



Computer Network Security

COMP 178 | Spring 2025 | University of the Pacific | Jeff Shafer

XP Cyber Labs

Upcoming Assignments

- **Lab 6 – Post Exploitation: Due Feb 26th**
- **Lab 7 – Password Testing: Due March 5th**
- **Video Presentation Peer Reviews – 3 each**
 - Canvas will auto-assign on March 2nd
(look in the same assignment where you uploaded the video)
 - **Due March 9th**

Bonus Resources

Bonus Resources on Class Website

Linux Post-Exploit Cheat Sheet

Windows Post-Exploit Cheat Sheet

Tools! More Tools! Yet More Tools!

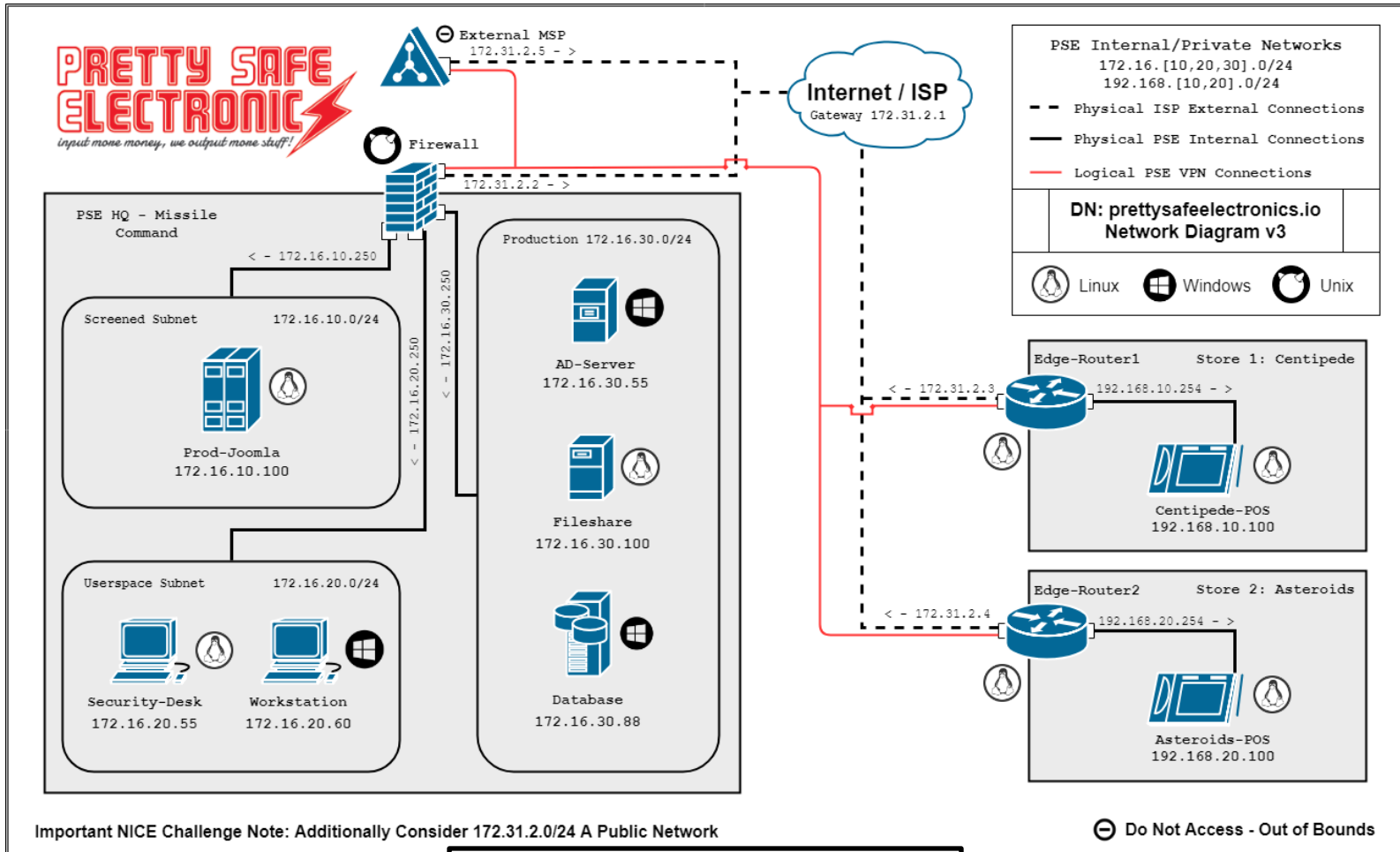
(For enumeration, privilege escalation, “living off the land”, ...)

