Scanner SNMP Auxiliary Modules a11y.text Scanner SNMP Auxiliary Modules snmp_enum a11y.text snmp_enum The snmp_enum module performs detailed enumeration of a host or range of hosts via SNMP similar to the standalone tools snmpenum and snmpcheck. msf > use auxiliary/scanner/snmp/snmp_enum

msf auxiliary(snmp_enum) > show options

Module options:

Name	Current Setting	Required	Description
COMMUNITY	public	yes	SNMP Community String
RETRIES	1	yes	SNMP Retries
RHOSTS		yes	The target address range or CIDR identifier
RPORT	161	yes	The target port
THREADS	1	yes	The number of concurrent threads
TIMEOUT	1	yes	SNMP Timeout
VERSION	1	yes	SNMP Version Although you can pass a range of hosts to this module, the output will become quite cluttered and confusing so it is best to simply do one host at a time. msf auxiliary(snmp_enum) > set RHOSTS 192.168.1.2

RHOSTS => 192.168.1.2

msf auxiliary(snmp_enum) > run

[*] System information

Hostname : Netgear-GSM7224

Description : GSM7224 L2 Managed Gigabit Switch

Contact : dookie

Location : Basement

Uptime snmp : 56 days, 00:36:28.00

Uptime system : -

System date : -

[*] Network information

IP forwarding enabled : no

Default TTL : 64

TCP segments received : 20782

TCP segments sent : 9973

TCP segments retrans. : 9973

Input datagrams : 4052407

Delivered datagrams : 1155615

Output datagrams : 18261

[*] Network interfaces

Interface [up] Unit: 1 Slot: 0 Port: 1 Gigabit - Level

Id : 1

Mac address : 00:0f:b5:fc:bd:24

Type : ethernet-csmacd

Speed : 1000 Mbps

Mtu : 1500

In octets : 3716564861

Out octets : 675201778

...snip...

[*] Routing information

Destination	Next hop	Mask	Metric
0.0.0.0	5.1.168.192	0.0.0.0	1
1.0.0.127	1.0.0.127	255.255.255.255	0

[*] TCP connections and listening ports

Local address	Local port	Remote address	Remote port	State
0.0.0.0	23	0.0.0.0	0	listen
0.0.0.0	80	0.0.0.0	0	listen
0.0.0.0	4242	0.0.0.0	0	listen
1.0.0.127	2222	0.0.0.0	0	listen

[*] Listening UDP ports

Local address	Local port
0.0.0.0	0
0.0.0.0	161
0.0.0.0	514

[*] Scanned 1 of 1 hosts (100% complete)

[*] Auxiliary module execution completed

msf auxiliary(snmp_enum) > snmp_enumshares a11y.text snmp_enumshares The snmp_enumshares module is a simple scanner that will query a range of hosts via SNMP to determine any available shares. msf > use auxiliary/scanner/snmp/snmp_enumshares

msf auxiliary(snmp_enumshares) > show options

Module options:

Name	Current Setting	Required	Description
COMMUNITY	public	yes	SNMP Community String
RETRIES	1	yes	SNMP Retries
RHOSTS		yes	The target address range or CIDR identifier
RPORT	161	yes	The target port
THREADS	1	yes	The number of concurrent threads
TIMEOUT	1	yes	SNMP Timeout
VERSION	1	yes	SNMP Version >1/2c> We configure the module by setting our RHOSTS range and THREADS value and let it run. msf auxiliary(snmp_enumshares) > set RHOSTS 192.168.1.200-210

RHOSTS => 192.168.1.200-210

msf auxiliary(snmp_enumshares) > set THREADS 11

THREADS => 11

msf auxiliary(snmp_enumshares) > run

[+] 192.168.1.201

shared_docs - (C:\Documents and Settings\Administrator\Desktop\shared_docs)

[*] Scanned 02 of 11 hosts (018% complete)

[*] Scanned 03 of 11 hosts (027% complete)

[*] Scanned 05 of 11 hosts (045% complete)

[*] Scanned 07 of 11 hosts (063% complete)

[*] Scanned 09 of 11 hosts (081% complete)

[*] Scanned 11 of 11 hosts (100% complete)

[*] Auxiliary module execution completed

msf auxiliary(snmp_enumshares) > snmp_enumusers a11y.text snmp_enumusers The snmp_enumusers module queries a range of hosts via SNMP and gathers a list of usernames on the remote system. msf > use auxiliary/scanner/snmp/snmp_enumusers

msf auxiliary(snmp_enumusers) > show options

Module options:

Name	Current Setting	Required	Description
COMMUNITY	public	yes	SNMP Community String
RETRIES	1	yes	SNMP Retries
RHOSTS		yes	The target address range or CIDR identifier
RPORT	161	yes	The target port
THREADS	1	yes	The number of concurrent threads
TIMEOUT	1	yes	SNMP Timeout
VERSION	1	yes	SNMP Version >1/2c> As with most auxiliary modules, we set our RHOSTS and THREADS value and launch it. msf auxiliary(snmp_enumusers) > set RHOSTS

192.168.1.200-211

RHOSTS => 192.168.1.200-211

msf auxiliary(snmp_enumusers) > set THREADS 11

THREADS => 11

msf auxiliary(snmp_enumusers) > run

[+] 192.168.1.201 Found Users: ASPNET, Administrator, Guest, HelpAssistant,

SUPPORT_388945a0, victim

[*] Scanned 02 of 12 hosts (016% complete)

[*] Scanned 05 of 12 hosts (041% complete)

[*] Scanned 06 of 12 hosts (050% complete)

[*] Scanned 07 of 12 hosts (058% complete)

[*] Scanned 08 of 12 hosts (066% complete)

[*] Scanned 09 of 12 hosts (075% complete)

[*] Scanned 11 of 12 hosts (091% complete)

[*] Scanned 12 of 12 hosts (100% complete)

[*] Auxiliary module execution completed

msf auxiliary(snmp_enumusers) > snmp_login a11y.text snmp_login The snmp_login scanner is a module that scans a range of IP addresses to determine the community string for SNMP-enabled devices. msf > use auxiliary/scanner/snmp/snmp_login

msf auxiliary(snmp_login) > show options

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

Name	Current Setting	Required	Description

BLANK_PASSWORDS false no Try blank passwords for all users

BRUTEFORCE_SPEED 5 yes How fast to bruteforce, from 0 to 5

DB_ALL_CREDS false no Try each user/password couple stored in the current database

DB_ALL_PASS false no Add all passwords in the current database to the list

DB_ALL_USERS false no Add all users in the current database to the list

PASSWORD no The password to test

PASS_FILE /usr/share/metasploit-framework/data/wordlists/snmp_default_pass.txt no File containing communities, one per line

RHOSTS yes The target address range or CIDR identifier

RPORT 161 yes The target port

STOP_ON_SUCCESS false yes Stop guessing when a credential works for a host

THREADS 1 yes The number of concurrent threads

USER_AS_PASS false no Try the username as the password for all users

VERBOSE true yes Whether to print output for all attempts

VERSION 1 yes The SNMP version to scan (Accepted: 1, 2c, all) We set our RHOSTS and THREADS values while using the default wordlist

and let the scanner run. msf auxiliary(snmp_login) > set RHOSTS 192.168.1.0/24

RHOSTS => 192.168.1.0/24

msf auxiliary(snmp_login) > set THREADS 254

THREADS => 254

msf auxiliary(snmp_login) > run

[+] SNMP: 192.168.1.2 community string: 'public' info: 'GSM7224 L2 Managed Gigabit Switch'

[+] SNMP: 192.168.1.199 community string: 'public' info: 'HP ETHERNET MULTI-ENVIRONMENT'

[+] SNMP: 192.168.1.2 community string: 'private' info: 'GSM7224 L2 Managed Gigabit Switch'

[+] SNMP: 192.168.1.199 community string: 'private' info: 'HP ETHERNET MULTI-ENVIRONMENT'

[*] Validating scan results from 2 hosts...

[*] Host 192.168.1.199 provides READ-WRITE access with community 'internal'

[*] Host 192.168.1.199 provides READ-WRITE access with community 'private'

[*] Host 192.168.1.199 provides READ-WRITE access with community 'public'

[*] Host 192.168.1.2 provides READ-WRITE access with community 'private'

[*] Host 192.168.1.2 provides READ-ONLY access with community 'public'

[*] Scanned 256 of 256 hosts (100% complete)

[*] Auxiliary module execution completed

msf auxiliary(snmp_login) > Our quick SNMP sweep found both the default public and private community strings of two devices on our network. This module can also be a useful tool for network administrators to identify attached devices that are insecurely configured. Next Scanner SSH Auxiliary Modules Prev Scanner SMTP Auxiliary Modules