Enough Security Consulting

February, 2023

Table of Contents

Confidentiality

This report is confidential and proprietary to *ACME Company*, and any disclosure, distribution, copying, or use of this report, in whole or in part, by any party other than *ACME Company* without the prior written consent of *Enough Security Consulting* is strictly prohibited. *Enough Security Consulting* warrants due care and diligence in the preparation of this report, but is not responsible for any damages, losses, or expenses incurred by any party arising from the use or reliance upon the information contained in this report. By accepting this report, *ACME Company* agrees to indemnify, defend, and hold harmless *Enough Security Consulting* from any and all claims arising from the use or reliance upon this report.

Disclaimer

The cybersecurity consulting services provided by *Enough Security Consulting* aim to improve the information security posture of *ACME Company*. However, no security measures can guarantee absolute protection against all possible security threats.

Enough Security Consulting will use its expertise to assess *ACME Company*'s security posture, identify potential vulnerabilities, and suggest improvements. However, *Enough Security Consulting* cannot guarantee that all vulnerabilities will be identified or that its recommendations will prevent all possible security incidents.

ACME Company assumes all risks associated with the implementation and management of its information security program. By engaging *Enough Security Consulting*, *ACME Company* agrees to assume all risks and acknowledges that any actions taken in response to the recommendations provided by *Enough Security Consulting* are *ACME Company*'s responsibility.

Point Of Contact Information

Lucas Parada	*774-722-9505*	*lucasparadap@gmail.com*

Executive Summary

Enough Security Consulting has conducted a comprehensive cyber security engineering report for ACME Company. The assessment identified numerous vulnerabilities, and we strongly recommend immediate action to prevent potential exploits.

During the network scan, our team discovered that there were too many open ports, leaving the network exposed to possible attacks. Additionally, the logs revealed multiple attacks, including web application attacks, code injection, DDOS attacks, and malware. Our analysis also showed that significant system hardening is needed to secure the infrastructure and data.

To enhance the organization's security posture, Enough Security recommends the implementation of a honeypot, specifically Cowrie, to lure and detect attackers. Furthermore, we suggest that the organization adopts Jira as a new internal system method to improve incident response and management.

As part of the recommendations, a plan for network hardening has been included with a detailed timeline for implementation. The plan includes the implementation of updated security policies, procedures, and controls, as well as regular security awareness training for all employees.

Finally, Enough Security strongly recommends a secondary assessment be conducted after the implementation of changes to ensure that the organization's security posture is improved and remains effective over time.

In conclusion, our cyber security engineering report highlights that ACME Company faces significant cyber security risks that require urgent attention. Our recommendations aim to address the vulnerabilities, minimize potential risks, maximize process efficiency, and improve the overall security posture of the organization.

ACME Network – Host Discovery

February, 2023

intnet-1: 192.168.10.1, 192.168.10.50, 192.168.10.210 (LAN)

192.168.10.50 – Internal PC1

```
Nmap scan report for 192.168.10.50
Host is up (0.00066s latency).
Not shown: 999 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.9p1 Ubuntu 3 (Ubuntu Linux; protocol 2.0)
| ssh hostkey:
|   256 [illegible]fb5603d1d95662caaf4995460c (ECDSA)
|_  256 133d72fb54aa9a3a2570d1ce91169caa (ED25519)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

192.168.10.210 – Internal PC2

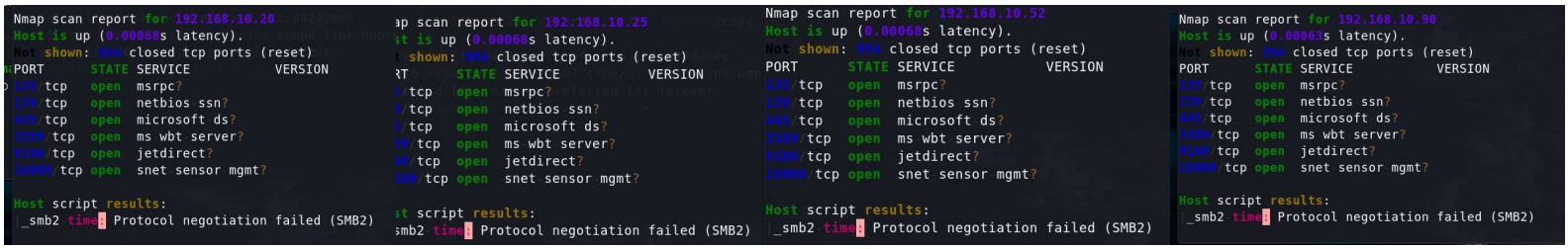
```
Nmap scan report for 192.168.10.210
Host is up (0.00067s latency).
Not shown: 997 closed tcp ports (reset)
PORT    STATE SERVICE     VERSION
22/tcp  open  ssh         OpenSSH 8.9p1 Ubuntu 3 (Ubuntu Linux; protocol 2.0)
| ssh hostkey:
|   256 b2c4498b91e40ab4dea45116d59432e0 (ECDSA)
|_  256 d28ace9528a5ac2ed32de8bb3b72d363 (ED25519)
139/tcp open  netbios ssn Samba smbd 4.6.2
445/tcp open  netbios ssn Samba smbd 4.6.2
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
| smb2 security mode:
|   311:
|_    Message signing enabled but not required
| smb2 time:
|   date: 2023-02-13T18:01:18
|_  start_date: N/A
|_nbstat: NetBIOS name: ACMEPC1, NetBIOS user: <unknown>, NetBIOS MAC: 000000000000 (Xerox)
```

intnet-1 (LAN) Peripheral Devices:

192.168.10.20, 192.168.10.25, 192.168.10.52, 192.168.10.90, 192.168.10.180, 192.168.10.181

(all hosts have same ports open – first 4 host screenshots included)



intnet-2: 192.168.20.100, 192.168.20.222 (DMZ)

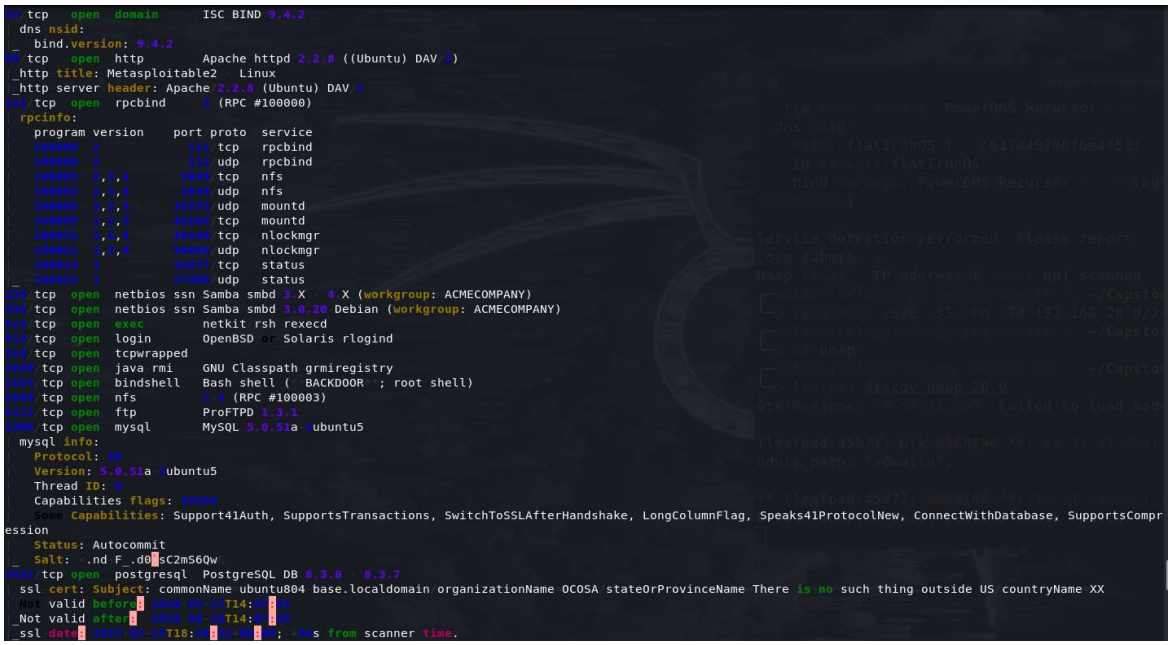
192.168.20.100 – ACME Web Server

