



Mississippi State
UNIVERSITY

J. A. “Drew” Hamilton, Jr., Ph.D.
Director, Center for Cyber Innovation
Professor, Computer Science & Engineering

CCI
Post Office Box 9627
Mississippi State, MS 39762

Voice: (662) 325-2294
Fax: (662) 325-7692
hamilton@cci.msstate.edu



Mississippi State University Center for Cyber Innovation



Threats, Attacks & Vulnerabilities

Reference:

Drew Hamilton Lecture Notes

Christopher I. G. Lanclos & DeMarcus Thomas

Security+ Exam Guide, 5th ed.

Conklin, White, Cothren, Davis and Williams



Domain Outline

- **Chapter 1: Malware & Indicators of Compromise**
- **Chapter 2: Attacks**
- **Chapter 3: Threat Actors**
- **Chapter 4: Vulnerability Scanning & Penetration Testing**
- **Chapter 5: Vulnerabilities & Impacts**



Malware and Indicators of Compromise Threats, Attacks & Vulnerabilities

Reference:

Drew Hamilton Lecture Notes

Christopher I. G. Lanclos & DeMarcus Thomas

Security+ Exam Guide, 5th ed.

Conklin, White, Cothren, Davis and Williams



Malware and Indicators of Compromise

- **This section will cover the following**
 - **Malware**
 - **Polymorphic malware**
 - **Ransomware**
 - **Rootkits**
 - **RAT**
 - **Etc.**
 - **Indicators of Compromise**
 - **Example Questions**



Malware

- **Malware is any software that has been design for some malicious intent or unwanted functionality**
- **Polymorphic malware is malware that can change its own code.**
 - **Used to trick anti-virus**
- **Armored Malware - encrypting malware is a way to slow down or protect malware from some types of malware analysis**
- **Many anti-virus software programs are signature-based detection**
 - **Signature-based detection compares malware to a list of other known malware**



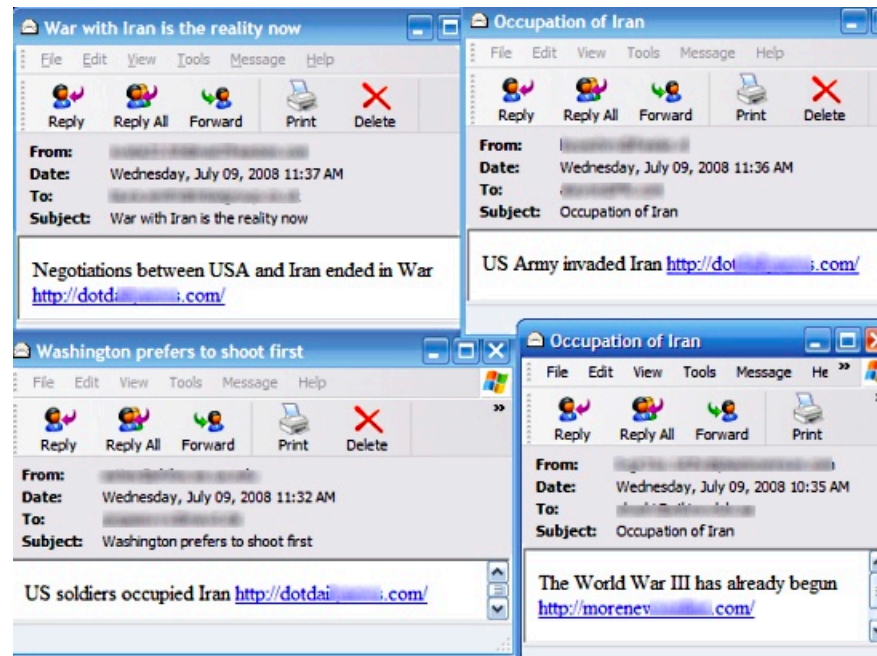
Malware cont.

- Designed to attack at least one of the principles from CIA triad



Polymorphic Malware Example

- **Storm Worm Email**
 - Spam email prominent in 2007
 - Evaded traditional anti-virus software by changing its source code every 30 minutes



Crypto-malware & Ransomware

- **Crypto-malware is malware that encrypts files on a computer system**
 - **It is used for multiple purposes**
 - **Denial-of-service**
 - **Ransomware (Most Common)**
- **WannaCry has infected over 300,000 computers globally**



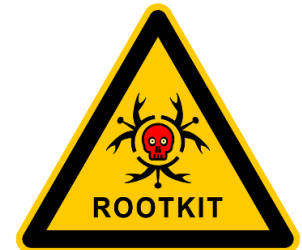
Rootkit Types

- **Modifies the operation of the operating system in some fashion to facilitate nonstandard functionality**
- **Rootkits are especially difficult to detect due to their ability to control system activity**
- **Common types of rootkits**
 - **Application**
 - **Replace standard files in your computer with rootkit files**
 - **Could change the way standard application work**
 - **Library**
 - **Most often impacts the system files used by the OS**
 - **Think Windows DLLs**



Rootkit Types cont.

- **Common types of rootkits**
 - **Kernel**
 - **Most severe type of rootkit as they work at the base of the operating system. Essentially can do anything**
 - **Virtual**
 - **Also called hypervisor rootkit which can intercept calls between the host OS and guest virtual machines**
 - **Firmware**
 - **This type of rootkit often does not have code integrity inspection and can go hidden**
 - **Can impact such things as a computer's hard drive system BIOS**



Keyloggers

- **Keyloggers**
 - **Are a piece of software that logs all the keystrokes of a system.**
 - **Purpose:**
 - **Monitoring user activity**
 - **Stealing passwords**



Viruses & Worms

- **Viruses are pieces of malware that replicate themselves by attaching to other executable files**
 - Requires user interaction to execute and spread
 - Must have some type of process or file to attach itself to
- **Worms are pieces of code that attempts to penetrate networks and computer systems**
 - Automatically execute and spread
 - Spread via email and/or instant messages
 - Can also explore vulnerabilities in network to spread to other systems



