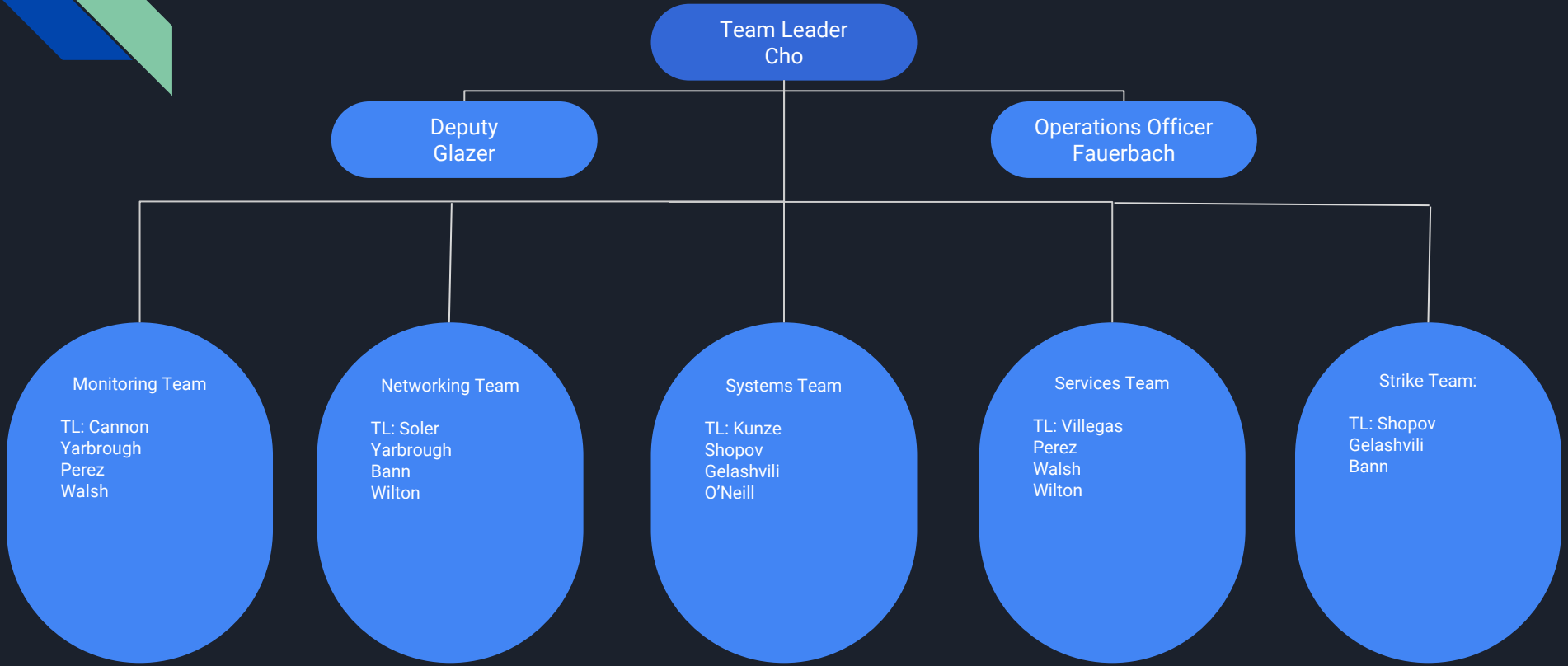
USMA CCDC

Task Organization



Headquarters

Team Leader: Cho

Deputy Team Leader: Glazer

Operations Officer: Fauerbach

Mission

To educate, train, and prepare the USMA Collegiate Cyber Defense Competition team for the Collegiate Cyber Defense Competition on 27 January 2018 in order to win the competition and create the foundation for future teams.

Available Assets

- Cisco Routers
- Cisco Switches
- Vsphere
- EECS Net
- Historical resources from previous CDX teams
- All online or printed resources
  - I.e server-world.info, other FAQs

http://www.nationalccdc.org/index.php/competition/competitors/rules

Constraints

- Time
- Number of VMs allowed and max processing power for each
- No paid resources
- Lack of internet access
- No external media

CCDC Essential Skill Set

- Common Unix Printing System (CUPS)
- Computer Forensics
- Database administration
- Directory services (e.g., Active Directory)
- Domain Name System (DNS)
- E-mail Servers (Exchange and sendmail)
- File Servers
- File Transfer Protocol (FTP) services
- Hacking Tools
- HTML
- Networking devices (to include switches, firewalls, routers)
- Samba
- Secure Shell (SSH)
- SQL
- Syslog
- Understand Cyber Law
- Virtual Private Networking (VPN)/remote access
- Web servers (both Apache and IIS)
- Windows and UNIX/Linux system administration and hardening

Risk Assessment

- Multiple operating systems
  - Windows 2008/7, Windows 2003/2000 Server and Professional, Windows XP Professional, Windows Vista, Various BSD distributions, various Linux distributions, and Solaris
- Diverse services
- Analyze live traffic for malware
- Inherit and Defend
  - Identify pre-installed backdoors
  - Troubleshooting
  - What does right look like

