Executive Report
Episode 2

Completed by:

Team Texas

Members:

Thomas Larkin

Colin Mullican

Graeme Dickerson-Southworth

Ikechukwu Igboemaka

Completed on:

4/14/2024

Objective

The objective of this report is to document our progress made as a team during episode 2, including an overview of statistics (hosts, services, tickets, flags), discovered incidents, offensive operations, and weekly progress reports.

Overview

As of 4/14/2024, the following statistics have been documented for episode 2:

Hosts

Hosts up: 35/35

Services

Services up: 146/160

Services down:

- abilene.textile.texas.tu (IIS)
  - NTLM
- allen.power.texas.tu (BIND)
  - DNS (IPv4)
- houston.mining.texas.tu (BIND)
  - Software Version Check
- leaguecity.power.texas.tu (MySQL)
  - Software Version Check
- mckinney.aero.texas.tu (File Server)
  - WinRM
- midland.chem.texas.tu (Apache)
  - Basic Authentication
  - SSH
  - Software Version Check
- pasadena.auto.texas.tu (Apache)
  - Basic Authentication
- roundrock.textile.texas.tu (Windows Workstation)
  - Software Version Check
  - psexec
- waco.chem.texas.tu (Apache)
  - SSH

    - Software Version Check

Service Warnings:

- mesquite.auto.texas.tu (Windows Workstation)
    - psexec

Tickets

Assigned: 57/60

Unassigned: 3/60

Resolved: 42/60

On Hold: 2/60

In Progress: 7/60

Replied: 4/60

Waiting Reply: 4/60

New: 1/60

Overdue:

