Sierra College
Blue Team Security Report for Cyber Challenge

NAME: Colby Heilner

Team A

Date: 12/12/2024

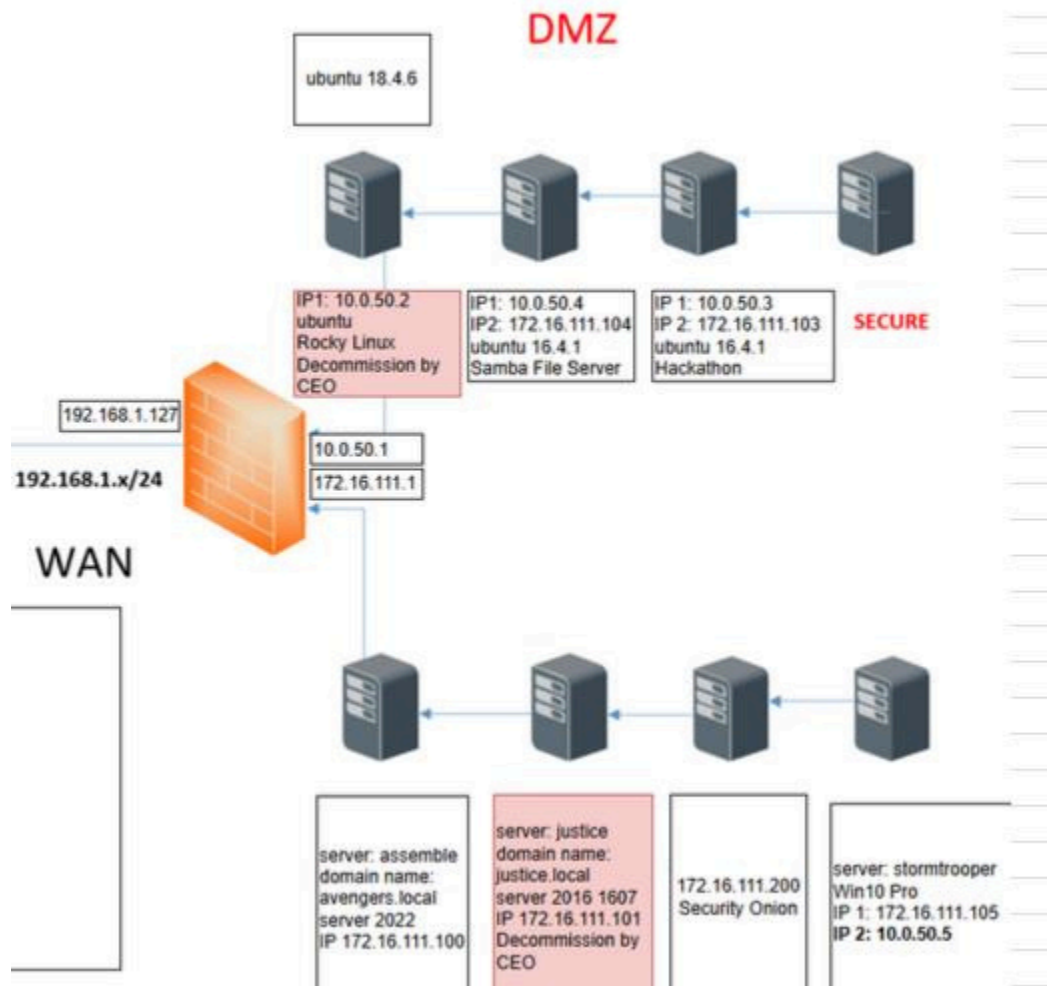# Table of Contents

1.0 Report – Intro

Our team was hired to take over for a previous lack of security management. From December 4th, 2024, to December 10th, 2024. Our primary task was to take the actions needed to secure and lock down the Sierra net Inc network and ensure their websites and business requirements remain active. We were also responsible for updating and maintaining users on all systems including system administrators.

