# Executive Report-
# Episode 1

Completed by:

Team Texas

Members:

Thomas Larkin

Colin Mullican

Graeme Dickerson-Southworth

Ikechukwu Igboemaka

Completed on:

03/04/2024

# Hosts & Services

*Up-*

- 24/25 hosts
- 56/89 services

*Down-*

- 1/25 hosts
- 33/89 services

# Weekly Reports

*Week 1-*

We as a team were tasked with familiarizing ourselves with our network's Steel and Mining domains inherited from the previous IT administration team, creating an asset report and user audit for our network, and creating a user account for each individual team member. We acquired knowledge of the different Organizational Units, user accounts on the domains, and services associated with each host machine. With this information, we created the asset report and user audit. We also created user accounts for each team member, assigning Administrator privileges to each user.

We were unable to complete the task of creating a webpage for file shares on the system. However, we aim to resolve this task as soon as possible.

*Week 2-*

We as a team were tasked with utilizing our Graylog server to query for specific system logs, familiarizing ourselves with our adversaries' host machines, and creating a table using the information we gathered through reconnaissance. The table contains our adversaries' networks, hostnames, IP addresses (IPv4 + IPv6), Operating Systems, and services running on each machine.

All tasks assigned this week have been completed.

*Week 3-*

We as a team were tasked with setting up a secondary DNS server and Domain Controller, building a Linux workstation, creating a password script for users, and backing up important files to be stored on and off the network. During this time, we started brainstorming and writing our first operation plan, unanimously agreeing to target Team Florida. The attack was denied at initial submission.

All tasks assigned this week have been completed.

*Week 4-*

We as a team were tasked with familiarizing ourselves with our network's newly assigned Aero domain, which consists of a Domain Controller, a Windows 11 workstation, 2 Windows servers, a Samba file server, and an Apache server. During this time, we started writing our first incident response, involving an adversary that implemented a script that exploited a vulnerability in misconfiguration of our SSH service, giving the attacker unauthorized root access to all our machines. Despite addressing and mitigating the issue, we believe the same adversary is now using initial access

acquired through the script to log into an Administrator account known as “zathras”. We are currently investigating and addressing the new threat at this present time.

Additionally, during this week, we as a team revised our operation plan to exploit a vulnerability in misconfiguration of our target’s SSH service, granting us access to a pre-determined user on the machine without password authentication.

From the tickets assigned this week, we are still working to establish the domain trust between the Aero and Steel domain, set up the machines within the Aero domain to send their system logs to Graylog, and assign proper permissions and privileges to the groups within our Apache server.

*Week 5-*

We as a team were tasked with familiarizing ourselves with our network’s newly assigned Auto domain, which consists of a Domain Controller, a Windows 10 workstation, an Apache server, and a MySQL server. Our objective for these individual hosts machines was to gain root access to each machine, which was not granted to us by the previous IT administration team. Currently, we have established root access to the Domain Controller, and are working to establish root access to the Apache and Windows 10 workstation.

Firstly, root access to the Domain Controller was established through default credentials on an administrator account, which upon gaining access to, was changed to include stronger credentials. Secondly, root access to the Apache server will be established through misconfigured read permissions to crontab, which allows non-root users to see what scripts are currently running. Upon opening and reading the file, we discovered that non-root users have read and write permissions to one of the scripts, which we used to obtain read and write access to /etc/passwd and /etc/shadow. We plan to use the acquired files to access the administrator account, and to patch the vulnerability. Thirdly, root access to the Windows 10 workstation will be established through misconfigured privileges that allow non-root users to read the registry keys. Upon viewing the registry, we discovered that the AlwaysInstallElevated value is set to 1, a misconfiguration that prompted us to create an msi file to run to gain root access to the machine. Lastly, the MySQL server was discovered to have default credentials assigned to several user accounts, allowing initial access to the machine. We are investigating further and working toward gaining root access to the machine at this present time.

## Discovered Incidents

At this present time, we as a team have noticed adversary activity within our network, through recorded events on our Graylog server. We have observed beacons, root SSH logins, and administrator account SSH logins. While we have patched the root SSH login vulnerability, we are working on gathering information regarding the beacons, as well as fixing the administrator account SSH login vulnerability.

## Offense Report

At this present time, we as a team have gained access to an adversary machine, escalated to root access, and exfiltrated sensitive documents such as browser history, passwords, asset reports, and user audits. We are working to create several means of persistence to the machine, such as startup scripts and copying login access to other user accounts, as well as obtain access to their Windows shared drive in a future operation, exfiltrating flags in the process.

# Conclusion

Overall, we have familiarized ourselves with all domains and machines assigned to us at this time. We have developed detection of compromise by our adversaries, through constant surveillance and auditing of unauthorized system access, and have gained access to one of our adversary's machines. Before the conclusion of this episode, we plan to complete tasks assigned on week 1, week 4, and week 5. Additionally, we plan to patch the discovered vulnerabilities within our network, that our adversaries have exploited to gain administrator and root access on our systems.