XP Cyber Labs

- **Real-world cybersecurity challenges**
 - Narrative scenarios
 - Full business environments (servers, services, workstations, networks)
- No installation required (web portal)



XP Cyber Labs



XP Cyber Labs

- Open ended labs
 - Given broad description of task to accomplish and perhaps a few hints
 - Multiple paths can lead to final solution
 - **You are expected to document your solution before submitting**

NICE Challenge Webportal

Jeff Shafer
Current User

PLAYER CURATOR

Dashboard Upcoming Reservations Workspaces Submissions Helpdesk & FAQ

spring_2020_comp_178 | Jeff Shafer

Submit Challenge Attempt

Virtual Machines

Machine Name	Status	Actions	Open	Console ?
Asteroids-PoS	Powered On	Action	HTML5	VMRC
Asteroids-Router	Powered On	Action	HTML5	VMRC
Centipede-PoS	Powered On	Action	HTML5	VMRC
Centipede-Router	Powered On	Action	HTML5	VMRC
Database	Powered On	Action	HTML5	VMRC
Domain-Controller	Powered On	Action	HTML5	VMRC
Fileshare	Powered On	Action	HTML5	VMRC
Firewall	Powered On	Action	HTML5	VMRC
Prod-Web	Powered On	Action	HTML5	VMRC
Security-Desk	Powered On	Action	HTML5	VMRC
Workstation-Desk	Powered On	Action	HTML5	VMRC

Checks

Status	Check Description	Check Type	Check State	Last Changed
✓	AD Accounts That Do Not Need a Password Reset Are Not Marked for One [Should Stay Green]	Integrity Check ?	Desired State	10:04 AM PST
✓	AD Accounts That Do Need a Password Reset Are Marked for One	Challenge Check ?	Desired State	10:26 AM PST

Remote desktop to virtual machines

Documentation Challenge Info Meeting Notes Network Map

Please enter any tools, programs, and utilities used to complete the challenge.

Document all necessary steps and actions taken to complete the challenge in the field below. Document as if you were writing documentation for the company. This information will be sent to your challenge Curator for review.*


Rich text editor with toolbar (bold, italic, underline, etc.) and a large text area for documentation.

Workspaces

portal.nice-challenge.com/webconsole?link=wss%3A%2F%2Fportal.nice-challenge.com%2Fwmksconsole%2Fb16f80a63f445e4d%3Fvmhost%3D...

Domain-Controller

Send CTRL-ALT-DEL



Recycle Bin

Windows Server 2012 R2

Windows Server 2012 R2 Standard
Build 9600

6:29 PM
3/1/2020

The image shows a remote desktop session of a Windows Server 2012 R2 desktop. The desktop background is black with the Windows logo and 'Windows Server 2012 R2' text. A single 'Recycle Bin' icon is visible in the top-left corner. The taskbar at the bottom is blue and contains icons for the Start menu, a folder, a command prompt, and a file explorer. The system tray on the right shows the time as 6:29 PM on 3/1/2020. The browser window title is 'Domain-Controller' and the address bar shows a URL from 'portal.nice-challenge.com'. A 'Send CTRL-ALT-DEL' button is located in the top-right corner of the remote desktop window.

