Безопасность в PJSIP

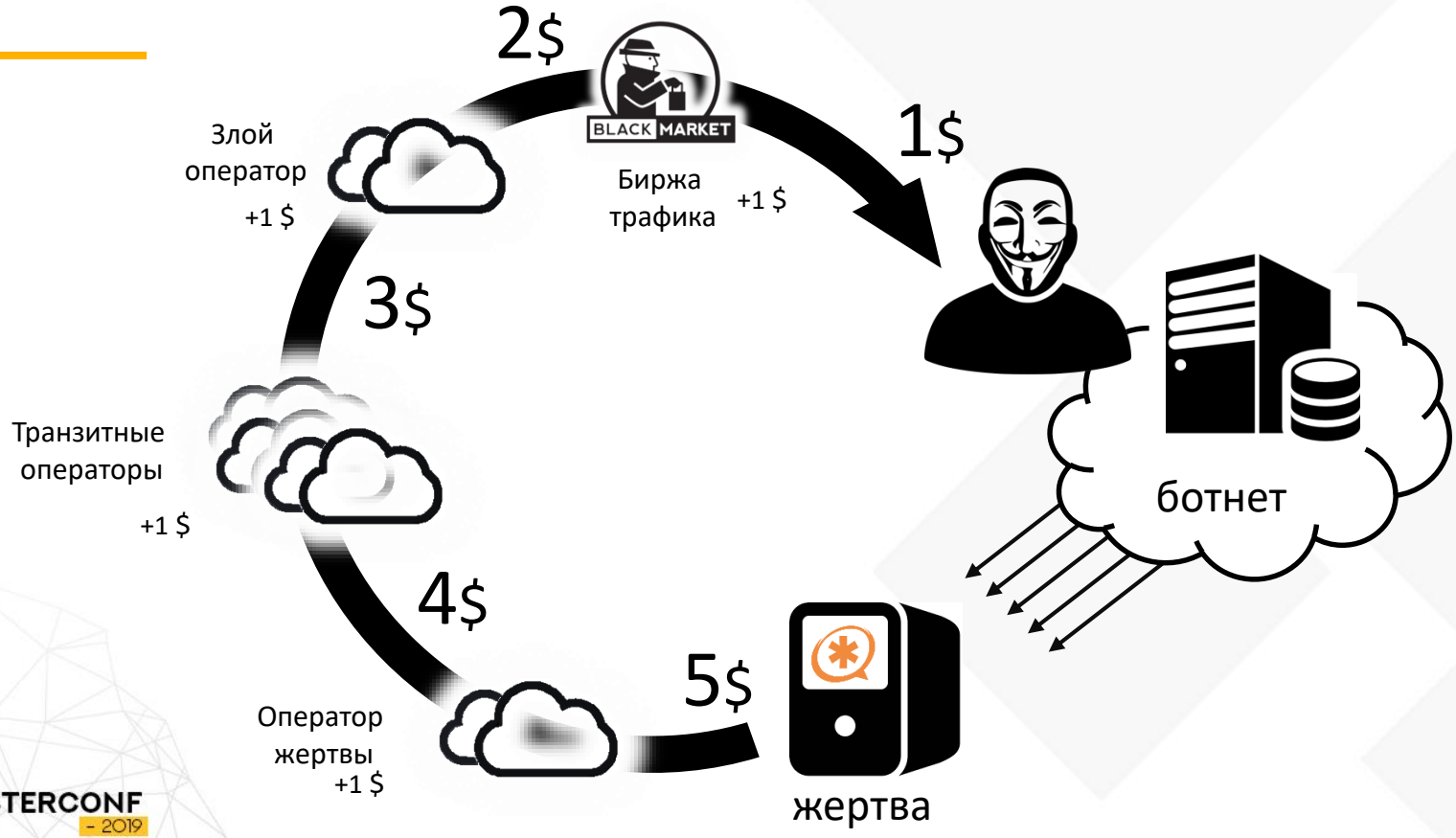
ASTERCONF - 2019

01

Почему это важно?