Tasks

Specified

- Establish COA for next 12 lessons
- Identify CCDC team for next semester (12 PAX)
- Prepare reference material for services

Implied

- Determine what we need to know for the CCDC
- Reach out to mentors to learn additional skill sets

Timeline

Lesson	Date	Item
28	07 NOV 17	Mission Analysis Brief
29	09 NOV 17	Identify familiar and new services
30	14 NOV 17	Identify tools and alternatives
31	16 NOV 17	Special Equipment requests due
32	20 NOV 17	Building systems from the ground up

Timeline

Lesson	Date	Item
33	22 NOV 17	Left seat/right seat
34	28 NOV 17	Pentest
35	30 NOV 17	Alternates configure network
36	04 DEC17	Fixing broken setups
37	06 DEC 17	Pentest
38	08 DEC 17	Formalize knowledge
39	12 DEC 17	Backbrief and AAR

Systems Team

Team Leader:	Kunze
Servers/SELinux (operate):	Shopov
End-user Unix (sanitize):	Gelashvili
End-user Windows (sanitize):	O’Neill

System Requests

Basic images:

- RedHat/SELinux
- VirtualBox
- CentOS
- Fedora Server

Risk Assessment:

- Pre-installed vulnerabilities (rootkits, backdoors, unnecessary services)
- Set up, configure, and harden: HTTP, SSH, FTP, RDP, Telnet, SSL, DNS, Certificates
- Create users and groups and set security policy
- Web, email, authentication services

Windows Machine

- Before receiving graycell image:
  - Learn how to use FTK imager, autoruns, and process hacker, and be able to install and run SCAP
  - Identify the startup registry keys.
  - Become familiar with Powershell and how it can bypass Group Policy
  - Become familiar with hidden files and directories.
  - Make sure Group Policy is set by the domain controller/Active Directory.
- Sanitization
  - Image RAM and cache to look for hidden processes.
  - Use installed utilities to find malware.
  - Check the startup registry keys
  - Remove any identified malware
  - Scrub Services
  - Scrub Programs allowed through the windows firewall
  - Scrub Through installed applications

Networking Team

Team Leader:	Soler
Firewall/Rtr./Switch:	Yarbrough
Proxy:	Bann

Network

Network Diagram

Firewall Implementation Plan

Proxy Plan

Services Team

Team Leader:	Villegas
DNS:	Perez
AD:	Wilton
HTTP/HTTPS:	Walsh
Email:	Perez
FTP:	Wilton

Services

For each service:

- Subnet
- OS selected (I.e. win7/8, win 0/3 server, linux/unix)
- Description of application software
- Config Required
- Summary of dependency on other services (if any)
- Transport-layer ports used
- Security measures taken
- Risk Assessment (eventually become attack tree)
- Create HowTos documentation

Monitoring Team

Team Leader:	Cannon
Ops. Monitoring:	Perez
Net. Monitoring:	Walsh
Host Monitoring:	Yarbrough

Monitoring

Operations- Understand how to score during CCDC and web scraping and data visualization

Network- Monitors network at application, transport and network layer, understand how to read packets sent between systems to see if they are malicious or not

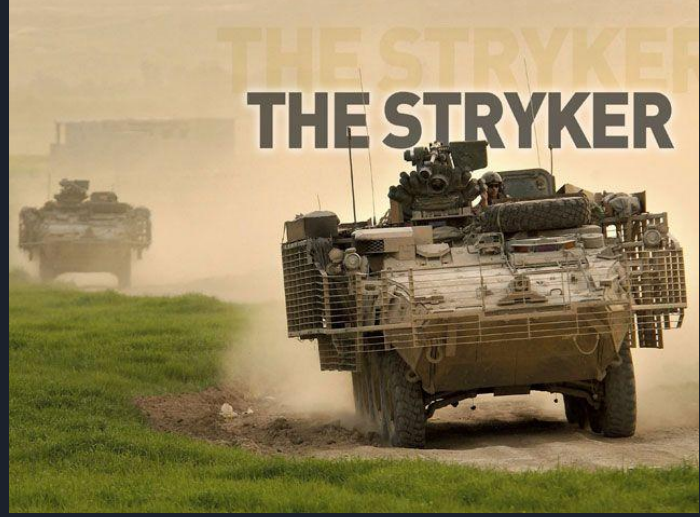
Host- Monitor individual services for loss of confidentiality and integrity, able to read system logs (http, https, smtp, pop3, ssh, sql, dns, ftp) details on appendix C and know bash/PowerShell scripts

- Fully understand how to interpret the percentage of scores and be able to visualize them
- Understand basic processes, common ports and packets that are used on the systems and network
- Understand common files, functionality and log files of different services

Strike Team

Team Leader:	Shopov
Malware/Reverse ENG:	Gelashvili
Network Forensics:	Bann
Offensive Ops:	Gelashvili

Strike Team



Forensics Toolkit:

- Nmap/Nessus - vulnerability scanner programs
- Encryption And Cryptanalysis

Forensic Challenges:

- Analyze potentially malicious code via static and dynamic methods
- Analyze malware to determine its functionality
- Based on those analyses, determine ways to mitigate the malware

CTF:

- Exploit vulnerable software to discover flags embedded in various systems.

Questions