

**Penetration Testing Report**

**HTB POV**

**Acme Corporation**

February 16, 2024

**Table of Contents**

[Statement of Confidentiality 3](#__RefHeading___Toc857_577955523)

[Engagement Contacts 4](#__RefHeading___Toc859_577955523)

[Executive Summary 5](#__RefHeading___Toc861_577955523)

[Approach 5](#__RefHeading___Toc3147_102085782)

[Scope 6](#__RefHeading___Toc863_577955523)

[In-Scope Assets 6](#__RefHeading___Toc3149_102085782)

[Assesment Overview and Recommendations 6](#__RefHeading___Toc3151_102085782)

[Penetration Test Assesment Summary 7](#__RefHeading___Toc865_577955523)

[Summary of Findings 7](#__RefHeading___Toc3153_102085782)

[[Internal/External] Network Compromise Walkthrough 8](#__RefHeading___Toc3155_102085782)

[Detailed Walkthrough 8](#__RefHeading___Toc3157_102085782)

Remediation [Summary 10](#__RefHeading___Toc3159_102085782)

[Short Term 10](#__RefHeading___Toc3161_102085782)

[Medium Term 10](#__RefHeading___Toc3163_102085782)

[Long Term 10](#__RefHeading___Toc3165_102085782)

[Technical Findings Details 11](#__RefHeading___Toc3167_102085782)

[Appendices 18](#__RefHeading___Toc3175_102085782)

[Appendix A – Finding Severities 18](#__RefHeading___Toc3177_102085782)

[Appendix B – Host & Service Discovery 19](#__RefHeading___Toc3179_102085782)

[Appendix C – Subdomain Discovery 20](#__RefHeading___Toc3183_102085782)

[Appendix D – Exploited Hosts 21](#__RefHeading___Toc3185_102085782)

[Appendix E – Compromised Users 22](#__RefHeading___Toc3187_102085782)

[Appendix F – Changes/Host Cleanup 23](#__RefHeading___Toc3189_102085782)

# Statement of Confidentiality

This pentest report contains sensitive and confidential information regarding the security vulnerabilities and weaknesses identified during the assessment. The report is intended solely for the designated recipient(s) and should not be disclosed, shared, or distributed to any unauthorized individuals or entities without explicit written consent from the organization responsible for commissioning the pentest.

By accessing this report, you acknowledge and agree to the following:

1. **Non-Disclosure:** You shall maintain strict confidentiality of this report and its contents. Do not disclose, reproduce, or distribute any part of this report without proper authorization.
2. **Limited Access:** Limit access to this report to individuals who have a legitimate need to know and are bound by a similar confidentiality agreement or professional code of ethics.
3. **Data Protection:** Safeguard the report and any associated files from unauthorized access, loss, or alteration. Take appropriate measures to protect the confidentiality and integrity of the information contained within.
4. **Responsible Use:** Utilize the information provided in this report solely for the purpose of improving the security posture and addressing the identified vulnerabilities. Do not exploit or misuse the discovered vulnerabilities for any malicious or unauthorized activities.
5. **Legal and Ethical Obligations:** Comply with all applicable laws, regulations, and ethical guidelines governing the handling of confidential information, privacy, and cybersecurity.

Any unauthorized disclosure, misuse, or distribution of this report may have legal and reputational consequences. If you have received this report in error, please notify the responsible party immediately and delete all copies from your systems.

By accessing and using this pentest report, you acknowledge the confidential nature of its contents and agree to abide by the terms outlined above to ensure the protection and integrity of the information contained within.

# Engagement Contacts

|  |  |  |
| --- | --- | --- |
| **Administrator Contacts** | | |
| **Name** | **Title** | **Email** |
| **Astrid Marrow** | Chief Executive Officer | astrid@acme.local |
| Ferdinand Mullins | Chief Technical Officer | ferdinand@acme.local |

|  |  |  |
| --- | --- | --- |
| **Assessor Contact** | | |
| **Name** | **Title** | **Email** |
| Safwan Luban | Security Consultant | toothless5143@gmail.com |

# Executive Summary

This executive summary provides a brief overview of the Network Penetration Test conducted for Acme Ltd., focusing on the evaluation of their externally facing network. The objective of this assessment was to identify security weaknesses, assess their impact on Acme Ltd., document findings comprehensively, and provide actionable remediation recommendations.

