

**CAPSTONE**

Mitchell Tyrer, Richard Brazzle, Matthew Dintrone, Matthew Brossman

SecureSet Academy

CORE: Capstone Project

Instructor: Bryan Frier

October 21, 2021

## **Executive Summary**

This capstone project was to test what we had learned in the CORE Cyber Security Engineering Program into a simulated real-world scenario. In this scenario, we were the newly hired Security Operations Center for the ACME ANVIL’s Company. Our task was to analyze a recent security breach, the network, the systems, and create recommendations to help secure the entire company against a future incident. This document is a compilation of all the individual documentation we created for the capstone project. Each document was in response to a simulated directive given to us by our Chief Information Security Officer (CISO). These documents are what we built our entire presentations from.

## **The Scenario**

ACME Anvil suffered a major data breach several weeks ago. Unfortunately, this is was due to the negligence of their former CISO and the third-party Security team they had been hiring. It would appear that they had become complacent and thought their network was untouchable. This breach’s fallout led to the hiring of a new CISO - Wile E. Coyote. Mr. Coyote in turn hired on a brand new internal Security Operations Center. This new SOC will be tasked with the investigation and overall installation of new security practices to help mitigate and properly handle a future security event.

Consultant Onboarding Documents

**Memorandum of Understanding**

Between

Acme Company

and

Road Runner Consulting Group

This Memorandum of Understanding (MOU) sets the terms and understanding between the Acme Company and the Road Runner Consulting Group before starting consultation.

**Background**

Three weeks ago, a data breach was found by ACME’s SOC, outsource to Cybersecurity Stooges. A few days after the reported breach, the former CISO of ACME Company quit. ACME responded quickly and installed a new CISO, named Wiley E Coyote. Coyote has established a plan to remedy the situation by firing the Cybersecurity Stooges and utilizing an in-house SOC. ACME Company got in touch with Road Runner Consulting around the same time.

**Purpose**

This MOU will establish the boundaries of ACME Company Employees, and the line of communication that is expected. ACME Company Employees are expected to have a clear communication strategy both within their team and with their Director of IT. If internal troubleshooting does not glean the solution desired, ACME Company Employees are able to reach out for help from Road Runner Consulting Group, with costs described in funding.

**Funding**

The purpose of Road Runner Consulting Group, and the costs associated, will be outlined herein. Road Runner Consulting Group is designed as a last case troubleshooting resource. This is the case due to the number of clients. Road Runner Consulting Group came to an agreement with ACME CISO Coyote, outlining that they would be employed by ACME on a per diem basis with each consultation costing a “flag”. This means that the more times ACME Company Employees engage in consulting with Road Runner Consulting Group, the lower the final “flag” score the company will receive. Both parties, ACME Company, and Road Runner Consulting Group are responsible for documenting these interactions.

**Reporting**

ACME Company and Road Runner Consulting Group are BOTH responsible for documenting the consulting engagements. Any lack of documentation, or over documentation of events by both parties amounts to fraud.

**Duration**

This MOU is at will and may be modified by mutual consent of authorized officials from ACME Corporation and Road Runner Corporation. This MOU shall become effective upon signature by the authorized officials from the ACME Corporation and the Road Runner Consulting Group and will remain in effect until modified or terminated by any one of the partners by mutual consent. In the absence of mutual agreement by the authorized officials from (list partners), this MOU shall end three weeks hence.

**Contact Information**

Acme Corporation

Wiley E Coyote

CISO

11100 Commerce Center Ave, Colorado Springs, CO

719-989-8989



\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Date: **Today**\_\_\_\_\_\_\_\_\_\_\_

(Partner signature)

Wiley E Coyote, ACME Corporation, CISO

**Road Runner Consulting Group**:

Tweed E. Byrde

CISO

1212 Brighton Blvd, Denver, CO

720-909-0909

*Mitchell Tyrer 10/12/2021*

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Date: \_\_\_\_\_\_\_\_\_\_\_\_\_

(Partner Signature 1)

*Matthew Dintrone 10/12/2021*

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Date: \_\_\_\_\_\_\_\_\_\_\_\_\_

(Partner Signature 2)

*Matthew Brossman 10/12/2021*

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Date: \_\_\_\_\_\_\_\_\_\_\_\_\_

(Partner Signature 3)

*Richard Brazzle 10/12/2021*

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Date: \_\_\_\_\_\_\_\_\_\_\_\_\_

(Partner Signature 4)

Icon

Description automatically generated

**ACME COMPANY**

Marvin the Martian

Security Operations

Director of IT Mitchell “Goodyear” Tyrer

Security Engineer Richard “Razzle” Brazzle

Security Engineer Matt “256” Dintrone

Security Engineer Matt “128” Brossman

ANALYSIS OF THE BREACH

**Analysis of Brocade Switch Logs**

Looking at the provided logs from the security breach three weeks ago, we can see some patterns of the attack that could help us harden our systems and network. This is a brief analysis of the logs produced from ACME’s Brocade Switch and what these could mean for possible attack vectors of the malicious actors. This will allow us to implement some recommendations to help prevent similar attacks in the future using these vulnerabilities

### **Observations**

After examining the brocade logs, it is apparent that the log messages may have become corrupted. This may be due to a system error, or it is possible that logs were intentionally corrupted to cover the attacker’s digital footprint after the data breach. These log messages are not in a human-readable format and do not produce any usable data when converted to other formats. The remaining fields of the log file that are readable do not provide a clear picture of events logged other than the date and time of logged events. Because of this, it is impossible to discern what is occurring or to correlate this log information from the logs provided in our IDS and Firewall.

### **Recommendations**

Due to the apparent corruption of the log messages, and the insufficient data shown in what we can read, it is impossible to offer any recommendations for security controls. This can be revisited should the log messages become human-readable.

**Analysis of Intrusion Detection System (IDS)Logs**

Looking at the provided logs from the security breach three weeks ago, we can see some patterns of the attack that could help us harden our systems and network. This is a brief analysis of the logs produced from ACME’s Intrusion Detection System (IDS) and what these could mean for possible attack vectors of the malicious actors. This will allow us to implement some recommendations to help prevent similar attacks in the future using these vulnerabilities

**Observations**

The first thing to take notice of in the IDS logs for ACME is the detection of spyware activity. The log indicates significant spyware activity that must be remediated to bring the system back to a safe baseline.

There is also evidence of a multi-day long port scan or ping sweep using ICMP packets on port 53 (DNS). Port scans can be used to identify open ports and services on a system and can be used by an attacker to identify vulnerabilities on a system or network.

Other log messages that appear are Invalid Transport Field; this message likely appears when there is an invalid transport number in which the source or destination port number for a protocol is zero. This could potentially be an attempt for malware to connect to a command and control (C2) server, although it was unsuccessful. There are also failed IPv6 message failure entries on the log. This could be connected to malware attempting to connect to other systems as well, though that is unknown.

Other notable events include that two successful outbound SSH connections may have been used for data exfiltration, and there were two FTP connections. One was external and the other was outbound.

### 

### **Recommendations**

* Implementing spyware/malware detection and removal software (such as malware bytes) is recommended to remove any artifacts of the spyware and repair altered files and settings.
* Disabling outbound ICMP traffic is recommended to limit external visibility if such a scan is attempted.
* If FTP is necessary for business operations, in the future it is recommended to use a secure version of FTP (either SFTP or FTPS).

## 

## **Analysis of Untangle Firewall Logs**

Looking at the provided logs from the security breach three weeks ago, we can see some patterns of the attack that could help us harden our systems and network. This is a brief analysis of the logs produced from ACME’s Untangle Firewall and what these could mean for possible attack vectors of the malicious actors. This will allow us to implement some recommendations to help prevent similar attacks in the future using these vulnerabilities.

### **Observations**

#### Header Injection and XSS

Based on the traffic captured by the Firewall, it appears there were several exploits on an Apache Server in our network. On several occasions, there is evidence of a Header Injection, an attack in which a malicious user supplies data that is copied into a response header in an unsafe way. Because they can inject newline characters into the header, they can create new HTTP headers and even break out of the headers into the message body. This vulnerability can allow for cross-site scripting attacks to occur because the attacker can construct a request that causes arbitrary Javascript to appear in the response body. Cross-Site Scripting (XSS) Attacks are also noted in the logs of the Firewall, so this seemed to be one of the many attack vectors those responsible for ACME’s data breach may have used.

XSS was also seen on the Microsoft Exchange OWA, the alternative to Microsoft Outlook that allows users to access their emails and public folders through a web browser. This is due to improper validation of user input, which could allow users to inject code into the server hosting the Internet Information Server and affect other users accessing the service.

#### Directory Traversal

The web server also seems to be vulnerable to directory traversal attacks. This vulnerability allows unauthorized users to traverse through the server via the URL to other areas of the file system. Once there, the attacker could gain access to sensitive files on the server or could upload and execute malicious code on the system hosting this webserver

#### Buffer Overflow

The logs also indicate that there was also a buffer overflow attack due to a known vulnerability in the SENKAS Kolibri Web Server 2.0. This vulnerability is due to a boundary error when handling a GET request, as noted in the logs. A buffer overflow attack would allow an attacker to execute commands stored in the buffer such as shellcode to gain access to a system. This vulnerability could also cause the application to create a denial-of-service condition as well.

#### SQL Injections

According to the logs, a plugin for the SQL database named userjournals\_menu had an injection attack performed against it. SQL injections are when user input pushes SQL commands to the database to grab more information than they should. This could lead to leaks in user data, such as credentials.

#### Linux Shellcode Remote Execution

The logs indicate that at least one of these attacks was successful in allowing the attackers to execute shellcode. The execution of shellcode could indicate successful privilege escalation on the target machine.

#### Deny Updates

The logs also seem to indicate that several of these attacks were successful, as the remainder of the logs seemed to deny an update from google. Though these updates should be managed by a patch management policy, it is good to note that whatever payload was exploited, it did not want to lose its access due to an update. We conclude that unless the policies are set up to prevent these automatic updates, that whatever attack succeeded is actively preventing Google Updates.

#### Affected Systems

A majority of the log files seem to target two workstations of Jessica and Thomas. It would appear that these host machines may have unintentionally allowed the attackers an in point to the network. However, some logs indicate that they simply fell victim to the Header Injections on the web server, **west-cp01\_outside**.

These users should be interviewed and more logs of their activities should be reviewed to see if additional Security Awareness Training is warranted.

### **Recommendations**

Though there are many remediations for each vulnerability found in these logs, a major first step would be to reconfigure the firewall to not just monitor these events but to actively attempt to stop them. This is more of an Intrusion Prevention System (IPS) configuration, however, we can assume from these logs, the firewall may have this built-in.

Here is a list of individual remediation techniques to prevent future attacks based on these vulnerabilities.

* Applications should avoid copying user-controllable data into the HTTP response headers. If unavoidable, then data needs to be strictly validated.
* Implement strong input validation and back-end input sanitation on things hosted on the webserver. This will help prevent XSS, Directory Traversal, SQL Injection, and any other injection attacks.
* Avoid passing user input to file system API altogether to prevent the ability for an attacker to traverse directories on the webserver
* Update the Microsoft Exchange Server hosting the Outlook Web Access to at least version 5.5 Service Pack 4 to prevent the XSS and Spoofing attack on that server
* Update the SENKAS Kolibri Web Server to a newer version, disable respective features, or if none of these options are available, look into replacing the product to remediate the buffer overflow of the GET request.

The logs indicate several other vulnerabilities relating to the webserver. However, based on our observation these are the immediate issues based on these logs.

## **Analysis of Compromised Systems**

### **Observations**

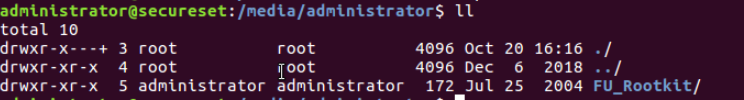
Based on the logs we analyzed we discovered many possible attack vectors that could have been used by attackers to gain the initial access into our network. However, the attackers would not stop there and would want to create a foothold on the network and remain persistent. We began by analyzing all the workstations and servers on the network with the provided credentials. During this investigation, we found three machines that have been compromised and had potential backdoors and persistence tools installed on them.

## **192.168.0.3 - Ubuntu 16.04 Machine 2**

This Linux workstation had several key pieces of evidence to describe how our attackers would maintain their access, as well as possible future attacks on the company. On this machine, we found a copy of the **FU Rootkit** mounted on the machine’s media drive. This rootkit is a kernel-based malicious software that will allow privileged persistent access to the attackers. It also will alter the kernel data structures to hide from malware detection.

