Defenses: Firewalls, Intrusion Detection, etc.

Robert H. Sloan

Security Intrusion

A security event, or a combination of multiple security events, that constitutes a security incident in which an intruder gains, or attempts to gain, access to a system (or system resource) without having authorization to do so.

—RFC 2828, Internet Security Glossary, (May 2000)

Configuration management: patch!

- Solid majority of attacks involve known, generally fixed, bugs in software of 1 of 3 vendors: Microsoft, Adobe, Apple (QuickTime).
- Patch *on* Patch Tuesday!
- Also, make sure default passwords get changed.

Perimeter defense

- Protect against misconfigured or under-protected systems
- Implement organization-wide policy
- Redundant protection—defense in depth
  - Some very simple packet filtering with organization's edge-most router
  - Proxy servers
  - Firewalls

Proxy servers

- Make requests to Internet servers on behalf of internal clients
- Provide 2 benefits:
  - Enhance network performance
  - Mask identity of requestor
- Most medium-large organizations have as security device; public ones on web as anonymity service

Filter: Firewalls

- **Firewall** is a perimeter defense: electronic fence at the outskirts of an organization's network
- Most widely sold form of protection
- Prevents (some or all) incoming network communications. Can also filter outgoing
- May be at any of Internet (packet), transport (TCP), or application layer.

Firewalls (cont)

- Network services (e.g., file sharing, remote login, web serving) lives at fixed address of IP + port number that clients use to connect
- Organization decides which services not to offer, and filters out requests for those at the gateway firewall
- Interior hosts thus protected against foreign intrusions

Software vs. Hardware firewalls

- Money vs. bandwidth tradeoff
- All of us in this room can use software firewall on our home network (unless major web server)
- University needs hardware firewall
- Related but distinct issue: personal vs. network firewall

Organization vs. host

- Organization will almost certainly have (at least one) hardware-based firewall.
  Dedicated computer with special-purpose minimal OS (NOT traditional Windows nor Linux nor Mac OS X) whose only job is firewall.
- Host: You and me—In addition.

Packet filtering

- Firewalls inspect packets (normally both incoming and outgoing) to determine whether to let them pass
- Earliest firewalls used only **static packet filtering**: look at each packet individually (e.g., source and destination IP # and port # and transport protocol) to determine whether it should be allowed.

Stateful inspection

- **Stateful** packet inspection keeps track of active connections to determine whether packets should be filtered
  - Necessary to have protocol where surfer sends from random high number port to Web Server at port 80 (standard) and Server replies and sets up connection from some other random high number port

Firewall topology

- Firewall must be located at some point where packets pass. This is for organization *in addition to* individual machines (personal firewall). Common choices:
  - Single gateway (bastion host)
  - Screened subnet (DMZ): Allow more access to subnet with public services e.g., web server, little/zero access to private internal. (Using 1 or 2 software/ hardware firewalls)

Firewall uses set of rules

- Ordered set of rules; first match is applied.
- Form is something like: **Allow** or **Deny** **protocol** (TCP, UDP, ICMP, IP) **from** source address **to** source address
- Unless you are a deep specialist, you don't want to be writing your own rules
- Mine are automatically generated for me by Mac OS X based on my preferences.

Block all incoming connections

Blocks all incoming connections except those required for basic Internet services, such as DHCP, Bonjour, and IPSec.

File Sharing (AFP)	Allow incoming connections
Printer Sharing	Allow incoming connections
Firefox	Allow incoming connections
iStatLocalDaemon	Block incoming connections
Microsoft Word	Allow incoming connections
Safari	Allow incoming connections

+ −

Automatically allow signed software to receive incoming connections

Allows software signed by a valid certificate authority to provide services accessed from the network.

Enable stealth mode

Don't respond to or acknowledge attempts to access this computer from the network by test applications using ICMP, such as Ping.

?

Cancel OK

Actual firewall rules

sloan$ sudo ipfw list

02000 allow ip from any to any via lo*
02010 deny ip from 127.0.0.0/8 to any in
02020 deny ip from any to 127.0.0.0/8 in
02030 deny ip from 224.0.0.0/3 to any in
02040 deny tcp from any to 224.0.0.0/3 in
02050 allow tcp from any to any out
02060 allow tcp from any to any established
02065 allow tcp from any to any frag
02070 allow tcp from any to any dst-port 548 in
02080 allow tcp from any to any dst-port 427 in
02090 allow tcp from any to any dst-port 3689 in
02100 allow tcp from any to any dst-port 631 in
02110 allow tcp from any to any dst-port 515 in
12190 deny log tcp from any to any
65535 allow ip from any to any

What the rules mean

1. Allow computer to talk to itself (loopback)
2. Deny well-known spoofing
3. Allow outbound connections
4. Allow established connections (stateful!)
5. Allow explicitly wanted inbound connections

Why do I need a Firewall?

