Operational Cybersecurity Labs IT Unconference

•••

Alex Keller, Stanford School of Engineering

Topic

Exploring the utility and benefits of authentic low-risk cybersecurity labs for experimentation and skills advancement.

Law of two feet -- No harm no foul if you duck out and check out another session!

Experimentation & Lab Infrastructure is Critical to Evolution

- Safe space to fail.
- Try new techniques, tactics, and technologies.
- Discovery -- It's not magic!
- Learning for the sake of curiosity, not just a specific objective.
- Build it, break it, fix it, repeat...

My Formative Experience - Collegiate Cybersecurity Competitions

- **Collegiate Cyber Defense Competition (CCDC)**
  Student team defends fictitious business infrastructure against professional Red Team.

- **Collegiate Penetration Testing Competition (CPTC)**
  Student team conducts an offensive engagement (penetration test) against a fictitious business.

Stanford Applied Cyber Team

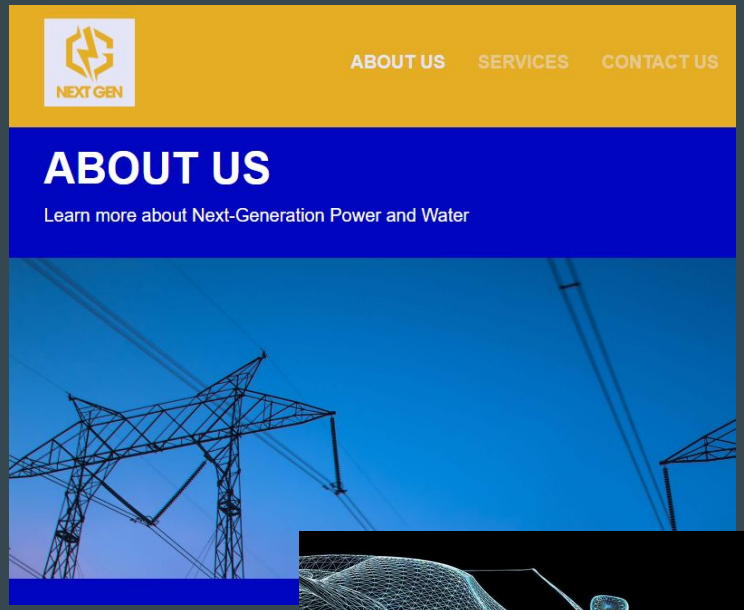
Current CPTC National Champions (3-peat) & CCDC ranked 3rd in Nation.

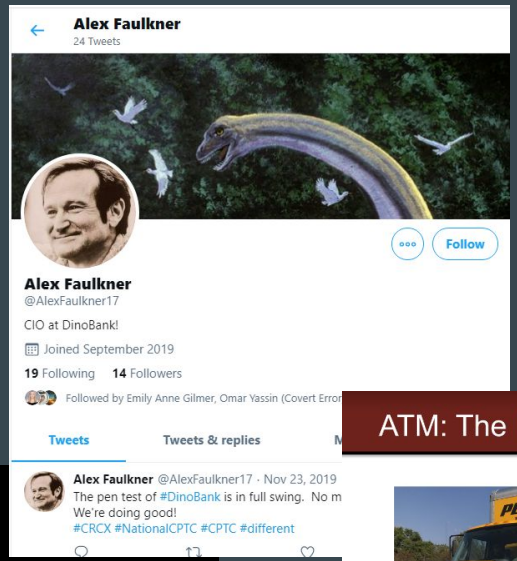
Placed 1st/2nd/3rd in 19 cyber competitions since January 2016.

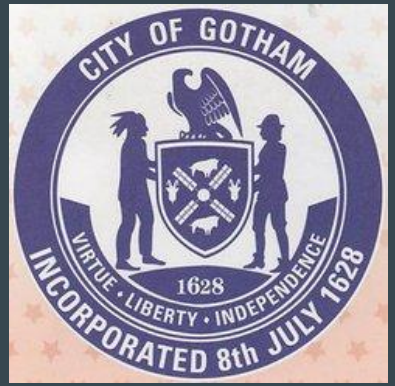
Discovered & Disclosed Vulnerabilities:

CVE-2019-19249 QueryTree authorization bypass
https://nvd.nist.gov/vuln/detail/CVE-2019-19249

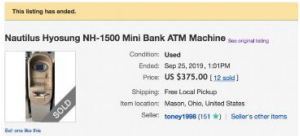
CVE-2019-19250 OpenTrade SQL injection
https://nvd.nist.gov/vuln/detail/CVE-2019-19250







ATM: The Hyosung 1500



#dinobankroadtrip

CONFIDENTIAL

Different discussion....

