ATTACKS AND MALICIOUS SOFTWARE

DR. ZIA UR REHMAN

DENIAL-OF-SERVICE ATTACK

- A **denial-of-service (DoS) attack** is an attack designed to prevent a system or service from functioning normally.
  - Can exploit a known vulnerability in a specific application or operating system
  - Can attack features (or weaknesses) in specific protocols or services
  - Attempts to deny authorized users access either to specific information or to the computer system or network itself

DENIAL-OF-SERVICE ATTACK (*CONTINUED*)

- A **SYN flood** attack can be used to prevent service to a system temporarily in order to take advantage of a trusted relationship that exists between that system and another.
  - Illustrates basic principles of most DoS attacks
  - Exploits weakness inherent to the TCP/IP protocol
  - Uses TCP three-way handshake to flood a system with faked connection requests

DENIAL-OF-SERVICE ATTACK (*CONTINUED*)

- TCP three-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.

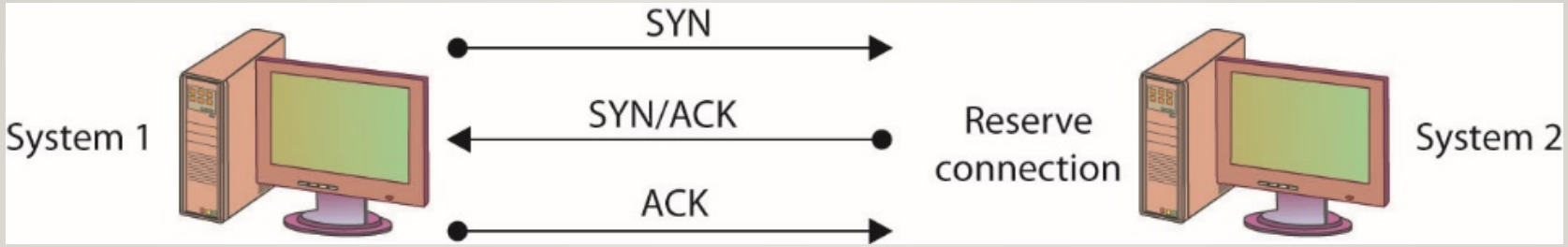

Figure 15.1 The TCP three-way handshake

DENIAL-OF-SERVICE ATTACK (*CONTINUED*)

- Steps of a SYN flood attack
  - Communication request sent to target system.
  - Target responds to faked IP address.
  - Target waits for non-existent system response.
  - Request eventually times out.
  - If the attacks outpace the requests timing-out, then systems resources will be exhausted.

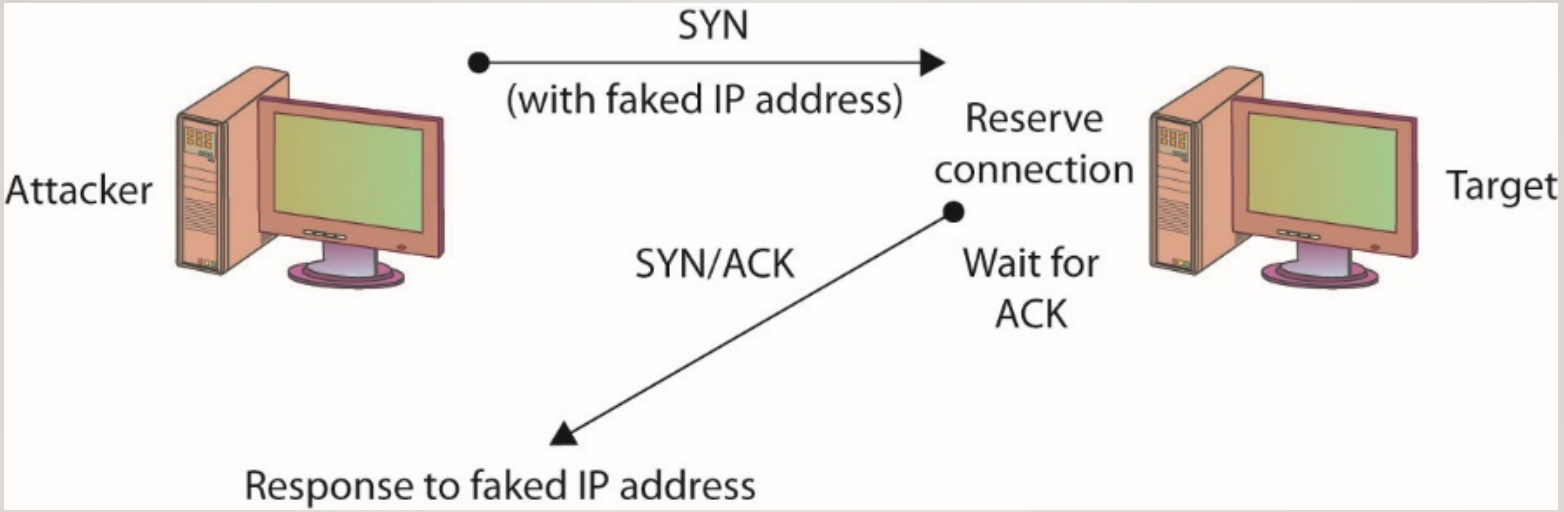

Figure 15.2 A SYN flooding–based DoS attack

DENIAL-OF-SERVICE ATTACK (*CONTINUED*)

- Another simple DoS attack is the infamous ping of death (POD).
  - POD targets a specific application or operating system.
  - Reminder: SYN flooding targets a protocol.
  - In the POD attack, the attacker sends an Internet Control Message Protocol (ICMP) ping packet equal to, or exceeding, 64KB.
  - Certain older systems are not able to handle this size of packet, and the system will hang or crash.

