Group 44’s Incident Response Plan

Finalized on 12/14/2023

Introduction:

1. Purpose

The Computer Incident Response Team (CIRT) is established to protect and safeguard the organization's information systems and data from security threats, and to ensure a coordinated and effective response to computer security incidents. This charter outlines the scope, responsibilities, and explicit permissions granted to the CIRT in alignment with industry standards, organizational policies, and best practices.

2. Scope

The CIRT is responsible for addressing computer security incidents within the organization. This includes, but is not limited to, incidents involving:

Unauthorized access to sensitive information.
Malware infections, including ransomware attacks.
Suspicious network activity and intrusion attempts.
Insider threats and data breaches.
System vulnerabilities and security misconfigurations.

3. CIRT Responsibilities and Permissions

3.1 Security Event Monitoring and Incident Detection

In adherence to industry standards and organizational policies, the CIRT is granted the authority to:

Monitor and audit equipment, systems, and network traffic for security event monitoring and incident detection.
Deploy and maintain intrusion detection systems and security monitoring tools.
Collect and analyze data for the purpose of identifying and responding to security incidents.

3.2 Incident Response and Management

The CIRT is authorized to take the following actions as necessary, in accordance with incident management procedures:

Execute efficient incident management procedures, including, but not limited to, disabling network access, revoking access rights and credentials, or seizing and conducting forensic examination of electronic and computing devices.
Isolate affected systems or networks to prevent further compromise.
Coordinate with relevant stakeholders to contain and mitigate security incidents.
Engage in legal and law enforcement interactions as required by applicable laws and regulations.

3.3 Data Handling and Storage

In adherence to applicable legal and regulatory requirements, the CIRT has the authority to:

Maintain exhaustive and exclusive control over detecting, capturing, storing, analyzing, or mitigating computer security incidents.
Ensure the confidentiality and integrity of data collected or analyzed during the course of an investigation.
Securely store and manage evidence, logs, and incident data.

3.4 Communication and Reporting

The CIRT is authorized to:

Notify senior management, relevant departments, and external entities such as law enforcement, vendors, and regulatory bodies as necessary, in adherence to industry standards and organizational policies.
Prepare incident reports, post-incident summaries, and compliance documentation.

3.5 Continuous Improvement

The CIRT has the authority to:

Conduct post-incident reviews to identify areas for improvement.
Develop, update, and implement incident response policies, procedures, and best practices.
Recommend security enhancements and remediation strategies to mitigate future incidents.

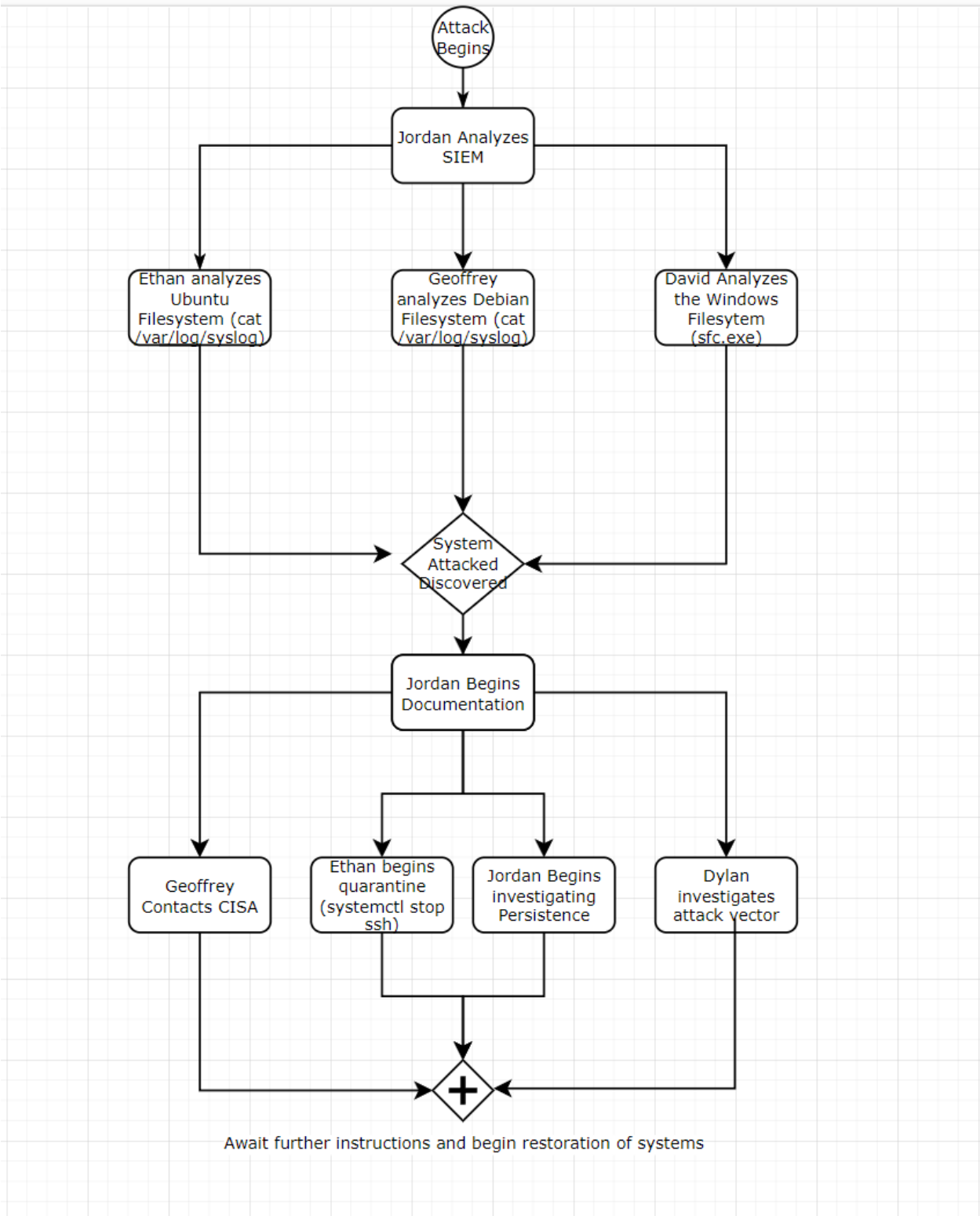
4. Compliance and Adherence

The CIRT shall operate in full compliance with all relevant industry standards, laws, and organizational policies. Any actions taken by the CIRT must be within the bounds of legal and ethical frameworks, ensuring the protection of individuals' privacy and organizational interests.

This charter is subject to periodic review and updates to reflect evolving security threats and regulatory changes. The CIRT shall collaborate closely with legal, compliance, and human resources departments to ensure alignment with organizational objectives and values.
[1]

[1] ***This introduction was in large part created by ChatGPT 3.5 and was modified by the incident response team to match the team's intended scope and permissions.***

5. Execution and Command Topology



Threat Profile:

Below is a risk register related to the linux systems in the environment. While there are both vulnerable linux machines and a vulnerable Windows machine, the linux machines exploits are much more common and catastrophic. These risks should be prioritized as they have potential to catastrophically affect the Linux systems and possibly give an attacker the ability to perform lateral movement to other systems in the environment.

Asset	**Vulnerability**	**Most likely/impactful Threats**	**Existing Controls**	**Likelihood**	**Impact**	**Risk**
Linux Kernel Mod32 register	CVE-2021-3444: Linux kernel does not properly handle register values, allowing for code execution.	If the register value can be changed to 0, remote code execution can be carried out.	Remove ability to load BPF programs. As this would likely be a local user, prioritize internal threat prevention.	Possible	Major	Extreme
Ubuntu 16.04 PHP EXIF Extension	CVE-2019-11050: Ubuntu 16.04 PHP EXIF Extension can be exploited for buffer overflow causing crashes or disruption.	If the extension is running, it can be used with certain values to overflow and crash servers.	Remove the extension or use different programs for EXIF reading. Keep machines with extension on an internal DMZ.	Rare	Minor	Low
Ubuntu 16.04 HTTP Server	CVE-2018-1000005: Ubuntu 16.04 HTTP server can mess up and overflow their HTTP trailer into the next header and cause crashes.	If the HTTP trailer is too big and overflows into next HTTP header, denial of service will occur.	Update HTTP servers and services. Block the ‘:’ character from the trailer field.	Likely	Major	Extreme
VNC Repeater	CVE-2018-20023: Ubuntu 16.04 VNC Repeater clients can read stack memory information that can lead to ASLR bypassing.	Stack memory exploitation and lead to other attacks. ASLR can be bypassed by exploitation of this vulnerability for information disclosure.	Disable VNC Repeater. Other methods of RDP can be used more effectively with less vulnerability likelihood.	Likely	Major	Extreme

Firefox on Ubuntu 16.04	CVE-2018-12397: Firefox version 63 can request access to local files without prompting the user causing content scripts to be run locally.	Local file access without permission from the user. This leads to information disclosure or script execution.	Update Firefox or use a different web browser. Disable permissions to use unapproved browser extensions.	Possible	Minor	Medium
Debian 9 Samba LDAP Server	CVE-2018-10919: Samba missing access control security checks allow for extraction of secure information from Active Directory as an “authenticated” user.	Unauthorized AD file extraction, credential extraction, C2 movement with elevated permissions.	Disable Samba, enable MFA for AD usage. Log SMB usage within the environment and sensitive file access.	Likely	Catastrophic	Extreme
Debian 9 Apache OfficeWriter and LibreOffice	CVE-2018-10583: Information disclosure occurs when these programs auto initiate an SMB request in a malicious file.	Unauthorized file extraction and file disclosure.	Disable SMB on machines that do not need access to remote shares on Windows Servers.	Likely	Major	Extreme
Debian 9 XFCE 4.16	CVE-2022-32278: XFCE Desktop software allows for clients to connect to malicious FTP Servers.	Malicious file extraction and execution on a local machine.	Disable FTP port on machines that do not need FTP. Block FTP usage on firewall for all IP Addresses other than necessary FTP servers.	Unlikely	Catastrophic	Extreme
Debian 9 Linux Kernel	CVE-2022-30594: Linux kernel mishandles seccomp request permissions allowing for flag manipulation.	Allow for malicious users to gain credentials and permissions to the environment by bypassing security flags.	Update Debian version and change permissions to access the flags in the kernel.	Unlikely	Major	High
Debian 9 Apache HTTP Server	CVE-2022-23943: Apache Server out-of-bounds memory vulnerability allows attackers to overwrite	Allows adversaries to add malicious code to local HTTP Servers.	Disable HTTP ports on unused servers. Disable write permissions on all HTTP server files.	Unlikely	Minor	Medium

	data with malicious code.	Malicious users could gain full control of systems.				
Debian 9 Linux Kernel	CVE-2022-0492: Debian 9 kernel cgroup_release_agent_ write flaw that allows for privilege escalation unintentionally.	Exploit allows for adversaries to bypass namespace rules and escalate privileges past their current credentials.	Disable port 53 if it is not needed in the current production environment. Update the kernel or disable all services associated with the release_agent feature for cgroup within the kernel.	Unlikely	Major	High

Governance:

Prioritization of assets and threats:

Cyber assets are all important to efficient functionality of Group 44. However, some systems must be prioritized for security vs. efficiency or in the event of an incident. In the case of an incident, the most mission-critical assets must be prioritized. For non-incident cases, efficiency must be sacrificed for security. Below are assets ranked in priority for incidents and security strength from highest to lowest.