### **Figure 1**

*Evidence of the rootkit on this machine*

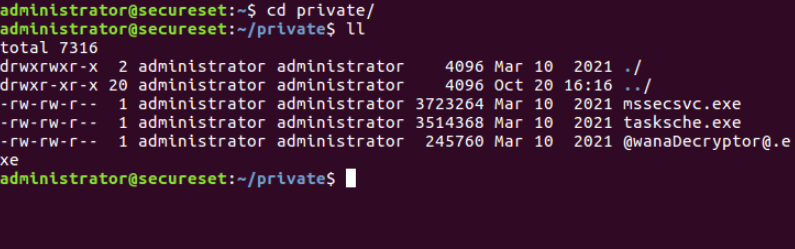
**

We also found evidence in a separate directory named **/private** of a possible future attack being planned by the attackers. This directory contained several files that are part of the WannaCry ransomware attack, first seen in May of 2017. We could deduce that they were planning on launching this attack on ACME in the future.

### 

### **Figure 2**

*WannaCry executables.*

**

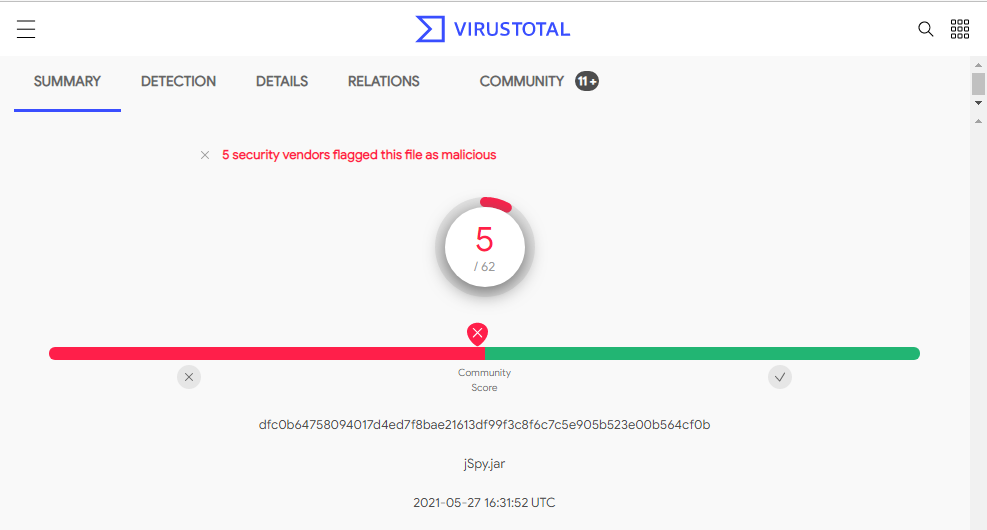
## **192.168.0.10 & 192.168.0.7 - Windows 10 Machine 2 & 4**

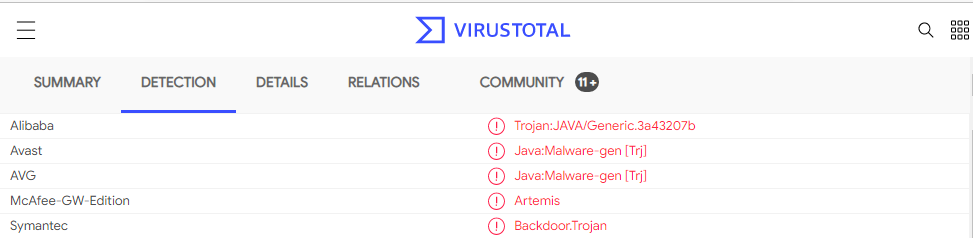
These two Windows 10 workstations also had evidence that they had fallen victim to the attackers. In this case, we found the same suspicious files in both machines’ download directors. These same files were also seen when analyzing one of the SMB Shares, meaning that service was probably used in the spreading of these files. Using VirusTotal, we analyzed these files and found that they were part of a different potential backdoor Trojan, flagged by 5 different security vendors, including McAfee, Avast, and Symantec.

### 

### **Figure 3**

*jSpy.jar VirusTotal Scan Results*

**

**

## 

## **Recommendations**

The presence of a rootkit means that attackers will have constant privileged access to the system. This is a critical security risk and must be dealt with quickly. Unfortunately, the only true way to make sure that a rootkit or backdoor is completely removed from a system is to reformat the hard drive and reinstall the operating system. This means that to secure our network we must:

1. Immediately Remove the infected system from the network and isolate it
2. If necessary, only backup important documents and data files to a CD or Tape. External drives may become compromised by the rootkit simply by being plugged in
   1. Avoid backing up any scripts, executables, and compressed files, as these could also be compromised.
3. Once all files are backed up safely and confirmed to not be corrupted, complete reformatting of the drive is recommended.
4. Install a fresh operating system and bring it back to a secure baseline before reconnecting to the network.

Asset Information

## Inventory of Assets

To understand the scope of our security posture, we need to have an active inventory of our network. Using our Vulnerability Scanner and Nmap, we were able to compile a list of all active hosts on the ACME Network as well as find services running on them and their open ports. Currently, there are 13 total hosts on the network. Here is a table of each host we discovered in our scans and the relevant information. Inventory like this should be done regularly, as we did find that there were several discrepancies with the original Network Diagram as well as the credentials we were given for certain systems.

## Table 1

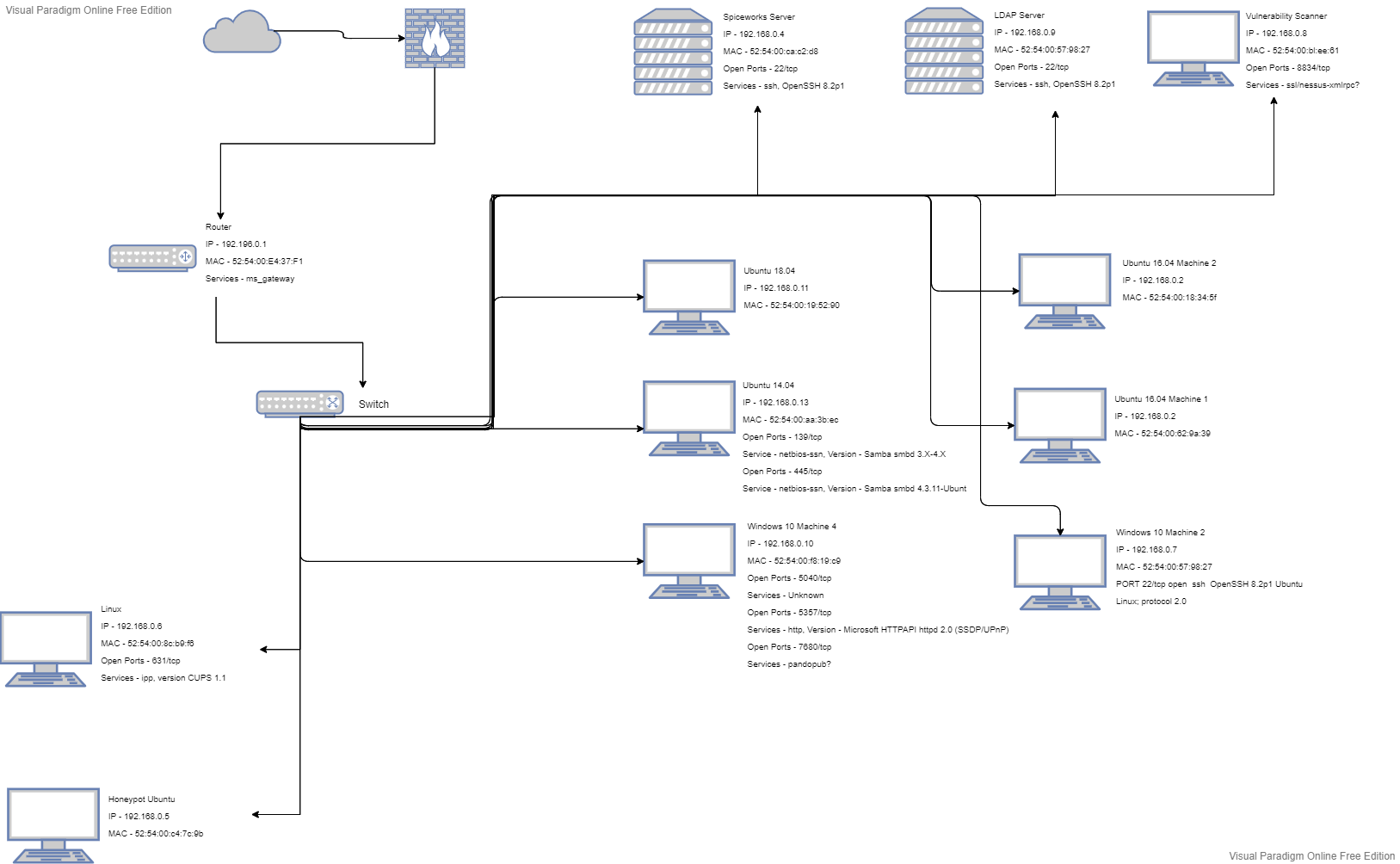
*Current Inventory based on Nessus and Nmap Scans.*

| **NAME** | **OS** | **PURPOSE** | **IP** | **MAC** | **PORT** | **SERVICE** |
| --- | --- | --- | --- | --- | --- | --- |
| Router | VyOS |  | 192.196.0.1 | 52:54:00:E4:37:F1 |  | ms\_gateway |
| Switch |  |  | 192.168.0.250 |  |  | DHCP? |
| Spiceworks Server | Windows Server 2012 | Spiceworks Ticketing Station | 192.168.0.4 | 52:54:00:ca:c2:d8 | 22/tcp | ssh, OpenSSH 8.2p1 |
| Vulnerability Scanner | Ubuntu Server 20.04 | Nessus Vulnerability Scanner | 192.168.0.8 | 52:54:00:bl:ee:61 | 8834/tcp | ssl/nessus-xmlrpc? |
| LDAP Server | Ubuntu  20.04 | LDAP | 192.168.0.9 | 52:54:00:57:98:27 | 22/tcp | ssh, OpenSSH 8.2p1 |
| Honeypot Ubuntu | Ubuntu Server 16.04.3 | WebBug/HoneyPot | 192.168.0.5 | 52:54:00:c4:7c:9b |  |  |
| Ubuntu 18.04 | Ubuntu 18.04 | Ubuntu box | 192.168.0.11 | 52:54:00:19:52:90 |  |  |
| Ubu-14.04-GA-Alpha | Ubuntu 14.04 Updated | workstation | 192.168.0.13 | 52:54:00:aa:3b:ec | 139/tcp  445/tcp | netbios-ssn, Version - Samba smbd 3.X-4.X  netbios-ssn, Version - Samba smbd 4.3.11-Ubuntu |
| Ubuntu 16.04 Machine 1 | Ubuntu 16.04 | Ubuntu box | 192.168.0.2 | 52:54:00:62:9a:39 |  |  |
| Linux | Linux | Testing | 192.168.0.6 | 52:54:00:8c:b9:f6 | 631/tcp | ipp, version CUPS 1.1  MySQL (unauthorized) |
| Windows 10 Machine 2 | Windows 10 | workstation | 192.168.0.7 | 52:54:00:57:98:27 | 22/tcp | OpenSSH 8.2p1 |
| Ubuntu 16.04 Machine 2 | Ubuntu  16.04  Desktop | workstation | 192.168.0.2 | 52:54:00:18:34:5f |  |  |
| Windows 10 Machine 4 | Windows 10 | workstation | 192.168.0.10 | 52:54:00:f8:19:c9 | 5040/tcp  5357/tcp  7680/tcp | Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)  pandopub? |

Based on this inventory, and the provided network map that was given to us earlier, we created this diagram of the current ACME network. In this, we also labeled assets as above.

## Figure 1

*Current Network Diagram*

**

When mapping out the systems, we noticed a few things that may need to be addressed to harden the network. First of all, having a honeypot is a great way to track and inspect incoming attacks to gain insight into techniques, tactics, and procedures. Kudos to you for having one! However, having a honeypot in the same network as your general workstations is a recipe for disaster. We would like to recommend that the honeypot be on an isolated network.

Something else that we noticed was that “Windows 10 Machine 3” (shown in the credentials list from the CISO) is no longer in use, or has been moved to a different network. We would encourage more detailed documentation and change management when adding or removing devices from the network.

