

# Objective-Based Penetration Testing Report

**ACME Inc.**

**Organization:** Acme Inc.

**Dates Assessed:** March 9, 2021 through April 9, 2021

**Report Date:** April 9, 2021

**Team:** Richard Rogerson | CISSP-ISSAP, GWAPT, GXPIN, GMOB, GSNA, OSCE, OSCP, OSWP, CISA

Denis Kucinic | CISSP, GWAPT, GCIH, OSCE, OSCP

Eric Salario | OSEP, OSCP, MCSA, CRTE, CRTP, eJPT, eCPTX

Ian Lin | GWAPT, OSCE, OSCP

Julie Mai | OSCP

# Table of Contents

1.	Risk Level Descriptions .....	03
2.	Executive Summary .....	04
3.	Approach .....	07
	3.1 Scope .....	07
	3.2 Constraints and Limitations .....	07
4.	Methodology .....	08
	4.1 Objective-Based Penetration Testing .....	08
5.	Technical Findings .....	12
	5.1 Objective/Physical Based Testing .....	16
	5.1.1 Unauthorized Access: Tailgating .....	16
	5.1.2 Unauthorized Access: Card Cloning .....	17
	5.2 Email And Public Reconnaissance .....	19
	5.2.1 Security Awareness: E-mail Phishing .....	19
	5.3 Infrastructure .....	22
	5.3.1 Unprotected Endpoints .....	22
	5.3.2 Windows Active Directory Domain Administrator Compromised .....	24
	5.3.3 LLMNR / NBT-NS Poisoning Vulnerability .....	26
	5.3.4 Missing Security Patches .....	28
	5.3.5 SMB Relay Attack Vulnerability .....	29
	5.3.6 Active Directory Domain Admins: Excessive Privileged Users .....	30
	5.3.7 Broken Security Boundary through Active Sessions: Acme .....	31
	5.3.8 Insecure Server Configuration (Lack of Hardening) .....	32
	5.4 Password Audit .....	35
	5.4.1 Active Directory Password Audit .....	35
	5.5 Network Security Testing .....	37
	5.6 Ransomware Simulation .....	38
	5.6.1 Findings .....	38
	5.6.2 Findings Breakdown .....	39
	5.6.3 Findings Breakdown: Credential Access .....	40
	5.6.4 Ransomware Scenario .....	40
6.	Recommendations .....	42
	6.1 Tactical Security Recommendations .....	42
7.	Appendix A: Mitigation Test Results .....	44
	7.1 Insecure SSL Configuration .....	44
8.	Appendix B: Credential Harvest Phishing Results .....	44



# 1. Risk Level Descriptions

## Risk Ratings



Exploitation and discovery of these findings typically require minimal skill and often result in high-privileged access to the affected systems or information. Remediation of critical-risk findings are of high precedence and should not be left unaddressed under any circumstances.



Exploitation of these items can directly lead to the compromise of systems, services or sensitive information. Exploitation is often possible with minimal effort and exploit code is likely to be publicly available or not required. It is recommended that these items be actioned as soon as possible.



Medium-risk findings may lead to a compromise of the environment or disclosure of sensitive information, but may require a significant amount of effort, time and complexity to successfully exploit. Medium risk findings should be actioned in a timely manner.



Low-risk findings have a small impact on the environment and a low likelihood of being exploited. It is generally recommended to address these risks at the lowest priority, occasionally the risk of these findings may be accepted and not actioned due to the limited impact and/or complexity to remediate.



Informational findings are observations made during the assessment which can be addressed with a lower priority. Informational findings typically do not pose a risk to the environment. This may include benign behavior such as bugs and broken functionality.



Remediated findings are findings where the identified vulnerabilities have been determined as fixed with no outstanding risk. Remediated findings do not pose a risk to the environment.





## 2. Executive Summary

### Penetration Test

Packetlabs was engaged to perform an objective-based Penetration Test of Acme Inc. The core objective of this assessment was to simulate a cyber-attack and evaluate the security controls across people, processes and technology in order to identify potential areas of weakness. Testing began on March 9, 2021 and completed on April 9, 2021. During this time, the testing was broken into logical components based on the type of testing performed including external and internal penetration testing, physical testing, e-mail phishing, and a comprehensive password audit across Microsoft Active Directory. There were six objectives that were in scope of the objective-based penetration test of the Acme environment. Of the six objectives, five objectives were accomplished. Below is a list of the complete and incomplete objectives.

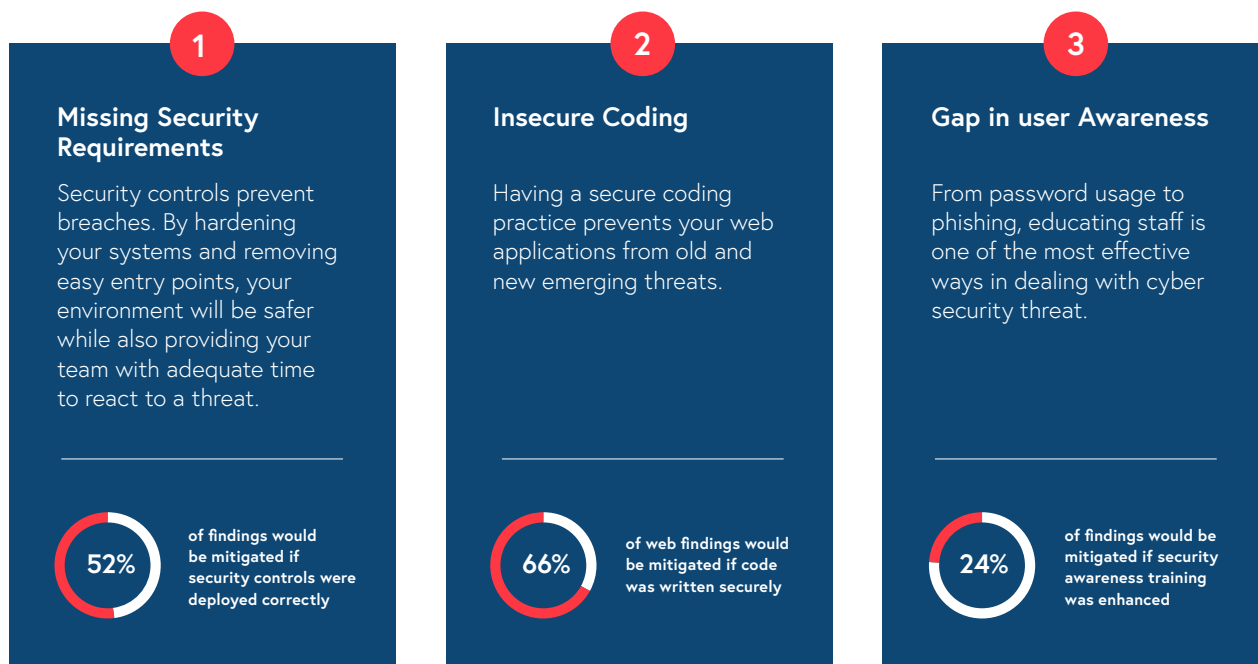
- ✓ Gain access to VPN and or Citrix
- ✓ Gain elevated access to systems with Personal Information
- ✓ Collect other user account credentials by monitoring network traffic
- ✓ Gain access to domain admin
- ✓ Gain access to users' credentials from the IT help desk
- ✓ Gain physical access through tailgating or card cloning

Overall, gaps were identified across **55%** of the SANS CIS Critical Security Controls, and 10% of the OWASP Top 10. The risk level for a compromise was found to be **high**.

Component	Key Findings	Overall Risk Level
 Objective Based Penetration Test	<ul style="list-style-type: none"><li>• Gaps in patching, and vulnerability management appear to consistently affect systems from endpoints to production servers. Overall, systems are susceptible to publicly available exploits resulting in remote code execution, unauthorized access, and sensitive information disclosure.</li><li>• Weak configurations enable unauthorized access and attackers to move freely throughout the network.</li><li>• Gaps in user awareness training enables attackers to gain unauthorized access to email and physical access to corporate offices.</li></ul>	 High

## Top Root Causes

As each finding is uncovered, a root cause is also identified to assist in remediation efforts. Knowing which areas of the business to allocate resources to can result in budgets being allocated to areas that require more effort. The results below have been calculated based on all root causes identified within the Client Name environment.