Jun 25 10:28:11 robert-sloans-powerbook-g4-12 ipfw: 12190 Deny TCP 121.11.91.3:52361 131.193.40.122:25 in via en0
Jun 25 10:28:14 robert-sloans-powerbook-g4-12 ipfw: 12190 Deny TCP 121.11.91.3:52361 131.193.40.122:25 in via en0
Jun 25 10:28:17 robert-sloans-powerbook-g4-12 ipfw: 12190 Deny TCP 121.11.91.3:52361 131.193.40.122:25 in via en0
Jun 25 10:28:21 robert-sloans-powerbook-g4-12 ipfw: 12190 Deny TCP 121.11.91.3:52361 131.193.40.122:25 in via en0
Jun 25 10:28:24 robert-sloans-powerbook-g4-12 ipfw: 12190 Deny TCP 121.11.91.3:52361 131.193.40.122:25 in via en0
Jun 25 10:28:27 robert-sloans-powerbook-g4-12 ipfw: 12190 Deny TCP 121.11.91.3:52361 131.193.40.122:25 in via en0
Jun 25 10:28:33 robert-sloans-powerbook-g4-12 ipfw: 12190 Deny TCP 121.11.91.3:52361 131.193.40.122:25 in via en0
Jun 25 10:28:45 robert-sloans-powerbook-g4-12 ipfw: 12190 Deny TCP 121.11.91.3:52361 131.193.40.122:25 in via en0
Jun 25 10:29:10 robert-sloans-powerbook-g4-12 ipfw: 12190 Deny TCP 121.11.91.3:52361 131.193.40.122:25 in via en0
Jun 25 10:29:11 robert-sloans-powerbook-g4-12 ipfw: 12190 Deny TCP 200.123.173.85:4155 131.193.40.122:25 in via en0
Jun 25 10:29:14 robert-sloans-powerbook-g4-12 ipfw: 12190 Deny TCP 200.123.173.85:4155 131.193.40.122:25 in via en0
Jun 25 10:29:20 robert-sloans-powerbook-g4-12 ipfw: 12190 Deny TCP 200.123.173.85:4155 131.193.40.122:25 in via en0
Jun 25 10:29:32 robert-sloans-powerbook-g4-12 ipfw: 12190 Deny TCP 200.123.173.85:4155 131.193.40.122:25 in via en0
Jun 25 10:29:56 robert-sloans-powerbook-g4-12 ipfw: 12190 Deny TCP 200.123.173.85:4155 131.193.40.122:25 in via en0

Analysis of my logs

- 4 day snippet ending Friday June 29 2007 at 13:26
- 1,323 TCP connections requested
- Most looking for port 25, SMTP—outgoing email. Spam, anyone? Also port 21, FTP (warez anyone?), various high-numbered ports that are probably known Windows vulnerabilities

Firewalls and encryption

- Firewalls work best when they can see all the traffic in the network
- Thus encryption of email, web pages, tends to work *against* firewalls

Firewall limitations

- Do not protect against attacks using allowed services
- Only as good as the configuration
- If they get in people's way, then they will work around them
- Have no effect on DDoS attack against me

Logging and auditing logs

- **Logging** is recording system events and keeping the record for some length of time. Issues:
  - What events to log?
  - How long to keep?
  - Which events should trigger which kind of immediate alert?

Tradeoffs

- Diligent review of logs in real world much more likely with small logs
- Massive overlogging can cause system performance hit
- Usually keep fixed # days or # bytes of log —don't want large number of trivial events overwriting serious incident

Analysis

- First need to determine baseline activity levels (CPU activity, IP traffic, RAM or disk memory consumption, etc.) including typical variance
- Then decide which deviations are significant, and how significant—think about next time skim the log files; send me an email now; beep my pager 24/7?

Securing logs themselves

- Logging is of course among first activities that malware with Superuser access stops —and next it erases the logs
- Solutions can include remote logging on separate machine elsewhere in network that is specially hardened; or printing immediately to printer in addition to computer file

Key audit log weakness

- Requires a knowledgeable human in the loop
- Difficult to impossible for smallish organization; effectively impossible for Small Office/Home Office types.

Intrusion Detection

Intrusion Detection: A security service that monitors and analyzes system events for the purpose of finding, and providing real-time or near real-time warning of, attempts to access system resources in an unauthorized manner.

—RFC 2828, Internet Security Glossary

Why IDS

1. If intrusion detected fast enough, intruder can be ejected before (much) harm
2. Can be a deterrent
3. Teaches white hats what to do to prevent next break-in

Modern trend: Intrusion Detection

- The next step beyond audit logs and firewalls are *Intrusion Detection Systems (IDS)*, sold typically to companies as a box.
  - Look (automated) for anomalous patterns
    - May or may not be attacks
    - Inform Sys Admin staff who can investigate
  - Roughly same high-level technical issues as audit logs.

IDS

- Two broad ways to go:

  1. Look for signatures of attacks to compare to database of attack signatures.
  2. Develop (machine learning) profile of "normal behavior" and "attack behavior"

- Multiple intruder behaviors?
  - Hacker vs. Criminal vs. Insider

Honeypot

- Deliberately insecure part of system that attracts the attention of an intruder long enough for their actions to be recorded.