Trojan

- Trojans horse, name inspired by Troy
- Trojan horses are a piece of software that appears to do one thing but hides some other functionality



<https://www.rottentomatoes.com/m/troy/#&gid=1&pid=h-36836>



Operating System Security

Trojan Horses

- **Does NOT self-replicate**
- **Free program made available to unsuspecting user**
 - **Contains code to do harm**
- **Place altered version of utility program on victim's computer**
 - **trick user into running that program**
 - **/usr/mal/ls**
- **Rootkits**
- **Remote Access Tools**
 - **PCAnywhere**
 - **Lapl原因**
 - **Back Orifice**



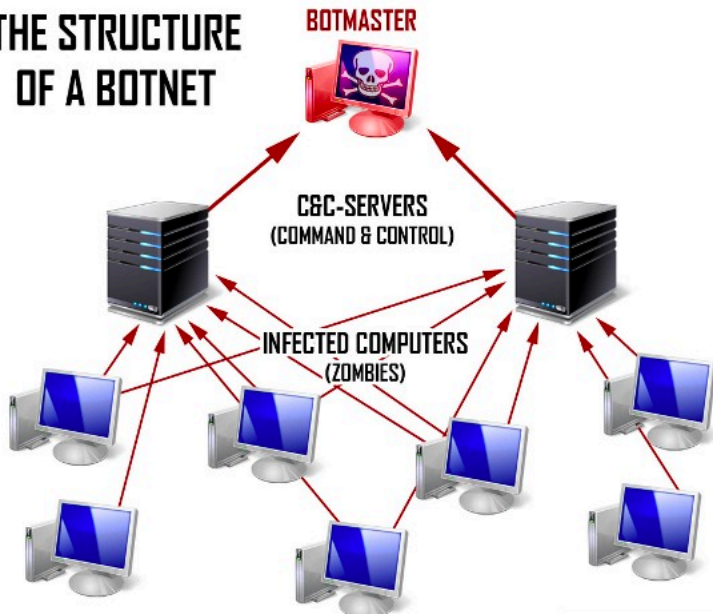
Adware & Spyware

- **Adware**
 - is software that presents unwanted ads
 - can be non-malicious, usually when you choose to use a free version of software for the trade-off of ad sharing being enabled
- **Spyware**
 - is software that “spies on users, recording and reports on their activities
 - Ex. Seeing an ad on your Facebook timeline about a product that you just looked up online.



Bots

THE STRUCTURE OF A BOTNET



Bots are a functioning piece of software that performs some task, under the control of another program.

- It is common that a program on one computer is controlling a program on another
- A group of bots is called a Botnet
- Used for a variety of functions

Good Bots or Not?

- **Good BOTs**
 - Search engines
 - Online games
 - IRC Bots
 - Price optimization
- **Bad BOTs**
 - Scan and distribute other malware
 - Send phishing emails and SPAM
 - DDoS attacks

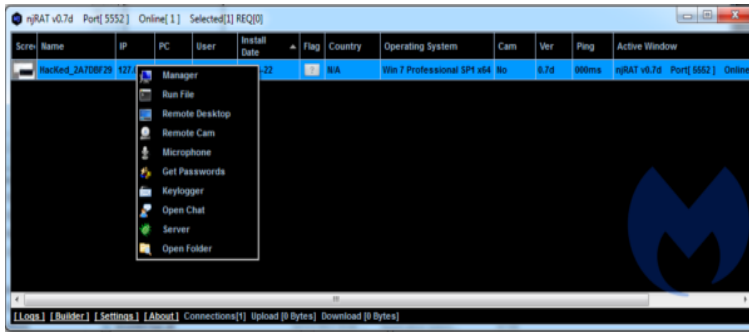


RATs, Logic Bombs & Backdoors

- **RAT (Remote Access Trojan)** A toolkit designed to provide the capability of covert surveillance and/or the capability to gain unauthorized access to a target system
- **Logic Bombs** are pieces of code that sit dormant for a period of time until some event or date invokes its malicious payload
- **Backdoors** are used to allow attackers to install other malware and continue to gain access to computer system



Remote Access Trojan



njRAT



BlackShades

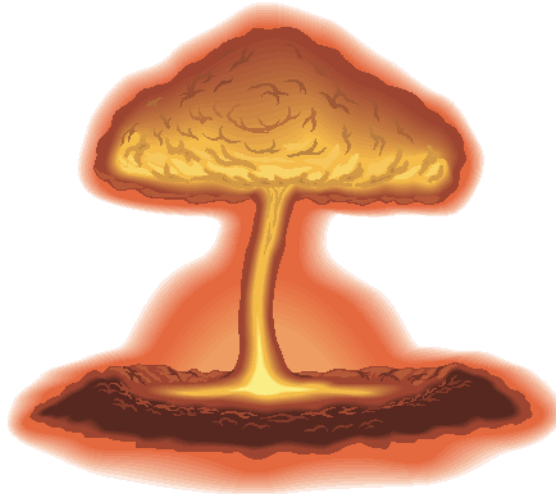


DarkComet



Logic Bombs

- **Company programmer writes program**
 - **Potential to do harm**
 - **OK if he/she enters password daily**
 - **If programmer fired, no password and bomb explodes**



Backdoors

```
while (TRUE) {  
    printf("login: ");  
    get_string(name);  
    disable_echoing();  
    printf("password: ");  
    get_string(password);  
    enable_echoing();  
    v = check_validity(name, password);  
    if (v) break;  
}  
execute_shell(name);
```

(a)

(a) Normal code.

```
while (TRUE) {  
    printf("login: ");  
    get_string(name);  
    disable_echoing();  
    printf("password: ");  
    get_string(password);  
    enable_echoing();  
    v = check_validity(name, password);  
    if (v || strcmp(name, "zzzzz") == 0) break;  
}  
execute_shell(name);
```

(b)