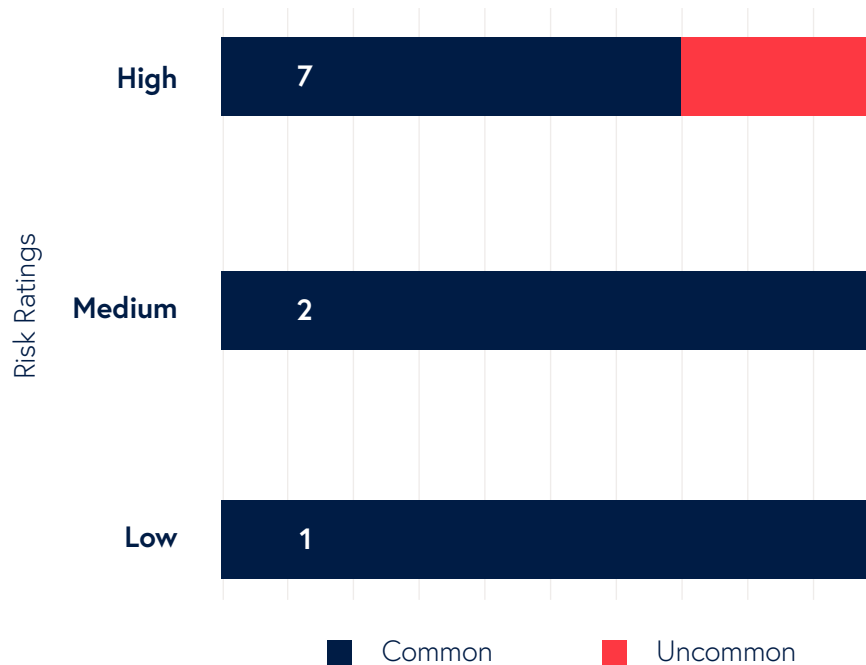
## Positive Takeaways

Below are areas where Acme performed well.

- **Endpoint Protection:** All workstations and servers have endpoint protection software.
- **Email Phishing Response:** Of the users who fell victim to attacks, several users updated their passwords within a quick period of time.
- **Up-to-date workstations:** The majority of user's workstations are Windows 10 operating systems, and have the latest patches.

## Common vs Uncommon Findings

The chart below groups the findings based on how often they are identified based on past engagements.



## Positive Takeaways

The following outlines recommendations provided to address the root cause of the findings identified. Specific strategic recommendations based on the engagement findings.

- Conduct an ISO 27001 assessment to identify Acme's security program alignment to an industry standard.
- Review corporate security standards related to application development and implementation/ adoption of a Software Development Lifecycle (SDLC).
- Assess security configuration standards and checklists to ensure default files and configuration settings are removed as part of the server/application hardening processes.
- Conduct annual application security assessments to provide continuous monitoring of environments, networks and applications.
- Standardize operating system imaging and device provisioning to ensure consistent hardening and protection of devices.



## 3. Approach

### Approach & Methodology

#### 3.1 Scope

The scope of this assessment was a Penetration Test of the Acme application. The following IPs/URLs were considered in scope:

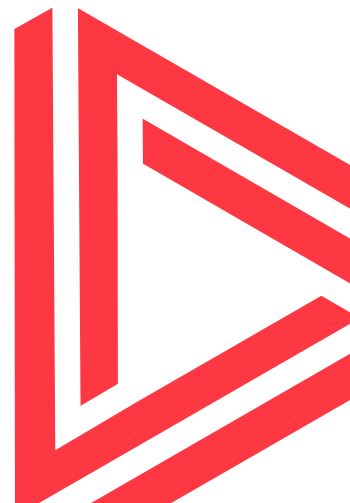
- Over 300 IPs were included in the scope and have been detailed in spreadsheet accompanying in this report.
- Office: 1 Acme Circle, Toronto
- Phishing: Acme Employees

The scope of this assessment was a Penetration Test of the Acme application. The following IPs/URLs were considered in scope:

### 3.2 Constraints and Limitations

Our objective in this Penetration Test was to identify publicly known vulnerabilities residing in systems, applications and infrastructure components. While we have performed extensive testing and analysis, there is no assurance that all vulnerabilities were identified.

Prior to the execution of our testing, we have taken measures to ensure that all of our tools are up to date and are running with the latest feed updates and plugins. This report represents the state of the systems tested on a particular point in time.





# 4. Methodology

## 4.1 Objective-based Penetration Testing

Packetlabs security testing methodology is based on industry standards and is primarily aligned with NIST SP800-115 to ensure compliance with most regulatory requirements. Below, the critical tasks within the methodology have been outlined.

Phase	Task Completed	Manual	Automated
<b>Information Gathering</b>	Identify restricted hosts (i.e., systems and devices not to be tested)	✓	✓
	Perform reconnaissance on target infrastructure via social media (e.g., LinkedIn, Facebook)	✓	✓
	Execute user enumeration to identify valid user accounts	✓	✓
	Conduct Google Hacking to identify potentially exposed infrastructure	✓	✓
	Harvest compromised password databases to assist with password profiling and password reuse attacks	✓	✓
<b>Objective-Based Testing</b>	<b>Infrastructure Security Testing</b>	✓	✓
	Comprehensive port scanning, fingerprinting of services and applications	✓	✓
	Utilization of automated scanning tools & technologies to identify publicly known operating system and application vulnerabilities. (Network-based or Authenticated Scans)	✓	✓
	Validation of findings, removing false-positive items and low-confidence findings where applicable	✓	✓
	Vulnerability testing using commercial and/or custom tools	✓	✓
	<b>Application Security Testing</b>	✓	✓
	Comprehensive mapping & manual crawling of the web applications to ensure coverage	✓	✓



Phase	Task Completed	Manual	Automated
<b>Objective-Based Testing</b>	Automated discovery of vulnerabilities using various commercial grade tools	✓	✓
	Validation of automated security testing results	✓	
	Testing for hard to find vulnerabilities including but not limited to: business logic, session handling, file upload functions, race conditions, hash-length extension, bit flipping attacks and authorization flaws	✓	
	Comprehensive coverage of PCI-DSS 6.5, OWASP Top 10:2017 and Sans Top 25	✓	
	<b>Email Phishing</b>		
	Create relevant e-mail templates for phishing attacks that resemble known web applications which deliver malicious payloads to end-users		
	Initially target a small group of users in order to collect intel about endpoint OS, browser and vulnerable plugins installed		
	Conduct subsequent phishing waves with targeted attacks based on discovered weaknesses including: fake software updates, browser exploits, or requesting user credentials		
	Obtain and demonstrate unauthorized access		
	<b>Device Planting / Lost USBs</b>		
	Configure and deploy an assortment of USB devices including HID (human interface device) attacks, client-side exploits, and Microsoft Office Macros and attempt to obtain unauthorized access		
	While onsite, survey physical network ports and install unauthorized devices throughout the network with reverse tunnels over various protocols		
	Leverage devices to perform client-side attacks on endpoints and attempt to obtain unauthorized access		
	<b>Tailgating</b>		
	Configure and deploy an assortment of devices capable of capturing low frequency access cards to gain unauthorized physical access		
	Perform tailgating attack scenarios on office locations during normal business hours and conduct subsequent tailgating attacks during peak times		
	Assess and note office egress and ingress doors for bypass weaknesses: <ul style="list-style-type: none"> <li>• Hinges installed outside</li> <li>• Poor door and frame fitment</li> <li>• Door latches</li> <li>• Installation of exit unlocks (push button, push/crash bars, motion or IR sensor, etc.)</li> </ul>		
	<b>Ransomware Assessment</b>		
	Automated and manual lateral movement attacks to evaluate ransomware propagation likelihood		

Phase	Task Completed	Manual	Automated
<b>Objective-Based Testing</b>	Automated and manual testing of file share permissions to identify data subject to ransomware (e.g., FTP, SMB, etc.)		
	Comprehensive testing to evaluate effectiveness of anti-malware controls		
	Comparison of findings against common malware strains		
	<b>Wireless Assessment</b>	✓	✓
	Identify wireless access points, networks for testing and physical locations	✓	✓
	Conduct wireless attacks to gain access to wireless networks: <ul style="list-style-type: none"> <li>• Credential Brute-forcing;</li> <li>• Attack wireless protocol-level vulnerabilities;</li> <li>• Handshake capture and deauthentication; and</li> <li>• Rogue access point attacks</li> </ul>	✓	✓
	Wireless packet capture of accessible areas within the wireless network range	✓	
	Use specialized computer hardware to attempt to crack any capture handshakes, to reveal the plain-text password	✓	
	Wireless network segmentation test	✓	
<b>Post-Exploitation</b>	<b>Permissions Testing and Privilege Escalation</b>		
	Identify and exploit endpoint-based privilege escalation vulnerabilities or misconfigurations on compromised systems	✓	✓
	Identify and exploit environment privilege escalation vulnerabilities or misconfigurations	✓	✓
	Conduct BloodHound enumeration and map privilege escalation paths for AD environments	✓	✓
	Test for Active Directory misconfigurations and vulnerabilities to elevate to a domain/enterprise administrator	✓	✓
	Test for user group segregation	✓	✓
	Test for file system permissions weakness	✓	✓
	Test for overly permissive share access	✓	✓
	Attempt to exfiltrate data out of restricted environment(s) if applicable	✓	✓
	Attempt to gain unauthorized access to mission critical application/systems with established access	✓	✓
	Service misconfigurations	✓	✓
	<b>Lateral Movement</b>		
	Pivot to from compromised systems to other internal systems	✓	