DENIAL-OF-SERVICE ATTACK (*CONTINUED*)

- A DoS attack employing multiple attacking systems is known as a **distributed denial-of-service (DDoS) attack**.
  - Denies access or service to authorized users
  - Uses resources of many systems combined into an attack network
  - Overwhelms target system or network
    - With enough attack agents, even simple web traffic can quickly affect a large website

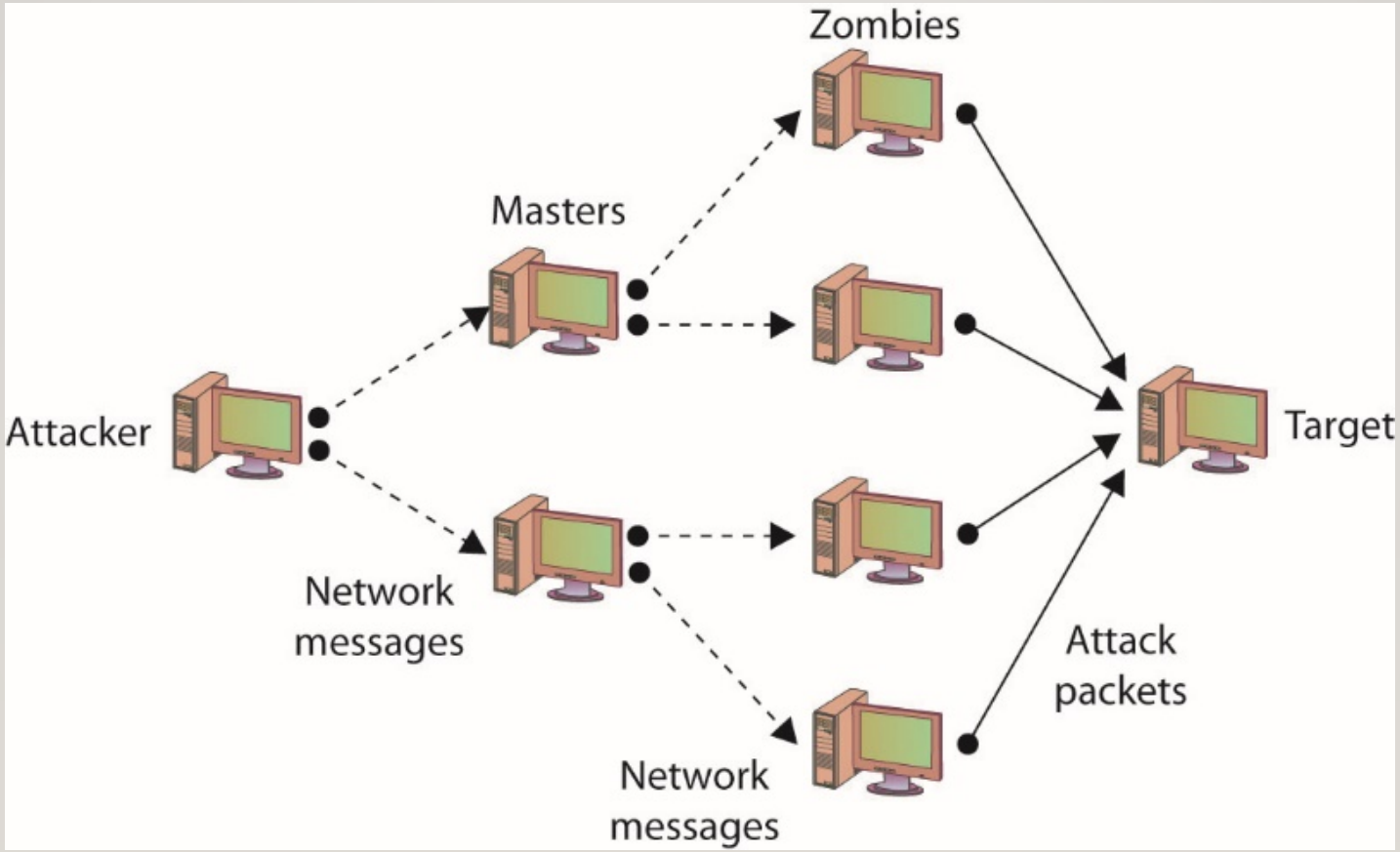

Figure 15.3 DDoS attack

DENIAL-OF-SERVICE ATTACK (*CONTINUED*)

- Smurf attack
  - In a specific DoS attack known as a *smurf attack*, the attacker sends a spoofed packet to the broadcast address for a network, which distributes the packet to all systems on that network.
  - Further details are listed in the IP Address Spoofing section.

DENIAL-OF-SERVICE ATTACK (*CONTINUED*)

- Defending against DOS-type attacks
  - Ensure you have applied the latest patches and upgrades to your systems and the applications running on them.
  - Change the time-out option for TCP connections so that attacks such as the SYN flooding attack are more difficult to perform.
  - For DDoS attacks, distribute your workload across several systems.
  - To prevent a DDoS attack, you must either be able to intercept or block the attack messages or keep the DDoS network from being established in the first place.

DENIAL-OF-SERVICE ATTACK (*CONTINUED*)

- *War-dialing* is the term used to describe an attacker's attempt to discover unprotected modem connections to computer systems and networks.
  - War-dialing was surprisingly successful, mostly because of *rogue modems*—unauthorized modems attached to computers on a network by authorized users.
- *War-driving* is the unauthorized scanning for and connecting to wireless access points.
  - Frequently done while driving near a facility

SOCIAL ENGINEERING

- Social engineering relies on lies and misrepresentation, which an attacker uses to trick an authorized user into providing information or access the attacker would not normally be entitled to.
- Social engineering examples include:
  - Contacting a system administrator and pretending to be an authorized user, asking to have a password reset
  - Posing as a representative from a vendor who needs temporary access to perform some emergency maintenance

SNIFFING

- **Sniffing** is when someone examines all the network traffic that passes their NIC, whether addressed for them or not.
  - A network sniffer is a software or hardware device.
    - The device can be used to view all traffic, or it can target a specific protocol, service, or even string of characters.
  - *Sniffers* may be able to modify some or all traffic in route
  - Network administrators can use a sniffer to monitor and troubleshoot network performance.

