Penetration Test Report
Presented to:

REDACTED

Date: [redacted], 2022
Version: 1.0

Table of Contents

Executive Summary

Aegis Security recently conducted an internal penetration test on **REDACTED** to assess their security posture. The test was performed by simulated attackers attempting to compromise **REDACTED** internal network, systems, and applications. This process allowed Aegis Security to identify vulnerabilities and assess the effectiveness of the **REDACTED** current security controls.

During the engagement, Aegis identified a significant issue with poor access control on file shares. This issue allowed the assessment team to access personally identifiable information (PII) and client information. This issue was caused by a lack of proper user access controls, which resulted in unauthorized individuals being able to access sensitive data. To address this issue, Aegis recommends that **REDACTED** implement stronger access controls on their file shares. This could include the use of access control lists, user permissions, and other measures to ensure that only authorized individuals have access to sensitive data.

It is important to note that the vulnerabilities identified during this engagement are not the only vulnerabilities that may exist in **REDACTED** systems. New vulnerabilities may emerge over time, and it is important for **REDACTED** to conduct regular security assessments to identify and address any potential vulnerabilities in their systems. This will help ensure the confidentiality, integrity, and availability of their data and systems.

Good Practices

Good Practice	Description
Strong Passwords	One of the good security controls implemented by **REDACTED** was the use of strong passwords for all users. Strong passwords are important because they are more difficult for attackers to guess or crack, making it harder for them to gain unauthorized access to the system. By requiring users to create and use strong passwords, **REDACTED** is helping to protect their systems and data from unauthorized access.
Limited Administrative Permissions	No users on the **REDACTED** network had excessive administrative permissions. Administrative permissions allow users to perform certain actions on the system, such as installing software or making changes to system settings. By limiting the number of users who have excessive administrative permissions, **REDACTED** is helping to prevent privilege escalation, which is the process of using legitimate access to gain unauthorized access to other resources. This is important because it helps to reduce the risk of a malicious actor using legitimate access to gain further access on the network.
Small Internal Footprint	**REDACTED** has a small internal footprint, which means they have a limited number of internal systems and networks. This is a good security control because it helps to reduce the attack surface, which is the total number of potential vulnerabilities that an attacker could exploit. A smaller attack surface means there are fewer potential vulnerabilities for an attacker to target, making it harder for them to gain unauthorized access to the system. By keeping their internal footprint small, **REDACTED** is helping to protect their systems and data from potential threats.

Scope and Methodology

The scope of the engagement included testing the security of **REDACTED** software and physical hardware. Specifically, Aegis Security conducted an internal penetration test on **REDACTED** systems and networks to identify vulnerabilities and assess the effectiveness of their current security controls.

Aegis was provided with one domain account for testing purposes, which allowed the assessment team to perform both authenticated and unauthenticated enumeration and exploitation on the network. This allowed them to test **REDACTED** defenses from multiple possible entry points.

Social engineering was not included in the scope of the engagement. This means Aegis Security did not attempt to manipulate or deceive individuals within the organization in order to gain access to their systems or data.

Overall, the scope of the engagement was focused on identifying vulnerabilities and testing the effectiveness of the **REDACTED** current security controls. By conducting this assessment, **REDACTED** can take steps to address any identified vulnerabilities and improve their overall security posture.

Risk Identification

Vulnerability severity ratings are used to identify the potential impact of a vulnerability on a system or network. These ratings help organizations prioritize their efforts to address vulnerabilities and protect their systems and data. There are typically four levels of severity:

Critical	A critical severity vulnerability is one that poses a significant and immediate risk to the system or network. This type of vulnerability is also very likely to occur and could allow an attacker to compromise sensitive data, disrupt operations, or gain unauthorized access to the system. It is important to address critical severity vulnerabilities as soon as possible to minimize the risk of a successful attack.
High	A high severity vulnerability is one that poses a significant risk to the system or network. While not as severe as a critical vulnerability, it is still important to address high severity vulnerabilities in a timely manner to minimize the risk of a successful attack.
Medium	A medium severity vulnerability is one that poses a moderate risk to the system or network. While not as severe as a critical or high severity vulnerability, it is still important to address medium severity vulnerabilities to minimize the risk of a successful attack.
Low	A low severity vulnerability is one that poses a minimal risk to the system or network. While it is important to address low severity vulnerabilities, they typically have a lower priority compared to vulnerabilities with higher severity ratings.

Risk	Impact			
Likelihood		Low	Medium	High
	Low	Low	Low	Medium
	Medium	Low	Medium	High
	High	Medium	High	Critical

Technical Findings

INT-01: LLMNR Spoofing

Risk: High	Impact: Medium	Likelihood: High

Observation

During the pentest, it was observed that the **REDACTED** network was vulnerable to spoofing of LLMNR (Link-Local Multicast Name Resolution) requests. This allowed for the capture of user NetNTLMv2 hashes, which are used to authenticate users on the network. Aegis Security was not able to crack any hashes to escalate privileges on the domain.

