Network Security: Overview

Raj Jain
Washington University in Saint Louis
Saint Louis, MO 63130
Jain@cse.wustl.edu
Audio/Video recordings of this lecture are available at:
http://www.cse.wustl.edu/~jain/cse571-17/

Overview

1. Security Components
2. Steps in Cracking a Network
3. Types of Malware
4. Types of Attacks
5. Security Mechanisms


1. Security Components

- **Confidentiality**: Need access control, Cryptography, Existence of data
- **Integrity**: No change, content, source, prevention mechanisms, detection mechanisms
- **Availability**: Denial of service attacks
  - **A=Availability, Authenticity or Accountability**
- Confidentiality, Integrity and Availability (CIA)
- CIA Triangle

Steps in Cracking a Network

- **Information Gathering**: Public sources/tools.
- **Port Scanning**: Find open TCP ports.
- **Network Enumeration**: Map the network. Servers and workstations. Routers, switches, firewalls.
- **Gaining Access**: Keeping root/administrator access
- **Modifying**: Using access and modifying information
- **Leaving a backdoor**: To return at a later date.
- **Covering tracks**
Types of Malware

- **Viruses**: Code that attaches itself to programs, disks, or memory to propagate itself.
- **Worms**: Installs copies of itself on other machines on a network, e.g., by finding user names and passwords.
- **Trojan horses**: Pretend to be a utility. Convince users to install on PC.
- **Rootkit**: Gets “root” (admin) privilege.

Types of Viruses

- Boot sector virus: Floppy disks
- Macro virus: Office documents
- Email malware: Attachments
- Web site malware: JavaScripts

Types of Malware (Cont)

- **Spyware**: Collect information. Legally used by employers.
- **Key Loggers**
- **Hoax**: Use emotion to propagate, e.g., child’s last wish.
- **Trap Door**: Undocumented entry point for debugging purposes.
- **Logic Bomb**: Instructions that trigger on some event in the future.
- **Zombie**: Malicious instructions that can be triggered remotely. The attacks seem to come from other victims.

Ref: [http://www.spywareguide.com/](http://www.spywareguide.com/)

Types of Attacks

- **Malware**
- **Security Breach**: unauthorized access
- **Denial of Service (DoS)**: Flooding with traffic/requests
- **Web attack**: SQL injection
- **Cross-Site Scripting**: Direct users to malicious sites using SQL injection
- **Session Hijacking**: Taking over an active session
- **DNS Poisoning**: Direct users to malicious sites
- **Brute Force**: Try all passwords.
- **Port Scanning**: Disable unnecessary services and close ports
- **Network Mapping**
Types of Attacks (Cont)

- **Cyber Stalking**: Harassing/threatening using Internet
- **Cyber Frauds**: Nigerian official wants to deposit large funds into your bank account
- **Identity Theft**: Get credit cards using your Social Security number
- **Phishing**: Email claiming to be from bank/employer/government

Buffer Overflows

- Return address are saved on the top of stack.
- Parameters are then saved on the stack.
- Writing data on stack causes stack overflow.
- Return the program control to a code segment written by the hacker.

DoS Attack

- **ICMP Flood**: Lots of ping with large message sizes
  `ping <addr> -l <buffer size> -w <timeout> -t` (till stopped)
  `ping 127.0.0.1 -l 65000 -w 0 -t`
- **Syn Flood**: Lots of incomplete connections => Server runs out of resources
- **UDP Flood**: No application at destination port generates “Destination unreachable” response to spoofed source address.
- **Smurf Attack**: A broadcast ICMP packet is sent to broadcast address. Everyone responds to the spoofed source address
- **Ping of Death**: Ping with a very large packet can crash the destination
- **Low Orbit Ion Cannon**: Open Source DoS attack tool
- **High Orbit Ion Cannon**: Open source DoS attack tool written in Basic. Can attack 256 URLs at the same time.