SNIFFING

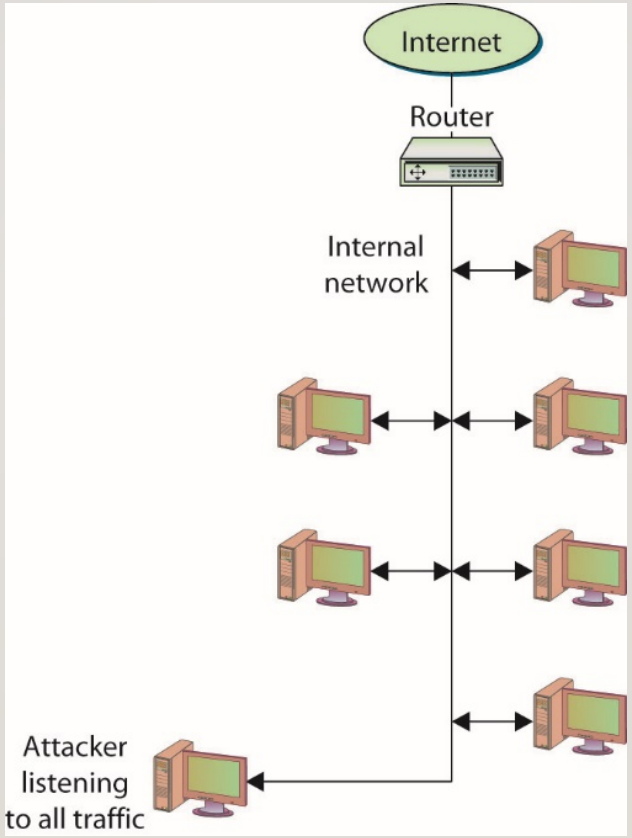

Figure 15.4 Network sniffers listen to all network traffic.

SPOOFING

- **Spoofing** is nothing more than making data look like it has come from a different source.
  - Spoofing is possible in TCP/IP because of the friendly assumptions behind the protocols.
    - Protocol assumed that individuals who had access to the network layer would be privileged users who could be trusted.

SPOOFING (*CONTINUED*)

- Spoofing e-mail
  - Occurs when a message is sent with a From address that differs from that of the sending system.
- E-mail spoofing examples
  - Telnet to port 25 on a mail server – From there, you can fill in any address for the From and To sections of the message, whether or not the addresses are yours or even actually exist.
  - E-mail spoofing variation – Attackers acquire a URL similar to the URL they want to spoof so that e-mail sent from their system appears to have come from the official site.

SPOOFING (*CONTINUED*)

- IP address spoofing
  - This occurs when a system inserts a different address in the From portion of the IP packet.
  - In a specific DoS attack known as a **smurf attack**, the attacker sends a spoofed packet to the broadcast address for a network, which distributes the packet to all systems on that network.

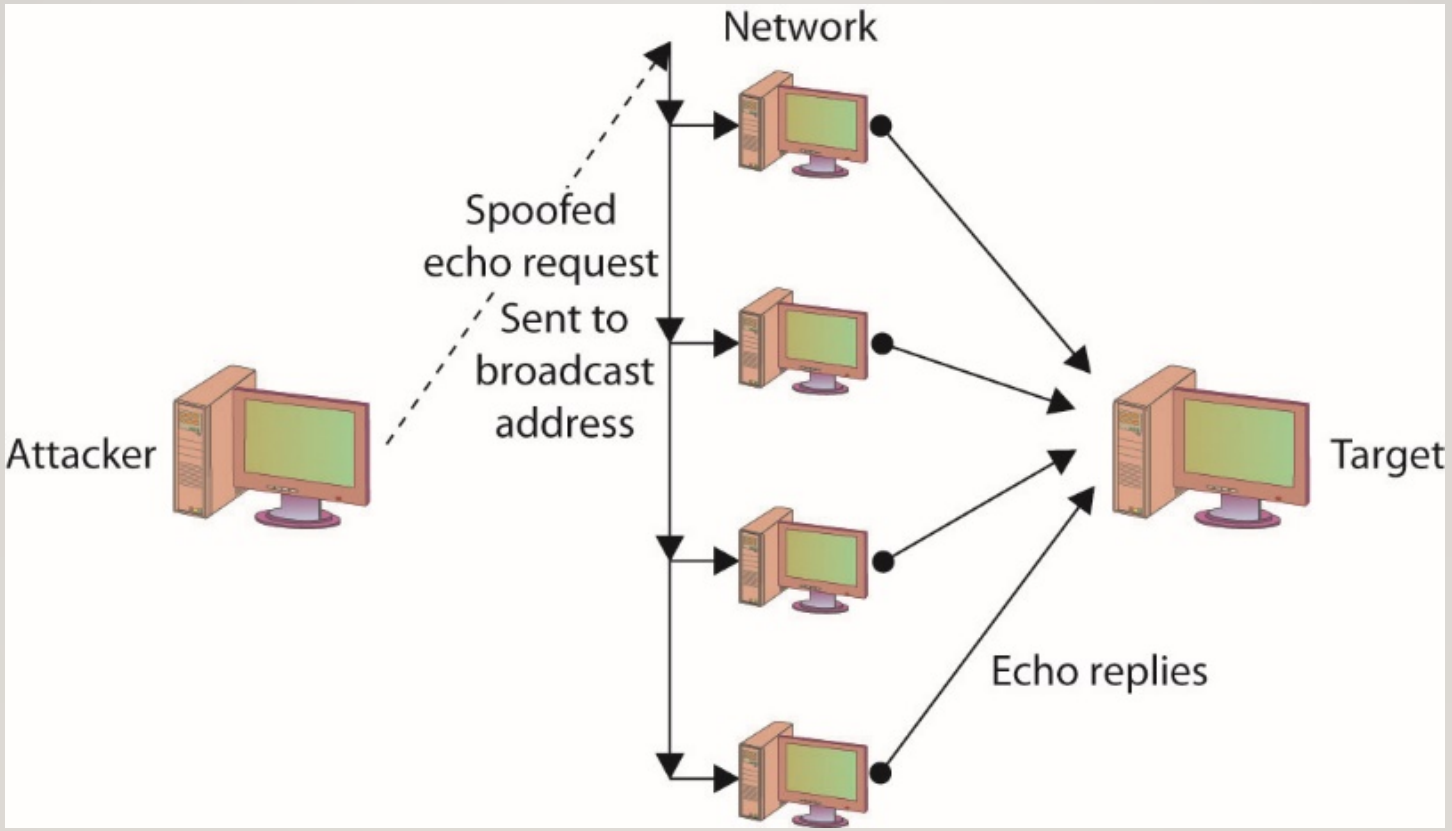

Figure 15.5 Smurfing used in a smurf DOS attack

SPOOFING (*CONTINUED*)

