Cabrillo College

CIS 76 Linux Lab Exercise

Lab X3 - Using Armitage to Attack the Network
Fall 2016

Lab X3 - Using Armitage to Attack the Network

This lab shows how to use Nmap and Armitage to attack and compromise an Internet facing Windows server. Then from that server, pivoting, and attacking additional Windows systems on an internal network.

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 12: Using Armitage to Attack the Network
   You can always release it if you finish early.

Part 1 – Using Nmap and Armitage to Attack the Internet Facing Device

1.1.3) Get screenshot on Zenmap "Ports/Hosts" tab showing open ports on 216.1.1.1.

1.1.4) Get the following:
   a. Screenshot of Zenmap "Nmap Output" tab and highlight the portion showing port 80 scan details.
   b. nmap script code used to check http server options and highlight the line that outputs "Potentially risky methods".
   c. OWASP webpage showing how to test for HTTP methods.

1.1.7) Get screenshot of Armitage with a "compromised" 216.1.1.1 and successful getsystem command in the meterpreter shell.

Part 2 – Using Armitage to Attack the Internal Server 2008

2.1.13) Get screenshot showing the two “compromised” systems, 216.1.1.1 and 192.168.1.200.

Part 3 – Using Armitage to Attack the Internal Server 2008

3.1.9) Get screenshot of the three “compromised” systems, 216.1.1.1, 192.168.1.200 and 192.168.1.175.

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.
   - All the screenshots or code collected above.
   - Each screenshot should be the full uncropped Netlab window.
   - Each screenshot should be labelled, captioned and readable.
   - Code may be shown either as a screen shot or text.

   As an example you can see Benji Simms’ report here:
   https://simms-teach.com/docs/cis76/cis76-labX3-simben76-redacted.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 (15 points)

1 points for 1.1.3) Zenmap overview of 216.1.1.1
3 points for 1.1.4a) Zenmap port 80 details of 216.1.1.1
1 points for 1.1.4b) Zenmap script used to check HTTP options
1 points for 1.1.4c) OWASP How to test HTTP methods
3 points for 1.1.7) Using Armitage to attack the Internet facing device
3 points for 2.1.13) Using Armitage to attack the internal Windows Server 2008
3 points for 2.1.13) Using Armitage to attack the internal Windows XP Machine