Phase	Task Completed	Manual	Automated
Post-Exploitation	Test for reoccurring usage of credentials	✓	
	Test for lateral movement on exposed network protocols	✓	✓
	Test for lateral movement with common system binaries	✓	✓
	Conduct exploitation of vulnerable remote services	✓	
	Encryption keys, i.e., SSH keys	✓	
	Test for network segregation	✓	
	Test for common Windows and Active Directory Lateral Movement techniques;		
	• Cached credentials		
	• Pass the hash attacks	✓	
	• Pass the ticket attacks		
	• Windows services (RDP, PSEXEC, task scheduler, etc.)		
	<b>Defense Evasion</b>		
	Attempt to bypass application whitelisting	✓	✓
	Attempt to bypass endpoint security solution	✓	✓
	Attempt to circumvent network access controls (Firewall, IDS, IPS, WAF, etc.)	✓	✓
	<b>Password Audit</b>	✓	✓
	Crack hashes using specialized computing hardware to reveal plain-text passwords	✓	✓
	Usage of optimized wordlists and masks for target organization and individual targets	✓	
	Conduct a breach analysis of cracked passwords	✓	✓
	Conduct a statistical analysis and review of all plain-text credentials obtained	✓	
	Customized recommendations for password policy improvements	✓	
Reporting	A draft detailed report outlining findings coupled with control recommendations including an executive summary outlining the overall state of the application.	✓	✓
	Document steps to reproduce findings to ensure application developers can validate remediation efforts prior to retesting.	✓	
	Conduct root cause analysis of findings outlining common themes observed with recommendations to improve security within the environment.	✓	











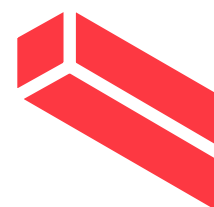
## 5. Technical Findings

### Attack Breakdown

A number of attack types were considered to explore the potential compromise through numerous vectors including external and internal penetration testing, e-mail phishing, web application testing, and network security testing. Beyond this, a number of physical attacks were utilized to explore potential compromise through tailgating and access card cloning. The overall findings and risk have been outlined in the following table.

Component	Key Findings	Overall Risk Level
 Physical/Objective Based Testing	<p>Two members of the Packetlabs team were able to successfully obtain unauthorized physical access to the Acme offices on the 4th floor of 1 Acme circle, Toronto. One team member obtained access by tailgating in as the employees left the backdoor on the North entrance. During the lunch hour, tailgating was performed when reception was away from their desk, and unauthorized access was obtained by tailgating employees returning from lunch.</p> <p>Access was also gained using an access badge cloning device. After entering an elevator with an Acme employee, the close proximity of the elevator allowed wireless cloning of the card. A cloned card was used to physically access the Acme Offices.</p> <p>After successfully gaining unauthorized access through tailgating and card cloning into the Acme offices, two malicious USB devices were dropped. 3 more devices were sent to remote locations. During the span of 2 weeks, none of the planted USBs were plugged into any systems.</p>	 High
 Phishing and Reconnaissance	<p>Phishing attacks consisted of two waves, the first was sent to 150 users which resulted in users downloading malware disguised as a Citrix Receiver update. As a result, four outbound connections from personal computers beacons back and unauthorized access was obtained. Since there was no evidence that this was in the Acme environment, access to those endpoints was quickly halted.</p> <p>A second phishing campaign was sent out to all of the Acme users which masqueraded itself as an Acme security tool to check the strength of user passwords. This campaign harvested 45 unique credentials, with multiple credentials enabling unauthorized access to Acme internal network and internal infrastructure.</p>	 High

Component	Key Findings	Overall Risk Level
 Infrastructure	<p>Infrastructure security testing was completed from both an internal and external network perspective. Externally, minor concerns regarding SSL configuration and certificates were found.</p> <p>On the internal side a lack of vulnerability management enabled the compromise of major corporate assets.</p>	
 Password Audit	<p>A comprehensive audit was completed on Active Directory (AD) for ACME-HQ, and ACME-CAD. To identify the usage of weak passwords. A significant number of employees make use of the same passwords. Furthermore, several privileged accounts were found to make use of weak passwords which makes each domain vulnerable to brute-force, and password guessing attacks.</p>	
 Network Security Testing	<p>Wireless penetration testing was performed at the guest and corporate networks of the Acme environment at two locations to measure the effectiveness of the security controls. The guest SSIDs of the four locations made use of WPA2-Personal and the four-way handshake was obtained through de-authenticating clients on the wireless network. It was not possible to crack the pre-shared key within the time window. The corporate SSIDs utilize WPA-Enterprise and require domain credentials.</p>	
 Ransomware Assessment	<p>Lack of secure configurations, memory protections configurations, and insufficient detections may enable ransomware attacks, data exfiltration, and unauthorized access throughout the Acme IT environment.</p>	



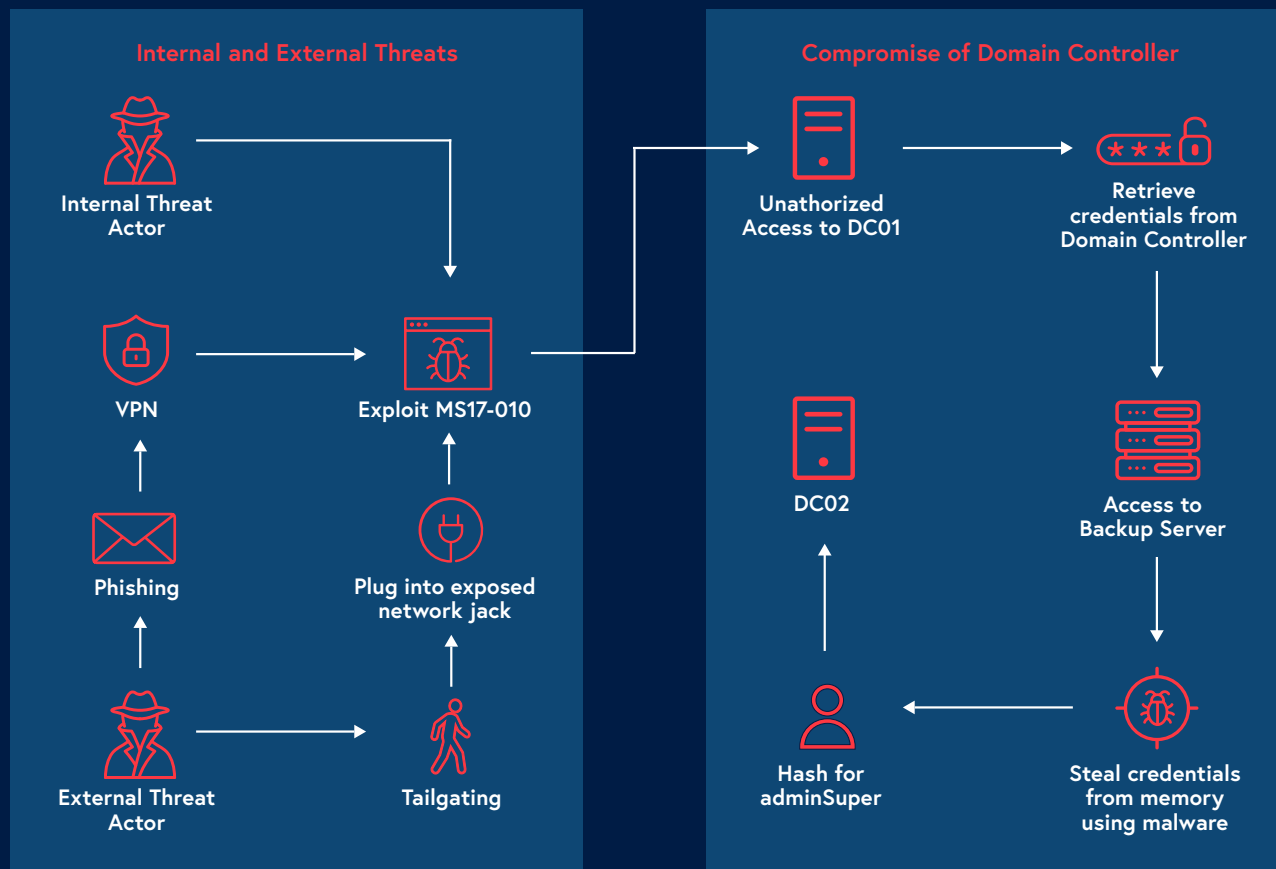
## Acme High-Level Attack Summary

The below diagram illustrates the attacks that lead to the compromise of all Acme IT systems. It identifies how an internal threat actor or an external threat actor can exploit vulnerabilities in the Acme environment to gain unauthorized access to all Active Directory domains (Acme-HQ, and Acme-CAD). This information is provided to assist with understanding Acme's internal and external exposures.