Asset Priority:

1. ICS or BES systems
2. Systems hosting IDS or IPS functions
3. Domain controllers and Certificate Authority Servers
4. SIEM tool systems
5. Web servers or other critical services
6. DNS Servers
7. Client machines on corporate networks
8. Clients on any guest networks

In accordance with government regulations, cooperation with other companies, and for the well-being of all U.S. public company systems, collaboration with other entities is crucial for an incident response team. External partners that Group 44 would need to coordinate with include parties such as:

1. CISA
2. Homeland Security
3. SEC
4. E-ISAC
5. MITRE ATT&CK
6. FBI (If necessary or critical infrastructure)
7. Online Security Bulletins
8. Parent, child, or associated companies

Coordinating with government parties ensures a level of compliance with the law. Coordinating with other businesses ensures a high level of moral standing as well as high financial standing if the company is associated as a parent, child, or partner. Online security bulletins aid other organizations to ensure that attackers do the smallest amount of harm possible to United States organizations and corporations.

Legal guidelines must be followed when coordinating with government agencies. Organization policies including CISA Binding directive, Homeland Security Act for Energy Providers, SEC disclosures, PCI-DSS, Graham-Leech-Bliley, Sarbanes-Oxley, Critical infrastructure cyber incident reporting, and state laws. Descriptions for required deliverables due to each of the above guidelines are outlined below:

CISA Binding Directive:

The purpose of a CISA Binding Directive is a direction that agencies are pointed in to protect federal information and systems. When national security is at risk, it is imperative to integrate communication to CISA to create a binding directive to expose the vulnerability or threat actor for them to replicate to government agencies.

Homeland Security Act for Energy Providers:

Homeland Security created this act to provide a flow of communication between government and commercial parties in the United States to protect sensitive information originating from the country's energy sector. Vulnerabilities and threats coming from energy sector parties should be passed to Homeland Security to propagate out to the federal government.

SEC Disclosures:

The SEC possesses a risk management directive to help propagate information about national cybersecurity incidents without "unreasonable delay." This delay is a 4 day window that they must disclose to the United States when a national incident has become present.

PCI-DSS Requirements:

PCI-DSS Requirements for a business are a set of standards that are not enforced, but recommended, by law to be responsible and secure. The requirements include firewall implementation, change of default passwords, protect client data, encrypt data, use antivirus software, develop security systems, implement access control, assign user IDs to all users, restrict physical access, track data, test systems, and possess an information security policy.

Graham-Leech-Bliley:

This act is enforced by the FTC and requires financial institutions to be transparent with clients of their intent to protect their sensitive data. This helps prevent data breaches and keeps clients confident giving data that that need to provide.

Sarbanes-Oxley:

This act is enforced by the SEC and requires rules for financial record keeping. Accounting data is considered sensitive data and is required to follow standards in the keeping of this data to protect clients as well as the organization responsible for holding the data.

Critical Infrastructure Cyber Incident Reporting:

Organizations considered to be critical infrastructure are held on a tighter leash than other organizations or businesses because they have a direct effect on each other and the nation. If one piece of critical infrastructure is compromised, it is imperative to inform the other forms of critical infrastructure so that they do not all become compromised and pose a risk to national security.

State Law:

State laws leave businesses and organizations separated in their privacy protection laws. For example, some states have different requirements for client data protection, and some states have more relaxed laws to promote efficiency over security. State laws also leave some state businesses more susceptible to attacks as they could be potentially more vulnerable than a different area.

IR Playbook

Most Significant Risk

Below is the IR Playbook created for CVE-2018-10919. This risk allows for a user with no authentication to extract vital information from the Debian system, including login credentials. This allows for attackers to gain admin access from the machine without actually initially gaining access to the functions of the machine. This playbook details the steps needed to be taken in order to resolve and contain the incident. It follows the CISA playbook template and is modified to fit the specific CVE being investigated.

Step	Incident Response Procedure	Action Taken	Date Completed	Steps Taken to Resolve
	Detection & Analysis			
1. Declare Incident				
1a.	Perform initial categorization of incident			Determine the extent of how much information was gathered and the impact by looking at samba and system logs
2. Determine Investigation Scope				
2a.	Identify the type and extent of the incident			Use the MITRE Attack framework to determine the type of attack
2b.	Assess operational or informational impact on organization's mission			Look at the system logs and samba logs to determine the amount of information captured and compromised Commands like cat /var/log/syslog and ls /var/log/samba then either cat the logs that exist or use a text editor and search for specific entries like logins.
3. Collect and Preserve Data				
3a.	Collect and preserve the data necessary for incident verification, categorization,			Copy both sets of logs with cp /var/log and

	prioritization, mitigation, reporting, attribution, and as potential evidence			move them off the machine, look through file systems and login logs for any suspicious behavior. If suspicious behavior is found then make a copy of the evidence and move it off the machine.
3b.	Log all evidence and note how the evidence was acquired, when it was acquired, and who acquired the evidence			Attach notes to the previously collected evidence noting how it was acquired, who acquired it, and the time and date it was acquired.
4. Perform Technical Analysis				
4a.	Develop a technical and contextual understanding of the incident			Use the evidence to understand how the attacker infiltrated the machine and what information they extracted
4b.	Based on the analysis, form a hypothesis of what the adversary was attempting to access/accomplish			Make an assumption using the amount of extracted data and the types of extracted data to make an educated guess about why the attacker infiltrated the system. If the attacker extracted login information then it was likely to prepare for a future attack. If it was confidential information then it was possible for ransom.
4c.	Update scope as investigation progresses and information evolves			Continue to gather information and update the previous steps as the evidence is collected.
4d.	Terminating Condition: Technical analysis is complete when the incident has been			Close out the Analysis step once no new

verified, the scope has been determined, the method(s) of persistent access to the network has/have been identified, the impact has been assessed, a hypothesis for the narrative of exploitation has been cultivated, and all stakeholders are proceeding with a common operating picture			evidence is found and the methods and motives of the attacker have been identified
Correlate Events and Document Timeline			
4e. Analyze logs to correlate events and adversary activity			Use the system logs and samba logs to create a timeline of events and use that timeline to possibly locate more evidence
4f. Establish an incident timeline that records events, description of events, date-time group of occurrences, impacts, and data sources. Keep updated with all relevant findings.			Use the newly created timeline to create a list of all events that happened during the timeframe, whether it seems legitimate or suspicious
Identify Anomalous Activity			
4g. Assess affected systems and networks for subtleties of adversary behavior which often may look legitimate			Use the timeline to examine other systems for possible signs of intrusion. Examine login logs and system logs for anything that happened towards the end of the attack or just after the attack
4h. Identify deviations from established baseline activity - particularly important to identify attempts to leverage legitimate credentials and native capabilities and tools			Use the baseline to check for any unusual logins or data transfers
Identify Root Cause and Enabling Conditions			
4i. Attempt to identify the root cause of the incident and collect threat information that can be used in further searches and inform			Check online for other incidents in which this attack has occurred.

	subsequent response efforts			Use former incidents to help determine where to check for possible evidence of an attack
4j.	Identify and document the conditions that enabled the adversary to access and operate within the environment.			Note the Samba and Debian versions that were used to carry out the attack.
4k.	Assess networks and systems for changes that may have been made to either evade defenses or facilitate persistent access			Check for any new processes using the ps aux command. Use the previously created baseline to determine any unusual running processes. Check for any new users or any logins from users that are not common
4l.	Identify attack vectors. This includes how the adversary is accessing the environment.			Use system logs to determine where any data manipulation or transferring is occurring.
4m.	Assess access (depth and breadth). This includes all compromised systems, users, services, and networks			Determine the amount of information stolen from the system, especially login information. If user accounts were stolen then go through users on other systems for any possible overlap
Gather Incident Indicators				
4n.	Review available CTI for precedent of similar activity			Research online for previous incidents involving this CVE. Use this to help determine a possible mitigation.
4o.	Analyze adversary tools			Use syslog and samba logs with timestamps to determine the transfer

			speed and the possible hardware that the adversary is using
4p. Identify and document the indicators that can be used for correlative analysis on the network			Use network bandwidth monitoring and timestamps from the initial attack to determine when the attack was at its strongest
4q. Share extracted threat information with internal response teams and CISA			Share the evidence collected along with the logs to the CISA.
Analyze for Common Adversary TTPs			
4r. Identify initial access techniques			Use syslogs and samba logs to determine when the attack first took place and through what channel
4s. Identify the techniques used by the adversary to achieve code execution			Use login logs and syslogs to determine if commands were run by any possibly compromised user accounts
4t. Assess compromised hosts to identify persistence mechanisms			Use login logs to identify any possibly compromised accounts
4u. Identify lateral movement techniques			Use login logs to identify any shared accounts that were logged into after the compromise occurred
4v. Identify the adversary's level of credential access and/or privilege escalation			Determine the compromised account that had the highest privilege
4w. Identify the method of remote access, credentials used to authenticate, and level of privilege. If access is by legitimate but compromised application, identify the method			Determine the compromised account if any exist, if not then identify how information was