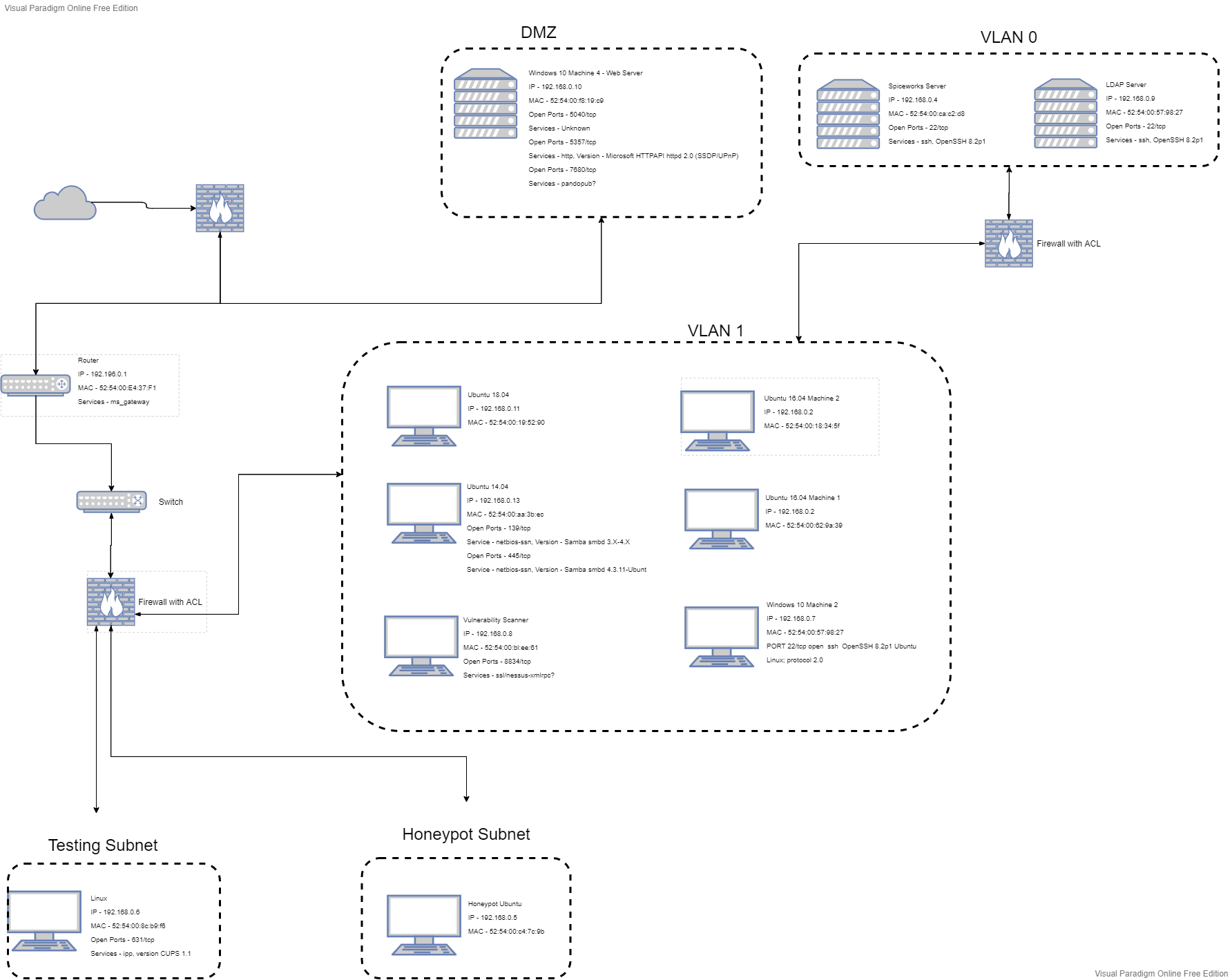
Another suggestion we have is to create subnets for different departments/purposes within the internal network. This allows for greater access control and permissions management across the network. It would also be in our best interests to create a DMZ for all public-facing web servers. Based on our research it seems that the web services we are offering were a major attack vector in the past. We also controlled segments of the network for our LDAP and Spiceworks Ticketing Servers. This will increase the security of these servers as we can then add access control to them and will decrease the risk of compromise should another breach occur. Having multiple network segments in place also allows us to move other assets into appropriate areas should that be required based on future findings.  
  
We would also want to place our test machine (Linux) into a similar separate network to prevent any weaknesses in that machine from spreading to the rest of the network. How we subnet this may be entirely dependent on what this test machine is being used to test. If it does not require outside internet access, it would be best to segment this away from the main router and instead allow access only to the VLAN through an access control list (similar to the LDAP and Spiceworks servers). However, if the internet is required to test web applications or other features, then it would need to be separated either like the honeypot or as part of the DMZ.

Below is an updated diagram based on these recommendations, currently assuming that the testing machine does need internet access.

## 

## Figure 2

*Updated Network Diagram based on current recommendations.*



Vulnerability Assessment

## **Executive Summary**

One of the first things we did to understand our network and the systems on it was to perform a vulnerability scan of the entire network. For this, we used the Tenable Nessus Scanner located on the dedicated machine at 192.168.0.8. From that scan, we created a spreadsheet with all the information necessary to come up with a plan to strengthen our security posture.

Based on our finding a majority of the risks found in our assessment of the systems and network simply require patches and updates. This will require us to come up with a Patch Management system as soon as possible to implement these fixes. There were also cases of creating access controls and enforcing digital signing to protect information.

Below is the table created assessing the vulnerabilities noted in the Nessus Scan with detailed information about the severity of each one and safeguards we can use to remediate the machine. This will help expedite the remediation of each system on the network quickly once we have the approval to begin the process of implementing the suggested safeguards, we will start assigning tasks to the team and assigning due dates for each task.

We have also attached the report created from the Nessus Scan to this document as a reference as a separate file as well as the original spreadsheet.

## **Table 1**

*Vulnerability Assessment based on the Nessus Advanced Scan.*

| **IT VULNERABILITY ASSESSMENT** | | | |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **IP Address** | **RISK** | **POSSIBLE THREATS**  **THE ASSET** | **CVE Number** | **CONSEQUENCE OF BREACH** | **RISK SEVERITY** | **RISK LIKELIHOOD** | **RISK LEVEL** | **CURRENT SAFEGUARDS** | **PROPOSED SAFEGUARDS** | **PRIORITY** | **TEAM MEMBERS ASSIGNED TO THIS RISK** | **DUE DATE** |
| 192.168.0.1 | IP forwarding is enabled on a machine that is not a router or firewall | An attacker can exploit this to route packets through the host and potentially bypass some firewalls/routers / NAC filtering. | CVE-1999-0511 | **Confidentiality** There is considerable informational disclosure.  **Integrity** Modification of some system files or information is possible the scope of what the attacker can affect is limited.  **Availability** There is reduced performance or interruptions in resource availability | ACCEPTABLE | POSSIBLE | **MEDIUM** | NONE | 192.168.0.1 is currently set as a router and IP forwarding is acceptable. Revisit to ensure that status remains constant. Recommended that disable IP forwarding. | **LOW** |  |  |
| 192.168.0.2 | Microsoft Windows SMB Shares Unprivileged Access | The remote has one or more Windows shares that can be accessed through the network with the given credentials.  Depending on the share rights, it may allow an attacker to read/write confidential data. | CVE-1999-0520  CVE-1999-0519 | **Confidentiality** There is considerable informational disclosure.  **Integrity** Modification of some system files or information is possible the scope of what the attacker can affect is limited.  **Availability** None | UNDESIRABLE | POSSIBLE | **HIGH** | NONE | To restrict access under Windows, open Explorer, do a right-click on each share, go to the 'sharing' tab, and click on 'permissions'. | **HIGH** |  |  |
| 192.168.0.2 | Signing is not required on the remote SMB server | An unauthenticated, remote attacker can exploit this to conduct man-in-the-middle attacks against the SMB server. | CVE-2016-2115 | **Confidentiality** None  **Integrity** Modification of some system files or information is possible the scope of what the attacker can affect is limited.  **Availability** None | TOLERABLE | POSSIBLE | **MEDIUM** | NONE | Enforce message signing in the host's configuration. On Windows, this is found in the policy setting 'Microsoft network server: Digitally sign communications (always)'. On Samba, the setting is called 'server signing'. See the 'see also' links for further details. | **MEDIUM** |  |  |
| 192.168.0.3 |  |  |  |  |  |  |  |  |  |  |  |  |
| 192.168.0.4 |  |  |  |  |  |  |  |  |  |  |  |  |
| 192.168.0.5 |  |  |  |  |  |  |  |  |  |  |  |  |
| 192.168.0.6 |  |  |  |  |  |  |  |  |  |  |  |  |
| 192.168.0.7 |  |  |  |  |  |  |  |  |  |  |  |  |
| 192.168.0.9 |  |  |  |  |  |  |  |  |  |  |  |  |
| 192.168.0.10 |  |  |  |  |  |  |  |  |  |  |  |  |
| 192.168.0.11 |  |  |  |  |  |  |  |  |  |  |  |  |
| 192.168.0.13 | Signing is not required on the remote SMB server | An unauthenticated, remote attacker can exploit this to conduct man-in-the-middle attacks against the SMB server. | CVE-2016-2115 | **Confidentiality** None  **Integrity** Modification of some system files or information is possible the scope of what the attacker can affect is limited.  **Availability** None | TOLERABLE | POSSIBLE | **MEDIUM** | NONE | Enforce message signing in the host's configuration. On Windows, this is found in the policy setting 'Microsoft network server: Digitally sign communications (always)'. On Samba, the setting is called 'server signing'. See the 'see also' links for further details. | **MEDIUM** |  |  |
| 192.168.0.250 | The remote DHCP server may expose information about the associated network. | A local attacker may use DHCP to become intimately familiar with the associated network. |  | **Confidentiality** There is considerable informational disclosure.  **Integrity** Modification of some system files or information is possible the scope of what the attacker can affect is limited.  **Availability** There is reduced performance or interruptions in resource availability | TOLERABLE | POSSIBLE | **LOW** | NONE | Apply filtering to keep this information off the network and remove any options that are not in use. | **LOW** |  |  |
| 192.168.0.xx |  |  |  |  |  |  |  |  |  |  |  |  |

## **Table 2**

*We created a separate table for the Vulnerability Scanner workstation itself due to the number of Vulnerabilities witnessed on the machine. Thankfully an update to this system will probably be able to remediate most if not all of them.*

