

Security, Part 1

Mark Hendricks and Ron Roeber

September 19, 2002

Preview of Security Topics:

- ! Concepts and Definitions
- ! Policy
- ! Services and Ports
- ! Exploits
- ! Protection

Why are we here?

- ! To learn about security
- ! To justify security to peers
- ! To learn how to manage security

The Nature of Security

- ! Security is a process
- ! Security is never finished
- ! Security is a way of building systems
- ! Security is a state of mind

Know your system

- ! To know how to defend a system, it helps to know how it can be attacked.
- ! You should ask : How can I break in here and fix it.

Why will they pick on me?

- ! Boot it and they will come...
- ! A system with nothing on it is a good place to hide.
- ! Your system can be used to attack other systems.

The Task

"... the rule is not to count on opponents not coming, but to rely on ways of dealing with them; not to count on opponents not attacking, but rely on what they can't attack."

Sun Tsu - The Art of War

Policy

- ! Policy Definition
- ! Implementation
- ! Monitoring and Auditing
- ! Incident Response
- ! Maintenance & Refinement

Policy Requirement Analysis

- ! Identify involved parties, resources and services (apps)
- ! Assess Risks and Analyze Costs
- ! Define Policy
- ! Implement Control
- ! Document Limitations
- ! Test

Implicit Policies

- ! User services should only be accessed by authorized users
- ! Files and resources should only be modified according to the intent of their owners
- ! Public services should be accessible

Fundamental Uncertainty Principle

"You cannot know that your site (computer) is secure."

Jim Dennis, Linux World Expo, 3/1/99

Costs of Compromise

- ! Productivity
- ! Connectivity
- ! Reputation
- ! Liability

Services and Ports

- ! Services are executables that provide functions
- ! Ports are addresses which services are accessed at

Examples of Services

Netbios	POP
Http	NFS
DNS	SSH
SMTP	FTP

- ! Services can be small and provide information about your system environment, or relatively large and provide (serve) remote access and control.
- ! Services generally run on standard ports, for example http on port 80, ssh on port 22, and ntp on port 123.

Services

- ! On Windows 2000
 - " C:\WINNT\system32\etc\services

Ports

- ! Open ports allow access to your system
- ! Open ports can tell others a lot about the functionality of you system

Scanning Ports

- ! Port scanning applications can quickly scan entire networks - pinpointing vulnerable systems by ip address and port
- ! Port scanning applications can also determine OS and thus help exploit weakness in system security
- ! Port scanning applications can also help you identify vulnerabilities and test your system

Closing ports

- ! It is best to close all the ports on your system that you are not using, limiting the possibility of exploits

Exploit Opportunities

- ! File sharing
- ! Clear text passwords, or absence of/or stock passwords
- ! Unapplied security fixes
- ! Published exploits
- ! Unattended computers without passwords
- ! "Dumpster Divers"
- ! Remote access programs without passwords

File sharing exploits

- ! Don't share files and folders if you don't have to...
- ! If you do, use a good password and encrypt it if possible

Good passwords

- ! Words that are not in the dictionary
- ! Combinations of words and numbers
- ! Words longer than eight characters

Bad passwords

- ! Publicly available information about you
- ! Your department or building name
- ! Number sequences like 123

Clear text passwords

- ! Sniffers can listen to a port and watch you enter your username and password
- ! Telnet, ftp and http are open to this type of exploit

Even good passwords

- ! On Windows 95/98/ME
 - " Password system is not robust
 - " Brute force password cracking software can decrypt file shares

Absence of passwords

- ! Without a password, anyone can login and use your stuff
- ! Many programs come with a widely known default password, which needs to be changed

Unapplied security patches

- ! As exploits are exposed, patches are released to secure the software
- ! If you fail to patch you apps, you can get hacked

Unattended Computers

If you leave your computer and you are logged on (or have no password) anyone can use and abuse your computer

Dumpster Divers

- ! A lot can be learned about you from your trash
- ! If you have critical data online, don't throw the name and password in the trash

Remote Access Programs

- ! Programs like *pc-anywhere* need password protection
- ! Hackers regularly look at phone books and try and find numbers close to your number to see if you have a modem online

Firewalls

- ! Firewalls filter network packets
- ! FW's can limit access by port, service, ip address and other methods
- ! Firewalls are another layer of a multi-layer security strategy
- ! FW's can make network security management easier
- ! Firewalls may only limit external network traffic - you still need to protect your computer

Personal Firewalls

- ! 'Protect' single system
- ! Configure to open and close ports to trusted and un-trusted users
- ! Can consume system resources
- ! Software: Black Ice Defender, Zone Alarm, Others
 - " Must be kept up to date like anti-virus software

Viruses and Worms

Viruses and worms can be very benign or very malicious

Virus

- ! Definition: A piece of code or application that gets into your system without your knowledge and runs against your wishes.
- ! Some viruses replicate themselves - this is dangerous because it will quickly use all available memory and bring the system to a halt.
- ! More dangerous is a type of virus capable of transmitting itself across networks and bypassing security systems - usually through email or file attachments.
- ! Viruses usually attack homogeneous systems, where they can use the same method to do the most harm.

Worm

- ! Definition I: Worms are similar to viruses in that they are computer programs that replicate themselves and that often, but not always, contain some functionality that will interfere with the normal use of a computer or a program.
- ! Definition II: Worms exist as separate entities; they do not attach themselves to other files or programs. A worm can spread itself automatically over the network from one computer to the next, taking advantage of file sending and receiving features found on many computers.

General protection

- ! Limit physical and virtual access to computers
- ! Use good passwords
- ! Backup data religiously - this will save you
- ! Keep software updated - especially system, virus protection and security software
- ! Perform intrusion analysis
- ! For servers maintain good logs

Resources: www.ianr.unl.edu/excite/