- Spoofing and trusted relationships
  - If two systems are configured to accept the authentication accomplished by each other, an individual logged onto one system might not be forced to go through an authentication process again to access the other system.
  - An attacker can take advantage of this arrangement 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.

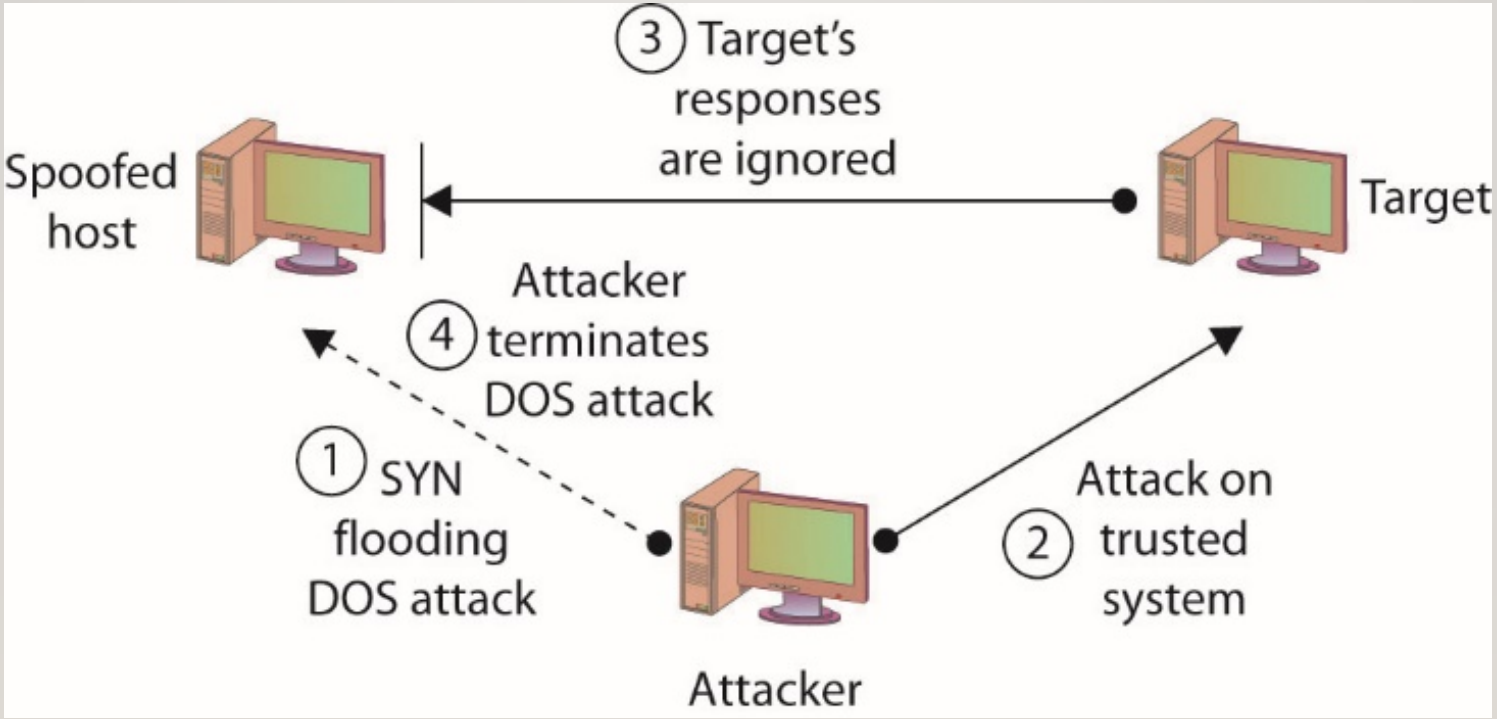

Figure 15.6 Spoofing to take advantage of a trusted relationship

SPOOFING (*CONTINUED*)

- Spoofing and sequence numbers
  - Formulating packets is more complicated for external attackers because of sequence number.
  - A **sequence number** is a 32-bit number established by the host that is incremented for each packet sent.
    - Packets are not guaranteed to be received in order; the sequence number can be used to help reorder packets.
  - The difference in the difficulty of attempting a spoofing attack from inside a network and from outside involves determining the sequence number.

