CS 333: Network Security and Defense

Capture the Flag - Firewall. Author: Jidong Xiao

1 Introduction

This in-class contest is mainly used to engage students in class, and help students to understand how firewall works. Students will be divided into two teams - blue team and red team.

2 Rules

- The blue team will act like defenders and configure firewalls based on given instructions. The red team will act like attackers and try to test the firewalls are securely configured or not.
- Each student in the blue team needs to pick an opponent from the red team. These two students will battle against each other.
- Setting window: once the game starts, every student in the blue team needs to finish the firewall configurations within a setting window, which is 3 minutes. The instructor might extend this time window if needed: e.g., if more than half of the students can't finish the configuration in 3 minutes.
- Testing window: after the setting window is closed, every student in the red team will do penetration test: verify if the firewall is correctly set. Any incorrect setting identified by a red team student earns the red team one point. The red team needs to finish the test within a testing window, which is 3 minutes.
- Points checking: once the testing window is closed, the two battlers come together and verify how many points the red team member earns. The instructor records how many points in total the red team earns.
- Role switch: once the above is done, the two teams switch roles. The original blue team will now be the red team, the original red team will now be the blue team. The two teams repeat the setting and testing procedure, and the red team will again earn points based on how many incorrect setting identified.
- Cheating Prevention: Before the setting window, the red team verify the blue team have no firewall settings: "sudo ufw status verbose" shows no rule.

3 Incentives

Five CTF games will be played during this semester. All the CTF game points will be accumulated, eventually the team with more accumulated points will be the winning team. The winning team will earn the following "awards":

- 1. Students (in the winning team) who are supposed to get B+ will be raised to A-; A- will be raised to A.
- 2. Students (in the winning team) who are supposed to get anything below than C, will be raised to C.

Exception: The prize doesn't apply to students who misses 4 or more than 4 classes.

4 Preparation

- Everybody: Install a command line browser on both of your VMs:

  [09/22/18]seed@VM: $ sudo apt-get install lynx

  Test if the browser works by:

  [09/22/18]seed@VM: $ lynx www.taylorswift.com (type Y whenever the server asks you something)

- Everybody: On both of your VMs, change your firewall default policy in /etc/default/ufw - see lab manual 2.1. And then enable your firewall on both of your VMs:

  [09/22/18]seed@VM: $ sudo ufw enable

- Everybody: Tell your opponent your host name - so that your opponent will be able to connect to your machine using ssh, e.g., ssh onyxnode24.

5 Blue Team Instructions: Firewall Setting

Note: The blue team should only use the ufw firewall program to achieve the following goals. Refer to https://help.ubuntu.com/community/UFW for ufw examples.

- Block telnet from VM1 to VM2 (Hints: telnet server uses port 23)
- Block telnet from VM2 to VM1
- Block ssh from VM1 to VM2 (Hints: ssh server uses port 22)
- Block ssh from VM2 to VM1
- Block access to website https://www.taylorswift.com from VM1 (Hints: block the website's ip address would be easier than block certain ports, and ping the website will get its ip address)
- Block access to website https://www.taylorswift.com from VM2
- Disable ping from anyone to VM1 - Hints: refer to https://help.ubuntu.com/community/UFW
- Disable ping from anyone to VM2

6 Red Team Instructions

Note: The red team should not rely on the ufw command for anything.

- Use arp -a to idenfity the ip address of the two VMs. (We assume VM2's ip address is "greater" than VM1's ip address)
- Use lynx to access websites.