| **192.168.0.8** | | | | | | | | | | | | | |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **# of Events** | **Vulnerabilities** | **RISK** | **POSSIBLE THREATS**  **THE ASSET** | **CVE Number** | **CONSEQUENCE OF BREACH** | **RISK SEVERITY** | **RISK LIKELIHOOD** | **RISK LEVEL** | **CURRENT SAFEGUARDS** | **PROPOSED SAFEGUARDS** | **PRIORITY** | **TEAM MEMBERS ASSIGNED TO THIS RISK** | **DUE DATE** |
| **1** | Ubuntu 18.04 LTS / 20.04 LTS / 21.04 : WebKitGTK vulnerabilities (USN-5024-1) | A use-after-free vulnerability exists in the way Webkits GraphicsContext handles certain events in WebKitGTK 2.30.4. | A victim must be tricked into visiting a malicious web page to trigger this vulnerability.  A specially crafted web page can lead to a potential information leak and further memory corruption. | CVE-2021-30799 | **Confidentiality** There is total information disclosure, resulting in all system files being revealed  **Integrity** There is a total compromise of system integrity. There is a complete loss of system protection, resulting in the entire system being compromised.  **Availability** There is a total shutdown of the affected resource. The attacker can render the resource completely unavailable. | INTOLERABLE | POSSIBLE | **HIGH** | NONE | Update the affected packages. | **HIGH** |  |  |
| **1** | Ubuntu 18.04 LTS / 20.04 LTS / 21.04 : MySQL vulnerabilities (USN-5022-1) | The remote Ubuntu host is missing one or more security updates. | The easily exploitable vulnerability allows a high privileged attacker with network access via multiple protocols to compromise MySQL Server.  Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of MySQL Server. | CVE-2021-2417 | **Confidentiality** There is considerable informational disclosure.  **Integrity** Modification of some system files or information is possible the scope of what the attacker can affect is limited.  **Availability** There is a total shutdown of the affected resource. The attacker can render the resource completely unavailable. | INTOLERABLE | PROBABLE | **HIGH** | NONE | Update the affected packages. | **HIGH** |  |  |
| **1** | Ubuntu 18.04 LTS / 20.04 LTS / 21.04 : Firefox vulnerabilities (USN-5074-1) | The remote Ubuntu host is missing one or more security updates. | Multiple security issues were discovered in Firefox. If a user were  tricked into opening a specially crafted website, an attacker could  potentially exploit these to cause a denial of service, bypass mixed  content blocking, or execute arbitrary code. | CVE-2021-38491, CVE-2021-38493, CVE-2021-38494 | **Confidentiality** None  **Integrity** Modification of some system files or information is possible the scope of what the attacker can affect is limited.  **Availability** There is reduced performance or interruptions in resource availability | UNDESIRABLE | POSSIBLE | **HIGH** | NONE | Update the affected packages. | **HIGH** |  |  |
| **1** | Ubuntu 18.04 LTS / 20.04 LTS / 21.04 : OpenSSL vulnerabilities (USN-5051-1) | The remote Ubuntu host is missing one or more security updates. | OpenSSL incorrectly handled decrypting SM2  data. A remote attacker could use this issue to cause applications using  OpenSSL to crash, resulting in a denial of service, or possibly change  application behavior. | CVE-2021-3711 | **Confidentiality** There is considerable informational disclosure.  **Integrity** Modification of some system files or information is possible, but the attacker does not have control over what can be modified, or the scope of what the attacker can affect is limited.  **Availability** There is reduced performance or interruptions in resource availability. | UNDESIRABLE | POSSIBLE | **HIGH** | NONE | Update the affected packages. | **HIGH** |  |  |
| **1** | Ubuntu 20.04 LTS : GnuTLS vulnerabilities (USN-5029-1) | The remote Ubuntu host is missing one or more security updates. | A flaw was found in gnutls. A use after free issue in client sending key\_share extension may lead to memory corruption and other consequences.  A flaw was found in gnutls. A use after free issue in client\_send\_params in lib/ext/pre\_shared\_key.c may lead to memory corruption and other potential consequences. | CVE-2021-20231, CVE-2021-20232 | **Confidentiality** There is considerable informational disclosure.  **Integrity** Modification of some system files or information is possible, but the attacker does not have control over what can be modified, or the scope of what the attacker can affect is limited.  **Availability** There is reduced performance or interruptions in resource availability. | UNDESIRABLE | POSSIBLE | **HIGH** | NONE | Update the affected packages. | **HIGH** |  |  |
| **1** | Ubuntu 20.04 LTS : Python vulnerability (USN-4973-2) | The remote Ubuntu host is missing one or more security updates. | In Python before 3,9,5, the IP address library mishandles leading zero characters in the octets of an IP address string. This (in some situations) allows attackers to bypass access control that is based on IP addresses. | CVE-2021-29921 | **Confidentiality** There is considerable informational disclosure.  **Integrity** Modification of some system files or information is possible the scope of what the attacker can affect is limited.  **Availability** There is reduced performance or interruptions in resource availability. | UNDESIRABLE | PROBABLE | **HIGH** | NONE | Update the affected packages. | **HIGH** |  |  |
| **2** | Ubuntu 18.04 LTS / 20.04 LTS : Linux kernel vulnerabilities (USN-5017-1) | The remote Ubuntu host is missing one or more security updates. | Bluetooth LE and BR/EDR secure pairing in Bluetooth Core Specification 2.1 through 5.2 may permit a nearby man-in-the-middle attacker to identify the Passkey used during pairing (in the Passkey authentication procedure) by reflection of the public key and the authentication evidence of the initiating device, potentially permitting this attacker to complete authenticated pairing with the responding device using the correct Passkey for the pairing session. The attack methodology determines the Passkey value one bit at a time. | CVE-2020-26558 | **Confidentiality** There is considerable informational disclosure.  **Integrity** Modification of some system files or information is possible the scope of what the attacker can affect is limited.  **Availability** None | TOLERABLE | POSSIBLE | **HIGH** | NONE | Update the affected packages. | **HIGH** |  |  |
| **1** | Ubuntu 20.04 LTS : Linux kernel vulnerabilities (USN-5091-1) | The remote Ubuntu host is missing one or more security updates. | \*\* DISPUTED \*\* In drivers/char/virtio\_console.c in the Linux kernel before 5.13.4, data corruption or loss can be triggered by an untrusted device that supplies a buf->len value exceeding the buffer size. NOTE: the vendor indicates that the cited data corruption is not a vulnerability in any existing use case; the length validation was added solely for robustness in the face of anomalous host OS behavior. | CVE-2021-38160 | **Confidentiality** here is total information disclosure, resulting in all system files being revealed.  **Integrity** There is a total compromise of system integrity. There is a complete loss of system protection, resulting in the entire system being compromised  **Availability** There is a total shutdown of the affected resource. The attacker can render the resource completely unavailable. | INTOLERABLE | PROBABLE | **HIGH** | NONE | Update the affected packages. | **HIGH** |  |  |
| **25** | Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS / 21.04 Applications | The remote Ubuntu host is missing a security update. | A multitude of vulnerabilities exist that allow various types of attacks to A vulnerof The A vulnerof abilitiesties |  | **Confidentiality** There is considerable informational disclosure.  **Integrity** Modification of some system files or information is possible the scope of what the attacker can affect is limited.  **Availability** There is reduced performance or interruptions in resource availability. | INTOLERABLE | PROBABLE | **MEDIUM** | NONE | Update the affected packages. | **EXTREME** |  |  |
| **1** | SSL Certificate Cannot Be Trusted | The SSL certificate for this service cannot be trusted. | If the remote host is a public host in production, any break in the chain makes it more difficult for users to verify the authenticity and identity of the webserver. This could make it easier to carry out man-in-the-middle attacks against the remotwebserverrverwebwebserver |  | **Confidentiality** No information available  **Integrity** No information available  **Availability** No information available | TOLERABLE | PROBABLE | **MEDIUM** | NONE | Purchase or generate a proper SSL certificate for this service. | **MEDIUM** |  |  |
| **1** | Ubuntu 18.04 LTS / 20.04 LTS / 20.10 / 21.04 : Avahi vulnerabilities | The remote Ubuntu host is missing one or more security updates. | Avahi incorrectly handled termination signals  on the Unix socket. A local attacker could use this issue to cause  Avahi to hang, resulting in a denial of service. This issue only affected  Ubuntu 18.04 LTS, Ubuntu 20.04 LTS, and Ubuntu 20.10. | CVE-2021-3468 | **Confidentiality** None  **Integrity** None  **Availability** There is reduced performance or interruptions in resource availability. | TOLERABLE | PROBABLE | **LOW** | NONE | Update the affected packages. | **LOW** |  |  |

## **Recommendations**

Based on the above scan, aside from immediately remediating the vulnerabilities outlined in the above tables, we should work to create a policy to protect all systems on our network by implementing system hardening best practices. We should then use these newly hardened systems to create a Common Operating Environment (COE) that we can deploy on any new machines that may need to be placed into the network. We can also create back-ups of these baselines and begin redundancy through continuous backups from this baseline for all systems.

Our Hardening Solutions are as follows:

* Implement a centralized Patch Management System to keep all systems up to date with the latest security patches. This will also allow for the testing of patches before deployment.
* Create a strong Password Policy across all systems.
  + ACME currently uses weak passwords; This should be updated to the following:
    - Minimum 14 characters long
    - Use of special Characters [ !, &, @ … ]
    - At least one uppercase character
    - Implement a password history and expiration
    - Passwords should not be stored as plain text on databases
  + Enable Account locks after several failed logins
  + Create strong authentication policies and procedures
    - Possibly implement multi-factor authentication to prevent the use of compromise of credentials
* Remove/Disable all unnecessary/unapproved applications and services
* Encrypt data that is at rest.

## **Host-Based Security System**

We should also choose and begin the installation of some form of host-based security software solutions, such as anti-malware. If possible we would like to recommend the implementation of a Host Based Security System (HBSS) to centralize management of this software, as well as be able to test policy changes before deployment and maintain updates across all systems.

An HBSS is an official term used by the U.S. Department of Defense for the suite of commercial off-the-shelf software used to monitor, detect, and defend computer networks and systems. As commercial off the shelf implies, this is something commercially available to all businesses. It is, however, a standard for all DoD Systems and Networks.

Most commonly this is a suite of security software developed by McAfee.

## **Benefits and Challenges of an HBSS**

As with any commercial security management solution, there are several pros and cons to each one. As a standard for all Department of Defense systems and networks, we know that this avenue is a strong means to increase our security posture on our endpoints. However, this will come at a cost for the automation that it will provide. Below we have listed the pros and cons of implementing a solution such as McAfee’s ePolicy Orchestrator (ePO).

**PROS**

* Provides a real-time overview of the security posture of desktop assets
* Ability to scan all assets for compliance
* Create a security benchmark across the organization and monitor changes
* HIPS/Firewall and Virus Scanner
* Ability to test policy updates before deployment
* Streamlined Incident Investigation and Remediation
* Detailed report capabilities

**CONS**

* Requires additional resources to manage
* Initial deployment could cause setbacks in day to day operations
* May have integration issues with existing security program
* Increase overall cost in the IT budget - this is due to training, additional manpower, infrastructure needs, and licensing

Due to the overall cost increase, this may not be possible, so as always the cheaper solution we may want to decide on is purchasing an enterprise-level license for a commercially available antivirus/antimalware software plan. This will divert some resources to either finding a solution of our own to centrally manage this software on each endpoint or regularly go in and make sure it is up to date and functioning properly on a regular schedule. This solution also does not have the scalability of an HBSS and may require the purchase of additional licenses to add more endpoints to our network.

Some notable vendors to consider.

* McAfee
* Norton
* Crowdstrike
* Malwarebytes

Either solution is better than not having any host-based solutions to help protect our endpoints and is strongly recommended we implement as quickly as possible as part of the hardening of our systems.

OSINT

## Executive Summary

Currently, ACME as an organization is lacking in many basic security policies and procedures that would be found if they had the strong guidance of a Risk Management Framework. With this under consideration, in our work to secure ACME’s network and systems, we have taken a look at some of the available open-source intelligence we could gather from the company and its employees. With this passive reconnaissance, we were able to identify possible threats, come up with several considerations for the types of information we should start collecting and monitoring, and write a rough draft of an organization-wide policy for employees to reduce risk to the organization.

Basic recommendations include the analysis of logs for outbound connections to external social media platforms, personal email clients, and other non-work-related web browsing to help reduce overall exposure to threats. There is also room to consider implementing blacklisting some third-party platforms on our corporate-owned workstations to reduce this monitoring. Our recommendations for the policy would be to include guidelines for employees’ outside use of these platforms to help limit the amount of information they are sharing on them, restrict email use on company workstations to an approved client and only connect work emails to it, eliminate/limit/segment access for non-company mobile devices and Security Awareness Training for all personnel to prevent unintentionally starting an attack. This will help reduce the number of attack vectors open to threats to the company.

## Threats

Many security breaches occur due to the ability of malicious actors to passively collect data freely provided by those employed at ACME. Based on the information at hand, three weeks ago there was a data breach of the network. Also, there appears to have been theft of intellectual property as knock-offs of ACME’s designs have been reported to be coming in from China. To help reduce the risk, it is first necessary to understand the threats that come with mismanagement of information leaving the company.

### Phishing/Spear Phishing

The act of phishing is attempting to deceive a user or a specific group of users into performing an action that could initiate an attack. This could be clicking a link or opening a document. Typically these are done through email, however, as our monitoring technology has improved, so has the attacker’s ingenuity. Now many of these links are being sent via social media messaging applications, which will bypass traditional email security controls. In all cases, this would require personal knowledge of a target, such as interests, travel plans, or events, and may not be specific to ACME at all.

### Social Engineering

When an employee joins a social media network and identifies themselves and the department they work in at ACME, they become a target for attackers to utilize in the early stages of an attack (the reconnaissance phase of the Cyber Kill Chain). The information that these social media sites can provide an attacker could include addresses, phone numbers, resumes, email accounts, work locations, family members, education, and other private information. This information could be used by attackers in not only phishing campaigns, but to also build trust relationships with targets to gain first-hand information.

