

Executive Report

Episode 3

Organization:

Team Texas

Members:

Thomas Larkin

Colin Mullican

Graeme Dickerson-Southworth

Ikechukwu Igboemaka

Completed on:

5/20/2024

Table Of Contents

Overview:.....	3
System Health:	3
Financials:	5
Incident Responses:	7
Bank Credential Theft:	7
PAExec:	8
Offensive Operation:	9
Risk Analysis Report	10
1. Overview:.....	10
2. Information Systems Focus:.....	10
2. Preparation and Scoring:	11
3. Scope:.....	13
4. Threat Source Assessment:.....	21
5. Vulnerabilities:.....	24
6. Threat Assessment	27

Overview:

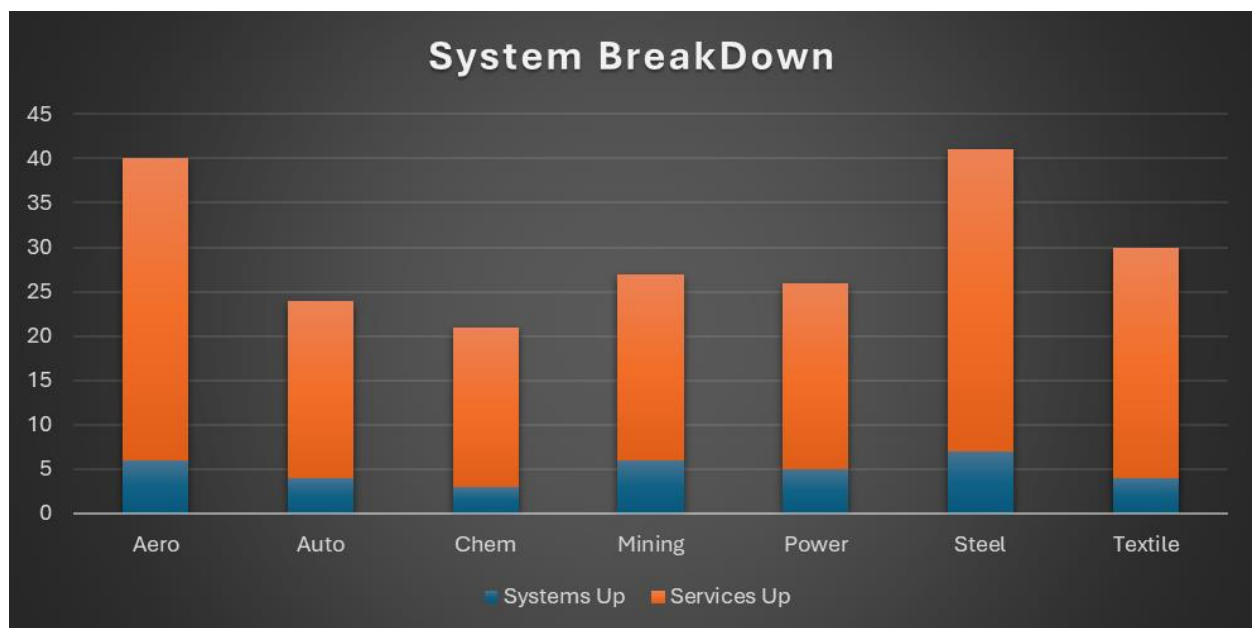
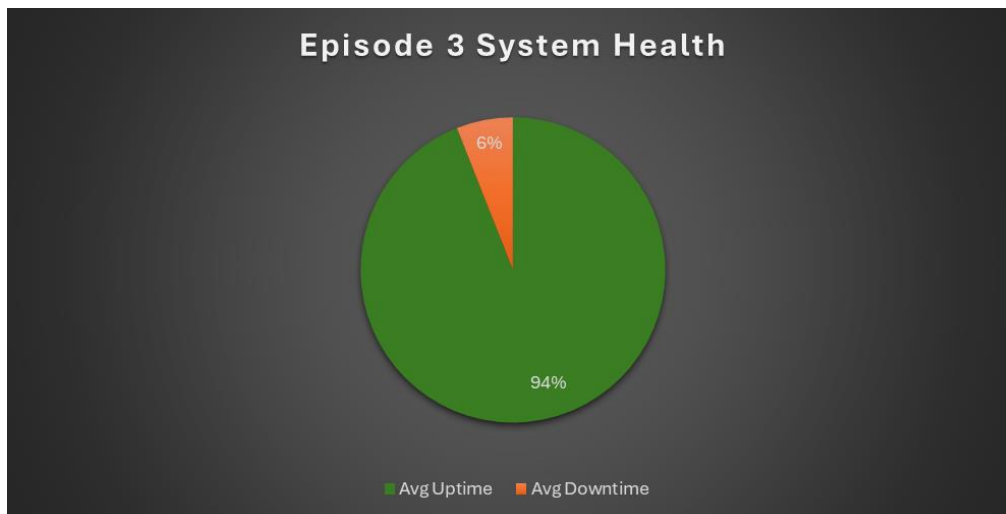
This report provides a comprehensive analysis of the current state of our organization, including the state of our organization's network and financial health. The report will start with an assessment of the overall health of our systems, highlighting uptime, along with any significant issues encountered. Then, the report will discuss details of the organization's financial balance, including a breakdown of company profit, expenses, and purchases of company flags.

Next, this report will cover all security reports and concerns received by the IT team, reviewing recent threats believed to have posed significant concern for the company. Then, the report will address offensive operations aimed at other organizations to exfiltrate valuable data that benefits the company. Finally, a NIST assessment will be presented at the end of this report, which will accomplish the following:

- Evaluate the current implementation and potential threats of our organization's information systems
- Identify potential risks within all aspects of the organization
- Raise the awareness of our team in the event of potential threats
- Serve as a guideline for documenting risk assessments in the future of the organization

System Health:

As of 05/19/2024, all systems and services within the organization's network are running and operational. The charts below show a high-level overview of our network's health and a breakdown of all networks/services being monitored for each domain over the course of the episode 3:

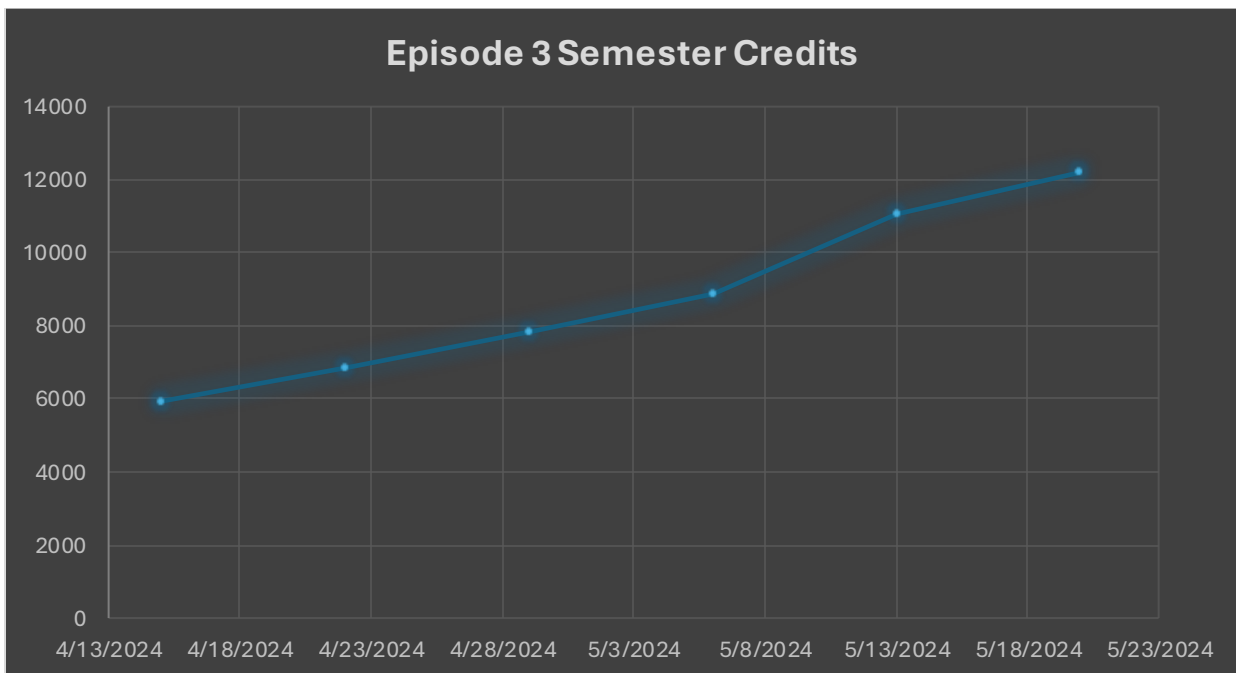
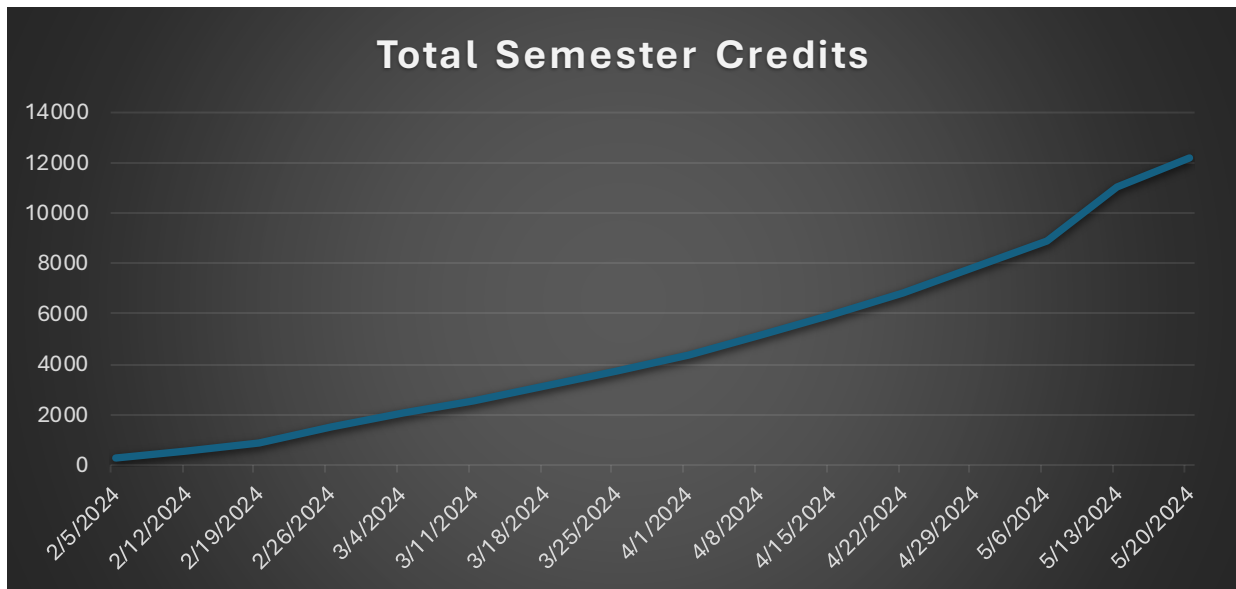