SAMPLE EXAM QUESTIONS (continued)

1. Which one of the following is the MOST important security consideration when selecting a new computer facility?

   (A) Local law enforcement response times
   (B) Adjacent to competitors' facilities
   (C) Aircraft flight paths
   (D) Utility infrastructure

   Answer - D

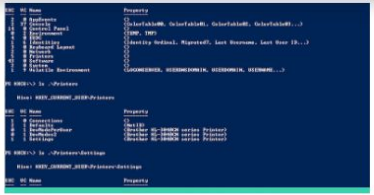
2. Which one of the following describes a SYN flood attack?

   (A) Rapid transmission of Internet Relay Chat (IRC) messages
   (B) Creating a high number of half-open connections
   (C) Disabling the Domain Name Service (DNS) server
   (D) Excessive list linking of users and files

   Answer - B

Qualys. Training & Certification

PowerShell Security Best Practices_



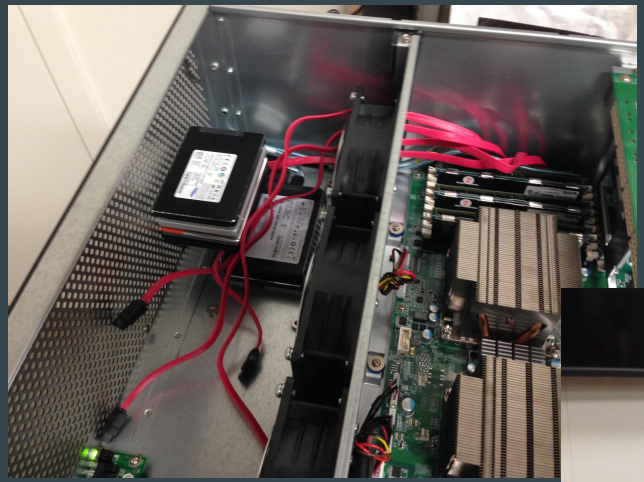
Isidoros Monogioudis

Read More From Isidoros Monogioudis >

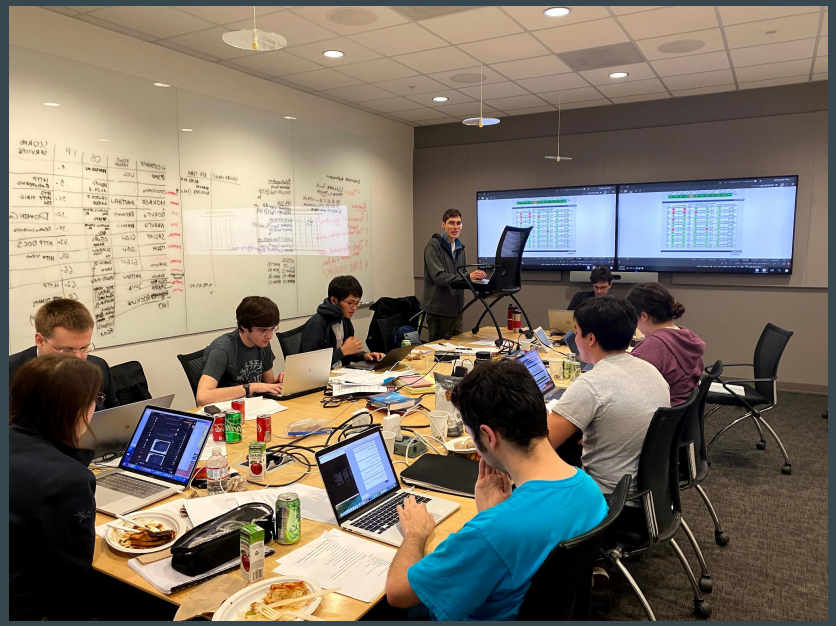
October 8, 2019 | 9 Min Read

Post Tweet Share

What does it look like?