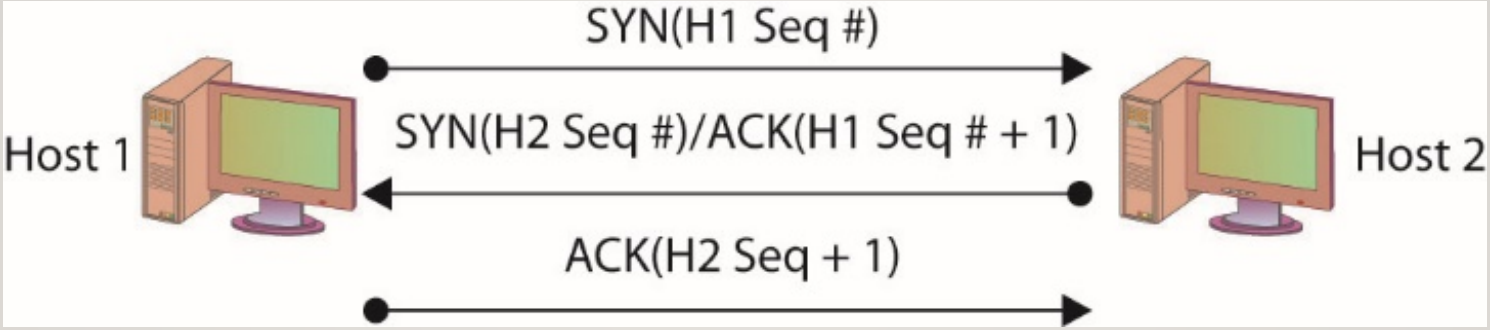

Figure 15.7 Three-way handshake with sequence numbers

TCP/IP HIJACKING

- **TCP/IP hijacking** and session hijacking are terms used to refer to the process of taking control of an already existing session between a client and a server.
  - Attacker does not have to circumvent any authentication mechanisms.
  - Attack can be disguised with a DoS attack.
  - Hijack attacks generally are used against web and Telnet sessions.

MAN-IN-THE-MIDDLE ATTACKS

- A **man-in-the-middle attack** generally occurs when attackers are able to place themselves in the middle of two other hosts that are communicating.
  - Attack is typically accomplished by compromising a router to alter the path of the traffic.
  - A common method of instantiating a man-in-the-middle attack is via session hijacking.
  - Session hijacking can occur when information such as a cookie is stolen, allowing the attacker to impersonate the legitimate session.
    - Can result from a cross-site scripting attack

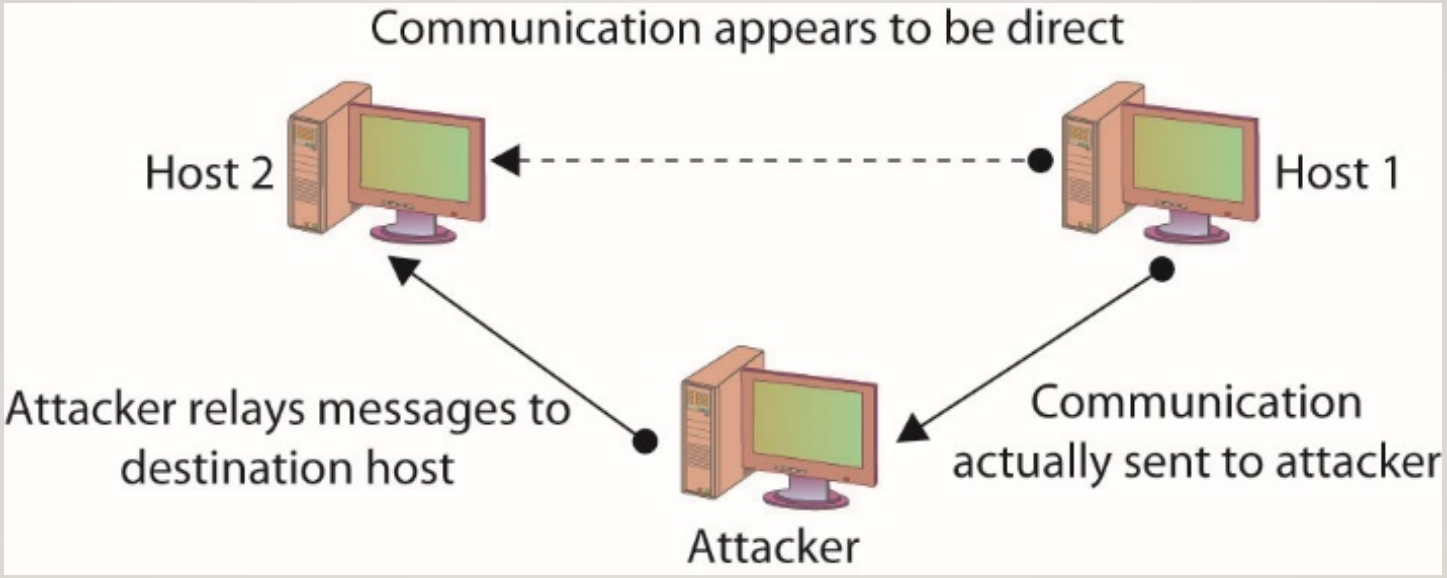

Figure 15.8 A man-in-the-middle attack

MAN-IN-THE-MIDDLE ATTACKS (*CONTINUED*)

- The term "man-in-the-middle attack" is sometimes used to refer to a more specific type of attack—one in which the encrypted traffic issue is addressed.
  - An attacker can conduct a man-in-the-middle attack by intercepting a request for a friend's public key and the sending of your public key to him.
  - Well-designed cryptographic products use techniques such as mutual authentication to avoid this problem.

REPLAY ATTACK

- A **replay attack** occurs when the attacker captures a portion of a communication between two parties and retransmits it at a later time.
  - Replay attacks are associated with attempts to circumvent authentication mechanisms.
  - The best way to prevent replay attacks is with encryption, cryptographic authentication, and time stamps.

TRANSITIVE ACCESS

- *Transitive access* is a means of attacking a system by violating the trust relationship between machines.
- A simple example is when servers are well protected and clients are not, and the servers trust the clients.
  - In this case, attacking a client can provide transitive access to the servers.

SPAM

- Though not generally considered a social engineering issue, nor a security issue for that matter, spam can, however, be a security concern.
  - Spam is bulk unsolicited e-mail.
  - It can be legitimate in the sense that it has been sent by a company advertising a product or service.
  - Spam can also be malicious and could include an attachment that contains malicious software designed to harm your system, or a link to a malicious web site that may attempt to obtain personal information from you.

SPIM

- Though not as well known, a variation on spam is *spim*, which is basically spam delivered via an instant messaging application such as Yahoo! Messenger or AOL Instant Messenger (AIM).
- The purpose of hostile spim is the same as that of spam—the delivery of malicious content or links.