### Web Application Attacks

Most web applications, like social media web pages, use new scripting techniques to improve functionality for their users, this, however, also opens these web pages to exploitation. Though the Open Web Application Security Project (OWASP) has published guidelines to secure web applications, it is hard to determine if a website is following these principles. There are several vulnerabilities such as Cross-Site Scripting, where attackers have altered a website to execute code in a client’s browser. Cross-Site Request Forgery (CSRF), the theft of a user’s “session” allowing attackers to hijack a connection to a specific site. It is also possible on some of these social media platforms that a third-party application could hide malicious code inside it.

These types of attack vectors could lead to unauthorized access into this network if these attacks are executed on a corporate workstation or a compromised personal device is allowed to connect to this network. So it would behoove us as an organization to limit these vulnerabilities as best we can through policy and governance.

## 

## Recommendations

Several recommendations could be made to strengthen our security posture while also reducing exposure to threats. The basic technical controls we should consider at this stage are:

* Network Controls
  + Monitoring outbound traffic logs
  + Web Content Filtering tools
  + Network Segmentation into “Trust Zones”
* Host-based Controls
  + Create a hardened Common Operating Environment (COE)
  + Multi-factor authentication
  + Whitelisting/Blacklisting of approved/unapproved applications/webpages

However, we feel at this stage the simplest solution to start tackling this problem would be to introduce an organization-wide policy on social media accounts and personal use of the internet on corporate-owned devices. On the following page is a rough draft of what that policy may look like. Several of these drafts procedures would require some technical controls, however, a majority are geared towards employee actions. Again, this is a rough draft.

# ACME Anvil’s Social Media and Personal Internet Use Policy

## PURPOSE

This policy provides guidance for employee use of social media and personal internet activity on company systems and networks, which should be broadly understood for purposes of this policy to include blogs, wikis, microblogs, message boards, chat rooms, electronic newsletters, online forums, social networking sites, and other sites and services that permit a user to share information with others in a contemporaneous manner.

## PROCEDURES

The following principles apply to professional use of social media on behalf of ACME as well as personal use of social media when referencing ACME.

* All personal mobile devices (smartphones, tablets, laptops, etc.) should only connect to the designated public access points. At no time should these devices be used to connect to or interact with any company services, networks, or systems.
* All emails viewed on company-owned workstations should be viewed through the preapproved email client. Personal email accounts accessed through a web-based client (e.g. Gmail) should be done on personal devices via the designated network access point.
* All Employees are required to complete Security Awareness Training to help prevent inadvertent compromise of the companies network and systems and teach each member of the ACME team proper education on what, when, and how to share information if any.
* Employees need to follow the ACME’s Code of Conduct, Employee Handbook, and other company policies when using social media while talking about ACME.
* Employees should be aware of the effect that their actions have on themselves, as well as ACME’s image. The information that employees post or publish may be publicly available for a long time.
* Employees should know that ACME may look into information made by employees through social media. Employees should use their best judgment in posting material that is neither inappropriate nor harmful to ACME, its employees, or customers.
* Specific examples of prohibited social media conduct include posting commentary, content, or images that are defamatory, pornographic, proprietary, harassing, or any means that can create a hostile work environment.
* Employees are not to publish, post or release any information that is considered confidential. If there are questions about what is considered confidential, employees should check with the Human Resources Department and/or supervisor.
* Social media networks, blogs, and other types of online content sometimes generate press and media attention or legal questions. Employees should refer these inquiries to authorized ACME spokespersons.
* Employees should get permission before they refer to or post images of current or former employees, members, vendors, or suppliers.
* Employees should get permission to use a third party’s copyrights, copyrighted material, trademarks, service marks, or other intellectual property.
* When using social media, it should not interfere with the employee’s responsibilities at ACME. ACME’s computer systems are to be used for business purposes only. When using ACME’s computer systems, use of social media for business purposes is allowed (ex: Facebook, Twitter, ACME blogs, and LinkedIn), but personal use of social media is discouraged and could result in disciplinary action.
* Subject to applicable law, after-hours online activity that violates the ACME’s Code of Conduct or any other company policy may subject an employee to disciplinary action or termination.
* If employees publish content after-hours that involves work or subjects associated with ACME, a disclaimer should be used, such as this: “The postings on this site are my own and may not represent ACME’s positions, strategies or opinions.”
* It is highly recommended that employees keep ACME-related social media accounts separate from personal accounts, if practical.

## OUTLINE

We here at ACME do want to discourage employees from showing off our brand on social media but need a clear social policy that helps inform employees what they can and should share on social media platforms and what they shouldn’t. Its main focus is not limited to preventing security breaches so our employees do not succumb to phishing or hacking through social engineering. Knowing when and how to respond to a crisis is also very important to our company so if something does happen this shows the best method of how to address the issue on social media platforms.

Security Plan with Timelines

## **Overview**

Currently, the ACME company’s overall security posture is very weak. To increase this we need to facilitate a multi-year plan to strengthen this and prevent future data breaches and other security incidents. To do this we will be utilizing the Capability Maturity Model Integration (CMMI), a process to help organizations like ACME streamline improvements to their processes, increase productivity, and reduce risk to security.

Based on this model, the Acme Company is level 1 (initial). As described by our Chief Information Security Officer (CISO), ACME as an organization is unplanned, unsystematic, and inconsistent (Ad-Hoc). There isn’t a consistent way of accomplishing any task. The only detail that is cared about is meeting the timeline of the objective and not having any quality of how the task is completed. Since this is the case there is also no standard of how things get done so that means that the same task can be accomplished in multiple different ways by different people potentially getting different outcomes and not the proper quality outcomes. This also leads to the suggestion that documentation of each task is lacking if not non-existent, meaning that if a task is repeated, data may be different.

At this level, the process is poorly controlled, unpredictable, and reactive. An example of this would be during a question-answer phase nothing is standardized or there are no test plans of any sort and even if these things are defined each member has a different way of doing things so the process is not consistent at all.

The goal of this plan is to get to level 5 (optimized) as described in the CMMI Model so we can have continuous improvement. To reach this goal we will be building a timeline of how long it should take to reach each consecutive milestone in this model.

## **Level 2 - 5 months**

Having identified that the company is currently at level 1 we know our next goal according to the CMMI is level 2 The projected goal to accomplish this is 5 months of starting the new program. Level 2 is Repeatable control: Initiate Defining processes at a high level.

During this phase, the company will establish better policies and procedures, require better documentation, and create/enforce standards across all areas. In this phase, we will also establish the roles and responsibilities to increase effectiveness during project management.

## **Level 3 - 18 months**

Moving towards level 3 of the CMMI model should occur within 18 months of applying this program to the company. Level 3 is all about identifying the necessary skills needed to use the new processes and standards effectively and providing training to do so if necessary. This phase also emphasizes the idea of motivating and supporting the resources required to follow those standards and processes. This means promoting collaboration amongst the team to help educate and train members.

The primary focus is on documenting, upholding standards, and integrating better methods. By this time the organization has developed its standards and process of monitoring and testing systems and networks. A methodology should have been created or be in the process of being created to maintain and upgrade security controls, monitor network activity, and update systems.

## **Level 4 - 24 months**

Within 24 months, ACME should be able to reach the guidelines of level 4 of the CMMI model. In this phase, we should shift to becoming more predictable in our processes and methodology. Allowing us to measure performance in a quantitative manner

Processes can be adjusted if needed without degrading the quality of the end of the security risk. An analysis is done by dividing the complete process into smaller processes and then those smaller processes are adjusted if need be. This level is called predictable because based on what we learned in level 3 and people’s prior experience and growth we can predict the process quantitatively and make use of this prediction for the upcoming processes. In short, during this level, the process is measured and controlled. For example, performing regular audits is a great idea here. This includes checking if the teams are following everything that has been put in place so far and following the processes defined using the standards and the methodology.

## **Level 5 - 36 months**

By the end of the third year (36 months) we should be upholding all standards and continuing to optimize how we handle our cyber security. At level 5 of the CMMI model, the overall goal of this initiative, there are innovative ways to further improve the processes and standards.

For this, the processes are watched and re-engineered continuously by adding new tools and technologies, by continually researching and studying, and keeping the company updated with the newest information on the market. The primary focus of this level is continuous process improvement. This includes organizational performance management and quantitative project management. For example, always improving the methodology based on the prior audit results and continually trying to update the security plan.

## **PLAN OF ACTION AND MILESTONES**

To help stay on track with this program, it is recommended that a detailed Plan of Action and Milestones (POAM) is created with detailed and specific tasks to be implemented to achieve these goals above. The below table the current POAM created based on our initial research. Note this table is considered a living document and will be updated as the investigation and risk assessment continues. Currently, there are some specific things we can implement in the current Network to reduce risk exposure.

## **Table 1**

*Current POAM table with controls to implement and time frame for each one. This will constantly be updated as new policies, procedures, and standards are created.*

| **Weakness** | **Priority** | **Responsible Office/Party** | **Scheduled Completion** | **Milestones with Interim completion dates** | **How was the weakness identified?** | **Status** |
| --- | --- | --- | --- | --- | --- | --- |
| Update: IPS/IDS system | High | Cybersecurity | Nov 15, 2021 | Immediate: explore options and vendors available  By Nov 1, 2021  Implement and install IPS/IDS systems  By Nov 15, 2021  Fully tune IPS/IDS systems to minimize false positives and false negatives | Annual cyber security assessment | ongoing |
| Subnetting not implemented | Medium | Network Admin | Nov 1, 2021 | Immediate: delineate subnets for each department | Annual cyber security assessment | ongoing |
| No DMZ established | High | Network Admin | Nov 1, 2021 | Establish a DMZ for publicly accessed resources. | Annual cyber security assessment | ongoing |
| Sign in not required on SMB server | Medium | Network Admin | Nov 1, 2021 | Implement access controls to ensure that sign-in is required to access the SMB server | Annual cyber security assessment | ongoing |
| Baselines not established for each host on the network | Low | System Admin | Nov 1, 2021 | Establish an acceptable baseline for each OS on the network | Annual cyber security assessment | ongoing |
| Malware detection system/anti-malware not in use | high | Cybersecurity | Nov 15, 2021 | Immediate:  Research available products and vendors  By Nov 15, 2021  Implement and tune malware detection and prevention | Annual cyber security assessment | ongoing |
| Hardening of each host OS | High | System Admin | Nov 1, 2021 | Install requisite updates and patches to ensure optimal security of each device on the network | Annual cyber security assessment | ongoing |
| No host-based security system | Medium | System Admin | Nov 15, 2021 | By Nov 1, 2021  Research available products and vendors  By Nov 15, 2021  Install and set up host-based security system of choice | Annual cyber security assessment | ongoing |
| Server hardening | High | System Admin | Nov 15, 2021 | By Nov 1, 2021  -Research available products and vendors for DDOS protection, antivirus/antimalware. -Implement a regular backup schedule and password management plan  By Nov 15, 2021  Implement DDOS Protection, and antivirus/antimalware solution. | Annual cyber security assessment | ongoing |
| No web application firewall | High | Network Admin | Nov 15, 2021 | By Nov 1, 2021  Research available products and vendors for proper firewall resources.  Install firewall within means to protect from XSS and other injections.  By Nov 15, 2021  Implement a firewall to start inspecting and filtering traffic. | Annual cyber security assessment | ongoing |
| Lack of social media and personal internet usage policy | Medium | Network Admin | Nov 15, 2021 | By Nov 1  Develop social media and personal internet usage policy, initiate training of employees  By Nov 15  All employees fully trained | Annual cyber security assessment | ongoing |
| Social engineering training | Medium | Cybersecurity | Nov 15, 2021 | By Nov 1, 2021  Employees must undergo annual cyber security training to be aware of potential threats.  By Nov 15, 2021  Understanding of all forms of social engineering Vishing, Phishing, etc. | Annual cyber security assessment | ongoing |

INCIDENT RESPONSE PLAN

**Table of Contents**

[**Purpose**](#_jbtzqf64114v) **3**

[**Definitions**](#_we6lchjn3cu3) **5**

[Incident -](#_lem5zw7eqkpc) 5

[Incident Response Team (IRT) -](#_62oy67y6py6z) 5

[Incident Response Manager (IRM) -](#_v6g5n4a0uqtu) 5

[Incident Logs -](#_51i0kz9enq7k) 5

[Incident Summary Report (ISR) -](#_je5yk6yizxq) 5

[Improvement Plan -](#_apu5q8a19kxx) 6

[**Incident Response Team**](#_po09p2f76syu) **7**

[**Management Principles**](#_7dhwliiggeqe) **9**

[Investigation](#_n486soa6bvws) 9

[Affected Stakeholders](#_xghy3q8osik5) 9

[Report Management](#_dxwmz4bp40qj) 9

[**Communication Guidelines**](#_is2fa2naok9h) **10**

[**Phases of Incident Response Plan**](#_6ti3rxcwcik1) **11**

[Preparation](#_6g36v0riky1r) 11

[Detection](#_8u8mwtze0jkx) 11

[Analysis](#_dli095sa8k6m) 12

[Containment, Eradication, and Recovery](#_ugza2ijol5z2) 13

[Post-Incident Activity](#_bgbn7q4fa6ig) 15

[Lessons Learned](#_b74d6m813xnv) 16

ACME Incident Response Policy

## **Purpose**

The ACME company is a privately owned, medium-sized manufacturer of anvil accessories located in Denver, Colorado. To maintain success in their business, ACME stores information of their internal business operations, their intellectual property, and personally identifiable information of their consumers, suppliers, and employees. ACME is dedicated to the protection of this data and is committed to the safety of all its partners and customers and their private information.

