CENTRAL ILLINOIS HIGH SCHOOL CYBER SECURITY COMPETITION

ILLINOIS STATE UNIVERSITY • SCHOOL OF IT

Presented by Dmitry Zhdanov
2025 CAE Symposium

ILLINOIS STATE UNIVERSITY
Illinois' first public university

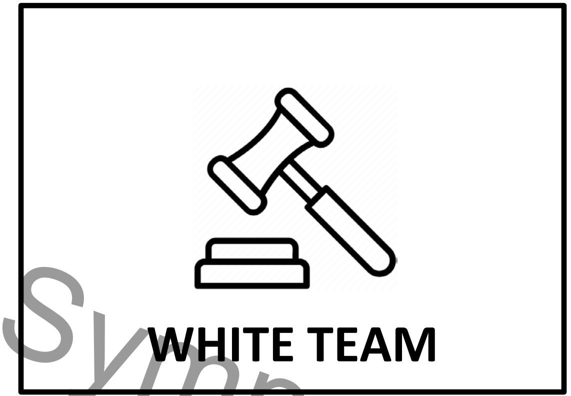
Industry Partner Support

- State Farm
- AFNI

Competition Structure

Offense

Defense



Management

Illinois State
University
Illinois' first public university

Central Illinois High School
Cyber Security
Competition
Illinois State University • School of IT

Blue Teams

1. Brimfield High School **(The Dream Team)**
2. Brimfield High School **(Renegade Dolphin)**
3. Normal Community High School **(NCHS Team 1)**
4. Normal Community High School **(NCHS Team 2)**
5. Pekin Community High School **(DNS)**
6. Pekin Community High School **(Dog4Shell)**
7. Wheaton Warrenville South High School **(Terrific Technological Tigers)**
8. Wheaton Warrenville South High School **(Ideal Data Collection)**
9. Illinois Valley Central High School **(Grey Ghosts)**
10. Gen Cyber Program **(Team GenCyber)**

