Cabrillo College

CIS 76 Ethical Hacking Lab Exercise

Lab 5: Scanning
Fall 2017

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 – Aggressive nmap SYN scan of pod VMs

1) Make sure these five pod VMs are configured and powered up:
   EH-pfSense, EH-OWASP, EH-Kali, EH-WinXP and EH-Win7
2) Turn off the firewall on EH-Win7.
3) On Kali, start a Wireshark capture on eth0.
4) Set the Wireshark filter to:
   ip.addr == 10.76.xx.207 and tcp.port == 445
   (where xx is your pod number)
5) On EH-Kali, do an "aggressive" SYN scan of your pod network:
   ```
   nmap -sS -T4 10.76.xx.0/24
   ```
6) Take a snapshot of your Wireshark capture showing the incomplete 3-way handshake with port 445.

Part 3 – Deeper port 80 nmap scan of EH-Win7 VM

1) On Kali, perform a deeper scan on your EH-win7 port 80 using:
   ```
   nmap -A 10.76.xx.207
   ```

Part 4 – Nikto vulnerability scan of EH-OWASP VM website

1) On Kali, perform a vulnerability scan on EH-OWASP VM website using:
   ```
   nikto -h 10.76.xx.101
   ```

Part 5 – OpenVAS vulnerability scans of your EH-Win7 VM

1) As the root user on Kali, install OpenVAS. Be patient, this can take some time!
   ```
   apt-get update
   apt-get upgrade
   ```
   (This step takes a LONG time!)
   ```
   apt-get install openvas
   ```
   (This step takes a LONG time!)
   ```
   openvas-setup
   ```
   (This step takes a LONG time!)
   Record the generated password for the next step.
2) In Firefox, browse to `https://127.0.0.1:9392` and login.
   a. Username: admin
   b. Password: password
   c. On Scans "tab" > Tasks use the ✳ task wizard to do an "immediate scan" of your EH-Win7 VM.
3) On the resulting EH-Win7 scan report, drill down and review the vulnerability titled "Microsoft Windows SMB Server Multiple Vulnerabilities-Remote".

Part 6 – Extra Credit

1) Find an exploit for the vulnerability you reviewed.
2) Use Metasploit on Kali to attack your EH-Win7 VM.
3) Using meterpreter, capture EH-Win7 sysinfo and hashdump information.

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:
     - Output from your nmap aggressive SYN scan of 5 VMs.
     - Labeled SCREEN SHOT of Wireshark showing an incomplete port 445 3-way handshake with your EH-Win7 VM.
   - For Part 3 include:
     - Output from your deeper nmap scan on your EH-Win7 VM.
   - For Part 4 include:
     - Nikto output from scanning your EH-OWASP VM.
   - For Part 5 include:
     - Labeled SCREEN SHOT of OpenVAS report for EH-Win7 VM.
     - Labeled SCREEN SHOT of OpenVAS report drill-down of "Microsoft Windows SMB Server Multiple Vulnerabilities-Remote" vulnerability.
   - For Part 6 include:
     - Labeled SCREEN SHOT of Metasploit attack showing output from the sysinfo and hashdump meterpreter commands

   - 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)

4 points for Part 2 aggressive NMAP SYN scan.
4 points for Part 2 related Wireshark capture showing incomplete handshake.
4 points for Part 3 deeper nmap port 80 scan of EH-Win7 VM.
4 points for Part 4 Nikto vulnerability scan of EH-OWASP VM website.

10 points for Part 5 OpenVAS vulnerability scan of EH-Win7 VM.
4 points for Part 5 OpenVAS SMB server vulnerabilities details.

Extra Credit (3 points)
3 points extra credit for successful Metasploit attack showing sysinfo and hashdump.