## Approach

Safwan Luban performed testing under a “black box” approach from 06/02/2024 to 10/02/2024 without credentials or any advance knowledge of Acme’s externally facing environment with the goal of identifying unknown weaknesses. Testing was performed from a non-evasive standpoint with the goal of uncovering as many misconfigurations and vulnerabilities as possible. Testing was performed remotely from Safwan Luban‘s assessment labs. Each weakness identified was documented and manually investigated to determine exploitation possibilities and escalation potential. Safwan Luban sought to demonstrate the full impact of every vulnerability, up to and including internal domain compromise. If Safwan Luban were able to gain a foothold in the internal network as a result of external network testing, Acme allowed for further testing including lateral movement and horizontal/vertical privilege escalation to demonstrate the impact of an internal network compromise.

# Scope

The scope of this assessment was limited to the externally facing network owned by Acme, with the objective of identifying potential vulnerabilities and weaknesses.

## In-Scope Assets

| **Host/URL/IP Address/Domain** | **Description** |
| --- | --- |
| 10.10.11.213 | Main Machine IP |

Table 1: Scope Details

## Assesment Overview and Recommendations

During the penetration test against Acme, Safwan Luban identified a total of <NUMBER (#)> findings that pose a threat to the confidentiality, integrity, and availability of Acme's information systems. These findings have been categorized into five (5) severity levels: critical, high, medium, low, and informative. Specifically, there were <NUMBER (#)> findings assigned a critical risk rating, <NUMBER (#)> findings assigned a high-risk rating, <NUMBER (#)> findings assigned a medium-risk rating, <NUMBER (#)> findings assigned a low-risk rating, and <NUMBER (#)> findings categorized as informative.

POV, a medium machine on HackTheBox, was vulnerable to Local File Inclusion (LFI) through the "cv download" option. This LFI allowed for the disclosure of the "web.config" file, which in turn exposed the validation key for ASP pages. By manipulating the \_\_VIEWSTATE payload using the validation key, attackers achieved Remote Code Execution (RCE) on the machine. Further exploration within the "sfitz" user's documents folder revealed a "connection.xml" file containing credentials for another user, "alaading." After escalating privileges to "alaading," the attacker discovered the "sedebugprivilege," which was subsequently exploited to gain complete control over the host.

Based on the severity of the findings, it is recommended that Acme creates a remediation plan, prioritizing the high and critical-risk findings for immediate attention according to the needs of the business. Acme should also consider implementing periodic vulnerability assessments if they are not already being performed. Once the issues identified in this report have been addressed, a more collaborative and in-depth Active Directory security assessment may be beneficial. This assessment can help identify additional opportunities to harden the Active Directory environment, making it more challenging for attackers to move within the network and increasing the likelihood of detecting and responding to suspicious activity.

# Penetration Test Assesment Summary

Safwan Luban began all testing activities from the perspective of an unauthenticated user on the internet.

## Summary of Findings

During the course of testing, Safwan Luban uncovered a total of <NUMBER (#)> findings that pose a material risk to Acme’s information systems. The below table provides a summary of the findings by severity level.

| **Finding Severity** | | | | |
| --- | --- | --- | --- | --- |
| **Critical** | **High** | **Medium** | **Low** | **Total** |
| **2** | **5** | **1** | **1** | **9** |

Table 2: Severity Summary

Below is a high-level overview of each finding identified during testing. These findings are covered in depth in the [Technical Findings Details](#_Technical_Findings_Details) section of this report.

| **Finding No.** | **Severity Level** | **Finding Name** |
| --- | --- | --- |
| 1. | **Critical** |  |
| 2. | **Critical** |  |
| 3. | **High** |  |
| 4. | **High** |  |
| 5. | **High** |  |
| 6. | **Medium** |  |
| 7. | **Low** |  |
| 8. | **Info** |  |

