Cybersecurity

Capstone Project

Red Team vs. Blue Team

This Week: Final Projects!

Project Overview:

- A Red Team vs. Blue Team group project
- You will first play the role of a Red Team pentester and hack into a vulnerable web server.
- Then, you will play the role of the Blue Team and investigate the attack via Snort logs.
- On the final day, each group will give a presentation that that focuses on a specific aspect of their project.

SUGGESTED TIME:
All Week!

This Week's Schedule:

Day 1: Red Team

In groups, you will infiltrate a web server to capture a flag. The web server is hosted on Cybrscore.

Day 2: Blue Team and Presentation Prep

- In groups, you will investigate a snort log from a different team's attack.
- You will also spend the second half of the day preparing your presentations.

Day 3: Presentations

- Students will present their findings.

Presentation Expectations

Presentation Criteria:

- Between 10-15 minutes long, followed by 5 minutes of Q&A.
- Each group should have a slide deck to use for their presentation.
- Each member of the group is expected to speak.
- Each member of the group is expected to contribute to the slide deck.

Important: Take screenshots of your work as they go through the activity so that they include these in their presentation decks.

Demo Day

These Projects can also be modified for Demo Day.

- Demo Day the time to demonstrate a project you've completed during the program.
- It is a chance to meet and network with employers and fellow bootcamp grads.
- While demonstrating a report is not very dynamic, you can communicate the process and thinking into a visually appealing slide deck and talk engagingly to potential employers.

Group Specific Topics:

- ☐ Vulnerabilities
- ☐ Attack Methods
- ☐ Post Exploitation
- ☐ Incident Response
- ☐ Mediation

Group Specific Topics:

Vulnerabilities

- How did you recognize this virtual machine was vulnerable?
- Were there any other vulnerabilities that you saw?
- What would you do to fix what you exploited?

Group Specific Topics:

Attack Methods

- What tools did you use to bypass the security?
- How did you know those would work?
- Would they work in the real world?
- What would you recommend to your clients?

Group Specific Topics:

Post Exploitation

- When you were in the machine, what user were you?
- Did you have access to the full machine?
- How would you be able to defend against this exploit?
- What would you do to maintain access to the server?

Group Specific Topics:

Incident Response

- What time did the attack start and how long did it last?
- What was the IP address of the attacker?
- Who was the attacker trying to login as? Was the attacker successful?
- How many passwords did the attacker use before they found the correct password?
- What kind of attack was the attacker using? How is this reflected in the report?

Group Specific Topics:

Mediation

- How would you protect your servers from these attacks?
- Are there any other vulnerabilities that the server would be prone to? What are they?
- How would you fix those?

Activity: Red Team

For the Red Team portion of the project, you will log into Cybrscore and use a Kali instance to log into a vulnerable web server.

- ☐ Log in to Cybrscore.
- ☐ Discover the IP address of the Linux server.
- ☐ Locate the hidden directory on the server.
- ☐ Brute force the password for the hidden directory.
- ☐ Break the hash password with John the Ripper
- ☐ Connect to the server via Webdav.
- ☐ Upload a reverse php connection payload.
- ☐ Capture and show the flag to your instructor.
- ☐ Show your instructor once you have captured the flag, and they will send you the pcap file for the next part of the capstone.

Important: Take screenshots of the process, so you can add them to your presentation.

Activity: Blue Team

After you infiltrated the vulnerable machine and have received the snort log, you will complete the following objectives:

