Cabrillo College

CIS 76 Linux Lab Exercise

Lab X1 - Reconnaissance with Nmap and Amap
Fall 2016

Lab X1 - Reconnaissance with Nmap and Amap

This lab provides more scanning practice with the Nmap and Amap tools.

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 associated Netlab+ pod.

Preparation

1) Reserve a Netlab+ pod for the maximum amount of time for this lab:
   NDG Lab 1: Reconnaissance with Nmap & Amap
   You can always release it if you finish early.

Part 1 – Nmap

1) Follow steps 1-26 which use nmap and view resulting network activity with Wireshark.
2) Document in your lab report the following:
   a. nmap -sT 192.168.68.12
      - Include a screen shot of this command with the output
      - Include a screen shot of the Wireshark capture using the display filter: tcp.port == 22
   b. nmap -F 192.168.68.12
      - Include a screen shot of this command with the output
      - Include a screen shot of the Wireshark capture using the display filter: tcp.port == 22
   c. Answers to the following questions:

- What does the nmap -sT option do?
- What does the nmap -F option do?
- How many packets were generated using the -sT option?
- How many packets were generated using the -F option?
- How did the method for checking port status differ between the -sT and -F options?

Part 2 – Amap

1) Follow steps 1-6 which use Amap
2) Document in your lab report the following:
    a. amap -A 192.168.68.12 22
        - Include a screen shot of this command with the output
    b. amap -B 192.168.68.12 22
        - Include a screen shot of this command with the output
    d. amap -P 192.168.68.12 22
        - Include a screen shot of this command with the output
    c. Answers to the following questions:
        - How many packets total (against all ports) were generated using the -A option?
        - How many packets total (against all ports) were generated using the -B option?
        - Does the -P option use a full connection or half-open "stealth" scan to check port status?

As an example you can see Benji Simms' report here:
https://simms-teach.com/docs/cis76/cis76-labX1-simben76-redacted.pdf

Submit your work

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

Remember **late work is not accepted.** If you run out of time submit what you have completed for partial credit.

Grading Rubric (15 points)

1 points for nmap -sT 192.168.68.12 screen shot
1 points for nmap -sT 192.168.68.12 filtered Wireshark screen shot
1 points for nmap -F 192.168.68.12 screen shot

1 points for nmap -F 192.168.68.12 filtered Wireshark screen shot
5 points for nmap questions 1-5
1 points for amap -A 192.168.68.12 22 screen shot
1 points for amap -B 192.168.68.12 22 screen shot
1 points for amap -P 192.168.68.12 22 screen shot
3 points for amap questions 1-3