

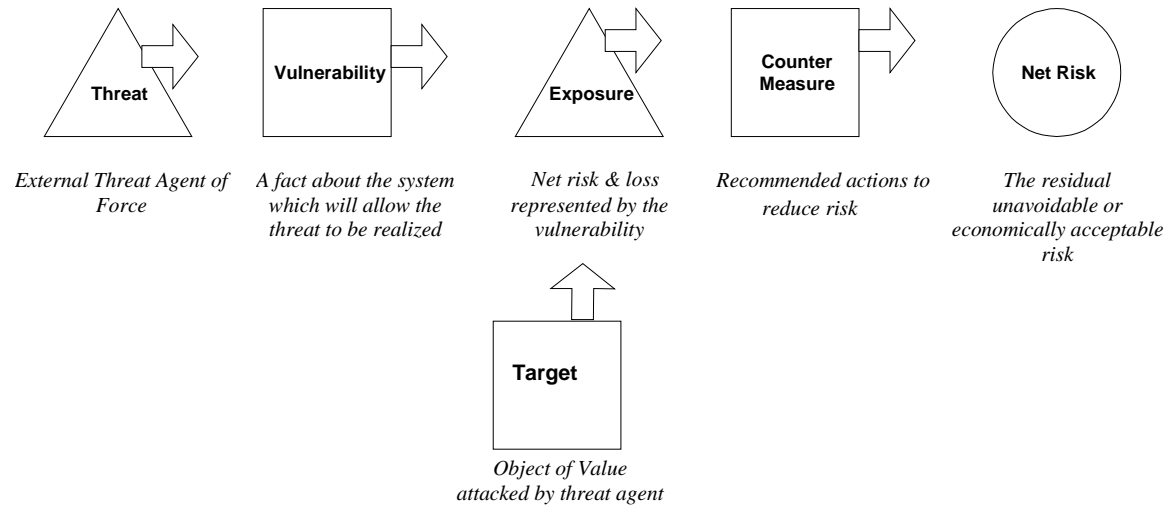
Basic Internet Security

Vincent LeVeque, Senior Security Engineer
Science Applications International Corporation
vleveque@earthlink.net

Real Basic AS/400 Advice

- Change default passwords
- Limit use of TCP/IP Services
- Beware of *PUBLIC
- Limit client/server application access
 - Exit programs
 - Application only access
- Follow IBM recommendations
 - Immediately apply security PTFs!!

Basic Security Threat Model



Basic Security Threat Model

- Threat - Who's out to get you?
- Vulnerability - How can they get you?
- Asset Value - How much damage will they do if they succeed?
- Countermeasures - How can you thwart them?
- Residual Risk - "Stuff Happens"

Threats

- Outsiders
 - Hackers
 - Spies
 - Common Crooks
- Your own employees
 - IT Staff
 - End Users & Management
- Contractors, temps, consultants
- Software vendors and support

Vulnerabilities

- Protocol flaws
- Poorly engineered software
- Configuration Flaws
- Poor administrative practices

How Hackers Operate

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

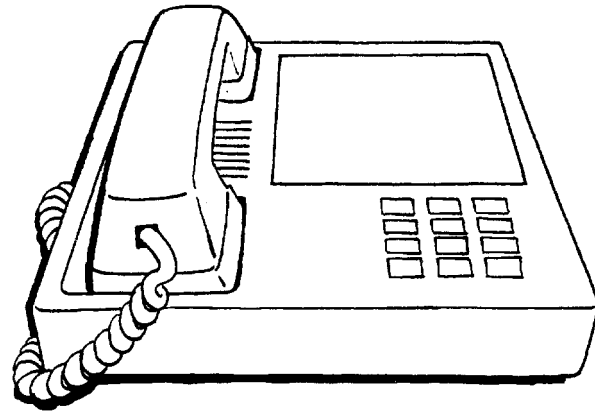


Port Scanning

- 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
- 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”)



Once they find you...

- Try to guess your operating system type and version & other services
 - Tools include queso & nmap
 - For now, these tools consistently mis-identify AS/400 Web servers
 - Look at login banners
- Find vulnerabilities that aren't fixed which will allow entry
- Vulnerability = bad software

How to “get root”

- Find an open service
- Get local access (telnet, etc.), upload exploit programs, and “upgrade” privileges
- Or, run a remote exploit against a target’s service (e.g. ftp, IMAP, etc.) and gain a privileges command shell
- Or find some misconfigured service to take advantage of (e.g. open Windows shares, etc.)

Basic Exploits

- Buffer overflows and underflows
 - Overwrite special memory locations (e.g., CPU instruction pointer) with branch to “shell” program
- Specifications oversights
 - Flaws in system or protocol designs (e.g., SYN flood)
- Flawed interpretation logic
 - Special case of above
 - Not properly validating input conditions
- Race conditions and privilege retention
 - “Time gap” in executing steps of a process so that an unprivileged process can “take over” privileged access rights

AS/400 Exploits?