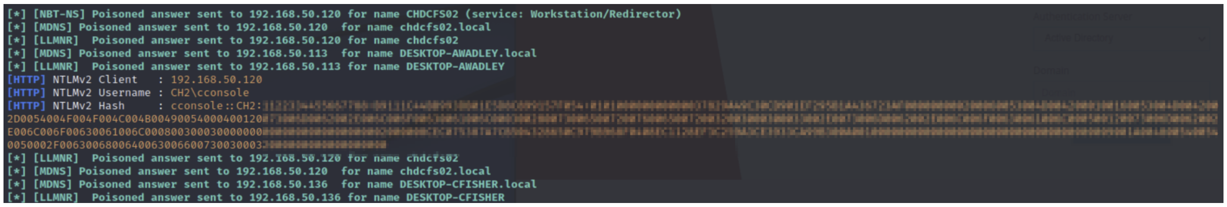
Impact

The ability to spoof LLMNR requests presents a risk because it allows for the potential capture of user hashes, which, if cracked, could be used to gain unauthorized access to the system or network. This is of particular concern because LLMNR is a protocol that is used to resolve hostnames to IP addresses on a local network, and it is enabled by default on many systems.

Remediation

To mitigate this risk, it is recommended to disable LLMNR on the network. If this is not possible, ensure that all user passwords are complex to prevent any chances of hashes being cracked.

Evidence



```
[*] [NBT-NS] Poisoned answer sent to 192.168.50.120 for name CHDCFS02 (service: Workstation/Redirector)
[*] [MDNS] Poisoned answer sent to 192.168.50.120  for name chdcfs02.local
[*] [LLMNR]  Poisoned answer sent to 192.168.50.120 for name chdcfs02
[*] [MDNS] Poisoned answer sent to 192.168.50.113  for name DESKTOP-AWADLEY.local
[*] [LLMNR]  Poisoned answer sent to 192.168.50.113 for name DESKTOP-AWADLEY
[HTTP] NTLMv2 Client   : 192.168.50.120
[HTTP] NTLMv2 Username : CH2\cconsole
[HTTP] NTLMv2 Hash     : cconsole::CH2:[redacted]
2D0054004F004F004C004B00490054000400120[redacted]
E006C006F00630061006C0008003000300000000[redacted]
0050002F00630068006400630066007300300003[redacted]
[*] [LLMNR]  Poisoned answer sent to 192.168.50.120 for name chdcfs02
[*] [MDNS] Poisoned answer sent to 192.168.50.120  for name chdcfs02.local
[*] [MDNS] Poisoned answer sent to 192.168.50.136  for name DESKTOP-CFISHER.local
[*] [LLMNR]  Poisoned answer sent to 192.168.50.136 for name DESKTOP-CFISHER
```

Successfully Captured a NetNTLMv2 hash

INT-02: SMB Signing Disabled

Risk: High	Impact: High	Likelihood: Medium

Observation

SMB Signing was disabled on two hosts within the **REDACTED** network. SMB Signing is a security feature that helps to protect against man-in-the-middle attacks by digitally signing SMB traffic.

Impact

When SMB Signing is disabled, it is possible for an attacker to intercept and modify SMB traffic without detection, potentially leading to the compromise of sensitive data or the unauthorized access to systems.

Affected Hosts

- desktop-**REDACTED**
- desktop-**REDACTED**

Remediation

It is recommended to enable SMB Signing on all hosts within their network. This can be done through group policy settings or by modifying the registry on affected systems.

INT-03: Sensitive Data Found in Network Share

Risk: High	Impact: Medium	Likelihood: High

Observation

It was observed that sensitive data, including personally identifiable information (PII), was present in a network share that did not require any elevated permissions to access. This means that any user with access to the network could potentially view or modify this data, regardless of their level of access or permissions.

Impact

The presence of sensitive data in a network share that is not properly protected is a significant risk because it could potentially result in the unauthorized access, disclosure, or modification of sensitive information. This could lead to reputational damage, financial loss, or legal consequences for **REDACTED.**