			extracted from samba and whether it was through authenticated means
4x. Identify the mechanism used for data exfiltration			Use syslogs and samba logs to identify what data was exfiltrated if any.
Validate and Refine Investigation Scope			
4y. Identify new potentially impacted systems, devices, and associated accounts			Continue to monitor other machines for common users and uncommon logins
4z. Feed new IOCs and TTPs into detection tools			Add possibly compromised accounts to detection tools to monitor for logins
4aa. Continue to update the scope and communicate the updated scope to all stakeholders to ensure a common operating picture			Add to the overall scope of the attack every time new information about the attack is uncovered. Share this information for any stakeholder.
5. Third-Party Analysis Support (if needed)			
5a. Identify if third-party analysis support is needed for incident investigation or response.			Identify if the attack is larger than the team is prepared for. If so, then contact an outside team for assistance
5b. Invoke Federal Network Authorization to enable CISA incident response and hunt assistance			If the attack is not prepared for then notify the CISA for assistance
5c. Coordinate and facilitate access if incorporating third-party analysis support into response efforts.			Provide the evidence acquired to the hired assistance and provide the assistance with temporary logins to the environment
5d. Coordinate response activities with agency service providers for systems hosted			Create a list of all findings from the new

	outside of the agency.			assistance and share with all agents
6. Adjust Tools				
6a.	Tune tools to slow the pace of advance and decrease dwell time by incorporating IOCs to protect/detect specific activity			Create access lists that only allow accepted users during accepted hours.
6b.	Introduce higher-fidelity modifications to tools. Tune tools to focus on tactics that must be used by the adversary to obtain operational objectives			If the attack seems deep enough, introduce a new IPS to prevent an external agent that is unauthorized from accessing the network.
	Containment			
7. Contain Activity				
7a.	Determine appropriate containment strategy			Remove the affected device from the network
7b.	System Backup to preserve evidence and continue investigation			Move all evidence off the machine and off the network
7c.	Coordinate with law enforcement to collect and preserve evidence prior to eradication, if applicable			Provide copies of the evidence to law enforcement to preserve the evidence
7d.	Isolate affected systems and networks			Remove the affected device from the network and disable any user accounts on any other device that may be compromised
7e.	Close specific ports and mail servers. Update firewall filtering.			Block all traffic from the debian machine to any other machine on the network. Block SSH for any user that may have been compromised to any other machine
7f	Change system admin passwords, rotate private keys, and service/application			Change all user account passwords and rotate all

	account secrets where compromise is suspected revoke privileged access			SSH keys. Disable SSH for Debian
7g.	Perform blocking (and logging) of unauthorized accesses, malware sources, and egress traffic to known attacker Internet Protocol (IP) addresses.			Setup UFW on debian to block any attempted SSH logins, setup network monitoring to monitor any access from outside sources
7h.	Prevent Domain Name Server (DNS) resolution of known attacker domain names			Disable DNS servers for the Debian server
7i.	Prevent compromised systems from connecting to other systems on the network			Block all traffic from the debian machine to any of the other devices on the network with a firewall
7j.	Advanced SOCs may direct adversaries to sandbox to monitor activity, gather additional evidence and identify TTPs.			Setup an environment with just the Debian machine to monitor any activity to the machine
7k.	Monitor for signs of threat actor response to containment activities			Monitor all systems for logins and monitor messaging for any attempts at a ransom
7l.	Report updated timeline and findings to CISA			Share the timeline created earlier with the CISA and continue to share evidence
7m.	If new signs of compromise are found, return to technical analysis to re-scope the incident			Return to step 4 if any new evidence turns up about the attack
7n	**Terminating Condition:** Upon successful containment (i.e., no new signs compromise), preserve evidence for reference and law enforcement investigation (if applicable), adjust detection tools, and move to eradication.			Share all evidence with law enforcement and the CISA
	Eradication & Recovery			
8. Execute Eradication Plan				
8a.	Develop a well-coordinated eradication			Turn off any unknown

	plan that considers scenarios for threat actor use of alternative attack vectors and multiple persistence mechanics			services that are not part of the baseline, change all account passwords, check for any unknown SSH keys
8b.	Provide Incident Status to CISA until all eradication activities are complete			Share new information with the CISA everytime a new step is performed
8c.	Remove artifacts of the incident from affected systems, networks, etc.			Disable any unused user accounts and remove any unknown processes. If any unknown documents are found then remove them.
8d.	Reimage affected systems from clean backups (i.e., ‘gold’ sources).			Do not restore to backup unless absolutely necessary as compromised passwords will return after being changed
8e.	Rebuild hardware (if rootkits involved).			Use the IR jumpbag to implement new hardware
8f.	Scan for malware to ensure removal of malicious code			Use malware scanners to check if any malware was installed post-compromise
8g.	Monitor closely for signs of threat actor response to eradication activities			Monitor all devices and all communication channels for any unusual activity
8h.	Allow adequate time to ensure all systems are clear of threat actor persistence mechanisms (such as backdoors) since adversaries often use more than one mechanism.			Monitor all devices for an extended period of time to ensure that there is no possible hidden activity
8i.	Update the timeline to incorporate all pertinent events from this step.			Continue to update the previously created timeline
8j.	Complete all actions for eradication			Complete all of the steps above

8k.	Continue with detection and analysis activities after executing the eradication plan to monitor for any signs of adversary re-entry or use of new access methods.			Continue to monitor for any unauthorized access to the machine over an extended period of time
8l.	If new adversary activity is discovered at the completion of the eradication step, contain the new activity and return to Technical Analysis until the true scope of the compromise and infection vectors are identified.			If any unauthorized access occurs, determine if it relates to this incident. If it seems to relate to this incident then return to step 4
8m.	If eradication is successful, move to Recovery			Once all the steps above are finished and no new access is monitored then move onto step 9
9. Recovery				
9a.	Restore agency systems to operational use: recovering mission/business data			Disable the firewall between the debian machine and all other machines, turn SSH back on for the debian machine
9b.	Revert all changes made during incident			Perform step 9a
9c.	Reset passwords on compromised accounts			Change the passwords for any accounts that seem to have been compromised and change all administrator passwords
9d.	Implement multi-factor authentication for all access methods			Implement either a new service or a new tool such as Google authenticator to login
9e.	Install updates and patches			Update all machines that aren't the debian or Ubuntu 16.04 machine
9f.	Tighten perimeter security and zero trust access rules			Implement access control lists to allow only access from trusted IPs and only during specific times of day
9g.	Test systems thoroughly to validate			Test the SSH service

	systems are operating normally before bringing back online in production networks.			and the samba service after bringing the services back up
9h.	Consider emulating adversarial TTPs to verify countermeasures are effective			If necessary create an environment where you can test the vulnerability that was carried out and practice responding to it
9i.	Review all relevant CTI to ensure situational awareness of the threat actor activity			Monitor news feeds for any similar attacks
9j.	Update incident timeline to incorporate all pertinent events from recovery step.			Continue to update the previously created timeline
9k.	Complete all actions for recovery.			Complete steps 9a-9j
	Post-Incident Activities			
10. Post-Incident Activities				
10a.	Document the incident, inform agency leadership, harden the environment to prevent similar incidents, and apply lessons learned to improve the handling of future incidents.			Setup firewalls to prevent unauthorized access to services, inform partners of current status, update any machine that isn't the debian or Ubuntu 16.04 machine. Implement a monthly required password change
Adjust Sensors, Alerts, and Log Collection				
10b.	Add enterprise-wide detections to mitigate against adversary TTPs that were successfully executed.			Setup login monitoring and login alerts to alert the response team in the case of unauthorized logins
10c.	Identify and address operational "blind spots" to adequate coverage moving forward.			Setup network monitoring in regards to services. Setup samba log integration into the SIEM

10d.	Continue to monitor the agency environment for evidence of persistent presence.			Continue to monitor logins and samba logs
Finalize Reports				
10e.	Provide post-incident updates as required by law and policy			Continue to supply evidence and status updates to the CISA and law enforcement
10f.	Publish post-incident report. Provide a step-by-step review of the entire incident and answer the Who, What, Where, why, and How questions.			Detail the attackers methods, possible motive, and any possible information about the identity of the attacker
10g.	Provide CISA with post-incident update with seven days of resolution or as directed by CISA in the Federal Incident Notification Guidelines			Provide the CISA with the post-incident report soon after completing the report
10h.	Work with CISA to provide required artifacts, close the ticket, and/or take additional response action.			Continue to work with the CISA to finish out the collaboration
Perform Hotwash				
10i.	Conduct lessons learned analysis with all involved parties to assess existing security measures and the incident handling process recently experienced.			Use the attackers methods and determine possible areas of improvement for the incident response team
10j.	Identify if agency IR processes were followed and if they were sufficient			Determine the time it took to resolve the incident and if it was sufficiently solved fast enough to prevent damage to the organization’s mission
10k.	Identify any policies and procedures in need of modification to prevent similar incidents from occurring.			Determine if the policy that prevents modification of the older systems is sufficient or if the policy should be modified to give the incident response team

			more freedom
10l. Identify how information sharing with CISA and other stakeholders can be improved during IR.			Identify the problems involved with communications during the incident. If any communications were slow or hindered then properly note them and provide possible methods to improve in future incidents.
10m. Identify any gaps in incident responder training.			Identify if any team member struggled in identifying their role and properly carrying it out. If a team member did struggle then address ways to improve the team members knowledge and skills in the proper area.
10n. Identify any unclear or undefined roles, responsibilities, interfaces, and authorities.			Identify any confusion amongst the team in terms of priorities. If an issue arises, help to clear it up before any future incidents.
10o. Identify precursors or indicators that should be monitored to detect similar incidents.			Identify what could have been done to have caught this attack even earlier than it was captured. Install software or update policies to facilitate this process.
10p. Identify if agency infrastructure for defense was sufficient. If not, identify the gaps.			Look for any gaps of time where nothing was done or could be done, adjust policy and technology to prevent this from occurring in the future.
10q. Identify if additional tools or resources are			Perform research on

	needed to improve detection and analysis and help mitigate future incidents.			how to adapt current tools or install new tools to help detect or prevent attacks.
10r.	Identify any deficiencies in the agency incident response planning process. If no deficiencies identified, identify how the agency intends to implement more rigor in its IR planning			Look for weaknesses in the incident response plan in which the team did not use, identify ways to improve these portions to ensure that the response plan can help in the future.
	Coordination with CISA			
11. Coordination with CISA				
11a.	Notify CISA with initial incident report within 1 hour after incident determination.			Immediately provide the CISA with any details involving suspicious artifacts or evidence
11b.	Receive incident tracking number and CISA National Cyber Incident Scoring System (NCISS) priority level from CISA.			Mark any emails or documents from the CISA as important and move to a secure location for future reference.
11c.	Comply with additional reporting requirements for Major incidents as mandated by OMB and other federal policy.			Immediately comply with any requests from Government organizations.
11d.	Provide incident updates until all eradication activities are complete.			Continue to provide all reported updates to the CISA until the incident is considered sufficiently responded to
11e.	Report incident updates			Complete step 11d
11f.	Share relevant atomic and behavioral indicators and countermeasures with CISA throughout the IR process			Provide the CISA with the attempted methods of resolving the incident
11g.	Provide post-incident updates as directed by CISA.			Continue to comply with the CISA and

			provide information
11h. ICT service providers and contractors who operate systems on behalf of FCEB agencies must promptly report incidents to such agencies and directly report to CISA whenever they do so.			Report to the CISA with any incidents when they occur

