



Hervey Allen

Network Startup Resource Center

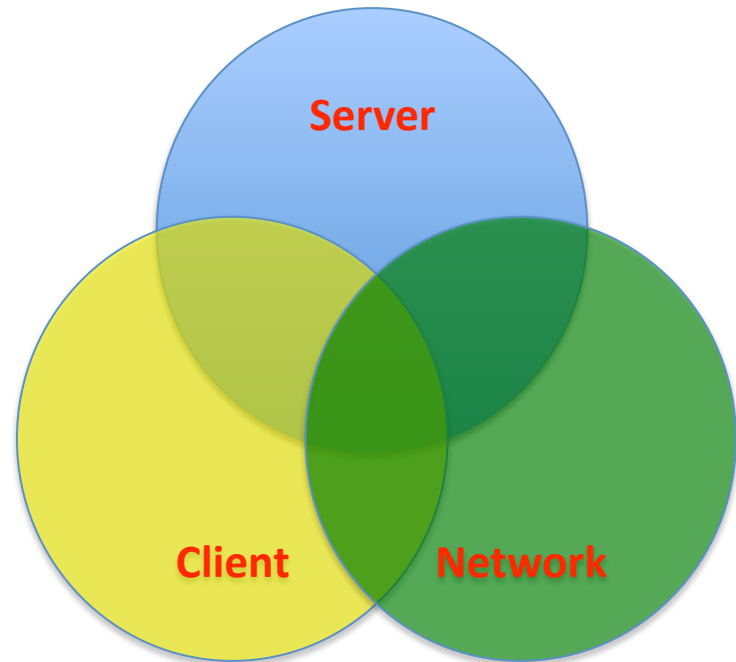
PacNOG 6: Nadi, Fiji

Security Overview

Security: A Massive Topic

Security Viewpoints

- Server
- Client
- Network
- Securing each overlaps the other →



So, what do we talk about...?

Security: Network

Network Security

- Keeping intruders out
- Resisting Denial of Service attacks
- Maintaining reliable service (see above)
- Assisting with your organization's reputation
 - You have compromised clients on your network.
Don't let this cause problems for others.
- Authenticate data sources as they enter your network.

Security: Server

Server-Side Security

- Keeping intruders out
- Resisting Denial of Service attacks
- Maintaining data on your server confidential
- Verifying the integrity of data on your server
- Authenticate user access to your server and services

Security: Client

Client-Side Security

- Keeping intruders out
- Maintaining the confidentiality of your data
- Maintaining the integrity of your data
- Authenticating access to your resources

Security Overlap

- As you can see the overlap is pervasive.
- What's the reality as a system or network administrator? What can and should you do?

Lots!

- Protect your clients and assume they are compromised.
 - But, keep on training them about security.

Steps to Take: Network

- Engineer your network with security in mind. What's behind routers and switches?
- Collect data needed to know what is happening on your network and to be able to investigate further.
- Back up network configurations.
- Use ingress/egress rules on routers.
- Enable flows (as possible)
- Prepare for DDoS attacks.

Steps to Take: Server

- Back up your data!
- Turn off unnecessary services
- Monitor your server and services
- Enforce security policies (passwords, backups)
- Learn how to enable firewalls if necessary, and block access to services as needed
- Create a disaster contingency plan
- Scan for security weaknesses

Steps to Take: Client

- Don't run unnecessary services (surprise!)
- Use anti-viral and anti-malware software
- Back up your data!
- Think about how to recover in case of disaster
- Use encryption (ssh, pgp, https/ssl)
- Be aware of physical security

Client-Server Security Steps

Maintaining Confidentiality

- Correct user and file permissions.
- Strong passwords.
- Trusting your users.
- Use of good cryptographic methods
- Be aware of physical security

Client-Server Security Steps

Ensuring Integrity

- Backup, backup, backup.
- Revision control.
- Intrusion detection systems (IDS).
 - This is hard
- Log and use log-watching software

Client-Server Security Steps

Authenticating Access

- Trusted users.
- Strong passwords.
- Public/Private keys.
- Maintain accounts properly.
- Correct user/group/file permissions.
- Scan and watch for SUID and SGID.
- Restrict root/administrator access

Client-Server Security Steps

Other Bits and Pieces

- Update and patch installed software
- Run only the services you use
- Use secure passwords or keys
- Consider quotas if necessary
- Use tcpwrappers, iptables (firewall software)
- Scan and watch for SUID and SGID.
- Restrict root/administrator access to your computer as well as to services

Security: Types of Attacks

Attacks on Your Server(s)

- Buffer overflow
- Passive attacks, such as sniffers, traffic analysis (*ngrep*, *dsniff*).
- Active attacks: - e.g. Connection hijacking, IP source spoofing, exploitation of weaknesses in IP stack or applications, scans like *nmap*.
- Denial of Service attacks: e.g. synflood.
- “Man in the middle” attacks: Hijacking services.
- Network scans for holes (ssh, MySQL injection, script attacks on http, etc.)

Security: Simplify

To see what is running use:

```
lsof -i
```

```
netstat -an -f inet
```

```
ps auxww | more
```

```
sockstat -4
```

what each and every item is. Simplify, simplify, simplify – remove any and all services you are not using.

Security: Cryptographic Offerings

Provide (almost) Only Secure Access to Services you are Running

- POP/IMAP with SSL only.
- Use TLS-Enabled SMTP.
- Remove Telnet replace with SSH.
- Remove FTP replace with SCP or SFTP.
- Anonymous FTP is OK, but be careful if you allow user uploads.
- Require HTTPS (HTTP over SSL) for sensitive information.