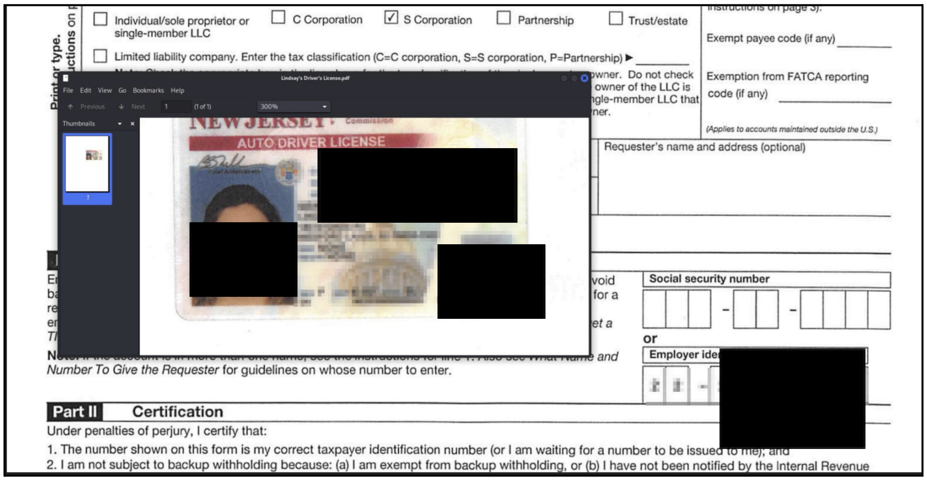
Affected Share/Folders

- \\REDACTED \BROOKE
- \\REDACTED \1.CLIENTS

Remediation

It is recommended to implement stronger access controls on network shares to ensure that only authorized users have access to sensitive data. This could include the use of access control lists, user permissions, and other measures to ensure that only authorized individuals have access to sensitive data. It is also important to regularly review and update access controls to ensure that they are effective in protecting sensitive data.

Evidence


Lindsay's Driver's License.pdf
File Edit View Go Bookmarks Help
Previous Next 1 (1 of 1) 300%
Thumbnails
NEW JERSEY
AUTO DRIVER LICENSE

[redacted]

[redacted]

[redacted]

instructions on page 3).

□ Individual/sole proprietor or single-member LLC □ C Corporation ☑ S Corporation □ Partnership □ Trust/estate

□ Limited liability company. Enter the tax classification (C=C corporation, S=S corporation, P=Partnership) ▶ ______

owner. Do not check owner of the LLC is ngle-member LLC that ner.

Exempt payee code (if any) ______

Exemption from FATCA reporting code (if any) ______

(Applies to accounts maintained outside the U.S.)

Requester's name and address (optional)

void for a et a

Social security number

□□□ – □□ – □□□□

or

Employer ide [redacted]

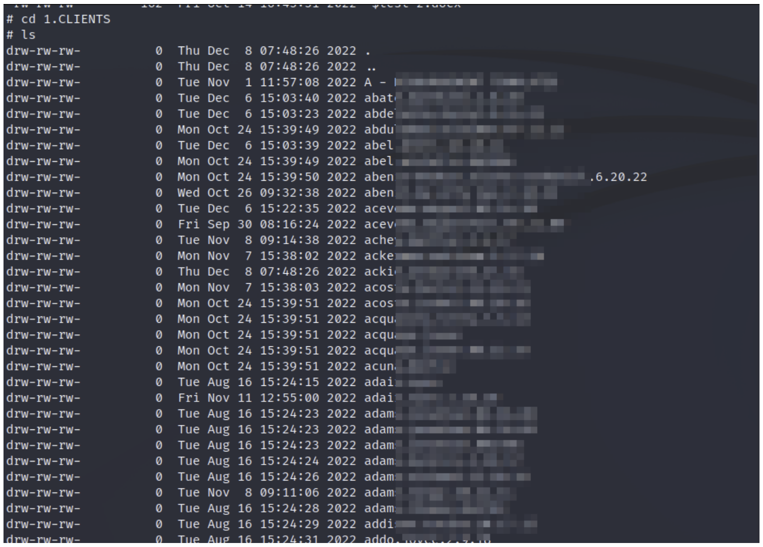
and Number To Give the Requester for guidelines on whose number to enter.

Part II **Certification**

Under penalties of perjury, I certify that:

1. The number shown on this form is my correct taxpayer identification number (or I am waiting for a number to be issued to me); and
2. I am not subject to backup withholding because: (a) I am exempt from backup withholding, or (b) I have not been notified by the Internal Revenue

