TYPES OF ATTACKS AND MALICIOUS SOFTWARE

Reading

- Chapter 15
- Ping of Death
  - https://en.wikipedia.org/wiki/Ping_(networking_utility)
  - https://en.wikipedia.org/wiki/Ping_flood
- Advanced Persistent Threat
  - https://en.wikipedia.org/wiki/Advanced_persistent_threat

Some topics in the book chapter have been covered in previous lectures
Objectives

- Become familiar with various types of attacks
- Be able to identify different types of malicious software
- Understand defenses against categories of attacks

Reasons for an Attack

- Random
  - Look for vulnerabilities, such as
    - Lacking current security patches
    - New attack approaches
    - Undefended networks
- Targeted
  - Political – Snowden
  - Military – Iran, Russia,
  - Financial – e.g., stealing credit card info
  - Hacktivist – e.g., fur coats
Direct vs. Indirect Attack

• Attacker might choose to attack directly
  • Detection probability is low
  • Value of attack point is limited

• Indirect
  • Attacker uses a series of intermediate hosts between launch point and target
  • More difficult to block

• Massed
  • Compromise third-party hosts and use them all
  • Botnets
  • Examples: DDoS, distributed capture of target’s network traffic

Types of Attacks

• Denial-of-service
• Backdoors/Trapdoors
• Sniffing
• Spoofing
• Man-in-the-middle
• TCP/IP hijacking

• Phishing/pharming
• Attacks on encryption
• Address system attacks
• Password guessing
• Hybrid attack
• Birthday attack
• Injection attack
Malicious Code (Malware)

- SW used or programmed by attackers to disrupt computer operation, gather sensitive information, or gain access to private computer systems
- Examples
  - Viruses
  - Trojan horses
  - Logic bombs
  - Spyware
  - Worms

Computer Viruses

- Characteristics
  - Self-replicating computer programs
  - Attached to other programs
  - Installed without the users consent
- Best-known malicious code
- Types:
  - Boot Sector virus – early
  - Program virus – attaches itself to executables
  - Macro virus – written in a macro language associated with an application (e.g., Word, Excel)
Virus Countermeasures

- Anti-virus software
- Scan for known virus pattern
- Software checksums
- Counter-Countermeasure
  - Polymorphic malware – code that changes on a regular basis

Worms

- Code that penetrates and replicates on systems
- Doesn’t need to attach to other files or code
- Spread by a variety of methods (e.g., e-mail, infected web sites, and P2P sharing networks
- Defenses
  - Install all patches
  - Use firewalls
  - Implement an intrusion detection system
  - Eliminate unnecessary services
  - Use extreme caution with e-mail attachments
Trojan Horses

- Non-replicating form of malware
- Software that appears to do one thing but contains hidden functionality
- Disguised well
- Delivers payload without user’s knowledge

Prevention

- Never run software of unknown origin or integrity
- Keep virus-checking program running continuously

Spyware

- Software capable of recording and reporting a user’s actions
- Typically installed without user’s knowledge
- Monitors software and system use (e.g., key-logging)
- Many states have banned spyware and other unauthorized software:
Logic Bombs

- Code intentionally inserted into a software system that will set off a malicious function when specified conditions are met
- Usually installed by authorized user
- Reinforces need for backups
- A time bomb is similar to the logic bomb, but delivers payload at a predetermined time/date

Defenses
- Separation of duties
- Periodic review of programs and services
- Active backup process

Crypto-Malware

- Malware that encrypts files on a system and then leaves them unusable
- Form of DoS attack

Examples
- WannaCry
- NotPetya
Minimizing Possible Avenues of Attack

• Ensure all patches are installed and current
• Use an anti-virus suite
• Limit the services being run on the system
  • Limit possible avenues of attack
  • Reduce the number of services the administrator must continually patch
• Limit public disclosure of private information about your organization
• Outsource external services

Trapdoors and Backdoors

• Trapdoor
  • Hard-coded access built into the program
  • Ensures access should normal access methods fail
  • Creates vulnerability in systems using the software
• Backdoor
  • Ensures continued unrestricted access in the future
  • Attackers implant them in compromised systems
  • Can be installed inadvertently with a Trojan horse
Denial-of-Service (DoS) Attack

- Purpose: prevent normal system operations for authorized users
- Exploits known identified vulnerabilities
- Can be accomplished by
  - Taking the system offline
  - Overwhelming the system with requests

DoS Example: SYN Flood Attack

- Illustrates basic principles of most DoS attacks
- Exploits
  - assumptions made by TCP/IP protocol designers
  - IP packets can easily fake the return IP address
SYN Flood Attack

- Based on TCP 3-way handshake
  - System 1 sends SYN packet to System 2.
  - System 2 responds with SYN/ACK packet.
  - System 1 sends ACK packet to System 2 and communications can then proceed

SYN Flood Attack

- Request fakes IP address with a non-existent one
- SYN/ACK times out waiting for ACK
- If SYN/ACK outpaces the timing-out, resources will be exhausted waiting for responses

Notice that the attack exploits a weakness in the IP protocol
**Distributed Denial-of-Service (DDoS)**

- Attacks through multiple systems
- Overwhelms target system or network
- Masks the attacker

---

**Example: Ping**

- **Ping** - network utility used to test the reachability of a host on an IP network; packet size is about 64 bytes
- **Ping of Death**
  - Attacker sends ICMP ping packet equal to or larger than the maximum IP packet size (64KB)
  - Some systems cannot handle a large packet, and system will hang or crash
- **Ping Flood**
  - Uses the flood feature of Ping to overwhelm the receiver with requests