Incident 1

Step	Incident Response Procedure	Action Taken	Date Completed
	Detection & Analysis		
1. Declare Incident			
1a.	Perform initial categorization of incident	Looked at initial logs and packet captures to identify as Denial of Service attack	11/28/2023
2. Determine Investigation Scope			
2a.	Identify the type and extent of the incident	Denial of Service against SSH on Ubuntu and Debian machine. MITRE Attack ID T1498.001 Network Denial of Service Attack	11/28/2023
2b.	Assess operational or informational impact on organization's mission	SSH still reachable, just slightly slowed, nothing else impacted	11/28/2023
3. Collect and Preserve Data			
3a.	Collect and preserve the data necessary for incident verification, categorization, prioritization, mitigation, reporting, attribution, and as potential evidence	Packet Capture saved, sysctl.conf date modified saved, login logs saved and Commands run:	11/28/2023

	sudo tcpdump -w - -U | sudo tee filename.$(date +%Y.%m.%d.%Z.%H.%M.%S) | sudo tcpdump -r - , sudo last, sudo lastb, sudo vi /etc/sysctl.conf, sudo stat sysctl.conf	
3b. Log all evidence and note how the evidence was acquired, when it was acquired, and who acquired the evidence	Packet captures acquired via sudo tcpdump -w - -U | sudo tee filename.$(date +%Y.%m.%d.%Z.%H.%M.%S) | sudo tcpdump -r -, cat /etc/syslog, stat /etc/sysctl.conf, last, and lastb	11/28/2023
4. Perform Technical Analysis		
4a. Develop a technical and contextual understanding of the incident	Syn packets are being sent in mass to the SSH port on the Ubuntu machine. The attacker is spoofing many different IP addresses. Only Syn packets are being received without further Syn Ack messages.	11/28/2023
4b. Based on the analysis, form a hypothesis of what the adversary was attempting to access/accomplish	The attacker is likely trying to disrupt service to the Ubuntu machine. After looking at SSH logins, only confirmed administrators has accessed the system since the attack has started so this is likely just a malicious attempt to	11/28/2023

	disrupt services.	
4c. Update scope as investigation progresses and information evolves	This attack is only on the ubuntu and debian machines and does not seem to have affected any internal logs	
4d. Terminating Condition: Technical analysis is complete when the incident has been verified, the scope has been determined, the method(s) of persistent access to the network has/have been identified, the impact has been assessed, a hypothesis for the narrative of exploitation has been cultivated, and all stakeholders are proceeding with a common operating picture	The attacker sent a syn flood in an attempt to deny access to the SSH service. This has only slightly slowed the service down. This attack seemingly only affects the Ubuntu machine but some of the packets are being sent to the Debian machine	11/28/2023
Correlate Events and Document Timeline		
4e. Analyze logs to correlate events and adversary activity	Syslog and login logs were analyzed, nothing out of the ordinary was noted. Auth.log was checked using cat /var/log/auth.log but nothing out of the ordinary was noted.	11/28/2023
4f. Establish an incident timeline that records events, description of events, date-time group of occurrences, impacts, and data sources. Keep updated with all relevant findings.	The SYN flood is consistent, starting early on the 27th and continuing through to the 28th. There has been no noticeable change in anything internally during the noted time frame.	11/28/2023
Identify Anomalous Activity		
4g. Assess affected systems and networks for subtleties	No changes were	11/28/2023

	of adversary behavior which often may look legitimate	noticed outside of the Syn flood. Logs and config files related to SSH were checked but seemingly not changed.	
4h.	Identify deviations from established baseline activity - particularly important to identify attempts to leverage legitimate credentials and native capabilities and tools	The only noted change from the baseline is the amount of network activity occurring due to the Syn Flood.	11/28/2023
Identify Root Cause and Enabling Conditions			
4i.	Attempt to identify the root cause of the incident and collect threat information that can be used in further searches and inform subsequent response efforts	The likely cause of this incident is the syncookies being set to false. The syncookies function exists to deter Syn flood attacks but was set to the non-default 0 at some point before reaching current administrator hands.	11/28/2023
4j.	Identify and document the conditions that enabled the adversary to access and operate within the environment.	As stated above, syncookies is set to the non-default option 0.	11/28/2023
4k.	Assess networks and systems for changes that may have been made to either evade defenses or facilitate persistent access	There has been no notable access to the system. No new processes are started and no new programs installed.	11/28/2023
4l.	Identify attack vectors. This includes how the adversary is accessing the environment.	A misconfigured sysctl.conf is what allowed the adversary to attack the Ubuntu and Debian machines.	11/28/2023

4m.	Assess access (depth and breadth). This includes all compromised systems, users, services, and networks	This attack seems to have only affected the SSH service, and only minorly at that. The system itself and its network seem to still have full functionality.	11/28/2023
Gather Incident Indicators			
4n.	Review available CTI for precedent of similar activity	Search for previous or current ongoing denial of service attacks against server services.	Not currently completed
4o.	Analyze adversary tools	Adversary seems to be using a bot to spoof IP addresses and send Syn messages to the SSH service on the machines.	11/28/2023
4p.	Identify and document the indicators that can be used for correlative analysis on the network	Tcpdump output can be used to identify the common spoofed IP addresses that are flooding the SSH services.	11/28/2023
4q.	Share extracted threat information with internal response teams and CISA	Send CISA report on the tcpdump information along with the spoofed IP addresses gathered from the tcpdump.	Not Completed
Analyze for Common Adversary TTPs			
4r.	Identify initial access techniques	The attacker exploited a misconfigured line in the sysctl.conf file to exploit the attack.	11/28/2023
4s.	Identify the techniques used by the adversary to achieve code execution	The attacker did not achieve local code execution.	11/28/2023

4t.	Assess compromised hosts to identify persistence mechanisms	The attacker did not achieve persistence through their own means, only through the misconfiguration in the sysctl.conf file.	11/28/2023
4u.	Identify lateral movement techniques	The attacker did not perform lateral movement, only attempted denial of service on the Ubuntu and Debian machines.	11/28/2023
4v.	Identify the adversary's level of credential access and/or privilege escalation	The attacker did not gain credential access or privilege escalation.	11/28/2023
4w.	Identify the method of remote access, credentials used to authenticate, and level of privilege. If access is by legitimate but compromised application, identify the method	There was no remote access, only attempted denial of service	11/28/2023
4x.	Identify the mechanism used for data exfiltration	There was no data exfiltration	11/28/2023
Validate and Refine Investigation Scope			
4y.	Identify new potentially impacted systems, devices, and associated accounts	The Ubuntu and Debian machines are the only affected systems, with their SSH services being the only impacted parts of the services.	11/28/2023
4z.	Feed new IOCs and TTPs into detection tools	Implement port mirroring and network audits.	Not Completed
4aa.	Continue to update the scope and communicate the updated scope to all stakeholders to ensure a common operating picture	Send information to stakeholders as it is discovered as well as document any new findings.	Not Completed
5. Third-Party Analysis Support (if needed)			

5a.	Identify if third-party analysis support is needed for incident investigation or response.	Not required	Not Completed
5b.	Invoke Federal Network Authorization to enable CISA incident response and hunt assistance	Not required	Not Completed
5c.	Coordinate and facilitate access if incorporating third-party analysis support into response efforts.	Not required	Not Completed
5d.	Coordinate response activities with agency service providers for systems hosted outside of the agency.	Not required	Not Completed
6. Adjust Tools			
6a.	Tune tools to slow the pace of advance and decrease dwell time by incorporating IOCs to protect/detect specific activity	Implement the port mirroring to mirror the only the vulnerable machines that are not protected by a firewall	Not Completed
6b.	Introduce higher-fidelity modifications to tools. Tune tools to focus on tactics that must be used by the adversary to obtain operational objectives	Setup network logs for the ELK stack to monitor unusual network behavior	Not Completed
	Containment		
7. Contain Activity			
7a.	Determine appropriate containment strategy	Send packet captures to non-affected machines and backup on the cloud. Possibly change SSH services temporarily to use different ports.	Not Completed
7b.	System Backup to preserve evidence and continue investigation	Backup the affected systems	Not Completed
7c.	Coordinate with law enforcement to collect and preserve evidence prior to eradication, if applicable	Notify law enforcement and collaborate on what evidence to save	Not Completed
7d.	Isolate affected systems and networks	Ensure firewalls are blocking unnecessary access	Not Completed

		to Windows machines	
7e.	Close specific ports and mail servers. Update firewall filtering.	Install and enable ufw on Ubuntu and Debian machines. Do not close ports as the ports are needed for normal access.	Not Completed.
7f	Change system admin passwords, rotate private keys, and service/application account secrets where compromise is suspected revoke privileged access	Compromise is not suspected, still change admin passwords and rotate private keys	Not Completed
7g.	Perform blocking (and logging) of unauthorized accesses, malware sources, and egress traffic to known attacker Internet Protocol (IP) addresses.	Setup network auditing and firewalls on Ubuntu and Debian machines	Not Completed
7h.	Prevent Domain Name Server (DNS) resolution of known attacker domain names	Disable DNS services of the Ubuntu and Debian machines until registered domain names can be confirmed	Not Completed
7i.	Prevent compromised systems from connecting to other systems on the network	Block access from the Ubuntu and Debian machines using the Windows firewall on the remaining servers	Not Completed
7j.	Advanced SOCs may direct adversaries to sandbox to monitor activity, gather additional evidence and identify TTPs.	Does not apply in this situation.	Not Completed
7k.	Monitor for signs of threat actor response to containment activities	Monitor active network traffic with tcpdump -v	Not Completed
7l.	Report updated timeline and findings to CISA	Send new tcpdump logs to CISA along with any new evidence found	Not Completed
7m.	If new signs of compromise are found, return to	Check through the	Not

