CompTIA Security+

3.0 Threats and Vulnerabilities

Categories of Attackers

- Malicious Insiders (Snowden)
- Electronic Activists (“Hacktivists”) (Anonymous)
- Data Thief (Corporate Espionage)
- Script Kiddie
- Electronic Vandal
- Cyberterrorist

Hackers and Attackers

- White Hats
  - (Good Guys)
- Black Hats
  - (Bad Guys)
- Grey Hats
  - (Good/bad)

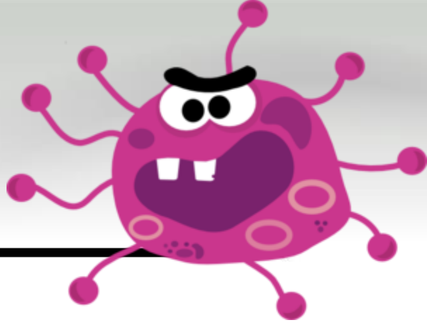
Objective 3.1

- Explain types of malware

Adware

- Advertising-supported software, or adware, is a form of spyware
- Tracking software can be installed that reports data to the company, such as your general surfing habits and which sites you have visited
- Section 5 of the FTC Act, which is codified at 15 U.S.C. § 45, provides that "Unfair methods of competition in or affecting commerce, and unfair or deceptive acts or practices in or affecting commerce, are hereby declared unlawful“
- Adware is legitimate only when users are informed up front that they will receive ads

Viruses



- A program or piece of code that runs on your computer without your knowledge
- Designed to attach itself to other code and replicate
- Replicates when an infected file is executed or launched
- It then attaches to other files, adds its code to the application’s code, and continues to spread
- Even a simple virus is dangerous because it can use all available resources and bring the system to a halt

Virus Types

- **Boot sector:** Placed into the first sector of the hard drive so that when the computer boots, the virus loads into memory
- ***Polymorphic:** alters their own code in order to avoid detection by antivirus scanners.
- **Macro:** Inserted only into a Microsoft Office document and emailed to unsuspecting users
- **Stealth:** avoids detection by masking or hiding their activities

Virus Types

- **Armored:** designed to be difficult to detect and remove
- **Retroviruses:** specifically targeted at antivirus systems to render them useless
- **Phage viruses:** modify or infect many aspects of a system so they can regenerate themselves from any remaining unremoved parts

Virus Types

- **Companion viruses:** borrows the root filename of a common executable and then gives itself the *.com* extension in an attempt to get itself launched rather than the intended application

- **Multipartite:** A hybrid of boot and program viruses. It first attacks a boot sector and then attacks system files or vice versa.

Exam Alert

- Viruses have to be executed by some type of action, such as running a program

Some Famous Virus

- **Love Bug**: Email titled “I Love You”, when the attachment was executed it sent copies to everyone listed in your address book
- Deleted files (MP3s, JPGs) and sent user info back to the attacker

- **Melissa**: 1999, a Macro virus that embedded in a Word document. Email itself to the first 50 addresses in your address book

- **Michelangelo**: Master boot record virus. Erases the content of the infected drive on March 6th every year (the birthday of Renaissance artist Michelangelo)

Worms

- Similar in function and behavior to a virus with the exception that worms are self-replicating

- Built to take advantage of a security hole in an existing application or OS and then find other systems running the same software and automatically replicate itself to the new host

- This process repeats with no user intervention

- Spreads by using email, IM, IRC, and file sharing (P2P)

Some Famous Worms

- **Morris**: 1988, used a Sendmail vulnerability and shut down the entire internet.
- **Nimda**: Mass emails, network shares
- **Code Red**: Buffer Overflow on web server using Windows 2000
- **Blaster**: Repeatedly reboots systems making it very hard to patch/fix
- **Mydoom**: Very fast spreading via email

Spyware

- Associated with behaviors such as advertising, collecting personal information, or changing your computer configuration without appropriately obtaining prior consent
- Communicates information from a user’s system to another party without notifying the user
- Information includes passwords, account numbers, and other private information

Indications of spyware infection

- The system is slow, especially when browsing the Internet
- It takes a long time for the Windows desktop to come up
- Clicking a link does nothing or goes to an unexpected website
- The browser home page changes, and you might not be able to reset it
- Web pages are automatically added to your favorites list

Trojan Horse or Trojan

- Programs disguised as useful applications
- Do not replicate themselves like viruses, but they can be just as destructive
- Its ability to spread depends on the popularity of the software and a user’s willingness to download and install the software

Some Famous Trojans

- **Acid Rain**: Old DOS Trojan, deletes system files, renames folders, creates many empty folders
- **Nuker**: Denial-of-Service (DoS) against a workstation connected to the internet
- **Mocmex**: Found in digital photo frames and collects online game passwords
- **Simpsons**: Self-extracting batch file that attempts to delete files
- **Vundo**: Downloads and displays fraudulent advertisements

Rootkits

- Software that can be installed and hidden on a computer mainly for the purpose of getting escalated privileges, such as administrative rights
- Modifies core file systems
  - Kernel
- Can be invisible to the OS
- Can also be invisible to anti-virus software

Backdoors

- Application code functions created intentionally or unintentionally that enable unauthorized access

- Debugging, maintenance hooks, or trap doors

- Example: Back Orifice, NetBus, and Sub7
- Common Port 1337 (“leet”)

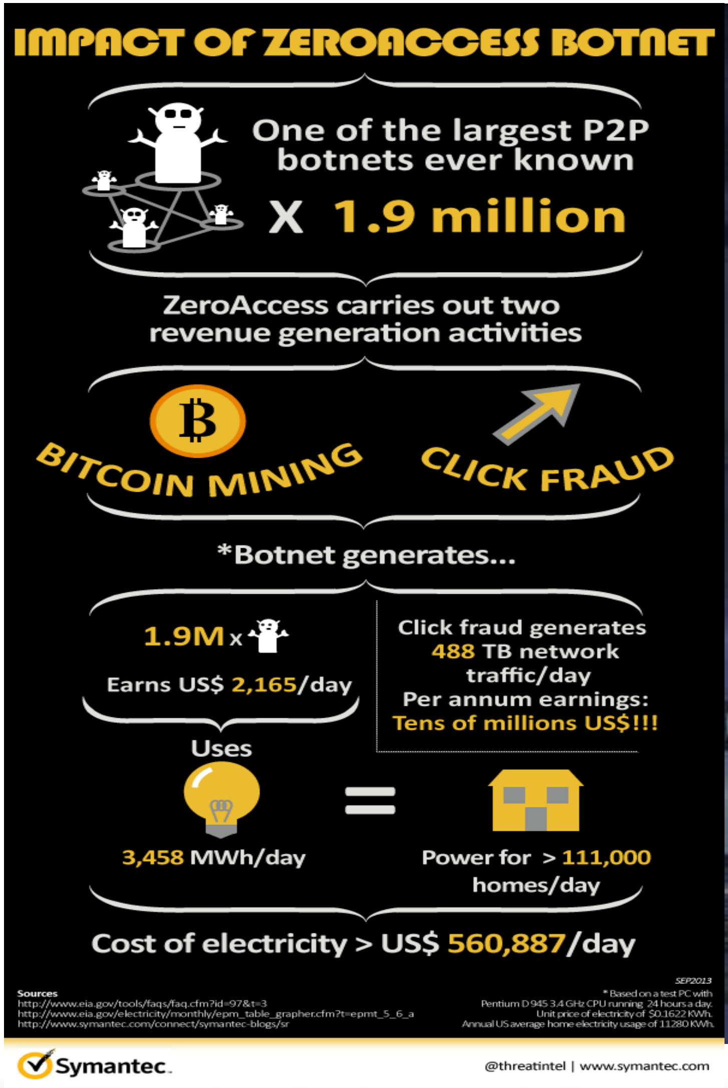
Logic Bombs

- A virus or Trojan horse designed to execute malicious actions when a certain event occurs or a period of time goes by
- Usually planted by a disgruntled employee

Botnets

- Robot network
- Once a machine is infected, it becomes a bot or zombie
- Introduced by Trojan, worm, etc…
- Used in Distributed Denial of Service (DDoS) attacks
- CoreFlood – Over 2M
- ZeroAccess – 1.9M in 2013
- Srizbi – 450,000 in 2008

Botnets



IMPACT OF ZEROACCESS BOTNET

One of the largest P2P botnets ever known

X 1.9 million

ZeroAccess carries out two revenue generation activities

BITCOIN MINING

CLICK FRAUD

*Botnet generates...

1.9M x

Earns US$ 2,165/day

Uses

3,458 MWh/day

=

Power for > 111,000 homes/day

Click fraud generates 488 TB network traffic/day

Per annum earnings: Tens of millions US$!!!

Cost of electricity > US$ 560,887/day

SEP2013

Sources
http://www.eia.gov/tools/faqs/faq.cfm?id=97&t=3
http://www.eia.gov/electricity/monthly/epm_table_grapher.cfm?t=epmt_5_6_a
http://www.symantec.com/connect/symantec-blogs/sr

* Based on a test PC with
Pentium D 945 3.4 GHz CPU running 24 hours a day.
Unit price of electricity of $0.1622 KWh.
Annual US average home electricity usage of 11280 KWh.

Symantec.

@threatintel | www.symantec.com

Trojans, Ransomware and Backdoors

Professor Messer

Trojans and Backdoors

Content provided by:
http://www.gtslearning.com

Student Check

Which one of the following best describes a polymorphic virus?

○ A. A virus that infects .exe files

○ B. A virus that attacks the boot sector and then attacks the system files

○ C. A virus inserted into a Microsoft Office document such as Word or Excel

○ D. A virus that changes its form each time it is executed

Student Check

Which one of the following best describes a polymorphic virus?

○ A. A virus that infects .exe files

○ B. A virus that attacks the boot sector and then attacks the system files

○ C. A virus inserted into a Microsoft Office document such as Word or Excel

○ D. A virus that changes its form each time it is executed

Student Check

Which one of the following is designed to execute malicious actions when a certain event occurs or a specific time period elapses?

- ○ A. Logic bomb
- ○ B. Spyware
- ○ C. Botnet
- ○ D. DDoS

Student Check

Which one of the following is designed to execute malicious actions when a certain event occurs or a specific time period elapses?

- ○ A. Logic bomb
- ○ B. Spyware
- ○ C. Botnet
- ○ D. DDoS

Student Check

What type of virus is able to regenerate itself if a single element of its infection is not removed from a compromised system?

○ A. Polymorphic
○ B. Armored
○ C. Retro
○ D. Phage

Student Check

What type of virus is able to regenerate itself if a single element of its infection is not removed from a compromised system?

○ A. Polymorphic

○ B. Armored

○ C. Retro

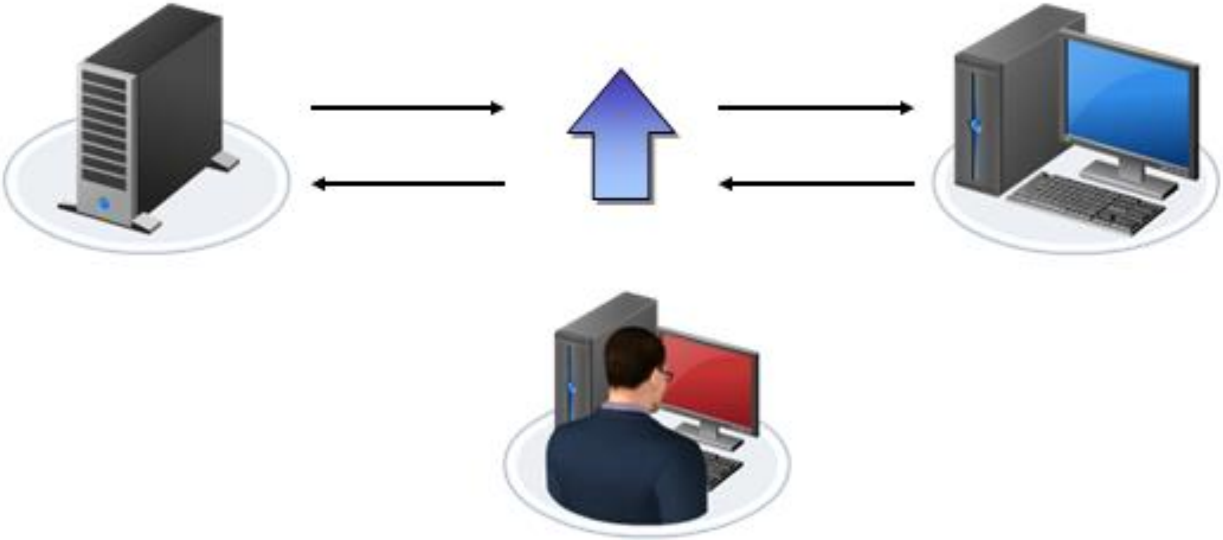
○ D. Phage

Objective 3.2

- Summarize various types of attacks

Man-in-the-Middle

- Takes place when an attacker intercepts traffic and then tricks the parties at both ends into believing that they are communicating with each other



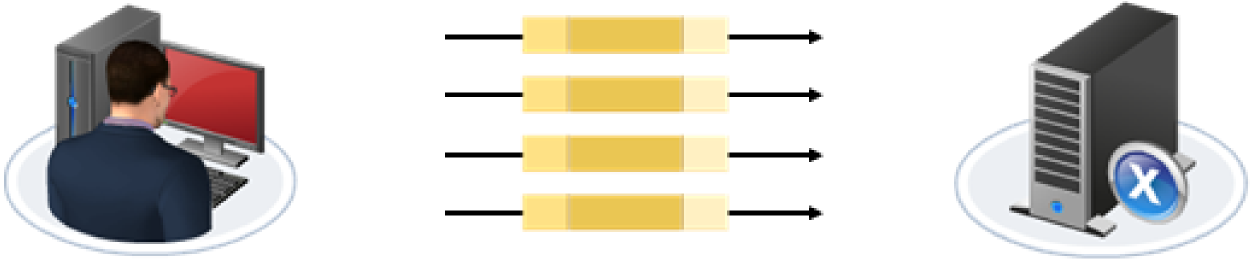
Denial of Service (DoS)

