VOLKIS™

Penetration Test

Prepared for Client, 26 February 2023

Table of Contents

Executive summary

Parent Company (Client) engaged Volkis to perform penetration testing on their internal, external and Wi-Fi infrastructure.

Volkis used the same hacking tools that hackers will use to investigate and understand the scope, then find and exploit identified security vulnerabilities. The testing investigated the internal and external infrastructure for security vulnerabilities that could present risk to Client. Such as viewing sales data, viewing/editing employee personal identifiable information (PII), business strategy documents, financial fraud and disruption to employee daily operations.

Volkis were unable to compromise Client's external environment within the duration of the engagement. However, Volkis was able to completely compromise the internal environment due to the presence of several high risk vulnerabilities.

The consultant was acting as a threat actor who had a planted device on the Client internal network. Chaining multiple vulnerabilities together allowed the consultant to compromise the **client.net.au** domain which gave the control of all Windows servers in the domain, access to employee PII, sales data and strategic documents. The root causes of the compromise can be attributed to weak password practices, insecure multi-factor authentication (MFA) policy and vulnerable active directory configurations.

Client's password policy allows for short and common passwords. When paired with a lack of awareness in password management, the results were passwords that were easy for an attacker to guess and crack. This aided in compromise of accounts within the Active Directory environment. After intercepting and cracking employee passwords, the consultants were able to access employee Microsoft 365 (M365) services such as SharePoint, Microsoft Teams and OneDrive due to an insecure conditional access policy bypassing the MFA requirement if an individual is on an Client office network. Furthermore, the Active Directory environment contained various default and vulnerable configurations which allow for privilege escalation to the highest level of access (Domain Admin) within the environment. This indicates that the Active Directory environment has not been hardened against threat actors.

An attacker with Domain Admin privileges can execute attacks against Client with the highest possible level of impact. This includes significant disruption to business operations by executing a ransomware attack against the windows servers in the internal environment from which it may be impossible to fully recover. Additionally, access to the Domain Admin account allows the attacker to extract and crack the passwords of all user accounts.

This could lead to compromise of employee Microsoft 365 accounts which are used to authenticate to third party systems such as Payroll software and document verification software. Exfiltration and sale of employee personal information, sensitive data or intellectual property may cause financial, legal, and reputational damages for Client.

The external penetration test identified two significant issues within the target environment. Firstly, there are unpatched systems, which present vulnerabilities that could be exploited by malicious actors to gain unauthorized access to sensitive information or cause a disruption to the service. Secondly, cryptography issues were identified, which could potentially lead to the exposure of sensitive data and compromise of the system's confidentiality.

To improve the overall security posture, Client should follow the recommendations laid out in this report. Volkis recommends performing the following high level tasks:

- Improve the password policy.
- Harden the Active Directory environment.
- Conduct information security awareness training for all employees.
- Disallow MFA exceptions if you are on the location on a Client office network.

For more information about this report, the identified vulnerabilities, and additional services that could help you in your security journey, please contact your Volkis consultant:

Volkis Consultant

- Email: consultant1@volkis.com.au
- Mobile: 0400 000 000

External

	Title	Risk
1	Unpatched systems	**High**
2	SSH misconfigurations	**Low**
3	TLS misconfigurations	**Low**

Internal

	Title	Risk
4	ADCS attacks	**High**
5	DHCPv6 poisoning	**High**
6	Kerberoasting	**High**
7	Name resolution poisoning	**High**
8	Unpatched and unsupported systems	**High**
9	Weak password policy	**High**

Continued on next page

	Title	Risk
10	Coerced authentication (authenticated)	**Medium**
11	Machine account quota	**Medium**
12	NTLM relay	**Medium**
13	Password stored in user description	**Medium**
14	Unconstrained delegation configuration	**Medium**
15	RDP terminal level authentication	**Low**

Wi-Fi

	Title	Risk
16	Evil twin attack	**Low**
17	MFA Bypass through Guest wireless network	**Low**

Overview

Client engaged Volkis to perform penetration testing on their Internet accessible external infrastructure as well as their internal and wireless environments.

Testing was performed in February 2023.

Scope

The scope of the penetration testing included:

External penetration test

IP Address	Location
x.x.x.x/29	ISP
x.x.x.x	ISP
x.x.x.x	ISP
x.x.x.x	ISP
x.x.x.x	ISP

Internal penetration test

- 10.0.0.0/16
- 172.16.0.0/24

Wi-Fi penetration test

- Client-Guest
- Client-Office

Root cause analysis

This section highlights what we determined to be the likely root cause of the vulnerabilities discovered. By addressing the root cause, you reduce the chances of introducing new vulnerabilities of the same class.

Active Directory hardening

The Active Directory has insecure default settings, possibly highlighting ineffective system hardening guidelines. These guidelines help to ensure that systems in-use are configured to security best practices and may protect against common attacks.

Several issues identified during the engagement were a result of Active Directory not being securely configured. Before systems are deployed their configurations should be hardened to meet a minimum security baseline. This reduces the overall attack surface [1] available to threat actors.

Information security awareness training

Even though most employees have no experience in information security, security is never-the-less becoming a key part of the work of every person who works with computers. This means the employees need training on the information security requirements and expectations for their work.

Effective Information Security Awareness Training (ISAT) programmes incorporate a mixture of classroom style presentations or computer-based training, regular updates using emails or announcements in team meetings, and posters in visible locations.

Client should consider implementing an ISAT programme for its staff. This will help to grow the security culture of the organisation and protect the company from social engineering attacks.

Insecure Multi-Factor Authentication (MFA) Policy

Client has successfully enrolled all employees onto MFA for their Microsoft 365 (M365) accounts. However, Client has configured a trusted locations policy which allows any employee to be exempt from MFA if they are located within any Client office.

This allowed the consultant to access employee M365 accounts without being prompted for MFA.

The consultant accessed M365 services such as SharePoint, OneDrive, Word, Excel, OneNote and Outlook without being prompted for MFA. This permitted the compromise of the HR System and other servers either via Single Sign On / clear text documents found in OneDrive or SharePoint.

Additionally, if you are connected to the Guest Wireless network, it is also considered a trusted location as it has the same outgoing IP address as the corporate network. If an attacker can compromise a set of Client employee credentials, they could bypass the MFA requirement by getting within physical distance to access the Guest Network.

Client should recommend turning off the Trusted Locations policy for MFA.

[1] https://en.wikipedia.org/wiki/Attack_surface

Password handling

The password handling of Client was ineffective at protecting against password guessing, password spraying, brute-force, and other password attacks. The insecure handling of passwords included:

- Reuse of passwords between accounts;
- Weak passwords based on dictionary words;
- Weak password requirements and group policy;
- Plaintext passwords stored in OneDrive/SharePoint.

Passwords are the key for accessing the sensitive data and business functions of the organisation. Weak passwords will lead to weak security and can lead to compromises in the organisation.

The following controls may assist in improving password handling at Client:

- Effective password policies combined with password selection being a part of user awareness training will help users to create stronger passwords.
- Using a password manager to generate secure password and storing them in the password vault.
- Multi-factor authentication can decrease the reliance on passwords as the single factor of security.

Patch management

A patch management program is designed to reduce Client exposure to newly released vulnerabilities. Several of Client operating systems and applications were affected by vulnerable software. This indicates that a patch management program may not be in place or if a patch management program is in place that it is not effective.

Create or update the patch management program to include Client's missing operating systems and applications.

System hardening

Systems were found to use insecure default settings, possibly highlighting ineffective system hardening guidelines. These guidelines help to ensure that systems in-use are configured to security best practices and may protect against common attacks.

Several issues identified during the engagement were a result of Internet facing systems not being securely configured. Before systems are deployed their configurations should be hardened to meet a minimum security baseline. This reduces the overall attack surface [2] available to threat actors.

Additional information on system hardening can be found at the Australian Cyber Security Centre (ACSC):

- https://www.cyber.gov.au/acsc/view-all-content/advice/guidelines-system-hardening

Effective security practices

Volkis likes to celebrate the positives! This section highlights some of the effective security practices and controls that were observed during the penetration test.

[2] https://en.wikipedia.org/wiki/Attack_surface

Security logging and monitoring

During the engagement, Volkis discovered Client performed appropriate security logging and monitoring which identified some of the activities that the consultants performed during the penetration test.

Additional recommendations

Defence-in-depth is a security concept that teaches multiple layers of protection against adversaries. These recommendations are not specifically related to a vulnerability but will increase the overall security of the organisation.

Access to management service

The phone system management console was exposed to the internet. Unauthorised access may allow for the phones to be reconfigured.

It would require the existence of other vulnerabilities for unauthorised access to be obtained, such as weak passwords.

Host	Port	Service	URL
x.x.x.x (Public IP)	5001	Phone System Management Console	https://x.x.x.x:5001/

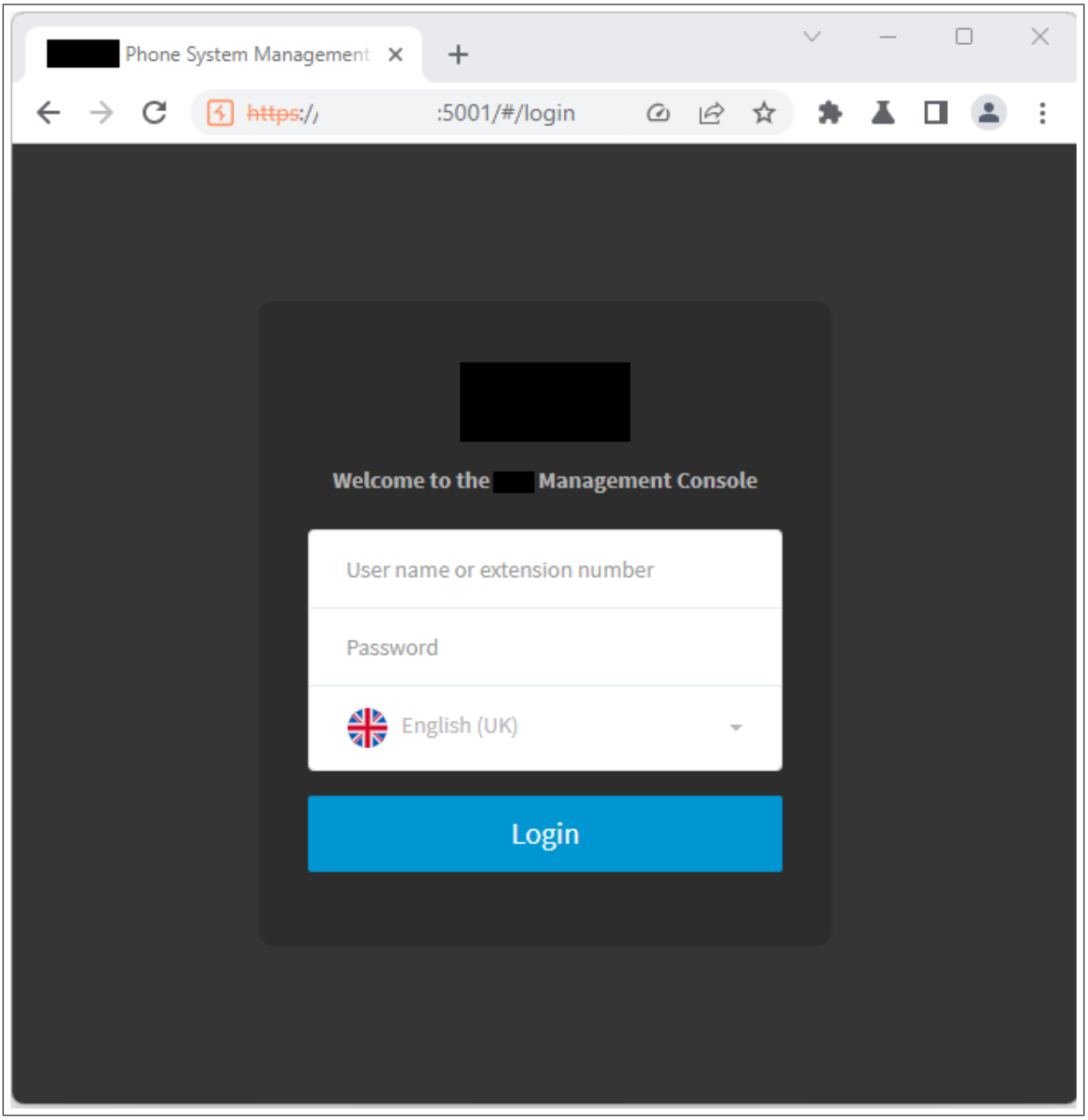


Figure 1: Phone management console

Restrict access to this service as much as possible.

Additional penetration testing

Additional hosts of Client were identified through enumeration that were not in scope for testing.

The following hosts were affected:

- client.com
- images.client.com

- server1.client.com
- vpn.client.com
- vpn2.client.com
- www.client.com

It is recommended that they be included in future penetration tests.

Avoid using domain-level administrators

During the internal penetration test, it was discovered that the domain-level Administrator accounts was used for normal network tasks. Hashed credentials for the Administrator account were found on other servers on the network and assisted the consultant in compromising the network.

This account is the most sensitive account in the entire domain and should only be used in emergency situations when other Domain Admin accounts are inaccessible.

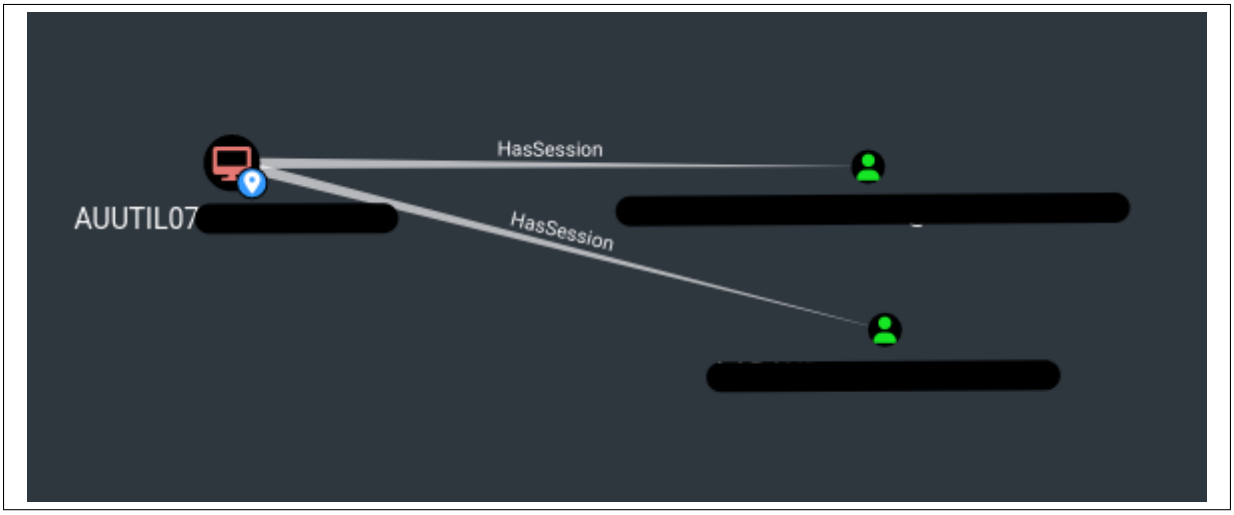


Figure 2: Two domain admins having sessions on server

Cloneable RFID Cards

The consultants identified that Client utilises HID Proximity RFID cards which are vulnerable to cloning.

If an attacker can get within half a metre of a Client employee, they can create their own RFID card from the cloning process. This would allow an attacker to have unauthorised access the Client office including the internal network.

Upgrading the RFID readers and cards to a modern solution is advised.

Disable Office Macros

Office macros are notorious for being abused by attackers performing phishing. They embed malicious code into the macro and create a pretext to trick victims into unwittingly running the macro. Due to the risk, macros should be disabled for all Office documents.

Recommendations

Set the following GPO items:

```
User Configuration\Policies\Administration Templates\Microsoft Office 2016\
    Security Settings\Automation Security
```

Value: Enabled

Set the Automation Security level: Disable macros by default

```
User Configuration\Policies\Administration Templates\Microsoft Office 2016\
    Security Settings\Automation Security
```

Value: Enabled

```
User Configuration\Policies\Administration Templates\Microsoft Office 2016\
    Security Settings\Trust Center\Allow mix of policy and user locations
```

Value: Disabled

Excessive Domain Administrators

Client has 35 users with Domain Admin privileges. Domain Admin privilege is the highest level of access that can be granted to a user, allowing that user to execute administrative actions on any domain joined system such as installation of software, management of services, users and groups, etc.