According to the above figures, our organization had an average of 6% downtime throughout the episode*. This downtime can be attributed to the introduction and configuration of the network's IPFire firewall & Power domain, as well as PAExec login issues. Correctly configuring the firewall to allow proper communication within the domain proved difficult, taking our team 2 weeks to complete. PAExec, which will be discussed further in incident responses, is a monitored service that allows users to run commands remotely. However, many users reported issues with the service timing out, requiring extensive time management amongst the IT team, alongside firewall & Wordpress/Joomla web service configuration for employees.

*- analyzed using weekly status reports throughout the episode

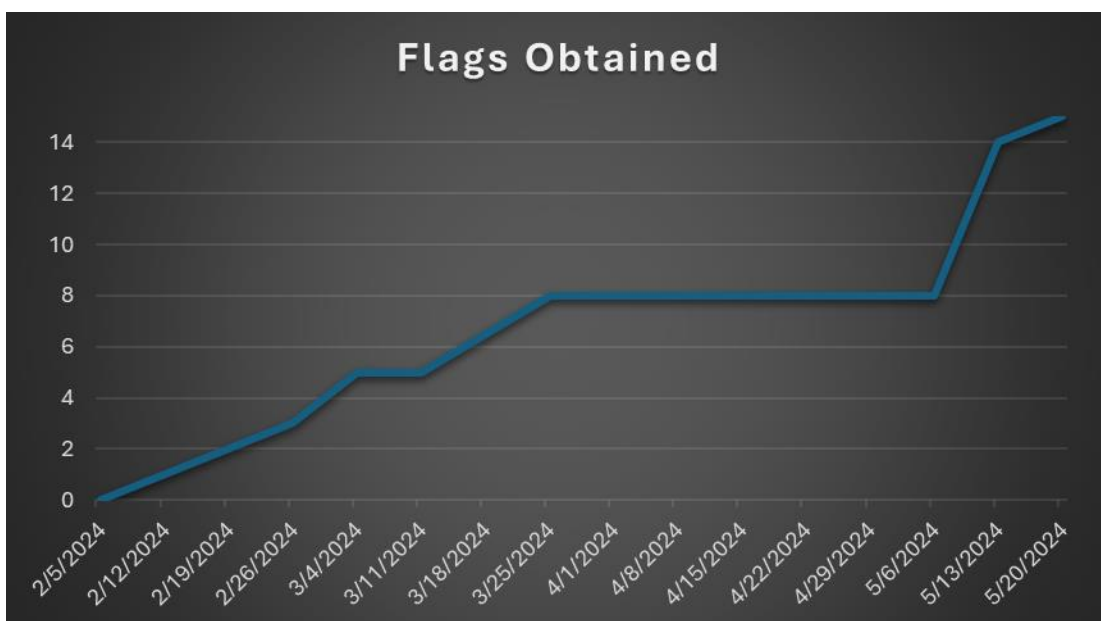
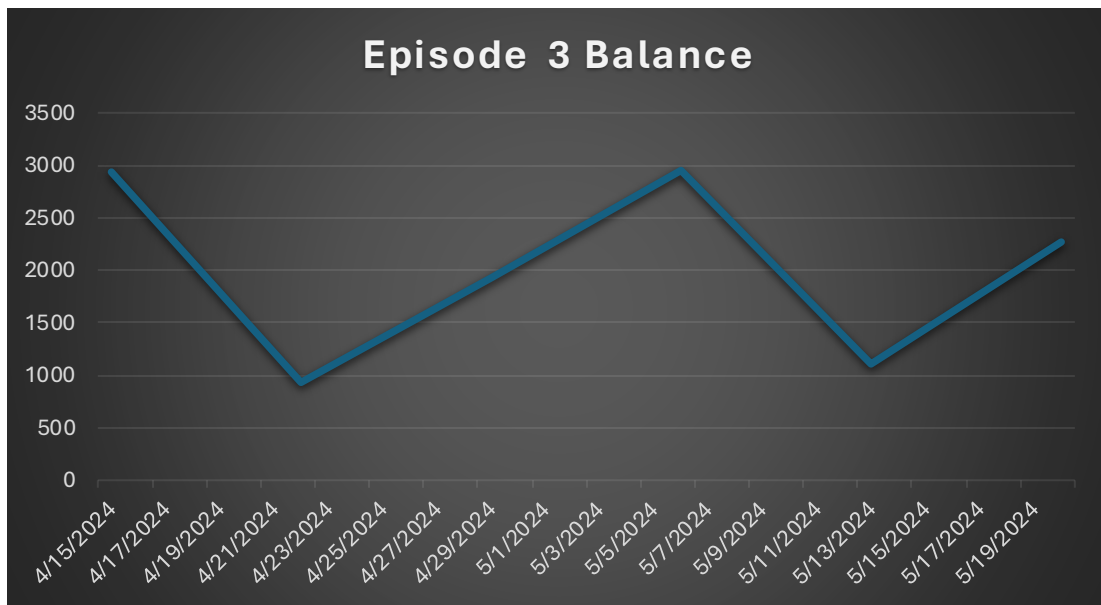
Financials:

As of 5/17/2024, the company's balance stands at 1760 current credits, with 5105 semester credits earned during episode three. This brings the company's overall semester credits to 11039 total credits with a 46% increase in total profit compared to episodes 1 and 2 combined. The graphs below show a breakdown of the total credits earned throughout the semester and a breakdown of total credits earned for episode 3*:



* - analyzed using weekly status reports received throughout the episode

After the attack on our bank on April 15th, the IT team focused diligently on recovering the 2934 credits lost. While our team was unsuccessful in recovering the stolen credits, the team was able to make up for the loss by stealing flags 9-12 from team Illinois on May 8th, valuing up to 3,200 credits (See offense operations for more details). Our IT team then used the credits built up between the incident and launch of the attack to purchase flags 13 and 14 (purchased same day as the attack), before finally purchasing flag 15 on May 13th and believed to be the first team to have successfully purchase all flags. The graphs below depict the credit balance/expenditure over the course of episode 3 along with a timeline of flags obtained:

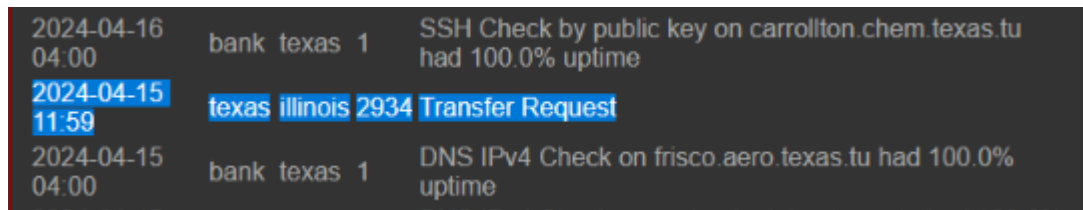


Incident Responses:

After the events of the Ransomware from team Illinois, exposing our attack and persistence on team Florida, our IT team was on high alert for retaliation attacks. While the team did not uncover attacks from rival organizations, below is a summary of all incident responses recorded by the team during the episode:

Bank Credential Theft:

On April 15th, we received word from the CEO that all funds within our bank account had been transferred. Reviewing the bank logs, it was discovered that the credits had been transferred to team Illinois. We discussed with Illinois and other teams (teams New York, Florida, and California) and discovered the threat actor used team Illinois bank account to funnel funds from all teams into their account, before transferring the funds to red team.



