This Incident Response plan will outline the procedures used by the ACME internal Security Operations Center (SOC) to detect and respond to the unauthorized access or disclosure of this private information from its systems and networks. This document specifically aims to define the roles and responsibilities of ACME staff during an incident, including but not limited to:

* Identification, isolation, and repair of data breaches
* Timing outlines to handle an incident
* Outline the content of communications
* Define required documents during the steps of the incident response.

ACME also aims to implement practices to proactively reduce the risk that a threat will be actualized on their systems, leading to unauthorized access or disclosure of sensitive information. These practices will include training all staff in security awareness, following appropriate physical and environmental security controls for the technical infrastructure, and deploying technical security controls (e.g. malware detection, firewalls, intrusion detection systems, etc.)

In the event a cyber security incident does occur, ACME’s internal SOC has been trained to expedite remediation of the incident. ACME will proactively maintain this training annually to help their teams easily detect anomalies in their systems and report them effectively to the Incident Response Manager. The Incident Response Team will be regularly kept up to date on new security threats and be trained in modern remediation techniques for each possible incident.

The confidentiality, integrity, and availability of all resources managed by and stored by ACME systems is of great importance to the organization and will be a core value of the organization

## **Definitions**

### Incident -

An incident is any event that threatens the confidentiality, integrity, or availability of all information or resources ACME utilizes internally, especially sensitive information such as personally identifiable information (PII) of our customers and employees or intellectual property and trade secrets. Theft or loss of this data may be harmful to individual customers, suppliers, or our employees.

### Incident Response Team (IRT) -

The IRT is composed of experts across the organization whose responsibility is the help navigate the entire organization through an incident from the initial detection and analysis, to mitigation and remediation, to the post-incident review. The team consists of the Incident Response Manager, hardware and networking experts, communication experts, and the members of the legal team.

### Incident Response Manager (IRM) -

Oversees all aspects of an incident. The primary focus of the IRM is to ensure the proper execution and implementation of the procedures outlined in this Incident Response Plan and maintain appropriate logs throughout the incident. The IRM is also tasked to facilitate communications between the IRT and the organization’s management team. After an incident has been resolved, the IRM will conduct the post-incident review and then produce the Incident Summary Report and an Improvement Plan.

### Incident Logs -

The logs are maintained by the IRM during the entire life-cycle of an incident. These logs will capture critical information concerning the incident and the organization’s response to said incident.

### Incident Summary Report (ISR) -

The ISR is a document produced by the IRM at the conclusion of an incident. It will provide a detailed summary of the incident, how and why the incident occurred, the estimated loss of data, affected parties, and impacted services. The ISR will also examine the procedures of the Incident Response Plan and how the IRT followed those procedures and if they require an update based on this incident.

### Improvement Plan -

Document produced by the IRM at the conclusion of the incident that will provide recommendations for avoiding or minimizing the impact of future incidents based upon the “lessons learned” from the post-incident review. This plan should be kept confidential for security purposes.

## **Incident Response Team**

As part of the preparation phase of incident response, it is paramount to clearly establish roles and responsibilities in the event of an incident as well as accurate and up-to-date contact information for parties involved in the incident response will be maintained and regularly updated as part of the onboarding and offboarding process.

| **Name** | **Email** | **Work Phone** | **Mobile Phone** |
| --- | --- | --- | --- |
| **Incident Response Manager** | | | |
|  |  |  |  |
| **Technical Contacts** | | | |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
| **Legal Counsel** | | | |
|  |  |  |  |
| **Communications Specialist** | | | |
|  |  |  |  |
| **Additional Members** | | | |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

*Additional Members may be required for the Incident Response Team depending on the scope and/or nature of the incident. For example, the IRT may require a software developer for the development team to help deal with a particular incident. These additional members will be chosen at the discretion of the IRM dependant on the individual incident.*

## **Management Principles**

### Investigation

During the investigation of an incident, the IRM or member of the IRT will be gathering information from multiple workstations and/or conducting interviews with key personnel depending on the scope of the incident. All information gathered during the investigation is strictly confidential throughout this process to maintain security. All members of the IRT will have been trained in the best practices associated with handling sensitive information and data privacy. No confidential information is to be shared during this process unless it is strictly relevant to the investigation into the incident or applies to the incident itself.

### Affected Stakeholders

If the incident involves the unauthorized access or disclosure of confidential information of customers, partners, or employees, ACME will communicate all relevant information of the incident to the affected parties. ACME will also provide any additional requested information that the affected party has a right to. ACME, however, does reserve the right to withhold certain information about the incident at the discretion of the IRM if that information could jeopardize current or future investigations or if it could pose additional security risks to ACME or other entities.

In the event that the incident is limited to ACME systems not containing sensitive or confidential information affecting other parties, it will be at the discretion of ACME administrators and the IRM whether or not to share information about the incident with any outside stakeholders

### Report Management

All Reports produced during the incident, along with gathered evidence of the incident will be stored and managed by the IRM. Physical records will be stored in the IRM’s office under lock and key. Digital records will be stored on the internal network share only accessible by the IRM and approved ACME administration. The digital share will also be backed up per ACME’s regular data backup procedures. If any reports need to be reviewed, a written request must be made to the IRM for access to those documents and the reason for the request. It is up to the IRM whether or not to approve the request.

## **Communication Guidelines**

Initial communication to affected stakeholders, customers, partners, and employees should occur a quickly as possible upon the identification of an incident. This may include an initial communication (email or phone call) that simply states ACME is aware of the incident and addressing it. In this initial communication, there should be a promise of a follow-up communication addressing the incident.

In the case that Personally Identifiable Information (PII) has been accessed or released by unauthorized persons, the following guidelines should be utilized:

* Should the unauthorized access, disclosure, or release of customer data occur in an incident, ACME shall notify affected customers no more than 14 calendar days after the breach is discovered.
* Should the unauthorized access, disclosure, or release of protected or confidential data occur, ACME shall notify the affected stakeholders nor more than 14 calendar days after the breach is discovered
* Should the unauthorized access, disclosure, or release of PII and/or confidential or protected data occur, ACME shall notify the Chief Privacy Officer (CPO) or Data Privacy Officer (DPO) no more than 72 hours after the breach is discovered per state and international regulations and compliance standards.

As personnel receives requests for more information from affected parties, they should pass those requests to the IRM. Updated communications will come from a designated member of the Administrative Team or the IRM.

All personnel should be informed of what information is public and what is strictly internal/confidential by the IRM and Administrative Team. Leadership should be aware that any information shared with personnel can and likely will be shared with the public.

Communication with news and media outlets should only be initiated by a designated member of the Administrative or Management Team. Any requests from news and media outlets for information about an incident should be passed to the IRT Communications Specialist or the IRM. Responses will be created as needed.

## **Phases of Incident Response Plan**

### Preparation

Preparation begins with training and awareness of best practices. The ISO (Information Security Office) will assign personnel to train all staff members (not limited to members of the IT team) on information security best practices. This includes, but is not limited to: phishing awareness training, PII awareness and proper disposal, social engineering awareness training, malware, and malicious program awareness, etc. Special care and attention will be given to instructing all staff members regarding the incident response plan and what to do in the case of an incident.

Physical and logical security measures must be established to minimize the impact of a potential incident and aid in the investigation of an incident, should one occur. These measures include, but are not limited to: Restricting access to sensitive areas by using key cards/pin pads, secure offsite data storage, regular backups of data, data encryption, the use of IDS and IPS, active firewall management, implementation, and monitoring of a SIEM.

### Detection

The IT staff member or affected department staff member who discovers the incident will refer to their contact list for both management personnel to be contacted and incident response members to be contacted. The staff member will call those designated on the list. The staff member will contact the incident response manager using both email and phone messages while being sure other appropriate and backup personnel and designated managers are contacted.

**Examples of common incidents and symptoms to look for (sourced from norton.com):**

* Worms
  + Slow computer performance, freezing/crashing, programs opening and running without user interaction, the sudden appearance of messages, images, sounds, etc, firewall warnings missing/modified files, the sudden appearance of unfamiliar desktop files or icons, system error messages, emails sent to contacts without user interaction.
* Viruses
  + Frequent pop-up windows, changes to your homepage, mass emails being sent from your email account, frequent crashes, unusually slow computer performance, unknown programs that startup when you turn on your computer, unusual activities like password changes.
* DOS and DDOS attacks
  + Slow access to files (locally or remotely), long-term inability to access a particular website, internet disconnection, problems accessing all websites, an excessive amount of spam emails
* Spyware
  + Your device is slow or crashes unexpectedly, suddenly your device is running out of hard drive space, frequent pop-ups when you are online or offline
* Ransomware
  + Pop-up windows stating that your data has been encrypted and payment must be received to decrypt the data

**The person receiving the report of the incident will log:**

1. Time of the call.
2. Contact information about the caller.
3. The nature of the incident.
4. What equipment or persons were involved?
5. Location of equipment or persons involved.
6. How the incident was detected.
7. When the event was first noticed that supported the idea that the incident occurred.

**If the person reporting the incident is an IT staff member with a working familiarity with the systems affected, the person receiving the report may choose to ask the following:**

* Is the equipment affected business-critical?
* What is the severity of the potential impact?
* Name of the system being targeted, along with the operating system, IP address, and location.
* Any information about the origin of the attack.

### Analysis

Once an anomalous activity has been reported it is up to the IRM to determine the level of intervention required. Members of the IRT may be required to provide input to help determine if an actual incident has occurred. If the IRM determines a legitimate incident or security event has occurred, they will notify the entire IRT immediately to address the situation as quickly as possible.

Regardless of whether or not the anomalous activity is deemed a security threat, the IRM will document everything in the Incident Logs so that it can be reviewed in the future.

**IRT members will meet or discuss the situation over the telephone and determine a response strategy. The information discussed may include:**

* Is the incident real or perceived?
* Is the incident still in progress?
* What data or property is threatened and how critical is it?
* What is the impact on the business should the attack succeed? Minimal, serious, or critical?
* What system or systems are targeted, where are they located physically and on the network?
* Is the incident inside the trusted network?
* Is the response urgent?
* Can the incident be quickly contained?
* Will the response alert the attacker and do we care?
* What type of incident is this? Example: virus, worm, intrusion, abuse, damage, ransomware, etc.

**An incident ticket will be created. The incident will be categorized into the highest applicable level of one of the following categories:**

* **Category one** - A threat to public safety or life.
* **Category two** - A threat to sensitive data
* **Category three** - A threat to computer systems
* **Category fou**r - A disruption of services

### Containment, Eradication, and Recovery

Once an incident has been determined to have occurred and is considered significant in nature, the IRM should notify Administration immediately. As more information becomes available through the investigation of the incident, Administrators should be briefed by the IRM so that appropriate decisions can be made across the organization and help determine which stakeholders to notify and the way to do so. Administrators will also determine whether law enforcement needs to be notified, and will decide on how to do that as well.

The initial response to any security incident should be to determine the origin of the incident and isolate the issue. Identification could be made through network traffic logs, system logs, or logs created by firewalls/IDS. Isolation could mean disconnecting compromised workstations or servers from the network. To ensure the issue has been properly contained vulnerability scans and the monitoring of firewall and system logs should be ongoing to ensure the incident has not spread to other areas of the network.

The following are recommended procedures for the IRM and IRT to take to help with the remediation and recovery process.

