

Types of Attacks and Malicious Software



Chapter 15

Important

Background

- Viruses
 - most talked about,
 - But not the only methods to attack computer systems and networks.
 - Various other ways to attack computers and networks

- Each type of attack threatens **at least** one of the three security services:
 - Confidentiality
 - Integrity
 - Availability



Avenues of Attack

- Computer mainly attacked for two reasons
 1. Specifically targeted by the attacker
 - Chosen based on attacker's motivation
 - Not reliant on target system's hardware and software
 - The attacker attempts to gain access to a specific target and find an existing vulnerability.
 - More difficult and take more time and effort
 2. Targets of opportunity
 - Systems with hardware or software vulnerable to a specific exploit
 - Often lacking current security patches
 - The attacker attempts to find any system that is susceptible to a specific vulnerability



The Steps in an Attack

1. Conducting reconnaissance
2. Scanning
3. Researching vulnerabilities
4. Performing the attack
5. Creating a backdoor
6. Covering tracks

Important

Conducting Reconnaissance

- Gather as much information as possible about the target system and organization.
 - Use the Internet.
 - Explore government records
 - For example: SEC's EDGAR website (www.sec.gov/edgar.shtml) for financial reports
 - Use tools such as Whois.Net.
- Key data include
 - names, phone numbers, IP addresses, physical addresses, networks maintained by the organization, and even the organizational structure or hierarchy.
- Don't worry yet whether the information being gathered is relevant or not.

It is important for attackers to verify the relevance of information being gathered while conducting Reconnaissance.

1.

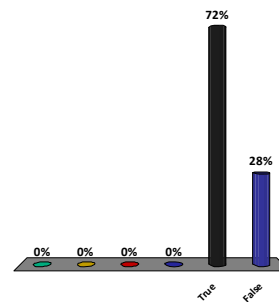
2.

3.

4.

5. True

6. False





Scanning

- **Identify target** systems that are active and accessible.
 - **Ping sweep**
 - Identify which machines on the target network are reachable
 - **Port scan**
 - Identify open ports and possibly even services running on the systems

- **Identify the operating system and other specific application programs** running on system.
 - accomplished by sending specifically formatted packets to the target system and analyzing the response
 - Tools such as nmap can be used to fingerprint an OS



Researching Vulnerabilities

- Once the software running on the target system has been determined
 - an attacker can then use the Internet to research vulnerabilities

- Wealth of information available through the World Wide Web
 - Lists of vulnerabilities in specified OS and application programs
 - Tools created to exploit vulnerabilities

System administrators may also find these types of web sites valuable in their efforts to stay abreast of new vulnerabilities that they must secure within their systems.



Performing the Attack

- Once vulnerabilities have been identified within the target systems,
 - it can then be attacked in a variety of ways depending on the attacker's objective.
- The variety of possible outcomes is as diverse as are the avenues for executing the attack.
- Some possible outcomes include
 - crashing the system
 - theft of information
 - defacement of a website.
- The key - Match the chosen attack to the vulnerability identified through reconnaissance.



Creating a Backdoor

- A way to more easily regain access to the target system in the future.
 - Provide the attacker with access to the previously hacked system.
- How it is done?
 - Adding themselves to the list of authorized users
 - Installing an agent which will initiate contact with the attacker at some future point

The key for the attacker is to capitalize on their current success by ensuring additional success in the future.

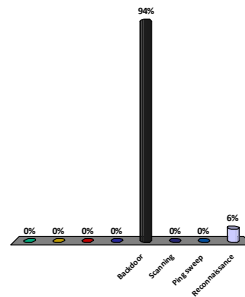
Covering Tracks

- In an effort to remain undetected, attackers endeavor to cover their tracks:
 - Erase pertinent log files from the system.
 - Change the file time stamps so that the files do not appear to have been altered by the attacker

A good defense against a hacker modifying or erasing log files –
Maintain them on a separate, remote log file server, with
restricted access. – **Why???**

_____ provides the attacker with access to
the previously hacked system

- 1.
- 2.
- 3.
- 4.
5. 😊 Backdoor
6. Scanning
7. Ping sweep
8. Reconnaissance





Minimizing Possible Avenues of Attack

- Minimizing the possibility of an attack
 - limit the exposure of the systems by minimizing the possible avenues an attacker can exploit
- Done in the following three steps:
 1. Ensure all patches are installed and current.
 2. Limit the services being run on the system.
 - Limits possible avenues of attack
 - Reduces number of services the administrator must continually patch
 3. Limit the amount of publicly available data about the system and organization.