Personally Identifiable Information found on share



```
# cd 1.CLIENTS
# ls
drw-rw-rw-          0  Thu Dec  8 07:48:26 2022 .
drw-rw-rw-          0  Thu Dec  8 07:48:26 2022 ..
drw-rw-rw-          0  Tue Nov  1 11:57:08 2022 A - 
drw-rw-rw-          0  Tue Dec  6 15:03:40 2022 abat
drw-rw-rw-          0  Tue Dec  6 15:03:23 2022 abde
drw-rw-rw-          0  Mon Oct 24 15:39:49 2022 abdu
drw-rw-rw-          0  Tue Dec  6 15:03:39 2022 abel
drw-rw-rw-          0  Mon Oct 24 15:39:49 2022 abel
drw-rw-rw-          0  Mon Oct 24 15:39:50 2022 aben                          .6.20.22
drw-rw-rw-          0  Wed Oct 26 09:32:38 2022 aben
drw-rw-rw-          0  Tue Dec  6 15:22:35 2022 acev
drw-rw-rw-          0  Fri Sep 30 08:16:24 2022 acev
drw-rw-rw-          0  Tue Nov  8 09:14:38 2022 ache
drw-rw-rw-          0  Mon Nov  7 15:38:02 2022 acke
drw-rw-rw-          0  Thu Dec  8 07:48:26 2022 acki
drw-rw-rw-          0  Mon Nov  7 15:38:03 2022 acos
drw-rw-rw-          0  Mon Oct 24 15:39:51 2022 acos
drw-rw-rw-          0  Mon Oct 24 15:39:51 2022 acqu
drw-rw-rw-          0  Mon Oct 24 15:39:51 2022 acqu
drw-rw-rw-          0  Mon Oct 24 15:39:51 2022 acqu
drw-rw-rw-          0  Mon Oct 24 15:39:51 2022 acun
drw-rw-rw-          0  Tue Aug 16 15:24:15 2022 adai
drw-rw-rw-          0  Fri Nov 11 12:55:00 2022 adai
drw-rw-rw-          0  Tue Aug 16 15:24:23 2022 adam
drw-rw-rw-          0  Tue Aug 16 15:24:23 2022 adam
drw-rw-rw-          0  Tue Aug 16 15:24:23 2022 adam
drw-rw-rw-          0  Tue Aug 16 15:24:24 2022 adam
drw-rw-rw-          0  Tue Aug 16 15:24:26 2022 adam
drw-rw-rw-          0  Tue Nov  8 09:11:06 2022 adam
drw-rw-rw-          0  Tue Aug 16 15:24:28 2022 adam
drw-rw-rw-          0  Tue Aug 16 15:24:29 2022 addi
drw-rw-rw-          0  Tue Aug 16 15:24:31 2022 addo
```

List of clients found on share

INT-04: Weak Domain Password Policy

Risk: Medium	Impact: Medium	Likelihood: Medium

Observation

It was observed that the **REDACTED** domain password policy was weak. While Aegis Security was not able to crack any passwords during the engagement, the password policy required a minimum of only 7 characters along with capital letters, numbers, and symbols. This is lower than industry best practices, which recommend using passwords that are at least 8 characters long and include the complexity requirements mentioned above.

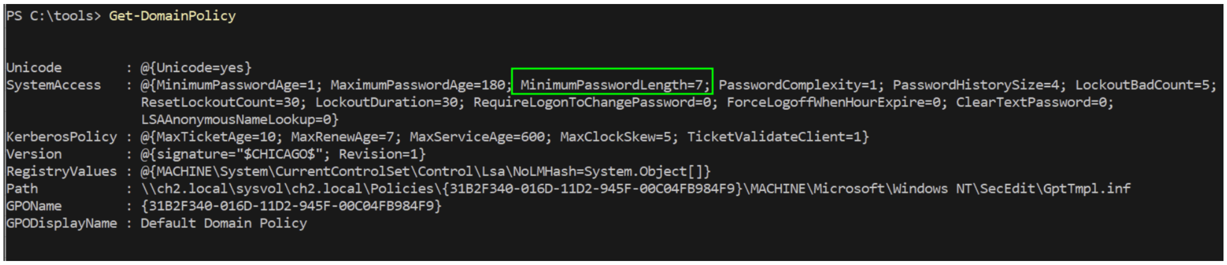
Impact

A weak password policy is a significant risk because it allows for the use of weak passwords, which are more vulnerable to being cracked or guessed by an attacker. This could potentially result in unauthorized access to sensitive data or systems.

Remediation

It is recommended to increase the minimum password length to at least 8 characters and to prevent common dictionary words in user passwords.

Evidence



```
PS C:\tools> Get-DomainPolicy


Unicode        : @{Unicode=yes}
SystemAccess   : @{MinimumPasswordAge=1; MaximumPasswordAge=180; MinimumPasswordLength=7; PasswordComplexity=1; PasswordHistorySize=4; LockoutBadCount=5;
                 ResetLockoutCount=30; LockoutDuration=30; RequireLogonToChangePassword=0; ForceLogoffWhenHourExpire=0; ClearTextPassword=0;
                 LSAAnonymousNameLookup=0}
KerberosPolicy : @{MaxTicketAge=10; MaxRenewAge=7; MaxServiceAge=600; MaxClockSkew=5; TicketValidateClient=1}
Version        : @{signature="$CHICAGO$"; Revision=1}
RegistryValues : @{MACHINE\System\CurrentControlSet\Control\Lsa\NoLMHash=System.Object[]}
Path           : \\ch2.local\sysvol\ch2.local\Policies\{31B2F340-016D-11D2-945F-00C04FB984F9}\MACHINE\Microsoft\Windows NT\SecEdit\GptTmpl.inf
GPOName        : {31B2F340-016D-11D2-945F-00C04FB984F9}
GPODisplayName : Default Domain Policy
```

Password policy retrieved from the domain

INT-05: Unprotected BIOS Settings

Risk: Medium	Impact: High	Likelihood: Low

Observation

It was observed that the BIOS settings on one of the employee workstations did not have a password set. The BIOS (Basic Input/Output System) is a low-level software that controls the hardware of a computer system, and it is responsible for booting the operating system.