**Team members will establish and follow one of the following procedures basing their response on the incident assessment**:

* Worm response procedure
* Virus response procedure
* System failure procedure
* Active intrusion response procedure - Is critical data at risk?
* Inactive Intrusion response procedure
* System abuse procedure
* Property theft response procedure
* Website denial of service response procedure
* Database or file denial of service response procedure
* Spyware response procedure
* Ransomware response procedure
* The team may create additional procedures which are not foreseen in this document. *If there is no procedure in place, the team must document what was done and later establish a procedure for the incident.*

**Team members will use forensic techniques, including reviewing system logs, looking for gaps in logs, reviewing intrusion detection logs, and interviewing witnesses and the incident victim to determine how the incident was caused. Only authorized personnel should be performing interviews or examining evidence, and the authorized personnel may vary based on the situation.**

**Team members will recommend changes to halt the current intrusion/incident (if ongoing) and prevent the occurrence from happening again or infecting other systems.**

* *Upon management approval*, the changes will be implemented.

**Team members will restore the affected system(s) to the uninfected state. They may do any of the following or more:**

* Re-install the affected system(s) from scratch and restore data from backups if necessary. Preserve evidence before doing this.
* Mandate that users change passwords if passwords may have been compromised.
* Harden the system(s) by turning off or uninstalling unused services.
* Ensure the system(s) are fully patched/updated.
* Ensure real-time antivirus and intrusion detection/prevention is up and running.
* Ensure the system(s) is logging the correct events and to the proper level.

Throughout this process, all evidence should be preserved and all measures taken should be documented in detail to help with the post-incident review and reporting processes once the incident has been resolved.

### Post-Incident Activity

Once an incident has been resolved and normal operations of the organization have been restored, the IRM will conduct a post-incident review and compile all available information into an ISR. Throughout the incident, the IRT is required to have maintained their own Incident Logs and documentation wherever possible. To help with this aspect of the Incident Response Plan, the following are best practices for all information gathering to produce an accurate account of the incident.

**Documentation—the following shall be documented:**

* How the incident was discovered.
* The category of the incident.
* The attack vector used (email, SQL injection, etc.)
* Where the attack came from, such as IP addresses and other related information about the attacker.
* What was done in response?
* Whether the response was effective.

**Evidence Preservation**

* Make copies of logs, email, and other communication. Keep lists of witnesses. Keep evidence as long as necessary to complete prosecution and beyond in case of an appeal.

**Assess damage and cost**

* Assess the damage to the organization and estimate both the damage cost and the cost of the containment efforts.

### 

### Lessons Learned

Once all review of material and information about the incident has been completed in the post-incident review, the IRM and possibly select members of the IRT will meet with Administrators and discuss the event in detail. This meeting will include a full debrief of the incident including the scope of the breach, vulnerabilities that may still exist, gaps in communication, the technical and procedural remediations, and the overall effectiveness of the current response plan.

As a group, we will then determine appropriate actions needed to increase the effectiveness of current policies and draft an Improvement Plan to address any items, processes, or vulnerabilities to prevent future incidents. The Improvement plan should review the response to the incident based on the meeting and determine what policies should be updated and how. It should take into consideration the following.

* Consider whether an additional policy could have prevented the intrusion.
* Consider whether a procedure or policy was not followed which allowed the intrusion, and then consider what could be changed to ensure that the procedure or policy is followed in the future.
* Was the incident response appropriate? How could it be improved?
* Was every appropriate party informed in a timely manner?
* Were the incident-response procedures detailed and did they cover the entire situation? How can they be improved?
* Have changes been made to prevent a re-infection? Have all systems been patched, systems locked down, passwords changed, antivirus updated, email policies set, etc.?
* Have changes been made to prevent a new and similar infection?
* Should any security policies be updated?
* What lessons have been learned from this experience?

This Improvement Plan shall remain confidential for security purposes. Any required communications to clients, stakeholders, customers, or the public must be produced separately and only necessary information to prevent future incidents. Any additional communications to clients, stakeholders, customers, or the public must be approved by the IRM based on his improvement Plan to maintain the confidentiality of that document.

Internal Honeypot

## **Purpose**

Setting up a honeypot is one of the best ways to gain insight into the types of attacks that malicious actors are using against your network and systems. A honey pot is an intentionally insecure computer used to entice attackers by making them think that it is low-hanging fruit containing attractive resources. A honeypot can use outdated versions of protocols, open vulnerable ports, and decoy data or databases to lure in potential attackers and make them think they have gathered pertinent information or critical data from the organization.

The purpose of having a honeypot is to draw attackers in and have them waste time penetrating a vulnerable but inconsequential system. With the right monitoring tools engaged, the organization can see what tactics, techniques, and procedures are used by the attackers to gain access to the computer and what types of data they are trying to exfiltrate. Information gathered about the attackers and their methods can be used to further harden the actual systems used on the network.

## **Configuration Recommendations**

Here are some basic guidelines for setting up a successful honeypot and gathering actionable data on attackers:

* Set up the honeypot on a separate VLAN - this could be the DMZ if it is mimicking a public-facing appliance. This prevents attackers from accessing systems that are not a part of the honeypot or honeynet. By doing this, you are adding an extra layer of protection between the hackers and your actual data/network.
* Use a VM as your honeypot. By using a VM as your honeypot, you can easily create a snapshot of a baseline that can easily be restored in the case that files or the system itself become corrupt due to an attacker’s actions.
* Set up the honeypot to use an administrator account with no password, or with a default password. This makes it easy for the attacker to escalate their privileges.
* Configure the honeypot to run unnecessary services and leave ports open to give the attackers several avenues to access the computer.
* Include decoy files or databases that mimic the data your organization keeps on file. An example of this might be a SQL database that includes customer PII and PCI.
* Make the honeypot as close in appearance and feel as real systems on the network as possible. This includes configuring it to show the same login warning messages, the same data fields, even the same logos as your real systems. This prevents the attacker from recognizing the honeypot as a decoy and targeting your actual systems instead.
* Employ stealthy and tamper-resistant monitoring methods to gather information on attacks and attackers. Tipping off an attacker that they are being monitored would be detrimental to the point of a honeypot.

## **Open Source Solutions**

Here are some recommendations for effective open source tools used for monitoring:

Network-based sniffing tools such as Wireshark. Wireshark can capture and record all network traffic to and from the honeypot. This is useful to identify IP addresses and ports that are being used to access data on the honeypot.

Host-based monitoring tools, such as Sebek, monitor host activity. The Sebek client operates as part of the kernel itself. It works by monitoring system call activity and recording data of interest. Sebek consists of two modules; Sebek.o which monitors activity and cleaner.o which protects Sebek from being discovered. This data is then exported covertly to the server.

Another fully developed, prepackaged opensource honeypot tool called “honeytrap” is available at <https://github.com/honeytrap/honeytrap>.

Honeytrap’s features:

* Combine multiple services to one honeypot, eg a LAMP server
* Honeytrap Agent will download the configuration from the Honeytrap Server
* Use the Honeytrap Agent to redirect traffic out of the network to a separate network
* Deploy a large amount agents while having one Honeytrap Server, the configuration will be downloaded automatically and logging centralized
* Payload detection to determine which service should handle the request, one port can handle multiple protocols
* Monitor lateral movement within your network with the Sensor listener. The sensor will complete the handshake (in case of TCP), and store the payload
* Create high interaction honeypots using the LXC or remote hosts directors, traffic will be man-in-the-middle proxied, while information will be extracted
* Extend honeytrap with existing honeypots (like cowrie or glutton), while using the logging and listening framework of Honeytrap
* Advanced logging system with filtering and logging to Elasticsearch, Kafka, Splunk, Raven, File, or Console
* Services are easily extensible and will extract as much information as possible
* Low- to high interaction Honeypots, where connections will be upgraded seamlessly to high interaction

## **Commercial Honeypots**

There are also several solutions commercially available to enterprises as a centrally managed solution to honeypots and honeynets. The benefit is that these are managed by the company they are purchased from through the cloud, meaning we would not need to hire additional manpower or divert current resources to manage them. However, this would increase cost depending on the commercial solution chosen. Some options are

**Acalvio ShadowPlex** - Cloud-based decoy delivery of a variety of different types Pricing not disclosed.

**Bad Packets** - A global network to detect botnets and malware, including Mirai. Pricing not disclosed.

**Illusive Networks** - Wide variety of decoys, including networks, systems, apps, and data. Pricing is $60 per user per year (varies depending on endpoints).

**Smokescreen Illusion Black** - Hundreds of decoys centrally managed across various types: servers, endpoints, and networks. Pricing starts at $200,000.

## **Final Thoughts**

It would be our final recommendation to maintain the honeypot, however, it will need to be completely reconfigured and actively maintained and monitored. This is because it currently is not a lucrative enough distraction for attackers and is not providing information necessary to strengthen our security postures properly. The most immediate and cost-effective solution would be to follow the recommendations stated above, implement opensource monitoring solutions, and divert staff to maintain and monitor the honeypot. However, it may be in our best interest to bring on additional manpower for this endeavor if possible.

The better solution in our opinion, should the honeypot be maintained as suggested, would be to completely rebuild it. The most cost-effective solution would be to again divert current staff and then utilize an open-source solution - we would recommend Honeytrap - and create a lucrative and well-monitored distraction. Again though, we would want to consider bringing on additional manpower for this task to not spread the current team too thin.

A commercial solution may also be an option should the budget allow for one. This is because this would transfer the configuration and monitoring of the system to a third party. These do come with a higher cost but remove the need for organizational level management and monitoring of the honeypot. If the cost of potentially hiring extra personnel to operate an open-source solution is greater than a commercial solution, it may be best to implement a commercial solution. If a current employee or team of employees has time in their schedule and the requisite knowledge to deploy and operate an open-source solution, that would be the most cost-effective solution.

Review Security Events  
&  
Creation of Monitoring and Metrics

## **Overview**

As we move forward in our process to increase the security posture of the ACME Anvils network and system, a key factor in that success will be the monitoring and reporting of events as they happen. The success of any Security Operations Center is the ability to quickly react to potential security events and incidents as they occur. In this document, we will be analyzing recent events that have occurred over the past year on all security appliances and endpoints in our network. We will be using this analysis to come up with a means to monitor events and metrics to track on a monthly, quarterly, and annual basis.

## **Past Security Events**

As detailed in our analysis of the logs from the current Intrusion Detection System (IDS) and our Firewall, several major events occurred on the network that could have been Indicators of Compromise had they been monitored appropriately. Had these events been monitored and analyzed earlier, the scope of the data breach that occurred several weeks ago may have been mitigated much more quickly.

A quick summary of these events is as follows. For a more detailed analysis of these observations, please refer to the documents  **Analysis of the Untangled Firewall Logs** and **Analysis of the IDS Logs**.

* From ACME’s Intrusion Detection System (IDS)
  + Evidence of spyware detected
  + Evidence of a ping sweep or port scan
  + Possible attempts to connect to a Command and Control (C2) Server over SSH and FTP
  + Failed IPv6 message connections to other workstations
* From ACME’s Firewall
  + Evidence of HTTP Header Injection leading to possible Cross-Site Scripting
  + Cross-Site Scripting on the Outlook Web Access (OWA) client
  + Evidence of Directory Traversal
  + Evidence of a GET request Buffer Overflow on the SENKAS Kolibri Web Server 2.0.
  + Evidence of the execution of Shell Code

The previously referred to documents also contain immediate recommendations for remediations of these issues.

## 

## **Endpoints**

As for Security Events on our endpoints, we only were able to observe three machines that were compromised if not the source of the attack. This evidence was extrapolated from the Firewall Logs. The impacted hosts to the possible vulnerabilities from the web server were:

* west-cp01\_outside
* west-acme-workstation-jessica7
* west-acme-workstation-Thomas2

These machines had several instances of HTTP Header Injections, Cross-site Scripting and spoofing, use in directory traversals, buffer overflow attacks, and even instances of shellcode remote execution. The two workstations in question may not have initiated the attack but merely fell victim to the exploited webserver and became positions of lateral movement by attackers. Remediations can be found in the previously referred to documents. System and Server Hardening recommendations can be found in the **Vulnerability Scan Assessment** and **Web Server Protection** documentation respectively.