Attacking Computer Systems and Networks

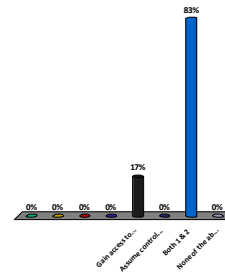
- What is an Attack?
- An attempt by an unauthorized person to:
 - Gain access to or modify information
 - Assume control of an authorized session
 - Disrupt the availability of service to authorized users

Attacking Computer Systems and Networks (continued)

- Attacks grouped into **two categories**:
 1. Attacks on specific software
 - Rely on code flaws or software bugs
 - Indicates lack of thorough code testing
 - These flaws should have been identified and corrected during the thorough testing phase of the software development lifecycle.
 2. Attacks on a specific protocol or service
 - Attempt to exploit a specific protocols or services by
 - Taking advantage of a specific feature of the protocol or service.
 - Using it in a manner different from its intended purpose

An attack is an attempt by an unauthorized person to

- 1.
- 2.
- 3.
- 4.
5. Gain access to or modify information
6. Assume control of an authorized session
- 😊 7. Both 1 & 2
8. None of the above





Types of Attacks

- Denial-of-service
- Backdoors/Trapdoors
- Null sessions
- Sniffing
- Spoofing
- Man-in-the-middle
- Replay
- TCP/IP hijacking
- Drive-by downloads
- Phishing/pharming
- Attacks on encryption
- Address system attacks
- Password guessing
- Hybrid attack
- Birthday attack

Important



Denial-of-Service Attacks

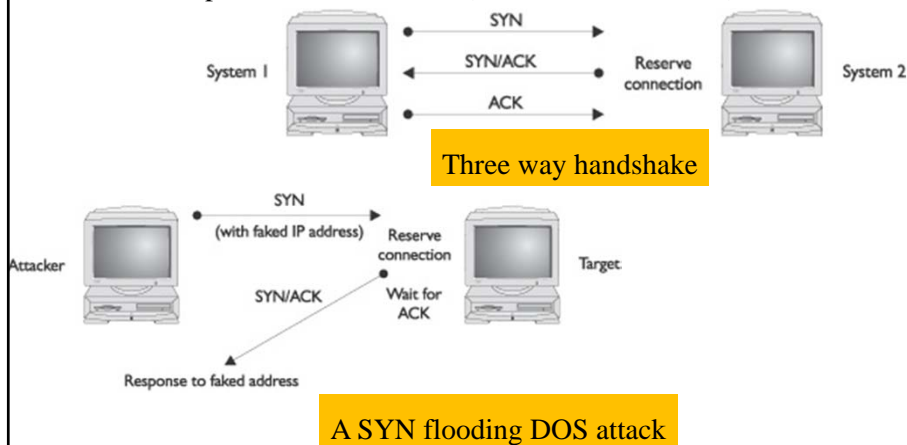
- **Denial-of-Service (DOS) attack**
 - Attacker attempts to deny authorized users access either to specific information or to the computer system or network.
 - Purpose-
 - To prevent normal system operations for authorized users
 - Can be used with other actions to gain unauthorized access to a computer or network.
 - Can be accomplished in multiple ways
 - Take the system offline
 - Overwhelm the system with requests

SYN Flood Attack

- **SYN flooding attack**
 - Temporarily prevents service to a system to take advantage of a trusted relationship that exists between that system and another.
- Exploit a weakness inherent to the function of the TCP/IP protocol
 - Uses TCP three-way handshake to flood a system with faked connection requests

SYN Flood

- In a SYN flood attack, the attacker sends fake communication requests to the targeted system.
 - Each request is answered by the target system which waits for the third part of the handshake (from the fake address)





SYN Flood

- **A nonexistent IP address is used in the requests.**
 - **Targets a protocol (TCP)**
 - The target system responds to a system that does not exist.
 - The target waits for responses that will never come.
 - The target system drops these connections after a specific **time-out period**.
 - **If the attacker sends requests faster than the time-out period eliminates them, the system is filled with requests.**
 - When more requests come in than can be processed, the system will soon be reserving all its connections for fake requests.
 - Further requests are dropped (ignored).
 - **Legitimate users who want to connect to the target system will not be able to do so.**

Important



Ping of Death

- **Ping of Death**
 - **Another simple DOS attack**
 - Illustrates the other type of attack
 - **targeted at a specific application or operating system.**
 - **In contrast, the SYN flood (previous slide) targets a protocol.**
- The attacker sends an Internet Control Message Protocol (ICMP) “ping” packet equal to, or exceeding 64KB ($64 * 1024 = 65,536$ bytes).
 - Packets this large should not occur naturally (there is no reason for a ping packet to be larger than 64KB).
 - Some systems cannot handle this size of packet.
 - The system hangs or crashes.

Important

SYN flood attack targets at a specific application or operating system

- 1.
- 2.
- 3.
- 4.
5. True
6. False

Response	Percentage
True	61%
False	39%

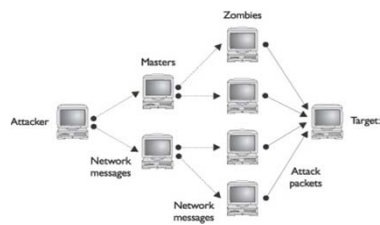
A SYN flood is an example of what type of attack?

- 1.
- 2.
- 3.
- 4.
5. Malicious code
6. DoS
7. Man-in-the-middle
8. Spoofing

Response	Percentage
Malicious code	0%
DoS	89%
Man-in-the-middle	0%
Spoofing	0%

Distributed Denial-of-Service

- The **DDOS attack overwhelms the target with traffic from many systems.**
 - A network of attack agents (zombies) is created by the attacker, and upon receiving the attack command, the attack agents commence sending a specific type of traffic against the target.
- **The attack agents are not willing agents.**
 - They are systems that have been compromised & the DDOS attack software has been installed.



