Ethical Hacking and Countermeasures
Svmap Cheat Sheet

EC-Council
Building A Culture Of Security

C|EH
Certified Ethical Hacker

Svmap
Source: https://github.com

Svmap is an Open Source scanner that can iden fy sip devices and PBX servers on a network. Svmap contains a list of methods which can be used to specify the scanning method, such as INVITE, REGISTER, etc.

1. Svmap Op ons
2. Svmap Methods
3. Svmap Commands
4. Svmap Commands to Specify Range of IP Address

1.Svmap Options

Syntax
svmap.py [options] host1 host2 hostrange

Options	
--version	Displays program version number and exit
-h, --help	Display help message and exit
-v, --verbose	To increase verbosity
-q, --quiet	Quiet mode
-s NAME, --save=NAME	Save the session
--resume=NAME	Resume a previous scan
--randomscan	Scan random IP addresses
-i scan1, --input=scan1	Scan IPs which were found in a previous scan. Pass the session name as the argument
-p PORT, --port=PORT	Use this DNS server
-P PORT, --localport=PORT	Specify the source port for our packets
-x IP, --externalip=IP	Specify the IP address to use as an external IP address
-b BINDINGIP --bindingip=BINDINGIP	Binds to the specified IP address
-t SELECTTIME, --timeout=SELECTTIME	Timeout for the select() func on
-c, --enablecompact	To enable compact mode. Makes packets smaller but possibly less compa ble
-m METHOD, --method=METHOD	Specify the request method - by default this is OPTIONS.
-d, --debug	To print the received SIP messages
-R, --reportback	Send the author an excep on traceback
--randomize	Randomize scanning instead of scanning consecu ve IP addresses
--srv	Scan the SRV records for SIP on the des na on domain name
--fromname=FROMNAME	Specify a name for the from header
--fingerprint, --fp	To enable fingerprin ng
--first=FIRST	Send the first given number of messages only

Data Source	Description
-e EXTENSION, --extension=EXTENSION	Specify an extension - by default this is not set
-I scan1, --inputtext=scan1	Scan a group of IP addresses found in a last scan
-A, --autogetip	Obtains the current IP address automa cally

2. Svmap Methods

Method	Description
INVITE	Use to invite a client to a session
ACK	Confirma on of client receiving the final response to INVITE request
BYE	Terminates the session
CANCEL	Deletes any pending request
OPTIONS	This method lists the capabili es of the server(op ons)
REGISTER	The listed address is registered in the To header field with SIP server by this method
PRACK	Provides provisional acknowledgement
SUBSCRIBE	This method subscribes for an Event of no fica on from the no fier
NOTIFY	This method will no fy the subscriber about new event
PUBLISH	This method is used to publish an event to the server.
INFO	Sends mid-session informa on
REFER	Used for asking recipient to issue SIP request
MESSAGE	Used for sending instant message using SIP
UPDATE	Used to modify the state of the session

3. Svmap Commands

Command	Description
./svmap <IP address/Subnet mask> -v	Scan a subnet with verbose mode
./svmap <IP address/Subnet mask> -p1024-2080 -c	Scan a subnet running compact mode on port range 1024-2080
./svmap -s scan1 <IP address/Subnet mask>	Scan a subnet and save the results to a session named "scan1"
./svmap -i scan1 -m INVITE	Scan a list of previously scanned hosts and make use of the INVITE method

4. Svmap Commands to Specify Range of IP Address

Command	Description
./svmap <IP address/Subnet mask>	Using CIDR nota on
./svmap <target name>	Name instead of an IP address
./svmap <target name/Subnet mask>	Using CIDR nota on with the name
./svmap <target ip1>-<target ip2>	Using "-"
./svmap <target ip>-20	Using shorter method
./svmap 1.1.*.*	Using wildcard
./svmap <target ip>-20 1.1.2.* <target website>/24	Combines the above methods
./svmap --randomscan	Randomly scans the internet ranges
./svmap --randomize <target website>/24	Randomly scans the internet ranges using name of the website