- Purpose is to disrupt the resources or services that a user would expect to have access to
- Executed by manipulating protocols and can happen without the need to be validated by the network
- Typically involves flooding a listening port on a machine with packets

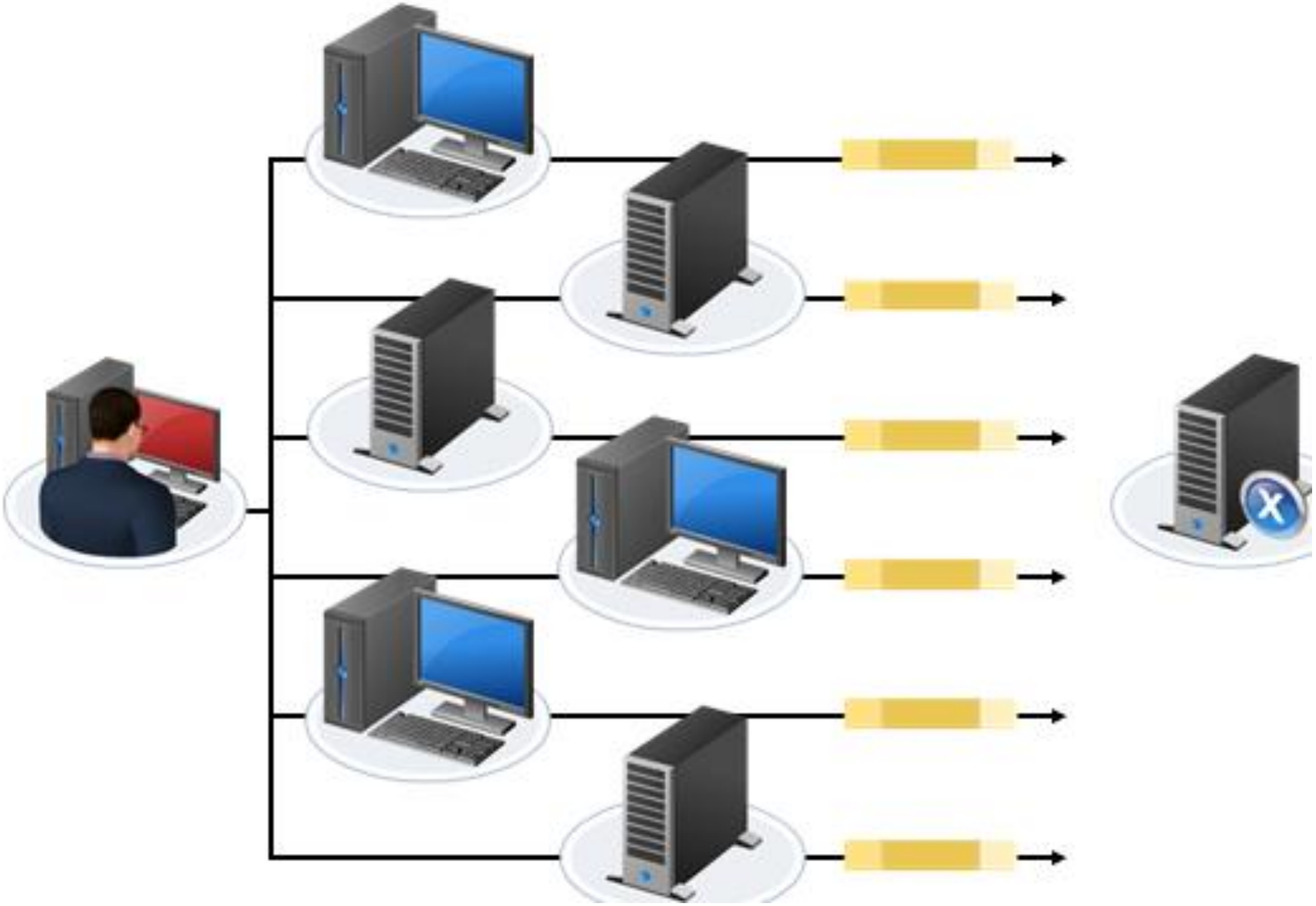
Denial of Service

- Premise is to make the system so busy processing the new connections that it cannot process legitimate service requests

- Many of the tools used to produce DoS attacks are readily available on the Internet



Distributed DoS (DDoS)



Exam Alert

- When an attacker has enough systems compromised with the installed zombie software, he can initiate an attack against a victim from a wide variety of hosts
- The attacks come in the form of the standard DoS attacks, but the effects are multiplied by the total number of zombie machines under the control of the attacker (Herder)

DoS and DDoS

Professor Messer

Denial of Service Attacks

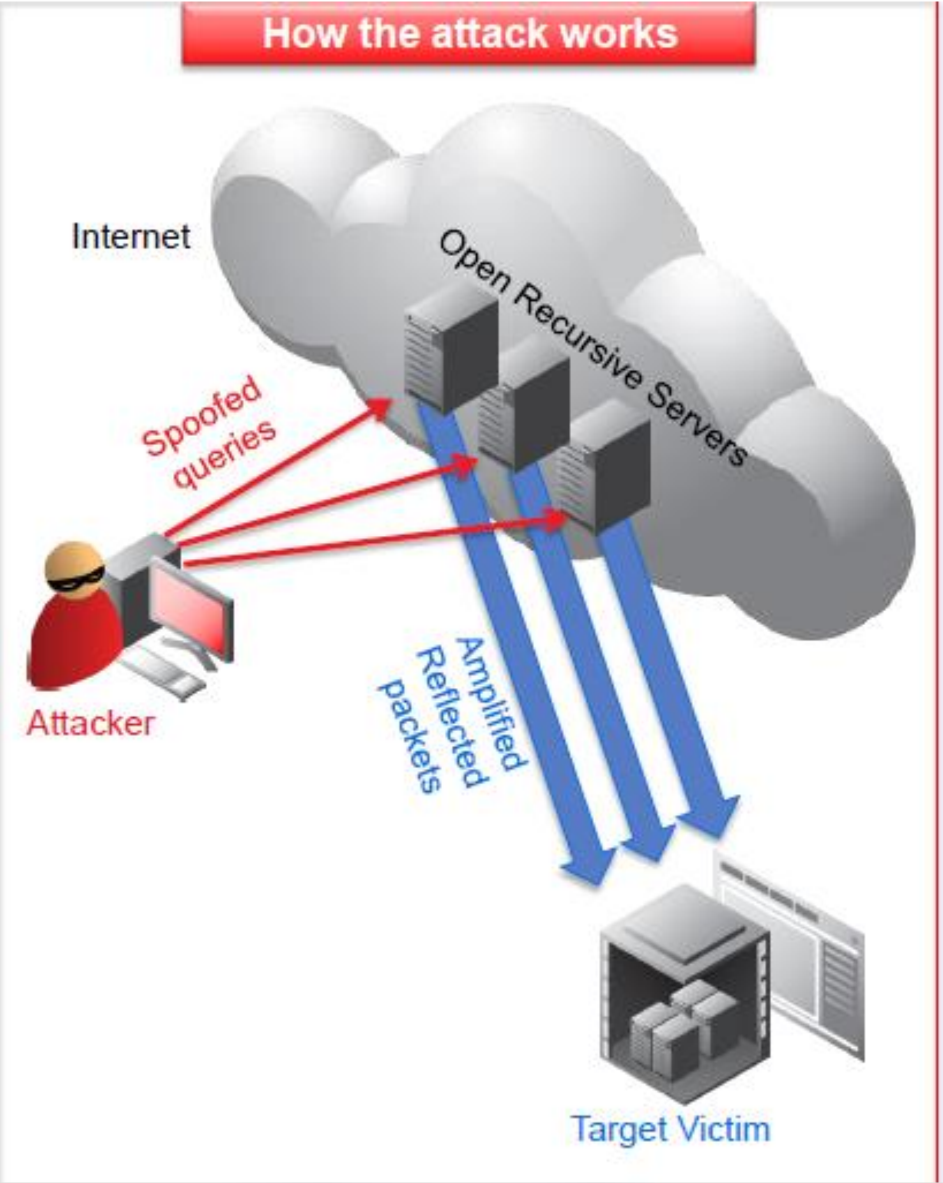
gtslearning

Content provided by:
http://www.gtslearning.com

Spoofing

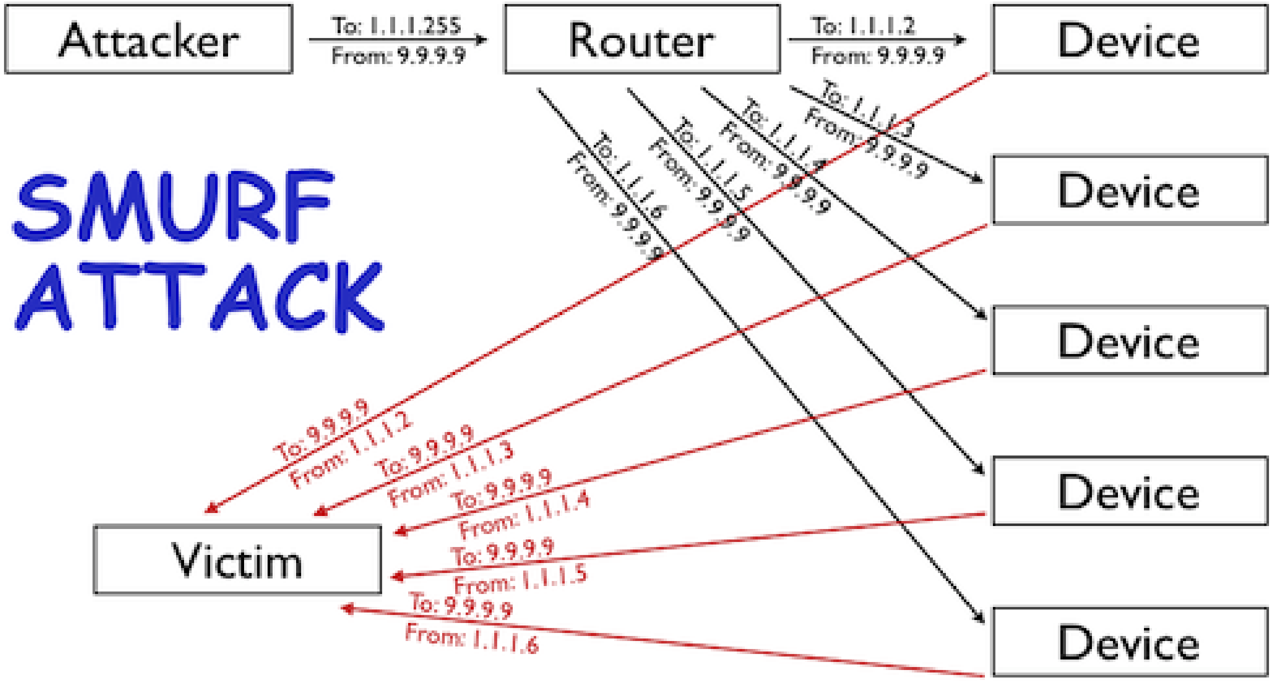
- Seeks to bypass IP address filters by setting up a connection from a client and sourcing the packets with an IP address that is allowed through the filter
- Services such as email, web, and file transfer can also be spoofed

Distributed Reflective DoS (DRDoS)



Smurf/Smurfing

the attacker sends ping packets to the broadcast address of the network, replacing the original source address in the ping packets with the source address of the victim, thus causing a flood of traffic to be sent to the unsuspecting network device.



Fraggle

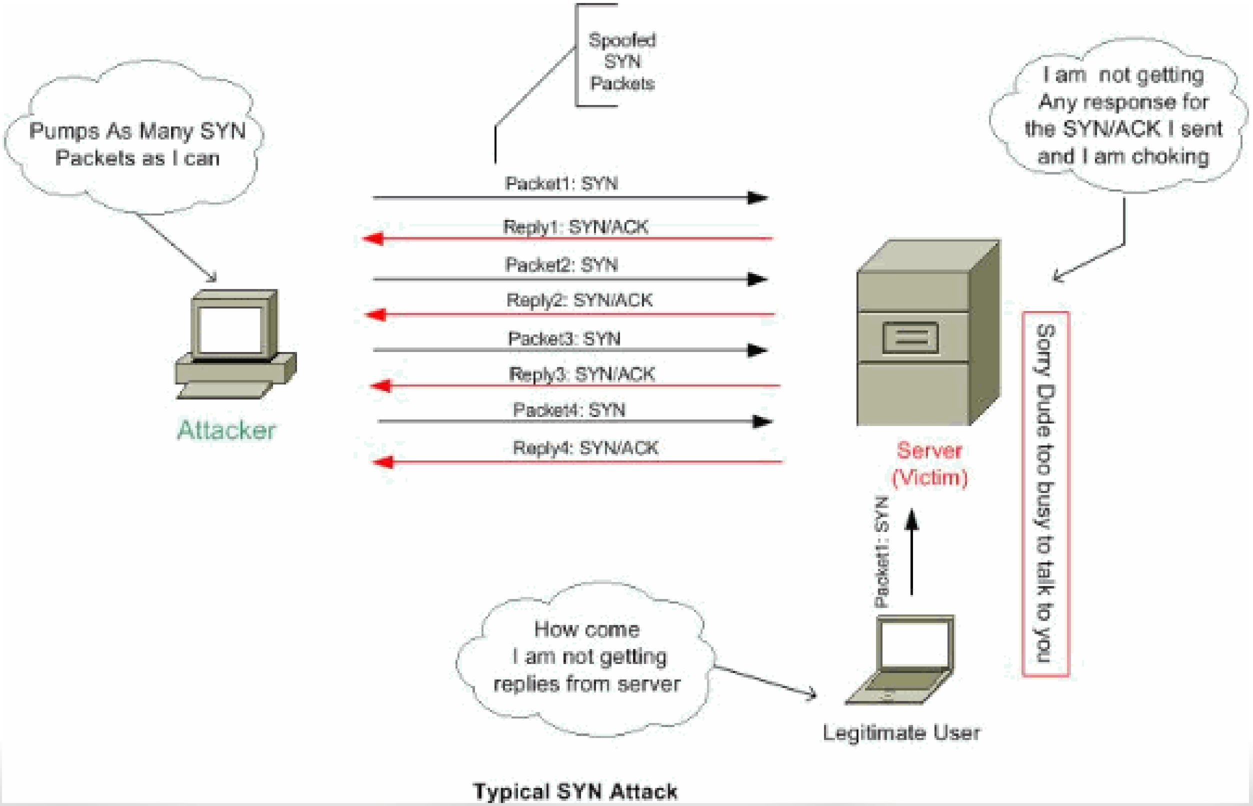
- This attack is similar to a Smurf attack. The difference is that it uses UDP rather than ICMP

- The attacker sends spoofed UDP packets to broadcast addresses as in the Smurf attack

- These UDP packets are directed to port 7 (Echo) or port 19 (Chargen)

SYN Flood

The source system sends a flood of synchronization (SYN) requests and never sends the final acknowledgment (ACK), thus creating half-open TCP sessions. Because the TCP stack waits before resetting the port, the attack overflows the destination computer’s connection buffer, making it impossible to service connection requests from valid users.