Он подскажет почему это важно

Как работает «слив трафика»

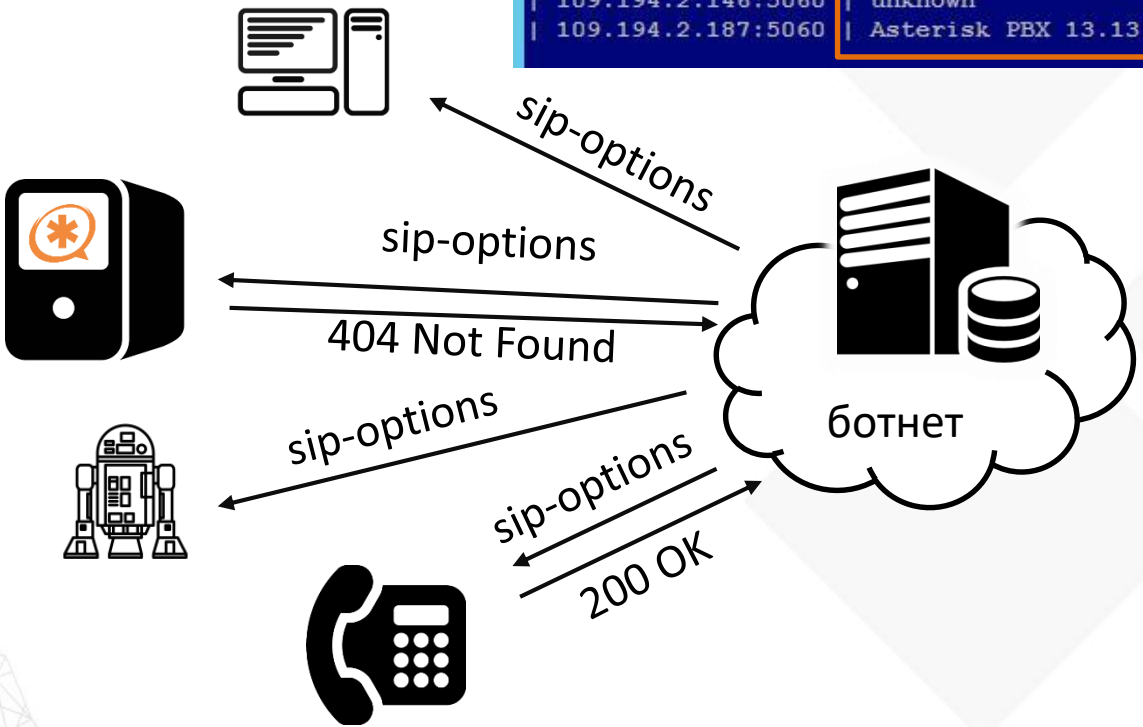


Методы и этапы атаки на SIP

- Просканировать сеть и выбрать жертву
- Определить SIP-логин
- Подобрать пароль к логину по словарю
  - Если есть гостевые звонки – перебирать диал-план для выхода на международку

Сканирование

```
[root@ITProfitPBX14 sipvicious]# ./svmap.py 109.194.2.0/24
WARNING:DrinkOrSip:could not bind to 0.0.0.0:5060 - some process might a
| SIP Device          | User Agent                        | Fingerprint |
-------------------------------------------------------------------------
| 109.194.2.48:5060   | ZXHN H218N/V1.02.01_ERS           | disabled    |
| 109.194.2.154:5060  | ZXHN H218N/V1.02.01_ERS           | disabled    |
| 109.194.2.173:5060  | Yealink SIP-T21P_E2 52.80.14.3    | disabled    |
| 109.194.2.146:5060  | unknown                           | disabled    |
| 109.194.2.187:5060  | Asterisk PBX 13.13.1              | disabled    |
```