2.0 Part 1

2.1 Discuss the Environment

Upon our initial survey of the environment, our team notices security issues. From the initial scans we had a total of 9 machines including our firewall. We were running a Pfsense firewall, 4 Linux computers along with 4 additional windows computers. The company has set up a DMZ and a LAN to separate traffic from the websites hosted on our Linux servers. These websites include Own cloud file hosting and Hackazon storefront website. They had also recently bought two other companies, Stormtroopers, and Justice. This explains why there are three domain controllers in the environment. There were also multiple systems in the environment that had multiple Nic cards installed. Lastly the firewall rules were messed up. Although Our firewall did have snort IPS installed. Which I configured and setup, which I will explain in more detail later.

See screenshot below for the full environment. (ignore decommission notes)

DMZ

ubuntu 18.4.6

IP1: 10.0.50.2
ubuntu
Rocky Linux
Decommission by
CEO

IP1: 10.0.50.4
IP2: 172.16.111.104
ubuntu 16.4.1
Samba File Server

IP 1: 10.0.50.3
IP 2: 172.16.111.103
ubuntu 16.4.1
Hackathon

SECURE

192.168.1.127

10.0.50.1

172.16.111.1

192.168.1.x/24

WAN

server: assemble
domain name:
avengers.local
server 2022
IP 172.16.111.100

server: justice
domain name:
justice.local
server 2016 1607
IP 172.16.111.101
Decommission by
CEO

172.16.111.200
Security Onion

server: stormtrooper
Win10 Pro
IP 1: 172.16.111.105
IP 2: 10.0.50.5

Multiple things were wrong with the environment, including more than one domain controller, Multiple Nic cards on DMZ machines. All passwords in the environment were default, yes all. On top of this all front-facing company websites were intentionally vulnerable web apps, such as hackazon. Our machines 10.0.50.4 10.0.50.3 had multiple ips causing severe problems in the network. Because they also had Lan ips they were able to talk directly to the LAN, which defeats the whole purpose of the DMZ. The firewall rules looked random and had no regard for security. I saw Any Any rules and NAT rules that were not business requirements.
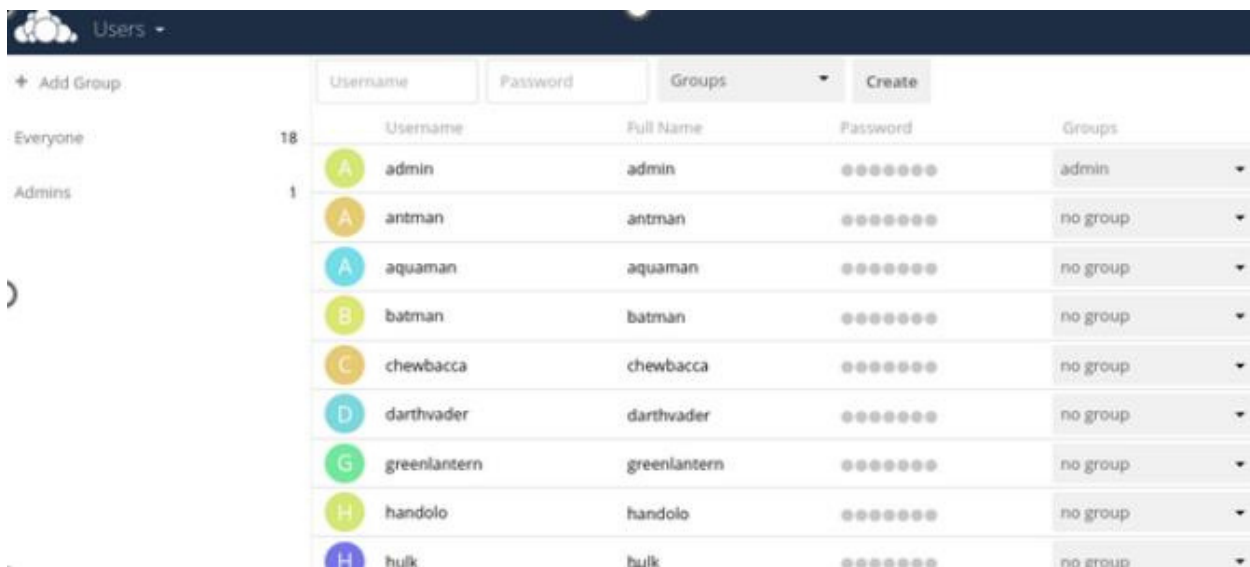
2.2 Actions on Environment

