Networking Capture the Flag

Cybersecurity

Networking 2, Day 3

9.3: Network 2 - Capture The Flag

Class Preparation

1. Check into BCS
2. Update your git repository with `` `git pull` ``
3. Launch and login to your Ubuntu VM
    - You do not need to update VirtualBox if prompted

Homeworks Due

- Unit 8 (Networking): due Sunday November 22
- Unit 9 (Networking 2): due Sunday November 29
- Homework Make Up: due Sunday November 29

Upcoming Units

- Week 10: Network Security (11/23 - 12/02)
- Week 11: Cloud Sec. & Virtualization (12/05 - 12/12)
- Week 12: Project Week (12/14 - 12/19)

Schedule Notes

Thanksgiving Break - No Class

- Off: Wed 11/25 & Sat 11/28
- Return on Monday 11/30

Project 1 (Individual; Required)

- Mon 12/14 - Sat 12/19

Winter Break - No Class

- Last class on Sat 12/19
- Off: Mon 12/21 - Sat 1/02
- Return on Monday 1/04

Schedule Change

- Crypto delayed until after Winter Break

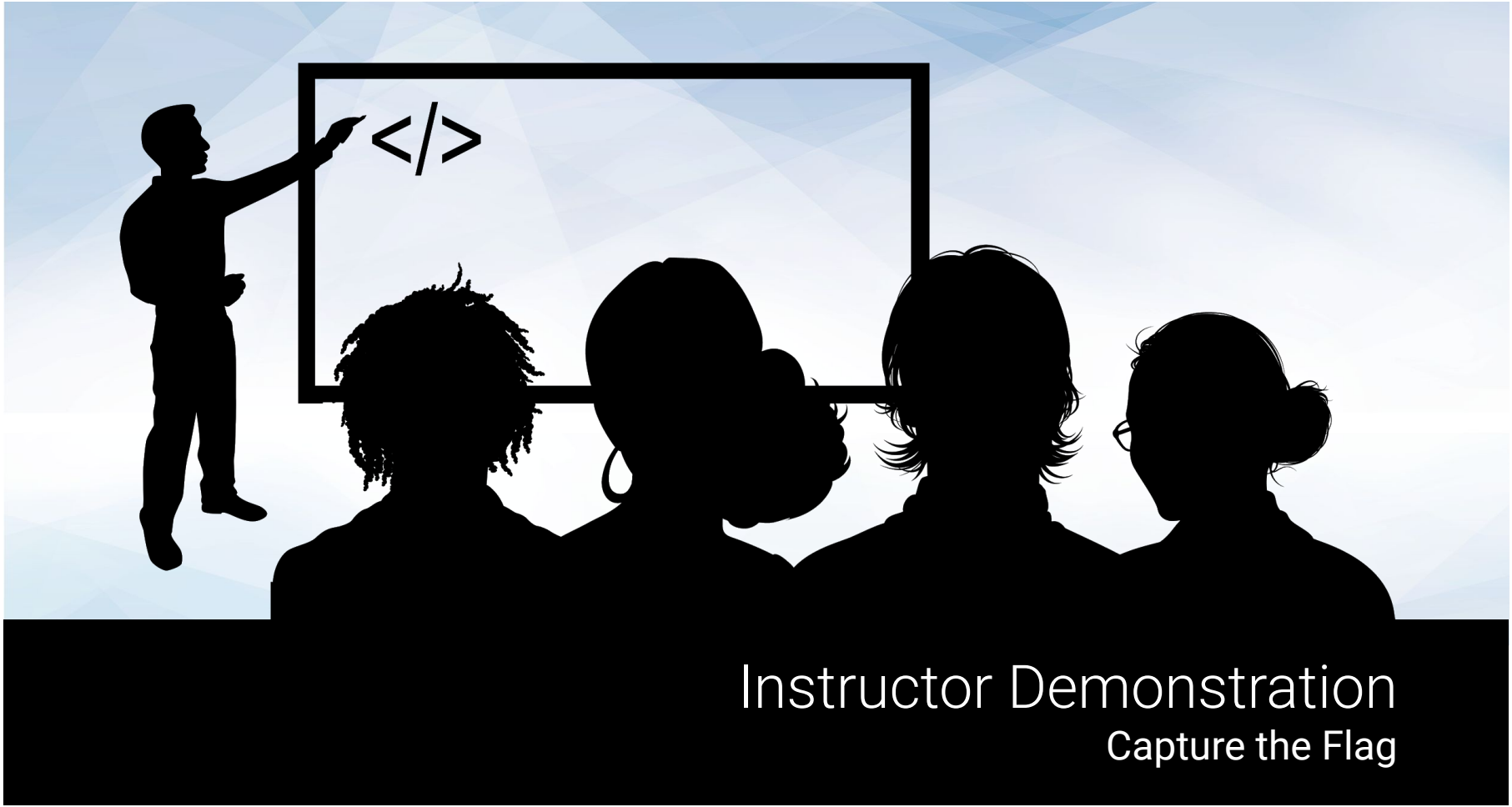
Today, we will be reviewing the past two networking units in a fun competition known as a **Capture the Flag (CTF)** contest.

CTF Instructions

- You'll be provided a spreadsheet with various networking questions.
- These are separated into topics (ports and protocols, packets, pings, etc.)
- You will download PCAP files to answer the questions. All answers for the PCAP items **are in the pcap**
- The answers to questions will serve as the **flags**, which you'll collect and document in your spreadsheet.
- Each flag has a different numeric point value. The more challenging the question, the higher the value.
- Total points will be calculated automatically in the spreadsheet.
- Whoever has the most points by the end of class, or whoever answers all questions correctly first, wins!

CTF Rules

- You can use your class notes, slides, and online materials (independent research)
- Flags don’t need to be answered in order.
- These will require independent research; we will not give you the answer
- Good luck! And have fun!



Instructor Demonstration

Capture the Flag

General Notes

- **For the PCAP items, all answers are in the PCAPs themselves**
  - If you try to use other resources you will get wrong answers
- **Enter answers in all lower case**
- **Any numerical answers should not include commas separating thousands**
  - E.g. 784567 not 784,567
- **All MAC addresses need “:” between pairs of hex characters**
  - Correct: 11:22:5f:88:77:9c
  - Wrong: 11225f88779c
- **Independent research is required; Google is your friend**
- **Using online conversion tools (like we used in class) is recommended**

Specific Section Notes

- **Where's Waldo's Address**
  - 27: This needs the hex of the ***ESC*** key/character (not the string "ESC")
  - 32: this needs the total IP count, not the count of *host/usable* IPs
- **Dragons Layers**
  - 35-39: use a word/name answer, not a number
- **The Ping Panther**
  - 44: the last name of the person who invented the ***ping*** command
  - 46: In Windows you run something other than "Traceroute" to perform a traceroute. This wants the name of that command.
- **The Grinch Stole my wifi Password**
  - 49: convert this binary into a string to get the WPA key
  - 50: this is to decrypt WPA; that is different than we we decrypted WEP