After investigating our systems, it was discovered that the certificates we had been using to authenticate with the classex domain had been falsified, with the issuer being “red team” and had been redirecting all users to a fake bank website, where they would steal the credentials typed in. It is unknown how long the red team had had access to our credentials but were likely waited until the credit’s within all banks had grown before striking.

In response to this attack, the IT team immediately requested to have the credentials changed and put together a new policy for accessing any website that required the use of the organizations exercise credentials. Starting from April 15th, all classex services will only be accessed by our two newly created systems, a windows 11 machine labeled “Paris” and an Ubuntu 22.04 machine labeled “orange”. These machines remain shut down when now in use, and all IT team members must be notified when a user accesses either of the machines. For regular use (checking credits, monitoring Nagios, or sending/receiving emails), IT employees will use Paris. This machine has all remote access policies disabled, uses a dynamic IP address, with a Firefox browser with the correct signed certificate for classex. The machine also has network connectivity disabled by default and is required for all IT members to disable when not in use while the system is online. When a member has finished using the system, they will disable the network, and shut the system

down. Our Ubuntu machine should only be used when files need to be transferred into or out of the system, following the same policies as our windows machine but allowing remote privileges. After the implementation of our new policy, we have had no issues or reports of our credentials being compromised. We hope by restricting the uptime of the system, and following a strict policy, we can minimize the amount of time our credentials are exposed to the network.

PAExec:

On April 8th, it was discovered that our mesquite machine had crashed with a windows error screen after too much ram was being used on the system. Restarting the system was found to have freed 2 Gigabytes of storage, however certain processes were starting to fail such as task manager receiving bad data and later crashing the windows service manager. On April 10th, the IT team managed to fix the services within the system, and was discovered to be caused when the number of services installed exceeds the limit of the number of services the system can control at a single time. This led to the discovery of small executables labeled by “nagios” to have been flooding the system seen in the photo below:

 PAExec-2951852-nagios.classex.tu.exe	4/13/2024 2:42 PM	Application	0 KB
 PAExec-2955205-nagios.classex.tu.exe	4/13/2024 2:44 PM	Application	0 KB
 PAExec-2958549-nagios.classex.tu.exe	4/13/2024 2:46 PM	Application	0 KB
 PAExec-2961967-nagios.classex.tu.exe	4/13/2024 2:48 PM	Application	0 KB
 PAExec-2965303-nagios.classex.tu.exe	4/13/2024 2:50 PM	Application	0 KB
 PAExec-2968640-nagios.classex.tu.exe	4/13/2024 2:52 PM	Application	0 KB
 PAExec-2971990-nagios.classex.tu.exe	4/13/2024 2:54 PM	Application	0 KB
 PAExec-2975385-nagios.classex.tu.exe	4/13/2024 2:56 PM	Application	0 KB
 PAExec-2978740-nagios.classex.tu.exe	4/13/2024 2:58 PM	Application	0 KB
 PAExec-2982068-nagios.classex.tu.exe	4/13/2024 3:00 PM	Application	0 KB
 PAExec-2985431-nagios.classex.tu.exe	4/13/2024 3:02 PM	Application	0 KB
 PAExec-2988772-nagios.classex.tu.exe	4/13/2024 3:04 PM	Application	0 KB
 PAExec-2992148-nagios.classex.tu.exe	4/13/2024 3:06 PM	Application	0 KB
 PAExec-2995479-nagios.classex.tu.exe	4/13/2024 3:08 PM	Application	0 KB
 PAExec-2998906-nagios.classex.tu.exe	4/13/2024 3:10 PM	Application	0 KB
 PAExec-3002314-nagios.classex.tu.exe	4/13/2024 3:12 PM	Application	0 KB

The incident would occur when employees successfully logged into the system, and their PA Exec scripts are successfully copied to the machine. The machine would then begin to execute the script (with the execution of the contents of the script being different depending on the user), but fail to clean up after successfully running, causing the service to continue running on the system, even after the user logs off, causing persistence on the system. We believe this to be a misconfiguration either unintentionally or deliberately

placed by the previously disgruntled employees after obtaining the system from the previously purchased Auto Domain.

In response, the IT team put together a powershell script to handle deleting unnecessary PAExec services on a 15 minutes timer. This was done by using windows Task Scheduler, a built in tool that allows users to automate the execution of tasks at specified times or in response to certain events on windows machines. A full breakdown of the command (and more in depth analysis of the attack) can be found within our incident response labeled “TEAM TEXAS PAEXEC INCIDENT RESPONSE”.

Offensive Operation:

On May 8th, our offensive operations team launched an offensive attack on team Illinois to exfiltrate flags from their Steel domain file share. The table below is a list of the targeted systems.

Hostname	IPv4	Operating System
peoria.steel.illinois.tu	172.21.140.118	Windows Server 2019
waukegan.steel.illinois.tu	172.21.140.240	Windows 2019
elgin.steel.illinois.tu	172.21.140.58	Windows Server 2019
schaumburg.steel.illinois.tu	172.21.140.17	Windows Server 2019
springfield.steel.illinois.tu	172.21.140.238	Linux
cicero.steel.illinois.tu	172.21.140.32	Windows 11 10 2022
champaign.steel.illinois.tu	172.21.140.252	Windows

This attack was performed using privately sent administrative credentials from our allies at team New York after the effects of their ransomware attack, including plain text passwords, associated with their steel domain. The connection was established using SSH and SFTP; SSH to mount the shared domain drive and move the flags to an accessible folder, and SFTP to transfer the files over.

The attack proved successful, and we were able to obtain flags 9-12 purchased within their system, totaling 3,200 credits in liquid assets. Using our remaining credits, we

were successful in obtaining flags 13-15, allowing us to (allegedly) become the first team to obtain all 15 flags.

Risk Analysis Report

1. Overview:

This document serves as a comprehensive analysis of risks within our organization. Today, many organizations face unexpected risks that can significantly impact or hinder the companies' operations and their ability to achieve their overarching mission. As our company has grown over the past few months, so has our interest in mission critical information. Within these past four months, our IT team has discovered attacks from notorious hacking groups like Kaiju, who have attacked and shutdown mission critical systems and stolen sensitive credentials and credits from our group. We have also discovered and been subject to similar AI State companies who have launched attacks to steal Flags, credits, and sensitive undisclosed information in the form of user credentials, plans of operation, and incident response reports. To mitigate the events of these attacks occurring in the future, this document serves to analyze potential threats (a threat being any action taken to cause harm, or put our company employees or systems in danger, in this case focusing on cyber-attacks and data breaches) discovered by the IT team throughout the semester and be used as an outline for creating and analyzing future risk assessments within the organization.

This document will be following the structure of the National Institute of Standards and Technology (NIST) framework for risk management. This framework provides a systematic approach for identifying, assessing, and mitigating risks across all domains within our network. By using this framework, we hope to identify any potential vulnerabilities, measure the impact these vulnerabilities may have, and better prepare for any unseen challenges that may arise.

2. Information Systems Focus:

Risk analysis reports tend to focus on specific aspects of an organization's operations, with each serving a specific purpose in identifying, assessing, and mitigating risks. This report will focus on the information systems within our network. An information

system encompasses any hardware/software that works alongside collecting, processing, and storing information regarding our companies' users and organizational activities. As a company striving to be at the forefront of AI technology, this makes our information systems a high priority target for attacks, potentially leading to the theft of sensitive data (i.e. employee credentials, undisclosed documents, plans of operation, etc.) which can lead to system shutdowns, ransomware attacks, and other dangerous acts.

2. Preparation and Scoring:

This focus will be following the NIST SP 800-30 publication as a guideline for conducting these risk assessments. This document will break down each risk into the following several steps:

- **Step 1: Scope and Threat source:** This step will outline the information system in question along with the potential threat sources which can adversely impact organizational operations via unauthorized access, disclosure, modification of the system/service, and/or denial of the system/service. A threat source is any individual or origin that could cause a threat to our information systems which causes harm to the organization's assets/operations. Each system will be summarized and ranked within the labeled "Scope" section of this document.
- **Step 2: Determine vulnerabilities:** This step will outline potential vulnerabilities involving the information system that can be exploited by the threat actor/source. It is important to note that these vulnerabilities can come from sources both inside and outside the system, including misconfigurations and policy vacuums. These vulnerabilities will all be listed under this step along with a description of how the vulnerability could occur/be abused.
- **Step 3: Risk Assessment:** This section will conduct an assessment on potential risks associated with our information systems given the vulnerabilities and threat sources concluded from Steps 1 and 2. Each risk will be organized from most to least important, using the formula evaluated in step 3c.