Distributed Denial-of-Service

- To compromise these agents,
 - the attacker gains unauthorized access to the system
 - Trick authorized users to run a program that installed the attack software.
- The creation of the attack network may be a multistep process.
 - The attacker compromises a few systems.
 - These are used as handlers or masters, and they compromise other systems.
- Once the attack network has been created, the agents wait for an attack message that includes data on the specific target.

Aim of _____ attack is to prevent normal system operations for authorized users

- 1.
- 2.
- 3.
- 4.
5. DoS
6. DDoS
7. Both 1 & 2
8. None of the above

Option	Percentage
DoS	11%
DDoS	0%
Both 1 & 2	89%
None of the above	0%

Preventing DoS & DDoS Attacks

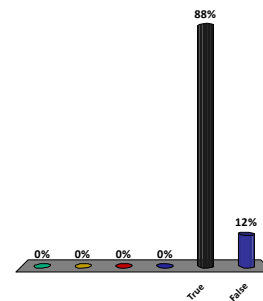
- **Ensure necessary patches and upgrades remain current.**
 - Attackers are quick to exploit newly discovered vulnerabilities
 - Administrators usually have a small window of opportunity in which to patch their systems
- **Change time-out period for TCP connections.**
 - Drops unused connections more quickly.
 - Makes it more difficult for attackers to disrupt the system with a SYN flooding attack.
- **Distribute workload across several systems.**
 - Causes attackers to target multiple hosts simultaneously to achieve success in disrupting service.
- **Block external ICMP packets at border.**
 - As many attacks rely on ICMP, blocking these packets or at least specific forms of ICMP can help to prevent attacks from occurring

Important

Chances of DoS attack can be minimized by distributing workload across several systems.

- 1.
- 2.
- 3.
- 4.

5. True
6. False



Trapdoors and Backdoors

- **Backdoor**
 - Ensures continued unrestricted access in the future
 - Attackers implant them in compromised systems
 - Can be installed inadvertently with a Trojan horse

- **Trapdoor**
 - Hard-coded access built into the program
 - benefit to software developers and system administrators
 - Ensures access should normal access methods fail
 - Creates vulnerability in systems using the software
 - Offers full access into the system where an attacker could cause serious harm



Sniffing

- Sniffing
 - An attacker examines all network traffic as it passes their NIC independent of whether or not the traffic is addressed to them or not.
 - Hope of viewing something as userID and password
- Network sniffer
 - A software, hardware, or combination of the two
 - Used to view all traffic, or to target specific protocol, service, string of characters, etc.
 - May be able to modify some or all traffic in route
- Also used by Network administrators to monitor and troubleshoot network performance.



Sniffing

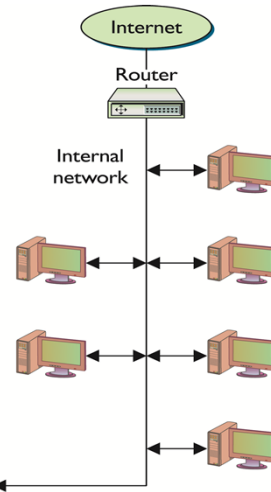
- The network device that connects a computer to a network is designed to ignore all traffic that is not destined for that computer.
- Sniffers ignore this friendly agreement
 - Observe all traffic on the network, whether destined for that computer or other computers.
 - A network card that is listening to all network traffic and not just its own is said to be in “promiscuous mode.”
- For network sniffers to be effective, they need to be on the internal network.

Sniffing (continued)

Physical security is key in preventing introduction of sniffers on the internal network.

Network sniffers listen to all network traffic

Attacker listening to all traffic

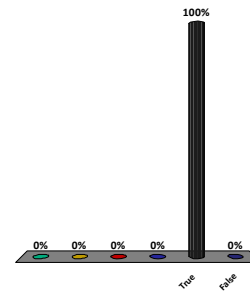



A network card that is listening to all network traffic and not just its own is said to be in “promiscuous mode.”

- 1.
- 2.
- 3.
- 4.
5. 
- 6.

True

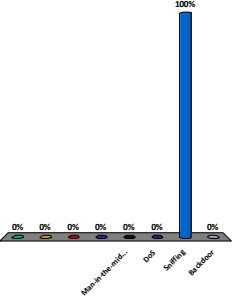
False






An attack in which the attacker simply listens to traffic being transmitted, in the hope of viewing something as userID and password is

- 1.
- 2.
- 3.
- 4.
5. Man-in-the-middle
6. DoS
7. Sniffing
8. Backdoor



Attack Type	Percentage
Man-in-the-middle	0%
DoS	0%
Sniffing	100%
Backdoor	0%



Spoofing

- **True source of data is disguised:**
 - When data appears be coming from a different source than it actually is, the data source is being spoofed
- **Commonly accomplished by altering packet header** information with false information
 - Systems should fill in the their own address as the source,
 - but attackers manipulate the system into filling in another system's address.