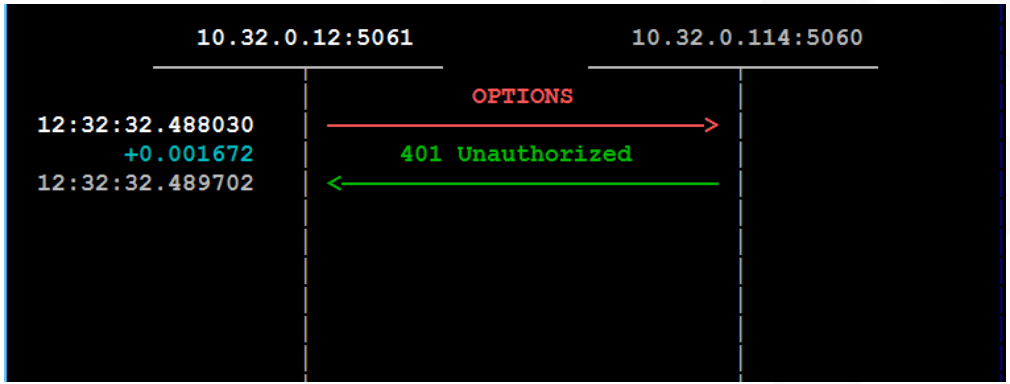
Реакция Asterisk на сканирование

CHAN_SIP

Реакция Asterisk на сканирование

PJSIP

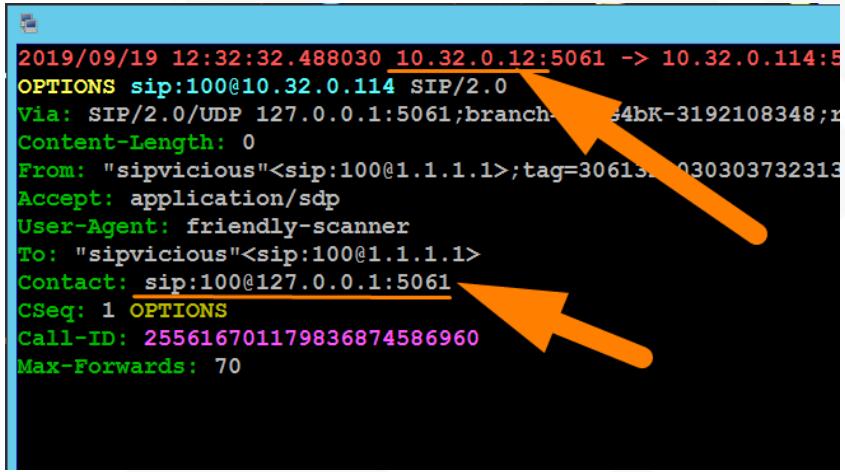
```
DESKTOP-H5QF8K9*CLI>
DESKTOP-H5QF8K9*CLI>
DESKTOP-H5QF8K9*CLI>
[Sep 19 10:41:58] NOTICE[773]: res_pjsip/pjsip_distributor.c:649 log_failed_request: Request 'OPTIONS' from '"sipvicious" <sip:100
@1.1.1.1>' failed for '10.32.0.12:5061' (callid: 111761247791945187889787O) - No matching endpoint found
DESKTOP-H5QF8K9*CLI>
```



Как защититься

PJSIP позволяет задать ACL глобально для всего SIP-трафика

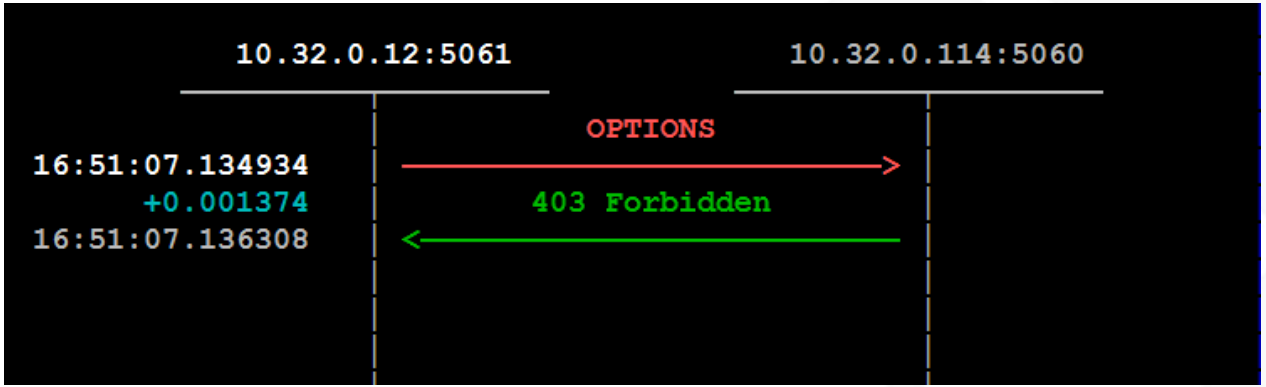
```
    /etc/asterisk/pjsip.conf      Modified


[acl]
type=acl
contact_deny=0.0.0.0/0.0.0.0
contact_permit=10.15.0.0
deny=0.0.0.0/0.0.0.0
permit=10.15.0.0/24, !10.15.0.11/32
```



