SMTP & SNMP

LinkedIn : https://www.linkedin.com/in/mohamed-elsayaad

GitHub : https://github.com/0xDos

SMTP Enumeration

SMTP <<< service مسؤوله عن ارسال واستقبال Emails بين الأنظمة

- **Simple Mail Transfer Protocol**

عندنا مثلا <<< ahmed@grab.com
ahmed دا مستخدم عادي
grab.com دا هيكون mail server تبع شركة grab

اهم جزئيه محتاجها في SMTP Enum <<< اني اشوف ايه Users ال موجوده ومتسجله عنده علي SMTP Server

- Scanning for the SMTP Service
  - VRFY users manual & auto
  - Nmap
  - Metasploit

• Scanning for the SMTP Service

• VRFY users manual & auto

Manual

```
┌──(kali㉿kali)-[~]
└─$ nc -nvv 192.168.1.30 25
(UNKNOWN) [192.168.1.30] 25 (smtp) open
220 metasploitable.localdomain ESMTP Postfix (Ubuntu)
500 5.5.2 Error: bad syntax
VRFY AHMED
550 5.1.1 <AHMED>: Recipient address rejected: User unknown in loc
VRFY ROOT
252 2.0.0 ROOT
VRFY admin
550 5.1.1 <admin>: Recipient address rejected: User unknown in loc
```

```
┌──(kali㉿WebServer)-[~]
└─$ telnet 192.168.1.30 25
Trying 192.168.1.30 ...
Connected to 192.168.1.30.
Escape character is '^]'.
VRFY220 metasploitable.localdomain ESMTP Postfix (Ubuntu)
VRFY ahmed
502 5.5.2 Error: command not recognized
VRFY ADEL
550 5.1.1 <ADEL>: Recipient address rejected: User unknown
```

Smtp بتشتغل علي بورت 25

VRFY >>> واحد من اشهر commands ال بتأكد بيه ان user موجود عنده ولا لأ

هل منطقي نقعد نجرب Manual وبالتالي هنعمل الاتي :

1) هاجيب file من علي السيستم موجود عليه users كتيره جدا اسمه common.txt
2) هاعمل script بنفسي او يوجد script جاهز اصطبه اسمه Smtp-user-enum
3) ادمج Smtp-user-enum مع common.txt في command واحد

• Scanning for the SMTP Service

• Nmap

```
┌──(kali㉿kali)-[/]
└─$ ls /usr/share/nmap/scripts/smtp-
Completing files
smtp-brute.nse          smtp-enum-users.nse     smtp-open-relay.nse     smtp-vuln-cve2010-4344.nse  smtp-vuln-cve2011-1764.nse
smtp-commands.nse       smtp-ntlm-info.nse      smtp-strangeport.nse    smtp-vuln-cve2011-1720.nse
```

Automate

```
┌──(kali㉿kali)-[~/Desktop]
└─$ smtp-user-enum -M VRFY -U /usr/share/wordlists/fern-wifi/common.txt -t 192.168.1.30 -w 20

\Starting smtp-user-enum v1.2 ( http://pentestmonkey.net/tools/smtp-user-enum )

 ----------------------------------------------------------
|                    Scan Information                      |
 ----------------------------------------------------------

Mode ..................... VRFY
Worker Processes ......... 5
Usernames file ........... /usr/share/wordlists/fern-wifi/common.txt
Target count ............. 1
Username count ........... 478
Target TCP port .......... 25
Query timeout ............ 20 secs
Target domain ............

######### Scan started at Wed Feb  2 14:00:49 2022 #########


 exists.1.30: lp
 exists.1.30: root
 exists.1.30: service
 exists.1.30: sys
 exists.1.30: user
 exists.1.30: MAIL
 exists.1.30: Root
 exists.1.30: SERVICE
 exists.1.30: SYS
 exists.1.30: Service
 exists.1.30: User
######### Scan completed at Wed Feb  2 14:16:49 2022 #########
11 results.

478 queries in 960 seconds (0.5 queries / sec)
```

```
┌──(kali㉿kali)-[~]
└─$ smtp-user-enum --help
/usr/bin/smtp-user-enum version [unknown] calling Getopt::Std::getopts (version 1.12 [paranoid]),
running under Perl version 5.32.1.

 -M mode  Method to use for username guessing EXPN, VRFY or RCPT (default: VRFY)
-U file   File of usernames to check via smtp service
  -t host  Server host running smtp service
-w n      Wait a maximum of n seconds for reply (default: 5)

Examples:

$ smtp-user-enum -M VRFY -U users.txt -t 10.0.0.1
$ smtp-user-enum -M EXPN -u admin1 -t 10.0.0.1
$ smtp-user-enum -M RCPT -U users.txt -T mail-server-ips.txt
```