- File Share Drive Mapping

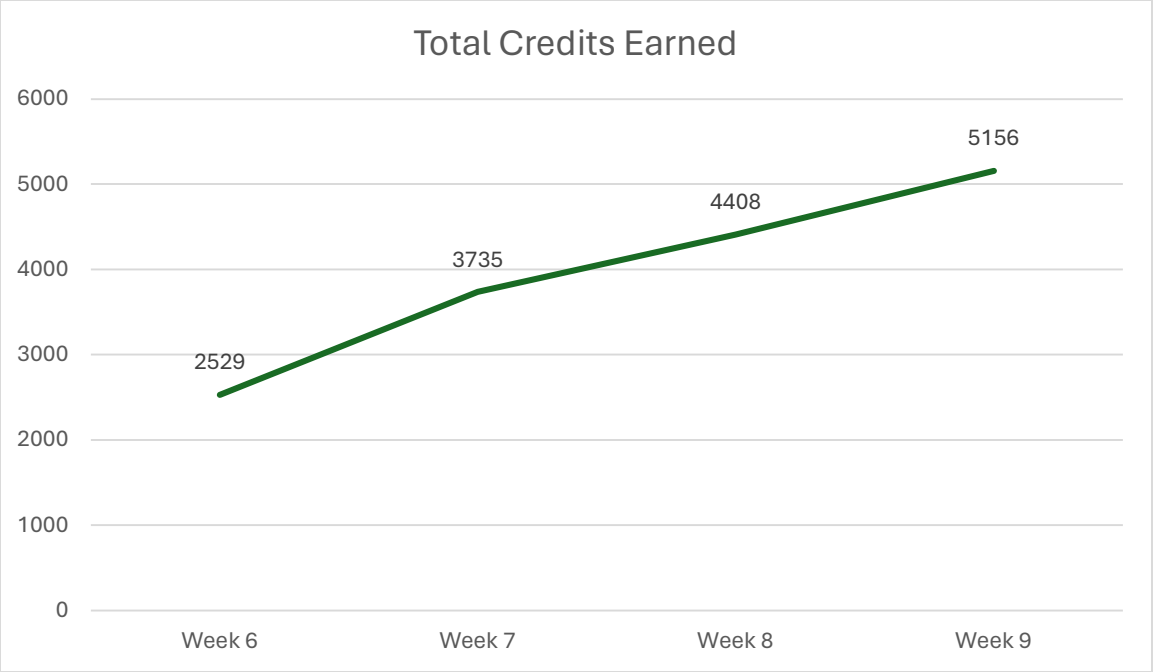
Flags

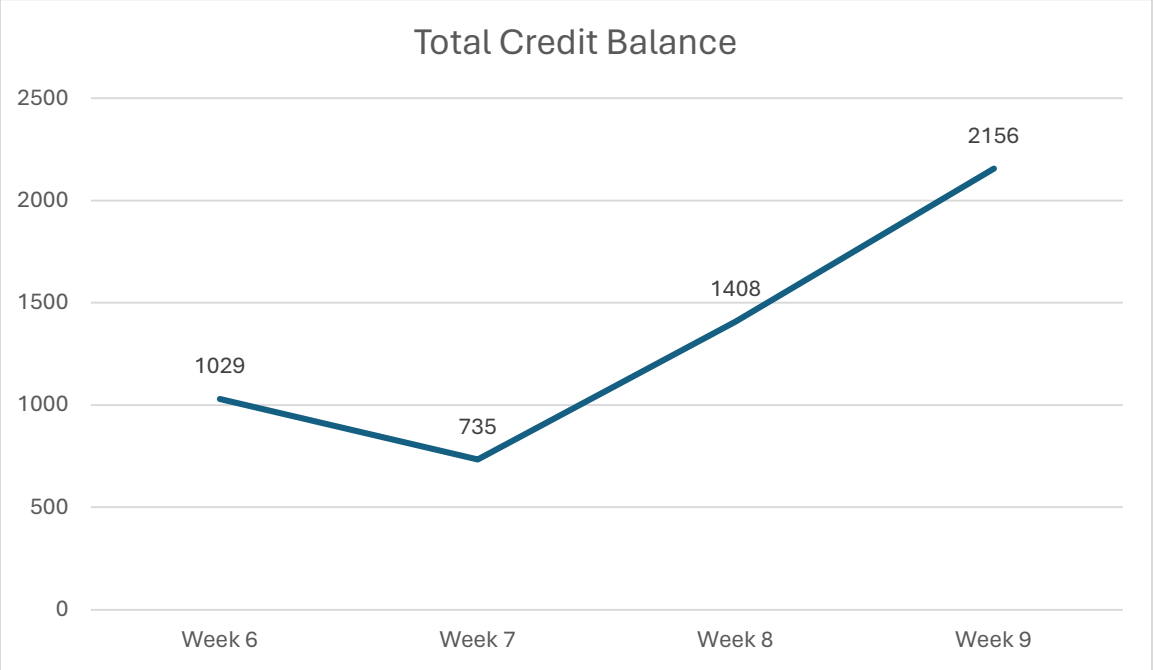
Flags purchased:

- Flag1
- Flag2
- Flag3
- Flag4
- Flag5
- Flag6
- Flag7
- Flag8

Graphs

(Note: Week 10 is ongoing, and has therefore been omitted from the graphs)


Total Credits Earned
6000
5000
4000
3000
2000
1000
0
2529
3735
4408
5156
Week 6
Week 7
Week 8
Week 9


Total Credit Balance
2500
2000
1500
1000
500
0
1029
735
1408
2156
Week 6
Week 7
Week 8
Week 9

Discovered Incidents

As of 4/14/2024, there have been **7** documented incidents during episode 2.

1. BIND Rebuild

Affected host: Houston

At the end of episode 1, our BIND server on Houston went down, because of a corruption within a partition of our hard drive. After accidentally overwriting said partition of data, we resorted to rebuilding the machine from scratch. This incident has been resolved, and our BIND server is back to being fully operational.

2. Keylogger

Affected hosts: ElPaso, Lubbock, CorpusChristi

On March 24th, one of our team members detected a keylogger within the ElPaso (labelled SearchUL.exe), Lubbock, and CorpusChristi systems (labelled StartUL.exe), through inspection of autoruns.exe. The keylogger is set to run and maintain persistence through a registry key associated with startup applications. The keylogger's output is sent to a malicious text document, and in one instance, logged exercise credentials (this was noted and changed immediately).