Реакция Asterisk на сканирование

PJSIP+ACL

```
[Sep 19 12:12:54] NOTICE[1051]: acl.c:715 ast_apply_acl: SIP Contact ACL: Rejecting '127.0.0.1' due to a fai
lure to pass ACL 'local'
[Sep 19 12:12:54] WARNING[1051]: res_pjsip_acl.c:173 apply_contact_acl: Incoming SIP message from 127.0.0.1:
0 did not pass ACL test
DESKTOP-H5QF8K9*CLI> _
```

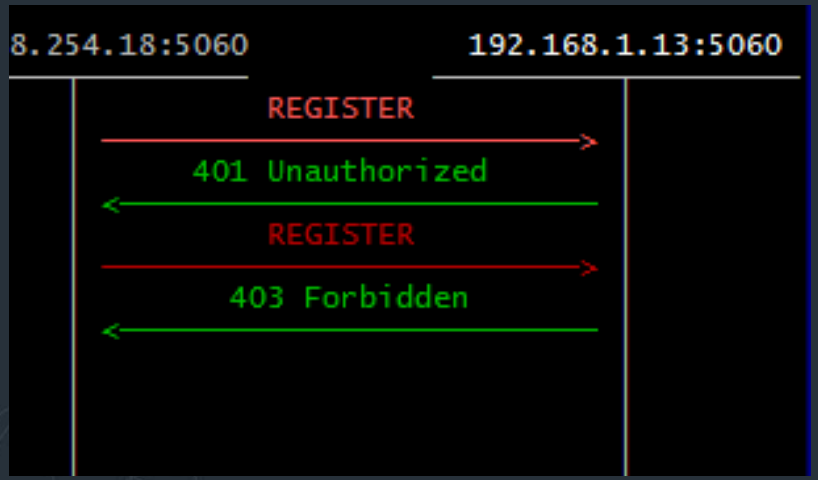


Защита от перебора логинов и паролей

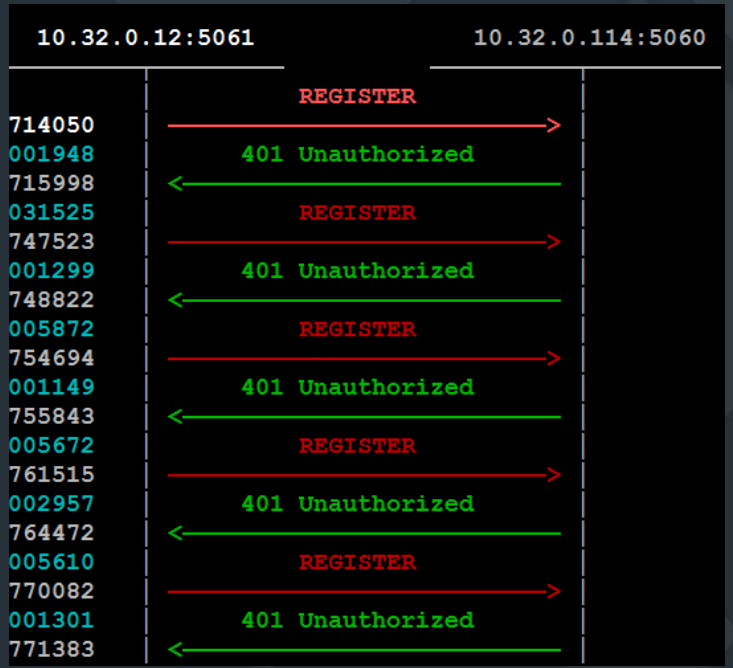
CHAN_SIP	PJSIP
AlwaysAuthReject=yes **AllowGuests=no**	Уже все сделано за нас, но можно все испортить **[anonymous]** **type=endpoint** **context=anonymous**