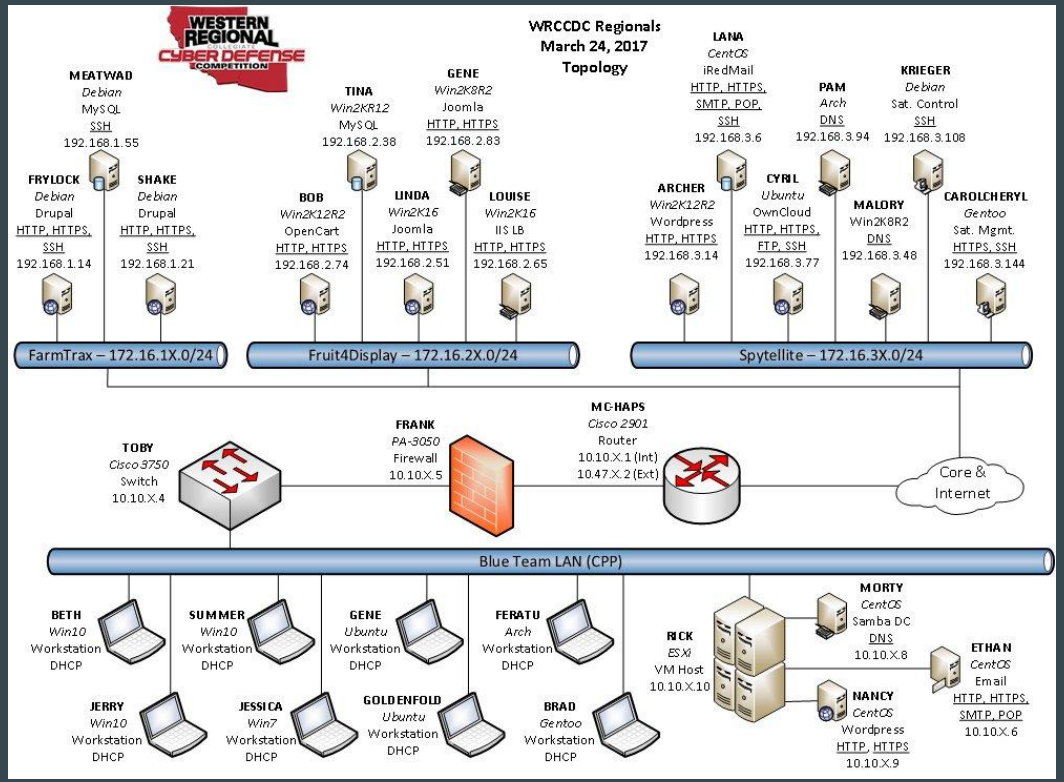
What does it look like?