```
Nmap scan report for 192.168.20.100
Host is up (0.00090s latency).
Not shown: 999 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
80/tcp open  http    Apache httpd 2.4.52 ((Ubuntu))
|_http-server-header: Apache/2.4.52 (Ubuntu)
|_http-title: ACME Intranet
```

192.168.20.222 – ACME DMZ Server

```
Nmap scan report for 192.168.20.222
Host is up (0.00048s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to 192.168.30.205
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      vsFTPd 2.3.4 - secure, fast, stable
|_End of status
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
| ssh-hostkey:
|   1024 600fcfe1c05f6a74d69024fac4d56ccd (DSA)
|_  2048 5656240f211ddea72bae61b1243de8f3 (RSA)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
| ssl-cert: Subject: commonName ubuntu804.base.localdomain organizationName OCOSA stateOrProvinceName There is no such thing outside US countryName XX
| Not valid before: 2010-03-17T14:07:45
|_Not valid after:  2010-04-16T14:07:45
|_ssl-date: 2023-01-17T18:40:27+00:00; +2m0s from scanner time.
|_smtp-commands: metasploitable.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME, DSN
| sslv2:
|   SSLv2 supported
|   ciphers:
|     SSL2_DES_64_CBC_WITH_MD5
|     SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
|     SSL2_RC4_128_EXPORT40_WITH_MD5
|     SSL2_RC2_128_CBC_WITH_MD5
|     SSL2_RC4_128_WITH_MD5
|_    SSL2_DES_192_EDE3_CBC_WITH_MD5
```

(nmap results continues on next page)



intnet-2 (DMZ) Peripheral Devices:

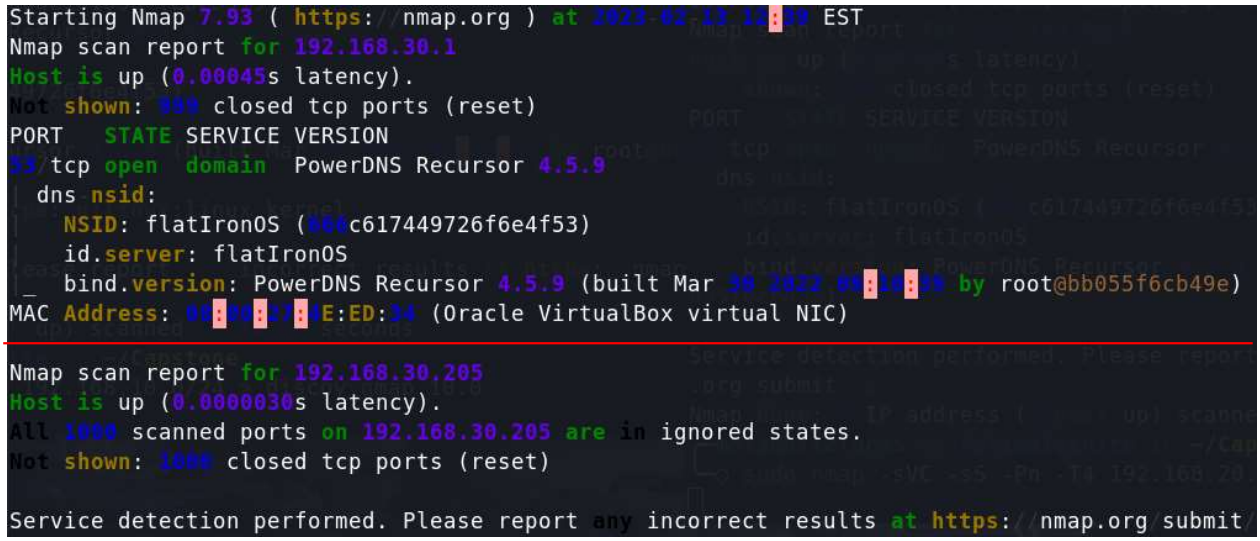
192.168.20.60, 192.168.20.61, 192.168.20.62, 192.168.20.74, 192.168.20.110, 192.168.10.111

(all hosts have same ports open – ".61" host ports included for reference)

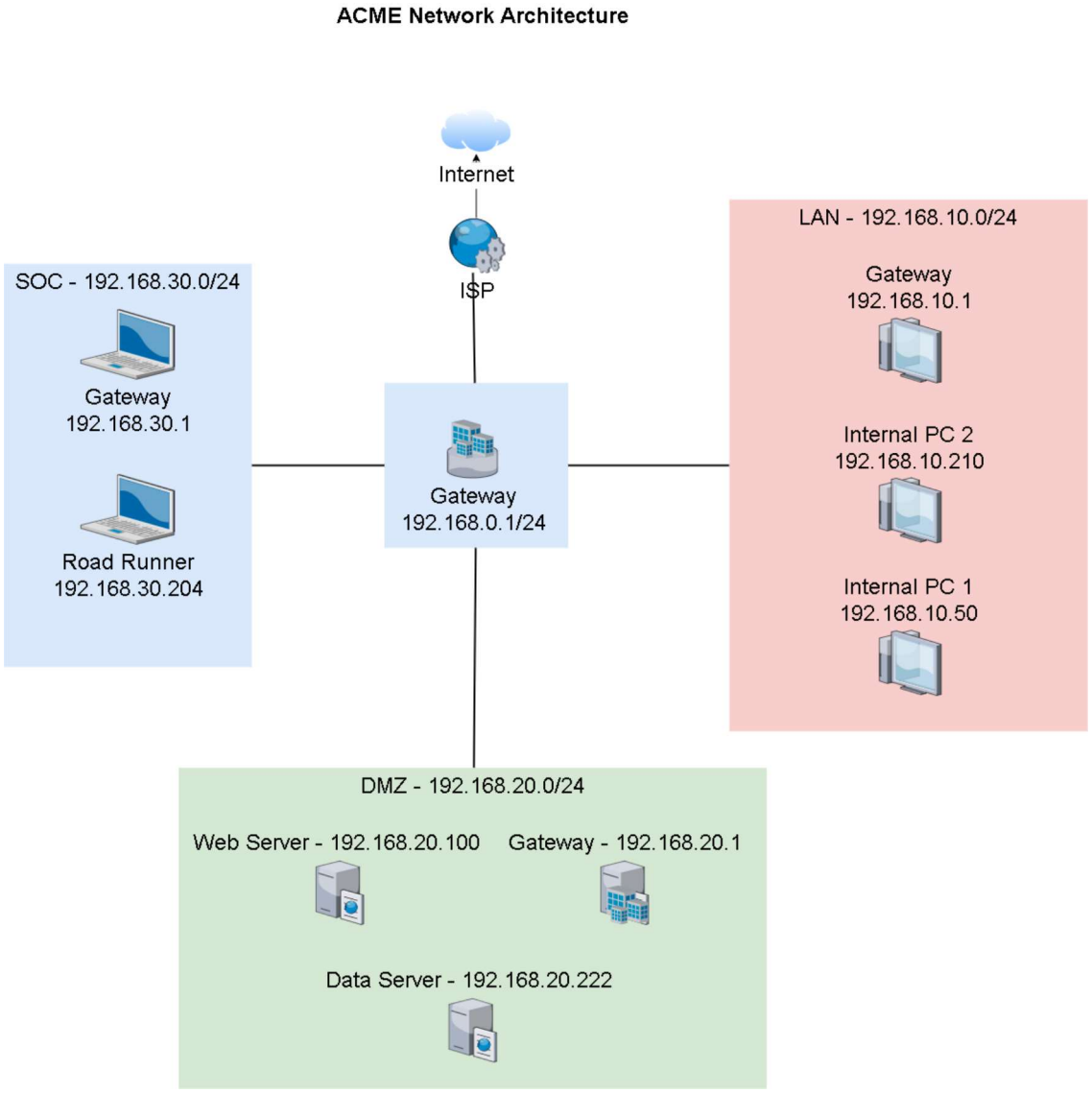
Nmap scan report for 192.168.20.61
Host is up (0.00085s latency).
Not shown: 994 closed tcp ports (reset)
PORT STATE SERVICE VERSION
21/tcp open ftp?
25/tcp open smtp?
|_smtp-commands: Couldn't establish connection on port 25
443/tcp open https?
1723/tcp open pptp?
8080/tcp open http-proxy?
8443/tcp open https-alt?

intnet-3: 192.168.30.1, 192.168.30.205 (SOC)

192.168.30.1 – Router // Gateway
192.168.30.205 – Enough Security Consulting Machine



intnet-3 (SOC) – NO Peripheral Devices



ACME Company Network Diagram

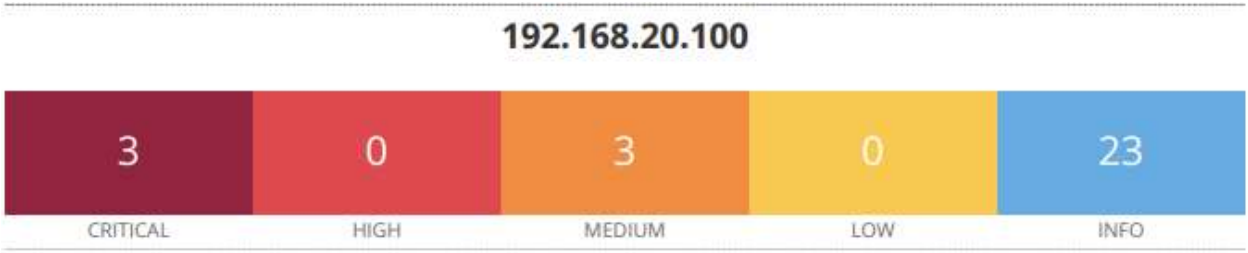
(No Peripheral Devices)

End of Host Discovery

ACME Network – Vulnerability Scan || Assessment

The purpose of this report is to summarize the results of the vulnerability scanning performed on the ACME network infrastructure. While there are many vulnerabilities, many are primarily harmless in that they would not grant an attack access to critical information or systems if penetrated. This report will focus on "High" & "Critical" severity vulnerabilities. Exploitation of these weaknesses could lead to the most substantial and long lasting security crises. Immediate mitigation implementation is recommended.

NESSUS FINDINGS:



Vulnerabilities Total: 29

SEVERITY	CVSS V3.0	PLUGIN	NAME
CRITICAL	9.8	158900	Apache 2.4.x < 2.4.53 Multiple Vulnerabilities
CRITICAL	9.8	161948	Apache 2.4.x < 2.4.54 Multiple Vulnerabilities
CRITICAL	9.0	170113	Apache 2.4.x < 2.4.55 Multiple Vulnerabilities

Summary of Findings - 192.168.20.100:

There are several vulnerabilities contained within these 3 Apache flags. Because ACME is running an outdated web-server it is vulnerable to many attacks. 5 specific weaknesses are listed below:

- ➔ CVE-2021-41773: Path traversal and file disclosure vulnerability.
- ➔ CVE-2021-42013: Remote code execution vulnerability in mod_auth_openidc.
- ➔ CVE-2021-36090: HTTP/2 related denial of service vulnerability.
- ➔ CVE-2021-33193: HTTP/2 related denial of service vulnerability.
- ➔ CVE-2021-31618: NULL pointer dereference vulnerability in mod_auth_digest.

192.168.20.222

10	10	28	7	92
CRITICAL	HIGH	MEDIUM	LOW	INFO

Vulnerabilities Total: 147

SEVERITY	CVSS V3.0	PLUGIN	NAME
CRITICAL	9.8	134862	Apache Tomcat AJP Connector Request Injection (Ghostcat)
CRITICAL	9.8	20007	SSL Version 2 and 3 Protocol Detection
CRITICAL	9.8	125855	phpMyAdmin prior to 4.8.6 SQLi vulnerablity (PMASA-2019-3)
CRITICAL	10.0	33850	Unix Operating System Unsupported Version Detection
CRITICAL	10.0*	32314	Debian OpenSSH/OpenSSL Package Random Number Generator Weakness
CRITICAL	10.0*	32321	Debian OpenSSH/OpenSSL Package Random Number Generator Weakness (SSL check)
CRITICAL	10.0*	11356	NFS Exported Share Information Disclosure
CRITICAL	10.0*	46882	UnrealIRCd Backdoor Detection
CRITICAL	10.0*	61708	VNC Server 'password' Password
CRITICAL	10.0*	10203	rexecd Service Detection
