Cabrillo College

CIS 76 Linux Lab Exercise

Lab 5: Scanning
Fall 2016

Lab 5: Scanning

This lab takes a look at doing port scans using nmap then following up with deeper vulnerability scans using Nikto and OpenVAS

Warning and Permission

Unauthorized hacking can result in prison terms, large fines, lawsuits and being dropped from this course!

For this lab you have authorization to hack the VMs in the VLab pod assigned to you.

Preparation

- Get the CIS 76 Login Credentials document. You will need usernames and passwords to log into VLab and each of the VMs. This document is on Canvas and the link is in the CIS 76 Welcome letter.

- Determine which VLab pod number you were assigned. See the link on the left panel of the class website.

Part 1 – Pod configuration

1) If you haven't already configured your pod in the previous labs, then follow the instructions here: https://simms-teach.com/docs/cis76/cis76-podSetup.pdf

Part 2 – Default nmap SYN scan of pod VMs

1) Make sure all the Pod VMs are powered up.
2) On Kali, set up for Wireshark capture with this filter:
   ```
   (tcp or icmp) and (ip.src >= 10.76.<pod>.1 &&
   ip.src <= 10.76.<pod>.254) and (! ssh)
   ```
3) On EH-Kali, do a default SYN scan of your pod network:
   ```
   nmap -sS 10.76.<pod>.0/24
   ```

Part 3 – Deeper port 80 nmap scan of EH-pfSense and EH-OVWASP VMs

1) On Kali, perform a deeper scan on EH-pfSense port 80 using:
   ```
   nmap -A -p 80 10.76.<pod>.1
   ```
2) On Kali, perform a deeper scan on EH-OWASP port 80 using:
   ```
   nmap -A -p 80 10.76.<pod>.101
   ```

Part 4 – Nikto vulnerability scans of EH-pfSense and EH-OVWASP VMs

1) On Kali, perform a vulnerability scan on EH-pfSense website using:
   ```
   nikto -h 10.76.<pod>.1
   ```
2) On Kali, perform a vulnerability scan on EH-OWASP website using:
   ```
   nikto -h 10.76.<pod>.101
   ```

Part 5 – OpenVAS vulnerability scans of EH-pfSense and EH-OVWASP VMs

1) As the root user on Kali, install OpenVAS. This can take some time!
   ```
   apt-get update
   apt-get install openvas
   ```
   (This step takes about 20 minutes with some errors!)
2) On the Kali desktop select:

   Applications > 02 – Vulnerability Analysis > openvas ini...*tial setup (first)*

   (This step takes at least 90 minutes!)
3) To fix the apt-get errors, edit /etc/redis/redis.conf:

   Change: **unixsocket ~~/var/lib/redis/redis.sock~~**

   To: **unixsocket /tmp/redis.sock**
4) **redis-server /etc/redis/redis.conf**
5) Applications > 02 – Vulnerability Analysis > openvas st...*art (second)*
6) **openvasmd --user=admin --new-password=password**
7) In Firefox, browse to **https://127.0.0.1:9392** and login.
   a. Username: admin
   b. Password: password
8) Use the "Quick start: Immediately scan an IP address" to:
   a. Generate a vulnerability report for EH-pfSense.
   b. Generate a vulnerability report for EH-OWASP.

c. On the second report, drill down and look at the first HTTP Brute Force Logins with default credentials item.

Submit your work

1) Prepare a report using the word processor and formatting of your choice. Your report should contain the following:

    - Course name, lab assignment name, your name, and date.
    - For Part 2 include:
        - Labeled SCREEN SHOT of nmap output showing default SYN scan of 4 VMs.
        - Labeled SCREEN SHOT of Wireshark showing the start of the nmap SYN scan.
    - For Part 3 include:
        - Labeled SCREEN SHOT of nmap output showing EH-pfSense port 80 scan results.
        - Labeled SCREEN SHOT of nmap output showing EH-OWASP port 80 scan results.
    - For Part 4 include:
        - Labeled SCREEN SHOT of Nikto output showing EH-pfSense scan results.
        - Labeled SCREEN SHOT of Nikto output showing EH-OWASP scan results.
    - For Part 5 include:
        - Labeled SCREEN SHOT of OpenVAS report for EH-OWASP – main page.
        - Labeled SCREEN SHOT of OpenVAS report for EH-OWASP – details on first Bute Force Logins with default credentials.

    - As an example you can see Benji Simms' report here: https://simms-teach.com/docs/cis76/cis76-lab05-simben76.pdf

2) Email your report to: **`risimms@cabrillo.edu`**

Remember **late work is not accepted.** If you can't finish the lab by the deadline submit what you have completed for partial credit.

Grading Rubric (30 points)

3 points for Part 2 default NMAP SYN scan.
3 points for Part 2 related Wireshark capture of start of nmap scan.
4 points for Part 3 deeper nmap port 80 scan of EH-pfSense VM.
4 points for Part 3 deeper nmap port 80 scan of EH-OWASP VM.
3 points for Part 4 Nikto vulnerability scan of EH-pfSense website.
3 points for Part 4 Nikto vulnerability scan of EH-OWASP website.

5 points for Part 5 OpenVAS vulnerability scan of EH-OWASP website.
5 points for Part 5 OpenVAS brute force vulnerability details.