Asterisk® Security Threats and Best Practices

Tips for Protecting your PBX from Attack

Agenda

- Typical Threats Overview
  - Call stealing
  - Compromising the server
- How to Protect the PBX
  - SSH communication
  - Separating data & voice
  - HTTP communication
  - Passwords
  - etc.

Typical Threats

- Stealing of calls via:
  - telephony
  - VoIP trunks
  - SIP
  - IAX2
- Compromising the Linux server via SSH/HTTP

Stealing Calls via Telephony or VoIP Trunks

- Disable the option of uncontrolled trunk-to-trunk calls
- DISA (Direct Inward System Access)
  - use long passwords

Stealing Calls via SIP / IAX2: Stage 1

- Find PBX IP address and port number
- Suggested tools:
  - nmap (http://nmap.org/)
  - svmap (http://code.google.com/p/sipvicious)

```
$ ./svmap.py 192.168.0.1/24
| SIP Device          | User Agent          | Fingerprint                    |
-------------------------------------------------------------------------
| 192.168.0.61:5060   | Asterisk PBX 1.6.2.| Asterisk / Linksys/PAP2T-3.1.|
| 192.168.0.185:5060 | Yealink SIP-T28P 2.| AVM or Speedport               |
| 192.168.0.124:5060 | Grandstream GXP2000| Grandstream phone              |
| 192.168.2.4:5060    | Yealink SIP-T26P 6.| AVM or Speedport               |
| 192.168.0.184:5060 | Yealink SIP-T22P 7.| AVM or Speedport               |
| 192.168.0.134:5060 | YATE/2.2.0          | AVM or Speedport               |
```

Stealing Calls via SIP / IAX2: Stage 2

- Find a PBX extension
  - svwar (http://code.google.com/p/sipvicious)
  - Attacker tries to differentiate between existing/non-existent extensions
  - SIP response to a REGISTER/INVITE/OPTION request analysis could be used for it
  - Asterisk could be configured to send an identical 401 or 407 response regardless of request rejection reason
  - Ref. “alwaysauthreject” parameter in the sip.conf

Stealing Calls via SIP / IAX2: Stage 3

- Find the password
  - svcrak (http://code.google.com/p/sipvicious)
  - When PBX is attacked there are many warning messages in the Asterisk log:

```
[Jun.. ] NOTICE[30940] chan_sip.c: Registration from '"308" failed
   for '192.168.0.192' - Wrong password
[Jun.. ] NOTICE[30940] chan_sip.c: Registration from '"308" failed
   for '192.168.0.192' - Wrong password
[Jun.. ] NOTICE[30940] chan_sip.c: Registration from '"308" failed
   for '192.168.0.192' - Wrong password
[Jun.. ] NOTICE[30940] chan_sip.c: Registration from '"308" failed
   for '192.168.0.192' - Wrong password
```