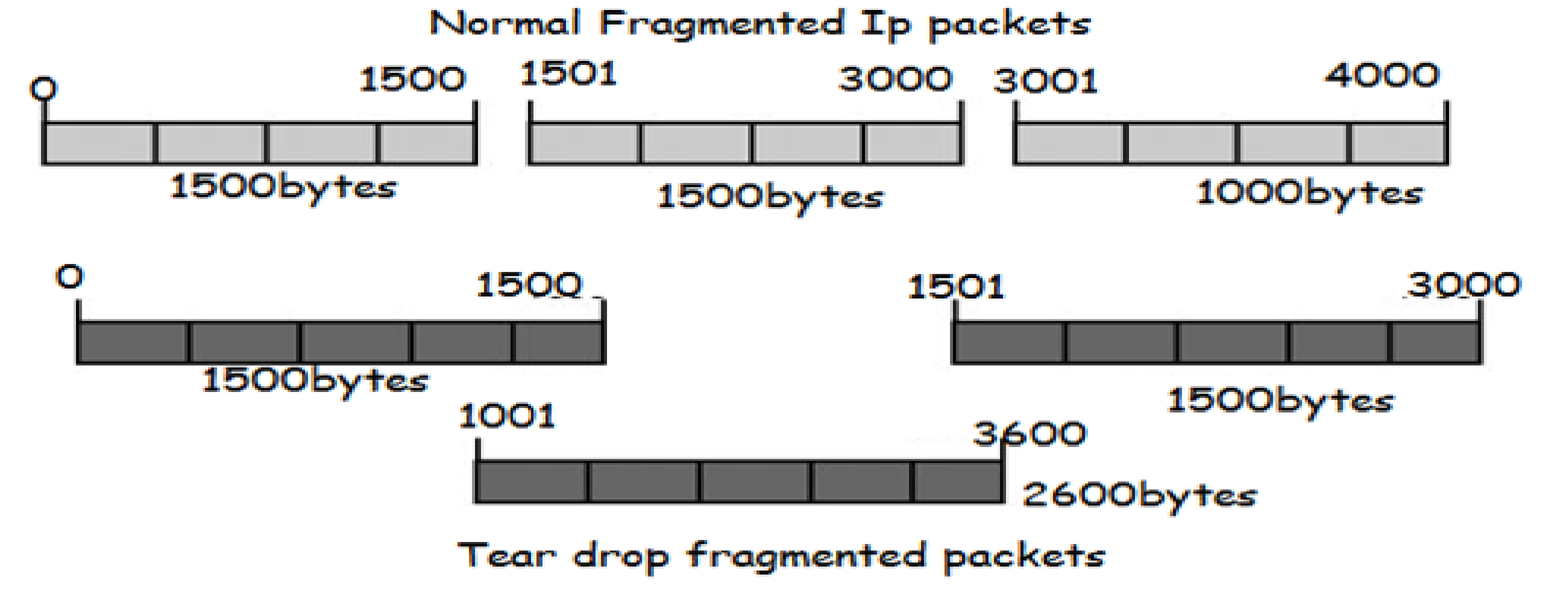


Teardrop

- This attack sends fragmented UDP packets to the victim with odd offset values in subsequent packets

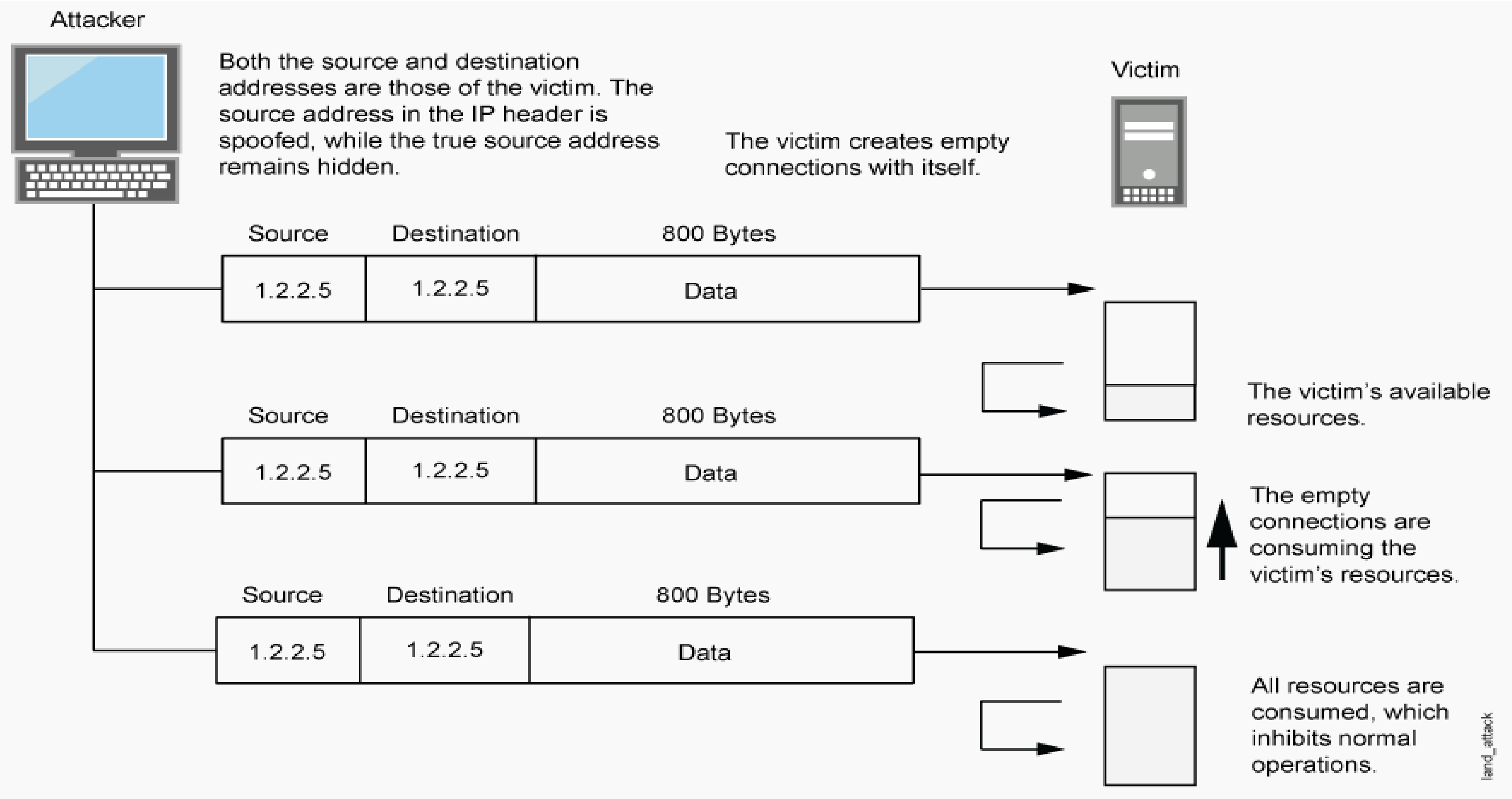
- When the operating system attempts to rebuild the original packets from the fragments, the fragments overwrite each other, causing confusion

- Because some operating systems cannot gracefully handle the error, the system will most likely crash or reboot



Land

- Numerous SYN packets are sent to the victim with source and destination addresses spoofed as the victim’s address. The victim is confused because it’s unable to respond to a packet it sent to itself that it has no record of sending



Both the source and destination addresses are those of the victim. The source address in the IP header is spoofed, while the true source address remains hidden.

The victim creates empty connections with itself.

Source	Destination	800 Bytes
1.2.2.5	1.2.2.5	Data

Source	Destination	800 Bytes
1.2.2.5	1.2.2.5	Data

Source	Destination	800 Bytes
1.2.2.5	1.2.2.5	Data

The victim’s available resources.

The empty connections are consuming the victim’s resources.

All resources are consumed, which inhibits normal operations.

Ping Flood/Ping of Death

Ping Flood:

- This attack attempts to block service or reduce activity on a host by sending ping requests directly to the victim

Ping of Death:

- A variation of this type of attack is the ping of death, in which the packet size is too large and the system doesn’t know how to handle the packets

Bonk/Boink

Bonk

- The attacker sends a corrupt UDP packet to DNS port 53. This type of attack may cause Windows systems to crash

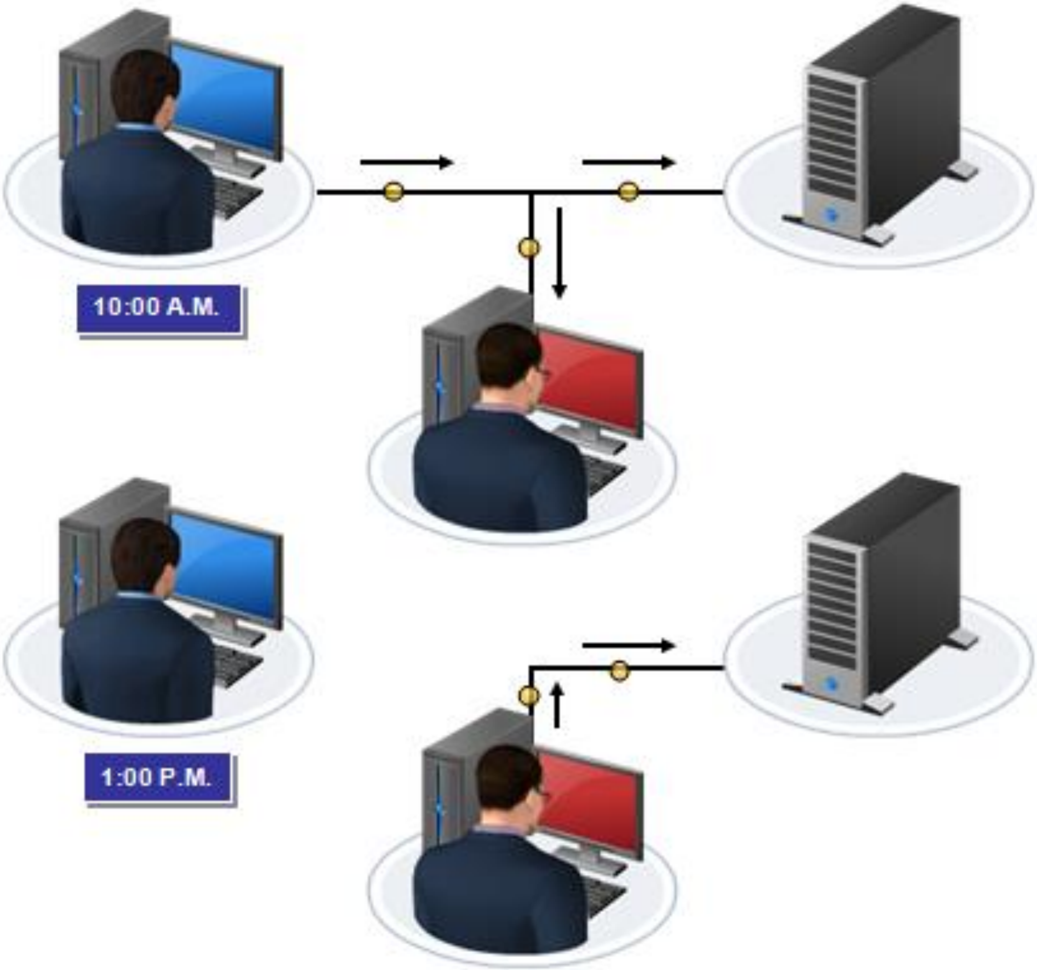
Boink

- The same as bonk, but the corrupt UDP packets are sent to numerous ports. The result may cause a Windows system to crash

Replay

- Packets are captured using sniffers
- After the pertinent information is extracted, the packets are placed back on the network
- Protecting yourself against replay attacks involves some type of time stamp associated with the packets or time-valued, non-repeating serial numbers
  - IPSec and Kerberos

Replay



Spam

- The sending of unsolicited email
- Can contain social engineering attacks and hoaxes
- Can cause DoS condition

Phishing

- Attempt to acquire sensitive information by masquerading as a trustworthy entity via an electronic communication, usually an email

