Cabrillo College

CIS 76 Ethical Hacking Lab Exercise

Lab X7 - Active and Passive Enumeration Techniques
Fall 2017

Lab X7 - Using Active and Passive Enumeration Techniques

This lab provides supplemental enumeration practice with nmap, Metasploit, tcpdump, Wireshark and Cain.

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:
   NISGTC Lab 01: Using Active and Passive Techniques to Enumerate Network Hosts
   You can always release it if you finish early.

NISGTC Lab Part 1 – Discovering Hosts with Nmap and Zenmap

1) Complete steps 1-5 of the NISGTC lab.
2) Take a screenshot of the tcpdump output showing there is a device at 192.168.1.175.
3) Use Ctrl-C to stop tcpdump.
4) Complete steps 8-17.
5) Take a screenshot of Wireshark ARP traffic showing the device at 192.168.1.175 being discovered. Note: This is the Windows XP Pro PC on the topology map.
6) Complete steps 18-20.
7) Take a screenshot of Wireshark traffic showing the TCP connection resets sent to 192.168.1.175 by zenmap. To find them you can use this filter:
   ```
   tcp.flags.reset==1 && ip.addr==192.168.1.175
   ```
8) Finish up remaining Part 1 steps.

NISGTC Lab Part 2 – Discovering Hosts with Windows Command Line Tools

1) Complete steps 1-11 of the NISGTC lab.
2) Take a screenshot showing output from the following commands:
```
net view
net view /domain
net view /domain:XYZcompany
net view /domain:WORKGROUP
rem completed by <your name>
```
3) Complete step 12.
4) Take a screenshot showing related Wireshark browser traffic.
5) Complete remaining steps in Part 2.

NISGTC Lab Part 3 – Discovering Hosts with Metasploit and Cain

1) Complete steps 1-10 of the NISGTC lab.
2) Take a screenshot showing output from the arp-sweep enumeration.
3) Complete steps 11-15 of the NISGTC lab.
4) Take a screenshot showing output from the nbname enumeration.
5) Complete steps 16-27.
6) Take a screenshot showing output from the Cain enumeration.
7) Complete remaining steps in Part 3.

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.
   - Labelled or captioned screenshots for:
     - Part 1 tcpdump output showing 192.168.1.175 (Step 5)
     - Part 1 Wireshark capture showing 192.168.1.175 ARP traffic (Step 17)
     - Part 1 Wireshark capture showing 192.168.1.175 resets (Step 20)
     - Part 2 net view commands and rem command (Steps 8-11)
     - Part 2 Wireshark capture of related BROWSER traffic (Step 12)
     - Part 3 Metasploit enumeration with arp_sweep (Step 10)
     - Part 3 Metasploit enumeration using nbname (Step 15)
     - Part 3 Cain enumeration (Step 27)

   As an example you can see Benji Simms' report here:
   https://simms-teach.com/docs/cis76/cis76-labX7-simben76.pdf

2) 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 (6 points)
2 points for the Part 1 screenshots.
2 points for the Part 2 screenshots.
2 points for the Part 3 screenshots.