	technical analysis to re-scope the incident	new evidence to see if any new compromises are discovered. If none, then continue. If there are new compromises, then return to step 4.	Completed
7n	**Terminating Condition:** Upon successful containment (i.e., no new signs compromise), preserve evidence for reference and law enforcement investigation (if applicable), adjust detection tools, and move to eradication.	Backup new tcpdump logs, setup network auditing for ELK stack.	Not Completed
	Eradication & Recovery		
8. Execute Eradication Plan			
8a.	Develop a well-coordinated eradication plan that considers scenarios for threat actor use of alternative attack vectors and multiple persistence mechanics	Enable syncookies, create a list of all spoofed IP addresses, setup ufw firewalls	Not completed
8b.	Provide Incident Status to CISA until all eradication activities are complete	Report the incident to report@cisa.gov with a status of the current incident and proof of tactic used.	Not completed
8c.	Remove artifacts of the incident from affected systems, networks, etc.	Enable syncookies and configure firewall to block specified IP addresses.	Not completed
8d.	Reimage affected systems from clean backups (i.e., ‘gold’ sources).	This item of eradication is not necessary for a synflood attack.	Not completed
8e.	Rebuild hardware (if rootkits involved).	This does not apply to a SYN flood attack	Not completed
8f.	Scan for malware to ensure removal of malicious code	This does not apply to a SYN flood attack	Not completed
8g.	Monitor closely for signs of threat actor response to	Frequently check	Not completed

	eradication activities	syslog logs and IDS outputs for known IP addresses and spikes on ports.	
8h.	Allow adequate time to ensure all systems are clear of threat actor persistence mechanisms (such as backdoors) since adversaries often use more than one mechanism.	Check configurations of affected services (SSH) and ensure no changes have been made.	11/28/2023
8i.	Update the timeline to incorporate all pertinent events from this step.	Append documentation with attacker tactics, preventative measures, and CIRP completed tasks.	Not completed
8j.	Complete all actions for eradication	Complete steps 8a-8h for eradication.	Not completed
8k.	Continue with detection and analysis activities after executing the eradication plan to monitor for any signs of adversary re-entry or use of new access methods.	Continue monitoring Syslog and SSH log files. Install IDS for further detection of syn flooding.	Not completed
8l.	If new adversary activity is discovered at the completion of the eradication step, contain the new activity and return to Technical Analysis until the true scope of the compromise and infection vectors are identified.	If a synflood is still occurring after step 8k, redo the technical analysis and assess which steps of containment needs to be reevaluated.	Not completed
8m.	If eradication is successful, move to Recovery	If the synflood is stopped, move on to recovery steps #9 below.	Not completed
9. Recovery			
9a.	Restore agency systems to operational use: recovering mission/business data	Re-enable the SSH service and ensure that the service is uninterrupted.	Not completed
9b.	Revert all changes made during incident	Re-enable DNS	Not completed

	services that were temporarily shut down and any specific ports closed down in the technical section.	
9c. Reset passwords on compromised accounts	Reset passwords on all admin accounts, root account, and any account used during the duration of the attack to lock the adversary out.	Not completed
9d. Implement multi-factor authentication for all access methods	Implement mandatory multi-factor authentication via Duo Mobile for all users.	Not completed
9e. Install updates and patches	Use sudo apt update && sudo apt upgrade to update to update all packages.	Not completed
9f. Tighten perimeter security and zero trust access rules	Implement mandatory access control for all services and files affected by synflood.	Not completed
9g. Test systems thoroughly to validate systems are operating normally before bringing back online in production networks.	Connect to a system via SSH with normal credentials and monitor the services to ensure there is no synflood occurring.	Not completed
9h. Consider emulating adversarial TTPs to verify countermeasures are effective	Install a Kali Linux VM and launch a synflood attack on port 22. Verify traffic is logged in correct files and synflood is picked up.	Not completed
9i. Review all relevant CTI to ensure situational awareness of the threat actor activity	Research Microsoft Threat Intel and	Not completed

	other trusted sources to verify all tactics are recognized for synfloods.	
9j. Update incident timeline to incorporate all pertinent events from recovery step.	Append current CIRP with completed recovery measures to restore full functionality to the services.	Not completed
9k. Complete all actions for recovery.	Complete steps 9a-j for recovery steps to be complete.	Not completed
Post-Incident Activities		
10. Post-Incident Activities		
10a. Document the incident, inform agency leadership, harden the environment to prevent similar incidents, and apply lessons learned to improve the handling of future incidents.	Documented incident, informed leadership, and in the process of applying lessons learned from incident. Setup more network logging and access to network tools to gain more visibility of the network. Setup Firewalls to prevent future incidents and enable syncookies.	Ongoing
Adjust Sensors, Alerts, and Log Collection		
10b. Add enterprise-wide detections to mitigate against adversary TTPs that were successfully executed.	Setup network logging for ELK stack.	Not Completed
10c. Identify and address operational “blind spots” to adequate coverage moving forward.	Perform Active Reconnaissance tests against network and address found weaknesses	Not Completed
10d. Continue to monitor the agency environment for evidence of persistent presence.	Review users and programs for evidence of a	Ongoing

	backdoor	
Finalize Reports		
10e. Provide post-incident updates as required by law and policy	Publish post-incident reports and actions that are still being taken and planned to be taken	Not Completed
10f. Publish post-incident report. Provide a step-by-step review of the entire incident and answer the Who, What, Where, why, and How questions.	Use previously gathered evidence to connect the dots of who(SSH Attacker), what(SSH service), where (Ubuntu and Debian machines), why(malicious attack to harm productivity), and how(SYN flood)	Not Completed
10g. Provide CISA with post-incident update with seven days of resolution or as directed by CISA in the Federal Incident Notification Guidelines	Provide the previously generated reports to the CISA	Not Completed
10h. Work with CISA to provide required artifacts, close the ticket, and/or take additional response action.	Provide any information the CISA requests and officially close the incident	Not Completed
Perform Hotwash		
10i. Conduct lessons learned analysis with all involved parties to assess existing security measures and the incident handling process recently experienced.	Decide on what can be taken away from this particular incident. In this incident for example, there was a severe lack of network monitoring services on the machines that would allow the attack to be captured. There was also no network integration into the ELK stack. This made detecting the	Not Completed

		attack much more difficult due to the lack of current instruments.	
10j.	Identify if agency IR processes were followed and if they were sufficient	Identify whether the attack was sufficiently mitigated, which in this case the attack could be mitigated by enabling syncookies and setting up a firewall to only allow certain IP addresses to connect to the machine	11/28/2023
10k.	Identify any policies and procedures in need of modification to prevent similar incidents from occurring.	Current procedures harm the possibility of preventing many harmful attacks. Procedures should allow for proper testing of services to see how an installation of a new service can affect the out-of-date system to help increase the security.	11/28/2023
10l.	Identify how information sharing with CISA and other stakeholders can be improved during IR.	Identify the current communication methods. Ask the CISA for a new way of communication if the current path is inefficient	Not Completed
10m.	Identify any gaps in incident responder training.	Determine if any members on the incident response team were not adequately prepared to deal with this current SYN flood incident. If there was any issue in the	Not Completed

	collection of evidence or the ability to determine ways to deter the attack then note where the responder was struggling and revise future training to make up for this issue.	
10n. Identify any unclear or undefined roles, responsibilities, interfaces, and authorities.	Determine if current roles defined in the CIRP aided in effectively identifying, containing, and responding to a synflood. If each member of the CIRT could effectively complete their job to respond to the situation, no change is needed.	11/28/2023
10o. Identify precursors or indicators that should be monitored to detect similar incidents.	Identify indicators that a synflood could be active in the future would include alerts from an IDS, or large sums of logs coming in on the same ports or from the same IP addresses disrupting a service.	11/28/2023
10p. Identify if agency infrastructure for defense was sufficient. If not, identify the gaps.	Determine if the synflood was caught in time by current tools in place on the system such that there was no negative effect on the company or its assets and did not disrupt company function.	11/28/2023

10q.	Identify if additional tools or resources are needed to improve detection and analysis and help mitigate future incidents.	If item 10p above is answered as insufficient, improve intrusion detection systems and retest proof of concept on a new and improved environment.	Not completed
10r.	Identify any deficiencies in the agency incident response planning process. If no deficiencies identified, identify how the agency intends to implement more rigor in its IR planning	Review CIRP and determine if the defined steps were necessary to appropriately identify, contain, and respond to the threat effectively and efficiently. If it is insufficient, modify the CIRP to adapt to an event such as a synflood.	11/28/2023
	Coordination with CISA		
11. Coordination with CISA			
11a.	Notify CISA with initial incident report within 1 hour after incident determination.	Email incident reports with evidence to cisa.gov	Not Completed
11b.	Receive incident tracking number and CISA National Cyber Incident Scoring System (NCISS) priority level from CISA.	Received after CISA response. Place this in CSEC bulletins such as E-ISAC for others to view.	Not Completed
11c.	Comply with additional reporting requirements for Major incidents as mandated by OMB and other federal policy.	Review reporting requirements and comply with additional reports. Work with government contacts to ensure legality requirements are met.	Not Completed
11d.	Provide incident updates until all eradication activities are complete.	Provide Incident Updates as they come up when	Not Completed

		investigating the threat impact to required parties and CISA.	
11e.	Report incident updates	Report incident updates to required parties as the investigation progresses.	Not Completed
11f.	Share relevant atomic and behavioral indicators and countermeasures with CISA throughout the IR process	Share our collected atomic and behavioral indicators with CISA.	Not Completed
11g.	Provide post-incident updates as directed by CISA.	Contact CISA with CIRP conclusion, mitigation tactics, and determined adversary tactics to provide to the public.	Not Completed
11h.	ICT service providers and contractors who operate systems on behalf of FCEB agencies must promptly report incidents to such agencies and directly report to CISA whenever they do so.	Not Applicable	Not Applicable

Incident 2

Step	Incident Response Procedure	Action Taken	Date Completed
	Detection & Analysis		
1. Declare Incident			
1a.	Perform initial categorization of incident	Looked at initial logs and service configurations to determine a service modification.	12/5/2023
2. Determine Investigation Scope			
2a.	Identify the type and extent of the incident	Defacement of the business. MITRE Attack ID T1491.002 External Defacement	12/5/2023
2b.	Assess operational or informational impact on organization's mission	Original Website is removed, replaced with Rick Astley's Never Gonna Give You Up	12/5/2023
3. Collect and Preserve Data			
3a.	Collect and preserve the data necessary for incident verification, categorization, prioritization, mitigation, reporting, attribution, and as potential evidence	Original index.html file content pre-attack saved, post-attack file content saved, root logins saved and reported, stat of index.html saved and reported.	12/5/2023
3b.	Log all evidence and note how the evidence was acquired, when it was acquired, and who acquired the evidence	Index.html changes acquired via stat /var/www/html/index.html, root logins acquired via cat /var/log/syslog and cat /var/log/auth.log	12/5/2023