LinkedIn : https://www.linkedin.com/in/mohamed-elsayaad
GitHub : https://github.com/0xDos

SMTP Enumeration

- SMTP provides 3 built-in-commands:
  - VRFY - Validates users
  - EXPN - Tells the actual delivery addresses of aliases and mailing lists
  - RCPT TO - Defines the recipients of the message
- SMTP servers respond differently to VRFY, EXPN, and RCPT TO commands for valid and invalid users from which we can determine valid users on SMTP server
- Attackers can directly interact with SMTP via the telnet prompt and collect list of valid users on the SMTP server

Using the SMTP VRFY Command

```
$ telnet 192.168.168.1 25
Trying 192.168.168.1...
Connected to 192.168.168.1.
Escape character is '^]'.
220 NYmailserver ESMTP Sendmail 8.9.3
HELO
501 HELO requires domain address
HELO x
250 NYmailserver Hello [10.0.0.86],
pleased to meet you
VRFY Jonathan
250 Super-User
<Jonathan@NYmailserver>
VRFY Smith
550 Smith... User unknown
```

Using the SMTP EXPN Command

```
$ telnet 192.168.168.1 25
Trying 192.168.168.1...
Connected to 192.168.168.1.
Escape character is '^]'.
220 NYmailserver ESMTP Sendmail 8.9.3
HELO
501 HELO requires domain address
HELO x
250 NYmailserver Hello [10.0.0.86],
pleased to meet you
EXPN Jonathan
250 Super-User
<Jonathan@NYmailserver>
EXPN Smith
550 Smith... User unknown
```

Using the SMTP RCPT TO Command

```
$ telnetl 192.168.168.1 25
Trying 192.168.168.1 ...
Connected to 192.168.168.1.
Escape character is '^]'.
220 NYmailserver ESMTP Sendmail 8.9.3
HELO
501 HELO requires domain address
HELO x
250 NYmailserver Hello [10.0.0.86],
pleased to meet you
MAIL FROM:Jonathan
250 Jonathan... Sender ok
RCPT TO:Ryder
250 Ryder... Recipient ok
RCPT TO: Smith
550 Smith... User unknown
```

Simple Mail Transport Protocol

- Used to send email between systems
- TCP/25

SMTP Verbs Available to Enumerate:

Command	Description
EXPN	Expand, show all recipients of an address.
VRFY	Verify, validates if a user exists.
RCPT TO	Sets the destination address of the email.

As simple as telnet <mailserver> 25 however, many modern mail servers will obfuscate the results.

LinkedIn : https://www.linkedin.com/in/mohamed-elsayaad

GitHub : https://github.com/0xDos

You can communicate directly with smtp server using telnet

telnet 10.1.1.1 25
-VRFY Yasser

It will respond with 250 super-user yasser@cbtme.com
Or it will respond with 550 Yasser……user unknown

-EXPN Yasser

Same above

RCPT TO: Yasser

It will respond with 250 Yasser …..Recipient OK
Or it will respond with 550 Yasser……user unknown

http://mxtoolbox.com/diagnostic.aspx
Use mail.abcxyz.com

Install telnet feature in your windows first from add roles & features

LinkedIn : https://www.linkedin.com/in/mohamed-elsayaad
GitHub : https://github.com/0xDos