PHISHING

- **Phishing** is the use of fraudulent e-mails or instant messages that appear to be genuine but are designed to trick users.
- The goal of a phishing attack is to obtain from the user information that can be used in an attack, such as login credentials or other critical information.

SPEAR PHISHING

- **Spear phishing** is the term that has been created to refer to a phishing attack that targets a specific group with something in common.
- By targeting a specific group, the ratio of successful attacks (that is, the number of responses received) to the total number of e-mails or messages sent usually increases because a targeted attack will seem more plausible than a message sent to users randomly.

VISHING

- *Vishing* is a variation of phishing that uses voice communication technology to obtain the information the attacker is seeking.
  - Vishing takes advantage of the trust that some people place in the telephone network.
  - Users are unaware that attackers can spoof (simulate) calls from legitimate entities using voice over IP (VoIP) technology.
  - Voice messaging can also be compromised and used in these attempts.
  - Attackers seek to obtain information for identity theft.

PHARMING

- **Pharming** consists of misdirecting users to fake web sites that have been made to look official.
  - Users directed to the fake web site as a result of activity such as DNS poisoning or modification of local host.
  - Once at the fake web site, the user may supply personal information, believing that they are connected to the legitimate site.

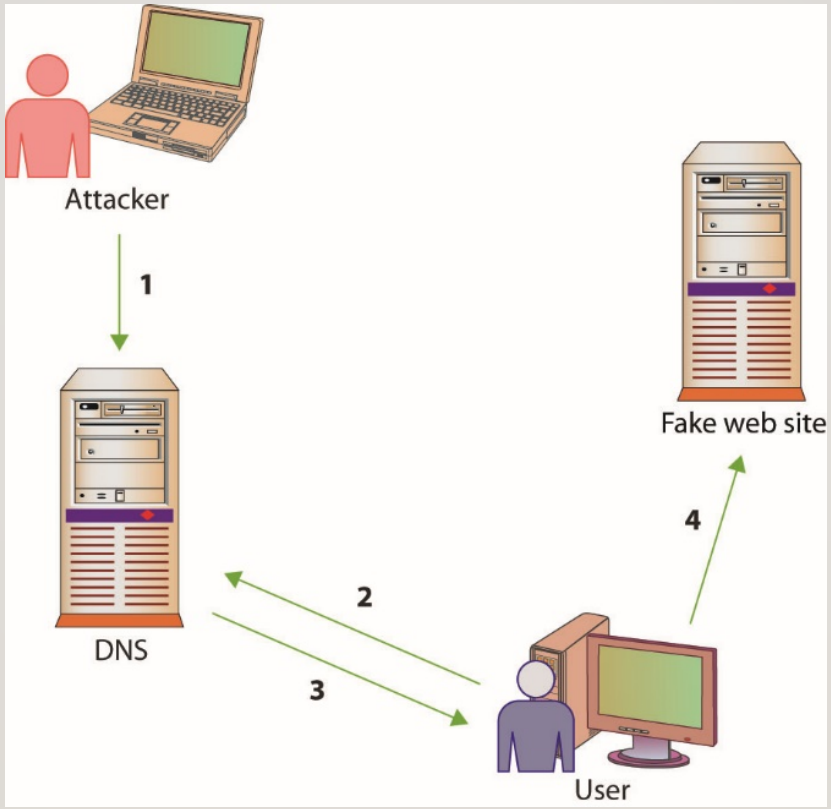

Figure 15.9 How pharming works

SCANNING ATTACKS

- Scanners can be used to send specifically crafted packets in an attempt to determine TCP/UDP port status.
- An XMAS scan uses the URG, PSH, and FIN flags to determine TCP port availability.
  - If the port is closed, an RST is returned.
  - If the port is open, there is typically no return.
- Advanced firewalls can detect these packets, alerting people to the scanning activities.

ATTACKS ON ENCRYPTION

- *Encryption* is the process of transforming *plaintext* into an unreadable format known as *ciphertext* using a specific technique or algorithm.
- Most encryption techniques use some form of key in the encryption process.
- *Cryptanalysis* is the process of attempting to break a cryptographic system—it is an attack on the specific method used to encrypt the plaintext.
- Cryptographic systems can be compromised in various ways.

ATTACKS ON ENCRYPTION (*CONTINUED*)

- Certain encryption algorithms may have specific keys that yield poor, or easily decrypted, ciphertext.
- An exhaustive search of the keyspace will decrypt the message.
  - The strength of the encryption method is related to the sheer size of the keyspace.
  - You cannot immediately compare different key lengths from different algorithms and assume relative strength.

ATTACKS ON ENCRYPTION (*CONTINUED*)

- One of the most common ways of attacking an encryption system is to find weaknesses in mechanisms surrounding the cryptography.
  - It is not the cryptographic algorithm itself that is being attacked, but rather the implementation of that algorithm in the real world.

ADDRESS SYSTEM ATTACKS

- IP addresses and other addresses can be manipulated.
- **DNS kiting**, is an economic attack against the terms of using a new DNS entry.
- Another twist on this scheme is the concept of domain name front running, where a registrar places a name on a five-day hold after someone searches for it, and then offers it for sale at a higher price.

CACHE POISONING

- Caches can also be poisoned, sending incorrect information to the end user's application, redirecting traffic, and changing system behaviors.

CACHE POISONING (*CONTINUED*)

- A DNS poisoning attack occurs when network connections are changed, resulting in different DNS lookups.
  - DNS poisoning can occur at any level.
  - At times, **nslookup** will return a nonauthoritative answer.
  - DNS poisoning is a variant of a larger attack class referred to as *DNS spoofing*, in which an attacker changes a DNS record through any of a multitude of means.