- **Step 3a:** Likelihood of Occurrence: This step will focus on the chances that a given threat can exploit each vulnerability described in step 2a. Variables such as historical evidence, the intent/capabilities of an adversary abusing the vulnerability, and the likelihood the threat results in an adverse impact will all be taken into consideration when formulating this answer.
- **Step 3b:** Impact of threat event: This step focuses on the magnitude of harm expected to result when a threat is capable of exploiting a given vulnerability. This can range from access/modification/destruction of unauthorized information, the shutdown of mission critical systems, and any harm that can be directly attributed to employees, stakeholders, and alliances.
- **Step 3c:** Uncertainty Estimate: Each evaluated risk/vulnerability comes with inherent uncertainties, including limitations of past occurrences, incomplete knowledge of the threat, undiscovered vulnerabilities, or unrecognized dependencies that can lead to adverse impacts. This section will measure each risk of uncertainty to determine how it contributes to its overall threat.
- **Step 3d:** Mitigation: This section measures how each risk described can be mitigated. While some risks pose dangerous impacts, the potential for mitigation can make up for their severity, however some risks may not have proper mitigation strategies, causing the threat to be a higher concern to the organization.
- **Step 3e:** Risk of threat event: This step will focus on evaluating a function that considers the scores given to each section discussed in step 3, to statistically determine the risk each threat event causes on our information systems. The formula for this function is the following, rounding up the solution:

$$\frac{Occurance + Impact + Uncertainty + Mitigation}{4}$$

Each section in step 3 will be scored a number depicted from the following table:

Label	Score
High	8-10
Medium	5-7
Low	1-4

High – A high rated score means that a threat should bring immediate concern to the organization and should be treated with the highest of concern. For example, a high rating for impact would mean that the listed threat has the potential to destroy mission critical progress for the organization, preventing most or the entire organization from performing any necessary tasks.

Medium – A medium rated score means that the section does not bring cause for immediate concern but should still be kept aware of. For example, a medium rating for impact would mean that the listed threat has the potential to halt progress for a specific individual group, with the outcome of the impact having the potential to become a high-risk threat.

Low – A low rated score means that the section provides only a small concern for the organization. While the section still raises concern, it should not be prioritized over other risks present within this assessment. For example, a low rating for impact would mean that the listed threat does not halt any immediate progress for the organization, with potential workaround being present to allow employees to continue working.

3. Scope:

Our IT division has put together a list of all Information systems within our organization that we believe warrant the following risk assessment. For determining the scope of this assessment, we concluded that all systems that were found to be hosting/sharing any information that our company employees can directly interact with fell within the scope of this assessment. While this includes information systems hosted within our own network, we also believe this to extend to information systems outside our immediate network that provides services involving mission critical/sensitive information (e.g. Classex services, including bank services and Nagios service maintenance). A table of the information systems can be found below:

Information System	System Hardware(s)	Hostname(s)	Domain(s)	Threat
--------------------	-----------------------	-------------	-----------	--------

HESK Ticketing Service	Windows Server 19-2004	CorpusChristi	Steel	Medium
Classex WebServices	External	Classex	Classex	High
Graylog Logging Server	Linux Ubuntu 22.04	Sanantonio	Mining	Medium
Samba File Share	Linux Ubuntu 20.04 CentOS 8.4	Amarillo Dallas	Aero Mining	High
Windows File share	Windows 2019-20H2 Windows 2019-1903	Mckinney Plano	Aero Steel	High
Certificate Webserver	Linux Rocky 9.0	Brownsville	Aero	Medium
Protected Webservers	Linux Rocky 9.0 Linux OpenSuSE 15.2 Linux Ubuntu 21.04 Linux OpenSuSE 15.0 Linux Rocky 8.6 Windows 2019-20H2 Windows 2019-1909 Windows 2019-1903	Brownsville Pasadena Waco Midland Richardson Abilene Grandprairie Pearland	Aero Auto Chem Chem Power Textile Aero Textile	Medium
Unprotected Webservers	Linux Rocky 9.0 Linux OpenSuSE 15.2 Windows 2019-20H2 Windows 2019-1903	Brownsville Pasadena Pearland	Aero Auto Textile	Low

It is important to note that while many of these sections may overlap (e.g. WordPress and Joomla, PHP sites are hosted within our IIS and Apache web services), we believe that these systems provide security risks that warrant discussion within their own category. However, multiple systems that fall under the same category (e.g. multiple Apache servers on the same system) will be discussed and assessed together to prevent redundancy. The following section breaks down each system in order, ranking from highest to lowest importance:

3.1 Classex Web Services

Classex Web Services is an external information system that hosts the following services:

User Directory: Provides a list of reference for users within the Texas network, including names, Job Title, and location within the organization.

Nagios: Provides a service that allows the IT organization to keep track of what systems and services are currently online within the network 24/7. This system has remained crucial for monitoring the health of the organization system as we continue to scale in growth over the first yearly quarter at the company. Without this system, it would be impossible to track what systems/services require critical attention without ticket reports from different users within our system.

Bank: Provides a service for receiving and storing the company's overall revenue in the form of credits. These credits allow the company to purchase flags and transfer funds to different organizations. If the credentials for the bank have been compromised, or the system goes offline, our organization/CEO would lose access to all of our funding, including the ability to obtain credits and potentially risk having all credits transferred to a different organization.

Email: Webapps also hosts our companies web email, including a corporate email encompassing the entire organization and anonymous emails for the team to use at their discretion. These emails allow for in-network communication between different teams, and the ability to report/confirm the submission of documents to corporate leaders. The credentials used for accessing these accounts are the same credentials used for Nagios and the Bank.

In a worst-case scenario that something happens to the Classex Web Services, or the credentials used for accessing the site become compromised, our company would simultaneously lose all the services provided above alongside suffering all the consequences that have been detailed. It is of the highest priority that the Classex Web Services remain online, with the credentials used to access the site stored and used with the highest level of confidentiality (including the systems used to access the web services).

3.2 Samba File share

The organization currently hosts two Samba file share systems, a shared folder for authorized employees to access, upload, and export classified documents. These shared folders are labeled "CommonShare" and are in the samba directory on both Linux systems. Users with proper permissions can access this folder locally using their respective user or can log in from a separate system by logging into their personal samba account (it is important to note that any user can log in and mount the CommonShare from any system so long as they have proper credentials linked with the file share).

Within these file shares holds the following information:

- Offensive Operation Plans: Reports containing offensive operations that are planned to be executed on different adversaries found within the network.
- Approved Operation Plans: Operation Plans that have been approved by our supervisor and are ready to be executed
- After Action Reports: Details discussing the success of our operation plans, along with any classified information that may have been exfiltrated.
- Network Reconnaissance: Details discussing the different systems discovered within the network our organization resides in, including the software the system is running and the subdomains that it runs on (i.e. other teams they may belong to).
- Incident Response Reports: Reports detailing incidents uncovered within the network performed by a particular threat actor, including the attackers point of entry, execution, exfiltration, systems targeted, and the IT team's response towards the incident.

These documents are then retrieved by the corporate to grade the overall progress of individual employees and the organization as a group. In the event the file share is compromised, threat actors would have access to highly classified data, including future operation plans (who we are targeting), persistence mechanisms used by our team within other systems, along with knowledge of potential incidents that, while potentially patched, can give insight to other vulnerabilities within our system. Threat actors can also create malicious files for employees to access, or even delete the contents found within our folders. In the event of a shutdown, where the file share is unable to be accessed, employees will be unable to submit necessary documentation with corporate being unable to review or approve any of the documents above. While alternative methods for submitting documents may exist while IT works on getting the file shares online, the security of the

files located within should not be underestimated and should be protected as much as possible.

3.3 Windows File share

Like our Samba servers hosted on Linux machines, our windows file shares function similarly but are hosted within our windows domain active directories. To access these file shares, users must log into their windows account with appropriate permissions. These file shares contain a folder called “Flags”, which serve as liquid assets for a corporation. These Flags are purchased from the Classex Bank and is the mission of every company to obtain all 15. Due to how sought out these flags are, other organizations (teams Florida, New York, Illinois, and California) have been known to launch offensive attacks to illegally obtain these flags for themselves. Teams looking to sabotage others may even delete the flags purchased by an organization, making it imperative that these files are backed up offline. Due to the highly sought out nature, and importance these flags serve, they should be treated with the same security and confidentiality as other classified documents (i.e. offense reports, incident response reports, episode reports, etc.).

3.4 Joomla/WordPress/Protected Sites

Our organization is currently hosting multiple webpages that require the user to enter their system login credentials to access the content of that site. As of 5/16/2024, the information being displayed on the sites themselves would not cause immediate concern if compromised. However, because the credentials are shared between system and webpage, a compromise of the user's webpage credentials would also mean a compromise of the users account for the domain the webpage is hosted on.

Our basic HTML webserver use default authentication methods. For our Apache (Linux) webserver, this would be “httpasswd” configuration, that restricts specific directories on a given website to require user credentials. These credentials are stored in a file located on the system hosting the Apache webserver and are currently configured to require the employee's username and password for the domain the webserver is located on.

Joomla and WordPress are two of the most popular systems for creating and managing websites. Both platforms offer a framework for developing dynamic websites, each with its own unique features and benefits. All implementations of Wordpress and Joomla interact with a database that can be found on a separate system than the one hosting the site, handling the storage of website content, user accounts/permissions, global extensions/permissions, comments (in the case of WordPress left by site visitors), and links.

In both scenarios, it is imperative that the credentials our employees are using always remain secure. While many the risks these information systems can be easily mitigated with proper employee training and policies for accessing secure websites, it only takes one user to compromise the entire organization system and has the potential to cause higher concerning information systems like our file shares to also be compromised.