Note: Only one workstation was tested during the assessment. All workstations should be checked for a BIOS password.

Impact

Not having a password set for the BIOS is a significant risk because it allows for unauthorized access to the BIOS settings, which could potentially result in the compromise of the system. An attacker could potentially change the boot order of the system, install malicious software, or disable security features.

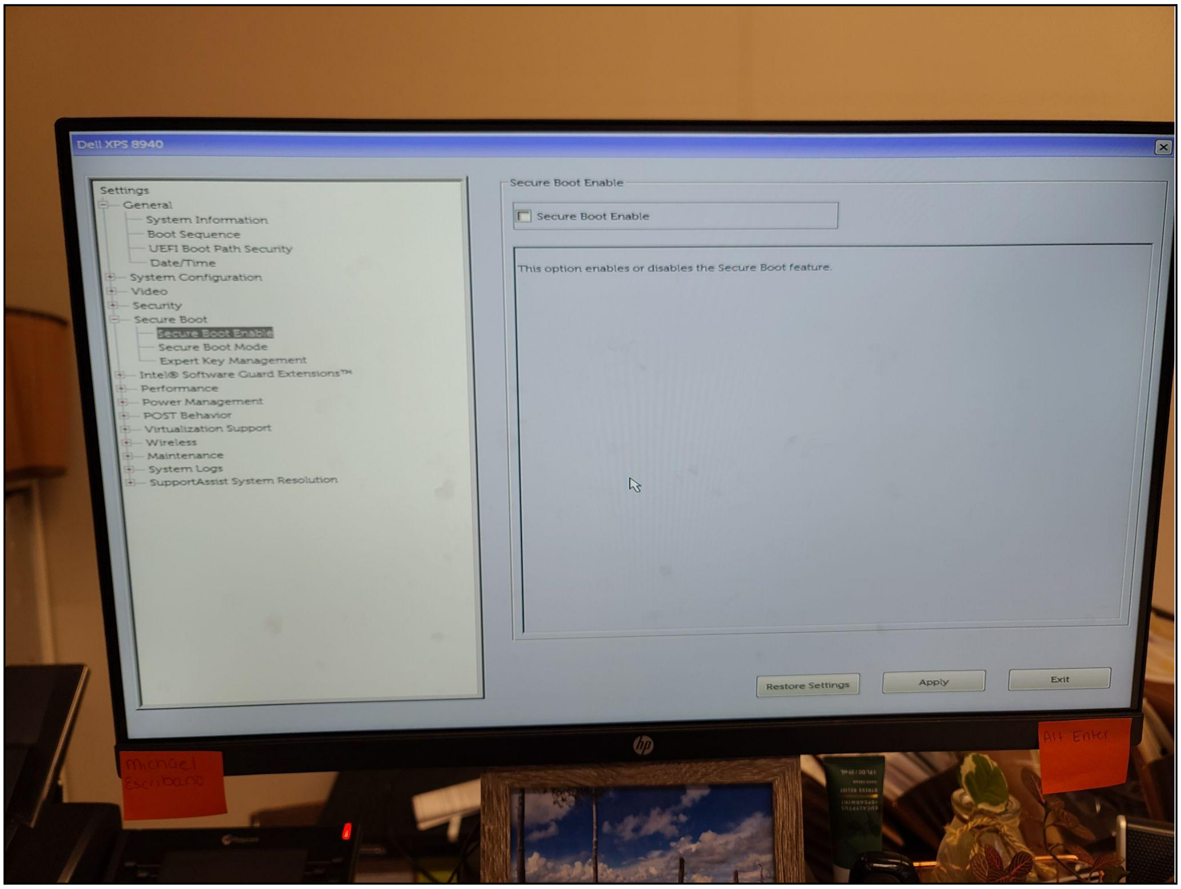
Affected Host

- DESKTOP-**REDACTED**

Remediation

To mitigate this risk, it is recommended to set a password for the BIOS on all workstations. This will help to protect against unauthorized access to the BIOS settings and ensure the integrity of the system.

Evidence



Secure Boot Enable

☐ Secure Boot Enable

This option enables or disables the Secure Boot feature.