A large number of Domain Admins is not a vulnerability, but it does increase the chances of an attacker gaining high-level privileges if passwords are not appropriately managed. Should any of these accounts be compromised by an attacker, they would have full control over Client's domain and servers. This could result in significant damages to Client.

Domain Admin privileges should only be granted to user accounts used for the management of the domain. If administrative privileges are required for a service, only the specific privileges required should be granted to the user.

It is recommended to audit Domain Admin group membership and remove all accounts that are not used to manage the domain.

Insecure methods enabled

The TRACE method is an HTTP method that allows clients to retrieve diagnostic information about the request and response messages exchanged with a web server.

Enabling the TRACE method could allow for Cross-Site Tracing (XST), which occurs when an attacker injects malicious JavaScript code into a vulnerable website that forces the browser to send an HTTP TRACE request to the attacker's server. The attacker can then capture sensitive information, such as session IDs, authentication tokens, or cookies, contained in the TRACE request header.

Host	Port	Header	URL
x.x.x.x (Public IP)	50000	TRACE	https://x.x.x.x:50000/

Disable the TRACE header if it is not required.

Network segmentation

Ineffective network segmentation was identified during the engagement. This means that any devices connected to the Client network can reach most other network subnets, including those containing business critical assets such as the SAP and TM1 servers.

If an attacker was able to gain access to an office site network, they could reach and attack business critical assets. They could leverage other vulnerabilities identified during the engagement to compromise the network. It also significantly increases the effectiveness of ransomware attacks, as the ransomware can reach most assets in the internal network.

Stringent network segmentation provides an extra layer of security by allowing control over access to network assets. It can also reduce the overall impact in the event of a compromise.

Perform a Standard Operating Environment (SOE) security review

To reduce the risk of adversaries gaining these credentials in the first place, Volkis recommends performing a SOE security review in order to harden the environment, since the most likely attack vector to the Client environment could be phishing. A hardened SOE image can reduce the impact of a cyber attack against Client employees. A SOE security review typically assesses a client's SOE image against multiple security standards such as CIS Benchmark[3], Essential 8[4] or the Information Security Manual[5].

Server isolation

Multiple hosts is scheduled to be decommissioned, as such any identified vulnerabilities may not be remediated. As there were vulnerabilities identified, it is recommended to isolate the host until it is decommissioned. This will help mitigate the risk of exploitation.

The following hosts were affected:

- OLD_SERVER01
- OLD_SERVER02
- OLD_SERVER03
- OLD_SERVER04

Isolation can be performed in a number of ways, such as:

- IP whitelist the corporate office IP address(es) and have any offsite employees use a VPN to allow them to access the internet using the office IP.

[3] https://www.cisecurity.org/cis-benchmarks
[4] https://www.cyber.gov.au/acsc/view-all-content/publications/essential-eight-maturity-model
[5] https://www.cyber.gov.au/acsc/view-all-content/ism

- Remove internet access from the host and only allow it to be accessible from the internal corporate network.

SharePoint files audit

A large number of network shares that are accessible to low privileged domain users was observed. A large number of shares can make it difficult to effectively manage and monitor sensitive data and increases the overall attack surface of the Client network.

It is recommended that a review of network shares be performed and shares that are no longer required be removed and backup locations be consolidated. Ensure that shares have their Access Control lists reviewed to prevent unauthorised access to business critical data.

Unnecessary service exposed

Limiting the attack surface of a system can help protect it from exploitation by cutting off avenues for access. As such, it is best practice to reduce the number of ports and services exposed on a host.

The ERP system is exposed to the Internet. Authentication is required to access this service and any sensitive information it contains.

Host	Port	Service	URL
x.x.x.x (Public IP)	50000	ERP system	https://x.x.x.x:50000/

This service should be reviewed to ensure it is necessary that they are exposed.

Unsupported system

A system that is no longer supported by the vendor implies no new security patches will be released for the product. It is more likely for security vulnerabilities to be discovered and remain unpatched if the software is not supported.

End of life systems are no longer supported by the vendor, which could lead to unpatchable vulnerabilities in the future. Remaining on a vendor supported version of systems allows future vulnerabilities to be patched as soon as possible.

Host	Port	System
x.x.x.5	50000	OpenSSL 0.9.8j
x.x.x.6	50000	OpenSSL 0.9.8j
x.x.x.5	2220	PHP 5.6.34
x.x.x.6	1521	Oracle Database 12.1.0.1.0
x.x.x.8	55622	Microsoft SQL Server 12.0.2269.0
x.x.x.125	80	Microsoft IIS 7.5

Continued on next page

Host	Port	System
x.x.x.125	443	Microsoft IIS 7.5
OLD_SERVER01.client.net.au	N/A	Windows Server 2008 R2 Standard Service Pack 1
OLD_SERVER02.client.net.au	N/A	Windows Server 2008 R2 Standard Service Pack 1
OLD_SERVER03.client.net.au	N/A	Windows Server 2008 R2 Standard Service Pack 1
OLD_SERVER04.client.net.au	N/A	Windows Server 2008 R2 Standard Service Pack 1

The systems should be updated to the latest supported version where possible. If not possible, apply all applicable security updates and plan to decommission the systems.

Conclusion

Volkis performed a penetration test on Client and discovered vulnerabilities that could cause **High** impact to the organisation. We recommend remediating the vulnerabilities found in the report and addressing their root causes to protect the organisation from attacks.

We're here to help! If you find yourself needing assistance with fixing a vulnerability in this report or are unsure what the next step in your security strategy should be, reach out. Volkis's consultants are experts in the information security field who love to talk shop.

Thank you for letting us hack your infrastructure and thank you for reading.

Volkis Consultant

Attack Walkthrough

This section describes the path the consultant took, starting with no access other than physical port access and eventually gaining full control over the network and sensitive company data. It demonstrates how combining multiple vulnerabilities and chaining exploits can result in a severe consequence for the organisation. Attackers in a similar position would likely gain the same result.

Reconnaissance

The consultant began by performing reconnaissance on the internal network using a tool called **nslookup** to identify where high value target servers, such as Domain Controllers were located.

Using the following **nslookup** command locates all four Domain Controllers on the internal network.

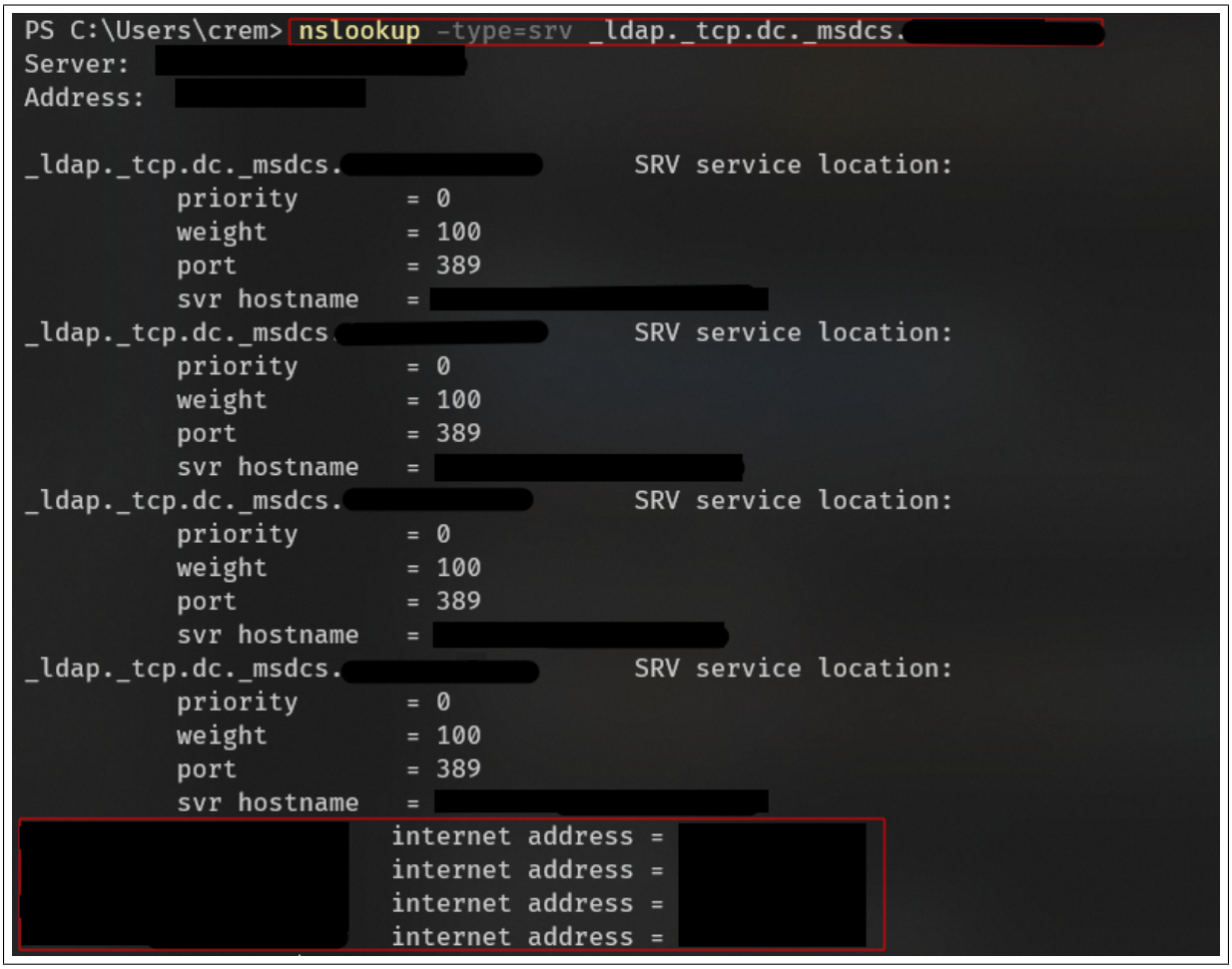


Figure 3: Using an nslookup command to locate the Domain Controllers

Other sensitive servers were identified via further enumeration using **CrackMapExec**, **nmap** and **wireshark**.

Gaining a low-privileged account

On an Active Directory network, name resolution protocols such as **Link-Local Multicast Name Resolution (LLMNR)** and **NetBIOS Name Service (NBT-NS)** are enabled by default. The consultant wanted to see if these protocols were enabled and then attack them using the tool **Responder**. **Responder** listens for incoming LLMNR/NBT-NS requests and replies back to any requested name with the attackers IP address (refer to **Vulnerability 7: Name resolution poisoning**). The attack did not require any user interaction.

Responder was able to capture a **NTLMv2 challenge** of a Client user.

Figure 4: NTLMv2 challenge from AD User

The consultant took this **NTLMv2 challenge** and cracked it offline using desktop computer with a GPU to obtain the user's password.

Figure 5: The cracked password from the NTLMv2 challenge

The low-privileged account can be used to query information about the Active Directory environment such as:

- Users
- Groups
- Group memberships
- Permissions
- Computers
- Password policy
- Group policy

The consultant checked what value the **ms-DS-MachineAccountQuota** Active Directory attribute as set to. The **ms-DS-MachineAccountQuota** attribute if not set to **0**, allows any Active Directory user to create a Computer Object in the Active Directory environment or join a computer to the Active Directory environment. The consultant created a Windows VM called **VOLKIS01** and joined it to the Active Directory environment.

Figure 6: Checking the value of ms-DS-MachineAccountQuota using CrackMapExec

Privilege Escalation

A common attack path within the Active Directory environment is abusing misconfiguration within **Active Directory Certificate Servers (ADCS)**. For this attack to work an ADCS server has to be identified within the network.

Finding ADCS server

Utilising low privileged credentials, the consultant found an ADCS server with the internal environment using an inbuilt Windows tool called **certutil**.

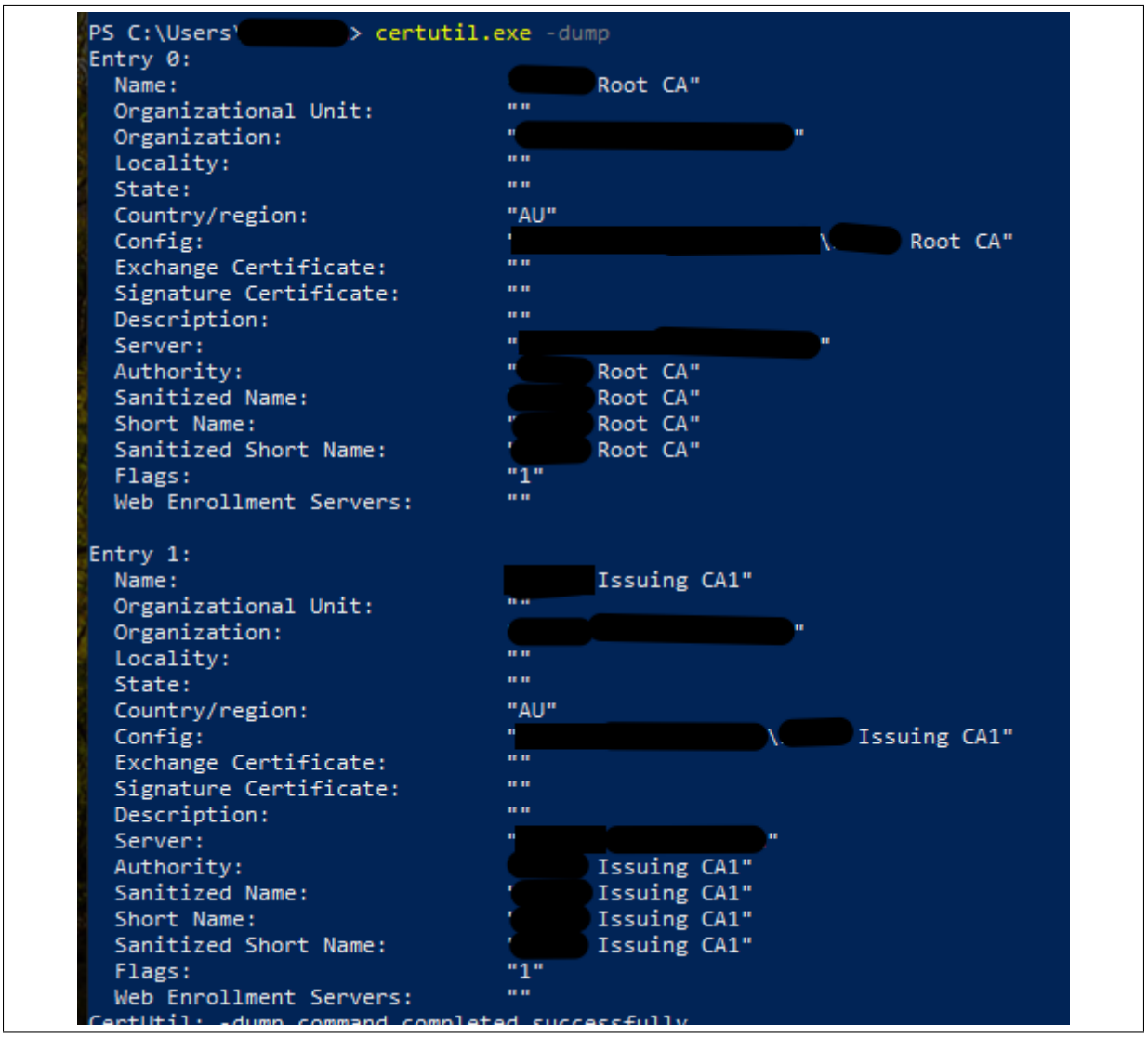


Figure 7: Finding ADCS Server using certutil

Finding vulnerable templates

The consultant identified 4 templates on the **Client Issuing CA1** ADCS server vulnerable to the **ESC4** vulnerability (refer to **Vulnerability 4: ADCS attacks**) where the `NT Authority\Authenticated Users` local group computer (any user logged into a Windows Computer) or `CLIENT\Domain Computers` domain group (any user that has administrative access over a computer) can alter an existing template so that they make request a certificate from the ADCS service for any user.