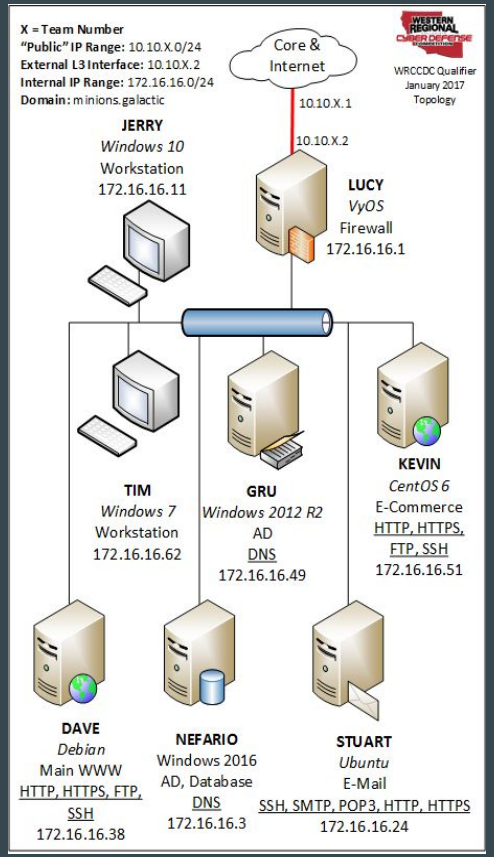


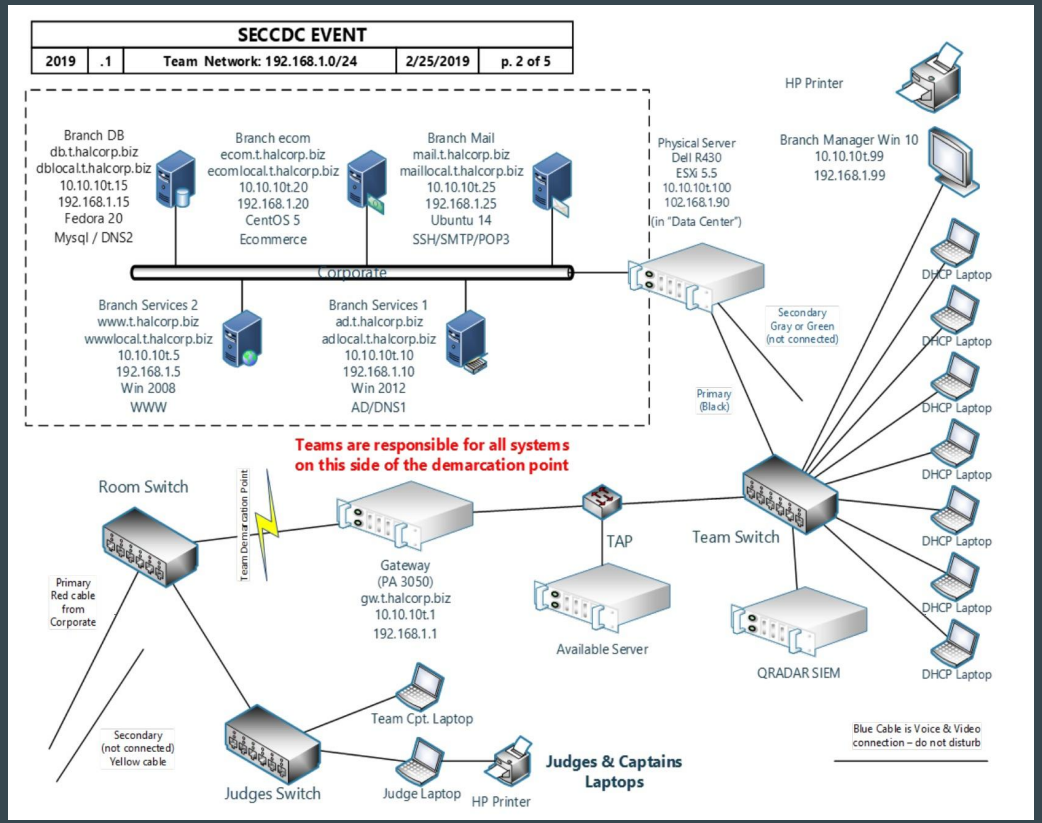
What does it look like?

