

Network Vulnerability

Open Source Security Tools for Information Technology Professionals

School of Professional Studies (SPS)

The City University of New York (CUNY)

Aron Trauring
Adjunct Professor
CEO, Zoteca

Class 12 December 12th, 2005

Application Layer Vulnerability

- Firewall protects up to transport layer
- Greatest vulnerability at application layer
- Most attackers use well-known published attacks
- Tools are available to exploit vulnerabilities
- Old vulnerabilities still exploited
- Attacks on “zero-day” exploits or unpublished security holes are very rare
- Increasing barriers lowers vulnerability (criminals look for easy targets)

Barriers to Protecting Networks — Not Enough Time or Staff

- Staff cuts
- Outsourcing and off-shoring
- Information Week: Security's Shaky State Dec. 5, 2005 http://www.informationweek.com/story/showArticle.jhtml?articleID=174900279&cid=RSSfeed_IWK_security

Barriers to Protecting Networks — Concerns About System Stability

- Some vendor patches might break stuff — e.g. Windows XP SP2
- Especially problematic for mission critical systems which need close to zero down time

Barriers to Protecting Networks — Overload

- Too many security patch notifications
- Particularly in larger organizations, cost of patching exceeds cost of software licensing and installation
- Even Microsoft servers get taken down even after they release patches

Barriers to Protecting Networks — Ignorance

- Windows automatic update might not cover all Microsoft software
- On GNU/Linux might have applications not installed through apt-get or other automated package system
- For software which is not part of some automated patching/notification system admin may not be aware of vulnerabilities

Router and Firewall Weaknesses

- Firewall set up is extremely complex — unless set up by expert likely to be mis-configured
- Time pressures and immediate access needs often lead to too much access (e.g. allow ftp and forget about it)
- Routers often run dangerous services — e.g. telnet, finger
- Routers often have default passwords which are unchanged
- Router/firewall web management interface can be exploited
- Lull into false sense of security

Web Server Exploits

- Built to provide files without authentication — high potential for exploitation
- As web servers expand functionality more likely to have vulnerabilities
- Modern web servers also execute code which is often insecure — ASP, PHP, ColdFusion etc.

Mail Server Exploits

- Exchange and Sendmail highly vulnerable
- SMTP is a simple and therefore vulnerable protocol
- Buffer overflow
- Executing shell commands via email server
- Server backdoors
- Stealing usernames and passwords

DNS Server Exploits

- Bind is a monolithic program
- Usually runs as root
- Often misconfigured
- Firewall settings for DNS often misconfigured
- DNS cache poisoning — fake DNS information stored in DNS server cache
- Can be used for phishing or delivering Trojan payloads

Database Exploits

- Web servers often interface with databases
- Authentication protocols may be insecure
- Code may be insecure and exploited via buffer overflows
- Specially crafted URLs can “inject” SQL code right into your system

The Never Expiring Password

- Database applications require authentication vis-a-vis the database
- Username and password embedded in application code
- Programmers have access to these
- In hosted settings staff at ISP has access to these
- Personnel leave but applications are never changed — far too much work

User and File Management

- Need to give user access while adhering to minimalist principles
- Laziness or lack of time leads to giving users too much access
- Windows has poor security by default, although improving in XP
- Former employee accounts are prime target for crackers — owner won't notice strange behavior
- Weak passwords another common vulnerability

Default Accounts in Hardware/Software Systems

- Routers, switches, firewalls, phone systems, alarm systems may have default passwords as well as back doors
- SNMP — Simple Management Network Protocol used in network management systems
- SNMP often comes with simple default passwords too
- `snmpwalk` — allows cracker to map network and take down devices
- SNMP buffer overflow exploits allows cracker to take over devices completely
- Default password lists can be found in seconds with a simple Google search

- **Default Passwords** `http://www.phenoelit.de/dpl/dpl.html`
- **Default Passwords** `http://www.cirt.net/cgi-bin/passwd.pl`

Blank or Weak Passwords

- No password or administrator/administrator
- Bad user passwords

Unneeded Services

- Violation of minimalist principle
- Legacy — `chargen`, `daytime`, `discard`, `echo`, `finger` and `quotd`
- “Personal” web servers
- Old code

Information Leaks

- Chatty operating systems (like Windows) gives out lot's of information about host and services
- Improperly configured DNS systems can expose your network topology
- Corporate information on public web servers expose information via Google
- Information can be exploited by cracker — e.g. username lists can simplify cracking passwords

Example System Crack

- DNS Stuff `http://www.dnsstuff.com/`
- Do DNS lookup on URL
- Click on IP to get a IPwhois — get corporate IP range
- Get sysadmin names (try brute force password attack)
- Port scan IP range (`nmap`)
- Vulnerability scan (`nessus`)
- e.g NETBIOS null sessions allowed on server — get all usernames, groups, machines, shares
- NETBIOS Null Sessions `http://www.brown.edu/Research/SysAdmins/articles/netbios_null_sessions.html`

- e.g. web server has buffer overflow vulnerability
- Download tool kit to exploit vulnerability (e.g. Attack Toolkit)
- Brute force attacks on passwords
- Social engineering to leverage information already have

General Principles for Limiting Vulnerabilities

- Minimalism — Install only what you need
- Minimalism — Keep only users that are currently live
- Vigilance — Install stable version on mission critical systems
- Vigilance — Automate patch installation process
- Vigilance — Firewall perimeter and hosts
- Vigilance — Use sniffers, scanners and data mining tools

Vulnerability Scanners

- Multiple and various points of attack
- Multiple vulnerabilities associated with these
- Vulnerability scanners check multiple points and their multiple weaknesses
- Requires constant signature updates

Considerations for Vulnerability Scanning

- Scan with permission
- Make sure you have current backups
- Time your scans when least disruptive
- Don't scan excessively
- Place scanner appropriately
- Use certificates so remote communication between client and server are encrypted

What Vulnerability Testing Doesn't Test

- Application logic error except for well known bugs in well known services
- Custom applications
- Social engineering attacks
- Undiscovered vulnerabilities
- Attacks that already happened