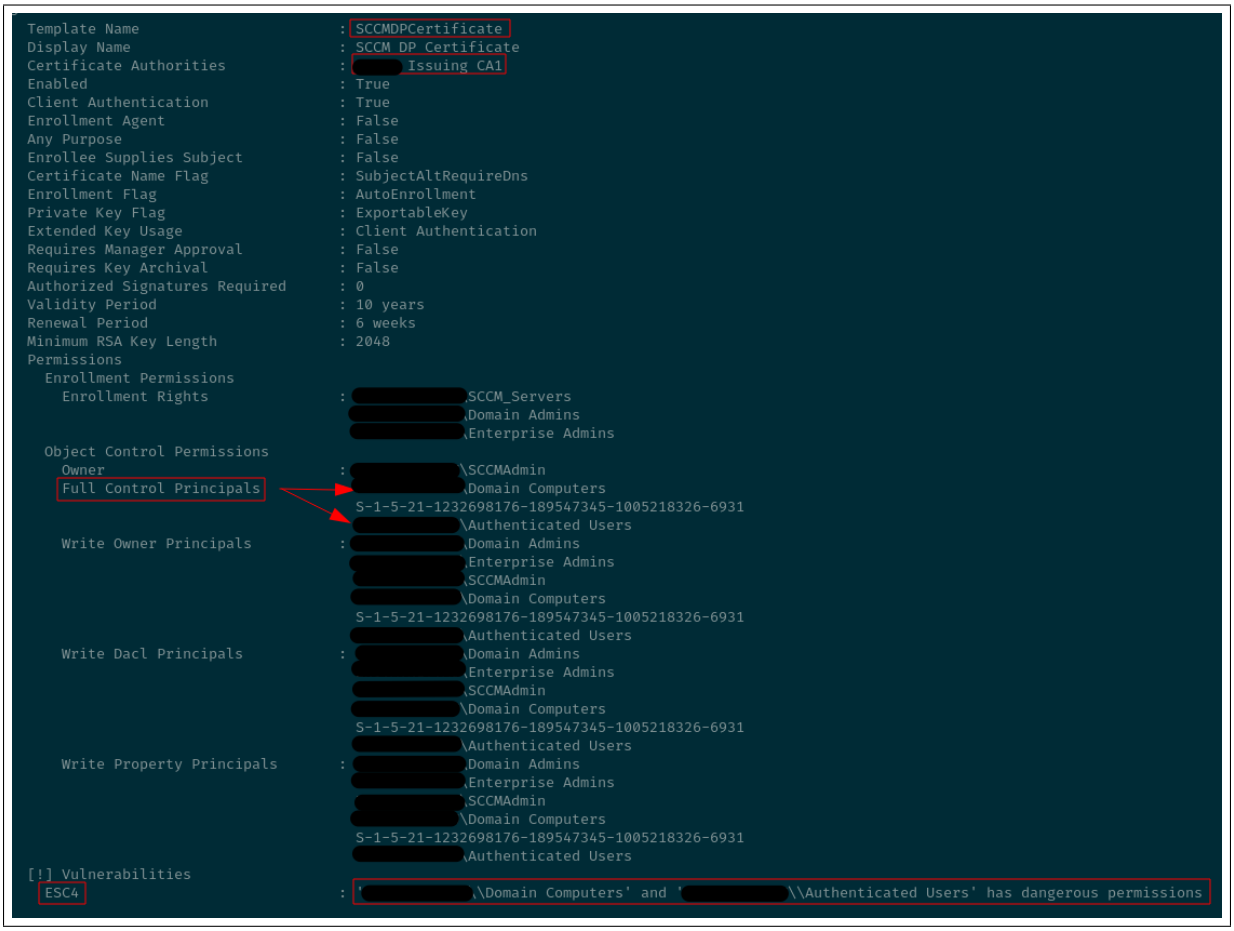


Figure 8: One of the ADCS template vulnerable to ESC4

Performing the ADCS ESC4 attack

A well known and publicly available tool called **Certipy** was used to abuse the **ESC4** vulnerability. The consultant altered an existing template to be vulnerable to be able to request a certificate for one of the Domain Admin users.

```
Certipy on  f3rn0s/main:main [?] via  v3.11.1 (certipy)
❯ certipy template -u [redacted]' -p "pa\$\$w0rd" -template SCCMDPCertificate -save-old
Certipy v4.3.0 - by Oliver Lyak (ly4k)

[*] Saved old configuration for 'SCCMDPCertificate' to 'SCCMDPCertificate.json'
[*] Updating certificate template 'SCCMDPCertificate'
[*] Successfully updated 'SCCMDPCertificate'
```

Figure 9: Using certipy to alter an ESC4 vulnerable template to be vulnerable to request a certificate for a Domain Admin

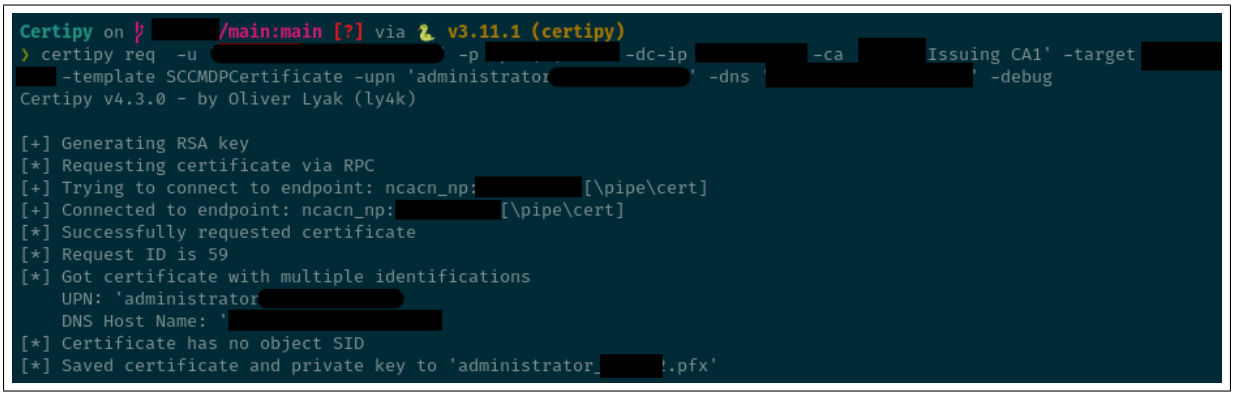


Figure 10: Requesting a Domain Admin Certificate

The **.pfx** file was then used for certificate based authentication using **Certipy** to obtain a Domain Admin's NTLM hash.

In an Active Directory environment, the user's password is not need and the NTLM hash can be used to authenticate as that user using a technique called "Pass The Hash".

Figure 11: Obtaining NTLM hash from certificate based authentication

The consultant then reverted the altered configuration to not introduce a vulnerability into the Client environment.

Figure 12: Reverting the ADCS Template

Pass The Hash to create a Domain Admin Account

Using the **VOLKIS01** domain joined computer, the consultant utilised **Mimikatz** to "Pass The Hash" to make a terminal process with Domain Admin privileges. The consultant then created his own Domain Admin called "crem".

```
C:\Windows\system32>net user crem SuperSecretPassword321+ /add
The password entered is longer than 14 characters.  Computers
with Windows prior to Windows 2000 will not be able to use
this account. Do you want to continue this operation? (Y/N) [Y]: Y^C
C:\Windows\system32>net user crem SuperSecretPassword321+ /add /domain
The password entered is longer than 14 characters.  Computers
with Windows prior to Windows 2000 will not be able to use
this account. Do you want to continue this operation? (Y/N) [Y]: Y
The request will be processed at a domain controller for domain [redacted]

The command completed successfully.


C:\Windows\system32>net group "Domain Admins" crem /add /domain
The request will be processed at a domain controller for domain [redacted].

The command completed successfully.
```

Figure 13: Adding the "crem" Domain Admin account

Using the created Domain Admin, the consultant used Remote Desktop Protocol (RDP) to execute system commands on one of the Domain Controllers to dump the contents of the **NTDS file** that contains all the NTLM hashes for the **client.net.au** domain. With access to this file, the consultant has obtained full access to all user accounts including other Domain Admin accounts.

```
PS C:\Windows\system32> ntdsutil "ac i ntds" "ifm" "create full c:\windows\temp\snapshot" q q
C:\Windows\system32\ntdsutil.exe: ac i ntds
Active instance set to "ntds".
C:\Windows\system32\ntdsutil.exe: ifm
ifm: create full c:\windows\temp\snapshot
Creating snapshot...
Snapshot set {c9669c4d-7e2b-4133-b4ac-47e964c76b63} generated successfully.
Snapshot {be3c201e-c013-4a02-9a39-cabac9f72f4d} mounted as C:\$SNAP_202302271420_VOLUMED$\
Snapshot {ceac2122-38be-4a41-afbf-73a247c344df} mounted as C:\$SNAP_202302271420_VOLUMEC$\
Initiating DEFRAGMENTATION mode...
     Source Database: C:\$SNAP_202302271420_VOLUMED$\NTDS\ntds.dit
     Target Database: c:\windows\temp\snapshot\Active Directory\ntds.dit

                Defragmentation  Status (% complete)

          0    10   20   30   40   50   60   70   80   90  100
          |----|----|----|----|----|----|----|----|----|----|
          ..................................................

Copying registry files...
Copying c:\windows\temp\snapshot\registry\SYSTEM
Copying c:\windows\temp\snapshot\registry\SECURITY
Snapshot {be3c201e-c013-4a02-9a39-cabac9f72f4d} unmounted.
Snapshot {ceac2122-38be-4a41-afbf-73a247c344df} unmounted.
IFM media created successfully in c:\windows\temp\snapshot
ifm: q
C:\Windows\system32\ntdsutil.exe: q
PS C:\Windows\system32>
```

Figure 14: Dumping the contents of the **NTDS file**

Post-Exploitation

The consultant ran the NTDS file through password cracking software for analysis. **85.6%** of current user passwords were cracked within 9 hours on a desktop computer system (refer to **Vulnerability 9: Weak password policy**)

The consultant attempted to access Microsoft 365 accounts and realised that a **Trusted Locations** policy for Multi-Factor authentication is enforced. This policy permits any user that is connected to the internal network in a Client office to not be prompted for multi-factor authentication.

With this level of access, the consultant demonstrated impact of a compromise by logging into various Microsoft 365 accounts including as the Chief Executive Officer. The consultant was able to access Microsoft 365 services such as OneDrive, Microsoft Teams, SharePoint. Furthermore, services connected to Single Sign-On such as Payroll software and document verification software.

Access to Payroll software allowed the consultant to view and edit Personal Identifiable Information (PII) of all employees including:

- Full name
- Date of birth
- Address
- Mobile phone number
- Email address
- Emergency contact
- Direct deposit information

Exfiltration and sale of employee PII may cause financial, legal, and reputational damages.

Access to document verification software could allow an attacker to sign documents such as contracts or invoices as the logged in user which could lead to reputational and financial damage to the business.

The consultant was able to acquire sales data from the TM1 and SAP servers. The TM1 information was acquired from compromising the TM1 server.

While the consultant was not able to compromise the SAP server during the engagement, data backups and exports of the South African SAP server were located on production servers without any form of encryption.

Disclosure of sales data could be sold to competitors which would result in financial damage to the business.

Detailed Vulnerabilities: External

Vulnerability 1: Unpatched systems

Likelihood	Impact	Risk
Possible	Severe	**High**

Risk assessment

The risk varies depending on the vulnerability. An individual rating is given to each unpatched software application and the highest is taken as the overall criticality.

The criticality rating considers the ease of exploitation, if there are existing exploits available and the impact of successful exploitation.

Description

Systems are missing patches that expose them to publicly known vulnerabilities.

The following systems are affected:

Host	System	Current version/Missing patch	Attack type	Criticality
x.x.x.x	OpenSSL	0.9.8j	RCE, DoS, Info	High
x.x.x.x	Apache	2.4.25	DoS, Info, Bypass	High

The table above outlines what vulnerabilities are present for each piece of software, such as:

- Remote Code Execution (RCE).
- Denial of Service (DoS).

- Information disclosure (Info).
- Access bypass (Bypass).

The vulnerabilities exposed may allow an attacker to execute arbitrary code, perform a denial of service attack or compromise sensitive information. Attackers could leverage this access to perform further attacks against the network.

Recommendations

Ensure that systems are running their latest versions by applying the patch using your regular patching process.

Additional application information can be found at:

Application	Reference
Apache httpd	https://httpd.apache.org/download.cgi
OpenSSL	https://www.openssl.org/source/

Vulnerability 2: SSH misconfigurations

Likelihood	Impact	Risk
Rare	Severe	**Low**

Risk assessment

Vulnerabilities in SSH are unique and treated differently by Volkis because of how unlikely their exploitation is. Attackers rarely go after this class of vulnerability due to the complex nature of the exploitation process, the high level of resources required and the prerequisite Man-in-the-Middle (MitM) position needed for the attack.

Successful exploitation may allow an attacker decrypt the encrypted traffic being sent to and from the client and server or gain access to the server. It may allow an attacker to steal login credentials, install malware, or create a backdoor to gain persistent access to the system. Stolen login credentials would allow an attacker to execute commands on the targeted system, gain access to sensitive data, or even take complete control of the system.

Description

SSH (Secure Shell) is a network protocol that allows you to securely connect to remote servers and execute commands or transfer files between your local computer and the remote server. It provides a secure encrypted communication channel over an unsecured network, such as the Internet. SSH uses public-key cryptography to authenticate the remote server and the client, and it encrypts all data transmitted between them.

The following table shows a summary of SSH misconfigurations found. For a detailed description of each vulnerability and how to remediate it, refer to **Appendix A: SSH misconfiguration details**.

Host	Port	Misconfiguration	Specifics
x.x.x.x	22	Weak encryption ciphers	diffie-hellman-group-exchange-sha1
x.x.x.x	22	Weak authentication	Password authentication enabled

Recommendations

For a detailed description of each misconfigurations and how to remediate it, refer to **Appendix A: SSH misconfiguration details**.

Vulnerability 3: TLS misconfigurations

Likelihood	Impact	Risk
Rare	Severe	**Low**

Risk assessment

Vulnerabilities in TLS are unique and treated differently by Volkis because of how unlikely their exploitation is. Attackers rarely go after this class of vulnerability due to the complex nature of the exploitation process, the high level of resources required and the prerequisite Man-in-the-Middle (MitM) position needed for the attack.

Successful exploitation may allow an attacker decrypt the encrypted traffic being sent to and from the client and server. It may allow an attacker to gain access to sensitive information being transferred, such as login credentials. Stolen login credentials would allow an attacker login to the application, exposing any sensitive information it contains.

Description

Transport Layer Security (TLS) and SSL (Secure Socket Layer) is a cryptographic protocol that is used to establish a secure communication channel over the internet between a client (such as a web browser) and a server (such as a website). SSL uses a combination of public and private key encryption to ensure that the data being transmitted between the client and server is secure and cannot be intercepted by unauthorized parties.

The following table shows a summary of TLS misconfigurations found. For a detailed description of each vulnerability and how to remediate it, refer to **Appendix B: TLS misconfiguration details**.

Host	Port	Vulnerability	Specifics
x.x.x.x	4001	Self-signed certificates	-
x.x.x.x	50000	Self-signed certificates	-
x.x.x.x	4001	Vulnerable TLS version supported	TLSv1
x.x.x.x	50000	Vulnerable TLS version supported	TLSv1
x.x.x.x	50000	Weak encryption ciphers	RC4-SHA

Recommendations

For a detailed description of each vulnerability and how to remediate it, refer to **Appendix B: TLS misconfiguration details**.

Detailed Vulnerabilities: Internal

Vulnerability 4: ADCS attacks

Likelihood	Impact	Risk
Possible	Severe	**High**

Risk assessment

Active Directory Certificate Services (ADCS) misconfigurations can allow an attacker to gain additional access on the network. However, exploitation of this class of vulnerability is dependent on the attacker having already compromised a user account within the domain.

If an attacker gains access to a domain user account, (e.g. through phishing or other means) an attacker could obtain Domain Admin which is the highest level of privilege available to a domain user. This could permit any number of attacks being launched leading to significant operational disruption, and legal, financial and reputational damages.

Description

Active Directory Certificate Services (ADCS) is used inside AD environments to facilitate the Public Key Infrastructure (PKI) for certificate generation and signing. Vulnerabilities exist with ADCS that could allow attackers to elevate their privileges. These vulnerabilities are dubbed **ESC1** through **ESC8** and the ones affecting Client are as follows.

Certificate templates that allow low-privilege user accounts to modify them are vulnerable to **ESC4**. Attackers can abuse this by forcing vulnerabilities into the certificate template that would then allow for privilege escalation via user impersonation. If dangerous access controls, such as “Full Control” or “Write”, are granted to low privileged users over a certificate template A common attack path is to change the configuration of a vulnerable template to request a certificate of a Domain Administrator.