Spear phishing

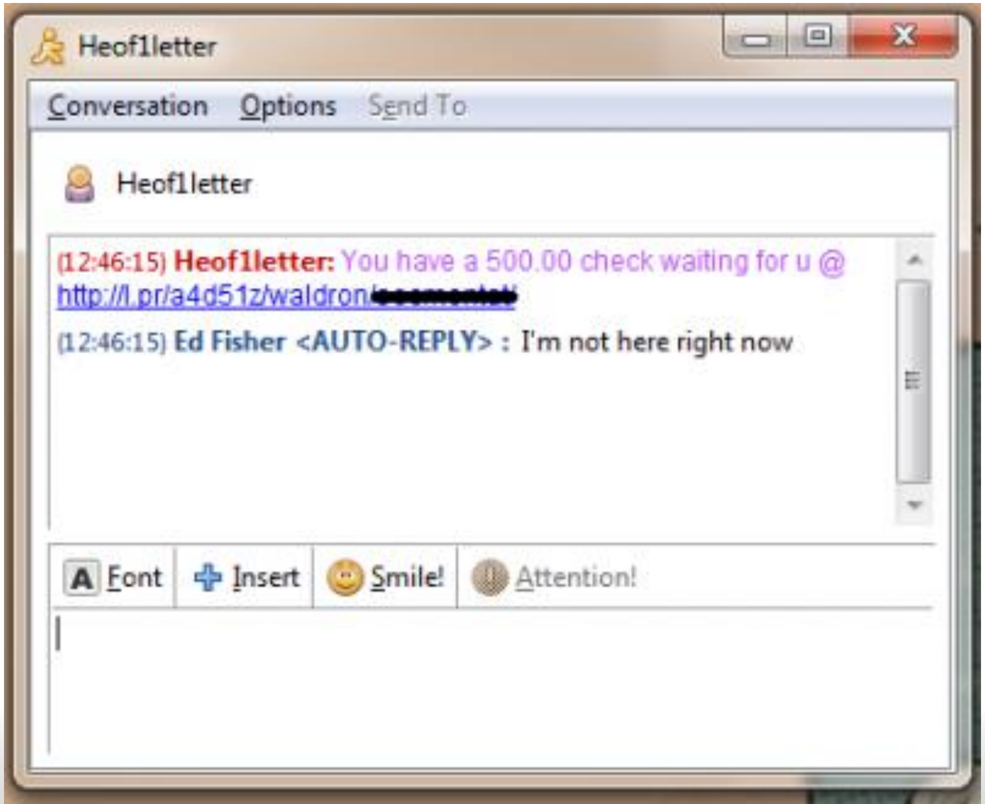
- A targeted version of phishing
- Whereas phishing often involves mass email, spear phishing might go after a smaller group or specific individual

Whaling

- Identical to spear phishing except for the "size of the fish"
- Whaling employs spear phishing tactics but is intended to go after high-profile targets such as an executive within a company

Spim

- The sending of unsolicited instant messages
- Can contain social engineering attacks, hoaxes, and sometimes DoS



(12:46:15) **Heof1letter:** You have a 500.00 check waiting for u @ http://l.pr/a4d51z/waldron/[redacted]

(12:46:15) **Ed Fisher <AUTO-REPLY> :** I'm not here right now

Vishing

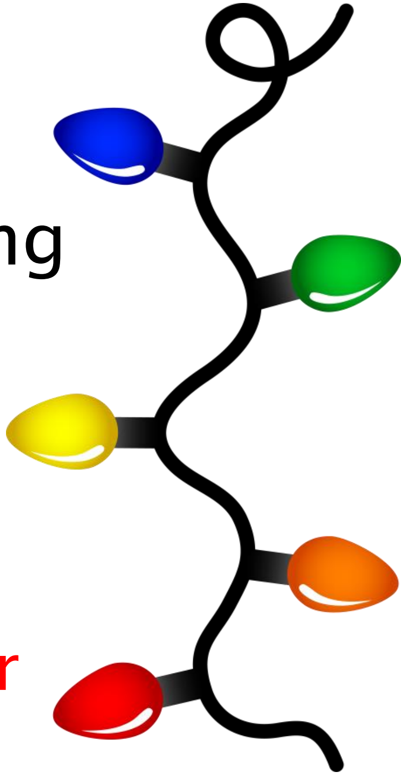
- Also known as voice phishing, the attacker often uses fake caller ID to appear as a trusted organization and attempts to get the individual to enter account details via the phone

Xmas Tree

- A Christmas tree is a packet that makes use of certain options for the underlying protocol

- Usually FIN+PSH+URG

- These packets require more processing



- SYN – Establish connection
- ACK – Acknowledge connection
- FIN – Close connection
- RST – Aborts the connection due to an error
- PSH – Client has no more data to send
- URG – Prioritize as urgent

Xmas Tree Attack

Professor Messer

Christmas Tree Attack

Content provided by:
http://www.gtslearning.com

gtslearning
CompTIA AUTHORIZED PARTNER PLATINUM

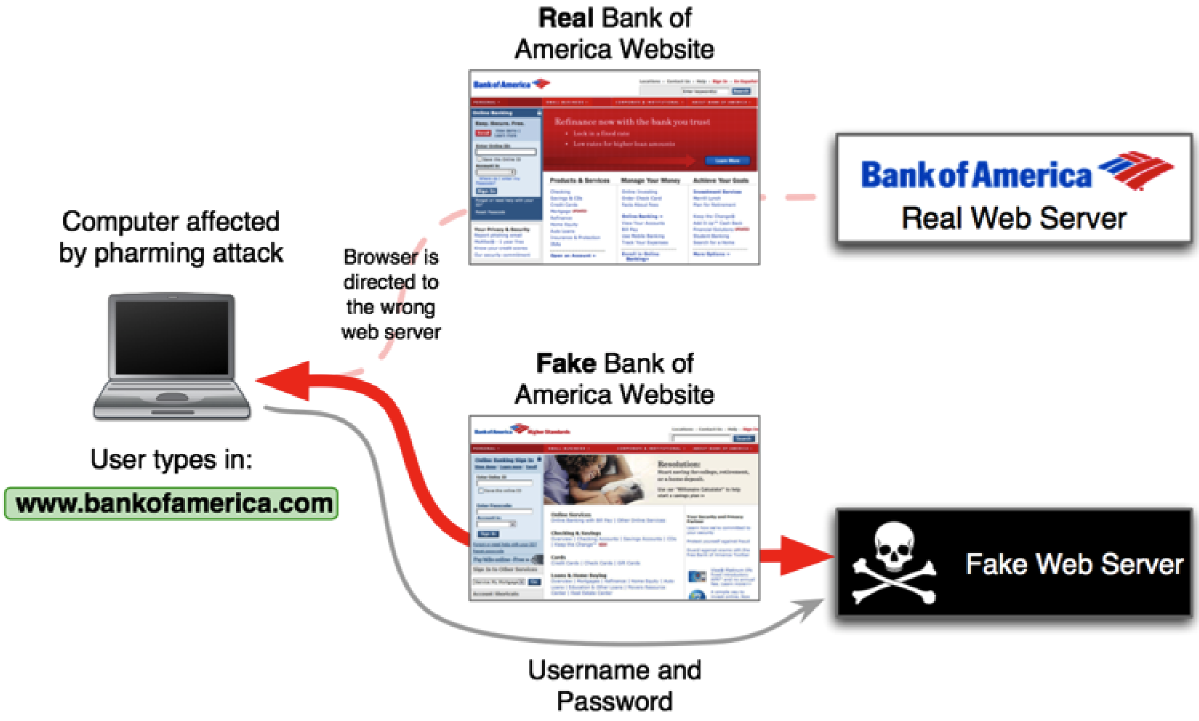
Smishing

- Also known as SMS phishing, this involves using phishing methods through text messaging

*Pharming

Pharming does not require the user to be tricked into clicking on a link

Pharming redirects victims to a bogus website, even if the user correctly entered the intended site. To accomplish this, the attacker employs another attack, such as DNS cache poisoning



Computer affected by pharming attack

User types in:

www.bankofamerica.com

Browser is directed to the wrong web server

Real Bank of America Website

Bank of America

Real Web Server

Fake Bank of America Website

Fake Web Server

Username and Password

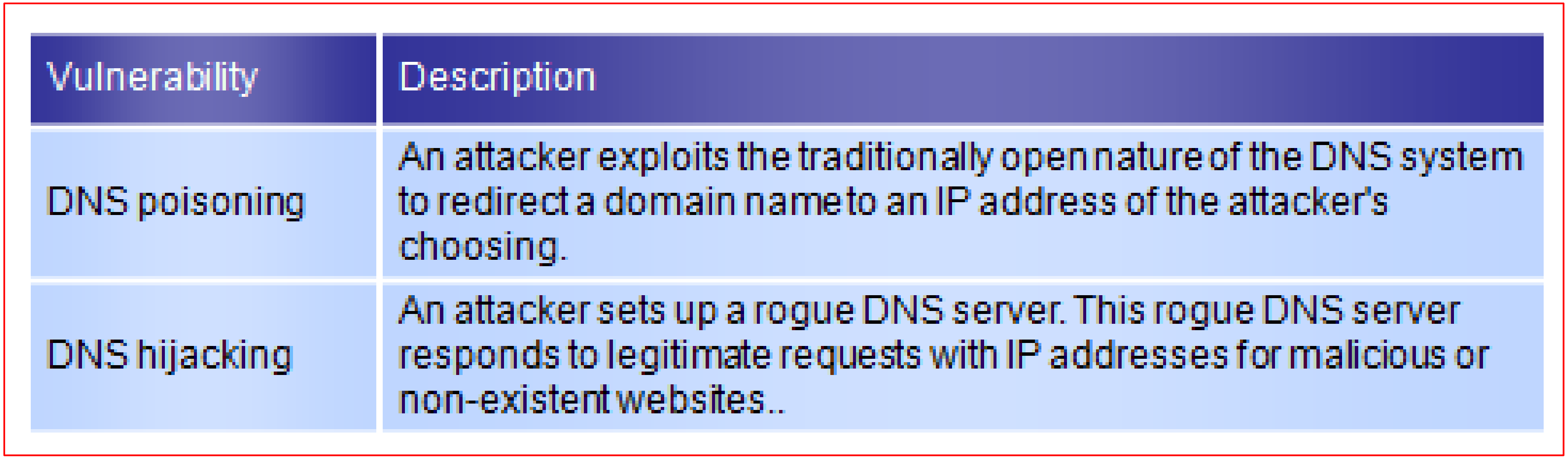
Privilege Escalation

- Programming errors can result in system compromise, allowing someone to gain unauthorized privileges
- Software exploitation takes advantage of a program’s flawed code, which then crashes the system and leaves it in a state where arbitrary code can be executed, or an intruder can function as an administrator

Malicious Insider Threat

- Typically motivated by financial gain, sabotage, and theft in order to gain a competitive advantage
- Includes employees who have the right intentions but are unaware of or ignore an organization’s security policy
- PFC Bradley (Chelsea) Manning

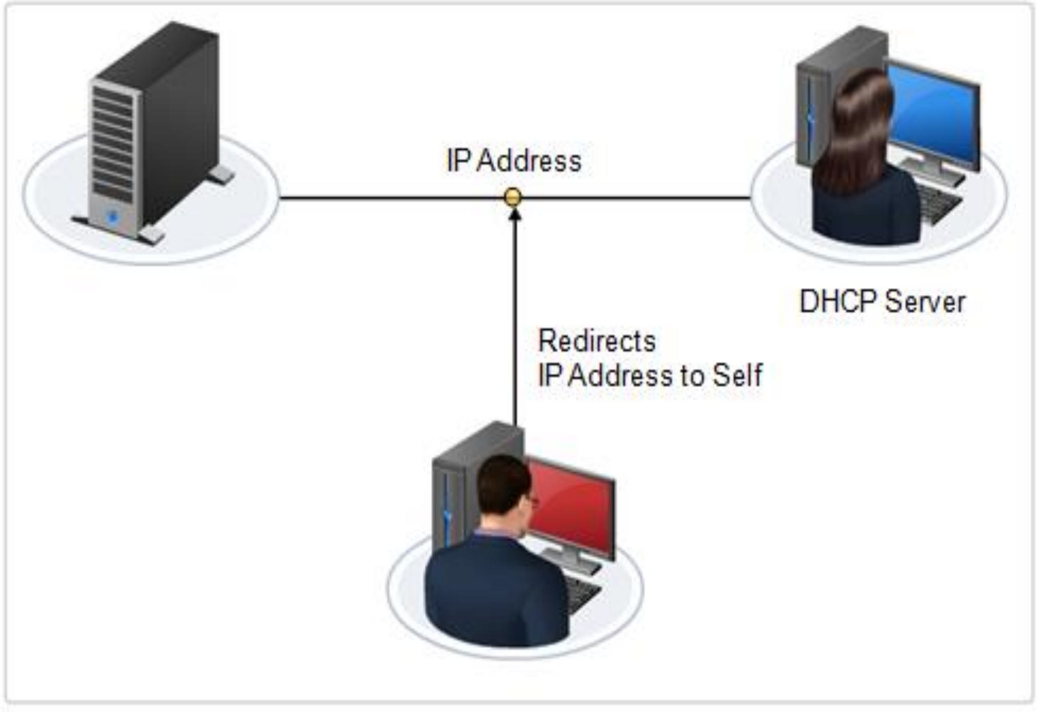
DNS Attacks



Vulnerability	Description
DNS poisoning	An attacker exploits the traditionally open nature of the DNS system to redirect a domain name to an IP address of the attacker's choosing.
DNS hijacking	An attacker sets up a rogue DNS server. This rogue DNS server responds to legitimate requests with IP addresses for malicious or non-existent websites..