4. Perform Technical Analysis		
4a. Develop a technical and contextual understanding of the incident	The attacker used the unknown root password to infiltrate the system. The attacker then defaced the company website to make a mockery of the company by making it link to Rick Astley's Never Gonna Give You Up.	12/5/2023
4b. Based on the analysis, form a hypothesis of what the adversary was attempting to access/accomplish	The attacker is trying to ruin the company's reputation. Doing this attack has no physical gain for the attacker and no immediate physical harm to the organization.	12/5/2023
4c. Update scope as investigation progresses and information evolves	This attack seems to be only on the Ubuntu machine. No logins have been noted to either the Windows machines or the Debian machine	12/5/2023
4d. Terminating Condition: Technical analysis is complete when the incident has been verified, the scope has been determined, the method(s) of persistent access to the network has/have been identified, the impact has been assessed, a hypothesis for the narrative of exploitation has been cultivated, and all stakeholders are proceeding with a common operating picture	The attacker likely used a compromised root account to modify the external facing web page. The compromised root account can be considered the method of persistence as the password cannot be changed unless it is known. The team needs to discover this password and	12/5/2023

	swiftly change it to prevent future attacks. The only notable impact was on the Ubuntu 16.04 machine.	
Correlate Events and Document Timeline		
4e. Analyze logs to correlate events and adversary activity	Syslog and login logs were analyzed, unrecognized root logins occurred December 1st at 3:30 p.m. server time.	12/5/2023
4f. Establish an incident timeline that records events, description of events, date-time group of occurrences, impacts, and data sources. Keep updated with all relevant findings.	The logins occurred at 3:30 p.m. server time on December 1st. The changes to the index.html file were shortly after these logins.	12/5/2023
Identify Anomalous Activity		
4g. Assess affected systems and networks for subtleties of adversary behavior which often may look legitimate	No changes were noticed outside of the website defacement. The root logins looked legitimate at first but after further evidence it was proven that these were used to attack the machine.	12/5/2023
4h. Identify deviations from established baseline activity - particularly important to identify attempts to leverage legitimate credentials and native capabilities and tools	The noted changes from the baseline were the index.html configuration and the amount of account logins. Root accounts did not login when conducting the baseline, showing this behavior to be	12/5/2023

	strange.	
Identify Root Cause and Enabling Conditions		
4i. Attempt to identify the root cause of the incident and collect threat information that can be used in further searches and inform subsequent response efforts	The likely cause of this incident is the compromised root account. Root has write access to the entire system and allowed the attacker to change whatever file they would have liked.	12/5/2023
4j. Identify and document the conditions that enabled the adversary to access and operate within the environment.	The Root password was unknown and not disclosed to the current blue team. The team also did not have permission to change the password to something more secure.	12/5/2023
4k. Assess networks and systems for changes that may have been made to either evade defenses or facilitate persistent access	The current root password is unknown. It is unclear whether the password was changed or not to continue persistence.	12/5/2023
4l. Identify attack vectors. This includes how the adversary is accessing the environment.	A compromised root account password was used to access the environment.	12/5/2023
4m. Assess access (depth and breadth). This includes all compromised systems, users, services, and networks	The attacker had full access to the system. With root access, the attacker could have changed any service or file they would have liked. This seems to only extend to the Ubuntu machine.	12/5/2023

Gather Incident Indicators		
4n. Review available CTI for precedent of similar activity	Search for previous or current ongoing defacement attacks against server services.	Not currently completed
4o. Analyze adversary tools	Adversary seems to be using several machines or spoofed IPs to remotely login to the machine.	12/5/2023
4p. Identify and document the indicators that can be used for correlative analysis on the network	Syslog and auth.log can be used to report the IPs of machines connecting to the machine.	12/5/2023
4q. Share extracted threat information with internal response teams and CISA	Send CISA report on the login log information along with the IPs of the machines and the changes made to the Index.html file	Not Completed
Analyze for Common Adversary TTPs		
4r. Identify initial access techniques	The attack exploited a compromised root account to gain access. MITRE ID 1078 Valid Accounts	12/5/2023
4s. Identify the techniques used by the adversary to achieve code execution	The attacker used a compromised root account to modify files. MITRE ID 1078 Valid Accounts	12/5/2023
4t. Assess compromised hosts to identify persistence mechanisms	The attacker knows the current root password and can login until the password is changed.	12/5/2023
4u. Identify lateral movement techniques	The attacker did not perform lateral	12/5/2023

	movement, seemingly the only machine that was compromised was the Ubuntu machine.	
4v. Identify the adversary's level of credential access and/or privilege escalation	The attacker has access to the root account on the Ubuntu machine.	12/5/2023
4w. Identify the method of remote access, credentials used to authenticate, and level of privilege. If access is by legitimate but compromised application, identify the method	The attacker used the root account to authenticate and gain root access.	12/5/2023
4x. Identify the mechanism used for data exfiltration	There is no evidence to show data exfiltration, only modification.	12/5/2023
Validate and Refine Investigation Scope		
4y. Identify new potentially impacted systems, devices, and associated accounts	Seemingly only the Ubuntu machine was impacted.	12/5/2023
4z. Feed new IOCs and TTPs into detection tools	Implement password changing and website content backups.	Not Completed
4aa. Continue to update the scope and communicate the updated scope to all stakeholders to ensure a common operating picture	Send information to stakeholders as it is discovered as well as document any new findings.	Not Completed
5. Third-Party Analysis Support (if needed)		
5a. Identify if third-party analysis support is needed for incident investigation or response.	Not required	Not Completed
5b. Invoke Federal Network Authorization to enable CISA incident response and hunt assistance	Not required	Not Completed
5c. Coordinate and facilitate access if incorporating third-party analysis support into response efforts.	Not required	Not Completed
5d. Coordinate response activities with agency service providers for systems hosted outside of the agency.	Not required	Not Completed

6. Adjust Tools		
6a. Tune tools to slow the pace of advance and decrease dwell time by incorporating IOCs to protect/detect specific activity	Implement stronger password policies and network logging to catch any attempts at logins.	Not Completed
6b. Introduce higher-fidelity modifications to tools. Tune tools to focus on tactics that must be used by the adversary to obtain operational objectives	Setup network logs for the ELK stack to monitor unusual attempted logins from unknown IPs.	Not Completed
Containment		
7. Contain Activity		
7a. Determine appropriate containment strategy	Change root passwords and admin passwords to comply with stronger requirements. Stop the apache2 service.	Not Completed
7b. System Backup to preserve evidence and continue investigation	Backup the affected systems	Not Completed
7c. Coordinate with law enforcement to collect and preserve evidence prior to eradication, if applicable	Notify law enforcement and collaborate on what evidence to save	Not Completed
7d. Isolate affected systems and networks	Ensure firewalls are blocking unnecessary access to Windows machines and linux machines	Not Completed
7e. Close specific ports and mail servers. Update firewall filtering.	Install and enable ufw on Ubuntu. Stop apache2 until the service is brought back up to its original standards. Do not close other ports as the ports are needed for normal access.	Not Completed.

7f	Change system admin passwords, rotate private keys, and service/application account secrets where compromise is suspected revoke privileged access	Change admin passwords and rotate private keys, shutdown apache2 service	Not Completed
7g.	Perform blocking (and logging) of unauthorized accesses, malware sources, and egress traffic to known attacker Internet Protocol (IP) addresses.	Setup access control to SSH from only known IPs, especially for the root account.	Not Completed
7h.	Prevent Domain Name Server (DNS) resolution of known attacker domain names	Disable DNS services of the Ubuntu machines until registered domain names can be confirmed	Not Completed
7i.	Prevent compromised systems from connecting to other systems on the network	Block access from the Ubuntu machine using the Windows firewall and Debian UFW on the remaining servers	Not Completed
7j.	Advanced SOCs may direct adversaries to sandbox to monitor activity, gather additional evidence and identify TTPs.	Does not apply in this situation.	Not Completed
7k.	Monitor for signs of threat actor response to containment activities	Continually monitor root logins and attempted logins, note any continual changes throughout the system.	Not Completed
7l.	Report updated timeline and findings to CISA	Send new login information to the CISA along with updates on any attempted logins.	Not Completed
7m.	If new signs of compromise are found, return to technical analysis to re-scope the incident	Check through the new evidence to see if any new compromises are discovered. If none, then continue. If there are new compromises, then	Not Completed

	return to step 4.	
7n **Terminating Condition:** Upon successful containment (i.e., no new signs compromise), preserve evidence for reference and law enforcement investigation (if applicable), adjust detection tools, and move to eradication.	Backup new login logs, setup network auditing for ELK stack to monitor attempted logins.	Not Completed
Eradication & Recovery		
8. Execute Eradication Plan		
8a. Develop a well-coordinated eradication plan that considers scenarios for threat actor use of alternative attack vectors and multiple persistence mechanics	Change the root password, create a list of all spoofed IP addresses, setup access control lists for SSH to only known IP addresses	Not completed
8b. Provide Incident Status to CISA until all eradication activities are complete	Report the incident to report@cisa.gov with a status of the current incident and proof of tactic used.	Not completed
8c. Remove artifacts of the incident from affected systems, networks, etc.	Return the index.html file to its original configuration.	Not completed
8d. Reimage affected systems from clean backups (i.e., 'gold' sources).	This item of eradication is not necessary for this defacement attack.	Not completed
8e. Rebuild hardware (if rootkits involved).	This attack seemingly did not involve rootkits.	Not completed
8f. Scan for malware to ensure removal of malicious code	This attack seemingly did not involve malware.	Not completed
8g. Monitor closely for signs of threat actor response to eradication activities	Frequently check syslog logs and auth.logs for attempted root logins. Monitor any new processes or service changes on	Not completed

	the system.	
8h. Allow adequate time to ensure all systems are clear of threat actor persistence mechanisms (such as backdoors) since adversaries often use more than one mechanism.	Return the index.html service configuration to its original state. Do not re-enable until no new processes have been confirmed over time and no new root logins have taken place.	Not Completed
8i. Update the timeline to incorporate all pertinent events from this step.	Append documentation with attacker tactics, preventative measures, and CIRP completed tasks.	Not completed
8j. Complete all actions for eradication	Complete steps 8a-8h for eradication.	Not completed
8k. Continue with detection and analysis activities after executing the eradication plan to monitor for any signs of adversary re-entry or use of new access methods.	Continue monitoring Syslog and auth.log log files. Install IDS for further detection of unusual account logins.	Not completed
8l. If new adversary activity is discovered at the completion of the eradication step, contain the new activity and return to Technical Analysis until the true scope of the compromise and infection vectors are identified.	If a new login is discovered or if a service has changed again, redo the technical analysis and assess which steps of containment needs to be reevaluated.	Not completed
8m. If eradication is successful, move to Recovery	If no new logins are discovered and no services have been changed, move on to recovery steps #9 below.	Not completed
9. Recovery		
9a. Restore agency systems to operational use:	Re-enable the	Not completed