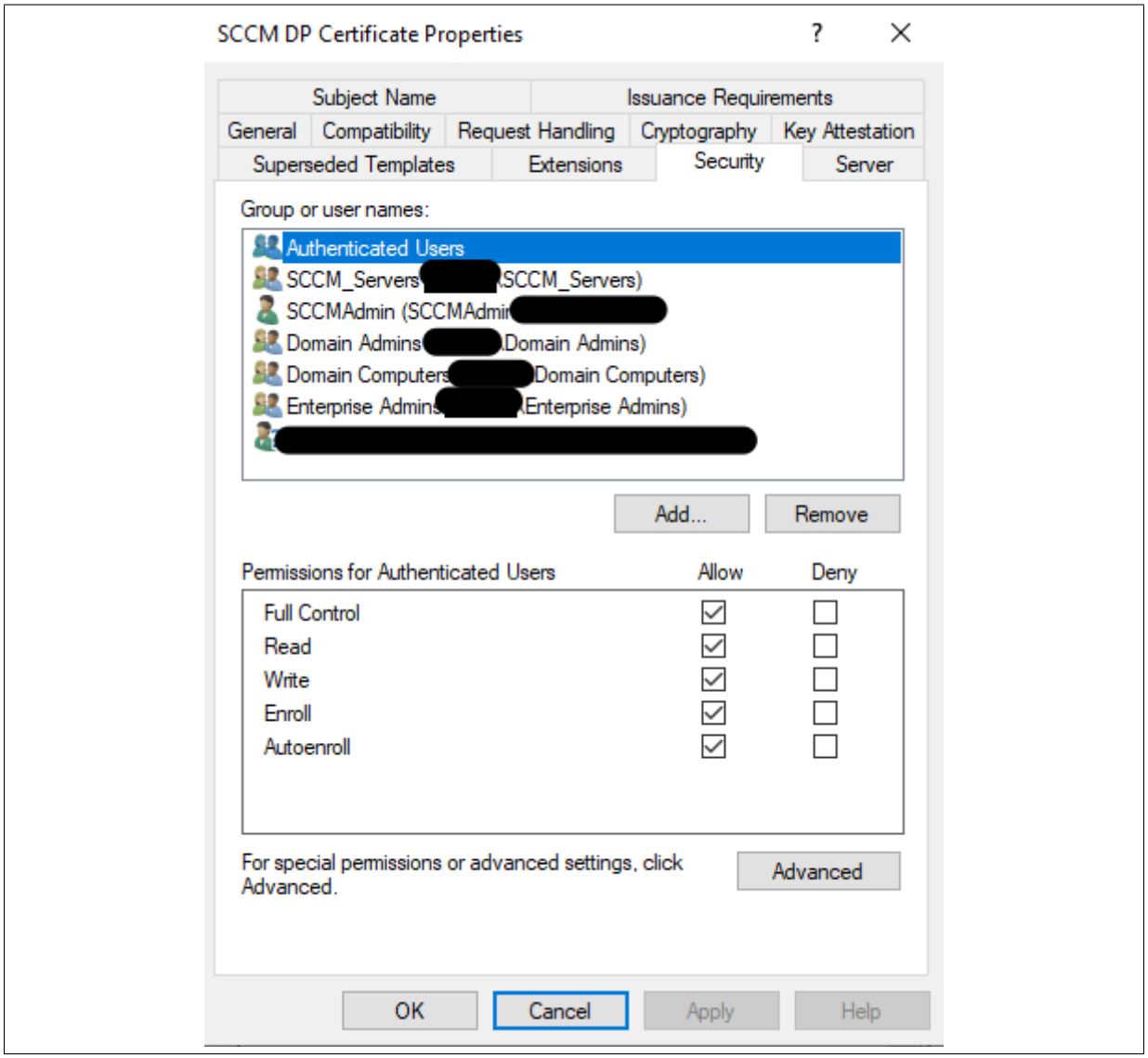


Figure 15: ESC4 Vulnerable template due to insecure ACEs for the Authenticated Users group

The following templates are vulnerable to ESC4:

- SCCMDPCertificate
- SCCMIISCertificate
- SCCMClientCertificate
- SCCMIISCertificate

ESC8 involves chaining **Coerced authentication** (refer to **Vulnerability 10: Coerced authentication (authenticated)**) and **NTLM Relay** (refer to **Vulnerability 12: NTLM relay**) to impersonate a Domain Controller machine account. This machine account NTLM challenge is relayed to the HTTP endpoint (http://CA/certsrv/certfnsh.asp) which is used to sign certificates. A certificate is then generated and then signed by the Certitficate Authority (CA) that can then be used to authenticate as the DC machine account. The certificate is provided as authentication to the DC and the account's privileges are used to retrieve the NTLM hashes of any account, including Domain

Admins, via **DCSync**.

The following ADCS servers were exploited:

- CA01.client.net.au
- CA02.client.net.au

Note: Volkis saw that the Certificate Authority "AUCA01.client.net.au" was configured to be vulnerable to **ESC8**. However, it looks like the web enrolment was not configured as all requests return a "403 - Forbidden: Access Denied" application response.

Recommendations

Disable certificate templates if there are no business requirements for them.

Audit all the certificate templates for insecure ACEs ("Full Control" or "Write") for low-privileged user groups such as "Authenticated Users" or "Domain Computers".

Disable NTLM on all ADCS servers in the domain via the **Restrict NTLM: Incoming NTLM traffic** group policy:

```
Computer Configuration > Windows Settings > Security Settings > Local Policies
    > Security Options > Network security: Restrict NTLM: Incoming NTLM traffic
    > Deny all accounts
```

Vulnerability 5: DHCPv6 poisoning

Likelihood	Impact	Risk
Likely	Severe	**High**

Risk assessment

Publicly available tools exist to assist attacker in exploiting this vulnerability. If successful, it would be possible for attackers on the internal network to perform Man-in-the-Middle (MitM) attacks to capture or manipulate data in transit.

Successful exploitation would result in data compromise, such as credentials and sensitive documents, and potentially injecting data into the connection that allows for administrator actions.

Account passwords hashes obtained via DHCPv6 poisoning can cracked offline using a GPU and can result in the compromise of the network due to vulnerability chaining.

Description

Hosts in the internal network are given IPv6 addresses using DHCPv6. There is a vulnerability in this protocol that allows attacks to control the DNS server used by client machines. By listening for broadcast IPv6 solicit packets, an attacker can reply to these requests with a DHCPv6 lease, providing the DNS server to use. By setting the DNS server to use as the attacker's machine, the attacker can control the flow of traffic through their own machine, gaining a MitM position.

Future incoming connections can be captured or relayed to other hosts. For example, the consultant used this attack to solicit incoming SMB requests which were then relayed to other machines on the network, allowing the consultant to query for domain usernames.

If an administrator account is tricked into connecting to the attacker's machine and relayed, the attacker would gain the same level of access as the relayed account.

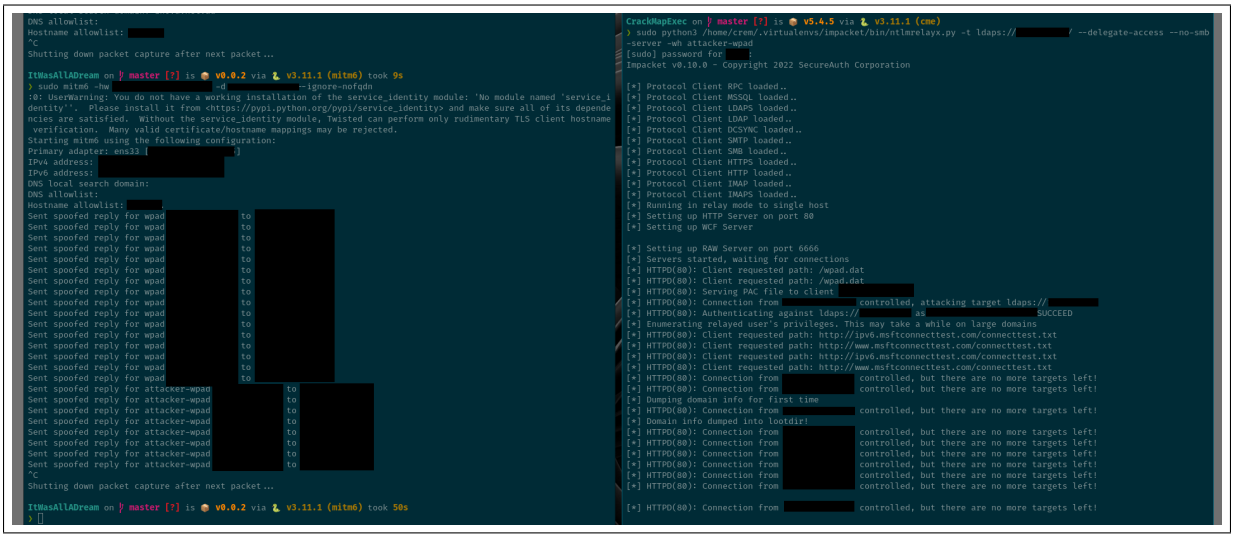


Figure 16: Poisoning IPv6 DNS resolvers

Recommendations

Disable IPv6 if it is not being used.

Otherwise, consider implementing one of the following protections:

1. **DHCPv6 Guard** - Available on Cisco devices, this inspects DHCPv6 traffic to only allow only authorised DHCPv6 packets through the switch.
2. Use a Layer 2 firewall to whitelist DHCP traffic from your known DHCP servers.

As an additional layer of protection, do not use high privilege accounts for day-to-day use.

Vulnerability 6: Kerberoasting

Likelihood	Impact	Risk
Possible	Severe	**High**

Risk assessment

The tools to retrieve the hash are publicly available. The attacker does, however, require a low privilege account to perform this attack. The likelihood is also impacted by how strong the password is. If an account is successfully cracked, the attacker would have the same privileges as that account. Service accounts usually have significant privileges to sensitive data and the impact of compromise could be severe.

The consultant was able to crack 8 of the 13 account hashes taken in the given engagement timeframe. One of the cracked accounts, "SVC_SERVICE" is a Domain Admin. This could permit any number of attacks being launched leading to significant operational disruption, and legal, financial and reputational damages.

Description

Accounts with Service Principal Names (SPNs) are vulnerable to **Kerberoast** attacks allowing attackers with a low privilege account to retrieve the service account's password hash. Since this hash uses a weak algorithm, RC4, it can then be cracked offline. The following accounts have SPNs:

- ADMINISTRATOR (Disabled) **(Domain Admin)**
- USER.ADM (Disabled)
- ABC_SRVACT
- DEF_SRVACT (Disabled)
- CLIENT.ADFS (Disabled)
- CLIENT.DBA (Disabled)
- CLIENT.SRV
- CLIENT.SHAREPOINT
- CLIENT_SQLADMIN
- SQLSVC (Disabled)
- SVCSCCMSQL
- SVC_SERVICE **(Domain Admin)**
- SVC_SHAREPOINT

Usually service account permissions are restricted to a single service. However, if an attacker can successfully crack the hash, they can use the access as a way to elevate privileges.

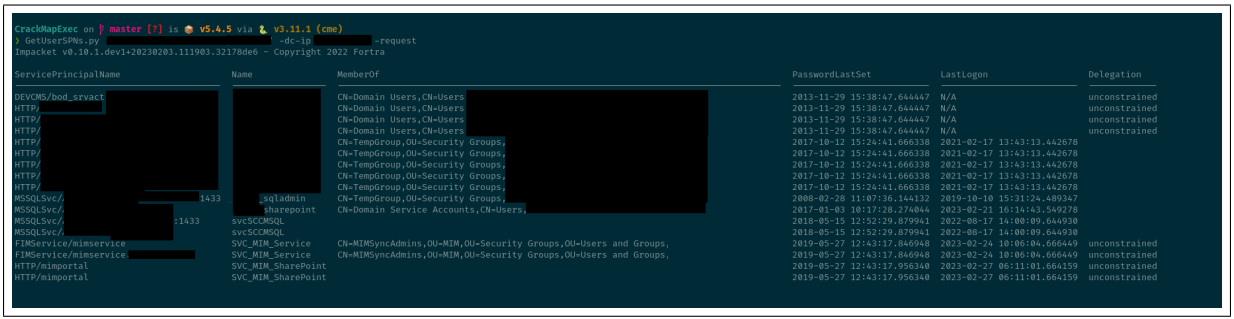


Figure 17: Kerberoasting

Note: 6 of the Kerberoastable accounts were disabled. If there is no business requirements for accounts, they should be deleted from Active Directory.

Recommendations

Service accounts should have a strong password and only support strong encryption methods. This can be set through the following GPO object:

(***Warning:*** *In rare cases, the following settings have been known to cause Domain trust errors. It is highly recommended to test on a subset of OUs first.)*

```
1  Computer Configuration > Windows Settings > Security Settings > Local Policies
       > Security Options > Network security: Configure encryption types allowed
       for Kerberos
```

Check the fields **AES128_HMAC_SHA1**, **AES256_HMAC_SHA1** and **Future encryption types**. Ensure the others remain unchecked.

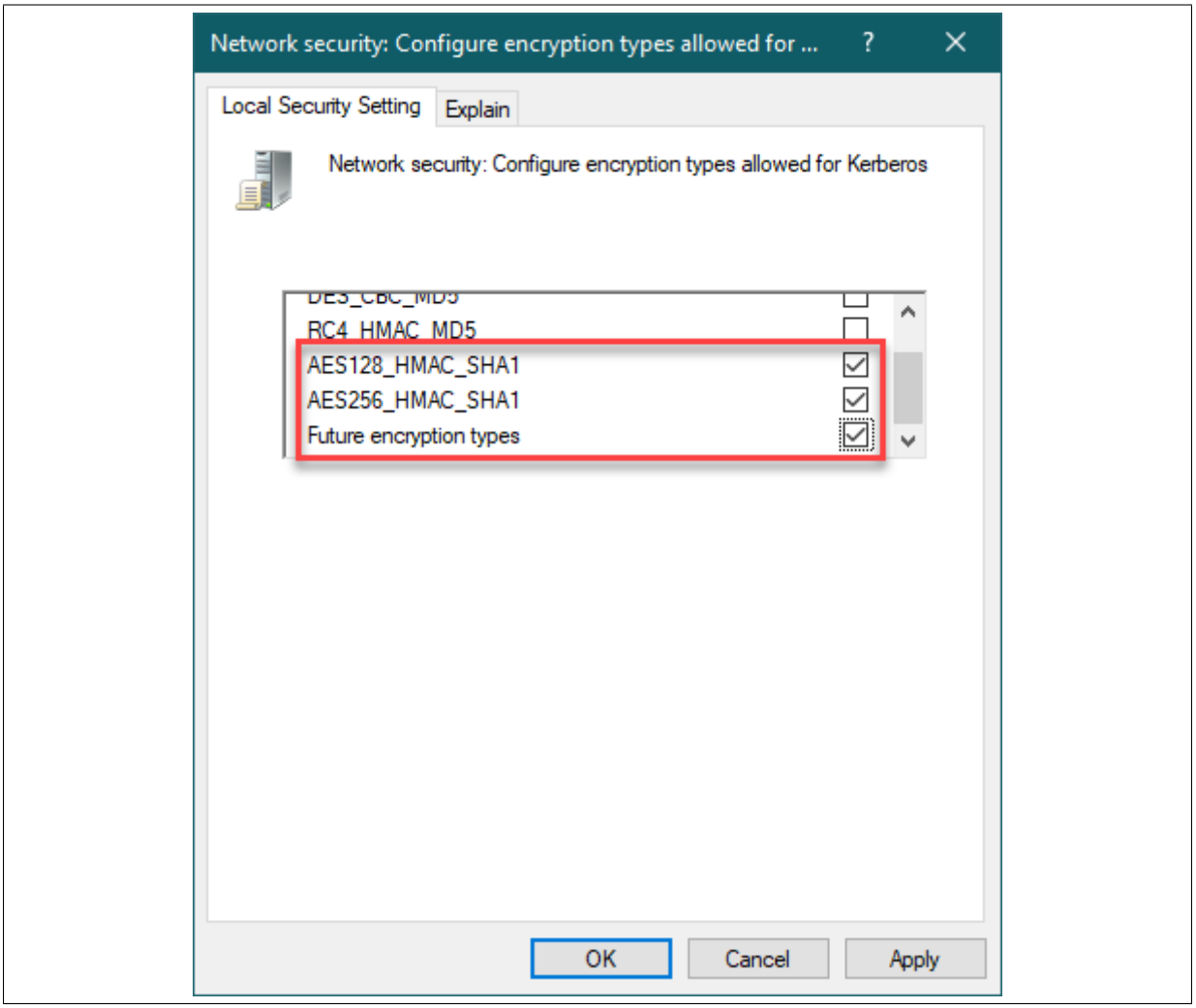


Figure 18: Secure Kerberos setting

Finally, remove all SPNs from **Domain Admin** accounts.

