CIS 76 Linux Lab Exercise

Lab 3: Network and Computer Attacks
Fall 2016

Lab 3: Network and Computer Attacks

This lab first gives you some practice using session hijacking to attack another computer. Next you will use SQL injection to install a RAT on a victim's server. Finally, you will do an SSH brute force attack to get a user's login credentials then steal their secret information.

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

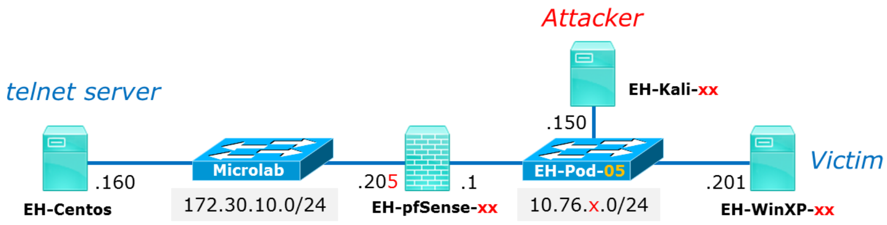
- Get the CIS 76 Login Credentials document. You will need usernames and passwords to log into VLab and each of the VMs. This document is on Canvas and the link is in the CIS 76 Welcome letter.

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

Part 1 – Pod configuration

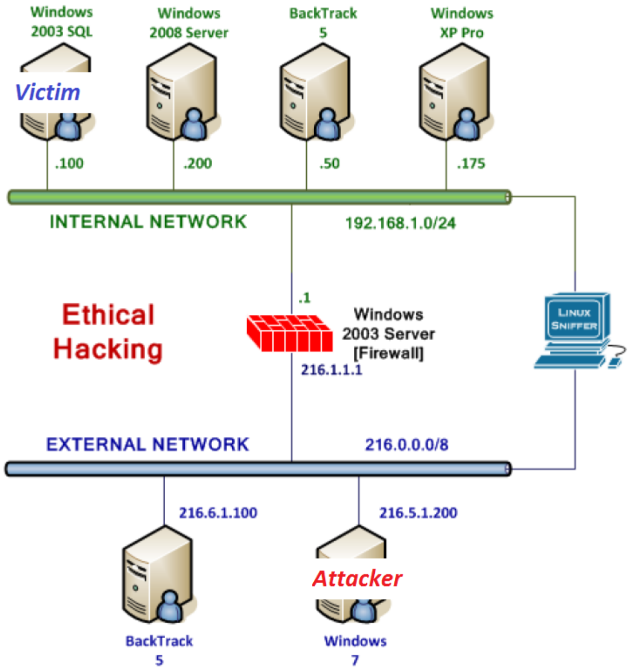
1) If you haven't already configured your pod in the previous labs then follow the instructions here:
https://simms-teach.com/docs/cis76/cis76-podSetup.pdf

Part 2 – [VLab] Telnet session hijack



a) From Kali use a MITM attack with Ettercap to get between the victim on the EH-WinXP VM and the EH-pfSense router. When the victim on EH-WinXP telnets into EH-Centos, capture the victim's login credentials. Rather than use those credentials do a session hijack of the telnet session with Shijack. This is a stealthier attack because you won't leave behind any revealing login information. One you have access to the victim's account on EH-Centos and leave your mark there by adding a file to the vistors directory. To do this see example here: https://simms-teach.com/docs/cis76/cis76-Telnet-Session-Hijack.pdf

Part 3 – [Netlab+] Utilizing malware (DarkComet)



a) Log into Netlab+, schedule a time slot and do the NISGST Ethical Hacking Lab 6 "Dark Comet". From Windows 7 use SQL Injection to transfer a RAT to the Windows 2003 SQL server and take control. At the end of the lab push a file with your name on it to the Salary folder.

Part 4 – [VLab] Brute force SSH attacks

a) From Kali generate a wordlist from https://simms-teach.com/cis76home.php and **do** a SSH brute-force attack on the ahdar user on eh-rouji.cis.cabrillo.edu. Find out what is in Ahdar's secret file.

Part 5 – Submit your work

a) 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 screenshots of:
    - [Kali] Screen capture of Ettercap showing pod hosts, ARP poison targets and captured credentials.
    - [Kali] Screen capture of commands being injected into the telnet session using Shijack.
    - [EH-Centos] Output of the **tree ~cis76/visitors** command showing evidence you created a file named after you there.
- For Part 3 include screenshots of:
    - [Windows 7] DarkComet showing the Computer Information view.
    - [Windows 7] DarkComet File Manager where you uploaded a file named for you to the victims' Salary folder.
- For Part 4 include screenshots of:
    - [Kali] head and tail output of your wordlist.
    - [Kali] The snipped output of your hydra attack showing the password.
    - [EH-Rouji] The contents of Ahdar's secret file

As an example you can see Benji Simms' report here:
https://simms-teach.com/docs/cis76/cis76-lab03-simben76.pdf

b) 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 Ettercap showing correct poison targets.
3 points for Ettercap showing correct captured credentials.
3 points for injecting commands using Shijack.

4 points for tree output showing named for you.
3 points for DarkComet Computer Information view.
4 points for DarkComet FileManager transferring file named for you to Win 2003 SQL server.
3 points for brute force word list.
3 points for hydra output showing password
4 points for Ahdar’s secret