To summarize, there is a critical vulnerability that exists throughout the Acme environment as a result of an insufficient patch management and vulnerability remediation program. The Eternal Blue exploit is a famous exploit leaked by the group known as the Shadow Brokers, who back in 2017 were disclosing software exploits believed to be stolen from the US National Security Agency. A month later, hackers weaponized the exploit leak, and WannaCry ransomware struck thousands of computers in more than 150 countries.

Unauthorized access to Acme's Acme-HQ domain controller was obtained through the same vector. ACME-CAD's domain controller was likewise affected by the same vulnerability; however, exploitation was not successful. Unauthorized access to ACME-CAD was obtained by utilizing credentials found on domain controllers and unprotected servers within the ACME-HQ environment.

### High level Attack Scenario



## Findings Breakdown

As each finding is uncovered, a root cause is also identified to assist in remediation efforts. Knowing which areas of the business to allocate resources to can result in budgets being allocated to areas that require more effort. The results below have been calculated based on all root causes identified within the Client Name environment.

Component	Findings	Overall Risk Level
 Physical/Objective Based testing	<ul style="list-style-type: none"> <li>5.1.1 Unauthorized Access: Tailgating</li> <li>5.1.2 Unauthorized Access: Card Cloning</li> </ul>	HIGH
 Phishing and Reconnaissance	<ul style="list-style-type: none"> <li>5.2.1 Security Awareness: E-mail Phishing</li> </ul>	HIGH
 Infrastructure	<ul style="list-style-type: none"> <li>5.3.1 Unprotected Endpoints</li> <li>5.3.2 Windows Active Directory Domain Administrator Compromised</li> <li>5.3.3 LLMNR / NBT-NS Poisoning Vulnerability</li> <li>5.3.4 Missing Security Patches</li> <li>5.3.5 SMB Relay Attack Vulnerability</li> <li>5.3.6 Active Directory Domain Admins: Excessive Privileged Users</li> <li>5.3.7 Broken Security Boundary through Active Sessions</li> <li>5.3.8 Insecure Server Configuration (Lack of Hardening)</li> </ul>	HIGH
 Password Audit	<ul style="list-style-type: none"> <li>5.4 Password Audit</li> </ul>	HIGH
 Wireless Network Security Testing	<ul style="list-style-type: none"> <li>5.5 Network Security Testing</li> </ul>	LOW
 Ransomware Assessment	<ul style="list-style-type: none"> <li>5.6 Ransomware Assessment</li> </ul>	MEDIUM

## 5.1 Objective/Physical Based Testing

### 5.1.1 Unauthorized Access: Tailgating



INDUSTRY REFERENCE

CSC17: Implement a Security Awareness and Training Program

IMPACT

Physical access to a restricted area

ROOT CAUSE

A Gap in user awareness

On Friday, June 15, 2019, two members of the Packetlabs team attempted to gain unauthorized physical access to the Acme offices located on the 4th floor of 1 Acme Circle, Toronto.

During the morning hours between 10 AM and 12 PM, members of the team noted several employees coming in and out of the office to identify the best point of entry. On the North entrance of the fourth floor, one team member was on the phone outside the door in between 10:25 AM to 10:55 AM. During this time, an Acme employee exited the office, and one team member walked in before the door closed. During entry, a malicious USB was placed in the East kitchen area. The team member was questioned after several minutes, but was successfully able to defuse any suspicion and remain in the office for a short time before leaving.

In between 12:15 PM to 1:05 PM, two separate attempts were made by the two Packetlabs team members to tailgate through the reception door. Reception staff were not at their desk, and the two Packetlabs members walked in following two different employees unchallenged throughout the office.

Calling out a suspicious person, questioning them on their right to be here without authorization is positive to take away. However, it seems that this behaviour was not common throughout the separate attempts to follow authorized employees into the office.

### Supporting Evidence

The below screenshot was the initial entry point that the Packetlabs team was able to gain unauthorized physical access to the Acme office.





## Affected Assets

- ▶ Acme Office and Personnel

## Recommendation

Ensure there is a policy defined for handling visitors and that the policy is known by all staff and adhered to under all circumstances. The policy should specify in detail the protocols to be followed when signing in guests. Have a mechanism to identify guests such as a visitor badge and internal contact. Guests must be associated with a Acme employee who is responsible for the guest, and have a procedure to follow when an unauthorized visitor is identified.

### 5.1.2 Unauthorized Access: Card Cloning



#### INDUSTRY REFERENCE

CSC20: Penetration Tests and Red Team Exercises

#### IMPACT

Physical access to a restricted area

#### ROOT CAUSE

A Gap in user awareness

On Friday, June 15, 2019, two members of the Packetlabs team attempted to gain unauthorized physical access to the Acme offices located on the 4th floor of 1 Acme Circle, Toronto.

An individual returning to the Acme office entered the elevator on the West entrance at around 11:55 PM. This elevator required keycard access and a Packetlabs team member followed the employee into the elevator carrying an access badge cloning device in a briefcase and pretended to go to the fifth floor. Elevators allow people to be in close proximity of each other, as a result their access card was wirelessly cloned. The Packetlabs member made their way to the downstairs lobby and cloned a card that enabled unauthorized access to all locked entrances of the Acme offices.

During entry, another malicious USB was dropped at an employee's desk around the North entrance.

## Supporting Evidence

On our briefcase cloning device, there was a web application that would log entries for all cards captured. After unauthorized access was obtained, we were roaming the halls for approximately 10 minutes without any Acme personnel challenging us. Below is a picture of the office demonstrating physical access was obtained.



## Affected Assets

- ▶ Acme Office

## Recommendation

Implement and mandate the use of encrypted RFID access cards. Alternatively, if this is not possible, consider implementing multi-factor authentication on physical access controls.

## 5.2 Email and Public Reconnaissance

### 5.2.1 Security Awareness: E-mail Phishing



#### INDUSTRY REFERENCE

CSC7: Email and Web  
Browser Protections

#### IMPACT

Sensitive Information Disclosure

#### ROOT CAUSE

A Gap in user awareness

Two comprehensive email phishing campaigns were conducted that resulted in numerous employees entering their credentials into an untrusted site, as well as downloading malicious software onto their workstations.

The first campaign sent emails urging employees to download a "Citrix Windows Update" to protect against malware and other attack vectors. Since Citrix is a known third-party application used within the company, a software update would seem convincing. Users who clicked on the link would download a binary that when executed would give a reverse shell to the attacker. At least 15 clicks and 4 remote shells were obtained with the full access and permissions of the user that was exploited.

The second campaign sent emails to all employees stating that Acme was partnering with ChangeMyPassword.ca, which checks if a password has been part of a data breach in the past, or if the password does not seem reasonable password strength. Phishing site found here: <https://changemypassword.ca/Acme/>). This partnership seemed reasonable since testing password complexity is a valid and useful resource. Once the user entered their password, the site would determine if the password is considered strong. If it is, then the user would be notified that their password is safe; otherwise, a strong password is suggested to the user for future use. The site received 101 views, 65 unique views, and 52 database entries detailing the following parameters:

- Email
- Password Entered
- Suggested Password (if applicable)
- Date
- Time
- User Agent
- IP Address

## Supporting Evidence

Photo of phishing email and phishing site are provided here for real engagements.

Please see the following tables for more information regarding each wave of the phishing campaign.

Send date	April 10th, 2021	
Send time	9:29 AM (EST)	
Number of emails sent	100	
Time to first click	9:31 AM (EST)	■ Within acceptable limit
Clicks	13	■ Slight below acceptable limit
Password submissions	4	■ Below acceptable limit
Passwords that were successfully used to further an attack	1	
Response time	9:56 AM (EST)	

## Affected Assets

- ▶ Multiple assets affected see Appendix B for a comprehensive list of affected assets.

## Recommendation

- Enhance security awareness training to ensure employees are verifying they are communicating with an authorized party.
- Remove Gmail whitelist on mail server. This is allowing spam into the environment.
- Personnel should report all phishing emails received to appropriate IT or IT Security staff. It was noted that IT staff were alerted by several users.

- Investigate reported phishing emails to take appropriate actions, which may include:
  - Blocking the malicious website
  - Blocking the sender's email address
  - Send out a notification email to personnel warning them about the specific phishing email and to be on alert for similar emails.
- Investigate network traffic and logs as well as email personnel to determine if any persons may have been successfully phished.
- If users were successfully phished, start the incident response process to determine the impacts of the attack (e.g., were credentials compromised. Has malware been downloaded or run on a system in the network).