Vulnerability 7: Name resolution poisoning

Likelihood	Impact	Risk
Likely	Severe	**High**

Risk assessment

Tools to exploit this vulnerability are publicly known and commonly employed when attacking internal networks making the attack likely to be performed if an attacker reaches the internal network. The impact to the business is severe as it could allow attackers to gain administrator access to potentially multiple systems if the right system is poisoned. Even if low privileged access is gained, it allows the attacker to perform further enumeration on the network and perform attacks that require credentials such as **ADCS attacks** (refer to **Vulnerability 4: ADCS attacks**), **Kerberoasting** (refer to **Vulnerability 4: ADCS attacks**) and **Coerced authentication** (refer to **Vulnerability 10: Coerced authentication (authenticated)**).

The result could in obtain Domain Admin access and lead to significant operational disruption, and legal, financial and reputational damages.

Description

Computers on the **client.net.au** domain use vulnerable name resolution protocols Link-Local Multicast Name Resolution (LLMNR) and NetBIOS Name Service (NBT-NS).

These protocols are enabled by default and are used as a fallback mechanism for resolving hostnames when DNS fails. However, unlike DNS, both protocols use a broadcast message that is sent to all other machines in the subnet. In a normal use case, a machine will reply back if it has the requested name. Attackers can abuse this by listening for incoming requests and replying back to any requested name, giving the attacker's IP address.

The victim machine will now make further requests to the attacker's machine rather than the real one. This attack can be used to solicit SMB connections to gather the NetNTLM hash from the victim machine or to relay incoming connection to another host as part of an NTLM relay attack.

Whether the password is cracked, or the connection is relayed, the attacker can gain the privileges on the victim user and perform actions on their behalf.

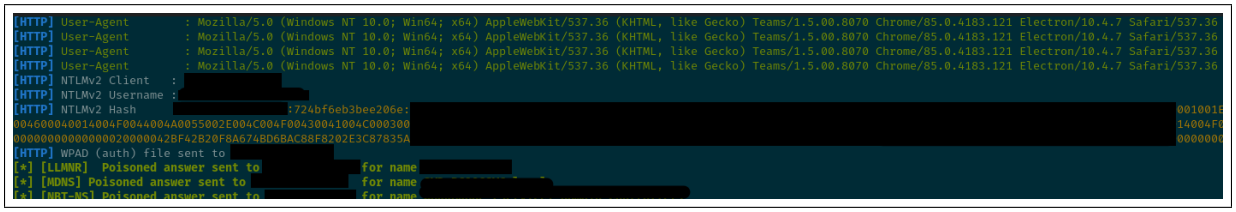


Figure 19: Capturing NTLMv2 challenge/response

Recommendations

Disable the use of these protocols. For LLMNR, change the following Group Policy Object to **Enabled**:

```
Computer Configuration > Administrative Templates > Network > DNS Client > Turn Off Multicast Name Resolution
```

As there is no GPO for disabling NBT-NS, the use of a logon script is recommended.

1. Create a PowerShell file (*.ps1) and add the following contents:

```
$regkey = "HKLM:SYSTEM\CurrentControlSet\services\NetBT\Parameters\Interfaces"
Get-ChildItem $regkey |foreach { Set-ItemProperty -Path "$regkey\$($_.pschildname)" -Name NetbiosOptions -Value 2 -Verbose}
```

2. Put the file in the in the following GPO location:

```
Computer Configuration > Policies > Windows Settings > Scripts > Startup > PowerShell Scripts
```

3. You may confirm that the script is working by running the following PowerShell command on each host:

```
Get-ChildItem "HKLM:SYSTEM\CurrentControlSet\services\NetBT\Parameters\Interfaces"
```

4. Ensure that each interface has the setting **NetbiosOptions** set to **2**.

Vulnerability 8: Unpatched and unsupported systems

Likelihood	Impact	Risk
Possible	Severe	**High**

Risk assessment

The risk varies depending on the vulnerability. An individual rating is given to each unpatched software application and the highest is taken as the overall criticality.

The criticality rating considers the ease of exploitation, if there are existing exploits available and the impact of successful exploitation.

The vulnerable software/operating system were identified using a vulnerability scanner and should be manually verified to confirm that it is not a false positive.

Description

Systems are missing patches that expose them to publicly known vulnerabilities.

The following systems are affected:

Host	System	Current version/Missing patch	Attack type	Risk
SERVER1	Windows Server	2008 R2 Standard Service Pack 1	RCE	High
SERVER2	Windows Server	2008 R2 Standard Service Pack 1	RCE	High
SERVER3	Windows Server	2008 R2 Standard Service Pack 1	RCE	High
SERVER4	Windows Server	2008 R2 Standard Service Pack 1	RCE	High
x.x.x.5	OpenSSL	0.9.8j	Buffer Overflow	High
x.x.x.5	PHP	5.6.34	RCE	High
x.x.x.6	Oracle Database	12.1.0.1.0	Path Traversal	High
x.x.x.8	Microsoft SQL Server	12.0.2269.0	RCE	High
x.x.x.125	Microsoft IIS Server	7.5	RCE	High
x.x.x.5	Apache httpd	2.4.25	DoS	Low

Continued on next page

Host	System	Current version/Missing patch	Attack type	Risk
x.x.x.74	Apache httpd	2.4.51	DoS	Low
x.x.x.70	Dell EMC iDRAC9	5.00.10.00.22	DoS	Low
x.x.x.71	Dell EMC iDRAC9	5.00.10.10.01	DoS	Low
x.x.x.72	Dell EMC iDRAC9	5.00.10.00.22	DoS	Low
x.x.x.127	IBM DB2	10.5.300.125	PrivEsc	Low

The table above outlines what vulnerabilities are present for each piece of software, such as:

- Remote Code Execution (RCE).
- Denial of Service (DoS).
- Cross-site Scripting (XXS).
- Information disclosure (Info).
- Access bypass (Bypass).
- Privilege escalation (PrivEsc)
- Buffer Overflow

The vulnerabilities exposed may allow an attacker to execute arbitrary code, perform a denial of service attack or compromise sensitive information. Attackers could leverage this access to perform further attacks against the network.

Recommendations

Ensure that systems are running their latest versions by applying the patch using your regular patching process.

Additional application information can be found at:

Application	Reference
Apache httpd	https://httpd.apache.org/download.cgi
OpenSSL	https://www.openssl.org/source/
iDRAC	https://www.dell.com/support/article/en-au/sln308699/idrac9-versions-and-release-notes?lang=en
Windows Server 2008	https://learn.microsoft.com/en-us/troubleshoot/windows-server/windows-server-eos-faq/end-of-support-windows-server-2008-2008r2

Continued on next page

Application	Reference
PHP	https://www.php.net/downloads.php
Oracle Database	https://www.oracle.com/au/database/technologies/oracle-database-software-downloads.html
Dell iDRAC	https://www.dell.com/support/kbdoc/en-au/000130533/dell-poweredge-how-to-update-the-firmware-via-https-connection-to-idrac
Microsoft SQL Server	https://www.microsoft.com/en-au/sql-server/sql-server-downloads
IBM DB2	https://www.ibm.com/products/db2/database?utm_content=SRCWW&p1=Search&p4=43700075363270788&p5=e&gclsrc=ds

Vulnerability 9: Weak password policy

Likelihood	Impact	Risk
Likely	Severe	**High**

Risk assessment

An organisation's password policy includes much more than just the Domain policy settings. It encompasses everything to do with passwords including how they are created, stored and audited.

A weak password policy encourages weak passwords that could be vulnerable to brute force and password guessing attacks. Compromises of these passwords could result in the compromise of sensitive data and business critical systems. The weak policy also encourages a lax security culture in the organisation.

Description

The password policy used at Client does not prevent users from choosing and handling passwords insecurely. User accounts had weak passwords that are vulnerable to brute force and password spray attacks yet give access to sensitive information and administrator privileges.

After gaining Domain Admin rights, the password hashes for all accounts in the client.net.au domain were taken from the NTDS file and were cracked offline using a GPU. The results are shown below:

	Passwords	Cracked	Percentage
Total	2636	2256	85.6%
Unique	1407	1035	73.6%

These results show that users are choosing insecure passwords for their accounts and are opting to select the minimum number of characters required by the domain password policy setting. The reasons behind the successful password cracking are likely to be:

1. A weak domain password policy;
2. A culture of using 1 dictionary word in passwords;
3. Multiple accounts using the same password;
4. Frequently expiring passwords.

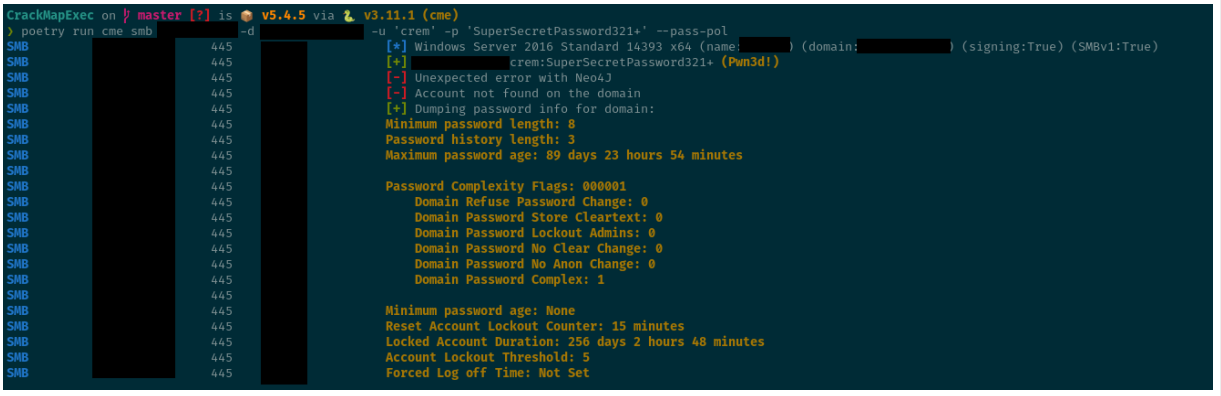


Figure 20: Password Policy

Requiring that passwords expire within a short timeframe (in this case, 90 days) overwhelmingly results in users reusing the same password with a simple change, such as incrementing a number on the end of the password. Multiple examples were found by examining the password history of users. A sample are included below:

```
ef3b5c61ded51bb2a47f0032af68d55c:Pa$$7466w0rd
f26d864ffd47c6db40ccde44ea9621dd:Pa$$8383w0rd
f4c9ca039de48959a2c2f7eff1370e50:Pa$$4946w0rd
5c186a0212ace082a125e3b0b8d16515:Pa$$7275w0rd
f781c29efc6e1380081e93f9d62b8a03:Pa$$5244w0rd
f63c0c9a9d2de2f5349c91b1b3648814:Pa$$4583w0rd
4cbf6a41744e4e2ed70d39a0b99f3bfc:Pa$$7075w0rd
3d4c2d5d05f76b11ab663c9620eedd2b:Pa$$535w0rd
bf374f07390bd93a131c7945a28bfb7e:Pa$$5514w0rd
4a105ad692cbe06e9cfa24cfd8117d85:Pa$$5073w0rd
df0253313d01148871aaa6b1b6c6bc56:Pa$$4495w0rd
ad682e0bf131e17c1a6b7a1cee10436f:Pa$$4633w0rd
cb35ecffc9c97cd20713aafe2ccf0b5c:Pa$$9351w0rd
d3d2703754327b5e90662cfb1b09c633:Pa$$7046w0rd
96faef8d785dac4299b405ba3c0efe84:Pa$$5365w0rd
854cedc43a012191c34e3a26d46501db:Pa$$7709w0rd
f18b14ba036304aabe0ae7cd7c5bace8:Pa$$9024w0rd
3db8bebffa31aa41e688fe80d259b715:Pa$$5795w0rd
c5d4bfe5ca716aae3fa9731e89459248:Pa$$6095w0rd
9db57271bdc5f67e6633f63b92113c3f:Pa$$7753w0rd
0d0e3fa9b1ff132ffd2c0079971f50c0:Pa$$4823w0rd
6d6a7dcf96fb56b2124ce5e4945b4915:Pa$$5843w0rd
e5b4c9b7b582f16d467f603f5bb99ca6:Pa$$8571w0rd
27f73cb88844901b3f04c13132b448ad:Pa$$5636w0rd
69731321fba4fcdd796e1cbac13bf1d7:Pa$$7515w0rd
0a2ca19c52463c60759f829acf354f49:Pa$$7535w0rd
9e03831b5ebe7066a83d8546fad5bc54:Pa$$4765w0rd
2dd82a5b79b6a297a517936cd0db217a:Pa$$7450w0rd
75c6d4d6ed8f3d9eb82e9d7eb2a92bc4:Pa$$8536w0rd
7b89a6d4fe22109905e2dcef9bd70ca6:Pa$$9721w0rd
35bac985a382480822c828c0172fc660:Pa$$7923w0rd
9f19d92f485a0c98181d15d3f8f6f101:Pa$$7591w0rd
```

Figure 21: Incrementing number on end of password due to password expiry

The following are the most used passwords:

Password	Count
pa$$w0rd	498
Disabl3d!	174
P@55w0rd	153
Welcome1	79

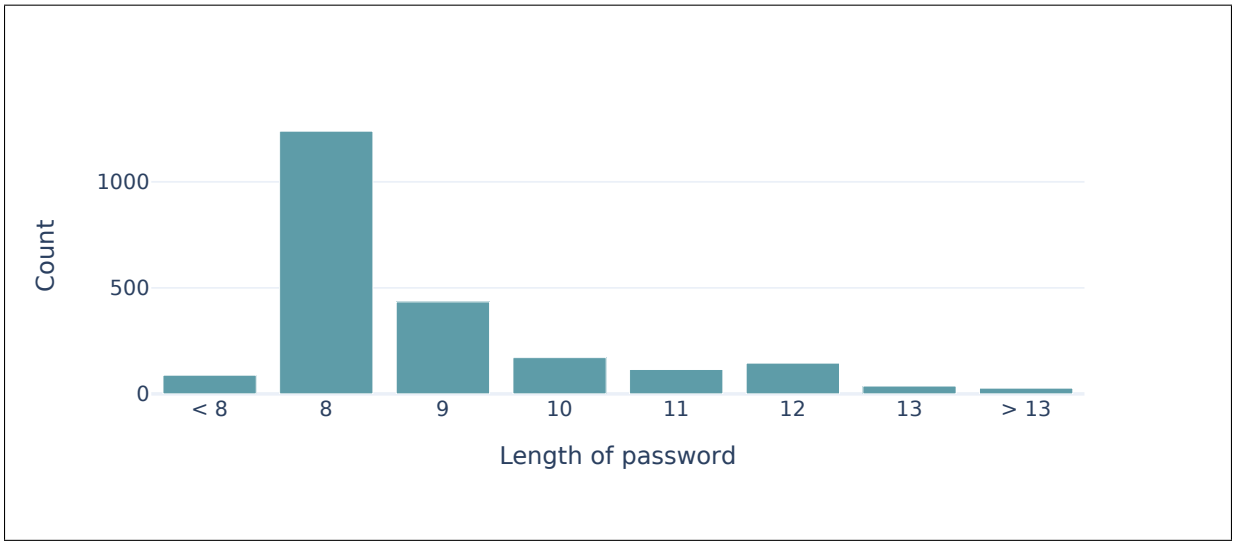


Figure 22: Number of passwords by character count

Multiple passwords were also found to be stored in cleartext in private files such as Word, Excel and text documents. A large amount of Client employees had a “Chrome Passwords.xlsx” file in their personal OneDrive which was an export of all credentials that was saved to the employees Google Chrome web browser. This includes various credentials for personal and business use. Their existence shows that there is either no password policy to prevent this, or it is not enforced. Storing password in cleartext makes it easier for attackers to gain access to sensitive information and critical systems.

“Chrome Passwords” Excel spreadsheet displaying cleartext credentials - Screenshot redacted

Recommendations

Create or improve your password policy. The following topics should be included as a minimum and tailored towards your company:

1. **Choosing passwords for accounts:** When educating people on password choice, length is more secure than complexity. A password with 16 lowercase characters is more secure than an 8-character password with letter, numbers and special characters. Users should be encouraged to choose a passphrase (rather than a password) consisting of multiple words.

2. **Domain password policy settings:** To encourage choosing passwords like the one above, and for added security against brute force attacks, the following settings are recommended.