HIGH	8.8	70728	Apache PHP-CGI Remote Code Execution
HIGH	8.8	19704	TWiki 'rev' Parameter Arbitrary Command Execution
HIGH	8.6	136769	ISC BIND Service Downgrade / Reflected DoS
HIGH	7.5	42256	NFS Shares World Readable
HIGH	7.5	42873	SSL Medium Strength Cipher Suites Supported (SWEET32)
HIGH	7.5	90509	Samba Badlock Vulnerability
HIGH	7.5*	59088	PHP PHP-CGI Query String Parameter Injection Arbitrary Code Execution
HIGH	7.5*	36171	phpMyAdmin Setup Script Configuration Parameters Arbitrary PHP Code Injection (PMASA-2009-4)
HIGH	7.5*	10205	rlogin Service Detection
HIGH	7.5*	10245	rsh Service Detection

Summary of Findings - 192.168.20.222**:**

As can be seen there are a significant number of vulnerabilities in this server. The large number of vulnerabilities corresponds to the large number of ports and open services on the server coupled with many of those services running out of date software – much of which has already been identified as significantly compromised by publicly disclosed vulnerabilities.

Critical Vulnerabilities:

- ➔ CVE-2020-1938 (Apache Tomcat AJP Connector Request Injection): A vulnerability in the Apache Tomcat AJP connector that allows remote attackers to read or include files on the server due to an incomplete fix for CVE-2020-1938.
- ➔ CVE-2014-3566 (SSL Version 2 and 3 Protocol Detection): A vulnerability in the SSL/TLS protocol that allows attackers to decrypt encrypted data by exploiting a weakness in the SSLv2 and SSLv3 protocols.
- ➔ CVE-2019-12922 (phpMyAdmin SQLi vulnerability): A SQL injection vulnerability in phpMyAdmin that allows remote attackers to execute arbitrary SQL commands via a specially crafted request.
- ➔ CVE-2018-7692 (Unix Operating System Unsupported Version Detection): A vulnerability in various Unix operating systems that allows local users to determine the existence of files and directories they do not have access to.
- ➔ CVE-2008-0166 (Debian OpenSSH/OpenSSL Package Random Number Generator Weakness): A weakness in the random number generator used by the Debian version of OpenSSH and OpenSSL, which makes it easier for attackers to guess private keys generated by the affected systems.
- ➔ CVE-2015-7575 (Debian OpenSSH/OpenSSL Package Random Number Generator Weakness (SSL check)): A weakness in the random number generator used by the Debian version of OpenSSL that affects the SSL/TLS encryption.
- ➔ CVE-2010-4250 (NFS Exported Share Information Disclosure): A vulnerability in the Network File System (NFS) that allows remote attackers to obtain sensitive information by accessing an NFS-exported file system.
- ➔ CVE-2010-2075 (UnrealIRCd Backdoor Detection): A backdoor in the UnrealIRCd Internet Relay Chat (IRC) daemon that allows attackers to execute arbitrary code with the privileges of the IRC daemon process.
- ➔ CVE-2015-6925 (VNC Server 'password' Password): A vulnerability in the Virtual Network Computing (VNC) server that allows attackers to guess the VNC password via a brute-force attack.

- ➔ CVE-1999-0059 (rexecd Service Detection): A vulnerability in the rexecd service that allows remote attackers to execute arbitrary commands via a buffer overflow attack.

High Vulnerabilities:

- ➔ CVE-2012-1823 (Apache PHP-CGI Remote Code Execution): A vulnerability in the way that Apache handles PHP scripts when using the Common Gateway Interface (CGI) module, which allows remote attackers to execute arbitrary code by sending a specially crafted request.

- ➔ CVE-2006-5876 (TWiki 'rev' Parameter Arbitrary Command Execution): A vulnerability in the TWiki application that allows remote attackers to execute arbitrary commands via the 'rev' parameter in the 'view' script.

- ➔ CVE-2021-25214 (ISC BIND Service Downgrade / Reflected DoS): A vulnerability in the BIND DNS server that allows an attacker to cause a service disruption by sending specially crafted DNS queries that cause a server to downgrade its security level or to perform a reflected denial-of-service (DoS) attack.

- ➔ CVE-2009-2610 (NFS Shares World Readable): A vulnerability in the Network File System (NFS) that allows remote attackers to read sensitive files by accessing an NFS-exported file system.

- ➔ CVE-2016-2183 (SSL Medium Strength Cipher Suites Supported (SWEET32)): A vulnerability in SSL/TLS encryption that allows attackers to perform a man-in-the-middle attack to decrypt session data using the SWEET32 attack.

- ➔ CVE-2016-2118 (Samba Badlock Vulnerability): A vulnerability in the Samba file and print services that allows remote attackers to execute arbitrary code or cause a denial of service (DoS) attack by sending a specially crafted authentication request.