## For Office365:

- Consider looking into a process that purges specific emails from Outlook using Powershell or other techniques.
- If Acme's O-365 subscription has Advanced Threat Protection, review the settings to ensure it is enabled and that each of the policies is configured. By default, ATP does not apply protections as they require configuration.
  - ATP policies: Safe Attachments, Safe Links, Anti-phishing
  - Policies are fine-grained and can be applied on a per-user or per-group basis.

## 5.3 Infrastructure

### 5.3.1 Unprotected Endpoints



INDUSTRY REFERENCE

CSC8: Malware Defenses

IMPACT

Unauthorized access, sensitive information disclosure

ROOT CAUSE

Missing security requirement

The Acme environment is found to have strong endpoint protection through their vendor's EDR solutions. Major servers and endpoints were found to have a Sophos collector agent present which prevented the execution of malware, disabling of host-based protections, and ability to escalate privileges. However, such measures are only as effective as the weakest endpoint or server in the environment. In the case of Acme, a backup server was accessed with credentials retrieved from ACME-HQ's domain controller. It was later found that no endpoint protections were enabled on what is presumably a test server. By introducing malware and scraping the memory from a privileged process (lsass.exe), a domain administrator credential to ACME-CAD was uncovered.

Throughout the penetration testing, this host was used to move laterally through Acme's network. Many enumeration techniques that were prohibited by Sophos were utilized on this host. It is possible that there are other test servers and endpoints that have little or no protection.

### Supporting Evidence

After the ACME-HQ domain controller was compromised, the backup server was accessed with adminAcme's credentials. Since this host did not have any host-based protections, it was possible to perform enumeration from this host. The below screenshot shows unauthorized access into backup server as well as enumeration with PowerShell being done on the Acme environment.

Upon enumeration, it was discovered that adminSuper was also logged in through RDP on this machine. The malware was then introduced to the host and clear-text credentials were retrieved from adminSuper. This enabled access into ACME-CAD's domain controller.

```

Administrator: Windows PowerShell
[*] lsass.exe found at 00007FF789780000
[*] wdigest.dll found at 00007FFB44D90000
[*] lsasrv.dll found at 00007FFB45600000
[*] Loaded lsasrv.dll locally at address 00007FFB45600000
[*] Found offset to AES/3Des/IV at 426968
[*] InitializationVector offset found as 1139167
[*] InitializationVector recovered as:
[*] ==== [ Start ] ====
[*] 80 a3 bf 46 f9 31 2e 3c 28 63 10 ae c3 5e 19 0b
[*] ==== [ End ] ====
[*] h3DesKey offset found as 1139325
[*] 3Des Key recovered as:
[*] ==== [ Start ] ====
[*] c2 8d 31 42 cb b7 0d 94 13 8b 02 fe 05 da 7c 4d 70 c4 e6 23 43 b1 f5 62
[*] ==== [ End ] ====
[*] Aes Key recovered as:
[*] ==== [ Start ] ====
[*] f6 71 e2 8a f5 88 43 f4 ba bc 3b 6e 43 85 df 3d
[*] ==== [ End ] ====
[*] Loaded wdigest.dll at address 00007FFB44D90000
[*] l_LogSessList offset found as 104787
[*] l_LogSessList found at address 000001FE6697ED50
[*] Credentials incoming... (hopefully)

[-->] Username: testuser
[-->] Hostname: DESKTOP-VACDP6S
[-->] Password: ThisIsASup3rLongP4ssword!!

[-->] Username: aaa
[-->] Hostname: DESKTOP-VACDP6S
[-->] Password: pppaaa

```

## Affected Assets

- ▶ 10.10.15.25 (backupserver.acme.com)

## Recommendation

Ensure that endpoint protections are also applied to test servers within the environment. Alternatively, limit access to test servers only to authorized users that need access.

# 5.3.2 Windows Active Directory Domain Administrator Compromised



**INDUSTRY REFERENCE**  
CSC3: Continuous Vulnerability Management  
CSC16: Account Monitoring and Control

**IMPACT**  
Compromise of corporate assets,  
sensitive information disclosure

**ROOT CAUSE**  
Missing security requirements

Utilizing Eternal Blue (MS17-010) to deliver a payload, the first domain controller (10.10.10.15) was used to create a local administrator user that was granted access to the remote desktop service. Through remote access to this system, a domain administrator was added. Afterwards, the ntds.dit and SYSTEM boot key was extracted for offline credential cracking. It is important to note that all of the domain controllers did contain endpoint detection and response (EDR) software, but failed to prevent the credentials from being dumped. These credentials along with the Insecure SMB/RPC Configuration was used to identify privileged users of three of the compromised domains.

One of those machines within the Acme network, which is presumed to be used for testing purposes (backupserver.Acme.com) failed to have endpoint protections enabled, allowed the attacker to upload malware to scrape for clear-text credentials. As a result, the user "adminSuper" was compromised, and access to the second domain controller (10.10.10.30) was obtained.

## Supporting Evidence

### 1. Domain Controller - 10.10.10.15 (HQ. Acme.com) compromised utilizing Eternal Blue

During the testing in the Acme environment, custom shellcode was used to create an administrative account called AcmeAdmin on domain controller DC01 (10.10.10.15) in the hq.Acme.com domain. This payload was delivered via the SMB remote code execution vulnerability knows as Eternal Blue MS17-010.





## 2. Domain Controller 2 - 10.10.10.30 (ACME-CAD) compromised through Credential Abuse

Credential dumping from system backupserver.Acme.com provided the ability to access the second domain controller DC02 (10.10.10.30) in the Acme-CAD domain.

### Affected Assets

- ▶ 10.10.10.15
- ▶ 10.10.10.30

### Recommendation

Restrict usage of shared credentials and prohibit interactive login where possible. At a minimum, shared credentials should be restricted to a class of systems (e.g., prod servers, test servers, QA servers, user endpoints). If possible, disable all shared user accounts in favour of individually assigned admin accounts. Continue usage of segregated accounts based on privilege requirements.

When each group is prohibited from performing logins to another tier, then even if one group is compromised, they are effectively segmented. Administrative accounts should be divided into different groups of different tiers, a good example is as follows:

- Workstation Administrators: should only be allowed to log in to workstations to perform administrative tasks on workstations
- Server Administrators: should only be allowed to log in servers
- Domain Administrators: should only be allowed to log in to domain controllers

### 5.3.3 LLMNR / NBT-NS Poisoning Vulnerability



#### INDUSTRY REFERENCE

CSC5: Secure Configuration for Hardware and Software  
CSC9: Limitation and Control of Network Ports, Protocols and Services

#### IMPACT

Disclosure of sensitive information,  
unauthorized access

#### ROOT CAUSE

Insecure configuration

Multiple hosts found in Acme' network were susceptible to LLMNR, NBT-NS attacks and the successful capture of usernames and passwords from cracked hashes. Link-Local Multicast Name Resolution (LLMNR) and NetBIOS Name Service (NBT-NS) are two components of Microsoft Windows systems used as a backup when DNS is not able to resolve the user's query. LLMNR was introduced in Windows Vista and is the successor to NBT-NS.

If one endpoint attempts to resolve a particular host, but DNS resolution fails, the machine will then attempt to ask all endpoints on the local network for the correct address via LLMNR or NBT-NS. Even though this seems harmless in theory, it enables an attacker to poison responses and perform various attacks to obtain unauthorized access to the network.

## Supporting Evidence

After being connected to the Acme internal network, it was found that the LLMNR and the NBT-NS protocols were enabled on the network. This enabled us to effectively answer all LLMNR and NBT-NS queries as the destination for any hostname requested. During the attack, NTLMv2 hashes were attempted to be captured through a failed DNS resolution. In certain cases, these hashes can be cracked, however, another attack vector was chosen and used to leverage a supplemental attack to gain unauthorized access. Please consult the SMB Relay Attack Vulnerability finding for more details.