Policy settings	Recommended value
Minimum password length	14
Complexity requirement	No
Minimum password age	0 days
Maximum password age	0 days
Account Lockout Threshold	3 attempts
Account Lockout Duration	1 hour
Reset account lockout counter after	30 minutes

Note that the **Maximum password age** should be set to `0` so that users are not forced to regularly change their passwords. Recent studies have shown that forcing users to regularly change passwords encourages weaker password choice. However, if a password is thought to be breached, then a new password should still be set. (Reference: https://pages.nist.gov/800-63-3/sp800-63b.html#memsecretver)

3. **Use a password manager:** Random, 32-character passwords are stronger than 16-character passwords but are extremely hard to remember. Using a password manager such as LastPass or KeePass allows admins and users to store randomly generated passwords in the vault and retrieve them using one master password. It also discourages the storage of cleartext passwords on systems or in file shares.
4. **Rotate shared account passwords**: Shared accounts should not be used if it can be avoided. There is no audit trail and the passwords are more likely to be leaked. However, for accounts that must be shared, ensure that passwords to these accounts are only viewable to authorised staff and are rotated on a regular basis. Again, a password manager can aid with this.
5. **Do not reuse passwords:** A password should never be used for more than one account. Each account should have a unique password whether that account is a domain account, local account or otherwise. Generating a random password and storing it in a password manager is one way to do this.
6. **Password audits:** Perform regular password audits by attempting to crack user passwords. Users that choose crackable passwords should be retrained and asked to choose a new password. As an incentive, users who choose secure passwords can be given a reward by the business.
7. **Password filter:** Consider implementing a password filter that prevents users choosing insecure and passwords commonly found in wordlists. This can be done by creating a DLL that is loaded by the LSA service on domain controllers. (More information: https://docs.microsoft.com/en-au/windows/win32/secmgmt/installing-and-registering-a-password-filter-dll)

Staff should be encouraged to follow these policies for both their work and personal account to build strong password habits. They should also be frequently reminded of the policy during security awareness training.

Vulnerability 10: Coerced authentication (authenticated)

Likelihood	Impact	Risk
Unlikely	Moderate	**Medium**

Risk assessment

Publicly available tools and documentation exist that aid attackers in performing this attack. However, this vulnerability must be chained with another vulnerability such as **NTLM Relay** (refer to **Vulnerability 12: NTLM relay**) or **ADCS Attacks** (refer to **Vulnerability 4: ADCS attacks**) making the likelihood **unlikely**.

In this environment, low privileged credentials are required to perform this attack. If the attack is done successfully, it could result in the compromise of the vulnerable system.

Description

Coerced authentication is a class of vulnerabilities that target various Windows protocols through RPC, aiming to have a server initiate a connection to the attacker's SMB or HTTP server. Examples of known vulnerabilities (named **PetitPotam** and **Printer Bug**) have targeted the MS-RPRN, MS-EFSR, MS-FSRVP, and MS-DFSNM protocols.

Coerced authentication, when combined with NTLM relay attacks, can allow an unauthenticated attacker to capture and relay credentials of the vulnerable server's machine account (AD accounts ending with **$**). This, in turn, allows an attacker to edit the Role-Based Constrained Delegation (RBCD) permissions of the vulnerable server, which gives the attacker the rights to log in to the vulnerable server as any user, including a Domain Admin.

The following hosts were vulnerable to coerced authentication and required credentials:

Hostname	IP Address
DC01	x.x.x.x
BDC01	x.x.x.x
DC02	x.x.x.x
BDC02	x.x.x.x

Recommendations

Multiple patches have been released by Microsoft to address this vulnerability. Apply the Windows patches using your regular patching method. Note that some patches require the host to be restarted before they are applied.

The patches do not completely remediate the vulnerability in some scenarios. Therefore, we recommend also performing the following remediation actions:

*(Note that the below settings **may break functionality** for old systems, so ensure the change is tested first.)*

Disable NTLM Authentication: Set the following Group Policy Object setting to `Deny all`:

```
Computer Configuration > Windows Settings > Security Settings > Local Policies
    > Security Options > Network security: Restrict NTLM: NTLM authentication in
     this domain
```

If certain functionality breaks as a result of the above settings, exceptions can be made for specific servers by adding them to the following setting:

```
Computer Configuration > Windows Settings > Security Settings > Local Policies
    > Security Options > Network security: Restrict NTLM: Add server exceptions
    in this domain
```

Implement RPC Filters: RPC Filters act like a firewall for the RPC protocol and will block connections to the vulnerable protocols.

For each of the vulnerable protocols, download the appropriate **RPC filter** file and create the filer using `netsh` .

Protocol	Filter File Location
MS-RPRN	https://gitlab.com/volkis/client-scripts/-/raw/master/RPC%20Filters/ms-rprn_filter.txt
MS-EFSR	https://gitlab.com/volkis/client-scripts/-/raw/master/RPC%20Filters/ms-efsr_filter.txt
MS-FSRVP	https://gitlab.com/volkis/client-scripts/-/raw/master/RPC%20Filters/ms-fsrvp_filter.txt
MS-DFSNM	https://gitlab.com/volkis/client-scripts/-/raw/master/RPC%20Filters/ms-dfsnm_filter.txt
All above	https://gitlab.com/volkis/client-scripts/-/raw/master/RPC%20Filters/all_filter.txt

To add the filter, run the following command on each of the vulnerable machines:

```
> netsh -f ms-xxxx_filter.txt
```

Vulnerability 11: Machine account quota

Likelihood	Impact	Risk
Possible	Moderate	**Medium**

Risk assessment

Tools are publicly available to perform this attack through either **NTLM relay** (refer to **Vulnerability 12: NTLM relay**) or through previously compromised account credentials making the attack **possible**.

In most cases, the newly created machine account does not have any special privileges but can make further exploitation in the domain easier. However, in some cases, this attack can be combined with **Resource-Based Constrained Delegation** (RBCD) to gain administrator-level access to servers in the internal network.

The consultant connected their own Windows virtual machine to the domain without the protections such as anti-virus put in place. Administrative rights of a domain joined machine allow for easier exploitation such as being able to run malicious binaries and scripts to attack the Client environment.

Description

The client.net.au domain has the value of the `ms-DS-MachineAccountQuota` attribute set to the default of 10. This allows any user (including machine accounts) to create up to 10 machine accounts on the domain. An attacker requires low-privilege user permissions, by compromising credentials or through NTLM Relay attacks for example, to create a new machine account. This functionality is intended by Microsoft.

An attacker can take advantage of this to create a low-privilege machine account on the domain by coupling this attack with an **NTLM relay** attack. This occurs when a user is coerced into authenticating to the attacker's machine, allowing the attacker to impersonate the victim's privileges on the Domain Controller. Attackers who have gained access to an internal network often seek domain credentials to use. The privileges of the credentials do not matter at this point in the attack sequence.

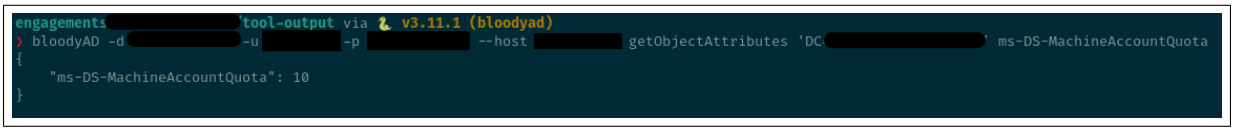


Figure 23: Adding a machine account

The machine account is just like a user account, for the attacker's purposes. It can be used to launch authenticated attacks against the domain including:

- List all user and groups in the domain
- List all group memberships
- List domain object permissions
- Access some file shares to hunt for sensitive information
- Coerce other machines to authenticate to the attacker's machine

The **Machine account quota** attack can also be coupled with RBCD to gain administrator access to another server. This attack takes advantage of a legitimate Kerberos feature whereby machine accounts can delegate access to other machine accounts. An attacker needs to be able to impersonate another server's machine account, through NTLM relaying for example, to perform this attack. However, if the attack succeeds, the attacker can authenticate to the victim server, pretending to be any user in the client.net.au domain.

Recommendations

Regular users should not have permissions to join computers to the domain. This permission can be revoked in 2 ways. Both should be implementing for coverage.

Set the ms-DS-MachineAccountQuota attribute to 0

This can be done as follows:

1. In the **Active Directory Services Interface Console (ADSI Edit)** select **Default naming context**.
2. Right-click on the domain OU and select **Properties**.
3. Find the **ms-DS-MachineAccountQuota** property and set it to **0**.

Remove the Authenticated Users principal

This can be done as follows:

1. Locate the Domain Controllers OU.
2. Add a new GPO with the following setting:

   Computer Configuration > **Policies** > **Windows Settings** > **Security Settings** > **Local Policies** > **User Rights Assignment** > **Add workstations to domain**

   Remove the **Authenticated Users** principal and ensure only high-privilege accounts are configured.

For more information please see:

- https://social.technet.microsoft.com/wiki/contents/articles/5446.active-directory-how-to-prevent-authenticated-users-from-joining-workstations-to-a-domain.aspx

Vulnerability 12: NTLM relay

Likelihood	Impact	Risk
Possible	Moderate	**Medium**

Risk assessment

Publicly available tools exist that aid attackers in performing this attack. The impact depends upon the privileges of the account being relayed and the network context. However, it is usually possible to gain command execution rights on an internal network.

NTLM Relay can also be combined with **Coerced Authentication** (refer to **Vulnerability 10: Coerced authentication (authenticated)**) and **ADCS attacks** (refer to **Vulnerability 4: ADCS attacks**) to achieve Domain Administrator on the network. However, it was not possible to achieve Domain Administrator like this.

Description

Computers in the **client.net.au** domain are vulnerable to NTLM relay attacks. In an NTLM relay attack, the attacker creates services that can use NTLM for authentication such as SMB, HTTP, MSSQL and LDAP. The attacker server listens for incoming connections on these protocols and requests that the client perform an NTLM authentication. This authentication process is then "relayed" or proxied to a third victim server.

Due to how the NTLM authentication handshake works, it is possible for attackers to do the relaying and create a valid session on the victim machine with the privileges of the connecting user. If that user was an administrator, it would mean that the attacker has gain admin rights over the victim server allowing them to execute commands. Low privilege credentials can also be relayed for information gathering purposes such as to get a list of domain users, groups, password policy and to access file shares.

Relay attack can also be performed against non-admin protocols such as to MSSQL to gain access to a database and to IMAP to gain access to a user's emails.

During the engagement, the consultant relayed a low privilege account to the Domain Controller and created a new low privilege computer account that could be used in further attacks.

Recommendations

Enable SMB Signing and LDAP Signing.

For SMB Signing, set for following two GPO objects to **Enabled**:

```
Computer Configuration > Policies > Windows Settings > Security Settings >
    Local Policies > Security Options > Microsoft network server: Digitally sign
     communications (always)
```

```
Computer Configuration > Policies > Windows Settings > Security Settings >
    Local Policies > Security Options > Microsoft network client: Digitally sign
     communications (always)
```

For LDAP Signing, set the following GPO object to **Require Signing**:

```
Computer Configuration > Windows Settings > Security Settings > Local Policies > Security Options > Domain controller: LDAP server signing requirements
```

Vulnerability 13: Password stored in user description

Likelihood	Impact	Risk
Likely	Low	**Medium**

Risk assessment

A low privilege user account is required to read the **Description** field that stores the password.

No special tools are required to retrieve this information; it can be done with a single PowerShell command.

It was possible to dump LDAP information by chaining DHCPv6 (Refer to **Vulnerability 5: DHCPv6 poisoning**) and NTLM Relay **Vulnerability 12: NTLM relay** without authentication.

Many of the passwords in description are from disabled accounts. These passwords can still give an indication of possible passwords to try with a password spray.

Description

The multiple user passwords has its password stored in plaintext in the domain object's **Description** field.

Username	Status
USER1	Enabled
USER2	Enabled
USER3	Disabled
USER4	Disabled
USER5	Disabled
USER6	Disabled
USER7	Disabled
USER8	Disabled
USER9	Disabled
USER10	Disabled

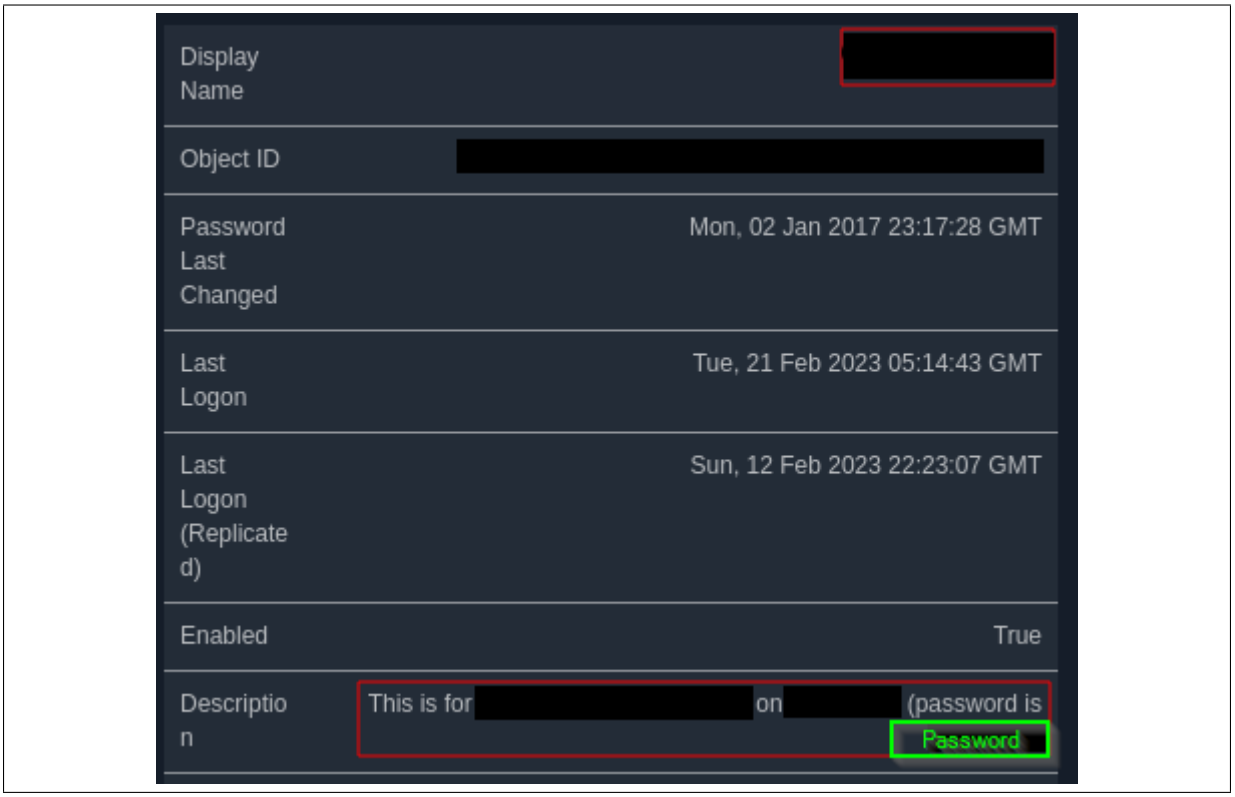


Figure 24: Password in description

Recommendations

Passwords should never be stored in domain object fields. Remove the password from this field and instead use a password manager to share passwords between IT team members.

Vulnerability 14: Unconstrained delegation configuration

Likelihood	Impact	Risk
Unlikely	Moderate	**Medium**

Risk assessment

Publicly available tools and documentation exist that aid attackers in performing this attack. However, this vulnerability must be chained with another vulnerability such as **NTLM Relay** (refer to **Vulnerability 12: NTLM relay**) or **Coerced Authentication** (refer to **Vulnerability 10: Coerced authentication (authenticated)**). Additionally, the affected host could not be compromised without a Domain Admin account and therefore making the likelihood **unlikely**.

If an attacker was able to perform **Coerced Authentication** and compromise the affected host, they would be able to gain Domain Admin privileges. This could permit any number of attacks being launched leading to significant operational disruption, and legal, financial and reputational damages.

Description

A computer object allows for delegation to any service to any resource on the domain as a user when the **Trust this computer for delegation to any service (Kerberos delegation only)** is enabled. This is commonly referred to as **Unconstrained Delegation**. This can be used to escalate privileges or lateral movement within the Active Directory domain.

The attack requires two preconditions to be successful:

1. Control of the host that has **Trust this computer for delegation to any service (Kerberos delegation only)** enabled.
2. The ability to coerce another object (typically a Domain Controller) in the Active Directory domain to authenticate to the unconstrained delegation host.

Coercing a Domain Controller to authenticate to an unconstrained delegation host will result in Domain Admin privileges in the Active Directory environment. Therefore, non-Domain Controller computer objects should not be configured for unconstrained delegation.

The following non-Domain Controller host was configured for unconstrained delegation:

- SERVER21

Recommendations

Disable unconstrained delegation if there is no business requirements for it.