(b) Code with a trapdoor inserted



Indicators of Compromise

- **Indicators of Compromise (IOC)** are indicators that a system has been compromised by unauthorized activity.
- **Systems to communication IOCs** have been created:
 - **OpenIOC**
 - **STIX/TAXII/CybOx**



Indicators of Compromise

- Unusual outbound network traffic
- Anomalies in privileged user account activity
- Geographical irregularities in network traffic
- Account login red flags
- Increases in database read volumes
- HTML response sizes
- Large numbers of request for the same file
- Mismatched port-application traffic, including encrypted traffic on plain ports
- Suspicious registry or system file changes
- Unusual DNS requests
- Unexpected patching of systems
- Mobile device profile changes
- Bundles of data in the wrong place
- Web traffic with nonhuman behavior
- Signs of DDoS activity, even if temporary
- Strange mutexes



Chapter 1 Quiz

<https://forms.gle/GfJuToGVpMarmTFi8>



Attacks

Threats, Attacks & Vulnerabilities

Reference:

Drew Hamilton Lecture Notes

Christopher I. G. Lanclos & DeMarcus Thomas

Security+ Exam Guide, 5th ed.

Conklin, White, Cothren, Davis and Williams



Attacks

- **This section will cover the following**
 - **Social Engineering Methods**
 - **Phishing**
 - **Etc.**
 - **Application/Service Attacks**
 - **Wireless Attacks**
 - **Cryptographic Attacks**
 - **Example Questions**



What is Social Engineering?

- **“Hello. This is Dr. Burnett of the cardiology department at Balboa Naval Medical Center in San Diego. Your patient, General Simmons, has just been admitted here unconscious. He has an unusual ventricular arrhythmia. Can you tell me if there is anything relevant in his record?”**
- **“Hi, I lost my password, can you reset it and tell me what it is?”**

From: Peter.Pace@jcs.mil
Sent: Sunday, March 28, 2004 8:10 AM
To: admin@drew-hamilton.com
Subject: Re: Flag Briefing Attached

Please read the attached file.



Social Engineering

- **Social engineering is an attack against a person, and it involves social interactions**
- **The goal is to manipulate the person to divulge information.**
- **Defenses:**
 - **Have processes**
 - **Training and Awareness**

Methods

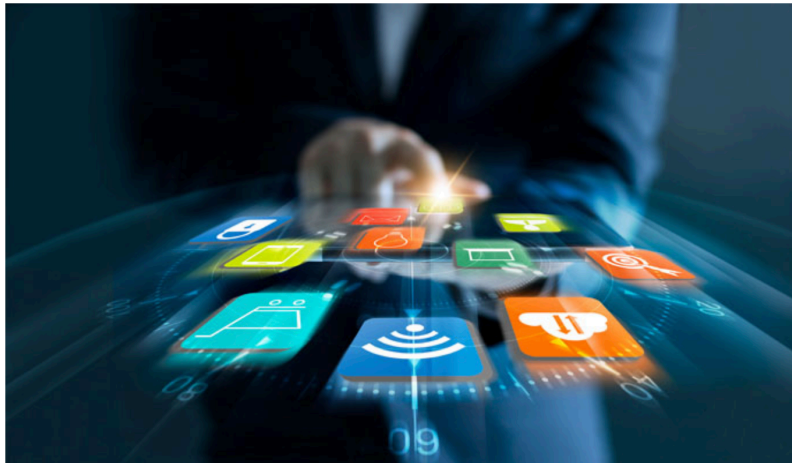
- **Phishing**
- **Spear phishing**
- **Whaling**
- **Vishing**
- **Tailgating**
- **Dumpster diving**
- **Shoulder surfing**
- **Hoax**
- **Watering hole attack**



Social Engineering in the News

Enterprise Mobile Phishing Attacks Spike Amid COVID-19 Crisis

Lookout research shows healthcare is the most targeted sector for phishing attacks, while enterprise mobile phishing attempts have steadily increased amid the COVID-19 crisis.



How to avoid the latest WhatsApp scam that aims to hijack your account

By Cat Ellis 12 days ago

Don't be their next victim



SE Types: Phishing

- **Pronounced “fishing”**
- **Social engineering technique where attackers attempt to obtain sensitive information by portraying themselves as a trusted party**
- **Attacks could target a variety of data**
 - **Username**
 - **Password**
 - **Credit card numbers**
 - **Bank accounts**
 - **Etc.**



SE Types: Spear Phishing



- **More targeted attacks that are geared towards a specific group of people**
 - **Students at a University**
 - **Employees from an organization**
 - **Family members**
 - **Etc.**
- **Attacks often use some type of background information that makes the email more plausible**

SE Types: Whaling

- **Attackers using this technique are targeting high value individuals**
 - Administrators
 - University Presidents
 - CEOs
 - CFOs
 - Etc.
- **These attacks are designed to look like normal business operations**



SE Types: Vishing

- **Variation of phishing that uses voice communication technology to obtain information the attacker is seeking**
- **Using Voice over IP (VoIP) technology, attackers can spoof (simulate) legitimate entities**
 - **Helps in establishing a level of trust with users**
- **Obtain use a sense of urgency to encourage information to be disclosed**



SE Types: Tailgating

- Also known as piggybacking
- Tactic of following closely behind a person who has just used their own access card or personal identification number (PIN) to access a room or building
- Attacker may attempt to start conversation with employees or carry large boxes to increase the chances of entering a building



SE Types: Dumpster Diving

- **Process of digging through a target's trash to find valuable information**
- **This tactic can be used on its own to steal information or can be a prerequisite to spear phishing or whaling**
 - **Not unique to the security community**
 - **Used by identify theft thieves, private investigators, law enforcement, etc.**
- **Consider shredding documents and securing trash receptacles**



SE Types: Shoulder Surfing

- **Attacker observing a target entering sensitive information on a form, keypad, or keyboard**
- **This could be as simple as looking over a shoulder or could be more concerted with such as action as installing cameras**
- **Many locations now have installed simple shields to protect against these types of observations**



SE Types: Impersonation

- **This tactic can be employed in many contexts**
 - In person
 - Over the phone
 - Online
- **Attacker uses the potential victim's biases to follow procedures**
- **Examples**
 - Third-Party Authorization
 - Help Desk/Tech Support
 - Contractors/ Outside Parties
 - Online Attacks



SE Types: Impersonation cont.