- ➔ CVE-2012-1824 (PHP PHP-CGI Query String Parameter Injection Arbitrary Code Execution): A vulnerability in PHP that allows remote attackers to execute arbitrary code via a query string parameter in a PHP script run by the PHP-CGI module.

- ➔ CVE-2009-1159 (phpMyAdmin Setup Script Configuration Parameters Arbitrary PHP Code Injection): A vulnerability in phpMyAdmin that allows remote attackers to execute arbitrary PHP code via the configuration parameters in the setup script.

- ➔ CVE-1999-0517 (rlogin Service Detection): A vulnerability in the rlogin service that allows remote attackers to execute arbitrary commands via a buffer overflow attack.

- ➔ CVE-1999-0526 (rsh Service Detection): A vulnerability in the rsh service that allows remote attackers to execute arbitrary commands via a buffer overflow attack.

Mitigation Strategies:

1. Upgrade to Apache HTTP Server version 2.4.50 or later, or apply a patch if available. Disable the 'mod_status' / 'mod_cgi' / 'mod_proxy' module if it is not required.

2. Apply patches to all or upgrade OS, software, and directory systems to close vulnerabilities in out-dated versions. This includes Linux Kernel patches, Windows updates, Ubuntu patches, Microsoft Exchange Server upgrades, OpenSSL upgrades, F5 BIG-IP, VMware vCenter Server, and Citrix ADC/Netscaler upgrading.

3. Disable SSLv2 and SSLv3, and use strong encryption ciphers instead.

4. Remove any unnecessary services, applications, or modules to reduce the attack surface.

5. Use strong and unique passwords, and enforce multi-factor authentication where possible.

6. Use network segmentation and firewalls to limit access to critical systems and services.

7. Regularly monitor and analyze system logs and network traffic for signs of suspicious activity.

8. Restrict file and directory permissions to limit access to sensitive data.

9. Regularly back up critical data and systems, and test the backups to ensure they can be restored.

10. Use intrusion detection and prevention systems to detect and block attacks in real-time.

11. Educate users on safe computing practices, such as avoiding suspicious emails and links, and not reusing passwords.

End of Vulnerability Assessment

ACME Network – Log File Review

Brocade Logs:

No Pertinent Security Information

Firewall Log Highlights:

(1/27/23-2/10/23)

	First Normal Date	Last Normal Date	Vendor Message ID	Group	Impacted Host	Object Name	URL	Command	Process	Process ID	Severity
2	12/14/99 01:23:00 PM	12/14/99 01:49:00 PM		QLB Production Servers	192.168.10.111	GoogleUpdateSetup.exe		None	Distributed ThreatRadar - Malicious IPs		High
3	12/14/99 01:07:00 PM	12/14/99 01:57:29 PM	40031	INT	192.168.153.9	GoogleUpdateSetup.exe		reset-both	unknown		High
4	12/14/99 01:14:00 PM	12/14/99 01:48:56 PM	40031	INT	192.168.4.111	RdrServicesUpdater.exe		reset-both	unknown		High
5	12/14/99 12:57:00 PM	12/14/99 01:25:29 PM	40031	INT	192.168.76.21	GoogleUpdateSetup.exe		reset-both	unknown		High
6	12/14/99 12:59:00 PM	12/14/99 01:48:51 PM	40031	INT	192.168.76.75	GoogleUpdateSetup.exe		reset-both	unknown		High
7	12/14/99 01:49:00 PM	12/14/99 01:58:51 PM	40031	INT	192.168.32.60	GoogleUpdateSetup.exe		reset-both	unknown		High
8	12/14/99 01:13:00 PM	12/14/99 01:57:04 PM	40031	INT	192.168.11.74	GoogleUpdateSetup.exe		reset-both	unknown		High
9	12/14/99 01:13:00 PM	12/14/99 01:57:23 PM	40031	INT	192.168.8.72	GoogleUpdateSetup.exe		reset-both	unknown		High
10	12/13/99 02:12:00 AM	12/13/99 02:12:52 AM	30861	REMOTEUSERS	192.168.3.5	GoogleUpdateSetup.exe		reset-both	any		informational
11	12/14/99 12:59:00 PM	12/14/99 12:59:50 PM	30861	REMOTEUSERS	192.168.25.18	GoogleUpdateSetup.exe		reset-both	any		informational
12	12/14/99 01:08:00 PM	12/14/99 01:08:12 PM	30861	REMOTEUSERS	192.168.33.170	GoogleUpdateSetup.exe		reset-both	any		informational

	Group	Impacted Host	Object Name	URL	Command
2	Apache Header Injection	192.168.0.15	GoogleUpdateSetup.exe		reject
3	Microsoft Exchange OWA cross-site scripting and spoofing (MS04-026)	192.168.0.102	srvsvc		monitor
4	Linux System Files Information Disclosure	192.168.0.102	reset-both		monitor
5	Web Servers Malicious URL Directory Traversal	192.168.10.107	deny		monitor
6	Failed to generate IP packet from fragments	192.168.10.109	GoogleUpdateSetup.exe		drop
7	CGI Namespace Conflict Man-In-The-Middle (httpoxy)	192.168.10.109	GoogleUpdateSetup.exe		monitor
8	Microsoft Exchange OWA cross-site scripting and spoofing (MS04-026)	192.168.10.109	GoogleUpdateSetup.exe		monitor
9	Linux Shellcode Remote Code Execution	192.168.10.109	GoogleUpdateSetup.exe		monitor