spring_2020_comp_178 | Jeff Shafer

Submit Challenge Attempt

Workspaces

Machine Name	Status	Actions	Open Console ?
Asteroids-PoS	Powered On	Action	HTML5 VMRC
Asteroids-Router	Powered On	Action	HTML5 VMRC
Centipede-PoS	Powered On	Action	HTML5 VMRC
Centipede-Router	Powered On	Action	HTML5 VMRC
Database	Powered On	Action	HTML5 VMRC
Domain-Controller	Powered On	Action	HTML5 VMRC
Fileshare	Powered On	Action	HTML5 VMRC
Firewall	Powered On	Action	HTML5 VMRC
Prod-Web	Powered On	Action	HTML5 VMRC
Security-Desk	Powered On	Action	HTML5 VMRC
Workstation-Desk	Powered On	Action	HTML5 VMRC

Status	Check Description	Check Type	Check State	Last Changed
✓	AD Accounts That Do Not Need a Password Reset Are Not Marked for One [Should Stay Green]	Integrity Check ?	Desired State	10:04 AM PST
✓	AD Accounts That Do Need a Password Reset Are Marked for One	Challenge Check ?	Desired State	10:26 AM PST

Recap of Challenge Objectives

Documentation Challenge Info Meeting Notes Network Map

Please enter any tools, programs, and utilities used to complete the challenge.

Input field with a plus button

Document all necessary steps and actions taken to complete the challenge in the field below. Document as if you were writing documentation for the company. This information will be sent to your challenge Curator for review.*

Rich text editor with toolbar and content area

portal.nice-challenge.com/workspace#

Filesnare	Powered On	Action	HTML5	VMRC
Firewall	Powered On	Action	HTML5	VMRC
Prod-Web	Powered On	Action	HTML5	VMRC
Security-Desk	Powered On	Action	HTML5	VMRC
Workstation-Desk	Powered On	Action	HTML5	VMRC

Documentation Challenge Info Meeting Notes Network Map

Ricardo Cortes
This might be pretty bad, I was reading an article online today and it talked about how businesses are being hacked more frequently because of weak passwords. How sure are we that this won't happen to us?

Ashley Steele
I know for sure that my password is strong, but I don't know about anyone else's.

Shawn O'Keefe
I'm in the same boat as Ashley. Perhaps @playerone could take this opportunity to get some penetration testing experience.

Ashley Steele
That's actually a great idea. Try performing a dictionary brute force attack on our Active Directory users. Perform a dictionary attack on all user logins except your own. Metasploit, Hydra, or Nmap probably have tools for something like this. Remember, you're a Domain Admin. So, if you get into an account, log in to Domain-Controller and set that user's account to require a password reset on next login.

Ricardo Cortes
I'll send out a notice saying that anyone who sees the reset screen needs to set their password to something more complex.

Ashley Steele
Good call, @rcortes.

Shawn O'Keefe
@asteele, do you have a recommended wordlist that playerone should use for the dictionary attack?

Ashley Steele
Kali comes with a good password list. You should be able to find it in /usr/share/wordlists on Security-Desk. I think it's called rockyou, or something like that.

Ricardo Cortes
@playerone, that is the wordlist I want you to use. Be sure to only request password resets from accounts that you were able to brute force with that wordlist. There's no need to force users to change their passwords if they're already pretty secure.

© 2016-2020 NICE Challenge Project | Legal Agreements

spring_2020_comp_178 | Jeff Shafer

Submit Challenge Attempt

Virtual Machines

Machine Name	Status	Actions	Open Console ?
Asteroids-PoS	Powered On	Action	HTML5 VMRC
Asteroids-Router	Powered On	Action	HTML5 VMRC
Centipede-PoS	Powered On	Action	HTML5 VMRC
Centipede-Router	Powered On	Action	HTML5 VMRC
Database	Powered On	Action	HTML5 VMRC
Domain-Controller	Powered On	Action	HTML5 VMRC
Fileshare	Powered On	Action	HTML5 VMRC
Firewall	Powered On	Action	HTML5 VMRC
Prod-Web	Powered On	Action	HTML5 VMRC
Security-Desk	Powered On	Action	HTML5 VMRC
Workstation-Desk	Powered On	Action	HTML5 VMRC

Checks

Status	Check Description	Check Type	Check State	Last Changed
✓	AD Accounts That Do Not Need a Password Reset Are Not Marked for One [Should Stay Green]	Integrity Check ?	Desired State	10:04 AM PST
✓	AD Accounts That Do Need a Password Reset Are Marked for One	Challenge Check ?	Desired State	10:26 AM PST

Network Topology

- Documentation
- Challenge Info
- Meeting Notes
- Network Map

Please enter any tools, programs, and utilities used to complete the challenge.