Table 3: Finding List

# Network Compromise Walkthrough

During the course of the assessment Safwan Luban was able gain a foothold via the external network, move laterally, and compromise the internal network, leading to full administrative control over the Format Host. The steps below demonstrate the steps taken from initial access to compromise and does not include all vulnerabilities and misconfigurations discovered during the course of testing. Any issues not used as part of the path to compromise are listed as separate, standalone issues in the [Technical Findings Details](#_Technical_Findings_Details_1) section, ranked by severity level. The intent of this attack chain is to demonstrate to Acme the impact of each vulnerability shown in this report and how they fit together to demonstrate the overall risk to the client environment and help to prioritize remediation efforts (i.e., patching two flaws quickly could break up the attack chain while the company works to remediate all issues reported). While other findings shown in this report could be leveraged to gain a similar level of access, this attack chain shows the initial path of least resistance taken by the tester to achieve host compromise.

## Detailed Walkthrough

Safwan Luban performed the following to fully compromise the XX domain.

1. From the Nmap scan found 1 open port 80 and a domain pov.htb.
2. Upon performing a VHOST enumeration found a VHOST named dev.pov.htb.
3. The cv download option is vulnerable to LFI specifically the file parameter.
4. By manipulating the LFI vulnerability it was possible to perform NTLM Theft on the user sfitz but the hash was uncrackable.
5. web.config file was disclosed by abusing the LFI which led to disclosure of the validation key of the ASP.
6. Using the validation key it was possible to generate its own payload containing a reverse shell which helped the attacker to gain RCE over the host at a basic level.
7. From the documents folder of the siftz user a connection.xml file was found for the user alaading.
8. Upon logging in as alaading user it was found out that the user has sedebugprivilege, which was abused later to elevate the privileges to the administrator user.

**Step-by-Step Reproduction of Attack Chain:**

From the initial port scan 1 standard HTTP port(80) was found open on the host which redirects the user to the domain pov.htb.

|  |
| --- |
| $ nmap -sV -Pn -sC --min-rate=5000 10.10.11.251  Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-28 01:01 EST  Nmap scan report for 10.10.11.251  Host is up (0.29s latency).  Not shown: 999 filtered tcp ports (no-response)  PORT STATE SERVICE VERSION  80/tcp open http Microsoft IIS httpd 10.0  |\_http-server-header: Microsoft-IIS/10.0  |\_http-title: pov.htb  Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows  Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .  Nmap done: 1 IP address (1 host up) scanned in 35.62 seconds |

Table 4: Port Scanning

From the VHOST enumeration a new subdomain dev.pov.htb was discovered.

|  |
| --- |
| $ ffuf -H "Host: FUZZ.pov.htb" -u http://pov.htb -w /usr/share/wordlists/SecLists-master/Discovery/DNS/subdomains-top1million-110000.txt -fs 12330  /'\_\_\_\ /'\_\_\_\ /'\_\_\_\  /\ \\_\_/ /\ \\_\_/ \_\_ \_\_ /\ \\_\_/  \ \ ,\_\_\\ \ ,\_\_\/\ \/\ \ \ \ ,\_\_\  \ \ \\_/ \ \ \\_/\ \ \\_\ \ \ \ \\_/  \ \\_\ \ \\_\ \ \\_\_\_\_/ \ \\_\  \/\_/ \/\_/ \/\_\_\_/ \/\_/  v2.1.0-dev  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  :: Method : GET  :: URL : http://pov.htb  :: Wordlist : FUZZ: /usr/share/wordlists/SecLists-master/Discovery/DNS/subdomains-top1million-110000.txt  :: Header : Host: FUZZ.pov.htb  :: Follow redirects : false  :: Calibration : false  :: Timeout : 10  :: Threads : 40  :: Matcher : Response status: 200-299,301,302,307,401,403,405,500  :: Filter : Response size: 12330  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  dev [Status: 302, Size: 152, Words: 9, Lines: 2, Duration: 295ms]  <SNIP> |

# Remediation Summary

1. As a result of this assessment there are several opportunities for Acme to strengthen its external and internal network security. Remediation efforts are prioritized below starting with those that will likely take the least amount of time and effort to complete. Acme should ensure that all remediation steps and mitigating controls are carefully planned and tested to prevent any service disruptions or loss of data.