10	Microsoft Exchange OWA cross-site scripting and spoofing (MS04-026)	192.168.10.109	GoogleUpdateSetup.exe		monitor
11	NULL Encoding detected within a HTTP request	192.168.10.109	GoogleUpdateSetup.exe		monitor
12	Failed to generate IP packet from fragments	192.168.10.109	GoogleUpdateSetup.exe		drop
13	Apache HTTP Server Header Injection Cross-Site Scripting	192.168.10.110	GoogleUpdateSetup.exe		monitor
14	Web Servers Malicious Encoding Directory Traversal	192.168.10.110	GoogleUpdateSetup.exe		monitor
15	OpenSSL TLS DTLS Overly-long Heartbeat Response Information Disclosure	192.168.10.110	GoogleUpdateSetup.exe		monitor
16	Microsoft IIS WebDAV Remote Buffer Overflow (MS03-007) - Ver2	192.168.10.110	GoogleUpdateSetup.exe		monitor
17	Microsoft IIS idq.dll IDAIDQ ISAPI Overflow Buffer Overflow - Ver2	192.168.10.110	GoogleUpdateSetup.exe		monitor
18	Web Servers Malicious URL Directory Traversal	192.168.10.110	GoogleUpdateSetup.exe		monitor
19	Apache HTTP Server Header Injection Cross-Site Scripting	192.168.10.110	GoogleUpdateSetup.exe		monitor
20	Microsoft Exchange OWA cross-site scripting and spoofing (MS04-026)	192.168.10.110	GoogleUpdateSetup.exe		monitor
21	Failed to generate IP packet from fragments	192.168.10.110	GoogleUpdateSetup.exe		drop
22	Web Servers Malicious URL Directory Traversal	192.168.10.110	GoogleUpdateSetup.exe		monitor
23	Web Servers Malicious URL Directory Traversal	192.168.10.110	GoogleUpdateSetup.exe		monitor
24	Apache Header Injection	192.168.10.110	GoogleUpdateSetup.exe		reject
25	PHP Easter Egg Information Disclosure	192.168.10.110	GoogleUpdateSetup.exe		monitor
26	NULL Encoding detected within a HTTP request	192.168.10.110	GoogleUpdateSetup.exe		monitor
27	SENKAS Kolibri Webserver GET Request Buffer Overflow	192.168.10.110	GoogleUpdateSetup.exe		monitor
28	NULL Encoding detected within a HTTP request	192.168.10.110	GoogleUpdateSetup.exe		monitor
29	Linux System Files Information Disclosure	192.168.10.110	GoogleUpdateSetup.exe		monitor
30	Apache Header Injection	192.168.10.110	GoogleUpdateSetup.exe		reject
31	Apache HTTP Server Header Injection Cross-Site Scripting	192.168.10.110	GoogleUpdateSetup.exe		monitor
32	Apache Header Injection	192.168.10.110	GoogleUpdateSetup.exe		reject
33	Email Parameter Cross-Site Scripting	192.168.10.110	GoogleUpdateSetup.exe		monitor
34	Linux System Files Information Disclosure	192.168.10.110	GoogleUpdateSetup.exe		monitor
35	Web Servers Malicious URL Directory Traversal	192.168.10.110	GoogleUpdateSetup.exe		monitor
36	Linux Shellcode Remote Code Execution	192.168.10.110	GoogleUpdateSetup.exe		monitor
37	Apache HTTP Server Header Injection Cross-Site Scripting	192.168.10.110	GoogleUpdateSetup.exe		monitor

Based on the log files analyzed, the following events indicate suspicious activity:

Apache Server Protection Violation

Date: 01/29/23 05:51:17 PM
Impacted Host: 192.168.0.15
Object Name: GoogleUpdateSetup.exe
Vendor Message ID: Apache Header Injection
Details: The log file indicates that there was a violation of Apache server protection due to header injection, where the client was able to inject malicious code into the header of the request to the server. This activity could be an attempt to exploit a vulnerability in the server or to gain unauthorized access.

Web Server Enforcement Violation

Date: 01/29/23 04:25:44 PM
Impacted Host: 192.168.10.109
Object Name: GoogleUpdateSetup.exe
Vendor Message ID: Microsoft Exchange OWA cross-site scripting and spoofing (MS04-026)
Details: The log file indicates that there was a violation of web server enforcement due to a cross-site scripting and spoofing vulnerability in Microsoft Exchange OWA. This activity could be an attempt to exploit the vulnerability in the server or to gain unauthorized access.

IP Fragments

Date: 01/29/23 05:08:00 PM
Impacted Host: 192.168.10.109
Object Name: GoogleUpdateSetup.exe
Vendor Message ID: Failed to generate IP packet from fragments
Details: The log file indicates that there was an issue with generating IP packets from fragments, which could indicate an attempt to evade detection by breaking up packets into smaller fragments.

Web Server Enforcement Violation

Date: 01/29/23 10:00:19 PM
Impacted Host: 192.168.10.109
Object Name: GoogleUpdateSetup.exe
Vendor Message ID: CGI Namespace Conflict Man-In-The-Middle (httpoxy)
Details: The log file indicates that there was a violation of web server enforcement due to a CGI Namespace Conflict Man-In-The-Middle (httpoxy) vulnerability. This activity could be an attempt to exploit the vulnerability in the server or to gain unauthorized access.

Content Protection Violation

Date: 01/29/23 03:16:35 PM