3.5 Graylog Logging Server

Graylog is an open-source log management/analysis tool designed collect and analyze log data from various sources within our organization. The site is only accessible to the IT staff on our Sanantonio system found in our mining domain. The site serves X key components:

1. **Log Collection:** By collecting logs from different systems within the organizations network, graylog serves as a centralized point of reference easy and convenient access to insight on what's happening within the network and supports all types of log recording for any systems (both windows and Linux). These logs are currently being stored for 20 days and will also record any logs that may have been deleted from the system being recorded.
2. **Log Filtering:** Along with collecting logs from different systems, Graylog also allows the user to filter the type of logs being collected into the database and the frequency the logs occur.
3. **Querying:** The most important feature of graylog is the ability to query its database for logs between specific times, logs that contain a set of characters, logs from a

specific system, and more. For the IT staff, it provides a convenient way to search for potential incidents that may have been reported by employees or any suspicious activity on all systems at once.

4. Alerting/Monitoring: Graylog can also be configured to automatically query specific user instructions that can be monitored on the dashboard, allowing the IT team to constantly monitor for suspicious logins, system shutdowns/reboots, or access to restricted files.

A compromise of Graylog can lead to multiple concerns. In the event the IT team's credentials are compromised, a threat actor can access any system that shares the same credentials as the IT team. While the passwords for our IT team are not bound by the same rules as other employees, their accounts typically have the highest permissions, allowing for the attacker to have immediate privilege escalation on that system and giving them full control over it. On Graylog, threat actors will have access to monitor the logs of all systems within our network, potentially giving insight to potential vulnerabilities that can be exploited, or to figure out methods to evade our current logging techniques.

Another concern is the loss of logs. In the event Graylog is down, logs from all systems will not be forwarded, meaning the IT will have to view any logs manually from that system. This may not seem concerning on its own, but the organization is currently hosting over 60 systems within the network and can eat valuable time manually skimming through system logs manually that could have been spent more efficiently elsewhere.

3.6 HESK Ticketing Server

HESK serves as our organization's ticketing server for creating and issuing service tickets for our company's IT staff to complete along with keeping records of all tickets completed by the IT staff. This system is currently being hosted on our Windows 2019 running on build 2004 labeled CorpusChristi found on our steel domain and can be accessed by using the link <https://corpuschristi.steel.texas.tu/HESK>. IT staff who want to log in must pass credentials affiliated with the service under the administrative login section. Upon logging into their respective account, users can create, modify, or delete tickets of varying levels of priority. Users with elevated privileges can create accounts for other users on the system, managing certain privileges like creating/deleting tickets and creating/deleting users. This is an essential information system within our network that

allows corporate a direct line of access on the status of a tickets progress while allowing IT staff an easy way to directly distribute tickets to individual team members and keep track of other members progress.

3.7 Certificate Webserver

Our Certificate webserver is a HTML website, hosted on an Apache Web Server locally on our Brownsville system, that serves to provide our employees with a certificate signed by our company's certificate authority that encrypts all data communication passed between the client and webserver. It is important that all communication between clients and the server is encrypted, to prevent threat actors looking to steal sensitive information (particularly user credentials) as our employee's log into other web servers containing sensitive information. If the webserver is ever compromised, threat actors can replace the certificate, creating a potentially malicious certificate that compromises the webserver communication of our employees, or shut down/remove the certificate, requiring employees to directly reach out to IT for a new certificate while they work on getting the system online. While the webserver being down has minor effects on the overall operation of the network, it is important the integrity of the certificate hosted remains authentic and that all users within our safely accessing webserver within the network.

3.8 Unprotected Sites

Along with protected sites, our organization also hosts HTTP websites, containing public content regarding our organization. These websites do not require any user credentials to access but are hosted on the same systems as our HTTPS websites. The site's nature offers a minimal risk level for the company, as users connecting to the site (while their communication will be unencrypted), does not require the input of any sensitive data. While someone could interfere with a user's connection to the server and redirect them to a malicious site, this would mean that the domain services of our organization have been compromised and would bring a much larger raise of concern. Overall, so long as the data being displayed on these sites are not confidential, and our users are made aware of potential security risks/threats regarding organization webpages (social engineering attacks), these information systems should provide minimal risk to the organization

4. Threat Source Assessment:

The following table outlines potential internal and external threat sources to our information systems (threat sources that originate from within and outside the organization).

Threat Source	Origin	Threat Level
Team Kaiju	External	High
Team Illinois	External	High
Employees	Internal	Medium
IT Team	Internal	High
Team Florida	External	Medium
Team New York	External	Low
Team California	External	Low

4.1 Team Kaiju/Red Team:

Team Kaiju, and to a further extent Red Team, have raised the highest concern for the company. Their knowledge and expertise on the specific systems used by our organization has been shown on numerous occasions to outweigh the knowledge and expertise of the IT team defending it, giving name to their notoriety within other organizations. These red team organizations have been broken down into smaller groups, however team Kaiju has been known to be the biggest and loudest threat within our systems. Their goals have ranged between stealing organizational credits, shutting down systems that allow our organizations domain to function properly, antagonize/impersonate other teams within the network, attempting to cause tension between organizations, and obtaining as much persistence as possible within our networks. Out of all the threat sources discussed within this section, Red Team/Team Kaiju have been noted to be the source of most of all incident/reports documented by our IT team, warranting the highest threat level of all sources.

4.2 Team Illinois:

Team Illinois serves as a rival AI organization with similar corporate goals to our own. During the events of episode 3, it was discovered that Illinois had launched an offensive operation to steal sensitive data from within our file share, and after a successful exfiltration, demanded for our team to send them credits or they would leak the passwords to all our users within our network. We believe that this attack would only be the start and will soon start targeting our flags and credits. This attack, and the recent rise of

notoriety/progress within AI organizations, is what gave rise to their high threat level within the organization. Unlike Team Kaiju's unpredictability, Team Illinois has been shown to leave vulnerabilities discovered and used in offensive operations within their own system, making it easy to launch counter attacks. We also found evidence that, like our own organization, they require offensive operation plans to be approved before being performed, allowing us to potentially investigate their operation before an attack and is what warrants the teams lower threat score compared to red team.

4.3 IT Team:

The IT team plays a crucial role in maintaining and securing organizational systems. They are tasked with promptly addressing technical issues/ensuring system functionality, implementing security measures/finding vulnerabilities to safeguard against potential threats, and perform offensive operations for the organization on other teams. While the teams' efforts are instrumental in minimizing downtime and protecting the systems, uncoordinated/untested fixes/changes to the network have been known to happen, causing unnecessary downtime on the network. The team has also focused on rebuilding broken systems instead of fixing them without a strict policy in place, minimizing downtime, but causing all data on the systems from our users to be lost. It is also important to note that all potential threats/concerns discussed within the employee section also apply here, but due to their power within the system, raises a higher degree of concern, warranting the high threat level we have provided.

4.4 Team Florida:

Like team Illinois, Team Florida is an AI organization that was discovered to be deploying offensive attacks on other AI organizations (such as our alliance Team Florida). Offensive operations had been retrieved by the IT team during episodes 1 and 2, where the success of these attacks has been variable. While this team has not performed an offensive operation on us, the team has discovered and has expressed discern for our offensive attacks on them, likely leading to a potential attack in the future. As the experience of their IT team continues to grow, we believe that Team Florida has the potential to become a formidable threat within the near future, with the IT team being on the lookout for any signs of attack originating from the team in episode 3.

4.5 Employees:

While employees are a critical asset to our organization, they also represent a potential threat source due to various factors. One of the primary concerns is insider threats, where they may intentionally or unintentionally compromise security measures. For an unintentional example, we can point to phishing, a common exploit where we have seen employees (used in both our offensive operation and recorded in other team's incident responses) click suspicious links, compromising the workstations they use for accessing their email and online web services. For an intentional example, we have seen many disgruntled (or fired) employees deploy backdoors or intentional backdoors to maintain persistence to sensitive company information, as seen with the previous IT company and laid off employees after purchasing the auto domain. Therefore, proper security protocols/policies need to be implemented to ensure continuous monitoring and awareness, and employee training programs tailored to each employee's access level to effectively mitigate potential threats.

4.6 Team New York:

Team New York is a corporation specializing in artificial intelligence that has pledged to form an alliance with us during the second episode of the course. Throughout the semester, our organizations have discussed potential compromises and offensive operation plans that have improved the overall progress of our organization, even providing support during the ransomware attack with Team Illinois. While the team has discovered attacks from third parties (Team Kaiju) masquerading as Team Florida within our systems, our incident response team has found no evidence of the team invading our systems and have always brought to our attention approval for things such as network reconnaissance.

Moving forward, we hope this alliance stands strong, and due to the nature of trust between teams, believe that team New York bodes less of a threat to our systems compared to teams listed above, who have shown to take aggressive action against our organization (Team Illinois and Kaiju) or belong on bad terms with the organization (Team Florida).

4.7 Team California:

Team California is the final AI corporation discovered and active within our organization's network scope. As of April 25th, 2024, our IT team still retains persistence within their organization file share, containing sensitive information regarding future operation plans, incident responses, and reconnaissance. Judging from the latest

documents received from our offensive operations team, and the network status of their company, we deem them to provide the lowest threat to our organization.