ARP Poisoning

- Because ARP does not require any type of validation, as ARP requests are sent the requesting devices believe that the incoming ARP replies are from the correct devices (On Local Network)
- This can allow a perpetrator to trick a device into thinking any IP is related to any MAC address

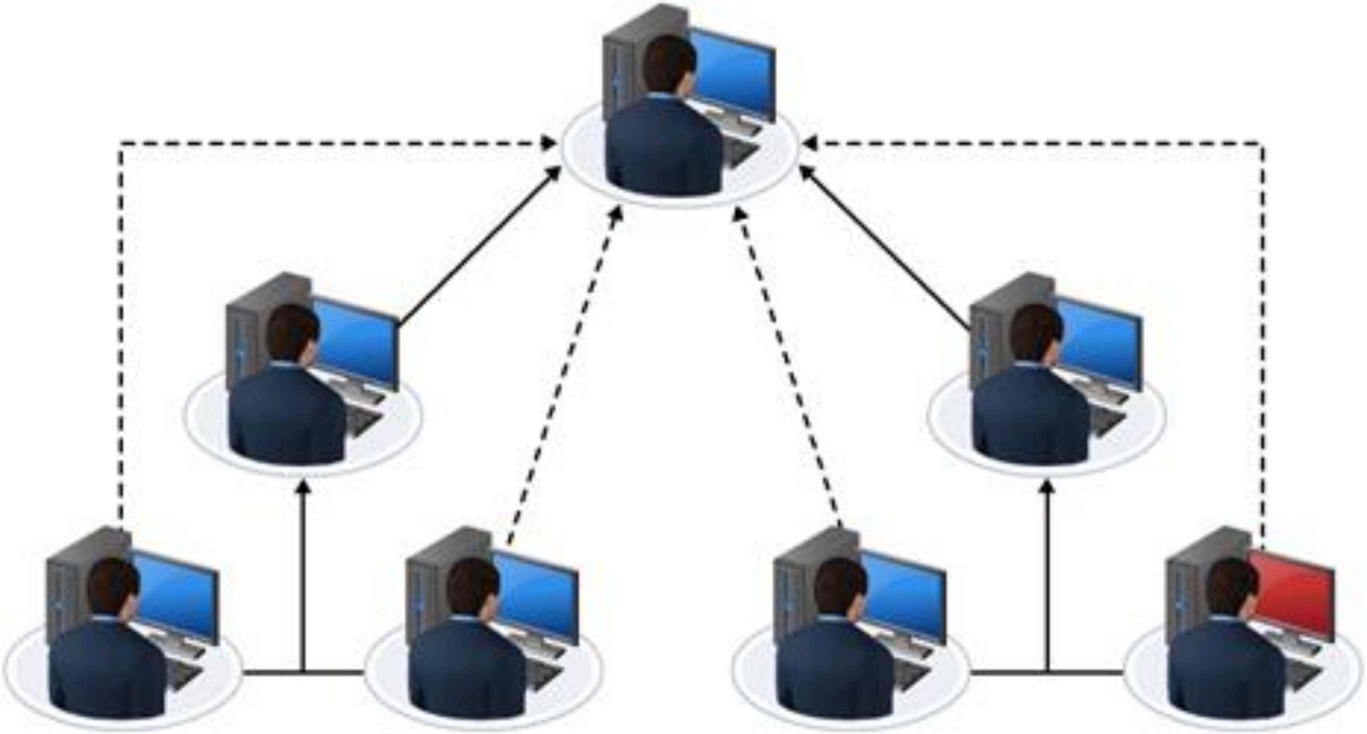


Man-in-the-Middle Attacks/ ARP Poisoning

Man-in-the-Middle Attacks

Content provided by:
http://www.gtslearning.com

Transitive Access



- Takes advantages of “trusts”

Client-side

- Servers are more secure than ever
- Attack the client
- Browsers, media applications, office programs, email clients
- Updates are important

Password Attacks

- Brute Force
- Dictionary
- Hybrid
- Birthday
- Rainbow Table

Brute Force

- *Brute-force attacks* generate hashes based on generated passwords

- A brute-force attack tries every valid combination for a password, starting with single characters and adding characters as it churns through the process

- The only limitation to Brute Force is hardware processing power

Dictionary attacks

- This attack generate hashes to compare by using prebuilt lists of potential passwords

- Often these lists are related to a person’s interests, hobbies, education, work environment, and so forth

- Dictionary attacks are remarkably successful against non-security professionals

Hybrid

- This attack takes the base dictionary list attack and perform various single-character and then multi-character manipulations on those base passwords

- This includes adding numbers or replacing letters with numbers or symbols

- Hybrid attacks are often successful even against security professionals who think they’re being smart by, for example, changing a to @ and o to 0 and adding the number 12 to the end of the name of their favorite movie character

Birthday Attack

- *Birthday attack* is another name for a brute-force attack

- However, it's derived from the birthday problem, which is found in the area of mathematics known as *probability theory*

- It is based on the concept that it takes only 23 people for there to be a 50 percent chance that two share the same birthday, and only 75 people are needed for a 99.9 percent chance

- When this logic is applied to cracking passwords (or encryption keys), it shows that because the target is part of a finite set, the likelihood of guessing correctly increases with each subsequent guess

- Each wrong guess removes one option from the remaining pool, so the next guess has a slightly greater chance of being correct

Rainbow Tables

- The really worrisome password attack on hashed passwords is called rainbow tables.

- Traditionally, password crackers hashed each potential password and then performed an Exclusive Or (XOR) comparison to check it against the stolen hash

- Hashed password file (ex: Microsoft Security Accounts Manager [SAM database])

Rainbow Tables

- A massive database of hashes created for every potential password, from single character on up, using all keyboard characters (or even all ASCII 255 characters)

- Currently, at 64 GB, a rainbow table for cracking Windows OS passwords is available that contains all the hashes for passwords from 1 to 14 characters using any keyboard character

- That database is in size, but it can be used in an attack to crack a password in less than 3 hours. This means all Windows OS passwords of 14 characters or less are worthless

- Passwords of 16+ characters are greatly encouraged

Defend against Rainbow Tables

- To prevent Rainbow Table attacks you should *salt* the hash value

- Salting the hash is the process of adding random data to the hashed value.

Typo Squatting/URL Hijacking

- *Typo squatting* or *URL hijacking* is a practice employed to capture traffic when a user mistypes the domain name or IP address of an intended resource. (Misspelling or .com/.gov)

- A squatter predicts URL typos and then registers those domain names to direct traffic to their own site. This can be done for competition or for malicious intent.

- The variations used for typo squatting include common misspellings (such as googel.com), typing errors (such as gooogle.com), variations on a name or word (for example, plurality, as in googles.com), and different top-level domains (such as google.org).

Watering Hole Attack

- A form of targeted attack against a region, a group, or an organization
- Three main phases:
  1. Observe for common resource
  2. Poison with malware
  3. Infect the group

- Effective against high security groups
- Example: see www.wired.com/threatlevel/2013/09/freedom-hosting-fbi/.

Student Check

You’re the security administrator for a bank. The users are complaining about the network being slow. It is not a particularly busy time of the day, however. You capture network packets and discover that hundreds of ICMP packets have been sent to the host.

What type of attack is likely being executed against your network?

- ○ A. Spoofing
- ○ B. Man-in-the-middle
- ○ C. DNS kiting
- ○ D. Denial of service (DoS)

Student Check

You’re the security administrator for a bank. The users are complaining about the network being slow. It is not a particularly busy time of the day, however. You capture network packets and discover that hundreds of ICMP packets have been sent to the host.

What type of attack is likely being executed against your network?

○ **A. Spoofing**
○ **B. Man-in-the-middle**
○ **C. DNS kiting**
○ **D. Denial of service (DoS)**

Student Check

Which one of the following is not an example of a denial-of-service attack?

○ A. Fraggle
○ B. Smurf
○ C. Gargomel
○ D. Xmas Tree

Student Check

Which one of the following is not an example of a denial-of-service attack?

○ A. Fraggle
○ B. Smurf
○ C. Gargomel
○ D. Xmas Tree

Student Check

Which of the following is a denial-of-service attack that uses network packets that have been spoofed so that the source and destination address are that of the victim?

- ○ **A. Land**
- ○ **B. Teardrop**
- ○ **C. Smurf**
- ○ **D. Fraggle**

Student Check

Which of the following is a denial-of-service attack that uses network packets that have been spoofed so that the source and destination address are that of the victim?

- ○ A. Land
- ○ B. Teardrop
- ○ C. Smurf
- ○ D. Fraggle

Objective 3.3

- Summarize social engineering attacks and the associated effectiveness with each attack

Social Engineering

- Attack that uses deception and trickery to convince unsuspecting users to provide sensitive data or to violate security guidelines
- Can be in person, through email, or over the phone

Shoulder Surfing

Dumpster Diving

- Scavenging for discarded equipment and documents

Tailgating

Tailgating

- Many high-security facilities employ mantraps (an airlock-like mechanism that allows only one person to pass at a time) to provide entrance control and prevent tailgating

Impersonation

- Pretend to be someone you aren’t
- Use information from other attacks
  - Dumpster diving, phishing, etc…
- Attack the victim as someone higher in rank
- Throw a lot of technical details around
- Be a buddy

Hoaxes

- A threat that doesn’t really exist
- Still can consume a lot of resources
- Often an email or social media
- May try to take your money
- www.snopes.com

Exam Alert

- Social engineering is a common practice used by attackers, and one that is not easily countered via technology
- It is important to understand that the best defense against social engineering is a program of ongoing user awareness and education

Principles (reasons for effectiveness)

- **Authority** - People are likely to respond to authority with obedience

- **Intimidation** - A derivative of the authority principle. Intimidation uses authority, confidence, or even the threat of harm to motivate someone to follow orders

- **Consensus/Social proof** - act of taking advantage of a person's natural tendency to mimic what others are doing or are perceived as having done in the past

- **Scarcity** - shoppers often feel motivated to make a purchase because of a limited-time offer, due to a dwindling stock level, or because an item is no longer manufactured

Principles (reasons for effectiveness)

- **Urgency** – often used as a method to get a quick response from a target before they have time to carefully consider or refuse compliance

- **Familiarity/liking** – attempts to exploit a person's native trust in that which is familiar

- **Trust** – attacker working to develop a relationship with a victim

Student Check

Which of the following is an effective way to get information in crowded places such as airports, conventions, or supermarkets?

- ○ A. Vishing
- ○ B. Shoulder surfing
- ○ C. Reverse social engineering
- ○ D. Phishing

Student Check

Which of the following is an effective way to get information in crowded places such as airports, conventions, or supermarkets?

- ○ A. Vishing
- ○ B. Shoulder surfing
- ○ C. Reverse social engineering
- ○ D. Phishing

Student Check

At your place of employment you are rushing to the door with your arms full of bags. As you approach, the woman before you scans her badge to gain entrance while holding the door for you, but not without asking to see your badge.

What did she just prevent?

- ○ **A. Phishing**
- ○ **B. Whaling**
- ○ **C. Tailgating**
- ○ **D. Door diving**

Student Check

At your place of employment you are rushing to the door with your arms full of bags. As you approach, the woman before you scans her badge to gain entrance while holding the door for you, but not without asking to see your badge.

What did she just prevent?

- ○ **A. Phishing**
- ○ **B. Whaling**
- ○ **C. Tailgating**
- ○ **D. Door diving**

Student Check

Which one of the following is not a type of phishing attack?

○ **A. Spear phishing**
○ **B. Wishing**
○ **C. Whaling**
○ **D. Smishing**

Student Check

Which one of the following is not a type of phishing attack?

○ A. Spear phishing
○ B. Wishing
○ C. Whaling
○ D. Smishing

Objective 3.4

- Analyze and Differentiate Among Types of Wireless Attacks

*Rogue Access Points

- Refers to situations in which an unauthorized wireless access point has been set up
- A specific type is an Evil Twin
- A common method to detect rogue access points is through the use of wireless sniffing applications such as AirMagnet or NetStumbler
  - Site survey

Jamming/Interference

- Radio waves can be disrupted
  - Microwaves, cordless phones, baby monitors
  - 2.4GHZ
- Can cause DoS condition
- Intentional jamming of signals is illegal in the U.S.

War Driving

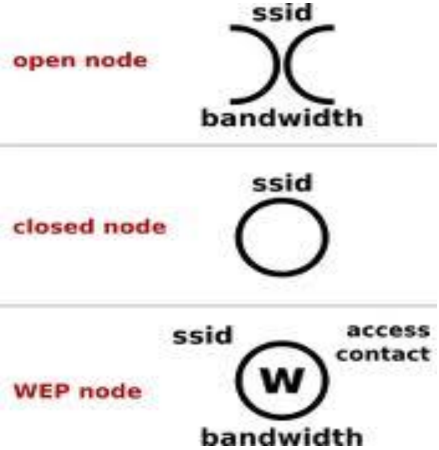
- Involves driving around with a laptop system configured to listen for open Access Points (APs)

- Many websites provide central repositories for identified networks to be collected, graphed, and even generated against city maps for the convenience of others looking for open access links to the Internet

Map
Satellite
Hybrid
Google
2000 ft
500 m
Map data ©2005 Tele Atlas - Imagery ©2005 DigitalGlobe - Terms of Use

War Chalking

- War chalking uses symbols to mark buildings, curbs, and other landmarks to indicate the presence of an available AP and its connection details



Bluejacking/Bluesnarfing

- Bluejacking
  - Unsolicited text and message broadcast spam sent from a nearby Bluetooth device
  - Goal is to *pair* to the victim's device
- Bluesnarfing
  - Once paired, the user's data becomes available for unauthorized access, modification, or deletion

Initialization Vector (IV) Attack

- An IV is an input to a cryptographic algorithm, which is essentially a random number
- Ideally, an IV should be unique and unpredictable
- An IV attack can occur when the IV is too short, predictable, or not unique
  - This is a weakness with WEP

Packetsniffing

- A wireless sniffer includes a hardware or software device capable of capturing the data or packets that traverse across the wireless channel

- In situations where traffic being sent across the network is unencrypted, packetsniffing enables the attacker to capture the data and decode it from its raw form into readable text

Near field communication

- Standard to establish radio communications between devices in close proximity
- It lets you perform a type of automatic synchronization and association between devices by touching them together or bringing them within inches of each other.
- Commonly found on smart phones and many mobile device accessories.
- NFC attacks can include man-in-the-middle, eavesdropping, data manipulation, and replay attacks.