Within our team we divided out tasks evenly to maximize efficiency. For my case I was consider the Firewall Engineer. This meant I oversaw maintaining the Pfsense rules, services and other things related to it. When I first started to change to the network, I helped with changing default passwords on Owncloud **1.1** and Hackazon **1.0.** These websites had a considerable number of accounts, and they needed to be updated from default passwords.

1.0

1.1

After changing the default password, I switch to my key role for my team with firewalls. I first changed all Pfsense rules to allow for our business requirements, this included the Nat rules **1.4**. This is the most important as to not lose business money. Once we had changed default passwords, made sure I followed the business requirements and disabled any over allowing rules. We were able to take more active security measures. I started by configuring and enabling snort IDS. This allowed us to receive alerts related to suspicious packets attempting to access our network or already inside. Over the first few days of our

employment, we had already got to know some "abusive ips". **1.3** These allowed us to know when false positives were false positives.

1.3

Current known abusive IPS
10.0.99.2, 10.0.99.6, 10.0.99.7, 10.0.99.3

1.4

|		Interface	Protocol	Source Address	Source Ports	Dest. Address	Dest. Ports	NAT IP	NAT Ports	Description	Actions
☐ ✔ ⤬		CYBERWAN	TCP	*	*	CYBERWAN address	8082	10.0.50.4	80 (HTTP)		✎☐🗑
☐ ✔ ⤬		CYBERWAN	TCP	*	*	CYBERWAN address	2222	172.16.111.104	22 (SSH)		✎☐🗑
☐ ✔ ⤬		CYBERWAN	TCP	*	*	CYBERWAN address	2222	10.0.50.4	22 (SSH)		✎☐🗑
☐ ✔		CYBERWAN	TCP	*	*	CYBERWAN address	81	172.16.111.100	80 (HTTP)		✎☐🗑
☐ ✔		CYBERWAN	TCP	*	*	CYBERWAN address	82	172.16.111.100	80 (HTTP)		✎☐🗑
☐ ✔		CYBERWAN	TCP	*	*	CYBERWAN address	3390	172.16.111.101	3389 (MS RDP)		✎☐🗑
☐ ✔		CYBERWAN	TCP/UDP	*	*	CYBERWAN address	3391	172.16.111.102	3389 (MS RDP)		✎☐🗑
☐ ✔ ⤬		CYBERWAN	TCP	*	*	CYBERWAN address	8081	172.16.111.103	80 (HTTP)		✎☐🗑
☐ ✔ ⤬		CYBERWAN	TCP	*	*	CYBERWAN address	8081	10.0.50.3	80 (HTTP)		✎☐🗑
☐ ✔		CYBERWAN	TCP	*	*	CYBERWAN address	139 (NetBIOS-SSN)	172.16.111.103	139 (NetBIOS-SSN)		✎☐🗑
☐ ✔		CYBERWAN	TCP	*	*	CYBERWAN address	2223	172.16.111.103	22 (SSH)		✎☐🗑
☐ ✔ ⤬		CYBERWAN	TCP	*	*	CYBERWAN address	22222	10.0.50.2	22 (SSH)		✎☐🗑
☐ ✔ ⤬		CYBERWAN	TCP	*	*	CYBERWAN address	443 (HTTPS)	10.0.50.2	80 (HTTP)		✎☐🗑
☐ ✔ ⤬		CYBERWAN	TCP	*	*	CYBERWAN address	3389 (MS RDP)	172.16.111.100	3389 (MS RDP)		✎☐🗑
☐ ✔		CYBERWAN	TCP	*	*	CYBERWAN address	8180	10.0.50.2	80 (HTTP)		✎☐🗑
☐ ✔ ⤬		CYBERWAN	TCP	*	*	CYBERWAN address	8082	172.16.111.104	80 (HTTP)		✎☐🗑