Security: Stay Up-to-Date

- Be sure that you track all the services you are running.
- If you run Bind (DNS), Apache (Web), Exim/Postfix/Sendmail/Qmail (MTA) then subscribe to the appropriate security mailing lists for each.
- Subscribe to generic security mailing lists that pertain to your OS or Linux version.
- Subscribe to general security lists.

Security-Related Mailing Lists

General security mailing lists

- BugTraq: <http://www.securityfocus.com/>
- CERT: <http://www.cert.org/>
- Rootshell: <http://www.rootshell.com/>

For Apache, Bind, Exim and SSH

- <http://www.apache.org/>
- <http://www.isc.org/> (*Bind*)
- <http://www.exim.org/>
- <http://www.openssh.org/>

Server Security a Few More Steps

- Logging
- Monitoring
- Backing Up
- Testing

Logging: we will cover this separately

Monitoring: We've already covered this 😊

Server Security: Backup

Pretty hard to stress this more. If your security is compromised what will you do without a backup?

A few basic items to consider are:

- What needs to be backed up.
- How often do you need to backup?
- Where will your backup media be in case of disaster (fire, flood, earthquake, theft)?
- What happens in case of total loss?
- What tools will you use? Tar, Arkeia, cpio, Amanda, Bacula, rsync, dd, other?

Server Security: Backup Details

- What do you want to backup?
- What do you need to backup?
 - User data
 - System configuration files
 - Operating system files
- How often must you backup?
- What is the backup rotation? Daily, weekly, monthly, semi-annually, yearly?
- What type of backup media are you going to use?
- Will you use the same media and software for each piece of your backup process?
- Where will you backup your data?
- Where will you keep copies of your backups?
- Have you tested your backups? I.E. have you tried a restore?
- What will you do if you lose your server? Do you have a place to restore your data in this case?

Server Security: Backup Tools

Arkeia: commercial product:

<http://www.arkeia.com/>

<http://nsrc/security/#backups>

dd: convert and copy a file.

man dd

dd if=/dev/sda of=/dev/fd0/bootsector.bin bs=512 count=1

Backs up a boot sector to a floppy

dd if=/dev/fd0/bootsector.bin of=/dev/sda bs=512 count=1

Recovers from floppy to sda. Be *very careful doing this!*

Server Security: Backup Tools

cpio: copy files to and from archives:

cpitool: <http://www.nickb.org/utils/>

man cpio

dump: ext2/ext3 filesystem backup.

man dump

rsync: remote copy.

man rsync.

tar: read

man tar (impressive!)

Server Security: Backup Examples

You can use ssh and tar together to quickly backup parts of your server. For instance, to backup all home directories to another server as a single image:

```
root@machine1# tar xzvf - /home/ | \  
ssh machine2 "cat > machine1-homes.tgz"
```

Or, you can use rsync over ssh if you wish to keep directories synchronized between two locations:

```
rsync -ave ssh remote:/home/docs .
```


Server Security: Backup Examples

- Later today we'll discuss ssh and the use of ssh keys to connect to a remote machine without passwords and use encryption.
- If in `/etc/cron.daily/sync-web` you do the following:

```
rsync -ae ssh /var/www/html/ backup.machine:/var/www/html/
```

- This recursively copies your root web documents to a backup machine using rsync via ssh.
- Use “`--delete`” to remove remote copies of files deleted locally.

Security: Backup with rsync

Real World Example

```
/usr/bin/rsync -avzpRl -e "/usr/bin/ssh -i /var/www/backups/  
afnog.org.freebsd/afnog-back-rsync-key -l root@afnog.org"  
root@afnog.org:'/etc /usr/local/libexec/autoreply /usr/  
local/mailman /usr/local/www /var/lib /root' /var/www/  
backups/afnog.org.freebsd/daily
```

What is this doing?

Server Security: Testing

- Once you have in place what you believe to be a secure server try connecting to it from an external machine. Verify that your security model works as expected. Try circumventing your own rules.
- Run a security scanner against your server (your network as well?). A nice tool to run against your server is Nessus. You can find this product here:
<http://www.nessus.org/>
- Or, you might try *nmap*:
<http://www.insecure.org/nmap/>

Security: Use of nmap

Network MAPper

Network Security

General Ideas

- Set up proper ingress and egress filters on your routers.
- Be sure to *not* route known bogus addresses.
- Use ssh on your routers, switches and anything you log in to remotely (or can log in on remotely)
- If you have budget build in extra capacity to deal with active attacks
- Back up your configurations! (RANCID)

Network Security Cont.

General Ideas cont:

- Don't share your network topology with everyone. This can be used to find known weaknesses
- Prepare for DDoS attacks. You are very likely to experience one at some point.
- Remember physical security of your equipment
- Know where your equipment is (Documentation).
- Patch software versions when necessary.

References

CERT (Coordinated Emergency Response Team)

<http://www.cert.org/> and <http://www.us-cert.gov/cas/index.html>

SANS Computer Security and Mailing Lists

<http://www.sans.org/> and <http://www.sans.org/newsletters/risk/>

Nice List of Security Resources for Linux/UNIX

<http://www.yolinux.com/TUTORIALS/LinuxSecurityTools.html>

Nessus Security Auditing Package

<http://nessus.org/>

nmap: Network exploration tool and security scanner

<http://www.insecure.org/nmap/>

O'Reilly Books

<http://www.oreilly.com/>

Security Documents from nsrc.org

<http://nsrc.org/security/>