site to determine the domain name servers used by www.corpnet.xyz.
- On Consult-Lap, use **nslookup** to determine the primary web server address.
- On Consult-Lap2, use Zenmap to perform an nmap search for open ports for the 198.28.1.0/24 network.
- Answer the questions.

Complete this lab as follows:

1. Find the name servers used by www.corpnet.xyz as follows:
 - a. From the taskbar, open Chrome.
 - b. In the URL field, type **whois.org** and press **Enter**.
 - c. In the Search for a domain name field, enter **www.corpnet.xyz**.
 - d. Select **Search**.
 - e. In the top right, select **Answer Questions**.
 - f. Answer question 1.
2. Find the IP address used by www.corpnet.xyz as follows:
 - a. Right-click **Start** and select **Windows PowerShell (Admin)**.
 - b. At the prompt, type **nslookup www.corpnet.xyz ns1.nethost.net** and press **Enter**.
 - c. Answer question 2.
 - d. Minimize the question dialog.
3. Use Zenmap to run an nmap command to scan for open ports as follows:
 - a. From the navigation tabs, select **Buildings**.
 - b. Under Red Cell, select **Consult-Lap2**.
 - c. From the Favorites bar, open Zenmap.
 - d. Maximize Zenmap for easier viewing.
 - e. In the Command field type **nmap -p- 198.28.1.0/24**.
 - f. Select **Scan** to scan for open ports on all servers located on this network.
 - g. In the top right, select **Answer Questions**.
 - h. Answer question 3.
 - i. Select **Score Lab**.