Because of this vulnerability, 14 hashes of accounts in the Acme environment were captured. Some of the captured hashes were high privileged accounts in one of the domains.

```
root@kali:~/user/share/Responder/Tools# python MultisRelay.py -t 10.10.10.14 -u All

Responder MultisRelay 2.0 NTLMv1/2 Relay
Relaying credentials for these users:
('All',)

Retrieving information for 10.10.10.14 -
SMB signing: False
OS version: 'Windows Server 2016 Standard 14393'
Hostname: 'APP1'

[+] Setting up HTTP relay with SMB challenge: b155c79aaa32c020f
[+] Received NTLMv2 hash from: 10.10.10.14
[+] Username: hdevic is whitelisted, forwarding credentials.
[+] SMB Session Auth sent.
[+] Relay Failed, Tree Connect AuthX denied. This is a low privileged user or SMB Signing is mandatory.
[+] Hashes were saved anyway in Responder/logs/ folder.

[+] Setting up HTTP relay with SMB challenge: 8b0a8b11c31fa3
[+] Received NTLMv2 hash from: 10.10.10.15 False
[+] Username: spatterson is whitelisted, forwarding credentials.
[+] SMB Session Auth sent.
[+] Relay Failed, Tree Connect AuthX denied. This is a low privileged user or SMB Signing is mandatory.
[+] Hashes were saved anyway in Responder/logs/ folder.
```

Below is a screenshot displaying the successful attack and obtaining SYSTEM level permissions against a target server.

```
Any other command than that will be run as SYSTEM on the target.
Connected as LocalSystem.
C:\Windows\system32\:#dump
The Windows Remote Registry Service is sleeping, waking it up...
BootKey: 63f2bf3blac6c847295ceb7ce53794ef
[+] Something went wrong, try something else.
C:\Windows\system32\:#ipconfig

Windows IP Configuration

Ethernet adapter Ethernet 2:

    Connection-specific DNS Suffix  . : 
    IPv4 Address. . . . . : 10.10.10.14
    Subnet Mask . . . . . : 255.255.0.0
    Default Gateway . . . . . : 10.1.2.1

Tunnel adapter isatap.{9016FAE1-442B-4818-923D-5CABF5F0D413}:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . : 

C:\Windows\system32\:#whoami
nt authority\system

C:\Windows\system32\:#
```

## Affected Assets

- ▶ Acme Internal Network

## Recommendation

Where possible, disable both LLMNR and NBT-NS, deprecate support for NTLMv1 and enforce SMB signing.

## 5.3.4 Missing Security Patches



### INDUSTRY REFERENCE

CSC3: Continuous Vulnerability Management  
CSC2: Inventory and Control of Software Assets

### IMPACT

Multiple

### ROOT CAUSE

Missing security patches

A number of systems were found to be missing security patches on internal and external systems in-scope of this testing, which expose the infrastructure to numerous vulnerabilities (e.g., privilege escalation, remote command execution, information disclosure, denial of service, client-side attacks). Overall, the vulnerable unpatched software discovered was related to: Microsoft, Adobe Acrobat, Adobe Flash Player, Adobe Reader, Adobe Shockwave, Microsoft .NET framework, Microsoft Excel, Internet Explorer, Microsoft Office, Microsoft SMB, Microsoft SQL, Microsoft Windows, Microsoft XML.

Among the missing security patches are resolutions to publicly available exploits such multiple Microsoft SMB server remote code execution vulnerabilities (MS17-010). These vulnerabilities have the potential to be used in attacks that lead to remote code execution and gaining full access to the system without authentication.

Beyond this, a significant number of end of life/obsolete software packages were found installed. End of life software is no longer supported by the developer and will not receive security patches for vulnerabilities discovered. These packages include: Microsoft Windows Server 2003/2008, Adobe Reader 10.x, Microsoft .Net Framework 1.1 & 4-4.5.1, Internet Explorer 7-8, Oracle Java SE/JRE/JDK 7/1.7.

## Supporting Evidence

Product	Last Patch Date	Severity
Adobe Flash Player	EOL	CRITICAL
Oracle Java SE/JRE/JDK 7/1.7	EOL	CRITICAL
IIS 7.5	EOL	CRITICAL
Oracle Java SE Critical Patch Update	July 2015	CRITICAL
Microsoft Internet Explorer 10	EOL	HIGH
Microsoft Windows Security Update	July 2017	HIGH
Microsoft .NET Framework Security Update	July 2019	HIGH
Microsoft .NET Framework & .NET Core Security Updates	July 2020	HIGH

## Affected Assets

- ▶ Please review supplemental documentation of the Acme VA's for a complete inventory.

## Recommendation

Apply the latest security patches and validate missing patches are part of recurring patch schedule.

### 5.3.5 SMB Relay Attack Vulnerability



#### INDUSTRY REFERENCE

CSC5: Secure Configurations for Hardware and Software

#### IMPACT

Disclosure of sensitive information, unauthorized access

#### ROOT CAUSE

Insecure configuration

Multiple servers in the Acme environment are vulnerable to SMB Relay attacks. This type of attack relies on listening for NTLMv1 and/or NTLMv2 authentication over SMB which is often used by patch management solutions to inventory assets on the network. NTLM is a challenge/response protocol that can be vulnerable to an attacker inserting themselves into the middle of the exchange. This attack is dangerous as it allows any potential attacker with access to capturing network traffic and then relaying it to get unauthorized access to potential servers or other hosts.

## Supporting Evidence

Once a user browses to a file share or mistypes a share name, their hash would be disclosed if attackers on the network were poisoning LLMNR & NBT-NS queries. While the hash could be cracked, in many cases, they also can be relayed to another host to gain unauthorized access, as seen in the LLMNR/NBT-NS finding above.

## Affected Assets

- ▶ Acme Internal Network

## Recommendation

Investigate corporate hardening standards and ensure SMB Signing is enabled.

## 5.3.6 Active Directory Domain Admins: Excessive Privileged Users



### INDUSTRY REFERENCE

CSC4: Controlled Use of Administrative Privileges

### IMPACT

Compromise of corporate assets, sensitive information disclosure

### ROOT CAUSE

Missing security requirements

In the Acme IT environment, there are more than 12 enabled users that have the Domain Admin privilege. Some notable accounts are the [user list] domain accounts. Investigate whether or not service accounts need to have this privilege. In many cases, vendors usually have an option to run these accounts without such privilege.

## Supporting Evidence

The screenshot below shows users of the Domain Admin group in the Acme IT environment.

[Screenshot of BloodHound output]

In another Active Directory environment ([domain]), the presence of an enable service account running as Domain Administrator was also found.

[Screenshot of BloodHound output]

## Affected Assets

- ▶ Acme Domain 1
- ▶ Acme Domain 2

## Recommendation

Adhere to the principle of least privilege within the Active Directory environment. Restrict remote access to only users that require access to the internal network. For general file sharing purposes, ensure proper credential hygiene is followed.

Investigate usage of Domain Admin service accounts in the environment. Consult vendor documentation on removing such privilege for these accounts. In addition, ensure that Domain Administrators do not leave live sessions in the environment. System administrators should practice logging out of their session instead of keeping their session alive and disconnected.

### 5.3.7 Broken Security Boundary through Active Sessions: Acme



INDUSTRY REFERENCE

CSC6: Maintenance, Monitoring, and Analysis of Audit Logs  
CSC16: Account Monitoring and Control

IMPACT

Compromise of corporate assets, sensitive information disclosure

ROOT CAUSE

Insecure design/implementation

Domain trusts allow domains to form interconnected relationships, and essentially all a trust does is link up authentication systems of the two domains and allow authentication traffic to flow between them. This is done by each domain negotiating an inter-realm trust key that can relay Kerberos referrals. In an Active Directory environment, the domain is not the trust boundary, but rather the forest.

However, the [account] account was found to have access to certain hosts within the [domain] environment. One such host was [host]. If administrative access was obtained on the host, it would disclose [account] credential as well.

### Supporting Evidence

Using [account] credentials that were previously used to compromise [system], it was determined that a session belonging to [account] was present as shown below.

[Screenshot of BloodHound output]

To execute this attack flow, a lateral movement attack was conducted against the [system] and unauthorized access was accomplished as shown below.

Since the session of [account] was present on the host, it is possible to steal this account's token (which would allow us to impersonate its privileges) as shown below. A listing of the remote C\$ drive was performed on [system] was tested to validate access.

[Screenshot of access]

This attack could also have been carried out by dumping lsass.exe again to retrieve [account] credentials.

[Screenshot of credentials]

Using [account] token or NTLM hash, it was possible to perform an interactive login via RDP to compromise the [system]. This effectively crosses the trust boundary between the two Active Directory environments.

## Affected Assets

- ▶ Acme IT

## Recommendation

Conduct an entitlement review of foreign group memberships between [domain 1] and [domain 2] and remove access where needed. In addition, management and maintenance of each domain's Domain Controllers should be performed by specific accounts tied to each domain to prevent disclosure of credentials.

### 5.3.8 Insecure Server Configuration (Lack of Hardening)



#### INDUSTRY REFERENCE

CSC4: Controlled Use of Administrative Privileges

#### IMPACT

Compromise of corporate assets, sensitive information disclosure

#### ROOT CAUSE

Missing security requirements

Lack of system hardening was identified on multiple systems, which may lead to services, software, and system functionality being used for malicious purposes. The various vulnerabilities were found:

- **Enabled cache logon credentials:** This feature is currently enabled on the host in which Windows NT may cache the last interactive logon.
- **Insecure password configuration:** The Administrator's account is currently set with a password that never expires.