While the team does not have an alliance, Fellow IT members in communication with the team regarded that their primary focus has been bringing systems online, typically discussing operation plans and potential targets in secret. This has led to a small pseudo alliance with the organization, with there being no reports obtained so far of the team targeting our organization for attack. While their team may have priorities elsewhere, we believe that, with the growth their organization has gone through within the past few months, this threat assessment could change by the end of the year.

5. Vulnerabilities:

The following is a list, from highest to lowest concern of exploitation, of vulnerabilities that were identified to be of concern to our information systems. While these vulnerabilities are described generically, each description will discuss the systems they particularly impact.

5.1 Software Version

Vulnerable libraries or functions allow adversaries to more easily gain unauthorized access to underlying infrastructure. Frequently updating software comes with the tradeoff of having to take a service offline for the period of time required to update it and may change its functionality. However, the benefits of updating software are that vulnerabilities are patched, and additional security features may be added to increase the resilience of a software to unauthorized access.

Unauthorized access comes in many forms. A couple of examples of unauthorized access to information systems are accessing administrative tools as a non-administrative user, and direct access to an underlying database from the system's browser interface.

The inability to update software to patch known and unknown vulnerabilities increases the likelihood of successful adversary activities.

5.2 Lack of Encryption

Weak or non-resilient methods being used to protect data. This can be in the form of hashes or other forms of cryptography. This could be in the form of WordPress credentials stored in plaintext or insecure webpage certificates.

Crackable encryption allows adversaries to gain privileged credentials in order to access sensitive information. On the other hand, storing plaintext credentials does not require any external tools to crack. Plaintext credentials are easier to use for those setting up a service but potentially provides malicious actors privileged credentials.

Insecure communication between web services is easier for adversaries to exploit when the certificate trusted by those services are themselves insecure. This can look like a website that doesn't support or use SSL, or a website with a malicious certificate that allows adversaries to conduct man-in-the-middle activities.

5.3 Weak Policies

Practices that increase the effectiveness of adversary attacks. This can be provided through lack of due diligence or foresight in standard practice. A few examples are user password reuse, insecure administrative work environments, or the use of sensitive credentials from multiple machines.

Adversary attacks to information systems should have as contained an impact as possible. Through weak policies, these attacks can potentially affect multiple systems, including those unintended by an adversary. This might look like an attack on a non-privileged user giving credentials to a privileged user due to credential reuse. Strong policies should increase the difficulty of gaining unauthorized access to privileged aspects of an information system.

5.4 Insufficient Logging

Records that are not kept of specific actions taking place on a system could easily lead to compromise. A few actions that should be logged are user logins to webpages, unsuccessful user logins to webpages, and access to database through webpage

Adversary attacks to information systems would be difficult to track as key information such as the time of attack is not tracked. Though insufficient logging itself is not a large vulnerability, it hinders efforts made to secure a system before, during, and after adversary attacks. The insufficient logging covered is not due to an attack, but due to the previously mentioned weak policies used to defend each information system.

Insufficient Filtering

Malicious and unauthorized network traffic should have difficulties going through an information system. This traffic could look like malicious commands sent over the network, or packets sent to known malicious IP addresses.

Defense of information systems becomes more difficult when adversaries are not inhibited in their ways of accessing a system. This could be through sending malicious packets to gain access to a privileged user through a known malicious IP address or having an information system communicate with a known malicious IP address to carry out persistence or an attack on the information system.

Due to the nature of the company and the services it provides, the range of filtered IP addresses must be limited. This means that only known malicious IP addresses with substantial proof of malicious activity can be filtered against.

5.5 Weak Configurations

Given the severity of settings inside information systems that result in increased effectiveness of adversary activities, keeping in line with best practice plays a large role in defense. Weak configurations could look like network section of configuration files being edited, unauthorized elevated user logins, or brute-force attacks on user logins.

Increased effectiveness of adversary activities potentially increases the number of vulnerabilities that must be patched in a system. This could be a setting that allows for administrative access without the need for a password, allowing an adversary to disable stronger configurations established in an information system. This would allow an adversary to have easier access to the compromised system and potentially enact persistence techniques by editing configuration files using compromised privileged credentials.

5.6 Weak Permissions

Access settings inside information systems that result in increased effectiveness of adversary activities pose a threat to those systems and the components connected to them. This could be unauthorized users reading and editing configuration files, or information system files.

Unauthenticated users should not be able to edit configuration files or access sensitive information stored on an information system or databases connected to those systems. This not only poses a threat from malicious employees, but adversaries as well.

This could be reading credentials stored on a website in order to access a privileged user or defacing a site using a non-privileged user with the ability to edit the contents of webpages.

6. Threat Assessment

The Following Table outlines potential threats to our information systems:

Threat	Likelihood of Occurrence	Impact	Uncertainty Estimate	Mitigation Risk	Risk Estimate
Data Loss/Ransomware	High (9)	High (10)	High (9)	Medium (6)	High (9)
Man-In-The-Middle	High (8)	High (9)	Medium (8)	Medium (6)	High (8)
Phishing	High (9)	High (9)	Medium (5)	Medium (7)	High (8)
Brute Force Attacks	Medium (7)	High (8)	Medium (5)	Medium (5)	Medium (7)
Insider Threat	Medium (7)	High (8)	High (8)	Low (4)	Medium (7)
Network Reconnaissance	High (10)	Low (2)	High (9)	Low (4)	Medium (7)
Counterfeit Certificates	Medium (6)	High (8)	Medium (5)	Low (2)	Medium (5)
Counterfeit Websites	Low (4)	High (8)	Low (3)	Low (2)	Low (4)
DDOS Attack	Low (2)	Low (4)	Low (4)	Low (1)	Low (3)

6.1 Data Loss/Ransomware

- **Description:** In the event that a user obtains access to an information system using the credentials obtained from an employee, they can attempt to exfiltrate any data within the information system (classified information, bank credentials, progress tickets, etc.) which can be used for their own benefit or be leveraged against us in the form of a Ransomware attack to extort more sensitive information.
- **Likelihood of Occurrence: High (9):** Throughout the semester, there have been 3 attacks on the organization regarding the loss of data and ransomware. Our organization has highly classified data in the form of reconnaissance, operation plans, incident response reports, flags, and credits that are a highly sought after target by all other teams. When the credentials of an employee have been

compromised, but the threat actor struggles to move laterally to sensitive information, they may resort to threatening easier to access classified information in return for compensation. We saw this during the ransomware attack with Illinois, where they were unable to access system flags or credits but attempted to leverage employee credentials for financial compensation. We also saw during the beginning of Episode 3, an attack from red team stealing the credits of all organizations within the system and continuing to steal credits from organizations that continued to have their credentials compromised. Finally, we must also consider the threat of fake ransomware attacks within our employee's emails, where the attacker may have nothing but still attempt to leverage falsified information for payment. We saw this during Episode 1, where a threat actor going by "red team" threatened other organizations to pay to keep their systems online via email. Overall, it is highly likely that in the event of a compromise, a threat actor will try to exfiltrate some form of data, either for their own benefit, or attempt to leverage that data (or false data) over the organization and its employees.

- **Impact: High (10):** Any form of data exfiltration within our system can lead to severe impact on the organization. Regardless of what data is exfiltrated, or what data is being leveraged in a ransomware attack, this loss of data will lead to the distrust of the company in the eyes of both the public and company employees. social media sites (in this case discord) and data dumping sites (in this case pastebin) make it easy for threat actors to publicly announce that a company's data has been compromised, making it easier to turn the public against us and put competing companies in the spotlight. Employees fearing their personal data will be stolen may also switch to different companies. We also must consider that the data being exfiltrated is highly confidential, like potential offense plans on other organizations that can easily place countermeasures and telegraph our attacks ahead time, or lead to the company's bankruptcy in the form of stolen credits or liquid assets like flags.
- **Uncertainty High (9):** Data loss and ransomware come with many forms of uncertainty. Depending on the skill/evasion of the threat actor, it can be hard to determine what data has been stolen until the threat actor leverages it. This can especially be the case in ransomware email attacks, as many threat actors may choose not to release the information they are leveraging, causing the company to have to guess if it's worth paying the ransomware. While organizations like the FBI may state to never pay and to report all ransomware threats, there are also examples of organizations like Colonial Pipeline who benefitted from paying their

ransomware. We must also consider that paying the ransomware does not guarantee the threat actor still won't keep their promise. While any loss of information is bad, uncertainties of whether to pay ransomware, or the internal impacts of data loss can vastly depend on the type of information being leveraged, the threat actor leveraging the threat, and how the threat is being leveraged.