With these rules and snort setup, I decided to take it one step further and enable IPS, which would activly block these abusive IPS and anyone not is our bluetteam whitelist. Here is a sample of a attack detected by our IPS/IDS. **1.5** Notice in the below, we see the red X indicated it was blocked for 15 minutes due to snort rules.

1.5

Date	Action	Pri	Proto	Class	Source IP	SPort	Destination IP	DPort	GID:SID	Description
Most Recent 250 Entries from Active Log										
2024-12-06 12:02:08	⚠	1	TCP	Attempted Administrator Privilege Gain	10.0.99.2 🔍⊞✕	43682	192.168.1.128 🔍⊞✕	8081	1:2030483 ⊞✕	ET EXPLOIT F5 TMUI RCE vulnerability CVE-2020-5902 Attempt M2
2024-12-06 12:02:08	⚠	1	TCP	Attempted Administrator Privilege Gain	10.0.99.2 🔍⊞✕	43682	192.168.1.128 🔍⊞✕	8081	1:2030469 ⊞✕	ET EXPLOIT F5 TMUI RCE vulnerability CVE-2020-5902 Attempt M1
2024-12-06 12:02:07	⚠	3	TCP	Unknown Traffic	10.0.99.2 🔍⊞✕	43672	192.168.1.128 🔍⊞✕	8081	119:18 ⊞✕	(http_inspect) WEBROOT DIRECTORY TRAVERSAL

2.3 Recommendations on Environment

If I had to recommend changes, they would be investing in a non-open-source firewall. Such as Palo Alto. I would recommend not having dual nic setups for computers in the DMZ as this defeats the purpose of separating them. For the websites that they need hosted, have the developers make some serious changed to the code and make them secure. They are insecure by default which causes tons of problems if they are to remain on the WAN. Lastly I would recommend having your sysadmin do a merge or purge of the two extra DCs on the network and consolidate into one.

3. Part 2

3.1 Security Tools

Discuss the security tools that you use within the environment.

I used various security tools while conducting our security practices. We used SecurityOnion an open source SIEM to manage and collect logs through deployed agents. We also used Wazuh which is a free and open source security platform that helped us see what exploits are computer were vulnerable to. It also helped with compliance by showing our compliance percentages.

3.2 Attacks Viewed

Discuss the attacks that you saw on the environment.

We mainly saw reconnaissance attacks; we can see this from our logs in Snort. As pervious screenshots have shown, they used nmap to try and scan our network for ports and services. Some things that were unique to our network were seeing a lot of web based attacks. We saw quite a bit of directory traversal and privilege escalation attempts. We saw CVE-2020-5902 pop up a lot.

3.3 Actions taken on Attacks

Discuss the actions that you took against the attacks on the environment.

Upon seeing these attacks, we realized that we needed A strong IPS, after seeing these attacks I made sure our rule book for snort would be properly updated. I also made sure that all admin accounts on websites and local user accounts were changed from default. Overall, this made us more secure the ever allowing our Snort IPS to take over and help defend our network from scans and brute force traversal.

3.4 Recommendations

What additional recommendations should the company take to ensure a secure infrastructure, safe from attacks.

Again, I would like to see Less open-source software and invest in some better services. It would be great to also see something like Splunk used for the SIEM. One thing this company could do would be to move the non-stand ports the websites are on to standard ports. The websites are running on 8081 8082 and other nonstandard ports and this makes it harder for customers to access them. Overall this network was a mess In the beginning, yet we were able to protect it and make a lot of the correct choices to secure it.