Impacted Host: 192.168.10.109
Object Name: GoogleUpdateSetup.exe
Vendor Message ID: Linux Shellcode Remote Code Execution

Details: The log file indicates that there was a violation of content protection due to remote code execution using Linux shellcode. This activity could be an attempt to exploit a vulnerability in the server or to gain unauthorized access.

IP Fragments

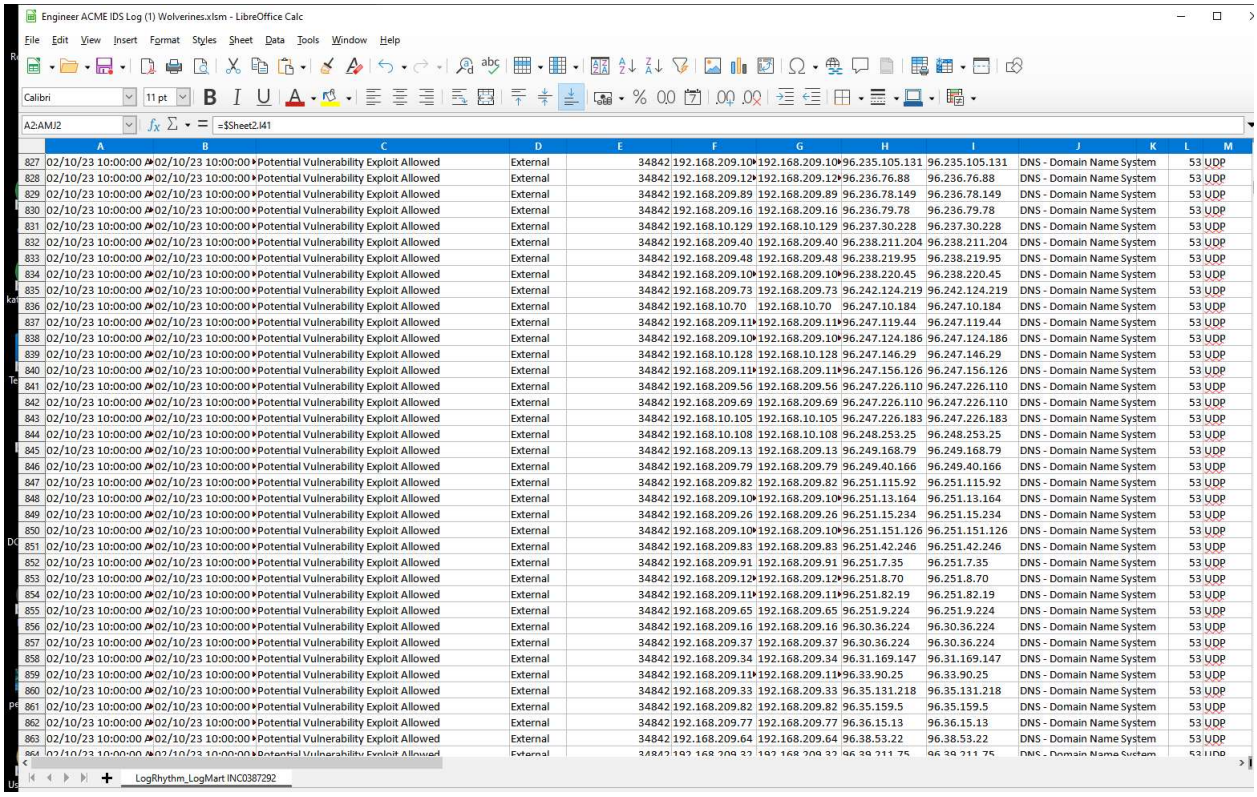
Date: 01/29/23 05:02:00 AM
Impacted Host: 192.168.10.109
Object Name: GoogleUpdateSetup.exe
Vendor Message ID: Failed to generate IP packet from fragments
Details: The log file indicates that there was an issue with generating IP packets from fragments, which could indicate an attempt to evade detection by breaking up packets into smaller fragments.

Apache Server Protection Violation

Date: 01/29/23 03:16:35 PM
Impacted Host: 192.168.10.110
Object Name: GoogleUpdateSetup.exe
Vendor Message ID: Apache HTTP Server Header Injection Cross-Site Scripting
Details: The log file indicates that there was a violation of Apache server protection due to cross-site scripting in the HTTP header. This activity could be an attempt to exploit a vulnerability in the server or to gain unauthorized access

IDS Log Highlights:

(2/10/23-2/12/23)



	Origin Host	Origin Host IP	Impacted Host	Impacted Host IP	Impacted Application	SPort	DPort	Protocol	Login	Account	Group
2	198.148.91.206	198.148.91.206	192.168.10.106	192.168.10.106					bgschneider		DefaultWEBVPNGroup
3	94.102.56.238	94.102.56.238	192.168.10.106	192.168.10.106					tbeitler		DefaultWEBVPNGroup
4	185.94.111.1	185.94.111.1	192.168.10.105	192.168.10.105					zlbyrd		DefaultWEBVPNGroup

Based on the log files provided, the following events have been flagged a substantial number of times and should be considered suspicious:

Detected Spyware Activity on Outbound traffic from several IP addresses to unknown UDP ports. For instance, on 02/10/23 at 12:00:00 PM, there was outbound traffic from 192.168.209.12 to an unknown UDP port on 1.84.89.211, which is an IP address that is not recognized. Similarly, on 02/10/23 at 10:00:00 AM, there was outbound traffic from 192.168.10.15 to an unknown UDP port on 1.9.119.125. This type of traffic is indicative of spyware activity, as it suggests that some unknown software is attempting to communicate with an external server.

Similarly, spyware activity has been detected on several IP addresses connecting to known DNS ports. For instance, on 02/10/23 at 11:00:00 AM, there was outbound traffic from 94.102.56.238 to port 53 (DNS) on 192.168.10.100. This type of traffic is also indicative of spyware activity, as it suggests that some unknown software is attempting to communicate with a DNS server in order to resolve domain names.

Invalid Transport Field: External traffic to unknown TCP ports. For instance, on 02/11/23 at 8:00:00 AM, there was external traffic from 103.195.100.26 to an unknown TCP port on 192.168.10.105. Similarly, on 02/10/23 at 10:00:00 PM, there was external traffic from 94.102.56.238 to an unknown TCP port on 192.168.10.105. This type of traffic is indicative of attempts to exploit vulnerabilities in network protocols or devices.

IPv6 Send Message Failed: Failed attempts to send IPv6 messages from internal IP addresses to unknown destinations. For instance, on 02/10/23 at 2:00:00 PM, there was a failed attempt to send an IPv6 message from 192.168.10.105 to an unknown destination on 185.94.111.1. Similarly, on 02/10/23 at 3:00:00 PM, there were failed attempts to send IPv6 messages from 192.168.10.106 to unknown destinations on 198.148.91.206 and 94.102.56.238. These failed attempts suggest that some unknown software or device is attempting to communicate with external entities using IPv6, which could potentially be used to bypass security measures that are designed to monitor IPv4 traffic.

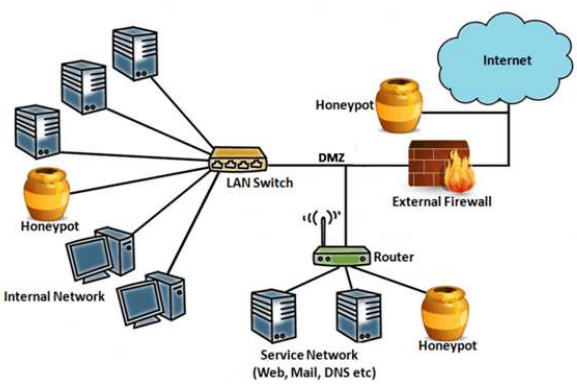
Potential Vulnerability Exploit Allowed: This log indicates a potential vulnerability exploit allowed, which means an attempt was made to exploit a vulnerability in the system. In this case, the exploit was allowed, which means the attacker was able to gain access to the system. It was noticed by Enough Security that the trajectory of applications affected by the “potential vulnerabilities exploit allowed” flag, progressed from web application protocols such as HTTP, HTTPS, IMAP, and SMTP, to server programs and directory systems, and ending with successful SSH shells. This could be an indication that malware has successfully infiltrated the ACME network, or potentially that someone has been able to gain access by manually hacking. Either way, these indicate the network has been compromised.