SNMP Enumeration

- **Simple Network Management Protocol**

- MIB OID
- Scanning for the SNMP Service
  - nmap
  - metasploit
  - Snmpwalk
  - Snmpset

LinkedIn : https://www.linkedin.com/in/mohamed-elsayaad **GitHub** : https://github.com/0xDos

SNMP

SNMP (Simple Network Management Protocol) Enumeration

- SNMP enumeration is a process of **enumerating user accounts and devices** on a target system using SNMP
- SNMP consists of a **manager** and an **agent**; agents are embedded on every network device, and the manager is installed on a separate computer

- SNMP holds **two passwords** to access and configure the SNMP agent from the management station
  - **Read community string**: It is public by default; allows viewing of device/system configuration
  - **Read/write community string**: It is private by default; allows remote editing of configuration

- Attacker uses these **default community strings** to extract information about a device
- Attackers enumerate SNMP to extract information about **network resources** such as hosts, routers, devices, shares, etc. and **network information** such as ARP tables, routing tables, traffic, etc.

MIB & OID

Management Information Base (MIB)

- MIB is a virtual database containing **formal description of all the network objects** that can be managed using SNMP

MIB قاعده بيانات تحتوي علي معلومات مفصله من **network objects** التي تدار بواسطه **SNMP**

- The MIB database is hierarchical and each managed object in a MIB is addressed through **Object Identifiers (OIDs)**

OID كل **network object** موجود في **MIB** معنون برقم تعريفي

- Two types of **managed objects** exist:
  - **Scalar objects** that define a single object instance
  - **Tabular objects** that define multiple related object instances are grouped in **MIB tables**
- The OID includes the type of **MIB object** such as counter, string, or address, access level such as not-accessible, accessible-for-notify, read-only or read-write, size restrictions, and range information
- SNMP uses the MIB's hierarchical namespace containing Object Identifiers (OIDs) to translate the **OID numbers** into a **human-readable** display

LinkedIn : https://www.linkedin.com/in/mohamed-elsayaad

GitHub : https://github.com/0xDos

SNMP Simple Network managment protocol

V1
V2
V2C
V3
} plain text ⇒ Password = Community string

Pc
Network managment station
NMS
Get request
Set request
Agent
OID
OID
MIB
Managment info Base

OID = object identifier
ex: .1.3.6.1.2.1.1.4.0

SNMP Simple Network managment protocol

V1
V2
V2C
V3
} plain text ⇒ Password = Community string

Pc
Network managment station
NMS
Trap
Agent
OID
OID
MIB
Managment info Base

Get / Set UDP 161

Trap (no ack) UDP 162

V3 informs (with ack)

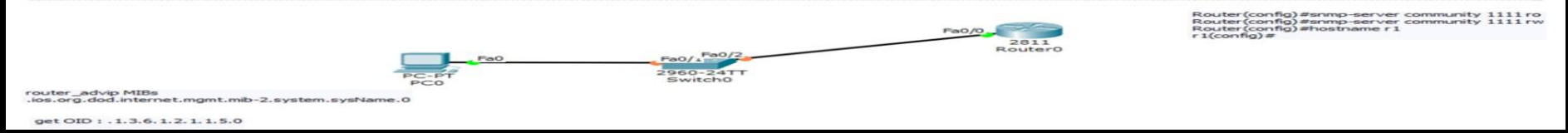
MIB tree

.1.3.6.1.2.1.1.4.0
leaves

Trunk of tree

ISO
1.2 → ISO, CCITT
1.3 → other org
1.6 → DoD

.1.3.6.1.4.1.9.2.16.0
Cisco
cisco free Memory info



LinkedIn : https://www.linkedin.com/in/mohamed-elsayaad

GitHub : https://github.com/0xDos

• Scanning for the SNMP Service

• nmap

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sU --script=snmp-win32-services.nse 192.168.1.17 -p 161
[sudo] password for kali:
Starting Nmap 7.92 ( https://nmap.org ) at 2022-02-02 16:07 EST
Nmap scan report for 192.168.1.17
Host is up (0.00054s latency).