Разница в обработке неудачной авторизации

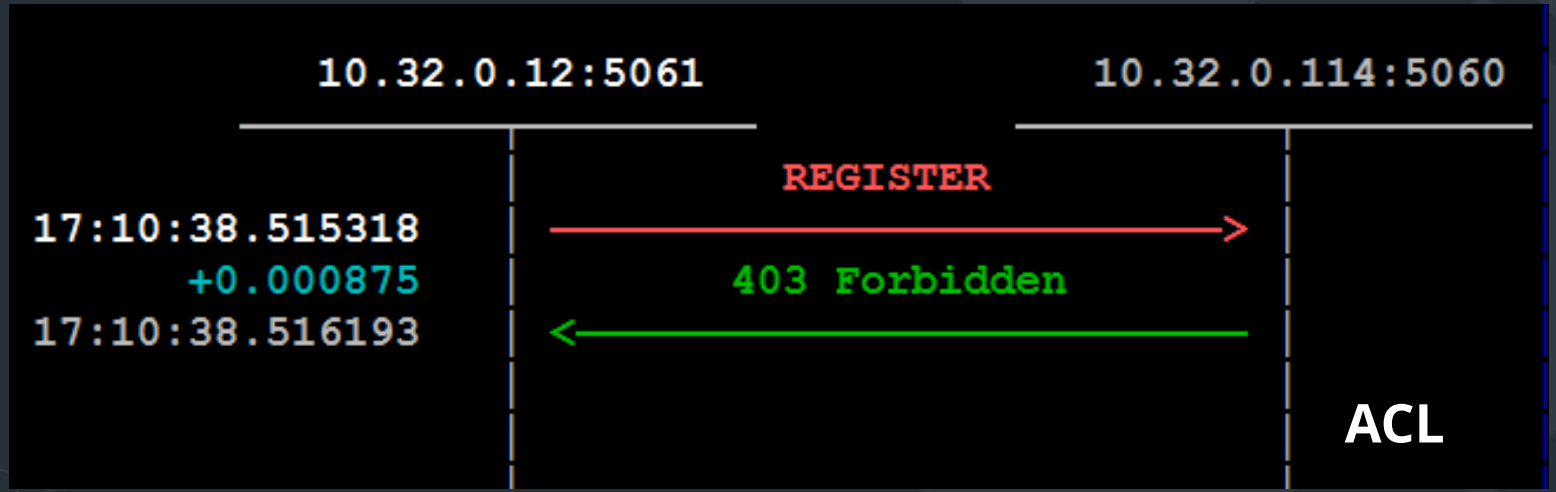
CHAN_SIP



PJSIP



Реакция PJSIP на перебор по словарю при включенном ACL



Что можно еще покрутить в PJSIP

[global]
unidentified_request_period=5
unidentified_request_count=5
user_agent=YuryLozzza
default_from_user=YuryLozzza
default_realm=YuryLozzza

[anonymous]
type=endpoint
sdp_session=YuryLozzza

```
SIP/2.0 200 OK
Via: SIP/2.0/UDP 10.32.0.201;rport=5060;received=10.32.0.201;bra
Call-ID: 9edd7e8e-87ad32a7-8e365b18@10.32.0.201
From: "1001" <sip:1001@10.32.0.12>;tag=F5FCE69A-1366F3D3
To: <sip:*43@10.32.0.12;user=phone>;tag=ee00b1fd-cd32-45bc-a93f-
CSeq: 2 INVITE
Server: DartVader
Contact: <sip:10.32.0.12:5060>
Allow: OPTIONS, SUBSCRIBE, NOTIFY, PUBLISH, INVITE, ACK, BYE, CA
Supported: 100rel, timer, replaces, norefersub
P-Asserted-Identity: "Echo Test" <sip:*43@10.32.0.12;user=phone>
Content-Type: application/sdp
Content-Length:   281

v=0
o=- 1456677698 1456677700 IN IP4 10.32.0.12
s=Asterisk
c=IN IP4 10.32.0.12
t=0 0
m=audio 16888 RTP/AVP 9 0 8 127
a=rtpmap:9 G722/8000
a=rtpmap:0 PCMU/8000
a=rtpmap:8 PCMA/8000
```

СПАСИБО,
Ваши вопросы?

IT-АУТСОРСИНГ
ИТ ПРОФИТ

Николай Шакин

Mob: +7 9206020084
E-mail: post@itprofit32.ru
Telegram (запрещённая на территории РФ организация) @ShakinNN

ASTERCONF
- 2019