End of Log Security + Threat Analysis

ACME Company Internal Honeypot System Recommendation

Enough Consulting recommends a Cowrie based honeypot to help detect present and deflect future attacks. A honeypot is a contained, safe, and highly monitored shell that is designed to fool an attacker into thinking they have a true foothold on their target machine. Once the attacker 'falls' into the honeypot, all activity is logged for later review by security analysts. ACME's Security Team can then use info gathered via the honeypot to harden systems in accordance with attack vectors used to gain access to cowrie and block the IP of an attacker. Furthermore we recommend placing cowrie inside the ACME network. This will ensure that internal threats can be identified. The more traditional method of only placing a honeypot between a web application and the exterior of the company network can be effective when trying to defend against outside attacks. However IDS log data in the previous section indicates that internal threats may be present and therefore the honeypot placement should reflect that possibility.

Cowrie is a good solution for ACME because it can utilize SSH and Telnet services which are already in use on multiple ACME machines (image below to illustrate) - this will help the honeypot blend in. Setting the honeypot up will consume about 8 hours of Security Engineer labor or other qualified IT personnel to configure. Cowrie itself is open source software and won't cost anything to use. The total estimated cost of implementation would be $360 (based on the wage of $45/hour * 8 hours to complete the work). Some tools the analyst will need to set up the honeypot are; A Linux machine with ssh and telnet services installed, port management tools and escalated privileges on the honey pot machine. Based on our asset discovery performed, Enough Security believes it will be possible to adapt one of ACME's currently under-utilized linux machines for this purpose.



End of Honeypot System Recommendation

ACME Company – Internal Ticketing System Recommendation

Recommended System: Atlassian Jira Service Management.

Budget: $89,500 annually for the Premium Package (based on 250 users)

Architecture Needed: Zero – No servers or database needed due to Cloud Based Provider. Due to various offices around the globe a Cloud Based Provider will work best for all employees to access regardless of location.

Reasoning: Currently there is no internal ticketing system in place at ACME Company. By not having a centralized ticketing system ACME limits its ability to track, organize, and systematically address IT issues as they arise. By implementing the use of Atlassian's Jira Service Management we can improve in the following ways:

1. Increased efficiency: Jira Service Management streamlines the service management process, allowing teams to manage requests and incidents in one centralized platform. This helps teams resolve issues faster and improves overall productivity.
2. Better visibility: Jira Service Management provides real-time insights into the status of requests and incidents, helping teams prioritize their workload and ensuring that nothing falls through the cracks.
3. Customizable workflows: Jira Service Management offers flexible workflows that can be customized to fit the specific needs of a team or organization. This makes it possible to automate repetitive tasks, freeing up time for more important work.
4. Improved collaboration: Jira Service Management enables teams to collaborate effectively, regardless of location or time zone. Teams can easily communicate and share information, reducing the time it takes to resolve issues.
5. Integration with other tools: Jira Service Management integrates with a wide range of tools, including other Atlassian products, making it possible to work seamlessly across multiple tools and platforms.
6. Customer-focused: Jira Service Management puts the customer at the center of the service management process, ensuring that their needs and requests are addressed quickly and efficiently.

End of Internal Ticketing System Recommendation

ACME Company

Security Plan with Timelines

Below is a list of the resolutions based on the vulnerability scan to the ACME Company. The strategies are listed in increments of fixes & mitigations within 90 days, 6 months, and 12-18 months.

Column Definitions:

- ➔ **Cost of Control**
  - ◆ based on the estimated financial cost of implementing the security control
- ➔ **Quick Win?**