- **The most effective defense against impersonation attacks is to have a clear procedure, make sure the procedure is unambiguous, and periodically retrain your employees**



SE Types: Hoax

- **Presents some sort of fake news or false event to spur users to perform an action**
 - **Describing some destructive new malware and getting users to edit their systems to protect themselves**
 - **Providing new COVID-19 vaccine information and asking to share personal information to check for eligibility**
 - **Discussing an event that will negatively impact a company and a fellow co-worker has sent you a link to get more information**



SE Types: Watering Hole Attack

- **Goes against the common tactic of attacking users directly**
- **The focus is on placing malware on websites that are used frequently to infect users in this passive manner**
- **Watering hole attacks are complex to achieve and appear to be backed by nation states and other high-resource attackers**
 - **In light of the stakes, the typical attack vector will be a zero day attack to further avoid detection**



Social Engineering Principles

- **Authority in social situations can lead to an environment where one party feels at risk in challenging another over an issue**
- **Intimidation can be either subtle, through perceived power, or more direct, through the use of communications that build an expectation of superiority**
 - **Third-Party Authorization**
 - **Help Desk/Tech Support**
 - **Contractors/Outside Parties**
 - **Online Attacks**



Social Engineering Principles cont.

- **Consensus is a group-wide decision.**
- **Scarcity is short supply of something that is perceived to be needed.**
- **Familiarity is creating a connection or making someone feel connected.**
- **Trust is defined as having an understanding of how something will act under specific conditions**
- **Urgency is created by making time have a shortage.**



Social Engineering Summary

- **Key in all social engineering attacks is that you are manipulating a person and their actions by manipulating their perception of a situation**
- **Most common methods to protect against social engineering is through training and awareness**



Denial-of-Service

- **Denial-of-Service (DoS) attacks can exploit a known vulnerability in a specific application or operating system by deny access to it**
- **Distributed (DDoS) attack is the same but using multiple systems to attack**
- **Example:**
 - **SYN flooding**
 - **Ping of death**
- **Amplification is a trick where an attacker uses a specific protocol aspect to achieve what a single machine cannot by itself**



IP Security Overview

- **IP Packets have no inherent security**
 - **Relatively easy to**
 - **forge contents of IP packets**
 - **modify contents of IP packets**
 - **inspect the contents of IP packets in transit**
- **Therefore, there is no guarantee that IP datagrams received:**
 - **are from the claimed sender (source address in the IP header)**
 - **contain the original data that the sender placed in them**
 - **were not inspected by a third party while the packet was being sent from source to destination**



TCP Review

- **The establishment of a TCP connection typically requires the exchange of three Internet packets between two machines in an interchange known as the TCP three-way handshake. Here's how it works:**
 - **SYN:** A TCP client (such as a web browser, ftp client, etc.) initiates a connection with a TCP server by sending a SYN packet to the server.
 - **SYN/ACK:** When a connection-requesting SYN packet is received at an 'open' TCP service port, the server's operating system replies with a connection-accepting SYN/ACK packet.
 - **ACK:** When the client receives the server's acknowledging SYN/ACK packet for the pending connection, it replies with an ACK packet.



TCP Three-Way Handshake

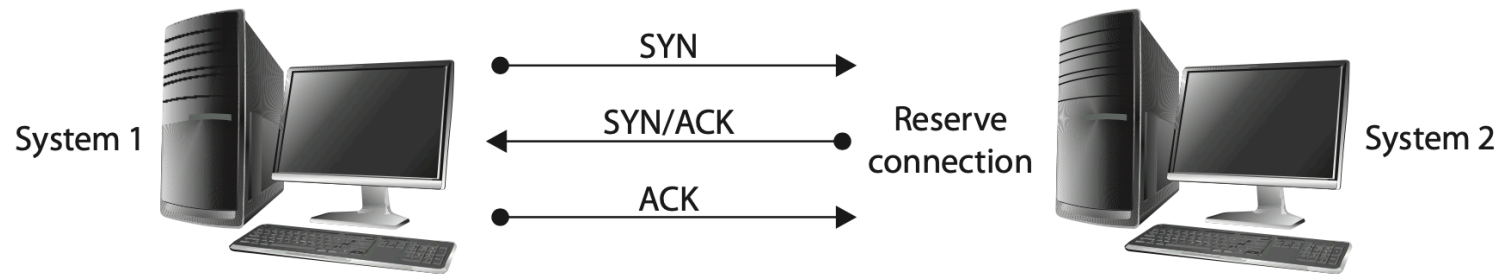


Figure 2-1 The TCP three-way handshake

Bandwidth Consumption DoS

- **Traditional SYN flooding DoS attacks are either one-on-one**
 - (one machine sending out enough SYN packets to the target machine to effectively choke off access to the other machine)
- **or many-on-one**
 - (SYN flooding ‘zombie’ programs loaded by the attacker into compromised machines and commanded by the attacker to send huge volumes of SYN commands to the target machine).