Enabling the “This account is sensitive and cannot be delegate” for any high privilege and sensitive accounts.

Placing high privilege and sensitive accounts inside the Protect Users group.[6]

[6] https://learn.microsoft.com/en-us/windows-server/security/credentials-protection-and-management/protected-users-security-group

Vulnerability 15: RDP terminal level authentication

Likelihood	Impact	Risk
Rare	Low	**Low**

Risk assessment

Attackers that receive a terminal prior to authentication can use the on-screen information for malicious purposes. Data such as usernames and domain names can be gathered from login screens.

Exploitation of this vulnerability will not directly result in compromise. However, it can be used as part of a larger attack.

Description

Hosts on the internal network do not restrict connections to Network Level Authentication (NLA) in the RDP protocol. NLA will authenticate users prior to establishing the network connection, making it more difficult to exploit vulnerabilities in the RDP protocol.

It is also possible for attackers to gather information from the terminal login screen prior to authentication. Current and past login usernames may be disclosed to attackers and used in further exploitation.

Recommendations

NLA should be enabled for all systems that expose the RDP protocol. It can be enabled using the following Group Policy setting:

```
Computer Configuration > Policies > Administrative Templates > Windows
    Components > Remote Desktop Services > Remote Desktop Session Host >
    Security > Require user authentication for remote connections by using
    Network Level Authentication
```

Microsoft has published a document with further information at the following URL:

https://social.technet.microsoft.com/wiki/contents/articles/5490.configure-network-level-authentication-for-remote-desktop-services-connections.aspx

Detailed Vulnerabilities: Wi-Fi

Vulnerability 16: Evil twin attack

Likelihood	Impact	Risk
Rare	Moderate	**Low**

Risk assessment

Exploitation requires the attacker to be physically close to client devices and generate a stronger wireless signal than real access points. Given the increase risk of being caught during a physical attack, it is **rare** that Client will be targeted in this way.

If exploitation is successful, however, staff credentials would be compromised and depending on the access level of the account can be used to access sensitive information in emails or SharePoint, or authenticate to applications using Single Sign-On such as Payroll or Document Verification software.

Description

The following wireless networks use WPA2-PEAP for authentication and do not enforce client certificate based authentication:

- Client-Guest
- Client-Office

This allows an attacker to perform what is known as an **Evil Twin** attack whereby the attacker creates an access point (AP) with the same name as the affected one. If the signal strength of the rogue AP is stronger than the real AP, client devices will automatically connect to the rogue AP instead and authenticate to it. A challenge/response based authentication occurs and both parts are captured by the attacker for offline password cracking.

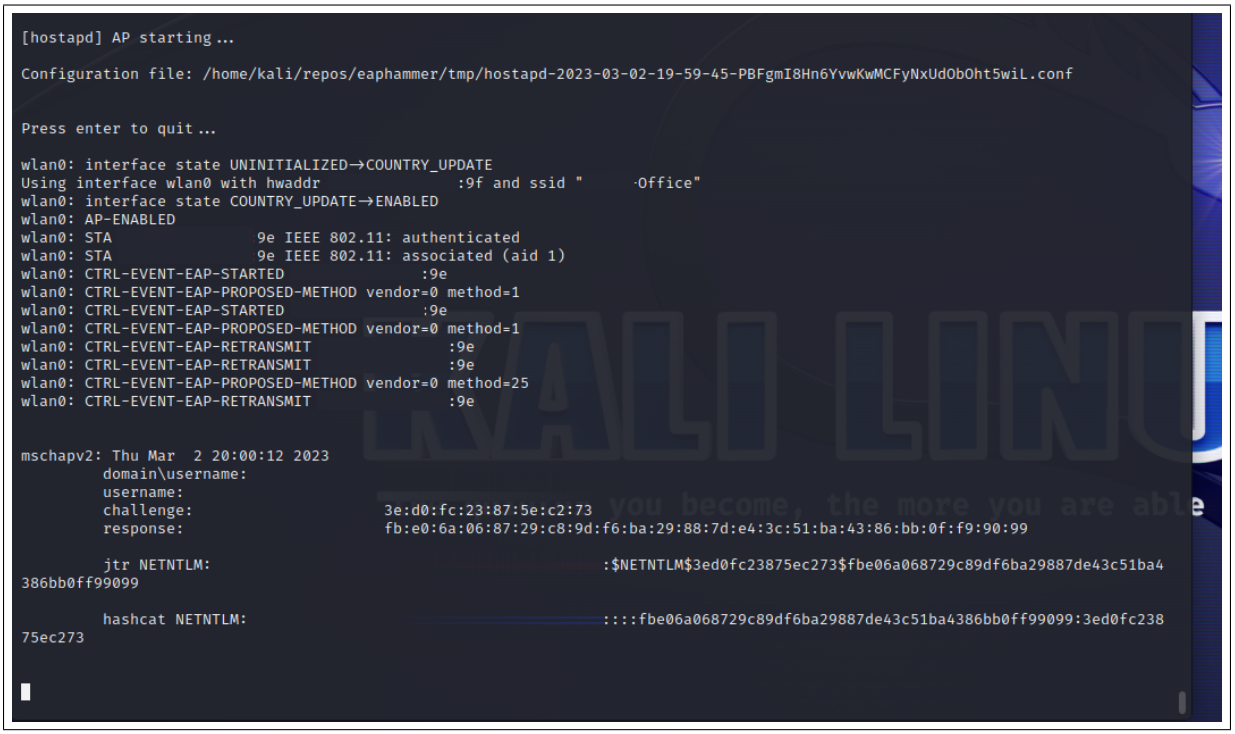


Figure 25: Client device authentication to evil twin

Active Directory (AD) credentials are used for authentication. If these credentials are compromised, they could be used with other services tied to AD such as Outlook, Sharepoint and VPNs.

Recommendations

Use certificate based authentication instead of utilising Active Directory credentials on the **Client Office** wireless network.

Consider making the **Client Guest** wireless network a WPA2 Personal network with a strong password.

Vulnerability 17: MFA Bypass through Guest wireless network

Likelihood	Impact	Risk
Rare	Severe	**Low**

Risk assessment

An attacker who has gained a valid set of credentials (through phishing or other means) could utilise Client's wireless network to circumvent Multi-Factor Authentication for user accounts.

Depending on the privilege level of the compromised user, this could provide the attacker with sensitive information such as confidential client information, personally identifiable information of clients or staff, intellectual property, etc.

An attacker with access to this information could cause financial and reputational damage to Client.

Description

Client has configured Microsoft 365 with conditional access to permit users to forgo Multi-Factor authentication while in trusted locations, such as inside the office. These "trusted locations" are identified by the outgoing IP address of the client. As the guest wireless network uses the same outgoing IP address as the corporate network, all Microsoft 365 login attempts to client.net accounts will automatically bypass the MFA check.

Wireless networks that use Active Directory credentials, but not certificates, for authentication can also be abused since attackers would have valid credentials through phishing or other means.

The following network can be used to bypass MFA:

- Client-Guest

An attacker with a valid set of user credentials could access Client's network and access the user's account information including emails, documents, OneDrive, and Teams directly through Microsoft's web portal.

Recommendations

Remove Conditional Access security configurations, forcing all users to use MFA at all times. This is the most secure and reliable way to prevent unauthorised access.

If Conditional Access is required in some cases (such as legacy applications) consider one of the following options:

1. Configure Condition Access to allow only **Trusted Devices** such as those bound to the client.net domain.
2. Route all non-corporate wireless network traffic through select outgoing IP addresses that have been specifically removed from the Conditional Access trusted IP pool.

More information on Conditional Access with locations can be found here:

- https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/location-condition#configure-mfa-trusted-ips

Appendices

Appendix A: SSH misconfiguration details

Password authentication enabled

SSH server's default configuration is to allow both password and public key logins. Password logins are susceptible to brute force attacks. If credentials are compromised, an attacker will have access to the system.

Remediation

Implement certificate authentication and then disable password authentication.

A guide on implement certificate authentication can be found at:

- https://www.ibm.com/docs/en/sia?topic=kbaula-enabling-rsa-key-based-authentication-unix-linux-operating-systems-3

To disable SSH password authentication:

1. Logon to the system.
2. Open the SSH configuration file, e.g. `sudo vi /etc/ssh/sshd_config`.
3. Update the PasswordAuthentication setting to `no`, e.g. `PasswordAuthentication no`.
4. Restart the SSH server, e.g. `sudo systemctl restart sshd`

SSH service supports weak cipher suites

When a client system creates a SSH connection with a server, multiple encryption algorithms are used at different stages of the SSH handshake process and during the transmission of the data. If the algorithms are using a small key or have known vulnerabilities, attackers are able to reverse engineer the keys and decrypt the captured data flowing between client and server.

During the SSH handshake, the client and the server will negotiate the strongest cipher suite that is supported by both parties. However, supporting weak cipher suites creates a risk if older clients that do not support newer, more secure ciphers connect to the server or if the attacker performs a downgrade attack forcing the server to use insecure encryption.

Remediation

Disable support for weak ciphers so that the server refuses any insecure connections.

To assist in identifying the weak ciphers the following command can be run, `sudo sshd -T | grep "\(ciphers\|macs\|kexalgorithms\)"`.

To disable SSH weak ciphers:

1. Logon to the system.
2. Open the SSH configuration file, e.g. `sudo vi /etc/ssh/sshd_config`.
3. Remove the weak ciphers from `Ciphers`.
4. Restart the SSH server, e.g. `sudo systemctl restart sshd`

Appendix B: TLS misconfiguration details

TLS service supports weak cipher suites

When a client system creates a TLS connection with a server, multiple encryption algorithms are used at different stages of the TLS handshake process and during the transmission of the data. If the algorithms are using a small key or have known vulnerabilities, attackers are able to reverse engineer the keys and decrypt the captured data flowing between client and server.

Any cipher that uses a key of less than 112 bits is considered weak and vulnerable. Further, specific algorithms with known attacks, such as 3DES, are also considered weak.

During the TLS handshake, the client and the server will negotiate the strongest cipher suite that is supported by both parties. However, supporting weak cipher suites creates a risk if older clients that do not support newer, more secure ciphers connect to the server or if the attacker performs a downgrade attack forcing the server to use insecure encryption.

Remediation Disable support for vulnerable ciphers so that the server refuses any insecure connections.

For **Microsoft IIS servers**, this can be done through Group Policy: 1. Navigate to **Computer Configuration** > **Administrative Templates** > **Network** > **SSL Configuration Settings** > **SSL Cipher Suite Order** 2. Change the value to the following (order is important):

```
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384,TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
    ,TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384,TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
    ,TLS_DHE_RSA_WITH_AES_256_GCM_SHA384,TLS_DHE_RSA_WITH_AES_128_GCM_SHA256,
    TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384,
    TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256,
    TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384,TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256,
    TLS_RSA_WITH_AES_256_GCM_SHA384,TLS_RSA_WITH_AES_128_GCM_SHA256,
    TLS_RSA_WITH_AES_256_CBC_SHA256,TLS_RSA_WITH_AES_128_CBC_SHA256
```

For **Apache HTTP servers**, add/edit the following line in the Apache configuration file:

```
SSLCipherSuite HIGH:!aNULL:!MD5
```

For **nginx**, add/edit the following line in the nginx configuration file:

```
ssl_ciphers EECDH+AESGCM:EDH+AESGCM:AES256+EECDH:AES256+EDH;
```

Vulnerable TLS version supported

SSL v2.0 and 3.0, and older TLS versions 1.0 and 1.1 have known vulnerabilities that could allow an attacker to perform brute-force attacks and obtain the encrypted data without knowing the key. This makes connections that use these versions susceptible to Man-in-the-Middle (MitM) attacks.

Multiple vulnerabilities are known to exist in deprecated transport layer encryption such as the Browser Exploit Against SSL/TLS (BEAST) attack. In this attack, Initialisation Vector (IV) can be guessed one byte at a time, significantly reducing the search space for a valid IV. Although practical exploitation of these vulnerabilities requires significant expertise and resources, they can still present a risk.

Modern browsers no longer support these protocols and multiple standards including NIST and PCI expressly forbid supporting them at all.

Remediation Disable support for any encryption protocol older than TLS 1.2 so that the server refuses any insecure connections.

For **Microsoft IIS servers**, this can be done by editing the registry. Copy the following lines into a new file with a `.reg` extension and run the file:

```
Windows Registry Editor Version 5.00

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL
    \Protocols\SSL 2.0\Client]
"DisabledByDefault"=dword:00000001
"Enabled"=dword:00000000

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL
    \Protocols\SSL 2.0\Server]
"DisabledByDefault"=dword:00000001
"Enabled"=dword:00000000

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL
    \Protocols\SSL 3.0\Client]
"DisabledByDefault"=dword:00000001
"Enabled"=dword:00000000

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL
    \Protocols\SSL 3.0\Server]
"DisabledByDefault"=dword:00000001
"Enabled"=dword:00000000

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL
    \Protocols\TLS 1.0\Client]
"DisabledByDefault"=dword:00000001
"Enabled"=dword:00000000

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL
    \Protocols\TLS 1.0\Server]
"DisabledByDefault"=dword:00000001
"Enabled"=dword:00000000

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL
    \Protocols\TLS 1.1\Client]
"DisabledByDefault"=dword:00000001
"Enabled"=dword:00000000

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL
    \Protocols\TLS 1.1\Server]
"DisabledByDefault"=dword:00000001
"Enabled"=dword:00000000
```

For **Apache HTTP servers**, add/edit the following line in the Apache configuration file:

```
SSLProtocol all -SSLv2 -SSLv3 -TLSv1 -TLSv1.1
```

For **nginx**, add/edit the following line in the nginx configuration file:

```
ssl_protocols TLSv1.2 TLSv1.3;
```

Self-signed certificates

A certificate, also known as a public key certificate, is an electronic document that is used to prove ownership of a public key. Certificate Authorities (CA) are responsible for signing certificates as a trusted third party. By checking a signed certificate a user's browser can confirm that the website they are visiting belongs to the certificate owner and is therefore the legitimate website.

A self-signed certificate is one that has not been signed by a Certificate Authority (CA). This means that a user browsing to the website cannot validate the owner of the website they are visiting.

Users trained to accept self-signed certificates risk exposing themselves and the business to possible compromise. An attacker could create their own self-signed certificate using the same Common Name of the target and present a malicious website as legitimate. A victim browsing the malicious website would have no indication of the website's illegitimacy causing risk to both the victim in the form of identity theft, and to the target business' reputation.

Remediation Obtain a valid certificate from a trusted Certificate Authority (CA).

For internal use, you can create your own CA and use Group Policy to push out the trusted CA Certificate to end points and other servers.

Refer to Microsoft's documentation for more details:

- https://docs.microsoft.com/en-us/windows-server/networking/core-network-guide/cncg/server-certs/install-the-certification-authority

Appendix C: External penetration testing methodology

Volkis will perform penetration testing on the internet-accessible systems and services within the target subnet. This will include the identification and enumeration of systems and services, identifying vulnerabilities within those systems and services, targeting weak authentication and account credentials, exploiting identified vulnerabilities, and then analysing and reporting on the results.

Identification and enumeration

Volkis will investigate the subnets in scope using scanning methods, active enumeration to identify what systems and services are accessible from the internet, and Open Source Intelligence (OSINT).

Volkis will scan the entirety of the in-scope subnet using a port scanner, scanning for common TCP and UDP open ports. Where possible and where systems can handle the traffic throughput, full TCP port scans will be launched against systems.

Accessible systems will be analysed to gather information about the system, including whether the system is running Microsoft Windows or Linux and the version including the operating system build or service pack information.

Open services and ports will be enumerated to identify what service is running and information about that service including the version, banner information, and any third-party plugins and modules that could be installed.

A search for hidden assets and endpoints will also be performed. This is to expand the attack surface and find things such as: - Non-linked admin/high value pages; - Websites behind a virtual hostname; - UAT pages/instances with live data.

The tester will investigate the organisation using common OSINT sources. This could include WHOIS information, social media sources and publicly available websites including the organisation's website. Other assets that may impact the security of the external network such as DNS, email, code repositories, third party hosting and Software as a Service providers will also be considered as part of the security posture.

Vulnerability identification

Each open system, service and asset will be investigated for potential vulnerabilities that could be used to compromise systems, gain access to information, make malicious changes to information or applications, or create impact on the availability of systems and information.

The vulnerability identification will begin with using automated vulnerability assessment tools on the environment. This will include running generalist network vulnerability assessment tools such as Tenable Nessus that will scan for potential misconfigurations, missing patches, out-of-date software, and other common vulnerabilities.