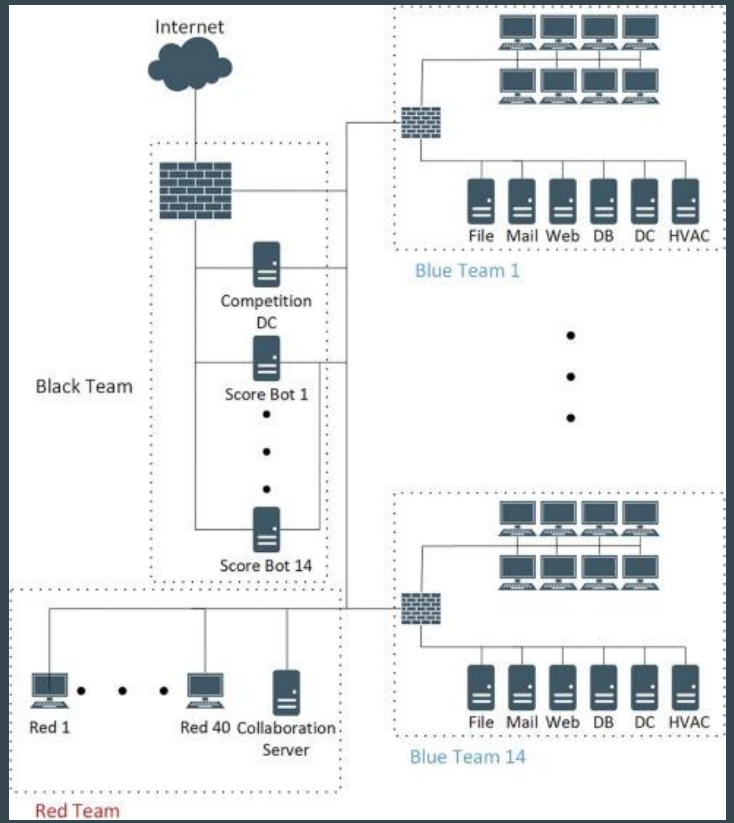
Photo Credit: Stacy Lee

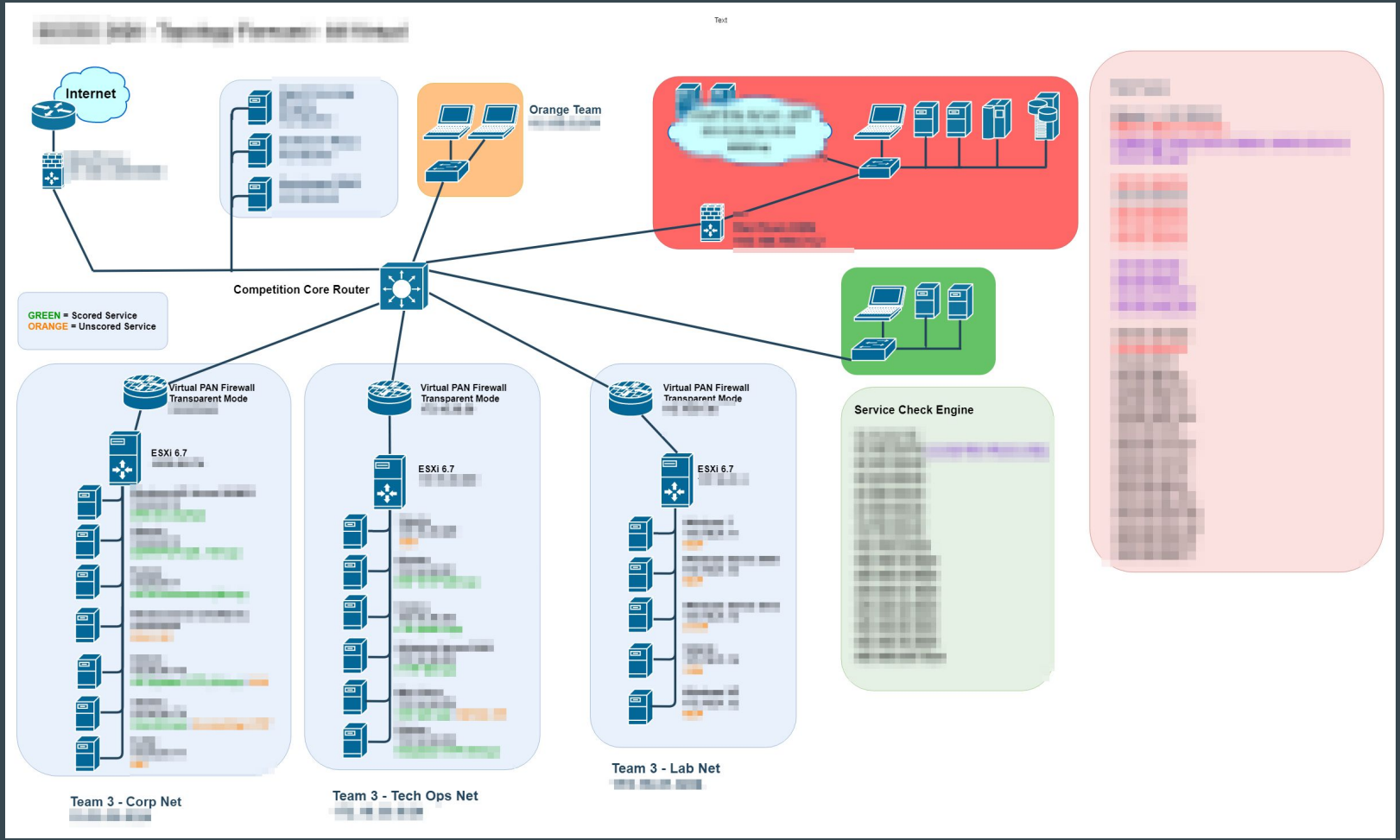
Real Infrastructure?