Red Team

Professionals from State Farm, and Illinois State University

White Team

School of IT Cybesecurity Faculty

School of IT Staff

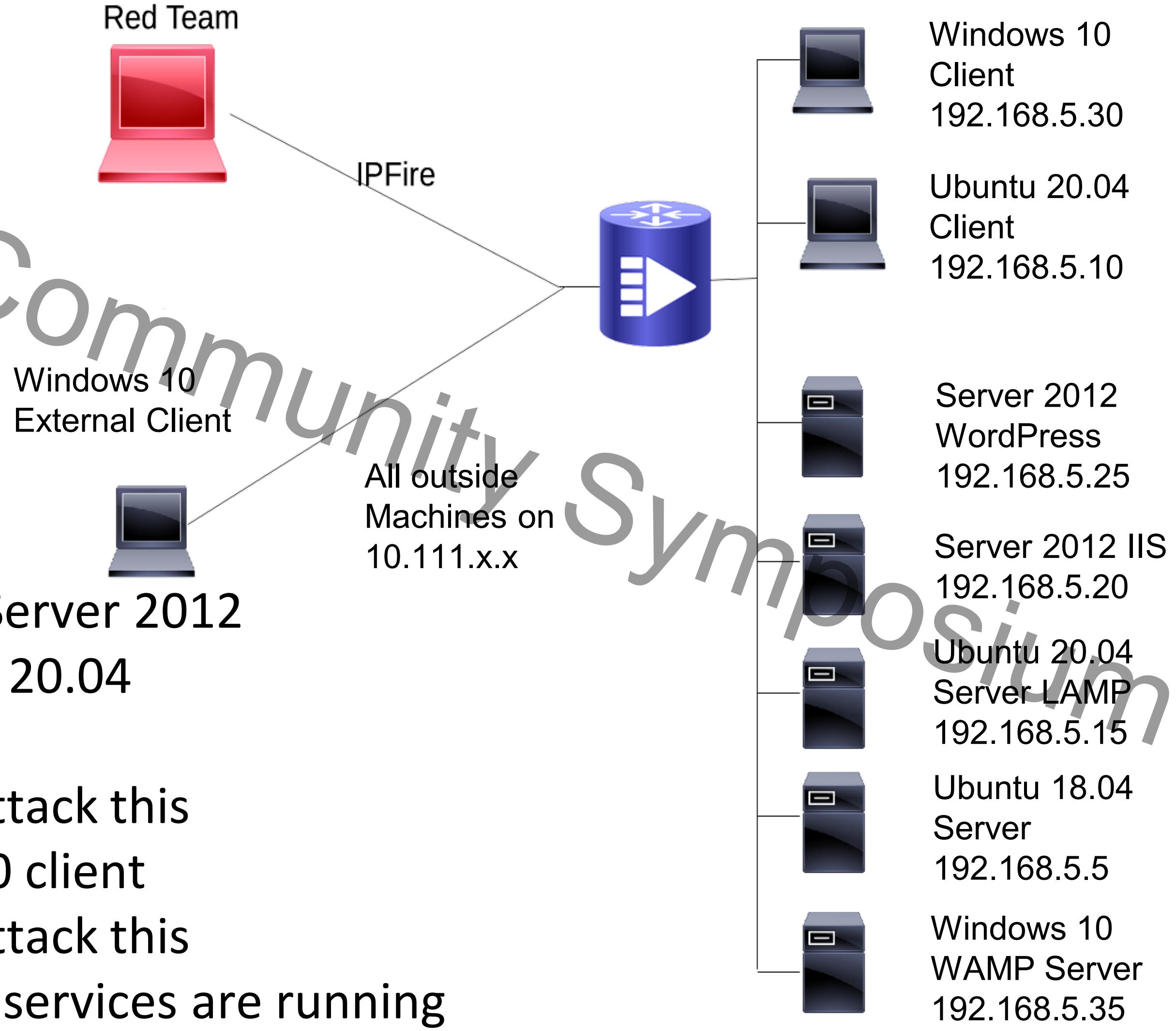
School of IT Student Volunteers

Scenario

Your team was just hired to work for a company, and you are inheriting the company network from some recently fired consultants (red team), who left on bad terms. Because of this, you are not really sure how secure the network is.

Your job is to evaluate the security of your network and protect its assets.

Topology and Services



- 7 Internal Machines
  - Windows 10 and Server 2012
  - Ubuntu 18.04 and 20.04
- IPFire Router
  - Red team won’t attack this
- 1 External Windows 10 client
  - Red team won’t attack this
  - Use to verify your services are running

Assets - Service Flags

Confirm through Win 10 External VM

Virtual Machine	Firewall Port	Flag (Text or file that must be present to be scored)
Ubuntu 18 Web	80	String cihscdc_white must exist in page service_check.html
Ubuntu 18 Web	22	File cihscdc_white.txt must exist in /home/cihscdc_white when logging in as “cihscdc_white”
Ubuntu 20 Client	222	File cihscdc_white.txt must exist in /home/cihscdc_white when logging in as “cihscdc_white”
Ubuntu 20 LAMP	800	String cihscdc_white must exist in page service_check.html
Win 2012 Web	220	File cihscdc_white.txt must exist in inetpub/ftproot
	8800	String cihscdc_white must exist in page service_check.html
Win 2012 WP	280	String cihscdc_white must exist in page service_check.html
Win 10 WAMP	8080	String cihscdc_white must exist in page service_check.html

Red Team Goal

- Change or delete the flags being served by various servers, listed in your team packet
- Launch other exploits

Scoring

- 33% - Services uptime
- 33% - Inject completion
- 33% - Defense against red team exploits

Injects

- Timed challenges from the White Team
- Goal is to
  - Find a flag hidden/encrypted in a file, code, or website
  - Install/configure/write a report
- Sent via Discord on your team’s channel after 10:30 am
- Submit via your team’s inject submission channel on Discord
  - Late submissions will have penalty

Injects details

- SSH attack
- Wireshark analysis
- File analysis
- Cryptanalysis (x2)
- Password cracking
- Resource inventory

Rules

- Don't change IP Addresses of VMs or chiscdc_white passwords
- Professional behavior at all times
- No assistance from anyone outside team
- No attacks on other teams, including white and red