PORT    STATE SERVICE
161/udp open  snmp
| snmp-win32-services:
|   Application Information
|   Background Intelligent Transfer Service
|   Base Filtering Engine
|   COM+ Event System
|   Computer Browser
|   Cryptographic Services
|   DCOM Server Process Launcher
|   DHCP Client
|   DNS Client
|   Desktop Window Manager Session Manager
|   Diagnostic Policy Service
|   Diagnostic Service Host
|   Diagnostics Tracking Service
|   Distributed Link Tracking Client
|   Distributed Transaction Coordinator
|   Group Policy Client
|   IKE and AuthIP IPsec Keying Modules
|   IP Helper
|   IPsec Policy Agent
|   Network Connections
|   Network List Service
|   Network Location Awareness
|   Network Store Interface Service
|   Offline Files
|   Plug and Play
|   Power
|   Print Spooler
|   Program Compatibility Assistant Service
|   RPC Endpoint Mapper
|   Remote Procedure Call (RPC)
|   SNMP Service
|   SPP Notification Service
|   SSDP Discovery
|   Security Accounts Manager
|   Security Center
|   Server
|   Shell Hardware Detection
|   Software Protection
|   Superfetch
|   System Event Notification Service
|   TCP/IP NetBIOS Helper
|   Task Scheduler
|   Themes
|   User Profile Service
|   VMware Alias Manager and Ticket Service
|   VMware SVGA Helper Service
|   VMware Tools
|   Windows Audio
|   Windows Audio Endpoint Builder
|   Windows Defender
|   Windows Event Log
```

• Scanning for the SNMP Service

• Snmpwalk