## **Monitoring Logs**

For us to properly respond to events as they occur, as well as have the ability to easily investigate incidents should they occur, the implementation of collecting logs is necessary. This will not only give us the bigger picture of a security event/incident in the future, but we can also use these logs to generate reports. The following areas should be considered for logs to be collected:

* System Logs
  + Agent-Based/Endpoint logs
  + Physical Security Logs
  + Application logs
* Networking Logs
  + Email
  + Firewalls
* Technical Logs
  + HTTP logs
  + DNS, DHCP, and FTP Logs
  + Server Logs
* Logs from Monitoring tools
  + Logs from Malware Protection
  + IDS/IPS
  + Other Relevant security management appliances and tools

The collection of logs will require the acquisition of additional secure storage, either on-premises or in the cloud. We will also need to create a policy for what logs to collect and how long we need to keep them. Currently, based on what is currently on the network, as well as some past recommendations, we estimate that to maintain an annual collection of logs we will need, a minimum of 8TB of additional storage. Though we would recommend rounding this off to 10TB to be safe.

## **Metrics**

As part of the monitoring and reporting of security events, we have come up with several metrics to monitor our network and systems to help identify possible security threats, as well as provide the Board with quantitative information to make decisions with. These metrics will require us to set a baseline of the network once we have determined the network and all systems are sufficiently secure. This will help with discovering anomalies in network activity.

**BANDWIDTH CONSUMPTION**

A sudden spike in bandwidth usage could indicate a chance of malicious activity, especially if that consumption occurs during off-hours, which could indicate a security event.

**RETRANSMISSION**

This occurs when a packet fails to reach its destination and could be the byproduct of an attack that overwhelms the network or takes legitimate endpoints offline. Unusual retransmission rates could be an indicator of a potential attack

**OPEN CONNECTIONS**

The total number of active endpoints on a network may fluctuate regularly for legitimate reasons, however, a network with a relatively stable number of connections suddenly seeing changes in activity may be a sign of an attack. Especially when connections to unknown endpoints occur.

**OPEN PORTS**

Tracking which ports are currently open and listening on which endpoints, as well as the change in port configurations over time, is another way to gain insight into possible attacks. A compromised host may open ports that may not normally be opened.

**IP ADDRESS CONFLICTS**

There is no reason for two endpoints to attempt to claim the same IP Address. Though this can be due to misconfiguration on the network, it could also be signs of an attacker attempting to spoof an endpoint.

**DETECTED INTRUSION ATTEMPTS**

Data of actual attempts to invade the network and our systems used to help maintain a state of security awareness, despite the lack of a major breach. This metric is to help prove that threats still exist, even if security has been increased.

**VULNERABILITY DATA**

Vulnerability scan data should be collected regularly and any found vulnerabilities in that data should be responded to quickly.

**NUMBER OF USERS - DATA AND ACCESS LEVELS**

Insider threats are just as dangerous as outside threats. This data should include the logging of employee onboarding and offboarding, application access tracking, and tracking of which systems users are accessing and whether they should have access or not.

**INCIDENT RATES**

There will be future incidents. It is important to maintain accurate data of each incident, its severity, and the overall response and remediation times. This metric will help show improvements in our security posture.

**OVERALL DATA GENERATION**

Though not particularly security-specific, will help demonstrate to the board the growth of our network based on the increase in traffic. As traffic increases, so do costs, and so does the need to protect that traffic.

## **Utilizing the Metrics**

The purpose of the above metrics is to not only alert the security team to a potential breach but also provide tangible easy to understand data to the Board of Directors. This data can then be used to help make decisions on an organizational level about our network and systems. As requested we have categorized when this data should be aggregated into reports for them, as well as metrics that we may want to be alerted to under specific conditions.

**Alerts** - When specific unacceptable thresholds are met in these metrics, security teams should be alerted immediately.

* Bandwidth Consumption
* Retransmission
* Open Connections
* IP Conflicts
* Detected Intrusion Attempts

**Monthly** - These metrics should have reports generated for them on a month-to-month basis for the Board.

* Bandwidth Consumption
* Open Ports
* Open Connections
* Detected Intrusion Attempts

**Quarterly** - These metrics should have reports generated for them every quarter for the Board

* Vulnerability Data
* Number of Users
* Incident Rates
* Overall Data Generation

**Yearly** - As these metrics are being reported regularly, an annual overall report that is an aggregation of the previous metrics over the year should suffice for the board.

## **Security Information and Event Manager**

To effectively collect, monitor, analyze, and easily understand all this data, we recommend the implementation of a Security Information and Event Manager (SIEM). This software is a tool that will help collect and normalize logs, allow for easy search and analysis of this data, and help with the creation of easy to read reports based on the data and metrics we are collecting. We can also create the required thresholds and conditions required to properly alert the team should major security events begin to occur on the network.

A SIEM will introduce an amount of configuration depending on our needs, and will constantly need to be tuned to those needs as they change. However, if the overall goal is to prevent another data breach, we highly recommend devoting some thought to implementing this tool.

There are several options out there, however, we have two suggestions for this tool to help us move forward. Elasticsearch and Splunk are two well-known SIEM’s that function relatively similarly in terms of log collection, aggregation of data, and reporting. However, each has its weaknesses.

**ELASTICSEARCH**

Elasticsearch is the leading free and open-source search and analytics solution out there. As it is open-source, we could easily build it from the ground up ourselves for our own needs. However, this will require a diversion of manpower to build and configure this SIEM, it is free. Being open-source, it will require more effort on our part to get it up and running, as there is no vendor support, and may divert team members’ attention to set up and constantly keep it configured properly.

**SPLUNK**

Splunk is a commercial leader in the SIEM market. As a commercial product, it offers things like vendor support, additional functionality through plugins and add-ons that are easier to deploy and is easier to scale to company growth. However, this comes at a steep price. An annual cost by volume for Splunk is $1,800 per GB of storage. A perpetual license is about $4,500 per GB. This is probably well outside the realm of budgeting currently, however, we would like to mention it as a solution for consideration if a commercial product is more desirable. However, even with this solution, some manpower would need to be utilized to configure it properly at the start and maintain its configuration as things change.

As it stands, our recommendation for this solution would be to build an Elasticsearch on an existing server and purchase the necessary additional storage to keep all the logs collected. We highly recommend the implementation of a SIEM to help monitor our data and generate the necessary reports for the described metrics.

If this is not possible, at the very least current security appliances should be audited and configured to alert us properly when anomalies occur, and we should still create a way to store all logs securely in a central location. However, we will need to manually go through these logs to aggregate the information necessary to generate reports.

Web Bugs with Deployment Plan

## **Overview**

Web security has become increasingly complex over the years. Web servers usually host several business sites, which store customer data, so they are common targets for attackers. Based on our review of the recent attack on ACME’s network and systems, it is clear that their current web server is not properly configured for security. This document is an overview of policies and procedures that we can implement to help protect ACME’s Web Server and mitigate its use as an attack vector for threats. Below are several best practices and tips to be employed for organizations looking to manage their web security. We have also included several commercial options to look into for additional monitoring without increasing internal manpower.

## **Internal Managing of Web Server Security**

### **Shared vs. Dedicated vs. Managed Hosting**

* Shared hosting is the most affordable for customers, but every site on the web host adds risk to other sites on the same server.
* A dedicated hosting model doesn’t have the risks from other websites, but it puts security in the hands of the customer. If the customer manages all aspects of the server’s settings, then vulnerabilities could be introduced by administrators, unfamiliar with cybersecurity best practices.
* Managed hosting is the best option for hosts because it takes all responsibility away from customers who have little cybersecurity knowledge and puts it in the hands of the host provider’s staff.

### **Securing Web Hosting Servers**

Securing a web server not only protects hoster assets but also safeguards customer data from hackers. Businesses that use hosting providers for website services rely on the hoster to safeguard their corporate data and keep the business site running smoothly.

### **Install and Configure a Web Application Firewall**

Using a WAF, hosters can block cross-site forgeries (CSF), cross-site scripting (XSS), SQL injections, and more. For example, if an attacker sends a malformed SQL string using a website’s contact form, the WAF detects it and blocks it. A good WAF will display statistics and information about blocked attacks so that the web host can identify vulnerabilities on customer sites.

### **Distributed Denial-of-Service Attack Protection**

Recommendations are listed below for free DDOS protection tools:

* Webroot DNS Protection.
* Nginx.
* DataDome.
* BitNinja.
* HAProxy.
* Reblaze.
* Ammune Defense Shield (ADS)
* DDoS-GUARD.

### **Recommendations and Best Practices**

Here is a list of best practices to help secure our web server internally:

* Use SFTP Instead of FTP
* Back-Up Data on Servers
* Use Whitelisting for Maintenance IPs
* SSL/TLS Connections
* Antivirus and Antimalware Protections
* Remove Unused Applications Not Used for Hosting
* Force Password Changes
* Configure the Host’s HTTP Strict Transport Security (HSTS) Header

## **Commercial Solutions**

Like most internal solutions, this will require time and the diversion or increase in manpower to implement, monitor, and maintain. Though with our current staff this could easily be achieved with regular audits and implementation of reporting features, there are also commercial options available to us to transfer those responsibilities to third-party companies that specialize in web server protection. We have provided two possible commercial products for management’s consideration should they wish to go this route to free up currently available internal resources, or to avoid hiring additional manpower.

### 

### **UPTRENDS - Part of ITRS Group**

The lowest cost commercial solution we found in our research into outsourcing Web Server Security.

**Graphical user interface, application

Description automatically generated**

### **Reports and dashboards**

**Real User Monitoring (Passive)**

* View actual user’s experience and collect and quantify website performance and user data directly from applications site’s visitors with Real User Monitoring (RUM).
* View your website performance from the actual browsers, devices, and platforms your visitors are using.
* View the geographical distribution of users and their load times.
* Analyze the exact breakdown (network, backend, and frontend) of load times experienced by your real users.

**Synthetic Monitoring (Active)**

* Validate if your site is up proactively.
* Test website functions and predictive click paths to be notified when something breaks before your users do.
* Analyze the root cause of load time spikes with rich waterfall reports on an element level.

### **Collect your data**

* You can set up your custom dashboards to show your API monitor performance data side-by-side with your custom metric data or put it in its dashboard. Data freedom is what Uptrends is about!
* Add alerts to view slow response times or failed validations, but you can also set up alerts based on your Custom Metrics.
* Schedule API’s custom metric data delivered automatically to your inbox with all of your other monitoring data.
* You can set up multi- or single-step API monitoring just for your Custom Metrics if you need to for easier reporting or alerting.

### **ISO 27001 security compliance**

Uptrends is ISO 27001 certified. ISO 27001 is a standardized management approach for the ongoing security and control of sensitive information. ISO 27001 is a system of strict rules and controls applied to people, processes, and IT systems required to ensure that they operate securely, and any data we process for our customers remains private. An external independent third party certifies that Uptrends is compliant with the security standard.

### **Barracuda Web Security and Filtering**

A more expensive commercial solution for Web Server Security, however, offers a more robust set of tools and options.

Graphical user interface, text, application, email

Description automatically generated

### **Enforce Corporate Policies**

Increase productivity, regulate bandwidth usage and prevent risky behavior by enforcing granular policies on user activities. The Barracuda Web Security Gateway can control access to websites, applications, and Web 2.0 platforms based on users, groups, time, bandwidth, and other criteria. SSL-filtering and inspection capabilities provide policy enforcement on social media and search platforms that are otherwise obfuscated.

### **Protect Against Web-Based Threats**

Keep networks and users safe by blocking spyware downloads, preventing viruses, and restricting requests to malicious websites by leveraging intelligence from thousands of collection points worldwide. Our award-winning antivirus and anti-spyware technologies combine preventive, proactive, and reactive measures to deliver industry-leading content filtering and malware protection.

### **Monitor Network and User Activity**

Gain complete insight into user activity and network threats via an intuitive dashboard and integrated reporting. This clear visibility lets administrators create effective policies and generate proactive alerts to properly respond to threats.

The Barracuda Reporting Server is a powerful platform that enables unified reporting for Barracuda Web Security Gateways. Designed to meet the demands of reporting on increasing amounts of user and security data, the Barracuda Reporting Server generates accurate, customizable reports in a fraction of the time that it takes built-in reporting engines, while also enabling aggregated reports for multiple connected devices.

*\*Price of service is dependent on the evaluation of ACME’s current network layout and security needs.*

Conclusion

This concludes the capstone project. This is all of the required documentation we created for this project as it was delivered individually. This overall project was a free-form exercise, built to simulate what may be a real-world scenario as we enter the workforce. All parts of this capstone relied on access to a virtual network provided to us by SecureSet School. All observations documented above are our own using the lab environment provided, and are actual recommendations based on the curriculum and individual research.

It was a pleasure to work on this project and helped each of us feel like we were ready to do this for real. Big thanks to all of our instructors for their genuine love of passing on their knowledge and helping us, help ourselves.