- Few publicized
- Design and “packaging” minimizes
- Little “hacker” interest
- Some found:
 - Password encryption broken
 - Cleartext password accessible via MI program
 - Lotus Domino exploits?
- Expect more, and expect more publicity for these

More Hacker Tricks

- Social Engineering
- Dumpster diving
- Cover tracks
 - Delete or tamper with logs
 - Upload “fixed” system utilities which do not display hacker tampering
- Expand attack
 - Use compromised system to attack other systems

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

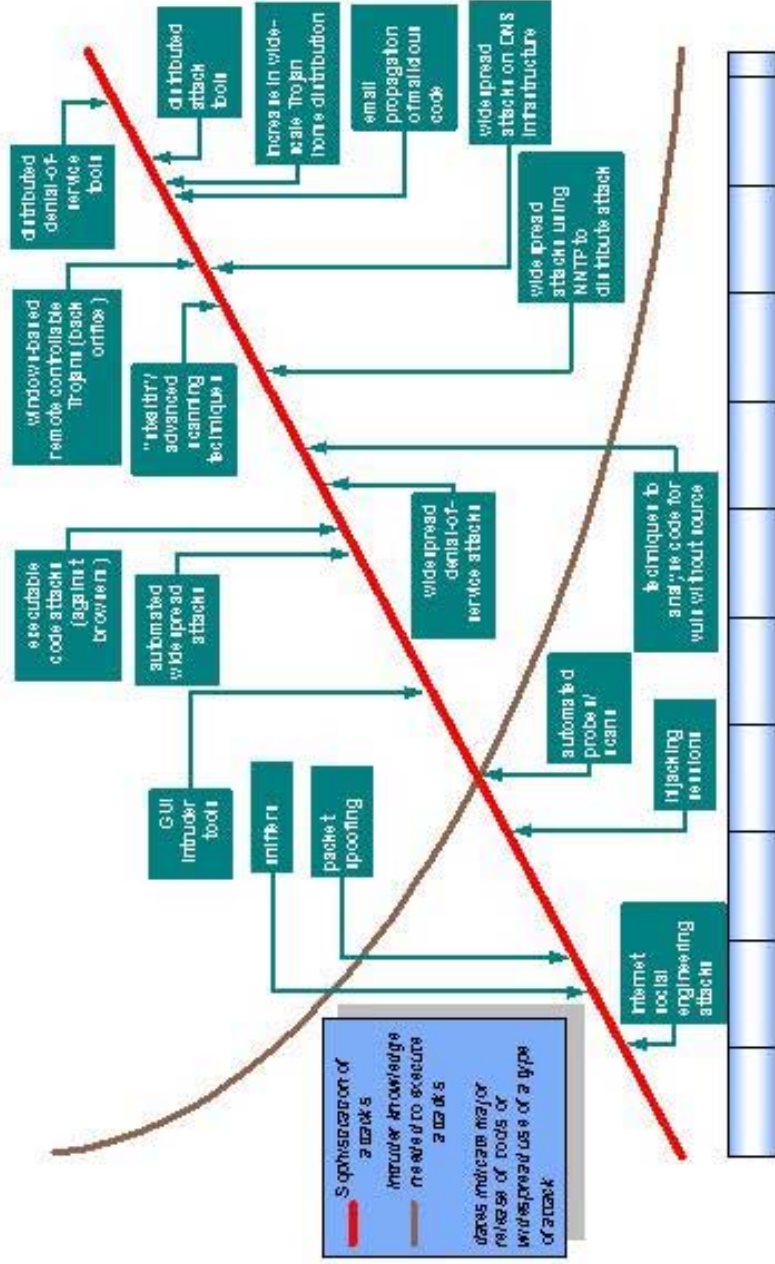


Risks have shifted

- Internet provides perceived (and sometimes actual) anonymity
- Physical presence not required to commit offence
- Mass production & distribution of break-in tools
- Low probability / low yield attacks become profitable
- Mass coordination of attacks from multiple compromised systems



Attack Sophistication vs. Required Intruder Knowledge



Keeping up on risk trends

- Computer Emergency Response Team (CERT)
 - Carnegie Mellon
 - Receives reports from sites under attack
 - Publishes vulnerabilities and current attack trends
 - www.cert.org
- Bugtraq
 - Roots in “hacker” community
 - Full disclosure
 - www.securityfocus.com/forums/bugtraq/faq.html



Recent CERT/CC Experiences (1)

	<u>1997</u>	<u>1998</u>	<u>1999</u>	<u>2000*</u>
Incidents handled	3,285	4,942	9,859	8,836
Vulnerabilities reported	196	262	417	442
Email msgs processed	38,406	31,933	34,612	26,413
CERT Advisories, Vendor Bulletins, and Vul Notes	44	34	20	9
CERT Summaries and Incident Notes	6	15	13	10

*January through June of 2000

Basic Information Valuation

- Management will never spend money on security unless a financial business case can be made!
- What is the value of your systems?
- How do systems and data create value for your business?
- How much damage would an attack do?
- How much should be spent on countermeasures?

Basic Countermeasures

- Design security into the process
- Have the best security your organization needs
- Know your systems
- Know your users
- Audit security events, and regularly review for trends and anomalies
- Know what to do when a security breach happens

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

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

Basic 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

Real Basic AS/400 Advice

- Change default passwords
- Limit use of TCP/IP Services
- Beware of *PUBLIC
- Limit client/server application access
 - Exit programs
 - Application only access
- Follow IBM recommendations
 - Immediately apply security PTFs!!