Spooftng Types

- **Spooftng e-mail:**
 - From address differs from sending system
 - Recipients rarely question authenticity of the e-mail

- **The URL Spoof**
 - not technically spoofing.
 - Attackers acquire a URL close to the one they want to spoof so that e-mail sent from their system appears to have come from the official site unless the address is read carefully.
 - Whitehouse.gov and Whitehouse.com (pornographic website)



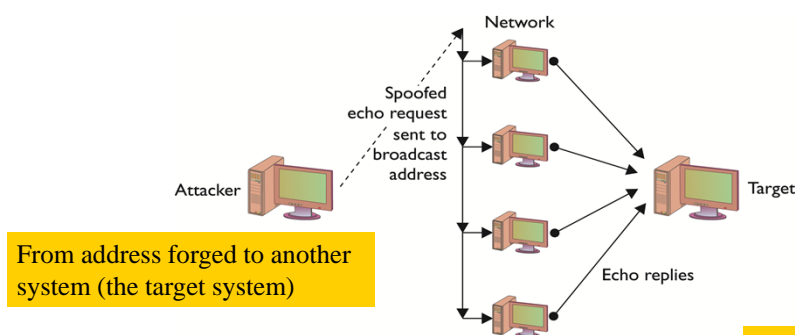
IP Address Spoofing

- **IP Address Spoofing**
 - The IP protocol works by having the originators of any IP packet include their own IP address in the “From” portion of the packet.
 - There is nothing that prevents a system from inserting a different address in the “From” portion of the packet

- **Smurf Attack**
 - A specific DoS attack
 - The attacker sends a spoofed packet to the broadcast address for a network
 - This packet is an echo request with the From address forged so that it appears that another system (the target system) has made the echo request.
 - The packet is distributed to all systems on that network.

IP Address Spoofing and DoS attack

- The attacker has sent one packet and has been able to generate various responses aimed at the target.
- Should the attacker send several of these spoofed requests, or send them to several different networks, the target can quickly become overwhelmed with the volume of echo replies it receives.



Spoofing and Trusted Relationships

- Spoofing can also take advantage of a trusted relationship between two systems.
- If two systems are configured to accept the authentication from each other, they have a trust relationship.
 - An individual logged on to one system might not go through authentication again to access the other system.
 - Attackers take advantage of this by sending a packet to one system that appears to have come from a trusted system.
 - Since the trusted relationship is in place, the targeted system may perform the requested task without authentication.

Contd.

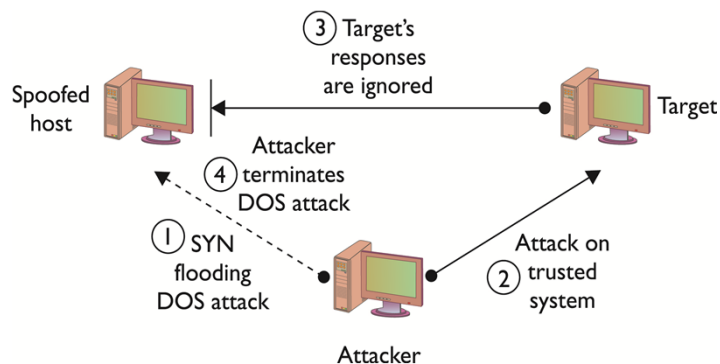
Important

Spoofting and Trusted Relationships

- A reply will often be sent once a packet is received
 - The system that is being impersonated could interfere with the attack as it would receive an acknowledgement for a request it never made.
- The attacker will often initially launch a DoS attack (such as a SYN flooding attack) to temporarily take out the spoofed system for the period of time **that the attacker is exploiting the trusted relationship**
- Once the attack is completed, the DoS attack on the spoofed system would be terminated
 - System administrators, apart from having a temporarily nonresponsive system, might never notice that the attack occurred.

Important

Spoofting and Trusted Relationships



Important

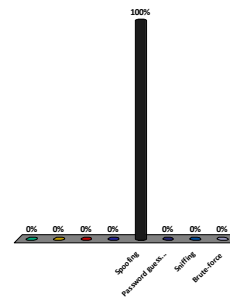
Spoofing and Trusted Relationships

- Countermeasures
 - Strictly limit any trusted relationships between hosts.
 - Firewalls should also be configured to **discard any packets from outside of the firewall that have From addresses indicating they originated from inside the network**
 - A situation that should not occur normally and that indicates spoofing is being attempted)

Important

Which attack takes advantage of a trusted relationship that exists between two systems?

- 1.
- 2.
- 3.
- 4.
5. 😊 Spoofing
6. Password guessing
7. Sniffing
8. Brute-force

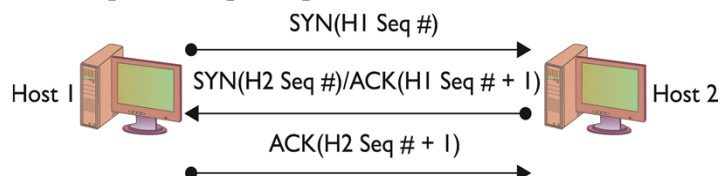


Sequence Numbers

- Sequence Numbers
 - A sequence number is a 32-bit number established by the host that is incremented for each packet sent.
 - As the packets are not guaranteed to be received in order, the sequence number can be used to
 - help reorder packets as they are received
 - refer to packets that may have been lost in transmission.

