Безопасность Asterisk

уязвимости в распространенных дистрибутивах

варианты атак

open-source инструменты для защиты

конфигурационные файлы сервера телефонии

Уязвимости

1.Пароли по умолчанию
-amp109/amp11/eLaStIx.2oo7

2.Слабые пароли
-mysql , sip , apache,webmin...

3.Старые библиотеки/инструменты
-mysql/phpmyadmin/sshd

4.Права на файлы
-/var/run
-/var/lib/
-/etc/asterisk/
-/var/lib/php/session/
-/etc/

5.Физический доступ
-открытые консоли физической машины
-консоль mysql , оставленная залогинненой
-консоль астериска в отдельном терминале (обзор safe_asterisk)

конфигурационные файлы 1-2

passwd

-лишние пользователи /sbin/nologin

my.cnf

-bind-address
-skip-networking
-table_cache/sort_buffer_size/query_cache_size

asterisk.conf

-execincludes/nocolor/runuser/rungroup/[files]
-safe_asterisk CONSOLE=no/PRIORITY=10

httpd.conf

-User/Group
-AllowOverride
-prefork.c/worker.c - оптимизируем работу

amportal.conf

-CHECKREFERER - защита от кросдоменных запросов
-FOPDISABLE/FOPRUN

sip.conf

-alwaysauthreject
-allowguest
-allow/deny

конфигурационные файлы 2-2

.htaccess

-<FilesMatch></FilesMatch>
-require valid-user
-Order allow,deny

crontab

-отдельный crontab для системного пользователя
-защита от переполнения директорий (@daily /usr/bin/find /var/lib/asterisk/backups/daily/* -mtime +3 -exec rm {} \;)

logrotate

-/var/log/httpd/
-/var/log/asterisk/

extensions.conf

-права на скрипты для exec включений
-fstab : /dev/tmp0   /tmp   ext2   loop,noexec,nosuid,rw 0 0
-include'ы - безопасность диаплана

fail2ban

filter.d/asterisk.conf

```
[Definition]
failregex = NOTICE.* .*: Registration from '.*' failed for '<HOST>' - Wrong password
            NOTICE.* .*: Registration from '.*' failed for '<HOST>' - No matching peer found
            NOTICE.* .*: Registration from '.*' failed for '<HOST>' - Username/auth name mismatch
            NOTICE.* .*: Registration from '.*' failed for '<HOST>' - Device does not match ACL
            NOTICE.* <HOST> failed to authenticate as '.*'$
            NOTICE.* .*: No registration for peer '.*' \(from <HOST>\)
            NOTICE.* .*: Host <HOST> failed MD5 authentication for '.*' (.*)
            NOTICE.* .*: Failed to authenticate user .*@<HOST>.*
```

jail.conf

```
[asterisk-iptables]
enabled  = true
filter   = asterisk
action   = iptables[name=ASTERISK, port=5060, protocol=udp]
           sendmail-whois[name=ASTERISK, dest=ss@line24.ru]
logpath  = /var/log/asterisk/full
maxretry = 10
bantime = 86400
findtime  = 60
ignoreip = 127.0.0.1 172.31.0.0/24 10.10.0.0/24 192.168.0.0/24
```

Варианты Атак

Брутфорс по ssh - прямой подбор по словарю (70% на 25 юзеров)

-SSH Brute Forcer
-SSHatter
-SSHBrute

DDOS на апач

-mod_security
-mod_limit
-iptables

SQL injection

-ошибки в коде (php/html)

подбор по SIP

-(allowguest,insecure,allow/deny,alwaysauthreject)
-ошибки в диаплане (IVR,callback)

Телефонное хулиганство

-телефонный/факсимильный спам

open-source инструменты для защиты

iptables и ipfw

-фаерволы до сервера телефонии и на (внешние и внутрение сети)

Fail2ban - анализ логов

-ssh фильтры

-фильтр логов астериска и нотификация о банах

rkhunter

-анализ системы на руткиты и прочие неприятности

-работа в кроне или демонах

Утилиты генерации паролей

-системные утилиты или пишем сами (pwgen и подобные)

-echo `< /dev/urandom tr -dc _A-Z-a-z-0-9 | head -c8`

sipvicious

- утилиты для проверки устойчивости sip конфигов

Sipp

-нагрузочное тестирование

sipvicious

svmap

./svmap 192.168.3.1/24

| SIP Device | User Agent |

 | 192.168.3.112:5060 | Asterisk PBX |

svwar

./svwar.py 192.168.3.112

| Extension | Authentication |

111	reqauth
222	reqauth
333	noauth

svcrack

./svcrack.py 192.168.3.112 -u 100

 | Extension | Password |

 | 222| 222|

./svcrack.py 192.168.3.112 -u 111 -d dictionary.txt

| Extension | Password |

 | 111| qwerty |

sipp

uac

./sipp -sn uac 127.0.0.1:5061 -s 999 -d 60000 -l 10 -r 2

```
[asterisk02]
type=friend
context=testing
host=127.0.0.1
port=5061
user=sipp
canreinvite=no
disallow=all
allow=ulaw

[testing]
exten => 999,1,Answer()
exten => 999,n,MusicOnHold(default,30)
```

uas

./sipp -sn uas -p 5061 -mp 10001 -f 3 -rtp_echo

Оконечное оборудование

IP-телефоны

-Cisco,Linksys,Skypemate,Audiocodes,Addpac

Платы потока

-Digium, Sangoma

- Также , как присоединение шлюзы E1-SIP

софт-фоны и Skype

-Linqphone, X-lite/eyebeam, Zoiper, Ekiga

-Skype