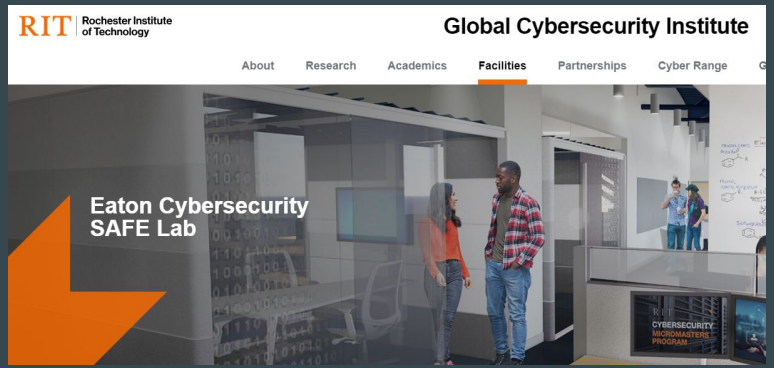

SECCDC EVENT
2019 .1 Team Network: 192.168.1.0/24 2/25/2019 p. 2 of 5
Branch DB
db.t.halcorp.biz
dblocal.t.halcorp.biz
10.10.10t.15
192.168.1.15
Fedora 20
Mysql / DNS2
Branch ecom
ecom.t.halcorp.biz
ecomlocal.t.halcorp.biz
10.10.10t.20
192.168.1.20
CentOS 5
Ecommerce
Branch Mail
mail.t.halcorp.biz
maillocal.t.halcorp.biz
10.10.10t.25
192.168.1.25
Ubuntu 14
SSH/SMTP/POP3
Corporate
Branch Services 2
www.t.halcorp.biz
wwwlocal.t.halcorp.biz
10.10.10t.5
192.168.1.5
Win 2008
WWW
Branch Services 1
ad.t.halcorp.biz
adlocal.t.halcorp.biz
10.10.10t.10
192.168.1.10
Win 2012
AD/DNS1
Physical Server
Dell R430
ESXi 5.5
10.10.10t.100
102.168.1.90
(in "Data Center")
HP Printer
Branch Manager Win 10
10.10.10t.99
192.168.1.99
DHCP Laptop
Secondary
Gray or Green
(not connected)
Primary
(Black)
Teams are responsible for all systems
on this side of the demarcation point
Room Switch
Team Demarcation Point
Gateway
(PA 3050)
gw.t.halcorp.biz
10.10.10t.1
192.168.1.1
TAP
Team Switch
Available Server
QRADAR SIEM
Primary
Red cable
from
Corporate
Secondary
(not connected)
Yellow cable
Team Cpt. Laptop
Judges Switch
Judge Laptop
HP Printer
Judges & Captains
Laptops
Blue Cable is Voice & Video
connection – do not disturb


Internet
File Mail Web DB DC HVAC
Blue Team 1
Competition
DC
Black Team
Score Bot 1
Score Bot 14
File Mail Web DB DC HVAC
Blue Team 14
Red 1
Red 40
Collaboration
Server
Red Team


Text
Internet
Orange Team
Competition Core Router
GREEN = Scored Service
ORANGE = Unscored Service
Virtual PAN Firewall
Transparent Mode
ESXi 6.7
Virtual PAN Firewall
Transparent Mode
ESXi 6.7
Virtual PAN Firewall
Transparent Mode
ESXi 6.7
Service Check Engine
Team 3 - Corp Net
Team 3 - Tech Ops Net
Team 3 - Lab Net

Other Examples (edu & commercial)