- **Mitigation: Medium (6):** Data Loss/ransomware can be mitigated by ensuring any sensitive data on our information systems are being properly protected, and ensuring only authorized users have the proper permissions to access this data. As of the writing of this document, employees within our network are placed into user groups, each with their own permission to perform specific commands. For example, only authors in our Joomla and wordpress systems have permission to create or delete articles, while only administrators have permission to add and delete users. However, our organization does not have any restrictions in place on what employees can access classified data within our shared drives, requiring all users to have access. We believe that new policy guidelines regarding access to sensitive data must be enforced within the company to better protect our organization's data.
- **Risk Estimate:** $\frac{(9+10+9+6)}{4} = 8.5 \rightarrow 9$ (High)

6.2 Man-in-the-Middle

- **Description:** Threat actors looking to steal credentials of users logging into different information systems may attempt to perform a man-in-the-Middle attack where, at a high level, occurs when the malicious actor intercepts communication between the user and the website our employees use for accessing a particular web-service without their knowledge.
- **Likelihood of Occurrence: High (8):** Man in the middle attacks can be performed between any information system and the user's client, and only requires the knowledge of the server host and an unsuspecting user not using SSL/TLS. For our Joomla, WordPress, and protected websites, threat actors looking to obtain credentials to move lateral within our organization may attempt to abuse our weak password practices (having the same password throughout all domains, with the

difference being a 3-character prefix appended for the specific domain) to obtain credentials to a specific domain. This likelihood is further raised when considering the credentials for mission critical information systems hosted on webapps (bank, Nagios, etc.). Obtaining these credentials would give threat actor access to our company's bank, which is the end goal of every offensive operation within the scope of the network.

- **Impact: High (8):** In the event a threat actors attack is successful, the credentials of the target logging into our server have been compromised. The threat actor can move laterally onto any machine that shares the password stolen and perform actions of that user's permission level. In a worst-case scenario, this would be the compromise of our company's exercise credentials, allowing the user to access our organization's bank and lead to the potential loss of all company credits, directly effecting the CEO of the organization (being unable to pay employees or maintenance fees), prevents the organization of reaching one of our mission critical goals of collecting all 15 flags, and lead the company to bankruptcy. In a best-case scenario, only the credentials of a low permission user belonging to one of our domains would be compromised. In this case, a point of entry into that domain will have been created, and the threat actor can exfiltrate any sensitive information of the user. This would mean both the user and domain will have been compromised, and the threat actor could attempt to move laterally by finding misconfigurations within the information system or system it is running on.
- **Uncertainty Estimate: High (8):** It can be to identify and correlating a man-in-the-middle attack in real time to a specific threat actor. They can spoof their IP address to make it appear that it is part of the network or employ techniques to downgrade the Secure HTTP that a user's client is using to connect to the server without their knowledge.

The employees of our system also play an uncertainty factor, as a man-in-the-middle attack mostly relies on the awareness of the employee. While mitigation ideas such as awareness campaigns and security policies can raise awareness of these attacks and the importance of secure connections, our company currently employs over 1100 employees, where only one employee needs to make a mistake.

We must consider our own network's complexity. Each domain hosts an information system that has houses a risk of being vulnerable to a MitM attack, each providing a different point of entry with different users logging into our information systems, with varying levels of permissions/authority, creating a varying level of uncertainty

within the impact. For example, the compromise of an intern's credentials would not equate to the severity of an administrative officer in our support department.

Finally, we have the uncertainty of compromise. Threat actors who have successfully stolen credentials may not immediately use them, and instead wait for a specific time before commencing an attack. We can trace this uncertainty back to a recent incident regarding the loss of bank credentials, where it was discovered afterwards that the threat actor had used a fake banking site to steal our exercise credentials but waited until our company had accumulated more credits within our bank before launching their attack to transfer them.

- **Mitigations: Medium (6):** Mitigating the risk of MitM attacks can be achieved by combining encryption, company policies/user awareness, and network auditing. By implementing strong encryption protocols, organizations ensure that data exchanged between clients and servers is securely encrypted, making it difficult for attackers to intercept or manipulate the data. Certificates, a key component of encryption, allow secure communication by validating the identity of servers and clients. Through digital certificates issued through our organizations trusted Certificate Authority (and using the trusted certificate provided by the Classex exercise information systems), servers can prove their authenticity to clients, mitigating the risk of MitM attacks attempting to fake our company's information systems.

Alongside encryption, company policies and user awareness play a crucial role in mitigating MitM threats. Establishing clear policies and protocols for secure communication practices and access controls (i.e. establishing policies for what systems can access certain information systems, and how those systems will be treated before and after accessing that information system) sets a sturdy foundation for mitigating how a threat actor can use a MitM attack (typically being a passive attack, relying on the organizational employee to make the mistake). Educating users about the risks of MitM attacks raises awareness to recognize suspicious activities and avoid falling victim to social engineering tactics and report any suspicious behavior to our incident response division. These can take the form of quarterly training sessions, security awareness campaigns, and policy enforcement mechanisms.

Furthermore, proper network auditing and monitoring policies would allow for our IT team to detect unauthorized devices or unusual communication patterns that may indicate attempts of MitM. Programs like Burp Suite can allow for scanning of

common vulnerabilities discussed above, showing the exact network traffic/packets of certain systems that could be leveraged in these types of attacks. These programs can be used a step further for penetration testing, simulating MitM attacks to discover areas of where our information system could be vulnerable.

- **Risk Estimate:** $\frac{(8+8+8+6)}{4} = 7.5 \rightarrow 8$ (high)

6.3 Phishing

- **Description:** A malicious attacker attempts to extract sensitive information from a legitimate user or install malware onto a system or network via email, text, or other means of electronic communication.
- **Likelihood of Occurrence: High (9).** Because of its simplicity and lack of substantial policies and training to identify and report phishing emails within the company, attackers are highly likely to use phishing to install malware onto our information systems. We have found evidence of our adversaries utilizing phishing to install malicious files onto other teams' systems via their file share.
- **Impact: High (9).** Phishing can be used to target important individuals within the company, such as domain administrators. This means that sensitive information of these individuals can be compromised via a targeted phishing email, resulting in unauthorized access to our information systems. Malware installed through a phishing email can result in slower performance of compromised information systems and leakage of confidential or classified data.
- **Uncertainty: Medium (5).** Phishing attacks are common and are typically easily identifiable. However, well-crafted phishing emails can be difficult to discern from legitimate emails, resulting in employees mistakenly allowing the payload within the email to run, whether it is malware or an attempt to gather sensitive data.
- **Mitigation: Medium (6).** Phishing attacks can be mitigated through proper training of employees with the goal of ensuring they can discern a legitimate email from a malicious email. In the event an employee mistakenly clicks on the payload within a malicious email and an attacker gains access to one of our information systems, data leakage or harm to system performance can be mitigated via proper

protections to stored data, as well as a robust intrusion detection system and regular monitoring of system resources.

- **Risk Estimate:** $\frac{(9+9+5+7)}{4} = 7.5 \rightarrow 8$ (High)

6.4 Brute Force Attacks

- **Description:** A brute force attack involves a threat actor targeting a particular user on an information system and attempting to guess the credentials by repeatedly attempting log-in attempts until the threat actor has successfully logged in.
- **Likelihood of Occurrence: Medium (7):** Brute-force attacks share similar benefits to MitM attacks, enticing threat actors with the reward of user credentials that can allow the user to move laterally within the same domain (if the threat actor is aware that the passwords between shared between domains is shared for each employee). This attack also has the benefit of being passive, with threat actors typically only requiring a script to automatically guess the password in the background, allowing them to focus on researching other vulnerabilities or deploying other attacks. One of the downsides of this attack is that it can be very time-consuming and resource intensive, systematically attempting every possible combination of passwords until the correct one is found. However, this downside is minimized by company policy, as our employees are only allowed to change their password to a list of 9,000 pre-determined, dictionary words. This significantly cuts down the potential for passwords, assuming the prefix is has not been compromised (a set of characters within our employees passwords that cannot be changed), the total combination of passwords to guess would be 7962624000 (assuming 28 english characters, multiplied by 2 for capitals, and 40 symbols on a keyboard, to the power of 3 for the first 3 prefixes, multiplied by 9000). Assuming the threat actor has a computer to crack one password a second, it would take 252 years for our user's password to be cracked. However, if the prefix has been compromised, this reduces the combinations down to 9000, with the password only having a lifespan of 2.5 hours before being compromised. While a brute force attack may be tempting, for the attack to be worthwhile, it relies on if the organization's prefixes have been compromised, leading many threat actors likely using MitM to obtain users credentials.
- **Impact: High (9):** The impact of a brute force attack is very similar to MitM, with the targeted employees' credentials for that domain having been compromised, which

subsequently compromises the system the information system is hosted on, along with all other systems within the domain. Also, like MitM, the threat the compromised password causes largely depends on the account compromised. Unlike MitM, however, the credentials in a brute-force attack can be targeted, making it more likely that the threat actor will choose the credentials of a user likely to have higher permissions within the system to move lateral and access non-disclosed information, making it potentially more dangerous. What's more, now that the threat actor has access to the user's password, the time needed for all subsequent brute-force attacks becomes significantly faster with the compromise of the domains prefix credentials (as corporate requires these to not be changed).

- **Uncertainty: Medium (5):** Brute force attacks require the threat actor to attempt to log in and authenticate to know if the credentials are correct, making the attack loud and telegraphed, making it easier to discover when and where the attack took place. However, many uncertainties rise when we consider if prefix credentials have been compromised. As mentioned above, the threat actor knowing the prefix credentials can change the amount of time required from 215 years to 2.5 hours, significantly impacting the likelihood of occurrence and impact of the attack.
- **Mitigation: Medium (5):** While it's impossible to stop a threat actor from guessing a password, there are mitigations that can be placed to increase the time and difficulty to perform the attack. Software like ModSecurity can log/limit the number of requests sent to our information systems at once, increasing the time it takes for the threat actor to complete an authentication. Account lockouts/login timeouts can also be implemented, locking users accounts from logging in after a certain amount of failed login attempts. Finally, these can be logged and forwarded to a central logging service, where a query monitors for excessive login attempts and alerts the IT team.
- **Risk Estimate:** $\frac{(7+9+5+5)}{4} = 6.5 \rightarrow 7$ (medium)

6.5 Insider Threat

- **Description:** An insider threat refers to the risk posed by individuals within an organization who have authorized access to our information systems and data that intentionally abuse this authorization to bring harm to the company. These can

include current and former employees and can range from simple backdoors to data breaches/whistleblowers.