3. *Keylogger #2*

Affected host: ElPaso

On April 5th, the keylogger appeared back on ElPaso with a modified registry key for persistence. Additionally, a malicious program labeled “msdaps.exe” was detected, and is being reverse engineered and analyzed at this given time.

4. *Reverse shells*

Affected host: ElPaso

On April 5th, several suspicious executables were analyzed from ElPaso, with each calling a reverse shell to attackers through associated services. We are working at this given time to mitigate persistence of these executables, through removal of services upon detection.

5. *svchost.exe*

Affected host: Lubbock

On April 6th, a process labelled “svchost.exe” was detected communicating over UDP with a system from Illinois (schaumberg.steel.illinois.tu). These connections were terminated, with increased surveillance on svchost.exe processes, as the process is a common target for malware, running multiple instances at once.

6. *Minecraft Server*

Affected host: SanAntonio

On April 6th, we became aware of a process associated with a Minecraft server within SanAntonio, running through a “server.jar” file. While mostly harmless, the process and its associated program were immediately removed from the system.

7. *Illinois Ransomware*

Affected domains: Mining, Auto

On April 11th, we received an email from Illinois, demanding 1000 credits to not release details on OP plans against Florida. They also demanded an additional 1500 credits to not release prefixes and passwords of several domains. After refusing to meet said demands, on April 12th, our prefixes and passwords for mining and auto domains were posted on exercise control, and while it wasn’t posted, we suspect Illinois individually sent our OP plans to Team Florida.

Offensive Report

As of 4/14/2024, there has been **1** operation plan created and executed during episode 2.

1. Operation Lateral

Targeted teams: California, Illinois, Florida

Date of Execution: 3/31/2024

Initial Access

Out of the targeted systems, **21 out of 28** systems were infected with our target vulnerability, allowing us to successfully exfiltrate sensitive data from the systems. Below is a table of all targeted systems, indicating whether initial access was successful or not:

California

IP	Success
172.17.71.56	Yes
172.17.71.59	Yes
172.17.71.93	Yes
172.17.71.114	Yes
172.17.71.145	Yes
172.17.159.7	Yes
172.17.159.197	Yes

Illinois

IP	Success
172.21.11.139	No
172.21.43.153	No
172.21.155.95	Yes
172.21.155.134	Yes

172.21.190.38	No
172.21.190.51	Yes
172.21.190.52	Yes
172.21.190.144	Yes
172.21.190.146	Yes
172.21.190.206	No

Florida

IP	Success
172.19.101.29	Yes
172.19.114.4	No
172.19.114.13	No
172.19.114.138	No
172.19.203.34	Yes
172.19.203.122	No
172.19.229.17	Yes
172.19.229.79	Yes
172.19.229.162	Yes
172.19.229.229	Yes
172.19.229.248	Yes

While many teams had patched the webclient account on each system, many had not patched the cron account, making it our primary target for logging into the systems. Upon logging in, we were given a shell to interact with the system.

Privilege Escalation

To escalate to sudo privileges, we abused misconfigured privileges on the cron account, allowing edit privileges on any file. By editing the sudoers files to put cron in the same group as root, we were granted sudo privileges.

Exfiltration

Upon escalating to sudo, we accessed each team's Samba servers, containing sensitive data such as operation plans, incident reponses, after-action reports, episodic reports, and reconnaissance. We successfully exfiltrated this content from each team's shared drive, and by searching for files labelled with keywords such as "password", "nagios", and "exercise", we exfiltrated data from California containing all usernames and passwords for all users in plain text.

Persistence

Persistence was maintained on each system through randomly selected administrative users. By inserting our public key into the users' authorized_keys files, we are able to log into the systems at any time through passwordless SSH, as long as the keys are not deleted from the file. Additionally, public keys were inserted into root, along with a bash script called in .bashrc, replacing the public keys upon login.

