10.3.5 Lab: Scan for Unsecure Protocols

Candidate: Richard Habib ()
Time Spent: 00:35

Score: 0%

Task Summary

Required Actions and Questions

✗ Use whois.org to discover name servers

✗ *Q1*: Which of the following name servers is being used by PartnerCorp.xyz?

   Your answer:

   Correct answer: ns1.nethost.net

✗ *Q2*: What is the IP address for www.partnercorp.xyz?

   Your answer:

   Correct answer: 73.44.215.1

✗ Use Zenmap to run an Nmap command (using --top-ports) to scan for open ports

---

✗ *Q3*: Which of the following servers use the potentially vulnerable FTP or Telnet ports?

   Your answer:

   Correct answer: 73.44.215.5

Explanation 🎧

Complete this lab as follows:

1. From the Analyst-Lap computer, find the domain name servers used by partnercorp.xyz.
   a. From the taskbar, select **Google Chrome**.
   b. Maximize the windows for better viewing.
   c. In the URL field, type **whois.org** and press **Enter**.
   d. In the *Search for a domain name* field, enter **partnercorp.xyz**.
   e. Select **Search**.
   f. In the top right, select **Questions**.
   g. Answer Question 1.

2. Find the IP address used by www.partnernetcorp.xyz.
   a. Right-click **Start** and select **Terminal (Admin)**.
   b. At the PowerShell prompt, type **nslookup www.partnercorp.xyz** *name_server* (see the answer to question 1) 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.

    a. From the navigation tabs, select **Buildings**.

    b. Under Blue Cell, select **Analyst-Lap2**.

    c. From the Favorites bar, select **Zenmap**.

    d. Maximize Zenmap for easier viewing.

    e. In the *Command* field, use **nmap --top-ports 50 73.44.215.0/24** to scan for open ports.

    f. Select **Scan** to scan for open ports on all servers located on this network.

    g. In the top right, select **Questions**.

    h. Answer Question 3.