Sequence Numbers

- In the TCP three-way handshake, two sets of sequence numbers are created.
 1. The first system chooses a sequence number to send with the original SYN packet.
 2. When the second host responds and sends its own SYN packet, it generates another sequence number. It also sends an ACK packet in response to the first host's SYN
 3. The original host system receives the SYN/ACK with both sequence numbers.
 4. It increments the second host's sequence number by one and passes it back in an ACK packet response.





Spoofing and Sequence Numbers

- How complicated the spoofing is depends on
 - whether the traffic is encrypted
 - where the attacker is located relative to the target.

- Spoofing attacks from inside a network are easier to perform.
 - The insider can observe the traffic to and from the target
 - Can do a better job of formulating the necessary packets.


- Formulating the packets is more complicated for external attackers.
 - There is a sequence number associated with TCP packets.
 - The sequence number the target system generates is not observed
 - Next to impossible for the attacker to provide the final ACK with the correct sequence number.

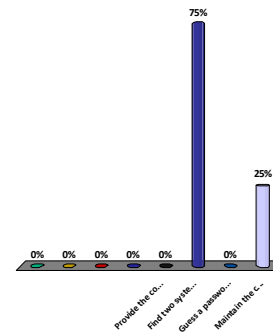


Spoofing and Sequence Numbers

- Predicting sequence numbers is possible, but difficult.
 - Session sequence numbers do not start from the same number.
 - Different packets from different concurrent connections will not have the same sequence numbers.
 - Sequence number for each new connection is incremented by some large number to keep them from being the same.
 - The sequence number may also be incremented by some large number every second (or some other time period).

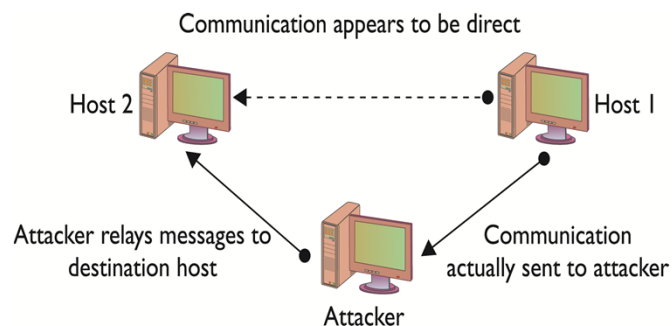
The trick in spoofing is in trying to:

- 1.
- 2.
- 3.
- 4.
5. Provide the correct authentication token
6. Find two systems between which a trusted relationship exists
7. Guess a password or brute-force a password to gain initial access to the system or network
8.  Maintain the correct sequence numbers for the response packets



Man-in-the-Middle Attack

- Attacker is positioned between two target hosts:
 - Typically accomplished by manipulating a router to alter the path of the traffic.
 - Traffic redirected to attacker, then relayed on to the target host
 - Attacker can intercept, modify, and/or block traffic
 - Communication appears normal to target hosts
 - Useful data collection reduced if traffic is encrypted





Replay Attacks


- Attacker intercepts part of an exchange between two hosts and retransmits message later.
 - Example: financial transaction can be conducted multiple times by the hacker
- Often used to bypass authentication mechanisms
- Prevented by encrypting traffic, cryptographic authentication, and time-stamping messages.
 - A portion of the certificate or ticket should include a date/time stamp or an expiration date/time.
 - This should be encrypted as part of the ticket or certificate.
 - Later replay proves useless – it will be rejected as expired.

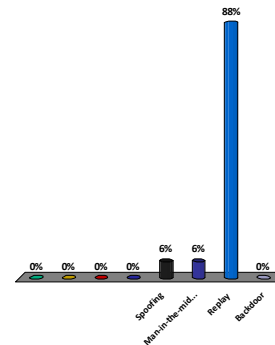


TCP/IP Hijacking

- TCP/IP hijacking and session hijacking
 - Processes of taking control of an already existing session between a client and a server.
- When the authentication sequence is complete, the attackers take over the session.
 - They can carry on as if they, and not the user, had authenticated with the system.
- As the user has already authenticated and established the session.
 - The advantage of hijacking over penetration of a computer system or network is that **the attacker does not have to circumvent any authentication mechanisms.**
- Hijack attacks generally are used against web and Telnet sessions.

In what type of attack does an attacker resend the series of commands and codes used in a financial transaction to cause the transaction to be conducted multiple times?