- **Allowed Null Sessions:** It is possible to login using NULL sessions. Anonymous users may exploit this vulnerability to obtain usernames and the share list.
- **Unquoted/Trusted Service Paths Security Issue:** Path names become ambiguous when a file name contains a space and is not quoted resulting in multiple different paths. This may be used to escalate privileges on the affected systems.
- **SMB Signing disabled or not required:** Additional security is introduced through SMB signing, in which the client and server authenticate an SMB session on a packet by packet basis.
- **LM/NTLMv1 Authentication method:** The affected systems were identified using LM and NTLMv1 authentication methods. These protocols are not secure and should no longer be used in production.
- **SMB version 1 enabled:** SMBv1 is outdated, has known vulnerabilities and was exploited by the infamous WannaCry ransomware attacks.
- **SNMP version 1 enable:** SNMPv1 is out-of-date, and authentication of clients is performed only by a "community string," in effect a type of password, which is transmitted in cleartext.
- **StickyKeys enabled:** Windows StickyKeys can be triggered before authentication on a Windows host by pressing the Shift key five times quickly which call the executable C:\Windows\System32\sethc.exe. If an attacker manages to replace the StickyKeys executable, they will be able to execute arbitrary code and gain Administrator privileges with minor difficulty.
- **VSSAdmin enabled:** The built-in Windows application vssadmin.exe enables local users to create shadow volume backups which can contain sensitive information such as account password hashes. An attacker can use these hashes in a replay attack to gain access to systems or crack the hashes to reveal the plain-text account credentials.
- **Default Administrator account not renamed:** The built-in local administrator was not found to be renamed and may be vulnerable to brute-force attacks.

## Affected Assets

- ▶ Multiple additional assets affected, please review the Acme Qualys VA files for a complete inventory.

## Recommendation

To remediate the vulnerabilities as a result of insecure configurations, the following is advised:



- **Enabled cache logon credentials:** Set or create a registry key REG\_SZ 'CachedLogonsCount' entry with a value of '0.'
- **Insecure password configuration:** Reconfigure the Administrator's Account password to expire and ensure it adheres to a strong corporate password policy.
- **Allowed Null Sessions:** Disable Windows null sessions (HKLM\SYSTEM\CurrentControlSet\Control\LSA RestrictAnonymous = 1).
- **Unquoted/Trusted Service Paths Security Issue:** Change all service paths to be encapsulated with double quotes if spaces exist in directory path or file name.
- **SMB Signing disabled or not required:** Where possible, implement SMB signing.
- **LM/NTLMv1 Authentication method:** Deprecate support for LM and NTLMv1.
- **SMB version 1 enabled:** Disable SMBv1 and mandate usage of SMBv3.
- **SNMP version 1 enable:** Disable SNMPv1 and implement SNMPv3.
- **StickyKeys enabled:** Disable StickyKeys on all Windows systems.
- **VSSAdmin enabled:** Rename or disable the vssadmin.exe application.
- **Default Administrator account not renamed:** Disable or rename the default account names so it will increase the difficulty level on brute forcing attacks.

## 5.4 Password Audit

### 5.4.1 Active Directory Password Audit

To validate the efficiency of the authentication and identity management systems in place at Acme Inc., a password audit was completed. The objective of this activity was to measure compliance with industry standards and understand the overall strength of user credentials.

The following table outlines the findings identified as part of this testing:

Location	Key Findings	Overall Risk Level
<div> Active Directory</div>	<ul style="list-style-type: none"><li>• Usage of weak credentials "Summer2021", "Winter2021", "Welcome1", and "Acme1" may be triggered by an operational process (onboarding) of new users.</li><li>• Consistent use of weak credentials "Welcome1" and shared credentials on high privileged accounts may lead to a cascading compromise of critical servers in the event one system is compromised.</li><li>• Some resources may still be using LM authentication.</li><li>• Lack of password complexity requirements enable users to have short passwords.</li></ul>	<div> High</div>

## Password Statistics

Top 10 passwords	Top 10 base words	Character sets	Password length
Summer2019! 100 (30.74%)	Summer 137 (14.35%)	mixedalphanum 604 (63.25%)	3 1 (0.1%)
Winter2019 32 (20.02%)	Winter 63 (6.6%)	mixedalphaspecialnum 263 (27.54%)	5 1 (0.1%)
Welcome1 28 (2.93%)	Welcome 50 (5.24%)	loweralpha 27 (2.83%)	6 21 (2.2%)
Acme1 24 (2.51%)	Acme 44 (4.61%)	loweralphaspecialnum 20 (2.09%)	7 19 (1.99%)
Winter2019 23 (2.41%)	password 30 (3.14%)	loweralphanum 16 (1.68%)	8 340 (35.6%)
Password123 22 (2.3%)	123456 28 (2.93%)	mixedalphaspecial 3 (0.31%)	9 172 (18.01%)
abcd!234 11 (1.15%)	monday 21 (2.2%)	upperalphaspecialnum 2 (0.21%)	10 246 (25.76%)
P@ssword1 11 (1.15%)	password 13 (1.36%)		11 116 (12.15%)
Temp123! 9 (0.94%)	newuser 10 (1.05%)		12 24 (2.51%)
acm31! 7 (0.73%)	temp 9 (0.94%)		13 7 (0.73%)
			14 4 (0.42%)
			15 2 (0.21%)
			16 2 (0.21%)

## Passwords Breached

The passwords obtained were tested through haveibeenpwned.com which checks if any of the passwords currently used at Acme Inc. have been previously disclosed in a breach.

**242 of the 493 recovered passwords have been breached.**

## Recommendation

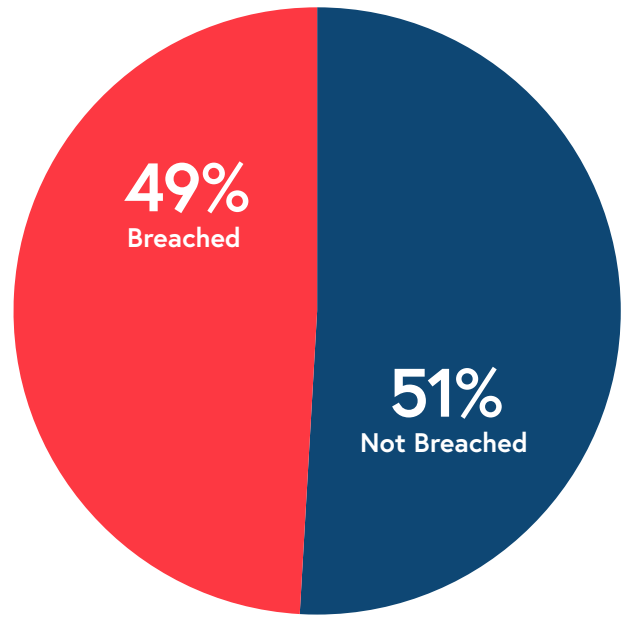
Revisit corporate password policies and where possible. There are generally two approaches to password policies:

### Complex Passwords:

- Usage of mixed-case (uppercase/lowercase alpha)
- Usage of special characters (e.g., !@#\$%^&\*()\_+)
- Usage of numbers
- Minimum length of 12 characters
- Consider the use of passphrases  
Rotation of passwords in 3-6 months per year

### Passphrases

- A phrase that is easy to remember, but very lengthy (no restriction on character sets)
- Minimum length of 16 characters





- Rotation of passwords in 6-12 months per year
- Example: My Password Is Good, But Not Great or MyPasswordIsGood,ButNotGreat

Ensure all cracked passwords are reset. Multiple Acme user accounts have been affected, please consult the Appendix B spreadsheet.

## 5.5 Network Security Testing

To validate the efficiency of the network-based restrictions implemented in the Acme Inc. network, Wireless penetration testing was performed at one Acme locations to measure the effectiveness of the security controls in place.

The following table outlines the findings identified as part of this testing:

Location	Findings	Overall Risk Level
 Wireless Network	The PMKID and the four-way handshake were obtained on two segments through de-authenticating clients, however, it was not possible to crack the pre-shared key within the time window. It was observed that enterprise SSIDs utilize WPA2-enterprise and require domain credentials to authenticate into the network.	LOW
 Wired Network	Various segments in the Acme environment broadcasts insecure protocols such as LLMNR, NBT-NS, and DHCPv6. Furthermore, all tested segments lack egress filtering which allows for trivial exfiltration of data, and reverse connections if malware was executed on user endpoints.	MEDIUM

## Supporting Evidence

Implement NAC / 802.1X on wired network to reduce the potential for unauthorized access.