  - ◆ indicates if the security control can be implemented quickly and easily to provide immediate benefit.
- ➔ **Resources**
  - ◆ indicates which department or team will be responsible for implementing the security control.
- ➔ **Employee Impact**
  - ◆ rates the potential impact on employees, ranging from low to high.

Within the next 90 Days

Security Control Measure	Cost of Control	Quick Win?	Resources	Initial Cost	Maintencance	Complexity	Employee Impact
Upgrade Apache to version 2.4.55 or later to address multiple vulnerabilities.	Low	Yes	IT Team	Moderate	Low	Moderate	Low
Upgrade phpMyAdmin to version 4.8.6 or later to address SQLi vulnerability (PMASA-2019-3).	Low	Yes	IT Team	Low	Low	Low	Low
Apply the appropriate hotfix for TWiki 'rev' Parameter Arbitrary Command Execution vulnerability.	Low	Yes	IT Team	Low	Low	Low	Low

Within the next 6 Months

Security Control Measure	Cost of Control	Quick Win?	Resources	Initial Cost	Maintencance	Complexity	Employee Impact
Upgrade BIND to version 9.11.22, 9.16.6, or 9.17.4 or later to address DoS vulnerability.	Moderate	Yes	IT Team	High	Low	High	Low
Upgrade Samba to version 4.2.11 / 4.3.8 / 4.4.2 or later to address Badlock vulnerability.	Moderate	Yes	IT Team	High	Low	Moderate	Low

Within the next 12-18 Months

Security Control Measure	Cost of Control	Quick Win?	Resources	Initial Cost	Maintencance	Complexity	Employee Impact
Upgrade Apache Tomcat to version 4.1.40 / 5.5.28 / 6.0.20 or later to address Tomcat Sample App cal2.jsp 'time' Parameter XSS.	High	No	IT Team	High	Low	High	Moderate
Re-download UnrealIRCd software, verify it using published MD5 / SHA1 checksums, and re-install it to address Backdoor Detection vulnerability.	Low	Yes	IT Team	Low	Low	Low	Low

Conclusion:

Put succinctly, the primary ACME security issue is the age of its IT infrastructure. While much of this technology may have been secure when it was first installed, in the time that has passed many vulnerabilities have been identified and subsequently exploited. Failure to install patches/updates/upgrades has also furthered infrastructure's insecurity. Doing a full upgrade on all systems, software, firmware, kernels, and IOT devices will eliminate a huge portion of ACME's current vulnerabilities. Specific vulnerability mitigation tactics can be found on page 14 and the scheduled plan to address certain fixes can be found on pages 22-23. The implementation of the suggested methods would ensure maximum protection from external threats and internal settings. We emphasize the need to consider PILP or "principle of least privilege. No employee should have more access and permission settings than needed to effectively do their job. Setting up the company directory system that way will help to prevent sensitive data slipping into the hands of people who shouldn't have access to it. Additional tuning of the IDS and the implementation of a SIEM would increase security visibility and incident response capabilities. A SIEM could centralize, automate, and track a lot of the security efforts needed. It would also help ensure the future success of security engineers and analysts at ACME. Password strength and frequency of required change policy hardening is encouraged. Credentials observed in logs are short and would be easy to brute-force crack. The implementation of a ticketing system will greatly improve the understanding and efficiency of ACME's IT team. This will mean more system functionality throughout the company and insight as to what systems are regularly causing problems; be them technical or security-related. Overall – ACME servers in their current state should be considered insecure. If an attacker wanted to gain access, it **would** be possible without much difficulty. Therefore it is the recommendation of Enough Security Consulting that ACME take action immediately. While the cost to overhaul the system will be significant, it will be less significant than a full compromise of the ACME servers which could cause irreparable harm to the brand and significant financial loss. Lastly, it is the opinion of Enough Security Consulting that a secondary assessment, combined with a penetration test would be the best way to test the upgraded security infrastructure. The above assessment takes only current systems and settings into consideration. Upon installation of new systems and upgrades, new loopholes and security issues may arise. Testing at the start of a new system and then intermittently afterwards is the strongest way to ensure security is staying current as technology and hackers get more sophisticated.

(Page Intentionally Left Blank)

END OF REPORT