## Short Term

1. [**Finding 2**] – Set strong (24+ character) passwords on all SPN accounts
2. <FILL IN AS APPROPRIATE>
3. Enforce a password change for all users because of the domain compromise

## Medium Term

1. [**Finding 1**] – Disable LLMNR and NBT-NS wherever possible
2. <FILL IN AS APPROPRIATE>

## Long Term

1. Perform ongoing internal network vulnerability assessments and domain password audits
2. Perform periodic Active Directory security assessments
3. Educate systems and network administrators and developers on security hardening best practices compromise
4. Enhance network segmentation to isolate critical hosts and limit the effects of an internal compromise
5. <FILL IN AS APPROPRIATE>

<FILL IN BASED ON FINDINGS, EXAMPLES LEFT FOR REFERENCE>

# Technical Findings Details

1. LLMNR/NBT-NS Response Spoofing - Critical

|  |  |
| --- | --- |
| 1. **CWE** | 1. [**CWE-522**](https://cwe.mitre.org/data/definitions/522.html) |
| 1. **CVSS 3.1 Score** | 1. 9.5 |
| 1. **Description (Incl. Root Cause)** | 1. By responding to LLMNR/NBT-NS network traffic, adversaries may spoof an authoritative source for name resolution to force communication with an adversary-controlled system. This activity may be used to collect or relay authentication materials. 2. Link-Local Multicast Name Resolution (LLMNR) and NetBIOS Name Service (NBT-NS) are Microsoft Windows components that serve as alternate methods of host identification. LLMNR is based upon the Domain Name System (DNS) format and allows hosts on the same local link to perform name resolution for other hosts. NBT-NS identifies systems on a local network by their NetBIOS name. |
| 1. **Security Impact** | 1. Adversaries can spoof an authoritative source for name resolution on a victim network by responding to LLMNR (UDP 5355)/NBT-NS (UDP 137) traffic as if they know the identity of the requested host, effectively poisoning the service so that the victims will communicate with the adversary-controlled system. If the requested host belongs to a resource that requires identification/authentication, the username and NTLMv2 hash will then be sent to the adversary-controlled system. The adversary can then collect the hash information sent over the wire through tools that monitor the ports for traffic or through Network Sniffing and crack the hashes offline through Brute Force to obtain the plaintext passwords. In some cases where an adversary has access to a system that is in the authentication path between systems or when automated scans that use credentials attempt to authenticate to an adversary-controlled system, the NTLMv2 hashes can be intercepted and relayed to access and execute code against a target system relay step can happen in conjunction with poisoning but may also be independent of it. 2. Several tools exist that can be used to poison name services within local networks such as NBNSpoof, Metasploit, and Responder. |
| 1. **Affected Domain/Host/Endpoint** | 1. ACME.LOCAL |
| 1. **Remediation** | 1. Disable LLMNR and NetBIOS in local computer security settings or by group policy if they are not needed within an environment 2. Use host-based security software to block LLMNR/NetBIOS traffic. Enabling SMB Signing can stop NTLMv2 relay attacks. 3. Network intrusion detection and prevention systems that can identify traffic patterns indicative of MiTM activity can be used to mitigate activity at the network level. 4. Network segmentation can be used to isolate infrastructure components that do not require broad network access. This may mitigate, or at least alleviate, the scope of MiTM activity. |
| 1. **External References** | 1. <https://attack.mitre.org/techniques/T1557/001/> |

1. **Detailed Reproduction Steps:** <SHOW ALL STEPS, NOT JUST A SINGLE SCREENSHOT>