- 1.
- 2.
- 3.
- 4.
5. Spoofing
6. Man-in-the-middle
7.  Replay
8. Backdoor



Drive-by Download Attack

- Browsers are used to navigate the Internet
 - Some of these files are images, some are scripts, and some are text based, and together they form the web pages that we see.
 - Users don't ask for each component—it is the job of the browser to identify the needed files and fetch them.
- Drive-by download attack
 - A new type of attack called a takes advantage of this process by initiating downloads of malware, whether a user clicks it or not.
 - Unsolicited malware downloads
 - May be hidden in legitimate ads or hosted from web sites that prey on unaware users



Phishing and Pharming

- Phishing
 - Fraudulent e-mails designed to trick users into divulging confidential information

- Pharming
 - Fake web sites created to elicit authentic user credentials



Attacks on Encryption

- Cryptography
 - The art of “secret writing.”
 - Encryption is the process of transforming plaintext into an unreadable format known as ciphertext using a specific technique or algorithm.

- Cryptanalysis
 - The process of attempting to break a cryptographic system.
 - It is an attack on the method used to encrypt the plaintext.



Attacks on Encryption

- Cryptanalysis attempts to crack encryption
- Common methods
- Weak keys
- Exhaustive search of key space
- Indirect attacks



Password Attacks

- Password attack methods
 - Guess
 - Dictionary
 - Brute force
 - Hybrid
 - Birthday



Password Guessing

- The least technical of the various password-attack techniques
 - The attacker simply attempting to guess the password of an authorized user of the system or network.
- Password guessing is possible due to poor passwords.
 - Users select passwords they can remember.
 - When choosing a password, many users select:
 - Birthday
 - Mother's maiden name
 - Spouse's name
 - Child's name
 - The userid itself



Dictionary Attack

- A method of determining passwords is to use a password-cracking program.
 - These programs use a dictionary of words.
 - The words can be used by themselves, or two or more smaller ones may be combined to form a single possible password.
 - The programs often permit the attacker to create various rules that tell the program how to combine words to form new possible passwords.
- Sometimes, users substitute numbers for specific letters.
- Rules can also be defined so that the cracking program will substitute special characters for other characters, or combine words together.



Brute-Force Attack

- Password-cracking program attempts all possible password combinations.
- The length of the password and the size of the set of possible characters in the password affects the time a brute-force attack will take.
- Increased computer speed reduces the time it takes to generate password combinations.
 - It is more feasible to launch brute-force attacks against computer systems and networks.
- Take place at two levels.
 - An attack on a system with the attacker attempting to guess the password at the login prompt.
 - The attack can be made more difficult by locking the account after a few failed login attempts.
 - An attack against the list of passwords contained in a password file.
 - The password file must be maintained securely, so that others may not obtain a copy of it.

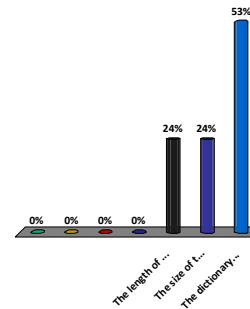


Birthday Attack

- The birthday attack is a special type of brute-force attack.
 - The attack gets its name from something known as the birthday paradox.
 - In a group of at least 23 people, the possibility that there will be two individuals with the same birthday is greater than 50 percent.
 - Mathematically, we can use the equation $1.2k^{1/2}$ (with k equal to the size of the set of possible values).
 - In the birthday paradox, k would be equal to 365 (the number of possible birthdays).
- This same phenomenon applies to passwords, with k just being quite a bit larger.

An attacker's ability to crack passwords is directly related to the method the user employed to create the password, as well as

- 1.
- 2.
- 3.
- 4.
5. The length of the password
6. The size of the character set used in generating the password
7. The dictionary and rules used by the cracking program



Software Exploitation

- An attack that takes advantage of bugs or weaknesses in software is referred to as software exploitation.
 - These weaknesses can be the result of
 - poor design
 - inadequate testing
 - bad coding practices.
- Buffer Overflow
 - A common weakness that has been exploited on a number of occasions is buffer overflows.
 - A buffer overflow occurs when a program is provided more data for input than it was designed to handle.
 - Allows programs to write to unauthorized sections of memory.



Wardialing and WarDriving

- Wardialing :
 - An attacker's attempt to discover unprotected modem connections to computer systems and networks.
 - Successful because of rogue modems which are unauthorized modems attached to computers by authorized users.
 - New technology has been developed to address this common backdoor into corporate networks.
 - Telephone firewalls block unauthorized modem connections into an organization.
- WarDriving
 - The activity where attackers wander throughout an area (often in a car) with a computer with wireless capability, searching for wireless networks they can access.
 - Recently increased due to the increase in the use of wireless networks.



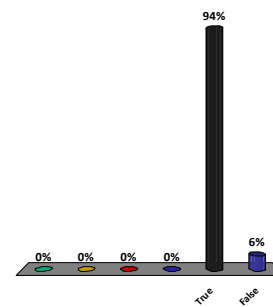
Social Engineering

- Social engineering
 - Depends on lies and misrepresentation.
 - Attackers trick authorized users to obtain information or access to which they would not be entitled.
- Social engineering also applies to physical access.
 - Poor security practices may allow physical access to an office.
 - With a little unsupervised time, a userid and password pair might be found on a notepad or sticky note.

An attack in which an attacker attempts to lie and misrepresent himself in order to gain access to information that can be useful in an attack is known as Social engineering

- 1.
- 2.
- 3.
- 4.
5. 😊
- 6.