Document all necessary steps and actions taken to complete the challenge in the field below. Document as if you were writing documentation for the company. This information will be sent to your challenge Curator for review.*

Rich text editor with toolbar (bold, italic, underline, etc.)

Workspaces

portal.nice-challenge.com/workspace#

Database	Powered On	Action	HTML5	VMRC
Domain-Controller	Powered On	Action	HTML5	VMRC
Fileshare	Powered On	Action	HTML5	VMRC
Firewall	Powered On	Action	HTML5	VMRC
Prod-Web	Powered On	Action	HTML5	VMRC
Security-Desk	Powered On	Action	HTML5	VMRC
Workstation-Desk	Powered On	Action	HTML5	VMRC

Documentation Challenge Info Meeting Notes Network Map

PRETTY SAFE ELECTRONIC
input more money, we output more stuff!

External MSP 172.31.2.5 ->

Internet / ISP Gateway 172.31.2.1

Firewall 172.31.2.2 ->

PSE Internal/Private Networks
 172.16. [10,20,30].0/24
 192.168. [10,20].0/24

-- Physical ISP External Connections
 — Physical PSE Internal Connections
 — Logical PSE VFN Connections

DN: prettysafeelectronics.io
Network Diagram v3

Linux Windows Unix

PSE HQ - Missile Command 172.16.10.250

Production 172.16.30.0/24

AD-Server 172.16.30.55

Fileshare 172.16.30.100

Database 172.16.30.88

Screened Subnet 172.16.10.0/24

Prod-Joomla 172.16.10.100

Userspace Subnet 172.16.20.0/24

Security-Desk 172.16.20.55

Workstation 172.16.20.60

Edge-Router1 Store 1: Centipede 192.168.10.254 ->

Centipede-POS 192.168.10.100

Edge-Router2 Store 2: Asteroids 192.168.20.254 ->

Asteroids-POS 192.168.20.100

Important NICE Challenge Note: Additionally Consider 172.31.2.0/24 A Public Network

⊘ Do Not Access - Out of Bounds

© 2016-2020 NICE Challenge Project | Legal Agreements

NICE Challenge Webportal

Jeff Shafer
Current User

PLAYER CURATOR

Dashboard Upcoming Reservations Workspaces Submissions Helpdesk & FAQ

spring_2020_comp_178 | Jeff Shafer

Submit Challenge Attempt

Workspaces

Machine Name	Status	Actions	Open Console ?
Asteroids-PoS	Powered On	Action	HTML5 VMRC
Asteroids-Router	Powered On	Action	HTML5 VMRC
Centipede-PoS	Powered On	Action	HTML5 VMRC
Centipede-Router	Powered On	Action	HTML5 VMRC
Database	Powered On	Action	HTML5 VMRC
Domain-Controller	Powered On	Action	HTML5 VMRC
Fileshare	Powered On	Action	HTML5 VMRC
Firewall	Powered On	Action	HTML5 VMRC
Prod-Web	Powered On	Action	HTML5 VMRC
Security-Desk	Powered On	Action	HTML5 VMRC
Workstation-Desk	Powered On	Action	HTML5 VMRC

Status	Check Description	Check Type	Check State	Last Changed
✓	AD Accounts That Do Not Need a Password Reset Are Not Marked for One [Should Stay Green]	Integrity Check ?	Desired State	10:04 AM PST
✓	AD Accounts That Do Need a Password Reset Are Marked for One	Challenge Check ?	Desired State	10:26 AM PST

Status of Tasks – Completed yet?
****GREEN IS GOOD****

WARNING: Might take 30-60 seconds to refresh – Don't panic!

Documentation Challenge Info Meeting Notes

Please enter any tools, programs, and utilities used to complete the challenge.