2. LLMNR/NBT-NS Response Spoofing - High

|  |  |
| --- | --- |
| 1. **CWE** | 1. [**CWE-522**](https://cwe.mitre.org/data/definitions/522.html) |
| 1. **CVSS 3.1 Score** | 1. 9.5 |
| 1. **Description (Incl. Root Cause)** | 1. By responding to LLMNR/NBT-NS network traffic, adversaries may spoof an authoritative source for name resolution to force communication with an adversary-controlled system. This activity may be used to collect or relay authentication materials. 2. Link-Local Multicast Name Resolution (LLMNR) and NetBIOS Name Service (NBT-NS) are Microsoft Windows components that serve as alternate methods of host identification. LLMNR is based upon the Domain Name System (DNS) format and allows hosts on the same local link to perform name resolution for other hosts. NBT-NS identifies systems on a local network by their NetBIOS name. |
| 1. **Security Impact** | 1. Adversaries can spoof an authoritative source for name resolution on a victim network by responding to LLMNR (UDP 5355)/NBT-NS (UDP 137) traffic as if they know the identity of the requested host, effectively poisoning the service so that the victims will communicate with the adversary-controlled system. If the requested host belongs to a resource that requires identification/authentication, the username and NTLMv2 hash will then be sent to the adversary-controlled system. The adversary can then collect the hash information sent over the wire through tools that monitor the ports for traffic or through Network Sniffing and crack the hashes offline through Brute Force to obtain the plaintext passwords. In some cases where an adversary has access to a system that is in the authentication path between systems or when automated scans that use credentials attempt to authenticate to an adversary-controlled system, the NTLMv2 hashes can be intercepted and relayed to access and execute code against a target system relay step can happen in conjunction with poisoning but may also be independent of it. 2. Several tools exist that can be used to poison name services within local networks such as NBNSpoof, Metasploit, and Responder. |
| 1. **Affected Domain** | 1. ACME.LOCAL |
| 1. **Remediation** | 1. Disable LLMNR and NetBIOS in local computer security settings or by group policy if they are not needed within an environment 2. Use host-based security software to block LLMNR/NetBIOS traffic. Enabling SMB Signing can stop NTLMv2 relay attacks. 3. Network intrusion detection and prevention systems that can identify traffic patterns indicative of MiTM activity can be used to mitigate activity at the network level. 4. Network segmentation can be used to isolate infrastructure components that do not require broad network access. This may mitigate, or at least alleviate, the scope of MiTM activity. |
| 1. **External References** | 1. <https://attack.mitre.org/techniques/T1557/001/> |

1. **Detailed Reproduction Steps:** <SHOW ALL STEPS, NOT JUST A SINGLE SCREENSHOT>

3. Insecure File Shares - Medium

|  |  |
| --- | --- |
| 1. **CWE** | 1. [**CWE-284**](https://cwe.mitre.org/data/definitions/284.html) |
| 1. **CVSS 3.1 Score** | 1. 6.2 |
| 1. **Description (Incl. Root Cause)** | 1. The tester uncovered multiple file shares where all Domain Users have read/write access. |
| 1. **Security Impact** | 1. An attacker who gains a foothold in this domain can use this access to search for files containing sensitive data such as credentials and potentially write malicious files to the file shares. |
| 1. **Affected Domain** | 1. ACME.LOCAL |
| 1. **Remediation** | 1. Review file share privileges to ensure that users are granted access in accordance with the principal of least privilege. |
| 1. **External References** | 1. <https://attack.mitre.org/techniques/T1135/> |

1. **Detailed Reproduction Steps:**

4. Directory Listing Enabled - Low

|  |  |
| --- | --- |
| 1. **CWE** | 1. [**CWE-548**](https://cwe.mitre.org/data/definitions/548.html) |
| 1. **CVSS 3.1 Score** | 1. 4.3 |
| 1. **Description (Incl. Root Cause)** | 1. The web application exposes a directory listing of some files in the web root and subfolders. |
| 1. **Security Impact** | 1. The severity of this finding depends on the sensitivity of the files exposed on the web server. If the directory exposes only files intended for public consumption, then the risk is lower but if an attacker can gain access to sensitive information such as configuration files, they may be able to use these to gain further access to the application or web server. |
| 1. **Affected Host(s)** | 1. 192.168.195.215 (80/TCP) |
| 1. **Remediation** | 1. Restrict access to files and directories based on the concept of least privilege. Enforce authentication wherever possible and disable directory listing in the web server configuration. |
| 1. **External References** | 1. <https://attack.mitre.org/techniques/T1083/> 2. <https://www.acunetix.com/blog/articles/directory-listing-information-disclosure/> |