```
┌──(kali㉿kali)-[~]
└─$ snmpwalk -v1 -c public 192.168.1.17
iso.3.6.1.2.1.1.1.0 = STRING: "Hardware: Intel64 Family 6 Model 42 Steppin
rsion 6.1 (Build 7601 Multiprocessor Free)"
iso.3.6.1.2.1.1.2.0 = OID: iso.3.6.1.4.1.311.1.1.3.1.1
iso.3.6.1.2.1.1.3.0 = Timeticks: (199647) 0:33:16.47
iso.3.6.1.2.1.1.4.0 = ""
iso.3.6.1.2.1.1.5.0 = STRING: "client7-PC"
iso.3.6.1.2.1.1.6.0 = ""
iso.3.6.1.2.1.1.7.0 = INTEGER: 76
iso.3.6.1.2.1.2.1.0 = INTEGER: 21
iso.3.6.1.2.1.2.2.1.1.1 = INTEGER: 1
iso.3.6.1.2.1.2.2.1.1.2 = INTEGER: 2
iso.3.6.1.2.1.2.2.1.1.3 = INTEGER: 3
iso.3.6.1.2.1.2.2.1.1.4 = INTEGER: 4
iso.3.6.1.2.1.2.2.1.1.5 = INTEGER: 5
iso.3.6.1.2.1.2.2.1.1.6 = INTEGER: 6
iso.3.6.1.2.1.2.2.1.1.7 = INTEGER: 7
iso.3.6.1.2.1.2.2.1.1.8 = INTEGER: 8
iso.3.6.1.2.1.2.2.1.1.9 = INTEGER: 9
iso.3.6.1.2.1.2.2.1.1.10 = INTEGER: 10
iso.3.6.1.2.1.2.2.1.1.11 = INTEGER: 11
iso.3.6.1.2.1.2.2.1.1.12 = INTEGER: 12
iso.3.6.1.2.1.2.2.1.1.13 = INTEGER: 13
iso.3.6.1.2.1.2.2.1.1.14 = INTEGER: 14
iso.3.6.1.2.1.2.2.1.1.15 = INTEGER: 15
iso.3.6.1.2.1.2.2.1.1.16 = INTEGER: 16
iso.3.6.1.2.1.2.2.1.1.17 = INTEGER: 17
iso.3.6.1.2.1.2.2.1.1.18 = INTEGER: 18
iso.3.6.1.2.1.2.2.1.1.19 = INTEGER: 19
iso.3.6.1.2.1.2.2.1.1.20 = INTEGER: 20
iso.3.6.1.2.1.2.2.1.1.21 = INTEGER: 21
iso.3.6.1.2.1.2.2.1.2.1 = Hex-STRING: 53 6F 66 74 77 61 72 65 20 4C 6F 6F
6B 20 49 6E 74 65 72 66 61 63 65 20 31 00
iso.3.6.1.2.1.2.2.1.2.2 = Hex-STRING: 57 41 4E 20 4D 69 6E 69 70 6F 72 74