Replay attacks

- A *replay attack* is the retransmission of captured communications in hope of gaining access to the targeted system.

WEP/WPA attacks

- *WEP and WPA attacks* can focus on either password guessing or encryption key discovery

- Rainbow Tables, IV attacks and Rogue Access Points are a few of the threats to WEP/WPA

- Enterprise access technologies such as 802.1x can aid in defending from these attacks

WPS attacks

- *WiFi Protected Setup (WPS)* is a security standard for wireless networks.

- It was intended to simplify the effort involved in adding new clients to a well-secured wireless network.

- It is operated by auto-connecting the first new wireless client to seek the network once the administrator triggered the feature by pressing the WPS button on the base station.

- Brute force attacks were used to exploit the access codes used during WPS connection negotiation without the need to physically press the button to connect

- Disabling this function is highly recommended

- With convenience comes vulnerability

Student Check

What is the term given to a rogue access point in which they serve as a man-in-the- middle from which further attacks can be carried out?

- ○ A. War driving
- ○ B. Evil twin
- ○ C. War twinning
- ○ D. Twin driving

Student Check

What is the term given to a rogue access point in which they serve as a man-in-the- middle from which further attacks can be carried out?

○ A. War driving

○ B. Evil twin

○ C. War twinning

○ D. Twin driving

Student Check

Which of the following best describes packetsniffing?

○ A. Packetsniffing allows an attacker to capture and decrypt data into readable text

○ B. Packetsniffing allows an attacker to smell which network components are transmitting sensitive data

○ C. Packetsniffing allows an attacker to capture and decode data from its raw form into readable text

○ D. Packetsniffing allows an attacker to encode and transmit packets to disrupt network services

Student Check

Which of the following best describes packetsniffing?

○ A. Packetsniffing allows an attacker to capture and decrypt data into readable text

○ B. Packetsniffing allows an attacker to smell which network components are transmitting sensitive data

○ C. Packetsniffing allows an attacker to capture and decode data from its raw form into readable text

○ D. Packetsniffing allows an attacker to encode and transmit packets to disrupt network services

Student Check

An initialization vector should be which of the following?

- ○ **A. Unique and unpredictable**
- ○ **B. Unique and predictable**
- ○ **C. Repeatable and random**
- ○ **D. Repeatable and unique**

Student Check

An initialization vector should be which of the following?

- ○ A. Unique and unpredictable
- ○ B. Unique and predictable
- ○ C. Repeatable and random
- ○ D. Repeatable and unique

Objective 3.5

- Explain types of application attacks

Cross-Site Scripting (XSS)

- By placing malicious client-side script on a website, an attacker can cause an unknowing browser user to conduct unauthorized access activities, expose confidential data, and provide logging of successful attacks back to the attacker without the user being aware of her participation
- XSS vulnerabilities can be used to hijack the user’s session or to cause the user accessing malware-tainted Site A to unknowingly attack Site B on behalf of the attacker who planted code on Site A

Cross-Site Request Forgery (CSRF)

- An attack in which the end user executes unwanted actions on a web application while the user is currently authenticated.
- Based on forging authenticated credentials during a current session

XSS vs CSRF

- The fundamental difference is that:

- Cross-Site Scripting (XSS), is designed to exploit the trust the user has for a particular site
- Used to obtain credentials

- Cross-Site Request Forgery (CSRF) aims to exploit the trust that a website has in the user’s browser using the user as authentication
- Attacker using the credentials of the authenticated user

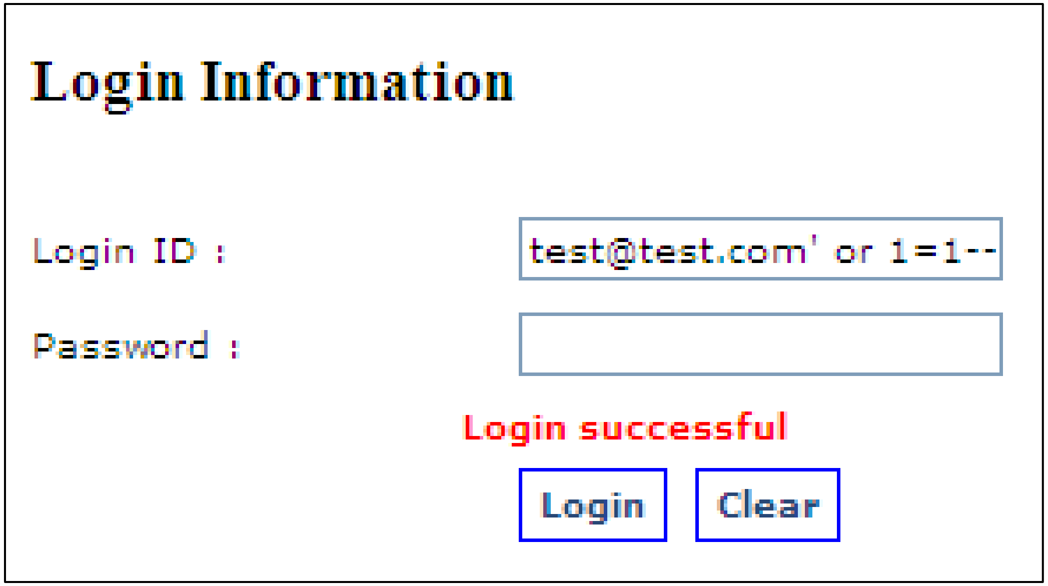
Cross-Site Scripting

Cross-site Scripting

Content provided by:
http://www.gtslearning.com

SQL injection

- Inserts malicious code into strings, which are later passed to a database server
- The SQL server then parses and executes this code
- Injection = Input
- Validation
- XML in question
- = in the answer



Login Information

Login ID : test@test.com' or 1=1--

Password :

Login successful

LDAP injection

- Some websites perform LDAP queries based upon data provided by the end user
- LDAP injection involves changing the LDAP input so that the web app runs with escalated privileges
- find("(&(cn=John)(userPassword=mypass))")

XML injection

- Uses malicious code to compromise XML applications, typically web services
- XML injection attempts to insert malicious content into the structure of an XML message to alter the logic of the targeted application

<xml/>

Directory Traversal

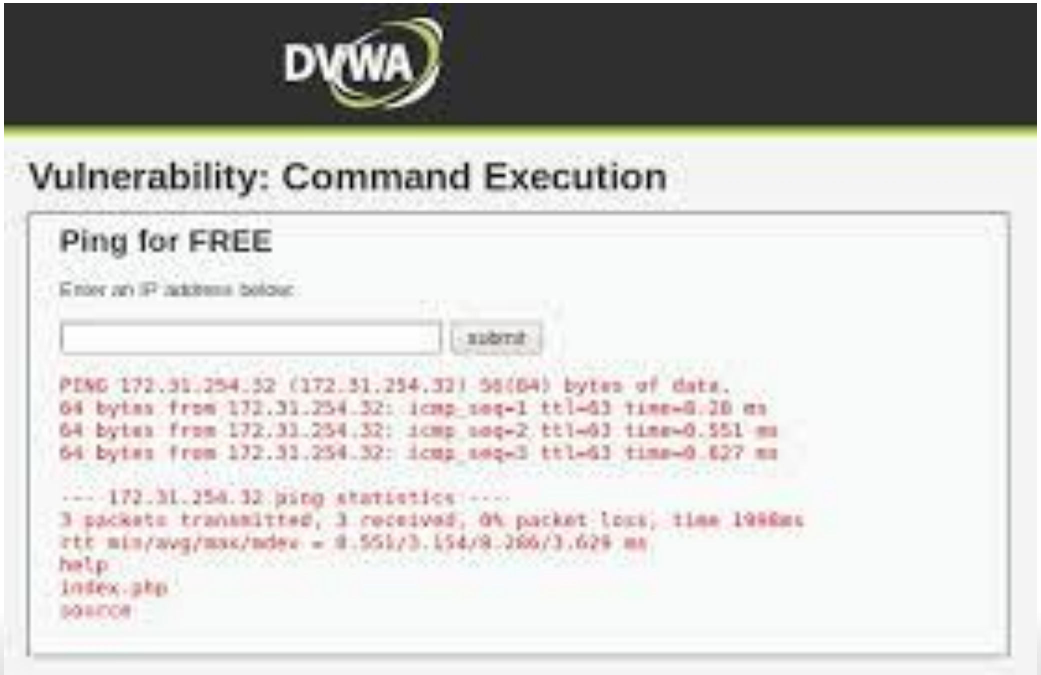
- Behind web pages is a system of files and directories

- Directory traversal allows one to navigate the directories or files that are restricted to normal users.

- http://victim.com/scripts/..% c0%af../..%c0%af../..%c0% af../..%c0%af../..% c0%af../..%c0 %af../winnt/system32/cmd.exe?/c+dir=c:\

Command Injections

- Using malicious code injection, attackers can perform a variety of attacks upon systems
- These attacks can result in the modification or theft of data



Vulnerability: Command Execution

Ping for FREE

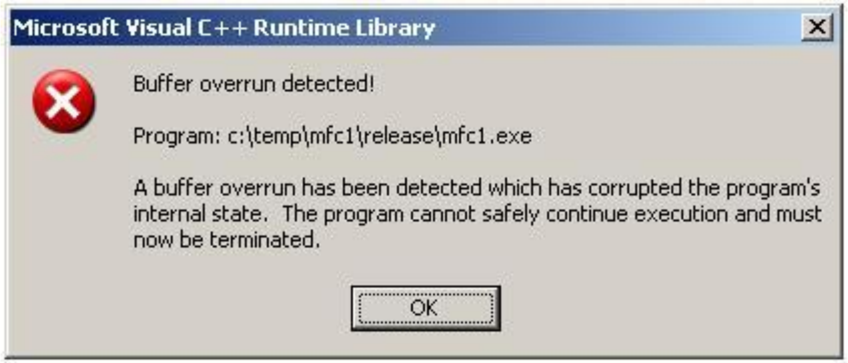
Enter an IP address below:

```
PING 172.31.254.32 (172.31.254.32) 56(84) bytes of data.
64 bytes from 172.31.254.32: icmp_seq=1 ttl=63 time=8.28 ms
64 bytes from 172.31.254.32: icmp_seq=2 ttl=63 time=0.551 ms
64 bytes from 172.31.254.32: icmp_seq=3 ttl=63 time=0.627 ms

--- 172.31.254.32 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 1998ms
rtt min/avg/max/mdev = 0.551/3.154/8.286/3.628 ms
help
index.php
source
```

Buffer Overflows

- Cause disruption of service and lost data
- Occurs when the data presented to an application or service exceeds the storage-space allocation that has been reserved in memory



Buffer overrun detected!

Program: c:\temp\mfc1\release\mfc1.exe

A buffer overrun has been detected which has corrupted the program's internal state. The program cannot safely continue execution and must now be terminated.

Integer overflow

- An *integer overflow* is the state that occurs when a mathematical operation attempts to create a numeric value that is too large to be contained or represented by the allocated storage space or memory structure

- For example, an 8-bit value can only hold the numbers 0 to 255. If an additional number is added to the maximum value, an integer overflow occurs

- Typically, the number rolls over to 0, but if it results in a negative number on a positive only program value, attackers can exploit this to pass malicious data

- Programmers need to understand the numeric limitations of their code and the platform for which they're developing

Buffer Overflows

Professor Messer

Integer Overflows and Buffer Overflows

gtslearning

Content provided by:
http://www.gtslearning.com

CompTIA AUTHORIZED PARTNER

Zero-day

- A zero-day (or zero-hour or day zero) attack or threat is a computer threat that tries to exploit computer application vulnerabilities that are unknown to others or the software developer

Cookies

- Temporary files stored in the client's browser cache to maintain settings across multiple pages, servers, or sites
- Used to maintain data such as user settings between visits to the same site on multiple days or to track user browsing habits
- Generally provide benefits to the end users
- Spyware would be most likely to use a tracking cookie
- A tracking cookie is a particular type of permanent cookie that sticks around, whereas a session cookie stays around only for that particular visit to a website

LSO (Local Shared Objects)

- LSO (Local Shared Objects) are small files or data sets that websites may store on a visitor's computer through the Adobe Flash Player

- LSOs are also known as Flash cookies

- Generally used to store user preferences and settings, but can be a form of tracking cookie

Malicious add-ons

- Active content within websites offers an attractive attack space for aggressors, who might craft special “drivers” required for content access that are in fact Trojans or other forms of malware

- Other attackers craft malware to take advantage of unpatched add-ons to directly inject code or gain access to a user’s system when a vulnerable browser is directed to an infected website

Session hijacking

- Browsers access resources on a remote server using a predefined port (80 for HTTP or 443 for HTTPS).