## 5.6 Ransomware Simulation

Each ransomware strain has its own unique way of propagating or worming through a network. The techniques used have been mimicked in the environment to identify the success or failures of each unique strain. The strains also utilize different attack vectors, or entry points into the network. Each of these scenarios have been tested to identify weaknesses across people, processes, and technology. The scenarios assessed include:

- Phishing to gain internal access. Every strain uses phishing to obtain credentials or to request a malicious download
- Unauthenticated internal access to the network – if a rogue individual plugs a device into the network, where could the ransomware reach
- Authenticated internal access – if a user was to execute ransomware, which areas are at risk. This test includes having access to multiple user accounts

### 5.6.1 Findings

The table below shows the status of the three scenarios that were assessed. The results indicate the number of shares that would be affected by ransomware.

Threat	Risk	Results
Phishing	LOW	Credentials were gained through a mass-phishing campaign, but internal access was not achieved.
Unauthenticated	LOW	No files or directories are accessible to non-domain joined users.
Authenticated	MEDIUM	3 shares with read, write permissions on 201 files or directories for domain users. 14 file shares with read-only access.  Access to backup servers was not obtained in the given timeframe of the engagement, thus lowering the impact in the case of a ransomware attack.

### 5.6.1.1 Unauthenticated Internal Access

No files or directories were accessible to non-domain joined users.

### 5.6.1.2 Authenticated Internal Access




The file shares below are read and writeable which can be problematic during a ransomware outbreak.

Share Drive	Permissions	Number of Files
//10.0.0.1/SHARE	Read/Write	51
//10.0.0.2/ACME	Read/Write	7
//10.0.0.3/IT	Read/Write	143

### 5.6.2 Findings Breakdown

Modern ransomware gangs utilize overlapping tactics, techniques, and procedures to infiltrate, laterally move, and execute their malware and exploit kits. These applications have automated functionality to propagate through the system or network in a predictable manner. The predictability allows for the root causes to be identified and to highlight potential weaknesses in the network. The table below was created to help visualize the tactics, techniques, and procedures to show how each protocol or binary could be used to infect or laterally move in the network.

Protocol	Description	Risk	Compensating Controls
Windows Management Instrumentation Command (WMIC)	Used to modify security settings or execute code on remote machines after obtaining credentials.	 <b>High</b>	No preventative compensating controls and a lack of network detection measures to prevent malware propagation through WMI.

Protocol	Description	Risk	Compensating Controls
Windows Remote Management	Uses remotely access or compromise hosts after obtaining credentials.	 <b>Medium</b>	While there are no compensating controls, most servers and endpoints do not utilize this remote management protocol.
Remote Desktop	Adversaries may use compromised accounts to login via authorized methods such as RDP.	 <b>High</b>	No compensating controls that limit the ability to perform RDP connections as this is the primary choice for managing servers in the environment.
Distributed Component Object Model	Uses credentials obtained by the system to laterally move.	 <b>High</b>	A pre-condition of this propagation technique relies on uploading xml or csproj files. [anti-virus] is effective at preventing such files to be uploaded.

### 5.6.3 Findings Breakdown: Credential Access

A core part of lateral movement is how adversaries attempts to access legitimate credentials in a given enterprise network. This finding attempts to illustrate an organization's host-based controls and host-based detections against common techniques that adversaries use to trivially bypass these controls to access privileged credentials. Organizations that have detections built against these tactics will often be able to detect an intrusion before a ransomware infection becomes imminent.

#### 1. Access to the Local Security Authority Subsystem Service

[Details on how access would be obtained]

### 5.6.4 Ransomware Scenario

In order to simulate a potential ransomware attack on the target environment, the following attack path was chosen to ensure maximum efficacy.

[Further details about how ransomware would propagate through the environment]



## Recommendation

- **Application Control**

Currently, [anti-virus] has the ability to maintain control of fixed-function devices with its application control features. During the ransomware simulation, a malicious XML file was uploaded and called with the MSbuild.exe application. This is usually benign because this binary is a legitimate Microsoft signed binary used for code compilation. This is indicative that Acme IT did not configure its EDR to block certain applications from executing malicious code.

- **Credential Protection**

Usually, if [anti-virus] is configured correctly, it would be sufficient in memory defense blocks. When this is configured, detections would be triggered when the lsass.exe process is attempted to be read or dumped. This would severely limit an attacker's ability to procure credentials for elevated access. In the Acme IT environment, credentials could be trivially procured by using Task Manager and creating a memory dump of the lsass.exe process.

- **Network Limitation**

Since Windows Active Directory environments often utilize WMI, SMB, and RDP protocols, it would not make sense to remove these protocols. Removal of these protocols will often break functionality or compatibility issues. Instead, Blue Teams should ensure that laptops connected onto the VPN or laptops in the corporate environment could not communicate using these protocols.



# 6. Recommendations

## Remediation Plan

Multiple components were found to have a **high** of compromise which indicates sensitive information is at risk for unauthorized access or disclosure. Based on this, the recommendations provided as part of this assessment have been prioritized based on risk and perceived impact.

### 6.1 Tactical Security Recommendations

#### Physical/Objective-Based Testing:

**HIGH**

5.1.1: Ensure there is a policy defined for handling visitors and that the policy is known by all staff and adhered to under all circumstances. The policy should specify in detail the protocols to be followed when signing in guests. Have a mechanism to identify guests such as a visitor badge and internal contact. Guests must be associated with a Acme employee who is responsible for the guest, and have a procedure to follow when an unauthorized visitor is identified.

**HIGH**

5.1.2: Implement and mandate the use of encrypted RFID access cards. Alternatively, if this is not possible, consider implementing multi-factor authentication on physical access controls.

#### Phishing and Reconnaissance:

**HIGH**

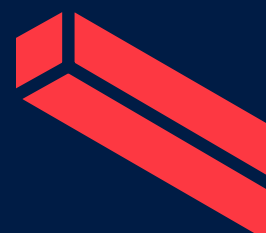
5.2.1: Enhance security awareness training.

#### Infrastructure:

**HIGH**

5.3.1: Ensure that endpoint protections are also applied to test servers within the environment. Alternatively, limit access to test servers only to authorized users that need access.

- HIGH** 5.3.2: Restrict usage of shared credentials and prohibit interactive login where possible. Restrict and reduce the number of users with Domain admin privileges are knowledge of Domain admin credentials. Install EDR software on all systems. Implement reoccurring update schedule.
- HIGH** 5.3.3: Where possible, disable both LLMNR and NBT-NS, deprecate support for NTLMv1 and enforce SMB signing.
- HIGH** 5.3.4: Apply the latest security patches and validate missing patches are part of recurring patch schedule.
- HIGH** 5.3.5: Investigate corporate hardening standards and ensure SMB Signing is enabled.
- HIGH** 5.3.6: Adhere to the principle of least privilege within the Active Directory environment. Restrict remote access to only users that require access to the internal network. For general file sharing purposes, ensure proper credential hygiene is followed.
- HIGH** 5.3.7: Conduct an entitlement review of foreign group memberships between [domain 1] and [domain 2] and remove access where needed.
- HIGH** 5.3.8: Adjust registry and disable insecure services to harden infrastructure.





# 7. Appendix A

## Mitigation Test Results

### 7.1 Insecure SSL Configuration

Our findings serve one key purpose - strengthening your security posture. With our comprehensive methodology, we not only analyze complex attack paths to find vulnerabilities, we offer up solutions that actually move the needle.

Vulnerability	Assets Affected
SSL/TLS supports TLSV1.0	<ul style="list-style-type: none"><li>10.10.10.56/443</li><li>10.10.10..65/443</li></ul>
SSL server has SSLV3 enabled vulnerability	<ul style="list-style-type: none"><li>10.10.10.15, tcp/636</li><li>10.10.10.15, tcp/3269</li><li>10.10.10.17, tcp/636</li></ul>
SSL server Has SSLV2 enabled vulnerability	<ul style="list-style-type: none"><li>10.10.10.15, tcp/636</li><li>10.10.10.15, tcp/3269</li><li>10.10.10.60, tcp/443</li></ul>

# 8. Appendix B

## Credential Harvest Phishing Results

Email	user1@acme.com
1st Password	Welcome1
2nd Password	null
Date	2019-06-08
Time (UTC)	13:05:20
IP Address	1.2.3.4

Email	user2@acme.com
1st Password	Summer2019!
2nd Password	null
Date	2019-06-08
Time (UTC)	13:09:43
IP Address	1.2.3.4



# Ready to strengthen your security posture?

There's simply no room  
for compromise.

Get in touch to share your  
cybersecurity needs with our  
team and get a free quote.

📞 647 797 9230

@ info@packetlabs.net

🌐 packetlabs.net

📍 606-6733 Mississauga Road, Mississauga, ON, L5N 6J5

🐦 @pktlabs

🌐 /packetlabs-ltd-

📘 @packetlabs



Scan **QR code**  
to book a virtual  
consultation with us.