1. **Detailed Reproduction Steps:**

5. Enhance Security Monitoring Capabilities - Info

|  |  |
| --- | --- |
| 1. **CWE** | 1. [**CWE-693**](https://cwe.mitre.org/data/definitions/693.html) |
| 1. **Description (Incl. Root Cause)** | 1. It appeared that Acme did not notice “noisy” activities during the course of testing. The tester was also not blocked when using standard open-source penetration testing tools. |
| 1. **Security Impact** | 1. If network and endpoint detection and response are inadequate, an attacker who can gain a foothold in the internal network may be able to move laterally, perform post-exploitation, and achieve persistence easily. |
| 1. **Remediation** | 1. Consider investing in a more advanced network monitoring solution, configuring logging on all hosts, and processing them for anomalies using a SIEM tool, and implementing endpoint detection on each server and workstation that is more difficult to bypass and tamper with. The organization should not rely on endpoint protection alone. When combined with a defense-in-depth security strategy, they can be an excellent tool for detecting an attacker who gains internal network access and is forced to perform “noisier” and riskier activities to the nature of the hardened environment. |
| 1. **External References** | 1. <https://attack.mitre.org/tactics/TA0005/> |

# Appendices

## Appendix A – Finding Severities

Each finding has been assigned a severity rating of high, medium, or low. The rating is based off of an assessment of the priority with which each finding should be viewed and the potential impact each has on the confidentiality, integrity, and availability of Acme’s data.

| **Rating** | **Severity Rating Definition** |
| --- | --- |
| **Critical** | Exploitation of the technical or procedural vulnerability will lead to severe and wide-ranging consequences, causing significant harm to the organization. The potential impact extends beyond financial and operational aspects, encompassing political, legal, and reputational damage. The threat exposure associated with this vulnerability is exceptionally high, significantly increasing the likelihood of its occurrence. |
| **High** | Exploitation of the technical or procedural vulnerability will cause substantial harm. Significant political, financial, and/or legal damage is likely to result. The threat exposure is high, thereby increasing the likelihood of occurrence. Security controls are not effectively implemented to reduce the severity of impact if the vulnerability were exploited. |
| **Medium** | Exploitation of the technical or procedural vulnerability will significantly impact the confidentiality, integrity, and/or availability of the system, application, or data. Exploitation of the vulnerability may cause moderate financial loss or public embarrassment. The threat exposure is moderate-to-high, thereby increasing the likelihood of occurrence. Security controls are in place to contain the severity of impact if the vulnerability were exploited, such that further political, financial, or legal damage will not occur.  - OR -  The vulnerability is such that it would otherwise be considered High Risk, but the threat exposure is so limited that the likelihood of occurrence is minimal. |
| Low | Exploitation of the technical or procedural vulnerability will cause minimal impact to operations. The Confidentiality, Integrity and Availability (CIA) of sensitive information are not at risk of compromise. Exploitation of the vulnerability may cause slight financial loss or public embarrassment. The threat exposure is moderate-to-low. Security controls are in place to contain the severity of impact if the vulnerability were exploited, such that further political, financial, or legal damage will not occur.  - OR -  The vulnerability is such that it would otherwise be considered Medium Risk, but the threat exposure is so limited that the likelihood of occurrence is minimal. |

Table 5: Severity Definitions

## Appendix B – Host & Service Discovery

| 1. **IP Address** | 1. **Port** | 1. **Service** | 1. **Notes** |
| --- | --- | --- | --- |
| 1. **<FILL IN AS APPROPRIATE>** |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Table 6: Discovered Hosts and Services

# 

## Appendix C – Subdomain Discovery

| **Subdomains** | **Description** | **Discovery Method** |
| --- | --- | --- |
| **<FILL IN DISCOVERED VHOSTS/SUBDOMAINS>** |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

Table 7: Discovered Subdomains

## Appendix D – Exploited Hosts

| **Host** | **Scope** | **Method** | **Notes** |
| --- | --- | --- | --- |
| **<FILL IN AS APPROPRIATE>** |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Table 8: Exploitation Attempt Details

## Appendix E – Compromised Users

| **Username** | **Type** | **Method** | **Notes** |
| --- | --- | --- | --- |
| **<FILL IN AS APPROPRIATE>** |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Table 9: User Accounts Compromised

## Appendix F – Changes/Host Cleanup

| **Host** | **Scope** | **Change/Cleanup Needed** |
| --- | --- | --- |
| **<FILL IN AS APPROPRIATE>** |  |  |
|  |  |  |

Table 10: Assessment Artifacts