Tips to be successful

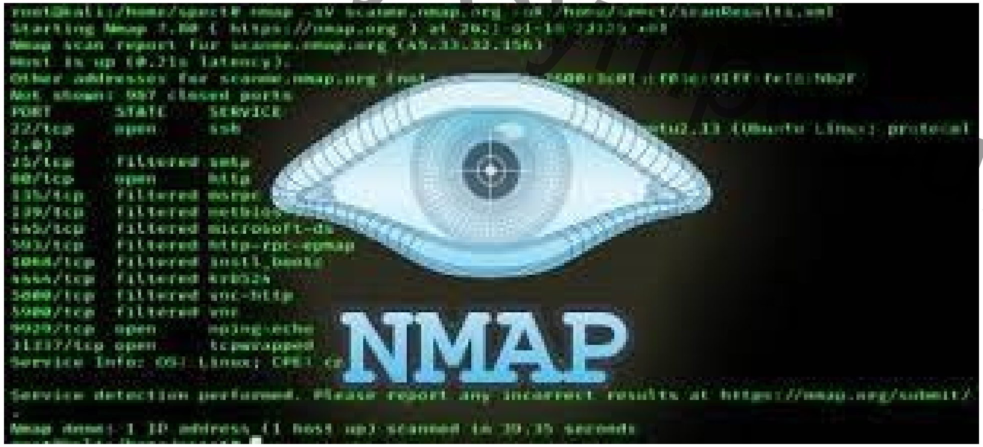
- Pick a captain
- Delegate duties
- “Area” experts
    - Linux, Windows, Firewall, networking, injects
- Have a plan!

Host Hardening

- Protect your VMs from red team's attacks
  - Change weak passwords
  - Update old versions of software that are vulnerable to attacks
  - Malware could be installed – check and remove!
  - Router and host firewall misconfigurations: verify!
  - Shut down unneeded services!

Remove Unnecessary services

- There could be vulnerable or malicious services opening ports
- You may close/delete unnecessary services
- Use a port scanner to detect what is listening



```
root@kali:/home/spect[illegible] nmap -sV scanme.nmap.org -oX /home/spect/scanResults.xml
Starting Nmap 7.80 ( https://nmap.org ) at 2021-01-18 [illegible]
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.21s latency).
Other addresses for scanme.nmap.org (not [illegible] 2600:3c01::f03c:91ff:fe18:bb2f
Not shown: 987 closed ports
PORT       STATE     SERVICE
22/tcp     open      ssh        [illegible]tu2.13 (Ubuntu Linux; protocol
2.0)
25/tcp     filtered  smtp
80/tcp     open      http
135/tcp    filtered  msrpc
139/tcp    filtered  netbios[illegible]
445/tcp    filtered  microsoft-ds
593/tcp    filtered  http-rpc-epmap
1068/tcp   filtered  instl_bootc
4444/tcp   filtered  krb524
5800/tcp   filtered  vnc-http
5900/tcp   filtered  vnc
9929/tcp   open      nping-echo
31337/tcp  open      tcpwrapped
Service Info: OS: Linux; CPE: c[illegible]

Service detection performed. Please report any incorrect results at https://nmap.org/submit/
.
Nmap done: 1 IP address (1 host up) scanned in 39.35 seconds
```

Be Proactive

- What did you miss in your strategy?
- Use a vulnerability scanner to discover existing threats
- Nessus is a free and easy to use scanner

White Team Volunteers

- Each team will have ISU white team volunteer helpers over the day
- Get them involved

- ASK QUESTIONS!

Event Schedule

[Venue: Julian 26-30]

10:00 a.m. – Competition begins

10:15 a.m. – Refreshments

11:00 a.m. – Red team starts hacking

12:00 p.m. – 1:00 p.m. – Lunch

1:00 p.m. – Competition resumes

3:00 p.m. – Competition ends

[Venue: STV 401]

3:30 – 4:00 p.m. – Awards ceremony, Red team reflection

Illinois State University
Illinois' first public university

Central Illinois High School
Cyber Security Competition
Illinois State University • School of IT

CIHSCDC Winners

Dog4 Shell (Pekin Community High School)

Team GenCyber

Normal Community High School Team 1

ILLINOIS STATE UNIVERSITY
Illinois' first public university

CENTRAL ILLINOIS HIGH SCHOOL CYBER SECURITY COMPETITION
ILLINOIS STATE UNIVERSITY • SCHOOL OF IT

Questions?

Thank you!