True
False



Malicious Code

- Viruses
- Trojan horses
- Spyware
- Logic bombs
- Rootkits
- Worms
- Zombies and botnets



Malware

- Software That Is Bad For You
- The term Malware (malicious code) is software designed for a nefarious purpose.
 - It may cause damage to a system by:
 - Deleting all files.
 - Modifying the operating system.
 - Creating a backdoor in the system to grant access to unauthorized individuals.



Viruses

- Virus
 - A type of malicious code that replicates by attaching itself to an authorized piece of executable code.
 - When the authorized code is executed, the virus executes.
 - It has the opportunity to infect other files and perform any other nefarious actions it is designed to do.
 - The specific way that a virus infects other files, and the type of files it infects, depends on the type of virus.
- Common types:
 - Boot Sector virus
 - Program virus
 - Macro virus
 - Stealth virus
 - Polymorphic virus



Virus

- **A boot sector virus**
 - Infects the boot sector portion of either a floppy disk or a hard drive.
 - When a computer is first turned on, a small portion of the operating system is loaded from the hardware.
 - This small operating system then loads the rest of the operating system from a specific location (sector) on either the floppy or the hard drive.

- **Program virus**
 - Attaches itself to executable files.
 - It attaches itself to files ending in .exe or .com on Windows-based systems.
 - The virus is attached in such a way that it executes before the program.



Stealth and Polymorphic Virus

- **Stealth and polymorphic virus**
 - Made it more difficult for antivirus software to do their job.

- **Stealth virus**
 - Employs techniques to evade being detected by antivirus software that uses checksums or other techniques.

- **Polymorphic viruses**
 - Evade detection by changing the virus itself (the virus “evolves”).
 - Since the virus changes, signatures for that virus may no longer be valid.
 - The virus may escape detection by antivirus software.



Avoiding Virus Infection

- Good Practices:
 - Being cautious about executing programs or opening documents.
 - Not opening programs or documents, if the source is unknown.

- Antivirus Software
 - Another security practice for protecting against virus infection is to install and run an antivirus program.



Virus Hoaxes

- Virus hoaxes
 - Inform people about a new virus and the extreme danger it poses.

 - Hoaxes can actually be even more destructive than just wasting time and bandwidth.
 - Some hoax warnings include instructions to delete certain files if found on the user's system.
 - These files may actually be part of the operating system and deleting them could keep the system from booting properly.



Trojan Horses

- Trojan horse (Trojan)
 - A piece of software that appears to do one thing but that hides another action.
 - A stand-alone program that must be copied or installed by the user.
 - The challenge for the attacker is enticing the user to copy and run the program.
 - The program must be disguised as something that the user would want to run.
 - Once the Trojan has been copied and executed, it is “inside” the system.

 - The best method to prevent a Trojan from entering a system is:
 - Never run software if unsure of its origin, security, and integrity.
 - Using a virus-checking program




Spyware

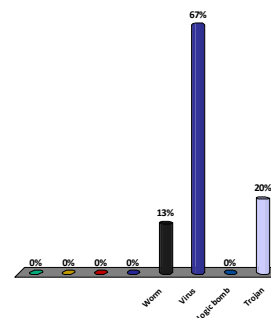
- Spyware
 - Software capable of recording and reporting a users actions:
 - Typically installed unbeknownst to users
 - Monitors software and system use
 - Can steal information through keylogging
 - Many states have banned spyware and other unauthorized software:

Logic Bombs

- Logic bomb
 - A type of malicious software deliberately installed by an authorized user.
 - Sits dormant until some event invokes its often-malicious payload.
 - If the trigger is some event, such as not finding a specific name in the personnel file, the code is referred to as a logic bomb.
 - If the event is a specific date or time, the program will often be referred to as a time bomb.
 - Difficult to detect since they are installed by authorized users who might even be administrators responsible for security.
- Countermeasure
 - Separation of duties.
 - Periodic review of all programs and services that are running.
 - An active backup program

A piece of malicious code that must attach itself to another file to replicate itself is known as:

- 1.
- 2.
- 3.
- 4.
5. Worm
6.  Virus
7. Logic bomb
8. Trojan



A piece of malicious code that appears to be designed to do one thing (and may in fact do that thing) but that hides some other payload (often malicious) is known as:

- 1.
- 2.
- 3.
- 4.
5. Worm
6. Virus
7. Logic bomb
8. Trojan

Malicious Code Type	Percentage
Worm	6%
Virus	0%
Logic bomb	6%
Trojan	88%

Worms

- A worm is a code that attempts to penetrate networks and computer systems.
 - Once penetration occurs, the worm creates a copy of itself on the penetrated system.
- Reproduction of a worm, unlike a virus, does not rely on the attachment of the virus to another piece of code or a file.
 - The blurring of the distinction between viruses and worms has come about because of the attachment of malicious code to e-mail.
- The important distinction, however, is whether the code has to attach itself to something else (a virus), or if it can “survive” on its own (a worm).