For specific services, more specialised vulnerability scanning and assessment tools will be used. These specific tools will give greater depth of vulnerability assessment than the general vulnerability assessment tools.

Following the vulnerability assessment, and with assistance of the results of the identification, enumeration, and vulnerability assessment results, the tester will then use manual techniques to uncover vulnerabilities that automated techniques will not see. This will include targeting custom developed services, leveraging the OSINT

information, investigating the feedback that the services provide when test cases are entered, and other manual techniques.

Vulnerabilities that are identified will not just be technical vulnerabilities, but could also include logic flaws, gaps in business process, or any other weakness of the application that could present risk to the organisation.

Exploitation

The tester will exploit identified vulnerabilities to better understand its impact and to eliminate the possibility of a false-positive.

The exploitation will occur alongside the vulnerability identification phase as vulnerabilities are identified. It will incorporate prioritisation, where vulnerabilities that tend to present higher risk to the organisation will be prioritised over low risk vulnerabilities. If there is a significant chance of service disruption, the tester will organise a window for exploitation, or not exploit it at all.

Exploitation will often involve the usage of publicly available tools, custom written tools, or specific actions taken by the tester.

Due to the nature of certain vulnerabilities, not every vulnerability can be exploited by the tester. This could be due to the level of network or system access required for exploitation, privilege requirements for exploitation, or specific conditions that need to be in place. These vulnerabilities will still be reported on even if exploitation was not achieved. The lack of exploitation will be a consideration when assessing the risk rating during the risk assessment.

Due to time limitations and prioritisation, not all vulnerabilities that are identified will be exploited during this phase. For example, the tester may choose not to exploit vulnerabilities that present a low risk to the organisation or that have a known impact.

Sensible precautions will be used during the exploitation phase to minimise the risks of availability issues. This could include performing exploitation out-of-hours or using a development or testing server. If the risks of exploitation are considered greater than the benefit of exploitation, and those risks cannot be mitigated or managed, the exploitation of the vulnerability will be skipped.

Exploitation of vulnerabilities that specifically create Denial of Service (DoS) condition will not be performed, nor will any sort of Distributed Denial of Service (DDoS).

Post-exploitation

Successful exploitation of vulnerabilities will provide the tester with additional access to information, functionality, and potential access to the internal environment. This additional access will be used by the tester to determine and prove the full scope of compromise, including the true business impact of the vulnerability.

The additional access will be fed back into the previous stages to determine if additional services can be enumerated and additional vulnerabilities can be found and exploited.

Appendix D: Internal penetration testing methodology

Volkis will perform penetration testing on the internal networks of the organisation. This will include the identification and enumeration of systems and services, passive and active reconnaissance, identifying vulnerabilities within systems and services, active interception and manipulation of traffic, targeting weak authentication and account credentials, exploiting identified vulnerabilities, and then analysing and reporting on the results.

Identification and enumeration

Volkis will investigate the subnets in scope using scanning methods, active enumeration to identify what systems and services are accessible, and Open Source Intelligence (OSINT).

Volkis will scan the entirety of the in-scope subnet using a port scanner, scanning for common TCP and UDP open ports. Where sensible and where systems can handle the traffic throughput, full TCP port scans may be launched against systems.

Accessible systems will be analysed to gather information about the system, including whether the system is running Microsoft Windows or Linux and the version including the operating system build or service pack information.

Open services and ports will be enumerated to identify what service is running and information about that service including the version, banner information, and any third party plugins and modules that could be installed. If there are open file shares, the tester may review them for sensitive information or account credentials.

A search for hidden assets and endpoints will also be performed. This is to expand the attack surface and find things such as: - Non-linked admin/high value pages; - Websites behind a virtual hostname; - UAT pages/instances with live data.

The tester will use a network sniffer to capture traffic that is being broadcast on the network. This may include connection requests, domain requests, and other potentially useful information.

If the organisation is using Active Directory, the tester will attempt to retrieve information about the directory using null sessions or authentication credentials. This can provide information about the users, systems, and group policy of the organisation.

Responding to and relaying internal traffic

The tester will analyse the traffic that is being broadcast on the internal network for opportunities to respond or relay authenticated connections. Although many protocols may be vulnerable to relay attacks, common vulnerable protocols include SMB, LDAP and HTTP.

When a user attempts to connect to a server, the tester will respond to that connection as if it were the server. The tester will then pass any information sent through that connection to the server. From the users' perspective there will be no change as they will be seeing the information they are expecting, but the tester will be able to gain access as the user to the target server.

The tester will then attempt to use this access to run commands, create new account objects, retrieve password hashes, or view sensitive file shares.

Vulnerability identification

Each open system, service and asset will be investigated for potential vulnerabilities that could be used to compromise systems, gain access to information, make malicious changes to information or applications, or create impact on the availability of systems and information.

The vulnerability identification will begin with using automated vulnerability assessment tools on the environment. This will include running generalist network vulnerability assessment tools such as Tenable Nessus that will scan for potential misconfigurations, missing patches, out-of-date software, and other common vulnerabilities.

For specific services, more specialised vulnerability scanning, and assessment tools will be used. These specific tools will give greater depth of vulnerability assessment than the general vulnerability assessment tools.

Following the vulnerability assessment, and with assistance of the results of the identification, enumeration, and vulnerability assessment results, the tester will then use manual techniques to uncover vulnerabilities that automated techniques will not see. This will include targeting custom developed services, leveraging the OSINT information, investigating the feedback that the services provide when test cases are entered, and other manual techniques.

Vulnerabilities that are identified will not just be technical vulnerabilities, but could also include logic flaws, gaps in business process, or any other weakness of the application that could present risk to the organisation.

Exploitation

The tester will exploit identified vulnerabilities to better understand its impact and to eliminate the possibility of a false-positive.

The exploitation will occur alongside the vulnerability identification phase as vulnerabilities are identified. It will incorporate prioritisation, where vulnerabilities that tend to present higher risk to the organisation will be prioritised over low risk vulnerabilities. If there is a significant chance of service disruption, the tester will organise a window for exploitation, or not exploit it at all.

Exploitation will often involve the usage of publicly available tools, custom written tools, or specific actions taken by the tester.

Due to the nature of certain vulnerabilities, not every vulnerability can be exploited by the tester. This could be due to the level of network or system access required for exploitation, privilege requirements for exploitation, or specific conditions that need to be in place. These vulnerabilities will still be reported on even if exploitation was not achieved. The lack of exploitation will be a consideration when assessing the risk rating during the risk assessment.

Due to time limitations and prioritisation, not all vulnerabilities that are identified will be exploited during this phase. For example, the tester may choose not to exploit vulnerabilities that present a low risk to the organisation or that have a known impact.

Sensible precautions will be used during the exploitation phase to minimise the risks of availability issues. This could include performing exploitation out-of-hours or using a development or testing server. If the risks of exploitation are considered greater than the benefit of exploitation, and those risks cannot be mitigated or managed, the exploitation of the vulnerability will be skipped.

Exploitation of vulnerabilities that specifically create Denial of Service (DoS) condition will not be performed, nor will any sort of Distributed Denial of Service (DDoS).

Post-exploitation

Successful exploitation of vulnerabilities will provide the tester with additional access to information, functionality, and potentially full control over all systems in the environment. This additional access will be used by the tester to determine and prove the full scope of compromise, including the true business impact of the vulnerability.

The additional access will be fed back into the previous stages to determine if additional services can be enumerated and additional vulnerabilities can be found and exploited.

As part of post-exploitation, the tester will seek out business-relevant information and functionality such as business critical applications, ERP systems, payroll, credit card information and customer databases, and procurement systems. This will be used to establish the real-world impact to the organisation of the compromise.

Appendix E: Wireless penetration testing methodology

Volkis will perform wireless penetration testing on the wireless infrastructure of the organisation. This will involve identification and enumeration of the wireless networks, capturing the authentication handshakes of WEP and WPA-PSK networks, impersonating WPA-Enterprise networks and checking for network segmentation. The goal of the wireless penetration test is to gain access to the internal network through wireless infrastructure.

Identification and enumeration

The consultant will use wireless capture tools to analyse each SSID in scope. The networks will be identified and enumerated, capturing the type of authentication and encryption used for each network be it WEP, WPA-PSK, WPA2-PSK, WPA-Enterprise or 802.1x. Signal strength between the consultant's machine, the access points and other wireless clients is also considered to assist in further attacks.

Identification of potentially vulnerable protocols such as WPS is performed at this point and noted for further exploitation attempts.

Capturing handshakes

In the case of networks protected with WEP or WPA(2)-PSK, the consultant will capture the initial handshakes of users connecting to the network. This is done by sending deauthentication packets to the connected wireless client. Since devices will automatically reconnect, this is usually transparent to the user. If no wireless client can be found connected the access point the consultant will attempt the PMKID attack to gather data that can be used to crack the passphrase.

For WEP networks, the consultant will then crack the encryption key used in the handshake to gain access to the network. For WPA-PSK networks, the consultant will use brute forcing techniques against the handshake to attempt to crack the pre-shared key. If the key cannot be cracked within a reasonable amount of time, the consultant may ask for the passphrase so that further checks can be performed while on the wireless network.

Evil twin attack

WPA-Enterprise (aka. WPA-EAP) uses multiple phases of authentication depending on the configuration. Most commonly, PEAP is used with MSCHAPv2. The consultant will create a fake access point that impersonates the real one. It may be possible to trick client devices to connect to the fake access point instead of the real one to capture authentication handshakes for offline cracking. Since the incoming connections also require an identify, this could possibly be a method of enumerating domain users.

The consultant will if a downgrade attack is possible by attempting to negotiate to a less secure authentication scheme. If possible, the attack may be abused to increase the chances of gaining access to the network.

If user devices are successfully trick into connecting to the fake access point, the consultant may use this Man-in-the-Middle position to perform attacks, such as NTLM relay, to gain access.

Network pivoting

Once on the wireless network, the consultant will attempt to gain access to the internal network. If the internal network is segmented, layer 2 network attacks and other exploits will be used to try and gain additional access.

If successful and an internal penetration test is also performed during the engagement, the consultant will combine the exploit path for a full picture of potential attacks.

Client isolation

On wireless networks that are likely to host untrusted users, such as on guest networks, the consultant will check for access to other wireless client devices to ensure attackers cannot exploit the organisation's guests.

Appendix F: Risk assessment methodology

A qualitative risk assessment is performed on each vulnerability to determine the impact and likelihood of the vulnerability being exploited. An overall risk is calculated based on the table below:

Impact \ Likelihood	Rare	Unlikely	Possible	Likely
Critical	**Medium**	**High**	**Critical**	**Critical**
Severe	**Low**	**Medium**	**High**	**High**
Moderate	**Low**	**Medium**	**Medium**	**High**
Low	**Low**	**Low**	**Low**	**Medium**

The risk assessment methodology is derived from industry standards such as ISO 31000[7] and OWASP Risk Rating Methodology[8].

The impact rating is deduced from multiple factors that consider both technical impact and business impact:

- **Loss of confidentiality**: How much sensitive information could be accessed or leaked and how sensitive was it?
- **Loss of integrity**: How much data could be corrupted and what degree of corruption was possible? Was it possible to perform actions on behalf of others?
- **Loss of availability**: How much services could be disrupted, preventing users from performing their tasks? What was the degree of impairment?
- **Financial damage**: How much money could be lost as a result?
- **Reputational damage**: How badly would the company's reputation be damaged and how much trust could customers lose?
- **Non-compliance**: Would the business be in breach of certain compliance standards they are obliged to comply with? (E.g. Privacy Act)

The likelihood is deduced from considering who the adversary may be and factors around the vulnerability:

- **Skill of adversary**: How skilful is the attacker likely to be?
- **Motive**: What are the motivating factors that the adversary may have?
- **Resources**: How much time and economic resources does the adversary have?
- **Ease of discovery**: How likely is the adversary to discover the vulnerability?
- **Ease of exploitation**: How easy is the vulnerability to exploit and are there publicly available tools to aid in doing so?
- **Detection**: How likely is the attack to be discovered by the organisation?

An overall rating (from Low to Critical) is given to each vulnerability. The vulnerabilities are then sorted in order from importance and urgency to remediate.

[7] https://www.iso.org/iso-31000-risk-management.html
[8] https://www.owasp.org/index.php/OWASP_Risk_Rating_Methodology

Appendix G: Document control

Document information

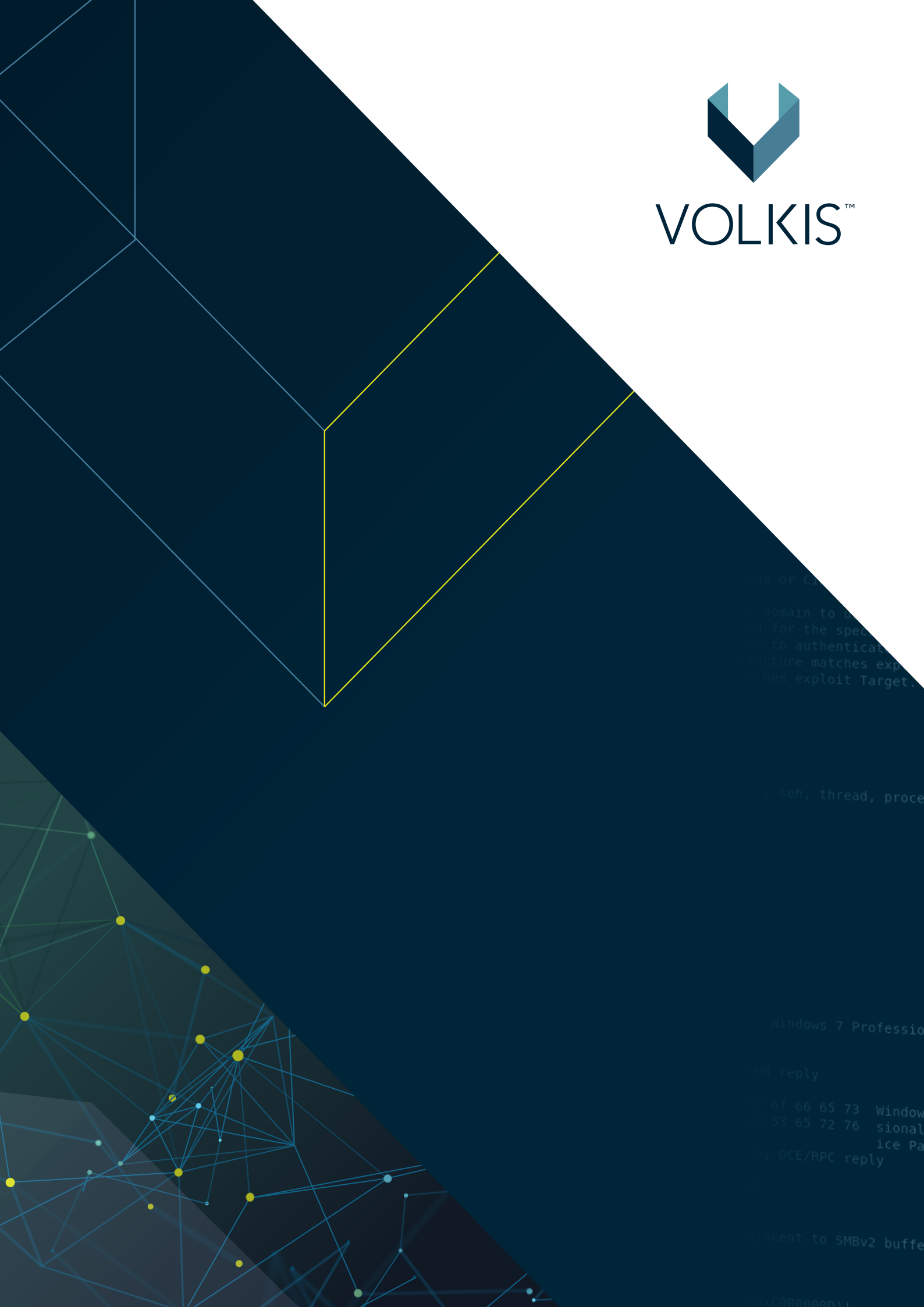
Client	Client
Document name	Penetration Test
Document version	1.0

Document changes

Version	Date	Name	Changes
0.1	2023-02-21	Volkis Consultant	Draft Report
0.2	2023-02-25	Volkis Senior Consultant	Added external penetration test results
1.0	2023-02-26	Volkis Consultant	Release Report

Document contributors

Name	Role	Phone number	Email address
Volkis Consultant	Security Consultant	0400 000 000	consultant1@volkis.com.au
Volkis Senior Consultant	Senior Security Consultant	0411 111 111	consultant2@volkis.com.au


VOLKIS™