	recovering mission/business data	apache2 service and ensure that the service is uninterrupted.	
9b.	Revert all changes made during incident	Re-enable DNS services that were temporarily shut down and any specific ports closed down in the technical section.	Not completed
9c.	Reset passwords on compromised accounts	Reset passwords on all admin accounts, root account, and any account used during the duration of the attack to lock the adversary out.	Not completed
9d.	Implement multi-factor authentication for all access methods	Implement mandatory multi-factor authentication via Duo Mobile for all users.	Not completed
9e.	Install updates and patches	Use sudo apt update && sudo apt upgrade to update the non-16.04 Ubuntu machines. Do not update the Debian 9 and Ubuntu 16.04 machines.	Not completed
9f.	Tighten perimeter security and zero trust access rules	Implement mandatory access control for all services and enable very strict access control lists for any user with sudo access, including root.	Not completed
9g.	Test systems thoroughly to validate systems are operating normally before bringing back online in	Test the website configuration to	Not completed

	production networks.	ensure that it is consistent with the pre-attack version. Ensure that the new root password cannot be brute forced through dictionary attacks.	
9h.	Consider emulating adversarial TTPs to verify countermeasures are effective	Install a Kali Linux VM and launch a brute force attack against the root account. Verify that the logins are being logged.	Not completed
9i.	Review all relevant CTI to ensure situational awareness of the threat actor activity	Research Microsoft Threat Intel and other trusted sources to verify all tactics are recognized for account compromises.	Not completed
9j.	Update incident timeline to incorporate all pertinent events from recovery step.	Append current CIRP with completed recovery measures to restore full functionality to the services.	Not completed
9k.	Complete all actions for recovery.	Complete steps 9a-j for recovery steps to be complete.	Not completed
	Post-Incident Activities		
10. Post-Incident Activities			
10a.	Document the incident, inform agency leadership, harden the environment to prevent similar incidents, and apply lessons learned to improve the handling of future incidents.	Documented incident, informed leadership, and in the process of applying lessons learned from incident. Setup robust password requirements and changed current	Ongoing

	passwords to meet the new requirements. Setup access control lists for root logins and for any account with the ability to sudo.	
Adjust Sensors, Alerts, and Log Collection		
10b. Add enterprise-wide detections to mitigate against adversary TTPs that were successfully executed.	Setup login monitoring for the ELK stack. Setup alerts to notify when the root account is logged into.	Not Completed
10c. Identify and address operational “blind spots” to adequate coverage moving forward.	Perform Active Reconnaissance tests against network and address found weaknesses	Not Completed
10d. Continue to monitor the agency environment for evidence of persistent presence.	Review users and programs for evidence of a backdoor	Ongoing
Finalize Reports		
10e. Provide post-incident updates as required by law and policy	Publish post-incident reports and actions that are still being taken and planned to be taken	Not Completed
10f. Publish post-incident report. Provide a step-by-step review of the entire incident and answer the Who, What, Where, why, and How questions.	Use previously gathered evidence to connect the dots of who(root login user), what(root account and apache2 service), where (Ubuntu 16.04), why(malicious attack to deface the company), and how(changing index.html to Rick Astley’s Never	Not Completed

		Gonna Give You Up)	
10g.	Provide CISA with post-incident update with seven days of resolution or as directed by CISA in the Federal Incident Notification Guidelines	Provide the previously generated reports to the CISA	Not Completed
10h.	Work with CISA to provide required artifacts, close the ticket, and/or take additional response action.	Provide any information the CISA requests and officially close the incident	Not Completed
Perform Hotwash			
10i.	Conduct lessons learned analysis with all involved parties to assess existing security measures and the incident handling process recently experienced.	Decide on what can be taken away from this particular incident. In this incident for example, the root password was unknown. The attacker used this unknown password to gain access to the system and deface the company's website. Any account with the ability to modify the filesystem should either be disabled or be closely monitored. These accounts should also have robust passwords to prevent brute-force attacks from finding weaker passwords.	Not Completed
10j.	Identify if agency IR processes were followed and if they were sufficient	Identify whether the attack was sufficiently mitigated, which in this case the attack could be mitigated by changing the root password and any	12/5/2023

		passwords that give access to write permissions for the file system.	
10k.	Identify any policies and procedures in need of modification to prevent similar incidents from occurring.	Current procedures harm the possibility of preventing many harmful attacks. Procedures should allow for proper testing of services to see how an installation of a new service can affect the out-of-date system to help increase the security. Password Policies should also be overhauled to prevent easy access to systems.	12/5/2023
10l.	Identify how information sharing with CISA and other stakeholders can be improved during IR.	Identify the current communication methods. Ask the CISA for a new way of communication if the current path is inefficient	Not Completed
10m.	Identify any gaps in incident responder training.	Determine if any members on the incident response team were not adequately prepared to deal with this current account compromise incident. If there was any issue in the collection of evidence or the ability to determine ways to deter the attack then note where the responder was struggling and revise future training to make up for this	Not Completed

	issue.	
10n. Identify any unclear or undefined roles, responsibilities, interfaces, and authorities.	Determine if current roles defined in the CIRP aided in effectively identifying, containing, and responding to an attack from a root login. If each member of the CIRT could effectively complete their job to respond to the situation, no change is needed.	12/5/2023
10o. Identify precursors or indicators that should be monitored to detect similar incidents.	Identify indicators that a compromised account could be active in the future would include login alerts from an IDS, or large amounts of attempted logins from unknown IPs.	12/5/2023
10p. Identify if agency infrastructure for defense was sufficient. If not, identify the gaps.	Determine if the compromised account was caught in time by current tools in place on the system such that there was no negative effect on the company or its assets and did not disrupt company function. The account was not caught before the website could be defaced. The service had to be brought offline to prevent possible reputation harm. New alerts to notify of logins should be put in	12/5/2023

	place.	
10q. Identify if additional tools or resources are needed to improve detection and analysis and help mitigate future incidents.	If item 10p above is answered as insufficient, improve intrusion detection systems and retest proof of concept on a new and improved environment.	Not completed
10r. Identify any deficiencies in the agency incident response planning process. If no deficiencies identified, identify how the agency intends to implement more rigor in its IR planning	Review CIRP and determine if the defined steps were necessary to appropriately identify, contain, and respond to the threat effectively and efficiently. If it is insufficient, modify the CIRP to adapt to an event..	12/5/2023
Coordination with CISA		
11. Coordination with CISA		
11a. Notify CISA with initial incident report within 1 hour after incident determination.	Email incident reports with evidence to cisa.gov	Not Completed
11b. Receive incident tracking number and CISA National Cyber Incident Scoring System (NCISS) priority level from CISA.	Received after CISA response. Place this in CSEC bulletins such as E-ISAC for others to view.	Not Completed
11c. Comply with additional reporting requirements for Major incidents as mandated by OMB and other federal policy.	Review reporting requirements and comply with additional reports. Work with government contacts to ensure legality requirements are met.	Not Completed
11d. Provide incident updates until all eradication activities are complete.	Provide Incident Updates as they	Not Completed

		come up when investigating the threat impact to required parties and CISA.	
11e.	Report incident updates	Report incident updates to required parties as the investigation progresses.	Not Completed
11f.	Share relevant atomic and behavioral indicators and countermeasures with CISA throughout the IR process	Share our collected atomic and behavioral indicators with CISA.	Not Completed
11g.	Provide post-incident updates as directed by CISA.	Contact CISA with CIRP conclusion, mitigation tactics, and determined adversary tactics to provide to the public.	Not Completed
11h.	ICT service providers and contractors who operate systems on behalf of FCEB agencies must promptly report incidents to such agencies and directly report to CISA whenever they do so.	Not Applicable	Not Applicable

Identify

Revise and Define Baseline Procedures

Baselining all the systems in the environment can prove to be the most useful step in creating and carrying out an incident response plan. There will always be an unknown area of declaring some intrusion as an incident or as a worker working outside of normal channels unless there is a clear comparison to draw to. Without this baseline, risk cannot be properly identified and documented. This comparison is the baseline that should document every part of a system that can be modified to ensure that there are no incidents that can cause future issues. This is a step that cannot be ignored in any incident response plan, especially when working with old vulnerable machines that can be accessed and manipulated through many different attack vectors.

When baselining, the baseline should start as general as possible. Document all files in all folders and save copies of the outputs when checking the files. Hashes should also be made of both the copies and the important files to easily check if there has been a change to the document when an incident occurs. Also save the timestamps of when the files were last modified and the user permissions on each document. After documenting the base filesystem, document the system settings, such as networking, DNS, and date. All of these system services work in unison to provide full operation to the system. If any of these services become changed or corrupted it could affect the system user services that are running.

After doing general baselining the system services should be baselined. Any of these services could be modified and used to affect other machines, making these services unbelievably important to baseline. Ensuring these services are running as normal should be top priority in responding to an incident. Check all configurations for any service running on the machines. Create copies of these configurations and hash both the copy and the original configuration. This will allow for the incident response team to easily replace the configuration if the service was modified through unauthorized means. Copies of the logs for these services should also be kept. This helps to create an idea of the normal traffic that utilizes the service. Without the copy, a team wouldn't be able to tell normal traffic from attacker traffic.

All system users should be documented and their activity should be noted as part of the baseline. Any user on a vulnerable system could gain access to the system. It is of the utmost importance to ensure that these users are monitored and any accounts that are not used are disabled. By disabling unused users the team can eliminate any unknown logins by accounts that have been forgotten. Administrator accounts should be documented and passwords should be rotated consistently. The frequency of these rotations should be baselined so that in the case of an incident occurring the response team can check to ensure that no administrator passwords were prematurely rotated in an attempt to lock out access to that account.

Computer resource management should then be baselined to determine the normal amount of resources in use for the system. Attackers could be performing an attack against the network in which the easiest way to discover this attack is to identify the difference in normal

network bandwidth against current network bandwidth. This should be performed on all of the resources available to the system. This includes RAM, network bandwidth, CPU usage, GPU usage, and storage usage. These baselines should be performed again anytime a new service is added to the system or if there are upgrades to the machine. New services can add to the CPU load and increase the usage, same with the other resources mentioned above.