SYN Flood Attack

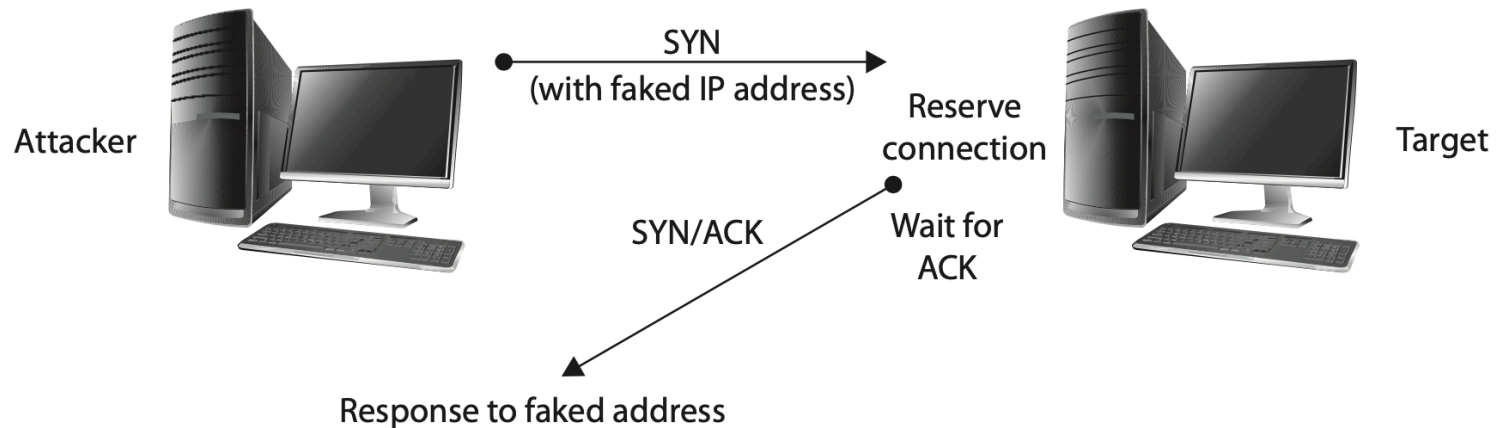
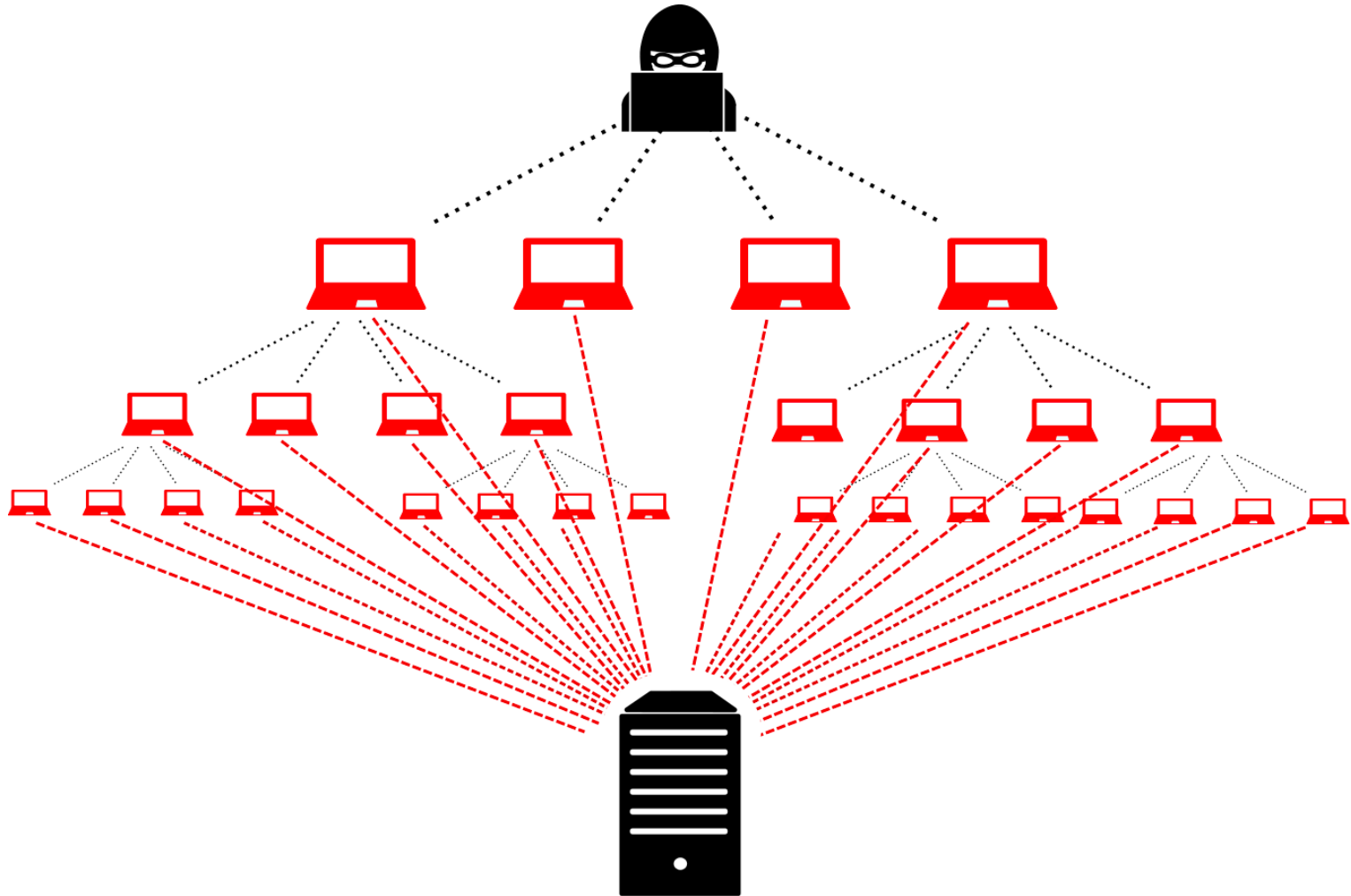