Distributed DoS Attacks

- **Tribe Flood Network** (TFN) clients are installed on compromised hosts.
- All clients start a simultaneous DoS attack on a victim on a trigger from the attacker.
- **Trinoo** attack works similarly. Use UDP packets. Trinoo client report to Trinoo master when the system comes up.
- **Stacheldraht** uses handlers on compromised hosts to receive encrypted commands from the attacker.
Phishing Example

Social Engineering

- **Reverse social engineering**: User is persuaded to ask Hacker for help.
- **Phone calls**:
  - Call from tech support to update the system.
  - High-level VP calling in emergency.
  - Requires employee training.
- **Electronic Social Engineering (Phishing)**:
  - EBay transactions, PayPal Accounts, Bank Account, Nigerian 419 scams (Section 419 of Nigerian criminal code), Lottery.
  - Anti-phishing workgroup (antiphishing.org) found that 5% of the recipients respond compared to 1% for spam.

Security Mechanisms

- Encipherment
- Digital Signature
- Access Control
- Data Integrity
- Authentication Exchange
- Traffic Padding
- Routing Control
- Notarization
- Least Privilege: Each user/service should have minimum privilege to do the job
**Honey Pots**

- Trap set for a potential system cracker
- All the services are simulated
- Honey pot raises alert allowing administrator to investigate

**Hackers**

- **White Hat Hackers**: Hackers that find vulnerabilities and inform the organization
- **Black Hat Hackers**: Hackers that exploit vulnerabilities
- **Red Team**: Penetration testers to find vulnerabilities
- **White Team**: Security protection personnel

**Perimeter vs. Layer Security**

- **Perimeter Security**: Inspection at entry points
- **Layered Security**: Security in every segment inside as well as at the perimeter ⇒ All systems are not affected.

**Summary**

1. Confidentiality, Integrity, and Availability (CIA)
2. Malware: Viruses, worms, trojan horses, rootkit, spyware, trap door, logic bomb
4. DoS Attacks: ICMP/Syn/UDP flood
Lab 2

1. Download and read about the following tools

2. Use **advanced port scanner** to scan one to three hosts on your local net (e.g., CSE571XPS and CSE571XPC in the security lab) to find their open ports.

3. Use **nmap** to show the map of all hosts on your local net

Lab 2 (Cont)

4. Ping [www.wustl.edu](http://www.wustl.edu) to find its address. Start Wireshark. Set capture filter option “IP Address” to capture all traffic to/from this address. Open a browser window and Open [www.wustl.edu](http://www.wustl.edu). Stop Wireshark. Submit a screen capture showing the packets seen.

---

**Security Related Websites**

- Computer Emergency Response Team (CERT), [http://www.cert.org/](http://www.cert.org/)
- IETF Security area, [https://datatracker.ietf.org/wg/](https://datatracker.ietf.org/wg/)

**Security Related Websites (Cont)**

- SANS Institute, [http://www.sans.org](http://www.sans.org)
- Google groups, [http://groups.google.com](http://groups.google.com)
- LinkedIn Groups, [http://www.linkedin.com](http://www.linkedin.com)
Acronyms

- AES: Advanced Encryption System
- CERT: Cyber Emergency Response Team
- DDoS: Distributed DoS
- DES: Data Encryption System
- DNS: Domain Name System
- DoS: Denial of Service
- ICMP: IP Control Message Protocol
- ID: Identifier
- IETF: Internet Engineering Task Force
- IP: Internet Protocol
- NIST: National Institute of Standards and Technology
- PC: Personal Computer
- RFC: Request for Comments
- SANS: Escal Institute of Advanced Technologies
- SQL: Structured Query Language
- TCP: Transmission Control Protocol

Acronyms (Cont)

- TFN: Tribe Flood Network
- UDP: User Datagram Protocol
- URL: Universal Resource Locator
- VP: Vice-President
- VPN: Virtual Private Network

Scan This to Download These Slides

Related Modules

CSE571S: Network Security (Spring 2017), http://www.cse.wustl.edu/~jain/cse571-17/index.html
CSE473S: Introduction to Computer Networks (Fall 2016), http://www.cse.wustl.edu/~jain/cse473-16/index.html
Wireless and Mobile Networking (Spring 2016), http://www.cse.wustl.edu/~jain/cse574-16/index.html
CSE571S: Network Security (Fall 2014), http://www.cse.wustl.edu/~jain/cse571-14/index.html
Audio/Video Recordings and Podcasts of Professor Raj Jain's Lectures, https://www.youtube.com/channel/UCN4-5wNP9-ruOzQM8-8NUw