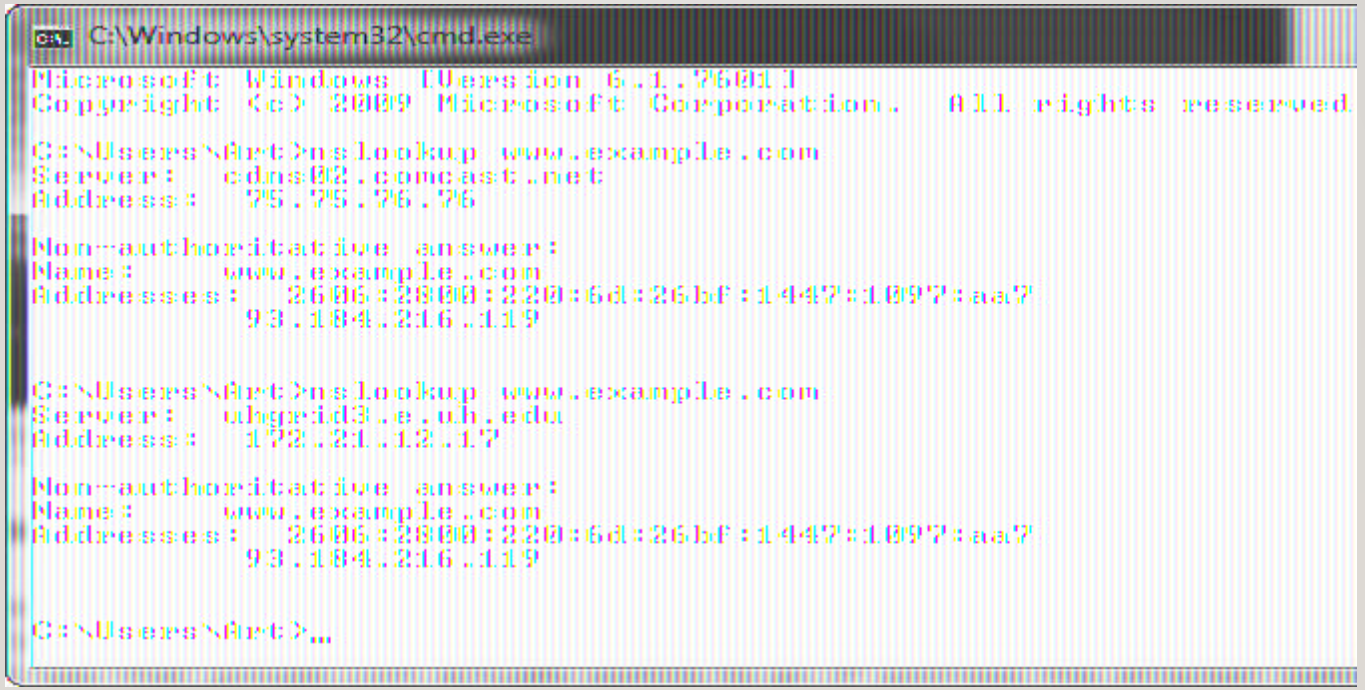

Figure 15.10 nslookup of a DNS query

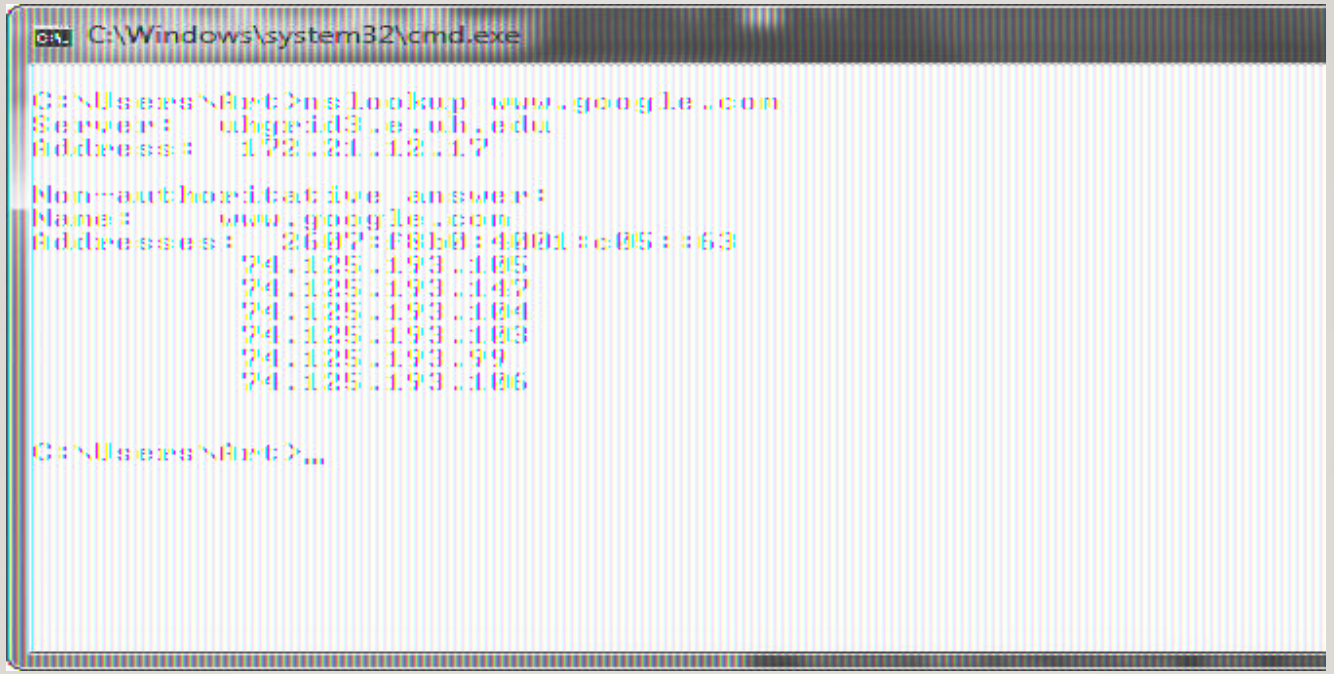

Figure 15.11 Cache response to a DNS query

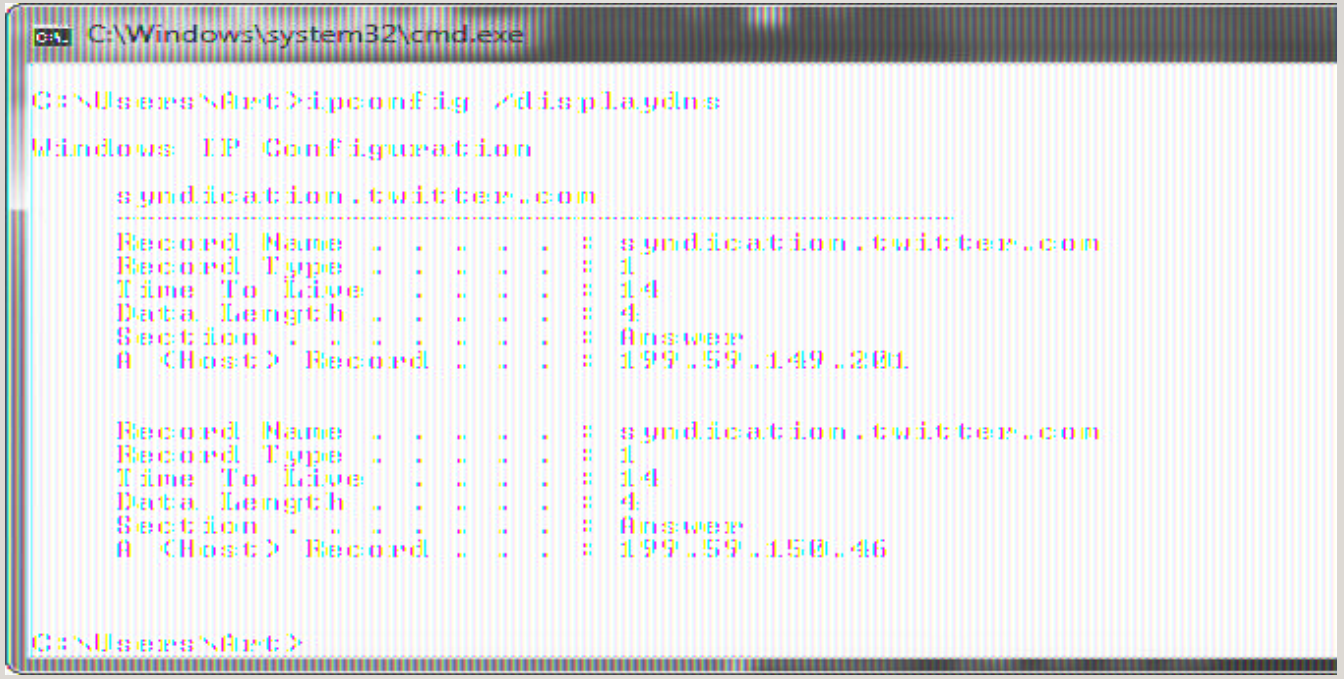

Figure 15.12 Cache response to a DNS table query

CACHE POISONING (*CONTINUED*)

- ARP poisoning involves an attacker sending messages, corrupting the ARP table, and causing packets to be misrouted.
  - This form of attack results in malicious address redirection.
  - This can allow a mechanism whereby an attacker can inject themselves into the middle of a conversation between two machines, a man-in-the-middle attack.
  - Local MAC addresses can also be poisoned in the same manner, although it is called ARP poisoning.

PASSWORD GUESSING

- The most common form of authentication is the user ID and password combination
- While it is not inherently a poor mechanism for authentication, the combination can be attacked in several ways.
- All too often, these attacks yield favorable results for the attacker not as a result of a weakness in the scheme but usually due to the user not following good password procedures.

PASSWORD GUESSING (*CONTINUED*)

- People are notorious for picking poor passwords.
  - Users need to select a password that they can remember, so they create simple passwords.
  - The attacker just needs to obtain a valid user ID and some information about the user before guessing can begin.
- A password-cracking program can uses a list of dictionary words to try to guess the password.
  - Rules can also be defined so that the cracking program will substitute special characters for other characters or combine words.

PASSWORD GUESSING (*CONTINUED*)

- In a brute-force attack, a password-cracking program attempts all possible character combinations.
- There are two levels of brute-force attack:
  - Use a password-cracking program to attempt to guess the password directly at a login prompt