Figure 2-2 A SYN flooding DoS attack

DDoS SYN Flood

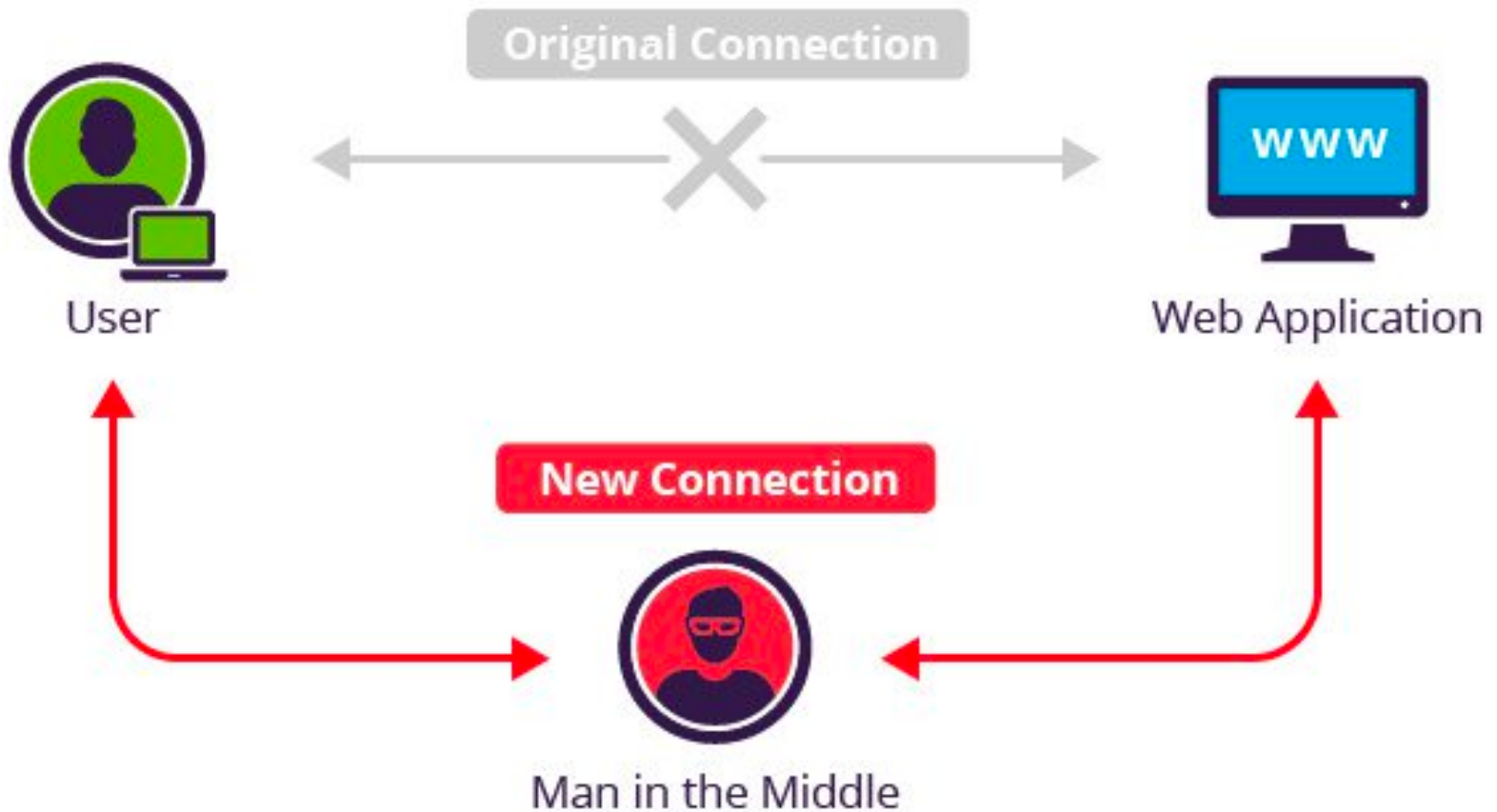


Man-in-the-Middle

- **Man-in-the-middle attack occurs when an attacker can put himself between two systems to communicate.**
- **This is done by ensuring that all communication going to or from the target host is routed through the attacker**
- **Example: Session hijacking can occur when information such as a cookie is stolen, which is used to allow the attacker to impersonate the legitimate session**



MITM Diagram



Buffer Overflow

- **Buffer overflows are input validation attacks, designed to take advantage of input routines that do not validate the length of inputs**
- **Simple and solvable, some languages are more prone to this attack**



Useful Definitions

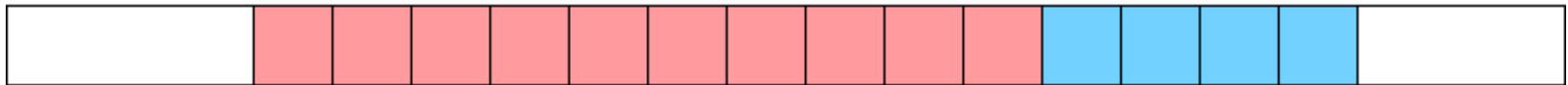
- The **heap** is an area of memory reserved for data that is created at runtime -- that is, when the program actually *executes*.
 - `malloc()` or `new`
- The **stack** is an area of memory used for data whose size can be determined when the program is *compiled*.
- When contiguous chunks of the same data type are allocated, the memory region is known as a **buffer**.
- **Buffer overflow** occurs by writing past the end of an array.
- **Bounds checking** refers to programmer and compiler strategies for preventing buffer overflows.



Buffer Overflow Example

```
char buf[10];
```

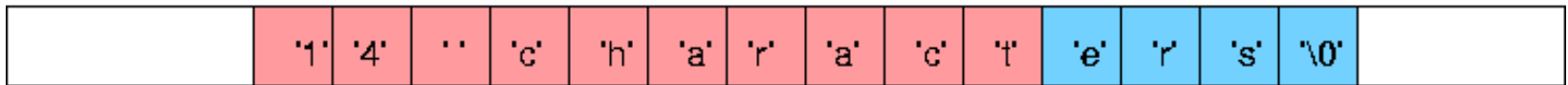
```
int x;
```



```
strcpy (buf, "14 characters");
```

```
char buf[10];
```

```
int x;
```

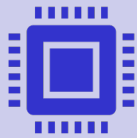


C, an average programming language

- **C is inherently unsafe – programs may overflow buffers at will.**
- **No runtime checks that prevent writing past the end of a buffer.**
- **Reading or writing past the end of a buffer can cause several behaviors**
 - **Programs may act in strange ways**
 - **Programs may fail completely**
 - **Programs may proceed without any noticeable difference in execution.**
- **Damage from a buffer overrun depends on:**
 - **How much data is written past the buffer bounds**
 - **What data (if any) are overwritten when the buffer gets full and spills over**
 - **Whether the program attempts to read data that are overwritten during the overflow**
 - **What data end up replacing the memory that gets overwritten**



Injection



SQL injection attacks involve the manipulation of input, resulting in a SQL statement that is different than intended by the designer



Similar:

XML

LDAP



Command injection attacks can occur when input is used in a fashion that allows command-line manipulation.