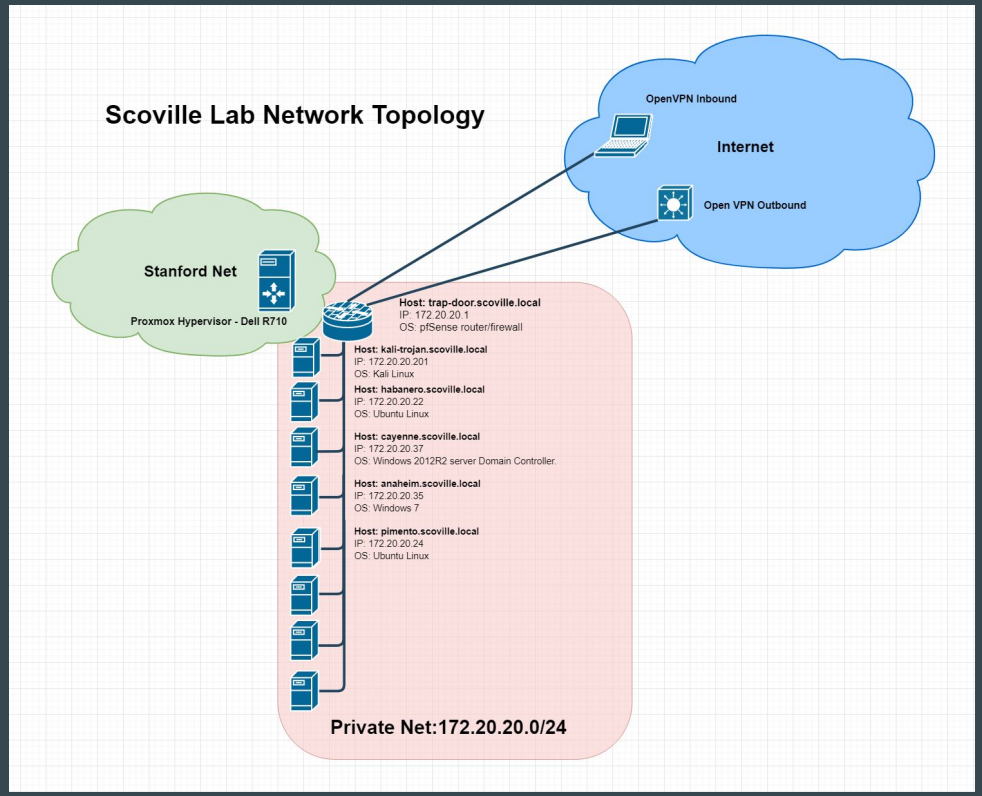
Hack The Box
PEN-TESTING LABS



Try Hack Me

Kaos Corp - Mini-Lab

- Dell R720
- Proxmox Hypervisor
- pfSense (virtualized) Router/Firewall/VPN
- VMs (reset every 4 hours)
  - Kali Linux
  - Windows 2012R2 DC
  - Windows 7
  - Ubuntu 18.04 web server
  - ????



Cybersecurity Lab Challenges

- Safety & Isolation
- Accessible
- Reasonable learning curve
- Repeatable
- Reliable
- Scalable
- ???

Exercises

- Blue Team
  - Attack surface discovery
  - Network fortification
  - Active defense
  - Network forensics
  - Host forensics
  - JIT (just in time) mitigation
  - Blue Team like Red Team (attack yourself!)

Exercises

- Red Team
  - OSINT (open source intelligence)
  - Reconnaissance
  - Enumeration
  - Exploitation
  - Privilege escalation
  - Persistence
  - C2 (command & control)

RED vs BLUE (or) King of the Hill

Discussion - What would you like to learn?

- Network mapping (Nmap)
- Process discovery (Process Monitor, AuditD, etc.)
- Network forensics (netflow, tcpdump, Wireshark)
- Exploitation (Metasploit, Empire, Impacket, Burp)
- Host monitoring (Suricata, OSSEC, Sysmon)
- Hardening
- ???

Discussion - How would we build it?

- Custom -- On premise?
  - ESXi, Proxmox, OpenStack, oVIRT, etc.
- Custom -- Cloud?
  - LaForge https://github.com/gen0cide/laforge
- Apache VCL? https://vcl.apache.org
- Emulab? https://www.emulab.net
- ???

Thanks!

- Stanford Engineering
- Stanford Applied Cyber
- Stanford Information Security Office

Misc.