Secure boot was disabled on the workstation

INT-06: Unencrypted Hard Drives

Risk: Medium	Impact: High	Likelihood: Low

Observation

A workstation hard drive was not encrypted, which allowed for the booting of a new operating system and the dumping of local hashes. Encrypting hard drives is a security measure that helps to protect the confidentiality and integrity of data by encoding it in a way that can only be accessed with a decryption key.

Impact

Not encrypting workstation hard drives is a significant risk because it allows for the potential access, disclosure, or modification of sensitive data. An attacker could potentially boot a new operating system on the workstation and dump the local hashes, which are used to authenticate users on the system. This could potentially result in unauthorized access to sensitive data or systems.

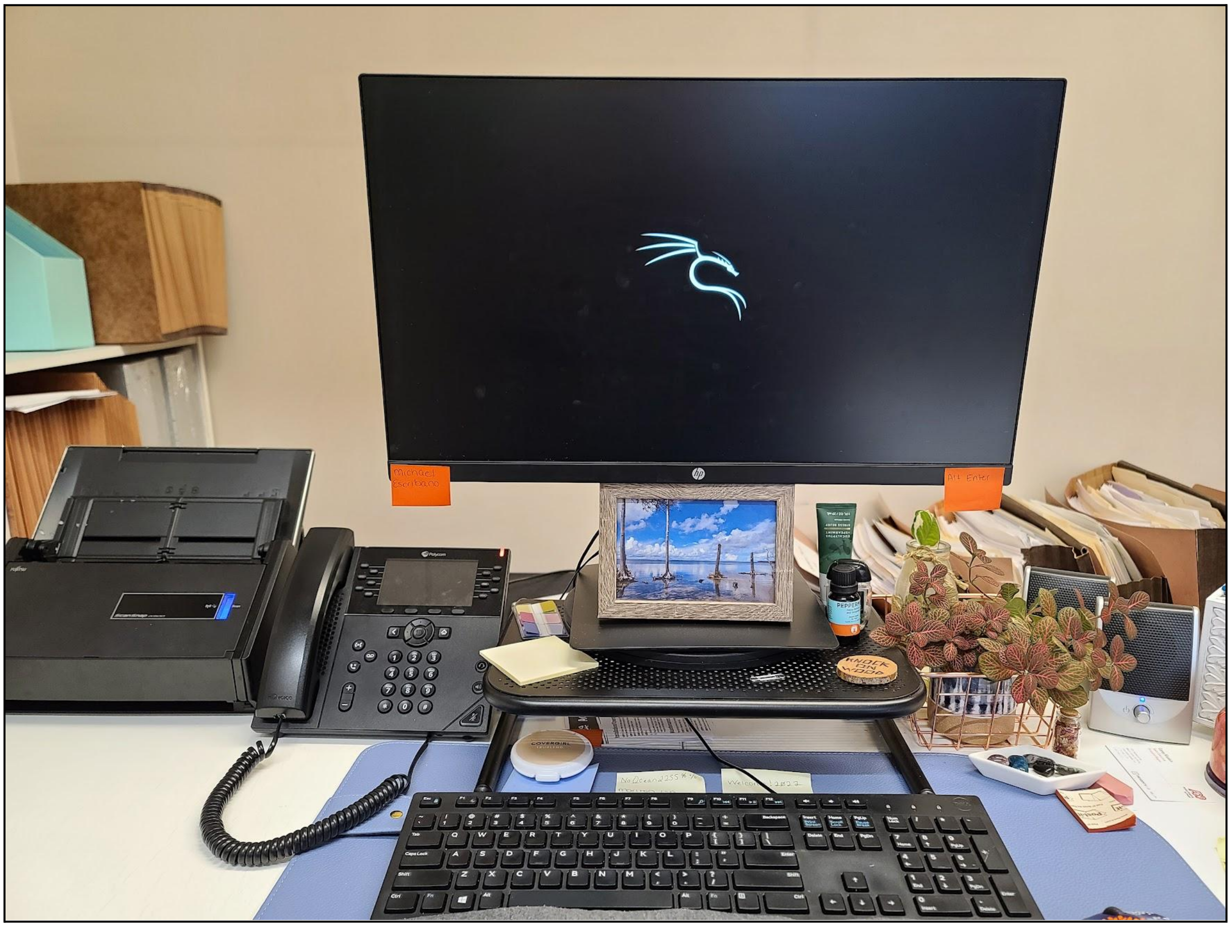
Affected Host

- DESKTOP-**REDACTED**

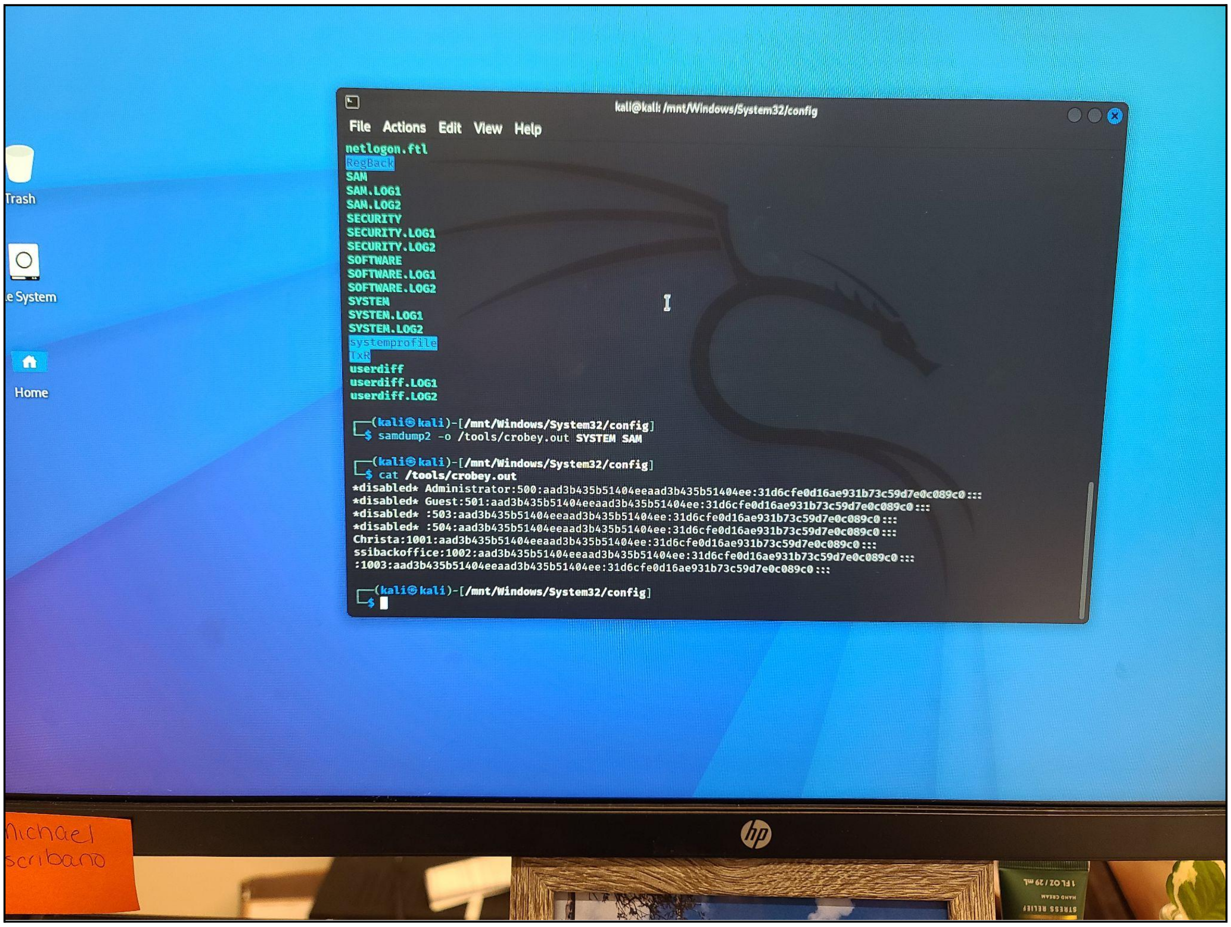
Remediation

It is recommended that workstation hard drives are encrypted using Bitlocker or similar encryption tools.

Evidence



Kali successfully booting on the workstation



```
netlogon.ftl
RegBack
SAM
SAM.LOG1
SAM.LOG2
SECURITY
SECURITY.LOG1
SECURITY.LOG2
SOFTWARE
SOFTWARE.LOG1
SOFTWARE.LOG2
SYSTEM
SYSTEM.LOG1
SYSTEM.LOG2
systemprofile
TxR
userdiff
userdiff.LOG1
userdiff.LOG2

┌──(kali㉿kali)-[/mnt/Windows/System32/config]
└─$ samdump2 -o /tools/crobey.out SYSTEM SAM

┌──(kali㉿kali)-[/mnt/Windows/System32/config]
└─$ cat /tools/crobey.out
*disabled* Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
*disabled* Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
*disabled* :503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
*disabled* :504:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Christa:1001:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
ssibackoffice:1002:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
:1003:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::

┌──(kali㉿kali)-[/mnt/Windows/System32/config]
└─$ 
```

Internal drive successfully mounted and NTLM hashes were dumped

INT-07: Passwords Stored on Physical Notes

Risk: Medium	Impact: High	Likelihood: Low

Observation

During the pentest, it was observed that there were two sticky notes with passwords written on them underneath an employee's keyboard. The use of sticky notes to store passwords is a security risk because it allows for the potential access, disclosure, or modification of sensitive information. An attacker could potentially find and use these passwords to gain unauthorized access to the system or data.