This can give an attacker command-line access at the privilege level of the application.



Cross-Site Scripting (XSS)

- **Cross-site scripting is when an attacker can include a script in their input and have it run as a web process.**
 - **Non-persistent XSS attack is immediately executed and passed back through a web server.**
 - **Persistent XSS attack is permanently stored on the web server or some back-end storage, which can spread to other users.**
 - **DOM-based XSS attack is executed in the browser in a Document Object Model (DOM) process verse the other attacks which happen on the web servers**
- **Caused by: Weak user input validation.**



Cross-Site Request Forgery

- **Cross-site request forgery (XSRF) attacks utilize unintended behaviors that are proper in defined use but are performed under circumstances outside the authorized use**
- **Example:**
 - **Assume your bank allows you to log in and perform financial transactions but does not validate the authentication for each subsequent transaction. If a user is logged in and has not closed their browser, then an action in another browser tab could send a hidden request to the bank, resulting in a transaction that appears to be authorized but in fact was not done by the user.**



ARP Poisoning

- **ARP (Address Resolution Protocol) Poisoning involves putting false information in an ARP table, which is used to direct packets from one machine to another, so that the packets are sent to the attackers.**
- **This allows the attacker get the information about the conversation between the machines**
- **Attackers can also inject themselves into conversation and provide false information**
 - **Performing a MITM attack**



DNS Poisoning & Domain Hijacking

- **Domain Name System (DNS) Poisoning is when the server information, specifically IP address, is changed to a false location**
- **Domain hijacking is the act of changing the registration of a domain name without the permission of its original registrant**



Zero Day, Replay and Pass the Hash



Zero-day attack is one that uses a vulnerability for which there is no previous knowledge outside of the attacker, or at least not the software vendor



Replay attacks occur when an attacker captures a portion of a communication between two parties and retransmits it later (Similar to Man-the-middle)



Pass the hash is a hacking technique where the attacker captures the hash used to authenticate a process



Hijacking Type Attacks

- **Hijacking is a form of attack where the attack takes over a user's experience**
- **Clickjacking is an attack against the design element of a user interface**
- **Session Hijacking are terms used to refer to the process of taking control of an already existing session between a client and a server**



Hijacking Type Attacks cont.

- **URL Hijacking is an attack that targets the URL**
 - **Generic name for a wide range of attacks that target the URL**
 - **Typo Squatting is an attack form that involves capitalizing upon common typo errors when writing URL**



Spoofting

- **Spoofting is the nothing more than making data look like it has come from a different source**
 - **MAC Spoofting is changing a MAC address to bypass security checks based on the MAC address.**
 - **IP Address Spoofting is designed to work so that the originators of any IP packet include their own IP address, so that the attacker can inject their IP address.**
 - **Smurf Attack is when the attacker sends a spoofed packet to the broadcast address for a network.**