  - Steal a password file and use a password-cracking program to compile a list of possible passwords based on the list of password hashes contained in the password file (offline)
    - Use narrower list to attempt to guess the password at the login prompt

PASSWORD GUESSING (*CONTINUED*)

- A hybrid password attack is an attack that combines the preceding dictionary and brute-force methods.
- The **birthday attack** is a special type of brute-force attack
  - Uses the *birthday paradox* that states that in a group of at least 23 people, the chance that two individuals will have the same birthday is greater than 50 percent.
    - Mathematically, the equation is $1.25 \times k^{1/2}$, where k equals the size of the set of possible values, which in the birthday paradox is 365

PASS-THE-HASH ATTACKS

- Pass the hash is a hacking technique where the attacker captures the hash used to authenticate a process.
- The attacker can then use this hash by injecting it into a process in place of the password.
- This is a highly technical attack, targeting the Windows authentication process, injecting a copy of the password hash directly into the system.
- The attacker does not need to know the password.

SOFTWARE EXPLOITATION

- *Software exploitation* is an attack that takes advantage of bugs or weaknesses in software.
  - Can be the result of poor design, poor testing, or poor coding practices
  - Can result from what are sometimes called "features"
  - A preventable problem
    - *Fuzzing:* the automated process of applying large sets of inputs to a system and analyzing the output to determine exploitable weaknesses
  - Can exploit error messages from applications

SOFTWARE EXPLOITATION (*CONTINUED*)

- A common weakness that has often been exploited is a **buffer overflow**, which occurs when a program is provided more data for input than it was designed to handle.
- An **integer overflow** is a programming error condition that occurs when a program attempts to store a numeric value, an integer, in a variable that is too small to hold it.