Impact

Given the time and opportunity, an attacker could easily find these notes and use these passwords in password spray attacks on both the domain and other online accounts associated with the affected user.

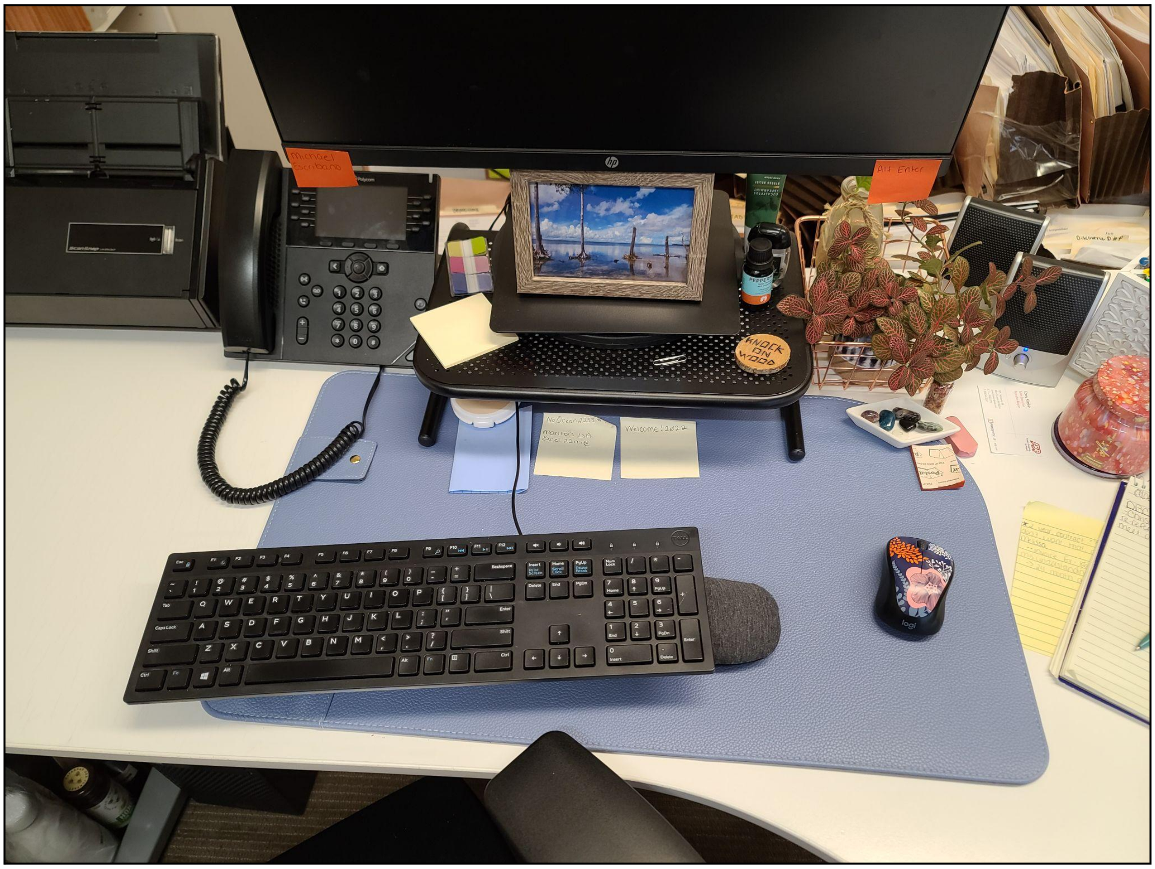
Affected User

- **REDACTED**

Remediation

It is recommended that **REDACTED** implements a password management policy to ensure that passwords are stored in a secure manner. This could include the use of a password manager, the implementation of strong passwords, and the regular review and update of passwords. It is also important for **REDACTED** to educate employees about good security practices and the importance of protecting sensitive information.

Evidence



Two sticky notes with passwords were found under a keyboard

Conclusion

Overall, the results of the penetration test indicate that **REDACTED** has a strong security posture. The testing identified several vulnerabilities and areas for improvement, but no methods of privilege escalation were found.

Overall, the **REDACTED** has implemented strong security controls, such as strong passwords and limited administrative permissions, which have helped to protect their systems and data from potential threats. By addressing the vulnerabilities identified during the test and continuing to implement good security practices, **REDACTED** can further strengthen their security posture and protect their systems and data from potential threats.

Appendix A - Tools Used

Tool	Availability
Nmap	Open Source
Responder	Open Source
Impacket	Open Source
Bloodhound	Open Source
Kali Linux	Open Source