Evasion

After the attack on each system, log files were deleted from the system. Additionally, when running a command as sudo from the root user, a command will not appear in a system's log. While data will be reported and sent to Graylog, the intent of the operation is to overwhelm and compromise as many systems as possible, requiring the victim teams to remove traces of the attack from multiple systems.

Outcome

Overall, we believe the operation to have been a major success, relying on a persistence mechanism left by other adversaries. Out of all exfiltrated data, we believe California's plain text username and password list, Florida's keylogger-based operation plan against California (which we can utilize by using Florida's keylogger for ourselves, saving us time and resources), and California's reconnaissance report, containing updated assets we added to our own reconnaissance.

Weekly Reports

The following are reports for each week of episode 2, which took place from 03/04 – 04/14[*]:

[*]- The week of 3/18 – 3/25 is omitted, due to an exercise-wide break (Spring Break)

Week 6 (March 4th – March 10th)

In week 6, we as a team were tasked with configuring hosts on the Auto domain, which were purchased and granted access in the previous week. The following is a list of each ticket assigned this week:

- Join all 4 systems to Auto domain
- Establish two-way trusts between the Auto domain and other existing corporate domains
- Configure data from each system to be sent to the preexisting log server
- Reset all domain user passwords
- Install nagios public key for each user
- Configure drive mappings on each Windows system

Of these tasks, we successfully joined all systems to the Auto domain, and set up logging & drive mappings for each system. Of the remaining 3 tasks, domain passwords and nagios public keys were addressed at a later date. The task of establishing trusts between domains has been put on hold and will be addressed as other tasks are completed. Additionally, we obtained full access to McAllen's MySQL system, using cracked passwords to privilege escalate to a sudo user, a task assigned from the previous week. Once in, we changed passwords for personal accounts, removed malicious code from each user's .bashrc file, and deleted SSH keys for each user, potentially left by a previous IT team.

Week 7 (March 11th – March 17th)

In week 7, we as a team were tasked with configuring Apache servers for preexisting systems, creating systems for a newly created chemistry division, and creating a Certificate Authority on a new or existing system. The following is a list of each ticket assigned this week:

- Run Apache server on Aero domain
- Run Apache server on Auto domain
- Create BIND system for Chem domain
- Create 2 Apache servers for Chem domain
- Create Certificate Authority

Of these tasks, we successfully created the Certificate Authority, as well as all 4 Apache servers at a later date. We are working at this given time to establish the BIND server for the Chem domain- the system has been built and configured, and groups need to be created, with each user being added to their respective groups.

Week 8 (March 25th – March 31st)

In week 8, we as a team were tasked with developing a network for the textile division. The following is a list of each ticket assigned this week:

- Create Domain Controller for Textile domain
- Create 2 IIS web servers for Textile domain
- Create administrative workstation for Textile domain
- Run IIS web server on Aero domain

Of these tasks, we successfully created all 3 IIS systems, as well as the administrative workstation at a later date. We are working at this given time to establish the Domain Controller for the Textile domain- the system has been built and configured, as well as users being added and awaiting OU assignments. Additionally, our offensive operation, Operation Lateral, was executed this week.

Weeks 9 & 10 (April 1st – April 14th)

In weeks 9 & 10, we as a team were tasked with developing a network for the power division. The primary task was creating a firewall for the domain, with 2 different interfaces used for different sets of systems. The green interface is used for internal traffic, while the orange interface is used for external traffic within the Demilitarized Zone of a network. The following is a list of each ticket assigned these weeks, with their corresponding interface included:

- Create firewall for Power domain
- Create Domain Controller for Power domain (GREEN)
- Create workstation for Power domain (GREEN)
- Create DNS server for Power domain (ORANGE)
- Create Apache server for Power domain (ORANGE)
- Create MySQL server for Power domain (GREEN)

To delegate these tasks and ensure we as a team could maintain efficiency, one member undertook all these tasks, while the remaining members cleaned up systems, in preparation for the new episode. Of these tasks, the firewall was created, as well as the Domain Controller and workstation. The rules for the green interface have been enabled, and the remaining systems are being worked on at this time, with the MySQL server being built, requiring users to be ported over.