- **Likelihood of Occurrence: Medium (7):** After the firing of the previous IT team, the current IT team had monitored unauthorized access to the previous IT teams accounts while the team was in the process of analyzing these accounts for any sensitive data before deletion. The team had also discovered back doors/unauthorized access of former disgruntled employees from the auto domain that was bought out by the organization (who also refused to hand over access to the systems). While there have been no reports of insider threats on our information systems (due to most being relatively new), the potential of users purposefully leaking information still exists as more employees are hired/let go by the company or house a particular vendetta against the company. We must also consider accidental threats caused by insiders, where employees may accidentally be causing threats within the system. We have seen potential examples of this happening with PAExec, where misconfigurations from previous IT teams (or by our own employees) have caused memory overloads within our systems, causing them to crash (while not directly relating to an information system, is an example of accidental threats).
- **Impact: High (8):** Internal will have a better understanding of sensitive data and system vulnerabilities over external threat actors. For example, the previous IT employees would have a better understanding of Graylog/HESK and may have uncovered vulnerabilities that were unreported that grant them back doors back into the system, to check on what data is being logged or what tickets are being completed. This is sensitive information that can breed other potential threats to our systems, including data loss/ransomware attacks discussed above, making it imperative that former employees are properly removed from our systems and current employees are properly educated on handling sensitive data (while also having proper authorization).
- **Uncertainty: High (8):** Insider threats can come with several uncertainties that can complicate detection and mitigation efforts. First, every potential inside threat will likely have different motivations for their attack, ranging from revenge, financial gain, to whistleblowing/righteous acts, and can be tough to determine an employee's change in nature. Mistakes made by employees can also be misclassified as an insider threat, which can make it difficult to judge the nature of the threat. Skilled insiders who understand the network can make it harder to pinpoint when the threat

occurred, creating situations where an information system could be compromised months before the insider acts.

- **Mitigation: Low (4):** Insider threats can be mitigated by incorporating a combination of user privileges/policies, employee training/awareness, and user auditing. Users who have been let go from the company should immediately have any system/account access on our information systems revoked. In the scope of our information systems, this includes new exercise credentials being generated after an IT member is changed/let go, along with regular audits of credentials our employees use to log into our various websites, including Joomla, WordPress, email, and sites containing protected content. Employees should be trained to report any suspicious behavior changes among fellow employees which may be becoming an insider threat. Finally, policies should be set in place for restricting access to classified content. As mentioned above, we believe that not all users should have access to classified documents contained within the shared drive, and access should only be granted to users who have certain levels of clearance/are trusted by the company.
- **Risk Estimate:** $\frac{(7+8+8+4)}{4} = 7$ (medium)

6.6 Network Reconnaissance

- **Description:** Network reconnaissance involves an adversary scanning the corporate network to gather intelligence on the operating systems and services installed on individual machines, enabling the creation of a network map. This information can be used to determine the vulnerabilities that exist on a target network for future exploitation.
- **Likelihood of Occurrence: High (10).** Network reconnaissance was performed by the IT team throughout the semester to gather information about our adversaries' networks, particularly as new systems were built and acquired. It can therefore be assumed that our adversaries conducted similar reconnaissance operations throughout the past four months.
- **Impact: Low (3).** The act of network reconnaissance on its own poses little threat to the company's information systems. The information gathered can be used to perform subsequent attacks which exploit existing vulnerabilities within our

information systems, however. It is therefore important that the IT team locates and patches these vulnerabilities promptly.

- **Uncertainty: High (9).** Currently, the IT team does not have a defined method to detect and counteract network reconnaissance attempts. This makes it difficult to determine when a network reconnaissance scan has been launched, and by whom. Once this is established, the uncertainty of network reconnaissance will be reduced.
- **Mitigation: Medium (4).** Although network reconnaissance scans can be detected by tools such as Wireshark and promptly reduced, the act of eliminating adversarial network scans entirely is difficult. As stated above, it is important that the IT team locates and patches vulnerabilities exposed by a network scan. This can be accomplished by performing internal reconnaissance on the company network.
- **Risk Estimate:** $\frac{(10+3+9+4)}{4} = 6.5 \rightarrow 7$ (Medium)

6.7 Counterfeit Certificates

- **Description:** An attacker installs malicious certificates onto company-owned websites with the goal of gaining and extracting sensitive data such as user credentials. Malicious actors can trick legitimate users into accessing a website with the counterfeit certificate and then entering their personal information, such as passwords, credit card numbers, etc.
- **Likelihood of Occurrence: Medium (6).** There have been instances of our adversaries using fake SSL/TLS certificates on company-owned websites. Most notably, there has been evidence of Kaiju using a false certificate on our Lubbock workstation machine; all company HTTPS websites contained a certificate signed by “Red Team.” Kaiju also used a counterfeit certificate in conjunction with a fake website to gain access to our bank and exfiltrate all our credits to their account on April 15, 2024.
- **Impact: High (8).** Kaiju’s use of counterfeit certificates resulted in stolen credentials, as stated previously. These can be used to gain administrative access to our information systems, allowing attackers to access and cause harm to

important data. Essential services such as the bank have been compromised, resulting in a massive financial loss and emergency.

- **Uncertainty: Medium (5).** It can be difficult to determine whether a legitimate certificate has been replaced with a counterfeit certificate. It can also be difficult to determine which websites have been affected by the malicious certificate. However, malicious certificates can be relatively easy to identify when compared with legitimate certificates issued by the company for its websites. As stated previously, a counterfeit certificate can be signed by a malicious party, in this case “Red Team” instead of the company name.
- **Mitigation: Low (2).** Malicious certificates can be mitigated by enforcing strict policies with SSL/TLS certificates, such as requiring certain encryption standards, avoiding self-signed certificates and certificates issued by unknown certificate authorities, and regularly auditing certificates to search for signs of a counterfeit certificate. After implementing these mitigation strategies, chances of a counterfeit certificate attack reoccurring are low.
- **Risk Estimate:** $\frac{(6+8+5+2)}{4} = 5.25 \rightarrow 5(\text{Medium})$

6.8 Counterfeit Websites:

- **Description:** Attackers set up a fake website which redirects users away from a legitimate company-owned website and towards a malicious website. Often used with counterfeit certificates to extract sensitive information and steal company resources, such as bank credits.
- **Likelihood of Occurrence: Medium (4).** There has been a major instance of Team Kaiju using a fake website to gain access to sensitive credentials. Throughout March and April 2024, Kaiju set up a fake bank website with a malicious certificate with the goal of obtaining the IT team’s exercise password. The information gathered allowed Kaiju to successfully attack the company’s bank account and exfiltrate all stored credits to their offshore account.
- **Impact: High (8).** Kaiju’s attack on the company’s bank account caused a major financial emergency. Although the IT team was able to recoup much of the

company's credits through maintenance of important services, the attack resulted in a pause of flag purchases for multiple weeks. The IT team was not able to access Kaiju's bank account to return the stolen bank credits.

- **Uncertainty: Low (3).** The motivation in setting up counterfeit websites is largely the same across different attack sources. User credentials and sensitive company information are targeted by actors setting up malicious websites and certificates. Determining whether a website is false or not is largely dependent on web traffic analysis and ensuring that legitimate SSL/TLS certificates are used.
- **Mitigation: Low (2).** Mitigation of attacks utilizing counterfeit websites can be performed by ensuring the correct certificates are installed, as well as regular maintenance of web traffic to check for any redirects from a legitimate site to a malicious site.
- **Risk Estimate:** $\frac{(4+3+8+2)}{4} = 4.25 \rightarrow 4$ (Low)

6.9 DDOS Attack

- **Description:** A Distributed Denial of Service (DDoS) attack involves threat actors attempting to disrupt the functionality/availability of our information system/services by overwhelming it with a flood of traffic, causing the system to overload and shutdown.
- **Likelihood of Occurrence: Low (2).** There have been little to no signs of a DDOS attack occurring against the company's information systems throughout the last several months.
- **Impact: Medium (4).** A DDOS attack would disrupt the availability of our information systems, hindering the company's workflow and ultimately harming revenue due to downed public-facing and internal services such as WordPress, Joomla, and Apache.
- **Uncertainty: Medium (4).** There is some uncertainty involved in the execution of DDOS attacks against our systems, namely where the DDOS attack originated and

who is responsible. Attackers are known for using botnets to conduct DDOS attacks, making the entity responsible difficult to track and identify.

- **Mitigation: Low (1).** DDOS attacks can be prevented through a reverse proxy, as well as DDOS detection and prevention services which block malicious traffic from reaching important information systems and send malicious traffic away from them.
- **Risk Estimate:** $\frac{(2+4+4+1)}{4} = 2.75 \rightarrow 3$ (Low)