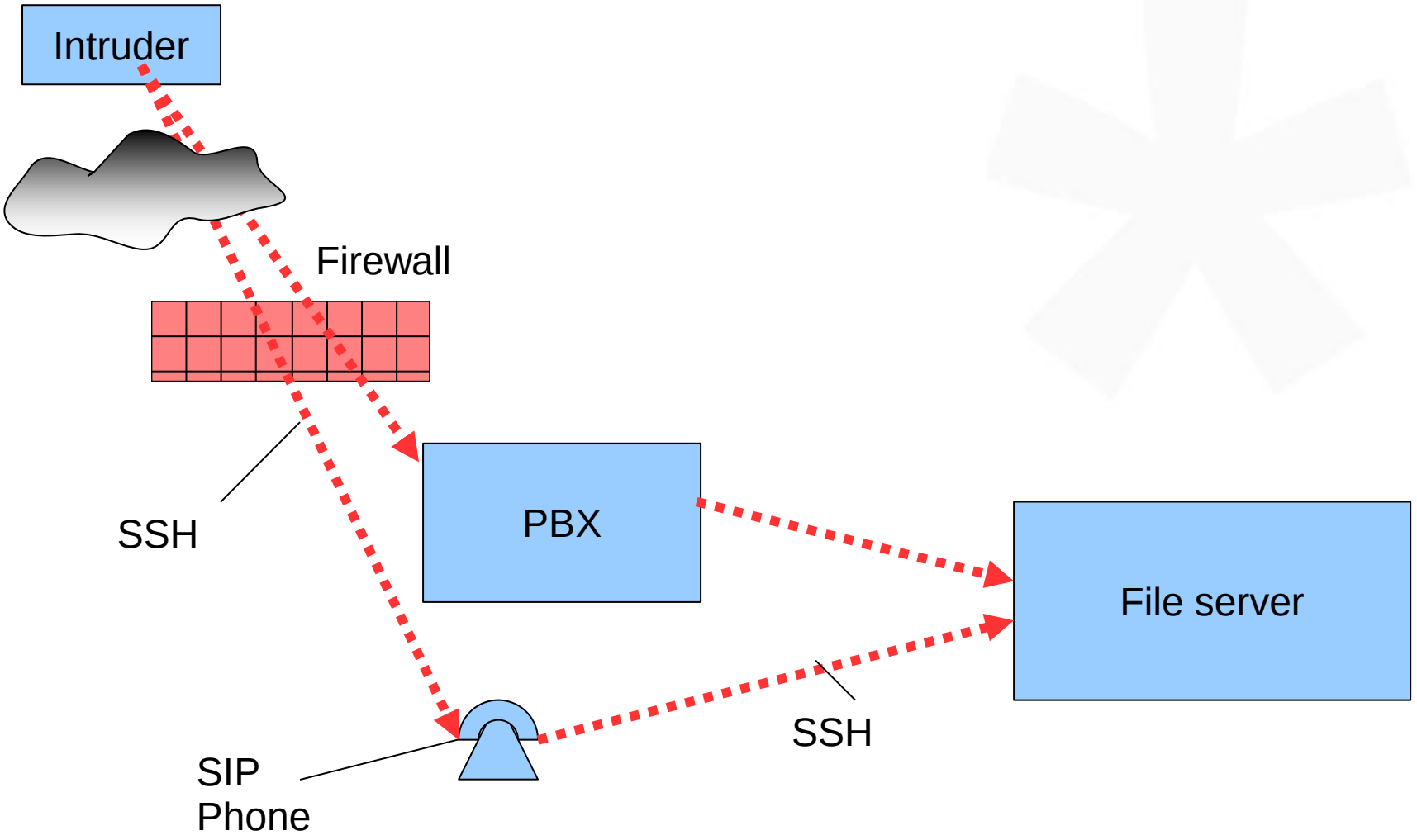
Stealing Calls via SIP / IAX2: Stage 4

- The PBX has been conquered
- A malicious user has registered an extension and makes calls for free
- In many cases this will be discovered only when the next telephone bill is received

Compromising the Linux Server

- An Asterisk server is a regular Linux machine that can also be compromised
- Malware (viruses, trojan horses etc) may infiltrate via different Linux networking services such as SSH or HTTP

Attack on Linux Server



How to Protect the PBX

- There are countless methods to “harden” a server against attack
- Each method has its price
- 99% of attacks are “simple” attacks, and there are simple means to prevent them

SSH Communication

- Use public/private key authentication instead of password authentication
- Create a user account and disable log in as 'root':
  - `/etc/ssh/sshd_config`
  - `PermitRootLogin no`
- or
  - `PermitRootLogin without-password`
- Then it will be possible to connect to the PBX as a non-'root' user, and then become a “super-user”:
  - `ssh john@my-pbx-ip -p 4245`
  - `su -`

SSH Communication cont'd

- Restrict the source IP addresses that are allowed to access the server
- Don't use the default SSH port (22/tcp)
  a. arrange port forwarding on the NAT router or
  b. change the listening port in the PBX SSH server configuration:
     - `/etc/ssh/sshd_config`
     - `#Port 22`
     - `Port 4245`

Separating Data & VoIP Networks

- Some customers with higher security requirements separate the VoIP network from the data network
- Dedicated cabling network not required; VLAN technology may be used instead
- Helps prevent company data servers from direct access from potentially vulnerable VoIP devices

HTTP Communication

- Don't expose the PBX Web server to the Internet
- Use SSH tunneling for the PBX Web-based management interface
- Windows users can create SSH tunnels very easily using PuTTY

Passwords

- Don't use the default passwords
- Don't use simple passwords

Secure VoIP Communication

- Don't expose SIP and IAX2 ports unless absolutely necessary
- Use IP restriction for internal VoIP extensions
  - Allows use of weak passwords or no passwords for the internal extensions
- Use strong passwords for remote extensions

LAN-only Registration for Extension

Intrusion Detection Options

- It is possible to use a network intrusion detection system
- Fail2Ban (http://www.fail2ban.org)
  - Scans the log files and updates firewall rules to reject the IP address
- Snort (http://www.snort.org)
  - Powerful network intrusion prevention and detection system (IDS/IPS)

Fail2Ban Features

- Log-based brute force blocker
- Runs as daemon
  - unlike cron-based tools, no delay before taking action
- can use iptables or TCP Wrappers (/etc/hosts.deny)
- can handle more than one service: sshd, apache, SIP traffic etc.
- can send e-mail notifications
- can ban IPs either for a limited amount of time or permanently

Snort Features

- Sniffer mode
- Logger mode
- NIDS mode
- Can capture and analyze traffic for several servers
- Intrusion prevention mode
- Extremely mature system; actively developed since 1998

Summary

- Types of threats
  - Call stealing
  - Intrusion
- Best practices
  - Protecting the PBX
  - Detecting attacks quickly

THANK YOU

www.xorcom.com