---

The name “ping” is taken from sonar technology

Ping is an example of a network feature designed without security considerations
Preventing DoS Attacks

• Ensure necessary patches and upgrades remain current
• Change time-out period for TCP connections (suitable for SYN flood attacks)
• Distribute workload across several systems
• Block external ICMP packets at border
  • Limits functionality
  • Can have selective blocking

Sniffing …

• Attacker observes all network traffic
• Internet protocols make this easy
• Implemented with SW or HW
• Ability to target specific protocol, service, string of characters (e.g., login credentials)
• Can be used to
  • Gather info for a later attack
  • Sweep up huge amounts of data
… Sniffing

• Physical security is key in prevention of sniffers on an internal network
• Strong encryption more suitable for an external network

IP Address Spoofing

• **Spoofing** – communication is sent from an unknown source disguised as a source known to the receiver
• Naïve assumptions in TCP/IP allow spoofing to easily occur
E-Mail Spoofing

• Message sent with a From address that differs from that of the sending system
• Weaknesses in the mail protocols
• Web address spoofing (e.g., whitehouse.com)

Spoofing and Trusted Relationships

• Spoofing can take advantage of a trusted relationship between two systems
• Can occur when two systems are set to accept the authentication performed by the other system
• Message sent to one trusted system by attacker appears to originate from the other trusted system
• Often accompanied by a DoS attack on the first system to disable any possible acknowledgements
• Defense – limit trusted relationships between hosts.
Session Hijacking

- Taking control of an existing client/server session
- No design provision for sessions in original Web protocols
- Web session data usually encoded in a cookie sent to the client
- Attacker takes control of an existing session and circumvents authentication
- Bypasses multi-factor authentication
- Can be disguised with a DoS attack on the original user
- Relies on an understanding of network traffic patterns
- Defense – encryption of all traffic post-SSL handshake

Cookie Process

1. Your servlet “sets a cookie” by including it in the response
2. Your browser stores the cookie in your cookies directory on your hard disk
3. Your browser sends the cookie every time a request is made to a server “in your domain”
Zero Day Attack

- Uses a system vulnerability for which there is no previous knowledge
- Since the vulnerability is not previously known, there usually is no defense in place
- Highly valued and difficult to generate

Ethical question – if the US government collects zero-day vulnerabilities for future attacks, should it release them in order to better build defenses?

Buffer Overflow Attack

- A program is provided more data than it was designed to handle
- Associated with programs that have poor error handling
- In some cases, the program will execute a command supplied by the attacker
- Attacks are effective against programs that use root-level access
Injection Attacks

• Including executable code in a data entry field
• One of the top vulnerabilities
• SQL injection most prominent

Auditing

• Security auditing – assessing the security state of an organization against an established standard
• Should be conducted on a regular basis
• May be mandated (e.g., regulated industries)
• Usually contracted out to a another party
• Sometimes the standard is industry "best practices"
• Penetration tests – assess vulnerability of organization’s system (not against an established standard)
• Focus on
  • Penetration attempts
  • Policies, procedures, and guidelines governing security
  • Employee training
Advanced Persistent Threat (APT)

- Coordinated team of attackers
- Team composed of various attack specialists
- Associated with targeted attacks
- Not consistent with an “outrun the bear” approach to security defenses

Steps in an Attack

- Conduct reconnaissance (profiling)
- Scan the network
- Look for vulnerabilities
- Perform the attack
- Create a backdoor
- Exfiltration
- Cover tracks
Conduct Reconnaissance

- Referred to as “target development”
- Gather information about the target
  - Public record data
  - Social networking
  - Organization
- Examples
  - Mapping US power grid
  - NY Times

“Most impressive tool in the attackers’ arsenal is Google” – cyber security expert, Gary McGraw

Scan

- Identify target systems that are active and accessible
  - Ping sweep (ICMP echo request)
  - Port scan (identify services)
- Identify operating system and application programs
- Analyze packet response to port requests
- Identify individuals (often low-level) that might make a good start to the attack
Identify Vulnerabilities

- Information available (e.g., hacker groups)
  - OS vulnerabilities
  - Application program vulnerabilities
  - Tools to exploit vulnerabilities

Perform the Attack

- Match an attack to an identified vulnerability
- Style of attack consistent with goals
  - Stealth (e.g., Iran, SecureID)
  - Obtain information (e.g., SecureID)
  - Harm the attacked site
  - Send a message
Create a Backdoor

- Future access to the attacker
  - Example - “authorization” for attacker
- Attacker goal: retain backdoor even if attack is detected
- APT might have a team member monitoring e-mail to learn defender actions
- Examples
  - Post attack (and clean-up) – thermostat and printer found sending messages to a server in China
  - Non-digital defense coordination (e.g., handwritten signs in hallways about password changes)

Exfiltration Phase

- Sometimes referred to as the “phone home” phase
- Massive amounts of data leave the target network
- When many successful APTs are detected
- Importance of anomaly detectors
- Goal: not reveal external contact point
- Common technique
  - Route data through way stations in multiple countries
  - Distinct legal jurisdictions make prosecution difficult
Cover Tracks

- To avoid detection, attackers sometimes cover their tracks:
  - Erase pertinent log files from the system
  - Change file time stamps to appear unaltered

Have You Met the Objectives?

- Become familiar with various types of attacks
- Be able to identify different types of malicious software
- Understand defenses against categories of attacks