

Internet Security 101

Vincent LeVeque
vleveque@earthlink.net

Security Basics

- Confidentiality
 - Keep business secrets
 - Protect third party privacy
- Integrity
 - Correct data
 - Confidence in other party's identity

Security Basics

- Availability
 - Data is available
 - As soon as needed
 - In the quality expected

Internet Security Issues

- Lack of reliable identification
 - “Nobody knows you’re a dog”
- Jurisdiction
 - Where are you?
 - Whose laws apply?
- Lack of privacy
- Protocol flaws
- Poorly engineered software

Risks have shifted

- Internet provides perceived (and sometimes actual) anonymity
- Lack of physical presence
- Mass production & distribution of break-in tools
- Low probability / low yield attacks become profitable

Hackers

- Most notorious threat
- Young, fascinated by technology
- Older generation broke phone codes (“phreakers”)
- Less skill now required
 - Easy to use tools
 - “script kiddies”

How Hackers Operate

- Pick target
- Research target systems
- Scan for vulnerabilities
- Exploit vulnerability to get root
- Set up back doors

Hacker Modus Operandi

- Attack for ego gratification
- Attack big-name sites
- Likes technical challenge



Port Scanning

- Checking for unlocked doors
- Can be done over the Internet, or internally
- May indicate possible attack, may not
- Most sites scanned several times/day to several times/week
 - <http://www.enteract.com/~lspitz/alert.log>
- Software used by hackers includes nmap

War Dials

- Call all numbers in a range to find modems
- Open modems for PC Anywhere, etc.
- Backdoor around firewall
- Software easy to use
 - Toneloc
 - THC (“The Hacker’s Choice”)



Modern Trojan Horses

- Stealth programs with malicious intent
- Always a threat, now real
- Real examples:
 - BackOrifice
 - NetBus
 - Maybe 70 more
 - <http://www.commodon.com>
- Creates back doors into your system



More Hacker Tricks

- Social Engineering
- Dumpster diving
- Exploit software flaws
- Exploit weak authentication
- Cover tracks
 - Delete/tamper with audit logs

Hackers are not your biggest threat!

- Internal fraud, theft, embezzlement
- Disgruntled employees
- Temp technical staff
- Untrustworthy system vendors
- Fraudulent or shady commercial enterprises
- Even plaintiff attorneys

So why pick on hackers?

- Seek (and are granted) publicity
- Less careful, less risk averse = more likely caught
- Techniques used by other, more straightforward crooks
 - “social engineering” a favorite of con artists
 - similar techniques to steal credit card numbers, etc.

Industrial Espionage

- Former spy agencies find work post-cold war
- Trade secret theft
- Dumpster diving
- Infiltration with temp employees, student interns, etc.

SPAM: Not the lunch meat

- Mass unsolicited incoming e-mail
 - Take over of **your** mail relay
 - Avoid SPAM
 - permit mail only to/from “real” hosts
 - block known SPAM addresses
 - block sites which permit relaying
 - have your ISP warn sending site e-mail is unsolicited
- <http://spam.abuse.net>



Basics of protection

- PROTECT
 - Don't leave doors unlocked unnecessarily
- DETECT
 - Know your system
 - Know when an attack has taken place
- REACT
 - Recover system, prevent further intrusions
 - prosecute

Auditing is essential

- If you can't secure it, audit it
- Audit it anyway
- How do you know if you have been attacked?
- Audit analysis can reveal possible attack attempts **BEFORE** they have succeeded

Preserving Evidence

- Computer records are “hearsay”
- Collect as part of normal business processes
- Document chain of custody
- Secure from any possible tampering
- Keep at least 3 months, 1 year better

Watch your desktops

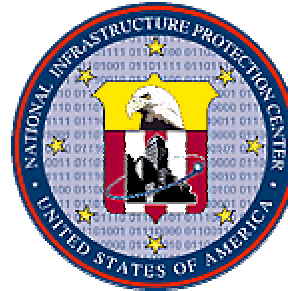
- Weakest link
- Unauthorized software prevalent
- Easy to physically compromise
- Win 95/98 inherently unsecurable

Modern Security Tools

- Intrusion detection
- Desktop inventory
- Encryption
- Strong authentication
- Virtual Private Networks
- Public Key Infrastructure

Info Warfare

- Control of Information
- Use of Information
- Attacking Information resources
- Winn Schwartau, “Information Warfare: Chaos on the Electronic Superhighway”
- President’s Commission on Critical Infrastructure Protection



Not all attacks are war...

- Info Vandalism
- Info Fraud
- Info Graffiti
- Info JoyRides
- Info Revenge
- Info “its spring break and I’m really bored”

Info Vandalism

- Denial of Service attacks
- Can be mitigated, cannot be eliminated
- Recent examples:
 - Ping of Death
 - Land
 - Smurf
 - Teardrop
 - WinNuke

Good Advice

- Get CERT advisories
- Subscribe to bugtraq
- Get rid of trivial passwords
- Get rid of passwords, period
- Be very careful configuring public access
- Know your systems
- Have a good policy and publicize it

Good AS/400 Advice

- Ensure robust application code
- Watch *PUBLIC authority
- NO default passwords
- Minimize TCP/IP services

Follow IBM security recommendations !

Surveillance: Cure? Cause?

- Protects against individual attacks, but also can be an attack against the individual
- Creates ability to monitor individual actions to a previously unheard-of degree
- Internet access subject to monitoring unthinkable for phones or US mail
- “Death of privacy?”