- The browser traffic is easily identifiable by an attacker who may elect to hijack legitimate user credentials and session data for unauthorized access to secured resources

Header Manipulation

- HTTP headers are control data used between the web browser and web server

- In most cases websites and applications do not rely upon the headers for important data, yet it was a common practice in the past, and it is still used across many less-secure applications and sites

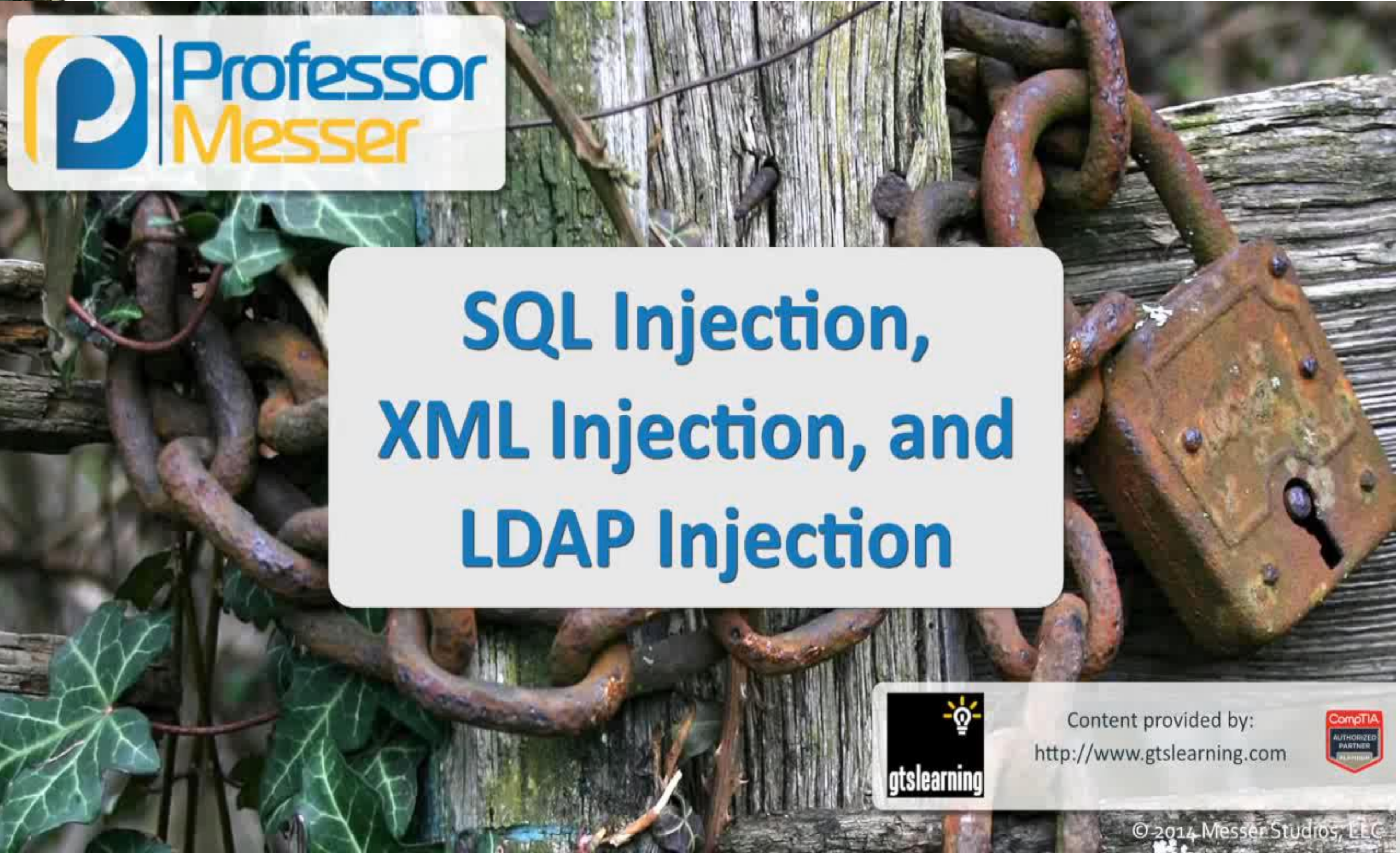
- In cases where a developer chooses to inspect and use the incoming headers, it is important to note that the headers originate at the client

- As a result, these headers could easily be modified by the user using freely available proxy software

Arbitrary code execution

- Arbitrary code execution is the ability to run any software on a target system
- Often combined with privilege escalation and other attacks to perform a local attack remotely

Injection Attacks



SQL Injection, XML Injection, and LDAP Injection

Content provided by:
http://www.gtslearning.com

Student Check

Spyware is most likely to use which one of the following types of cookies?

- ○ A. Session
- ○ B. Transport
- ○ C. Tracking
- ○ D. Poisonous

Student Check

Spyware is most likely to use which one of the following types of cookies?

○ A. Session
○ B. Transport
○ C. Tracking
○ D. Poisonous

Student Check

Which of the following types of attacks can result from the length of variables not being properly checked in the code of a program?

- ○ **A. Buffer overflow**
- ○ **B. Replay**
- ○ **C. Spoofing**
- ○ **D. Denial of service**

Student Check

Which of the following types of attacks can result from the length of variables not being properly checked in the code of a program?

○ A. Buffer overflow
○ B. Replay
○ C. Spoofing
○ D. Denial of service

Student Check

Which one of the following is a best practice to prevent code injection attacks?

○ A. Session cookies

○ B. Input validation

○ C. Implementing the latest security patches

○ D. Using unbound variables

Student Check

Which one of the following is a best practice to prevent code injection attacks?

- ○ A. Session cookies
- ○ B. Input validation
- ○ C. Implementing the latest security patches
- ○ D. Using unbound variables

Objective 3.6

- Analyze and Differentiate Among Types of Mitigation and Deterrent Techniques

Monitoring System Logs

- A lot of information from a lot of different sources
  - Workstations, servers, routers, switches, IDS/IPS, firewalls, etc…

- Different uses for different types of logs
  - Event logs, Audit log, Security log, Access log

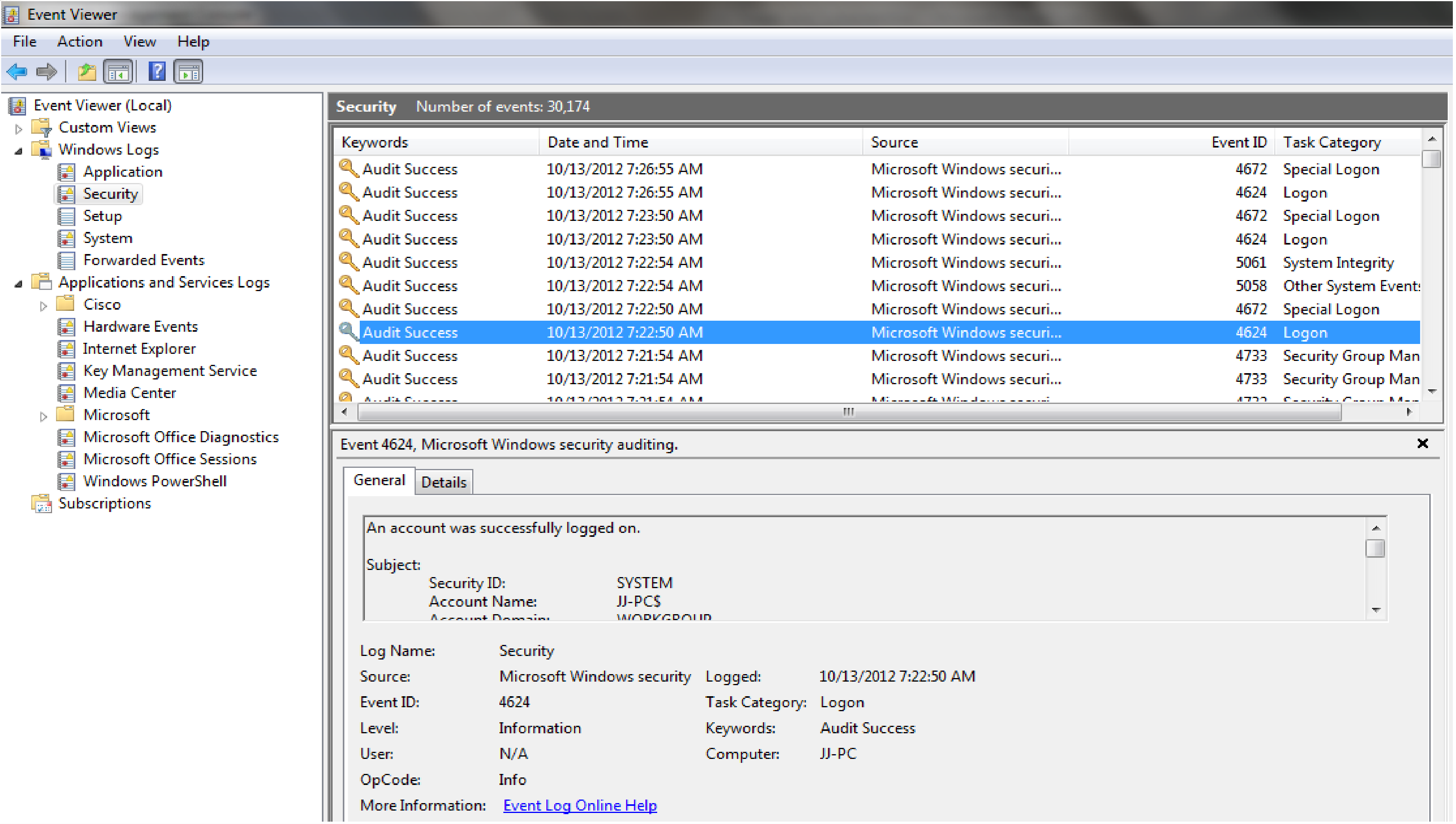
- Automation is key to auditing the logs

- Security baselines are important
  - Number of incorrect authentications, server downloads, network throughput, memory usage

- If threshold is exceeded you should receive alert

- Securing logs is important; they contain sensitive information and may be used in the forensic process if needed

Monitoring System Logs



Security Number of events: 30,174

Keywords	Date and Time	Source	Event ID	Task Category
Audit Success	10/13/2012 7:26:55 AM	Microsoft Windows securi...	4672	Special Logon
Audit Success	10/13/2012 7:26:55 AM	Microsoft Windows securi...	4624	Logon
Audit Success	10/13/2012 7:23:50 AM	Microsoft Windows securi...	4672	Special Logon
Audit Success	10/13/2012 7:23:50 AM	Microsoft Windows securi...	4624	Logon
Audit Success	10/13/2012 7:22:54 AM	Microsoft Windows securi...	5061	System Integrity
Audit Success	10/13/2012 7:22:54 AM	Microsoft Windows securi...	5058	Other System Event:
Audit Success	10/13/2012 7:22:50 AM	Microsoft Windows securi...	4672	Special Logon
Audit Success	10/13/2012 7:22:50 AM	Microsoft Windows securi...	4624	Logon
Audit Success	10/13/2012 7:21:54 AM	Microsoft Windows securi...	4733	Security Group Man
Audit Success	10/13/2012 7:21:54 AM	Microsoft Windows securi...	4733	Security Group Man
Audit Success	10/13/2012 7:21:54 AM	Microsoft Windows securi...	4733	Security Group Man

Event 4624, Microsoft Windows security auditing.

```
An account was successfully logged on.

Subject:
        Security ID:            SYSTEM
        Account Name:           JJ-PC$
        Account Domain:         WORKGROUP
```

Log Name:	Security		
Source:	Microsoft Windows security	Logged:	10/13/2012 7:22:50 AM
Event ID:	4624	Task Category:	Logon
Level:	Information	Keywords:	Audit Success
User:	N/A	Computer:	JJ-PC
OpCode:	Info		
More Information:	Event Log Online Help		

Hardening

- Refers to reducing security exposure and strengthening defenses against unauthorized access attempts and other forms of malicious attention

- A “soft” system is one that is installed with default configurations or unnecessary services, or one that is not maintained to include emerging security updates

Hardening

- Disabling unnecessary services
- Protecting management interfaces and applications
- Password protection
- Disabling unnecessary accounts
- Updates

Updates

- **Hotfixes**: Typically, small and specific-purpose updates that alter the behavior of installed applications in a limited manner

- **Patches**: Like hotfixes, are usually focused updates that affect installed applications. Patches are generally used to add new functionality, update existing code operation, or to extend existing application capabilities

- **Service packs**: Major revisions of functionality or service operation in an installed application. Usually cumulative, including all prior service packs, hotfixes, and patches

Port Security

- Mac limiting and filtering
- 802.1x
- Disabling unused ports

Security Posture

- Initial baseline configuration
  - Different systems have different baselines
- Continuous security monitoring
  - New threats are announced daily
  - IAVA – Information Assurance Vulnerability Alert
  - IAVM – Information Assurance Vulnerability Management
- Remediation
  - NAC/802.1x
  - Make sure systems meet the baseline before they are allowed access