Document all necessary steps and actions taken to complete the challenge in the field below. Document as if you were writing documentation for the company. This information will be sent to your challenge Curator for review.*

Rich text editor with toolbar (bold, italic, underline, etc.) and a large text area for documentation.

portal.nice-challenge.com/workspace#

NICE Challenge Webportal

Jeff Shafer
Current User

PLAYER CURATOR

Dashboard Upcoming Reservations Workspaces Submissions Helpdesk & FAQ

spring_2020_comp_178 | Jeff Shafer

Submit Challenge Attempt

Virtual Machines

Machine Name	Status	Actions	Open Console ?
Asteroids-PoS	Powered On	Action	HTML5 VMRC
Asteroids-Router	Powered On	Action	HTML5 VMRC
Centipede-PoS	Powered On	Action	HTML5 VMRC
Centipede-Router	Powered On	Action	HTML5 VMRC
Database	Powered On	Action	HTML5 VMRC
Domain-Controller	Powered On	Action	HTML5 VMRC
Fileshare	Powered On	Action	HTML5 VMRC
Firewall	Powered On	Action	HTML5 VMRC
Prod-Web	Powered On	Action	HTML5 VMRC
Security-Desk	Powered On	Action	HTML5 VMRC
Workstation-Desk	Powered On	Action	HTML5 VMRC

Checks

Status	Check Description	Check Type	Check State	Last Changed
✓	AD Accounts That Do Not Need a Password Reset Are Not Marked for One [Should Stay Green]	Integrity Check ?	Desired State	10:04 AM PST
✓	AD Accounts That Do Need a Password Reset Are Marked for One	Challenge Check ?	Desired State	10:26 AM PST

For submission: List tools used and describe how you solved the challenge

Documentation Challenge Info Meeting Notes Network Map

Please enter any tools, programs, and utilities used to complete the challenge.

Document all necessary steps and actions taken to complete the challenge in the field below. Document as if you were writing documentation for a peer. This information will be sent to your challenge Curator for review.*

Rich text editor toolbar: Bold, Italic, Underline, Strikethrough, Text color, Background color, Bulleted list, Numbered list, Indent, Outdent, Undo, Redo, Styles.

spring_2020_comp_178 | Jeff Shafer

Submit Challenge Attempt

Workspaces

Machine Name	Status	Actions	Open Console ?
Asteroids-PoS	Powered On	Action	HTML5 VMRC
Asteroids-Router	Powered On	Action	HTML5 VMRC
Centipede-PoS	Powered On	Action	HTML5 VMRC
Centipede-Router	Powered On	Action	HTML5 VMRC
Database	Powered On	Action	HTML5 VMRC
Domain-Controller	Powered On	Action	HTML5 VMRC
Fileshare	Powered On	Action	HTML5 VMRC
Firewall	Powered On	Action	HTML5 VMRC
Prod-Web	Powered On	Action	HTML5 VMRC
Security-Desk	Powered On	Action	HTML5 VMRC
Workstation-Desk	Powered On	Action	HTML5 VMRC

Status	Check Description	Check Type	Check State	Last Changed
✓	AD Accounts That Do Not Need a Password Reset Are Not Marked for One [Should Stay Green]	Integrity Check ?	Desired State	10:04 AM PST
✓	AD Accounts That Do Need a Password Reset Are Marked for One	Challenge Check ?	Desired State	10:26 AM PST

Submit for credit!

Documentation Challenge Info Meeting Notes Network Map

Please enter any tools, programs, and utilities used to complete the challenge.

Document all necessary steps and actions taken to complete the challenge in the field below. Document as if you were writing documentation for the company. This information will be sent to your challenge Curator for review.*

Rich text editor with toolbar (bold, italic, underline, etc.) and a large text area for documentation.

Lab 7

Environment: **Pretty Safe Electronics**
Challenge Title: ***Penetration Testing:
Bringing Passwords Up To Snuff***

Access via <https://range.xpcyber.com/>

XP Cyber Labs

- ****Warning about scheduling****
- Labs are “available” for 1 week and reservations are needed!
 - Virtual machines are used by other students at other universities – Can’t hold onto it
- **You reserve your own 48-hour access period within that 1-week window**
- Reservations must be made the day prior (midnight deadline)