54 50 29 00
iso.3.6.1.2.1.2.2.1.2.3 = Hex-STRING: 57 41 4E 20 4D 69 6E 69 70 6F 72 74
54 50 29 00
iso.3.6.1.2.1.2.2.1.2.4 = Hex-STRING: 57 41 4E 20 4D 69 6E 69 70 6F 72 74
54 50 29 00
iso.3.6.1.2.1.2.2.1.2.5 = Hex-STRING: 57 41 4E 20 4D 69 6E 69 70 6F 72 74
50 4F 45 29 00
iso.3.6.1.2.1.2.2.1.2.6 = Hex-STRING: 57 41 4E 20 4D 69 6E 69 70 6F 72 74
76 36 29 00
iso.3.6.1.2.1.2.2.1.2.7 = Hex-STRING: 57 41 4E 20 4D 69 6E 69 70 6F 72 74
74 77 6F 72 6B 20 4D 6F 6E 69 74 6F 72 29 00
iso.3.6.1.2.1.2.2.1.2.8 = Hex-STRING: 57 41 4E 20 4D 69 6E 69 70 6F 72 74
29 00
iso.3.6.1.2.1.2.2.1.2.9 = Hex-STRING: 52 41 53 20 41 73 79 6E 63 20 41 64
72 00
iso.3.6.1.2.1.2.2.1.2.10 = Hex-STRING: 57 41 4E 20 4D 69 6E 69 70 6F 72 74
45 76 32 29 00
iso.3.6.1.2.1.2.2.1.2.11 = Hex-STRING: 49 6E 74 65 6C 28 52 29 20 50 52 4F
30 20 4D 54 20 4E 65 74 77 6F 72 6B 20 43 6F 6E
6E 65 63 74 69 6F 6E 00
iso.3.6.1.2.1.2.2.1.2.12 = Hex-STRING: 4D 69 63 72 6F 73 6F 66 74 20 49 53
20 41 64 61 70 74 65 72 00
iso.3.6.1.2.1.2.2.1.2.13 = Hex-STRING: 49 6E 74 65 6C 28 52 29 20 50 52 4F
30 20 4D 54 20 4E 65 74 77 6F 72 6B 20 43 6F 6E
6E 65 63 74 69 6F 6E 2D 4E 70 63 61 70 20 50 61
63 6B 65 74 20 44 72 69 76 65 72 20 28 4E 50 43
```


LinkedIn : https://www.linkedin.com/in/mohamed-elsayaad

GitHub : https://github.com/0xDos

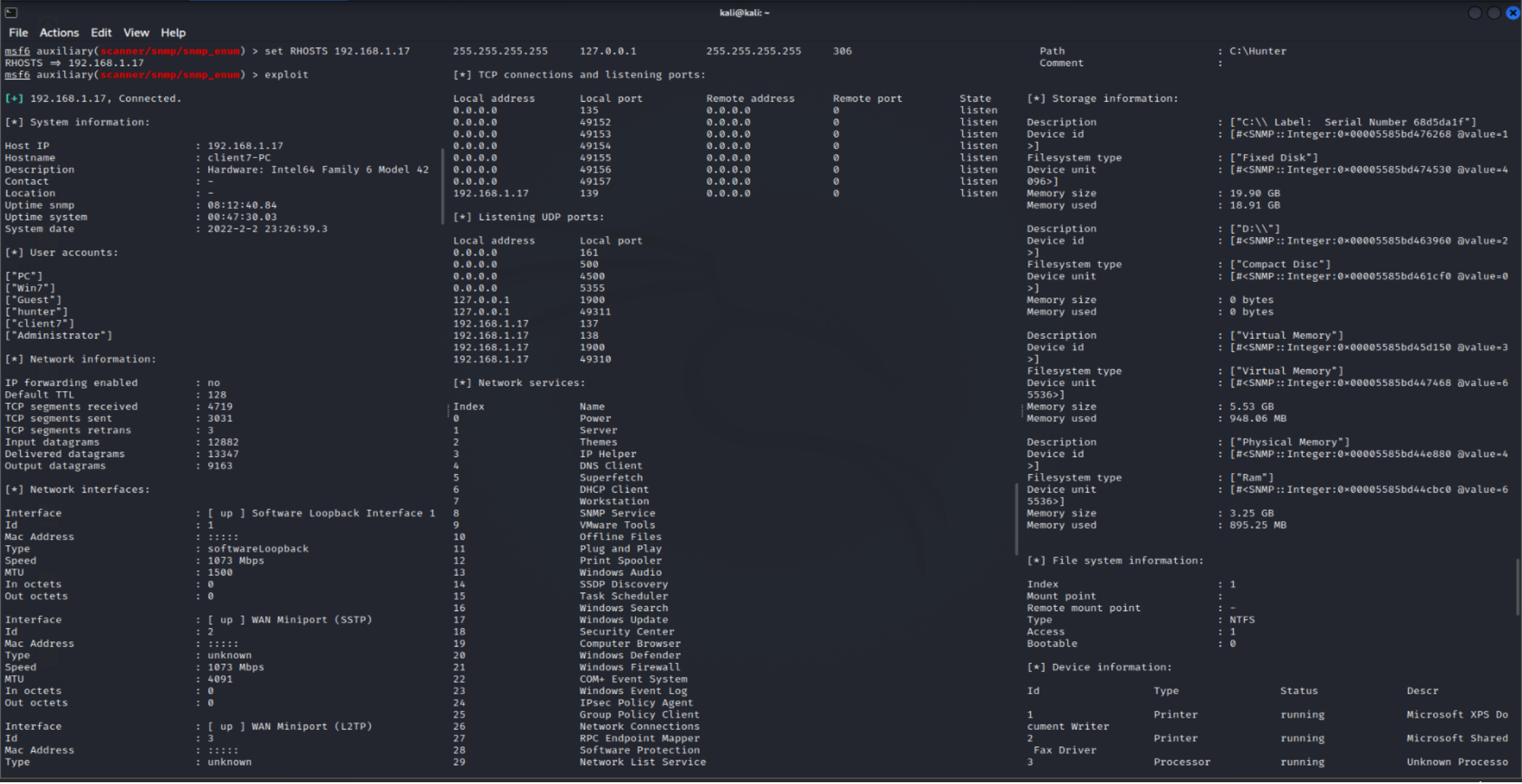
• Scanning for the SNMP Service

• metasploit

