Tiger Server Security

Charles Edge
Partner, Three18

Threats

Viruses

Malware

Hackers

Man in the Middle Attacks

Data Loss

Data Theft

Password Cracks

Identity Theft

Hijacked Systems

Legal Issues Due to Hijacked Systems

Script Kiddies

Denial of Service

And the List goes on and on and on and on...

For Starters

Basic Server Security

- Regularly review your logs
- Keep software up-to-date (system and non-system and)
- Know the products (built-in services and third party)
- Know your users and how they manage their data
- Know thy network

Know What's Running on Your Server

- Activity Monitor
- top
- Use Network Utility or nmap to port scan yourself
- Review Launchd (lingon)
- Check Cron

Client Security

- Users should have complex passwords that are changed at regular intervals
- Users should have access to the minimum permissions required
- Protect clients at the network edge who have trust relationships other hosts
- Keep client software up-to-date
- Push MCX (policies) to client systems

Root

- The root account is enabled by default in Tiger Server
- This can be disabled in NetInfo Manager
- Limit the use of su and sudo
- Try to limit su usage specifically

Built-in GUI Security

- Configure Firewall using Server Admin
- Configure SACLs in Server Admin
- Good Share Point Management
- FileVault
- Login Items and StartupItems
- Require Password to wake Server

Gateway Security

- Keep the open ports to the server to a minimum
- Use stateful packet inspection
- Use a VPN to minimize incoming ports
- Deny outgoing ports on the firewall unless otherwise defined (especially if you have Windows systems on the network)
- Use a proxy on your network

From the Command Line

IPFW

- Firewall is ipfw
- ipfw list
- /etc/ipfilter/ipfw.conf
- /var/log/ipfw.log
- ipfilter
- divert
- Review your logs

CLI Security Utilities

- rpcinfo
- Hosts_options

Files to think/worry about

- Keep trusted copies of
  - `/bin`
  - `/usr/sbin`
  - `/usr/bin`
  - `/sbin`
- Keep backups of all essential conf files in (most are stored in `/etc`
- `If you think one of these files has been compromised you can compare date stamps and byte counts for a quick`

I think I have a rootkit?!?!

- netstat -a displays the ports listening for traffic.
- RootKit Hunter
- Intrusion Detection - Tripwire

Viruses??? But I have a Mac...

- There are more viruses for the Mac than ever
- Macs and Windows exchange files more than ever
- The days of not running virus scans on Mac servers are over
- Scans should be performed regularly on servers

Services

AFP

- Use Kerberos Authentication
- Disable Guest Access
- Disable the option to allow administrator to Masquerade as any user
- Enable Logging and log everything
- Disconnect all clients when inactive
- Limit the maximum number of connections
- Disable guest access to each Share Point

Samba

- Windows sharing is done using Samba
- /etc/smb.conf is the smb configuration file
- If you are using smb as an nt4 pdc then make sure to use a backup
- Do not allow guest shares

NFS

- When possible do not use NFS as it relies on IP addresses for security
- If you must use NFS, use Workgroup Manager to limit the permissions on NFS volumes
  - Map Root user to nobody
  - Map All users to nobody
  - Read-only

DHCP

- Use seperate subnets for Windows computers when possible
- Limit number of IP addresses in each DHCP pool
- Use Static Maps when possible in order to trace which clients may have issues
- DHCP should not be run on most servers unless you are using static maps

DNS

- Use a separate DNS server for external domain information for the world
- Keep DNS internal especially in Open Directory setups
- Increase the logging levels
- /Library/Logs/named.log is the default location when

Email

- Only enable required mail protocols
- Limit IMAP connections to mitigate DoS vulnerability
- Scan mail before it comes into the server
- Scan mail again when it comes in using SpamAssassin and ClamAV
- Implement Quotas
- Log as much as you can
- Use Kerberos Authentication when possible

Web Security Basics

- There's a lot of things that can be done to secure the web server
- Web servers that are running the default sites (including uncustomized error codes) are vulnerable to Google hacking
- Keep number of modules limited
- Don't enable any options not required
- Realm Third party packages such as awstats, phpmysql, etc.

iChat Server

- Use SSL to protect the messages sent over iChat Server
- iChat Server is Jabber
- /etc/jabber/jabber.xml allows administrators to use an IP filter for the jabber service, limit ability of users to create their own accounts and use settings to limit DoS possibilities
- For more security use a service like FireChat to encrypt your communications

The Extras

Network Intrusion Detection Systems

- NIDS servers can scan network traffic and automatically update the firewall for traffic meeting signatures that are known attack sequences
- SNORT is becoming an open source industry standard
- SNORT can be used in conjunction with Letterstick and Guardian

BACKUPBACKUPBACKUPBACKUP

- Backup is not going to help you in the event that confidential data is leaked onto the Internet
- Backup is going to help in contingency planning and disaster recover
- Backups should be protected as well as live data
- backups should be layered for maximum protection

Penetration Testing

- OS Fingerprinting
- Look up the security vulnerabilities for each port you can get in using
- Attempt to attack

Links for more information

- http://www.securityfocus.com
- http://macsecurity.org
- http://securemac.com
- http://www.macenterprise.org
- http://www.afp548.com

Questions

- Charles Edge
  - cedge@three18.com
  - http://www.three18.com