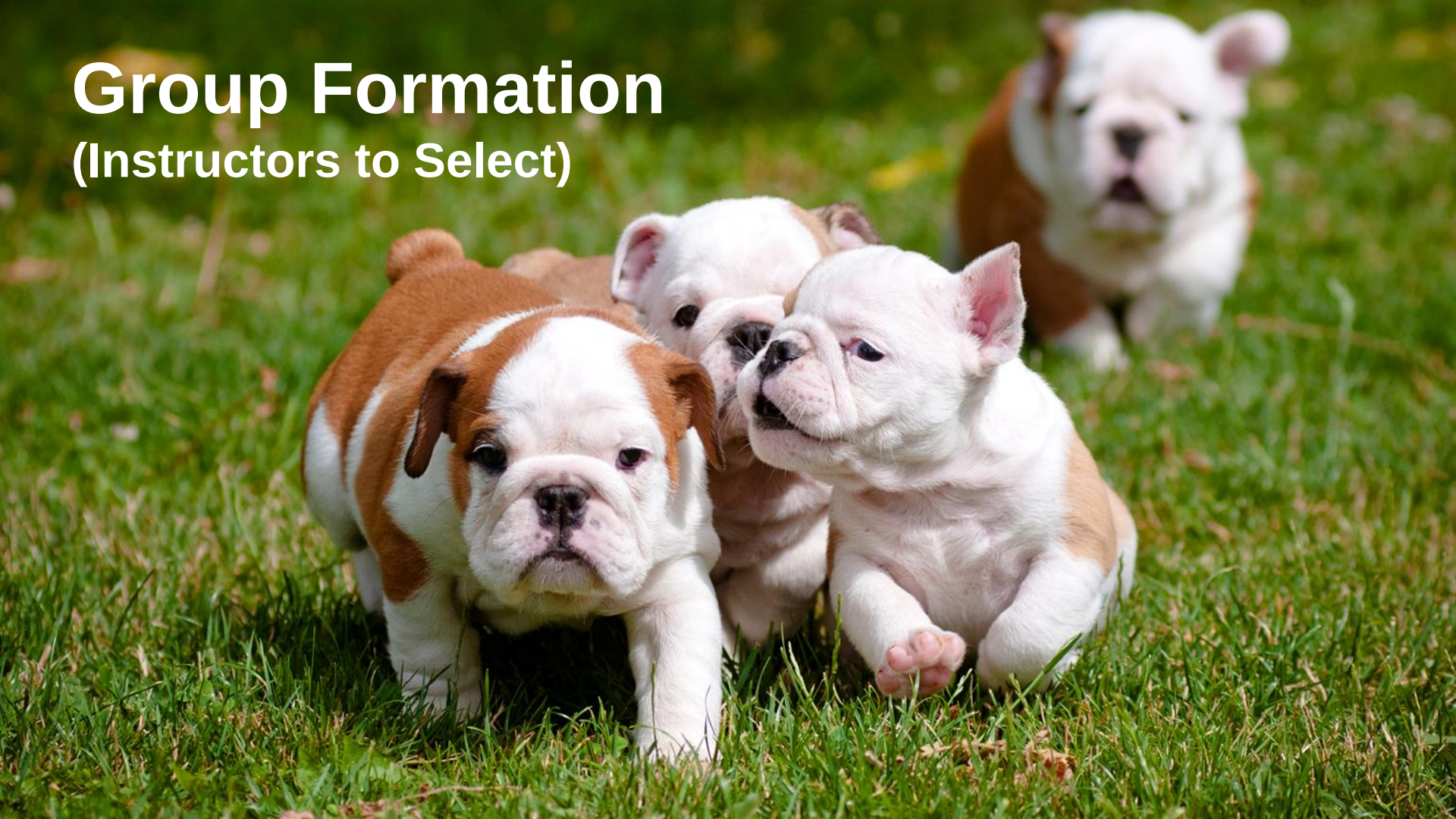
- ☐ On your Kali machine, use Wireshark to open the Snort log.
- ☐ Look through the data and answer the following questions according to Wireshark:
  - How long did the attack last?
  - How many password attempts were made?
  - In which packet was the correct password found?
  - In which packet was the shell placed onto the server?
  - In which packet was the shell activated?

Important: Take screenshots of the process, so you can add them to your presentation.

Due Dates:

Presentations will be on Day 3 of class.

Group Formation
(Instructors to Select)



Questions