Reporting

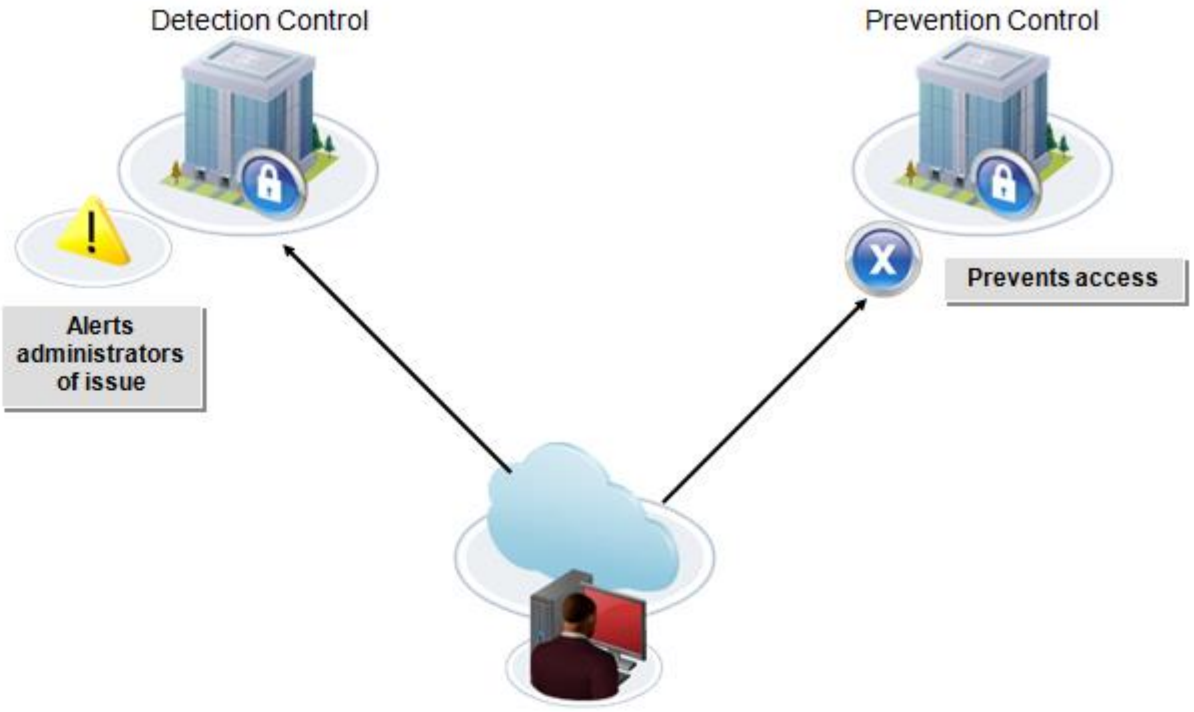
- Proper and effective reporting is critical to the overall health and security of an organization
- The use of reporting should be dictated by a policy based upon the overall risk of the infrastructure and data
- This will help define what types of reports are required, the frequency of the reports, as well as how often they are examined

Reporting

- Alarms
  - The purpose is to report a critical event that typically requires some type of immediate response
- Alerts
  - Less critical than an alarm and likely does not require an immediate response
- Trends
  - Help prevent the unnecessary response to something that initially might seem warranted but is actually not

Detection Controls vs. Prevention Controls

- IDS vs. IPS
- Camera vs. guard



Student Check

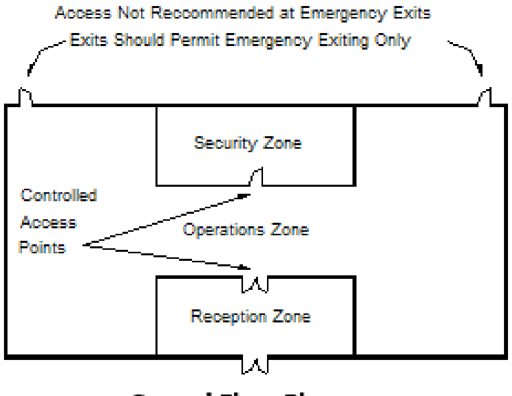
In order to harden a system, which one of the following is a critical step?

- ○ A. Isolate the system in a below–freezing environment
- ○ B. Disable all unnecessary ports and services
- ○ C. Disable the WWW service
- ○ D. Isolate the system physically from other critical systems

Physical Security

- Physical access to a system or network creates many avenues for a breach in security

- Physical security zones
  - External, perimeter, public, restricted, secure
  - Usually separated with a barrier
  - Fence, door, lock, guard


Access Not Reccommended at Emergency Exits
Exits Should Permit Emergency Exiting Only
Security Zone
Controlled
Access
Points
Operations Zone
Reception Zone

Ground Floor Plan

Student Check

In order to harden a system, which one of the following is a critical step?

○ A. Isolate the system in a below–freezing environment

○ B. Disable all unnecessary ports and services

○ C. Disable the WWW service

○ D. Isolate the system physically from other critical systems

Student Check

Which one of the following is the most common method of video surveillance?

○ A. CCTV
○ B. IPTV
○ C. CTV
○ D. ICTV

Student Check

Which one of the following is the most common method of video surveillance?

○ A. CCTV
○ B. IPTV
○ C. CTV
○ D. ICTV

Student Check

Which one of the following controls is not a physical security measure?

- ○ **A. Motion detector**
- ○ **B. Antivirus software**
- ○ **C. CCTV**
- ○ **D. Fence**

Student Check

Which one of the following controls is not a physical security measure?

○ A. Motion detector

○ B. Antivirus software

○ C. CCTV

○ D. Fence

Objective 3.7

- Implement Assessment Tools and Techniques to Discover Security Threats and Vulnerabilities

Interpreting Results

- The output of these scanners and tools require careful interpretation
- The interpretation of the results typically result in one of three things:
  - Doing nothing either because it’s a false positive or there is not a significant risk presented to the organization
  - Fixing or eliminating the vulnerability
  - Accepting the vulnerability but implementing mitigating controls

*Vulnerability Scanning

- Passively testing security controls
  - Designed to not interfere with normal activity or degrade performance

- Identifying vulnerability
  - Using software to test systems for known vulnerabilities or weaknesses
  - Protocol Analyzer/Sniffer
  - Vulnerabilty Scanner
  - Honeypots/Honeynets
  - Systems configured to simulate one or more services within a network and left exposed to network access
  - Attackers activities are logged and monitored so that their actions and methods can be late reviewed in detail
  - Port Scanner
  - Banner Grabbing (HTTP server enumeration)

Vulnerability Scanning

- Identifying lack of security controls
  - Provides for the opportunity to remediate the weakness

- Identifying common misconfigurations
  - Most beneficial when compared against an organization’s security policies and standards

Assessment Techniques

- Baseline reporting
  - Compares existing implementations against expected baselines

- Code review
  - Typically conducted using automated software programs designed to check code

  - Also manual human checks in which someone not associated with development combs through the code

Assessment Techniques

- Determine the attack surface
  - Refers to the amount of running code, services, and user-interaction fields and interfaces
- Architecture Review
  - Considers the entire system
- Design Review
  - Refers more specifically to the components of the architecture at a more micro level

Student Check

Which one of the following is used to capture network traffic?

- ○ A. Honeynet
- ○ B. Vulnerability scanner
- ○ C. Honeypot
- ○ D. Protocol analyzer

Student Check

Which one of the following is used to capture network traffic?

○ A. Honeynet
○ B. Vulnerability scanner
○ C. Honeypot
○ D. Protocol analyzer

Student Check

Reviews of architecture, design, and code, as well as baseline reporting and understanding attack surface, are all considered which one of the following?

○ **A. Control procedure techniques to protect against insider threats**

○ **B. Countermeasures designed to eliminate risk**

○ **C. Techniques for assessing threats and vulnerabilities**

○ **D. Design procedures for creating sustainable and usable applications**

Student Check

Reviews of architecture, design, and code, as well as baseline reporting and understanding attack surface, are all considered which one of the following?

○ A. Control procedure techniques to protect against insider threats

○ B. Countermeasures designed to eliminate risk

○ C. Techniques for assessing threats and vulnerabilities

○ D. Design procedures for creating sustainable and usable applications

Student Check

Which one of the following is not true of port scanners?

○ **A. They are useful for nefarious purposes.**

○ **B. They can be stand alone or part of a vulnerability assessment solution.**

○ **C. They allow interaction with the attacker to enable logging.**

○ **D. They can provide operating system information.**

Student Check

Which one of the following is not true of port scanners?

○ A. They are useful for nefarious purposes.

○ B. They can be stand alone or part of a vulnerability assessment solution.

○ C. They allow interaction with the attacker to enable logging.

○ D. They can provide operating system information.

Objective 3.8

- Within the Realm of Vulnerability Assessments, Explain the Proper Use of Penetration Testing versus Vulnerability Scanning

Exam Alert

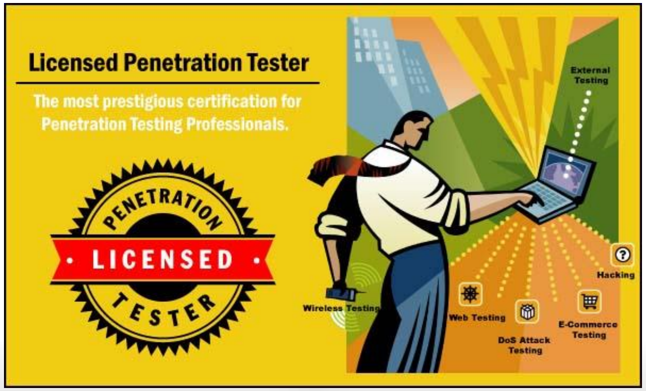
- Penetration tests are almost always considered **active**
- Vulnerability scans are most often **passive** attempts to identify weaknesses

Penetration Testing

- Verify a threat exists
  - A penetration tests **seeks to exploit vulnerabilities**
  - It is necessary to first understand a threat and to what extent that threat exists in the first place
- Bypass security controls
  - Penetration tests should seek to bypass security controls

- Vulnerability is inside to outside

- Penetration is outside to in



Penetration Testing

- Actively test security controls
  - Active techniques include direct interaction with a specific target
  - Seek to identify if controls are implemented properly
  - Example: door lock
- Exploiting vulnerabilities
  - Executing an attack is the core of a penetration test
  - A resulting exploit verifies the vulnerability and should lead to mitigation techniques and controls to deal with the security exposure

The Hacking Process

- 1 – Footprinting
  - Hacker gathers information that is readily available

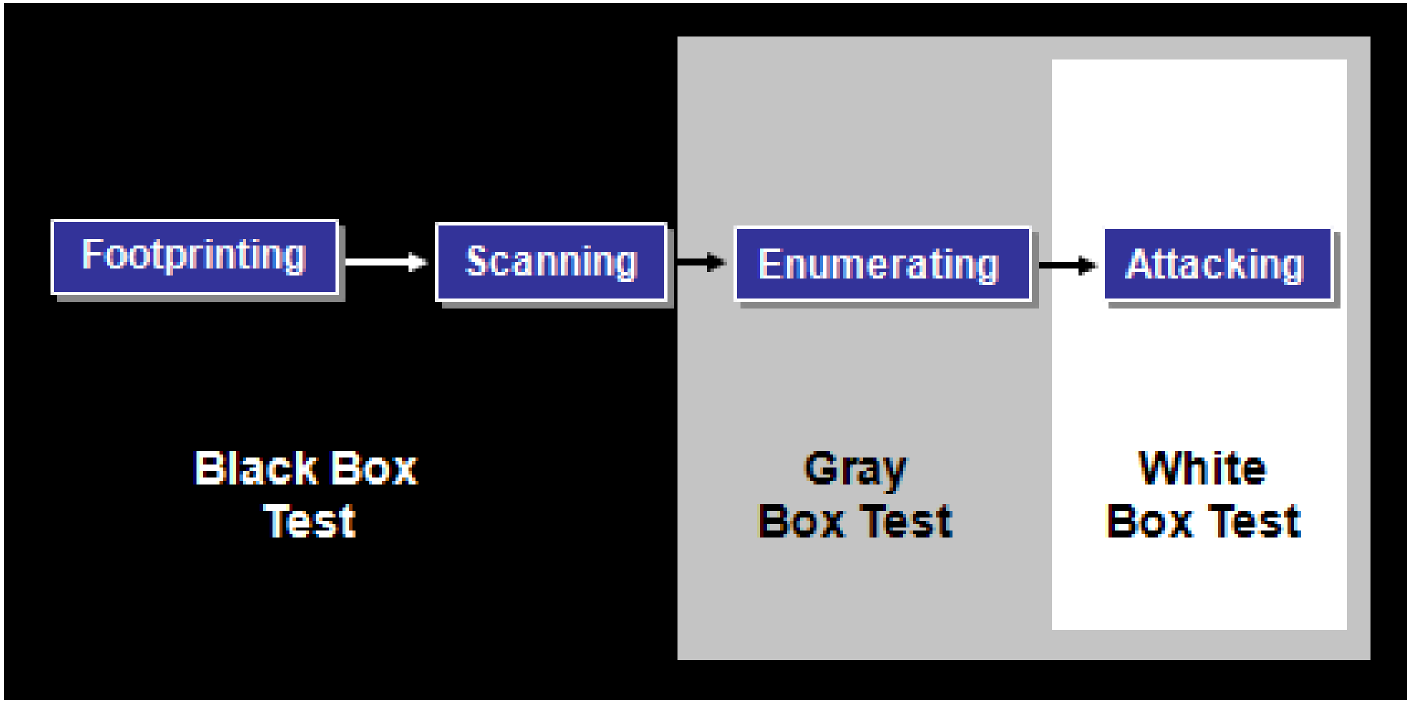
- 2 – Scanning
  - Scans for vulnerabilities
  - Port scan, ping sweep

- 3 – Enumerating
  - Hacker tries to gain access to resources or other information such as users, groups, and network shares
  - May use social engineering

- 4 – Attacking

Testing

Black box – no prior knowledge
Grey Box – some prior knowledge
White Box – All information needed



Student Check

You are conducting a penetration test on a software application for a client. The client provides you with details around some of the source code and development process. What type of test will you likely be conducting?

○ A. Black box
○ B. Vulnerability
○ C. White box
○ D. Answer A & C

Student Check

You are conducting a penetration test on a software application for a client. The client provides you with details around some of the source code and development process. What type of test will you likely be conducting?

- ○ A. Black box
- ○ B. Vulnerability
- ○ C. White box
- ○ D. Answer A & C

Student Check

Which of the following would be a reason to conduct a penetration test?

○ A. To passively test security controls
○ B. To identify the vulnerabilities
○ C. To test the adequacy of security measures put in place
○ D. To steal data for malicious purposes

Student Check

Which of the following would be a reason to conduct a penetration test?

- ○ **A. To passively test security controls**
- ○ **B. To identify the vulnerabilities**
- ○ **C. To test the adequacy of security measures put in place**
- ○ **D. To steal data for malicious purposes**