The Morris Worm

- The most famous example of a worm was the Morris worm in 1988.
 - Also referred to as the Internet worm, because of its effect on the early Internet
 - the worm was able to insert itself into so many systems connected to the Internet that it has been repeatedly credited with “bringing the Internet to its knees” for several days.
- **The Morris worm was created by a graduate named Robert Morris.** His father was a scientist at NSA.
 - It used several known vulnerabilities to gain access to a system.
 - It also relied on password guessing to obtain access to accounts.



The Morris Worm

- Once a system had been compromised, a small program was inserted into the new system and executed.
 - This program downloaded the rest of the worm system.
 - The worm had stealth characteristics to make it harder to determine what it was doing.
- The worm would not be loaded if a copy of it was on a system.
 - It periodically ignored this check to ensure that the worm could not be easily eliminated.
- Interconnected systems were constantly re-infected.
 - Eventually, systems were running so many copies of the worm that the system response time ground to a stop.



Code-Red

- On July 19, 2001, the Code-Red worm infected over 350,000 computers connected to the Internet in only 14 hours.
- It cost more than \$2.5 billion.
- Lessons from the Code-Red worm are as applicable today as they were in 2001.
 - The exploited vulnerability was not revealed as a result of the attack.
 - The vulnerability had been known for a month.
 - The worm was memory resident.
 - Turning the machine off will eliminate the worm.
 - Unless the system is patched, it is likely to be re-infected after reconnecting to the Internet.



Code-Red Version 1

- The worm did not carry a malicious payload.
 - If the date were between the first and nineteenth of the month, the worm would generate a random list of IP addresses to infect them.
 - It used the same seed for the random number generator so each system actually generated the same list of IP addresses.
 - If the date were between the 20th and 28th of the month, it launched a Denial-of-Service attack against a Web site owned by the White House.
 - After the 28th, the worm remained dormant until the 1st of the next month.



Code-Red Version 2

- The second version of the worm was released on July 19th, 2001.
 - The second version of the worm used new seeds and caused a different list of random IP addresses to be created.
- Additional problems were seen with the second version since routers, switches, and other networked devices were still unable to handle the data volume causing many of them to crash or reboot.



Slammer

- On Saturday, January 25, 2003, the Slammer was released.
 - It exploited a buffer overflow vulnerability in computers running various forms of Microsoft's SQL Server.
- By the next day, it had infected at least 120,000 hosts and caused network outages and disruption of airline flights, elections, and ATMs.
 - Slammer-infected hosts generated a reported 1 terabit of worm-related traffic every second.
 - The worm doubled in the number of infected hosts every 8 seconds.



Slammer

- It took less than ten minutes to reach global proportions and infect 90 percent of the possible hosts.
 - Once a machine was infected, the host would start selecting targets randomly and sending packets to them to attempt infection at a rate of 25,000 per second.
- Like Code-Red, Slammer did not contain a malicious payload.
 - It caused a massive overload on networks, which could not sustain the traffic being generated by the thousands of infected hosts.
- The worm sent its single packet to UDP port 1434.
 - Blocking this port provided a fix for networks.



Protection Against Worms

- Key steps:
 - Install all patches.
 - Use firewalls.
 - Enforce good password security
 - Implement an intrusion detection system.
 - Eliminate unnecessary services.
 - Use extreme caution with e-mail attachments.



Malware Defense

- Attacks typically exploit multiple vulnerabilities
 - Network, OS, application, and user level
- Steps to prevent malware
 - Use an antivirus program.
 - Ensure all software is up-to-date.



Auditing

- Auditing:
 - It is the process of assessing the security state of an organization against an established standard.
 - Measure how effective deployed countermeasures actually are in mitigating previously identified risks.
 - Helps ensure that employees follow established procedures and guidelines.
 - An important element in auditing is the standard that is used to evaluate personnel and procedures.
 - Organizations from different communities have widely different standards.
 - Any audit needs to consider the appropriate elements for the specific community.
 - FIRPA
 - HIPAA



Security Auditing


- Should be conducted on a regular basis
- May be mandated depending on the industry
- Can be contracted out to a another party

- Focus on
 - Security perimeter
 - Policies, procedures, and guidelines governing security
 - Employee training



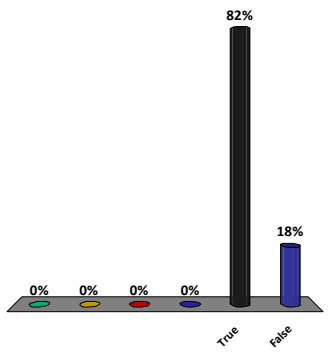
Auditing

- Penetration tests
 - They are conducted against systems to find any holes in security.
 - Penetrate the security rather than measuring it against some standard.
 - Penetration tests are viewed as white-hat hacking.
 - Methods used often mirror those that an attacker might use.
- Conduct some security audit or assessment on a regular basis.
 - Many things may be evaluated during an assessment.
 - The security perimeter.
 - All components, including host-based security.
 - The organization's policies, procedures, and guidelines governing security.
- Employee Training



Auditing is the process of assessing the security state of an organization against an established standard

- 1.
- 2.
- 3.
- 4.
5. True
6. False



Response	Percentage
True	82%
False	18%
Other 1	0%
Other 2	0%
Other 3	0%
Other 4	0%