```
File  Actions  Edit  View  Help
Matching Modules
================

   #   Name                                                  Disclosure Date  Rank       Check  Description
   -   ----                                                  ---------------  ----       -----  -----------
   0   auxiliary/scanner/snmp/aix_version                                     normal     No     AIX SNMP Scanner Auxiliary Module
   1   auxiliary/scanner/snmp/sbg6580_enum                                    normal     No     ARRIS / Motorola SBG6580 Cable Modem SNMP Enumeration Module
   2   auxiliary/scanner/snmp/arris_dg950                                     normal     No     Arris DG950A Cable Modem Wifi Enumeration
   3   exploit/linux/snmp/awind_snmp_exec                    2019-03-27       excellent  Yes    AwindInc SNMP Service Command Injection
   4   auxiliary/scanner/snmp/brocade_enumhash                                normal     No     Brocade Password Hash Enumeration
   5   auxiliary/scanner/snmp/cnpilot_r_snmp_loot                             normal     No     Cambium cnPilot r200/r201 SNMP Enumeration
   6   auxiliary/scanner/snmp/epmp1000_snmp_loot                              normal     No     Cambium ePMP 1000 SNMP Enumeration
   7   auxiliary/admin/networking/cisco_asa_extrabacon                        normal     Yes    Cisco ASA Authentication Bypass (EXTRABACON)
   8   auxiliary/scanner/snmp/cisco_config_tftp                               normal     No     Cisco IOS SNMP Configuration Grabber (TFTP)
   9   auxiliary/scanner/snmp/cisco_upload_file                               normal     No     Cisco IOS SNMP File Upload (TFTP)
   10  exploit/linux/misc/hp_jetdirect_path_traversal        2017-04-05       normal     No     HP Jetdirect Path Traversal Arbitrary Code Execution
   11  auxiliary/scanner/snmp/snmp_enum_hp_laserjet                           normal     No     HP LaserJet Printer SNMP Enumeration
   12  exploit/windows/http/hp_nnm_snmp                      2009-12-09       great      No     HP OpenView Network Node Manager Snmp.exe CGI Buffer Overflow
   13  exploit/windows/http/hp_nnm_ovwebsnmpsrv_uro          2010-06-08       great      No     HP OpenView Network Node Manager ovwebsnmpsrv.exe Unrecognized Option Buffer Overflow
   14  exploit/windows/http/hp_nnm_ovwebsnmpsrv_main         2010-06-16       great      No     HP OpenView Network Node Manager ovwebsnmpsrv.exe main Buffer Overflow
   15  exploit/windows/http/hp_nnm_ovwebsnmpsrv_ovutil       2010-06-16       great      No     HP OpenView Network Node Manager ovwebsnmpsrv.exe ovutil Buffer Overflow
   16  exploit/windows/http/hp_nnm_snmpviewer_actapp         2010-05-11       great      No     HP OpenView Network Node Manager snmpviewer.exe Buffer Overflow
   17  exploit/multi/http/hp_sys_mgmt_exec                   2013-06-11       excellent  Yes    HP System Management Homepage JustGetSNMPQueue Command Injection
   18  auxiliary/admin/scada/moxa_credentials_recovery       2015-07-28       normal     Yes    Moxa Device Credential Retrieval
   19  exploit/linux/http/nagios_xi_snmptrap_authenticated_rce 2020-10-20     excellent  Yes    Nagios XI 5.5.0-5.7.3 - Snmptrap Authenticated Remote Code Exection
   20  exploit/linux/snmp/net_snmpd_rw_access                2004-05-10       normal     No     Net-SNMPd Write Access SNMP-EXTEND-MIB arbitrary code execution
   21  auxiliary/scanner/snmp/netopia_enum                                    normal     No     Netopia 3347 Cable Modem Wifi Enumeration
   22  auxiliary/scanner/misc/oki_scanner                                     normal     No     OKI Printer Default Login Credential Scanner
   23  exploit/windows/ftp/oracle9i_xdb_ftp_unlock           2003-08-18       great      Yes    Oracle 9i XDB FTP UNLOCK Overflow (win32)
   24  auxiliary/scanner/snmp/snmp_login                                      normal     No     SNMP Community Login Scanner
   25  auxiliary/scanner/snmp/snmp_enum                                       normal     No     SNMP Enumeration Module
   26  auxiliary/scanner/snmp/snmp_set                                        normal     No     SNMP Set Module
   27  auxiliary/scanner/snmp/snmp_enumshares                                 normal     No     SNMP Windows SMB Share Enumeration
   28  auxiliary/scanner/snmp/snmp_enumusers                                  normal     No     SNMP Windows Username Enumeration
   29  exploit/freebsd/webapp/spamtitan_unauth_rce           2020-04-17       normal     Yes    SpamTitan Unauthenticated RCE
   30  exploit/windows/scada/sunway_force_control_netdbsrv   2011-09-22       great      No     Sunway Forcecontrol SNMP NetDBServer.exe Opcode 0x57
   31  auxiliary/scanner/snmp/ubee_ddw3611                                    normal     No     Ubee DDW3611b Cable Modem Wifi Enumeration
   32  post/windows/gather/enum_snmp                                          normal     No     Windows Gather SNMP Settings Enumeration (Registry)
   33  auxiliary/scanner/snmp/xerox_workcentre_enumusers                      normal     No     Xerox WorkCentre User Enumeration (SNMP)