Baselining is not a step that should be taken lightly. A proper baseline can mean the difference between a hardened system or a system that is primed to deliver malware that can disrupt and bankrupt a company. When our team carried out our baselining, we did not properly fully baseline the Windows operating systems. If an incident arose on those machines, the team would not be properly prepared to deal with it. The linux systems, however, were fully baselined and the team was prepared for the incidents that did arise against these systems. Any baselining carried out in the future will properly be carried out to ensure that all facets of a system are documented and our team will be properly prepared for any risk/

Detection & Reporting

Instrumentation Updates

The prior incidents mentioned above made it clear that updates must be made to some of the detection services. There were several issues that arose when attempting to respond to these incidents. This was not exclusive to one machine or service but across the entire network.

The first service that experienced issues was the SIEM. The SIEM initially had storage issues in which the machine ran out of space and did not collect logs relating to the initial attack of incident 1. This was remedied by giving the machine more space. The SIEM then had an issue of crashing any time a log was uploaded. This was not properly remedied in the short amount of time the incidents happened. In the future this issue must be remedied as the SIEM is an important tool for the detection process. There was also the issue of the SIEM not properly collecting all information due to the lack of beats installed on clients. For future responses, more beats should be installed on all machines to ensure the SIEM contains the proper information for incident response.

The SIEM not working as intended was a massive hindrance to the team as it was supposed to enable easy filtering of logs across all machines. SIEMs are an important tool for the initial detection and the continued monitoring of incidents. The log aggregation that a SIEM provides can prevent hours of unnecessary work of filtering through logs to find every line of evidence available to the team.

The OSSEC IDS also had many issues when it was used to respond to incidents. The boundaries were not properly set when installed so it returned many false positives when normal activity was happening in the environment. This created more work to sift through all the false positives left by the IDS. In future implementations, proper boundaries should be set to ensure prevention of extra work on unnecessary aspects of incident response.

The one service that functioned as intended was the honeypot. There were no attacks against the systems file transfer services but our team is certain that the honeypot is adequate in its deception strategy. Both of the vulnerable linux machines run FTP which can be exploited for file extraction. Our team set up the honeypot to attempt to capture the attacker if they used FTP for data extraction. In future implementations, the only possible change the team may carry out is to include more services like SSH and TFTP.

Another service that worked as intended were the network traffic monitors available on every system. TCPdump was set up on the two vulnerable Linux machines and Wireshark was installed onto the vulnerable Windows machine. This provided the team with valuable insight into the traffic that was crossing the machines and onto the network. This also helped to detect the syn flood incident as the incident did not fully deny the service of SSH. Without these services, this incident would have gone fully undetected and the lack of syncookies on the machines would have never been found.

Analysis

Jumpbag and checklist

In today's interconnected digital landscape, organizations face a constant threat from cyberattacks and security incidents that can disrupt operations, compromise sensitive data, and damage their reputation. A Computer Incident Response Jump Bag is a crucial tool for cybersecurity professionals and incident responders to effectively address and mitigate these threats. This executive summary outlines the pressing need for organizations to invest in and equip their teams with these specialized kits.

Cyberattacks are becoming increasingly sophisticated and frequent, targeting organizations of all sizes and industries. From ransomware attacks to data breaches and advanced persistent threats, the potential impact on an organization's bottom line and reputation is substantial. To respond effectively to these threats, organizations must have a robust incident response plan in place, supported by skilled professionals and the necessary tools.

A Computer Incident Response Jump Bag is a pre-packed collection of essential tools, hardware, and software used by cybersecurity and incident response teams during the initial stages of an incident. These bags are designed to facilitate rapid response and help teams assess, contain, and mitigate the impact of a cyber incident.

The current necessary items in a cybersecurity professional’s go bag are outlined below in the “Jump Bag Budget” table. Keep in mind that this is the price of a single jump bag, and will need to be repeated for the number of incident responders that are present.

Hardware Jump Bag Budget

Item	**Price**
Locked locker with laptops	$200
Dell Latitude 7440 2GB RAM, 1TB NVME Laptop	$2,000
Laptop Charger	Included with laptop purchase
Corsair 32 GB 4800 MHz DDR5 Laptop RAM	$90
Cable kit	$100
500 ft. Cat 6 Cable	$140
Cable Ties	$2
Scissors	$2

Cell Phone with hotspot capabilities	$150
Notebook	$2
Pencils	$2
Pens	$3
Notebooks (Bulk)	$50
4 TB External Barracuda hard drives	$30
Weibetech Write blocker	$200
Kingston 256 GB USB Drives	$50
Pliers	$15
Static bags	$5
Documentation	Free
Copy of CIRP	Free
Dell USB Hub	$50
Cisco Router	$100
Headphones with microphone	$50
Flashlight	$10
Copy of credentials	Free
Emergency Medical Kit	$30
Extra pack of clothes	Brought personally
Toiletries	Brought personally
CyberPower 1500 VA Battery Back-Up System UPS	$230
Predator 3500 Watt Inverter Generator	$900
Lenovo Tab M8 8” Tablet - Cortex A53 Quad-core CPU 3 GB RAM 32 GB Storage Android 12	$140
Fire Extinguisher	$70

Cobra PX650 Professional Walkie Talkies 6 Pack	$350
Syntech USB C to USB Adapter Pack	$9
Ruaeoda USB to USB Cable 3 ft	$6
4 PowerBear 4K HDMI Cable 10 ft	$36
4 Dell 24 Monitor - SE2422H	$400
C2G 6FT Replacement AC Power Cord 10 Pack	$40
Multi Charging Cable 3.5A 5 Pack	$70
4 Extra Geforce RTX 3060 graphics cards	$1120
4 2-Packs Extra Corsair Vengeance 16GB DDR4 RAM	$180
4 Extra Intel i7 9700K Desktop Processor 8 Cores 3.6 GHz	$1120
4 Extra ASUS LGA 1150 motherboards	$280
4 Extra EVGA power supplies	$520
4 Extra EVGA PSU cables	$104
4 Extra Corsair case fans	$300
4 Extra 500GB WD Blue SSDs	$150
4 Rii RK907 Ultra-Slim Compact USB Wired Keyboard	$40
4 Logitech B100 Corded Mouse	$32
Total Hardware	$9,428

Software Jump Bag Budget

Package	**Price**
Kali Linux	Free
Ubuntu Linux	Free
Debian Linux	Free
Mint Linux	Free

Wireshark	Free
Network Mapper (nmap)	Free
FTK Imager	$3000
Autopsy Forensics	Free
WinHex Hex Editor	Free
MS Office	Included in company plan
MS Excel	Included in company plan
MS Word	Included in company plan
MS Teams	Included in company plan
IPS tool access	Included in company plan
IDS tool access	Included in company plan
EDR tool access	Included in company plan
NDR tool access	Included in company plan
SIEM tool access	Included in company plan
Cloud storage access	Included in company plan
NetSpot	Free
OpenVAS	Free
Security Onion	Free
Windows Powershell	Free
Total Software	$3000

Total Hardware Budget: $9,428

Total Software Budget: $3,000

Total Budget: $12,401

Post Mortem Clean Up

Plan Revisions

No plan is ever perfect. After responding to incidents, it is clear that there are weaknesses in this plan. One such weakness is its lack of procedures when responding to a more common incident. One such incident was carried out against our machines in the form of a denial of service attack against the SSH of the Debian and Ubuntu machines. Due to the minor nature of this attack, members of the response team were unsure how to actually respond to the incident outside of disconnecting the network of the machines. In future revisions incidents of all sizes should have procedures that guide the response team on how to respond.

Another weakness noticed within the original plan was the limited amount of baselining. Baselining is considered one of the most important parts of the preparation process as it identifies exactly what assets need protection and what exact states the assets are in. Without a proper baseline then a response team can never be sure whether their machine was attacked or not. This current plan revises the way baselining is carried out. If an incident ever occurs in which a baseline does not provide a clear image of what the asset looked like before the incident then the baseline should be revised. This should be an ongoing process until a baseline is robust enough to handle any incident.

Secure Provisioning

The current implementation of systems is not sufficient enough to provide an environment free from constant attacks. The hardware and software being used must be updated to ensure strong defenses against attackers. The systems currently in place however must always be up which makes provisioning new systems difficult. To properly provision new secure systems the team must create a separate environment for testing. With this new environment the team can create similar devices to the older systems and test the services to ensure that all services function the same way as the older systems.

In this new environment tests can be run against the newer systems to ensure that they are hardened against all forms of attacks. Attacks should be run against these systems to emulate incidents. After each attack the system should be modified and hardened to prevent the attack. Once all possible known attacks have been emulated and the systems have been hardened against them then they should be prepared to replace the older systems. Before connecting the machines to the network their settings should be set to the same values as the machines they are replacing such that their IPs, DNS, and port settings are identical. The old systems should then be disconnected from the environment and the new systems should be connected to the environment. This should create a relatively seamless transition to new hardware.

Lessons Learned

The whole process of creating the plan and systems was a learning process for the teams. Due to the fragile nature of the machines inherited, there were many learning opportunities for all members of the incident response team. The first lesson that was learned stemmed from risk register generation. As the risk register was being created, a sense of likelihood and impact became more apparent and it was necessary to go back through the risks already addressed and reevaluate the decision that was made. This created a more effective and accurate risk register for the CIRP as there was more experience behind the ratings of all fields.

The next lesson that was learned pertained to the baseline portion of the CIRP. When creating a baseline for your systems, it is important to remember that each operating system and UNIX distribution have different commands or methods to obtain the information required by a baseline. For example, a PowerShell command that works in the current Windows Server 2022 might not work for an old Windows Server 2008 system. When creating a list of commands or script for baselining, it is imperative to be detailed with baseline instructions. Failure to do this may lead to inaccurate information and the creation of a false positive incident or a waste of time trying to search for the right commands.

The last lesson that was learned was efficiency in incident detection and cause. Throughout the last month, there were multiple attacks that were supposed to happen to the virtual machines, but did not actually occur. This led the team to start investigations when there was no actual threat that had compromised the systems. A false positive is a very realistic event that can occur in an incident response environment. This helped in guidance for realistic incident response practice as well as gave a deeper understanding of the environments in the lab. This in turn made it easier to find the actual threat when the attack did happen due to the background knowledge that the team possessed on the current systems. All of the lessons learned throughout the creation of the final CIRP has helped the team learn the inner workings of a functioning CIRP much better.