Some Practical Security

AfNOG 2004 Workshop

Hervey Allen
May 2004

Liberal borrowing from Brian Candler

Main Security Concerns

- Confidentiality
- Keeping our data safe from prying eyes
- Integrity
  - Protecting our data from loss or unauthorised alteration
- Authentication and Authorisation
  - Is this person who they claim to be?
  - Is this person allowed to do this?
- Availability
  - Are our systems working when we need them? (Denial of Service)

Basic steps to securing a server

- Run only the services you plan on using.
- Use only the services that are necessary.
- Stay up-to-date and patch services as needed.
- Use secure passwords and force your users to use them.
- Restrict root access to a minimal set of services.
- Restrict access to services via tcpwrappers if appropriate.
- Restrict access to your box using IP Firewall services (ipfw).
- Log events and understand your logs.
- Install intrusion detection software.
- Back up your server's data!
- Think about physical security.
- Don't forget about your clients.

Some useful web links

The FreeBSD Handbook Security Section

- http://www.freebsd.org/doc/en_US.ISO8859-1/books/handbook/security.html

FreeBSD Website "intrusion detection" Software

- http://www.freebsd.org/cgi/ports.cgi?query=intrusion+detection&stype=all

FreeBSD Security Notifications Mailing List

- http://lists.freebsd.org/mailman/listinfo/freebsd-security-notifications

Security Documents from nsrc.org

- http://nsrc.org/security/ and http://nsrc.org/freebsd-tips.html

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/

Security implications of connecting to the Internet

- The Internet lets you connect to millions of hosts
  - but they can also connect to you!
- Many points of access (e.g. telephone, cyber-cafe)
  - even if you can trace an attack to a point on the Internet, the real source may be untraceable
- Your host runs many Internet services
  - many potential points of vulnerability
  - many servers run as "root" !

Network-based attacks

- Passive attacks
  - e.g. packet sniffers, traffic analysis (*dsniff*)
- Active attacks
  - e.g. connection hijacking, IP source spoofing, exploitation of weaknesses in IP stack or applications
- Denial of Service attacks
  - e.g. synflood
- “Man in the middle” attacks
  - Hijacking services
- Attacks against the network itself
  - e.g. smurf

Other common attacks

- Brute-force and Dictionary attacks (password guessing)
- Viruses
- Trojan horses (in the form of emails).
- Humans are often the weakest link
  - "Hi, this is Bob, what's the root password?"

Authentication: Passwords

- Can be guessed
- If too complex, users tend to write them down
- *If sent unencrypted, can be "sniffed" from the network and re-used*

Choosing good passwords

- Combinations of upper and lower-case letters, numbers and symbols
  - 'brute force' attacker has to try many more combinations
- Not in any dictionary, including hackers dictionaries

$40&yc4f
"Money for nothing and your chicks for free"

wsR!vst?
"workshop students aRe not very sleepy today ?"

Authentication: Host name

- Very weak
- DNS is easily attacked (e.g. by loading false information into cache)
- Slight protection by ensuring that reverse and forward DNS matches
  - e.g. Connection received from 84.201.255.1
  - Lookup 84.201.255.1 -> noc.ws.afnog.org
  - Lookup noc.ws.afnog.org -> 84.201.255.1
- This is why many sites won't let you connect unless your forward and reverse matches

Cryptographic methods

- Can provide REALLY SECURE solutions to authentication, privacy and integrity
- Some are hard to implement, many different tools, usually requires special clients, but becoming much more widespread.
- Export and usage restrictions (less of a problem these days)
- Take care to understand where weaknesses lie, like “Man in the Middle”, “entropy with random numbers”, etc.

Simple combinations

- The lock on your front door can be picked
- Two locks are better than one
- The thief is more likely to try somewhere else

IP source address AND password authentication

- You can use "tcp wrappers" (/etc/hosts.allow) to add IP source authentication to any service run from inetd
  - For info and examples: man 5 hosts_access
- The application also typically has password authentication

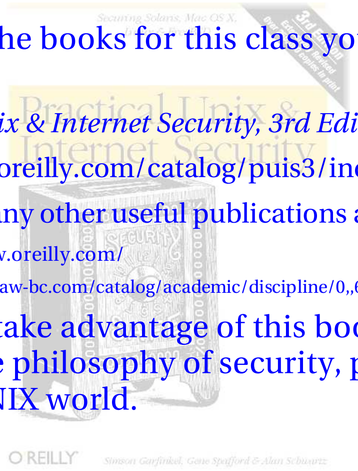
Exercise

- Enable telnet (note: bad idea!)
  - Uncomment telnet ... tcp line in /etc/inetd.conf
  - killall -1 inetd
  - Check other people can telnet to your machine
- Now restrict access to only yourself and your neighbour
  - Add two lines to top of /etc/hosts.allow
  - telnetd : 84.201.31.12, 84.201.31.13 : allow
  - telnetd : ALL : deny
- Get someone on a different row to try to telnet to you. What happens if you telnet to 127.0.0.1 ?

UNDERSTAND what you're doing

- A bad security solution is worse than no security at all
- Know what you're doing
  - Read all the documentation
  - Read sample configurations
  - Build test machines
  - Ask questions
  - Join the announcements mailing list for your O/S and applications
- Test what you've done
  - Try connecting from outside your network
  - Try circumventing your own rules
- For instance: *Windows vs. UNIX.* Securing a box.

Practical UNIX security



As part of the books for this class you've been given:

Practical Unix & Internet Security, 3rd Edition

http://www.oreilly.com/catalog/puis3/index.html

There are many other useful publications at:

- http://www.oreilly.com/
- http://www.aw-bc.com/catalog/academic/discipline/0,,69948,00.html

Be sure to take advantage of this book to learn about the philosophy of security, particularly in the UNIX world.

Summary

- Disable all services which are not needed
- Apply security patches promptly; join the announcement mailing lists
- Good password management
- Combine passwords with IP access controls where possible
- Use cryptographic methods where possible
- Understand what it is that you are doing!