Interact with a module by name or index. For example info 33, use 33 or use auxiliary/scanner/snmp/xerox_workcentre_enumusers

msf6 > use 25
msf6 auxiliary(scanner/snmp/snmp_enum) > show options

Module options (auxiliary/scanner/snmp/snmp_enum):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   COMMUNITY  public           yes       SNMP Community String
   RETRIES    1                yes       SNMP Retries
   RHOSTS                      yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
   RPORT      161              yes       The target port (UDP)
   THREADS    1                yes       The number of concurrent threads (max one per host)
   TIMEOUT    1                yes       SNMP Timeout
   VERSION    1                yes       SNMP Version <1/2c>

msf6 auxiliary(scanner/snmp/snmp_enum) > set RHOSTS 192.168.1.17
RHOSTS => 192.168.1.17
msf6 auxiliary(scanner/snmp/snmp_enum) > exploit
```


LinkedIn : https://www.linkedin.com/in/mohamed-elsayaad

GitHub : https://github.com/0xDos



LinkedIn : https://www.linkedin.com/in/mohamed-elsayaad

GitHub : https://github.com/0xDos

Security Levels

SNMP offers 3 different security levels:

- **noAuthNoPriv**
- **AuthNoPriv**
- **AuthPriv**

Auth stands for **Authentication** and Priv for **Privacy** (encryption).

- noAuthNoPriv = *no authentication and no encryption.*
- AuthNoPriv = *authentication but no encryption.*
- AuthPriv = *authentication AND encryption.*

SNMPv1 and SNMPv2 **only support noAuthNoPriv** since they don't offer any authentication or encryption. SNMPv3 supports *any* of the three security levels. When you decide to use noAuthNoPriv for SNMPv3 then the username will **replace the community-string**.

The community-string for SNMPv1 and SNMPv2 is send in clear-text. SNMPv3 is far more secure because it doesn't send the user passwords in clear-text but uses MD5 or SHA1 hash-based authentication, encryption is done using DES, 3DES or AES.

content of MIB can be accessed & viewed through MIB Browser such as Oputils or Solarwinds IP network browser.
http:\\10.1.1.1\lservice.mib

Microsoft install with snmp service the following MIBs

- DHCP.MIB monitor network traffic between dhcp client and server
- HOSTMIB.MIB monitor and manage host resources
- LNMIB2.MIB object types for services
- WINS.MIB https://msdn.microsoft.com/en-us/library/windows/desktop/aa379157(v=vs.85).aspx

https://support.managed.com/kb/a764/how-to-install-snmp-and-configure-the-community-string-for-windows.aspx

http://www.oidview.com/mibs/311/md-311-1.html

SoftPerfect Network Scanner

https://support.managed.com/kb/a764/how-to-install-snmp-and-configure-the- community-string-for-windows.aspx

Snmpenum tool

LinkedIn : https://www.linkedin.com/in/mohamed-elsayaad

GitHub : https://github.com/0xDos