Spoofting

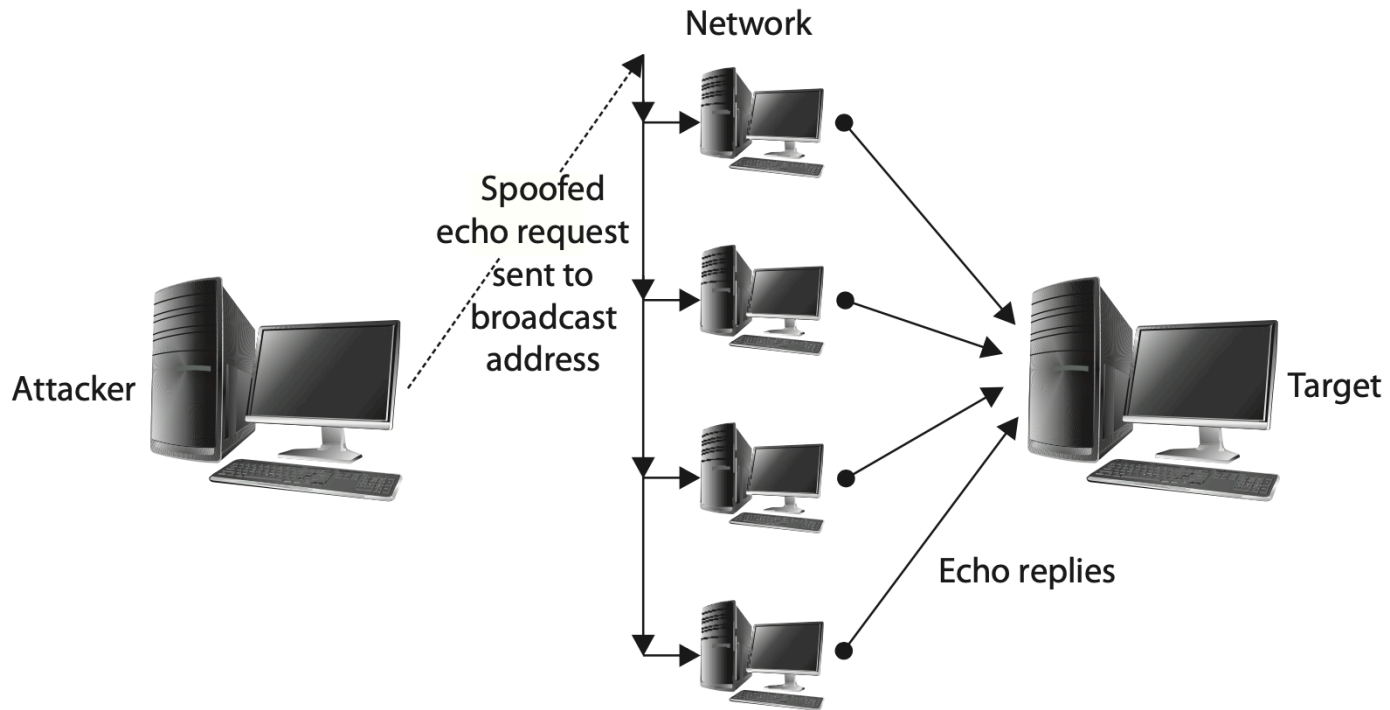


Figure 2-8 CompTIA Security+ All-in-One Exam Guide

Wireless Attacks

- **Replay attacks on wireless attacks works by repeating information to get a system to repeat a behavior.**
- **Initialization Vectors (IV) are used to start a connection, this attack tries to figure it out so it can figure out the repeating key sequence.**
- **Evil Twin is an attack against the wireless protocol via substitute hardware, that pretends to be a legitimate connection.**
- **Rogue AP (Access Point) attempts to get clients to connect to it as if it were authorized and then simply authenticate to the real AP.**
- **Jamming is a form of DoS that targets the radio spectrum aspect of wireless.**



More Wireless Attacks

- **Bluejacking is a term used for the sending of unauthorized messages through Bluetooth devices.**
- **Bluesnarfing is copying information from the user's device.**
- **Radio Frequency Identification (RFID) attacks can range from attacks against the RFID devices themselves, the communication channels being used or the readers and back-end system.**
- **Near field communication (NFC) is a set of wireless technologies that enable smartphones and other devices to pass information**
- **Disassociation attacks against a wireless system are attacks design to disassociate a host from the wireless access point, and from the wireless network.**
 - **Accomplished by taking advantage of the de-authentication frame in the Wi-Fi protocol.**



Cryptographic Attacks



Birthday attacks are a special type of brute force attack that uses the birthday problem in statistics as its bases. Essentially, in a birthday attack your trying to find collisions of a hash function.



Known plaintext/ciphertext attacks rely on knowing the original plaintext and ciphertext of a message and is used then to determine the key through brute force attempts.



Cryptographic Attacks (2)



Rainbow tables are precomputed tables or hash values related to passwords.

Defense against this are salted strings being adding to the end of the information being hashed.



Dictionary attacks refers to a password-cracking program that uses a list of dictionary words to try to guess password



Brute force attacks are the only reliable way of password-cracking but if following good password practices it is unpractical to do it.

Online when it happens in real life.
Offline is when you compare hashes after stealing the password file



Cryptographic Attacks (3)

- **Brute force attacks are the only reliable way of password-cracking.**
 - **Defense is to make brute force infeasible**
 - **Limit guesses**
 - **Monitor failed access attempts**
 - **Online when it happens in real life.**
 - **Offline is when you compare hashes after stealing the password file**
- **Many password attacks rely on:**
 - **Collision attacks**
 - **Trying to use different input to produce the hash of another input**



Downgrade and Weak Implementation

- **Downgrade attacks are used to downgrade the encryption used between the server and browser, by lowering the supported encryption allowed by one of the systems**
- **Weak implementation is when software or protocols are used that are old or have been basically installed without any defense-in-depth**
- **Weak implementations are another problem associated with backward compatibility.**



Chapter 2: Quiz

<https://forms.gle/yjR6KChWRu71Ukm8A>



Threat Actors

Threats, Attacks & Vulnerabilities

Reference:

Drew Hamilton Lecture Notes

Christopher I. G. Lanclos & DeMarcus Thomas

Security+ Exam Guide, 5th ed.

Conklin, White, Cothren, Davis and Williams



Threat Actors

- **This chapter will cover the following**
 - **Types of Actors**
 - **Attributes of Actors**
 - **Use of Open Source Intelligence**
 - **Example Questions**



Threat Actors



Script Kiddies are people who do not have much technical expertise to develop their own scripts or find new vulnerabilities



Hacktivists have a range of technical expertise, usually not very high, and are motivated by their beliefs

Often see themselves as humanitarians

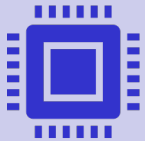


Organized Crime is no different from criminal activity offline: fraud, extortion, theft, embezzlement, and forgery

Structured threat category is characterized by a greater amount of planning, which is different from script kiddies and sometimes hacktivists.



Threat Actors cont.



Nation States/APT (Advance Persistent Threats) usually have elite hackers.

APT many times require a lot of resources, planning and timing, which is why they are usually supported by Nation States. Targets are usually infrastructure.



Competitors are usually related to businesses, which are trying to copy, steal or disrupt normal business.



Categories of Threat Actors

- **Unstructured Threat**
 - Involve attacks that occur over a short period of time
 - Do not include many people and have little financial backing
 - **Script Kiddies**
 - **Hacktivist**
- **Structured Threat**
 - Characterized by an extended amount of planning
 - Activity are executed over longer durations of time and can have some consistent financial backing
 - **Organized Crime**



Categories of Threat Actors cont.

- **Highly Structured Threat**
 - Tend to include planning periods of a year or longer
 - Backed by significant financial resources
 - Includes a larger group of well-organized participants
 - **Nation State Attacks**
 - Often develop capabilities in information warfare
- **Advanced Persistent Threats (APTs)**
 - Highlighted by toolkits to achieve access on networks
 - Do not just steal information, but maintains persistence on the target network
 - Primary goals are to maintain admin access and avoiding detection on a target network



Attributes of Actors

- **Internal threats are the most dangerous because threat actors are more likely to have physical access to systems**
 - **Common failure for installing security mechanisms is not accounting for insider attacks**
 - **In some cases services such as janitorial staff can not only have physical access to facilities, but also to computer systems and networks.**
- **External threats are threats that come from outside**
 - **Presents many of the same problems as with internal threats**
 - **External attackers have the added step of establishing persistence on system under attack**



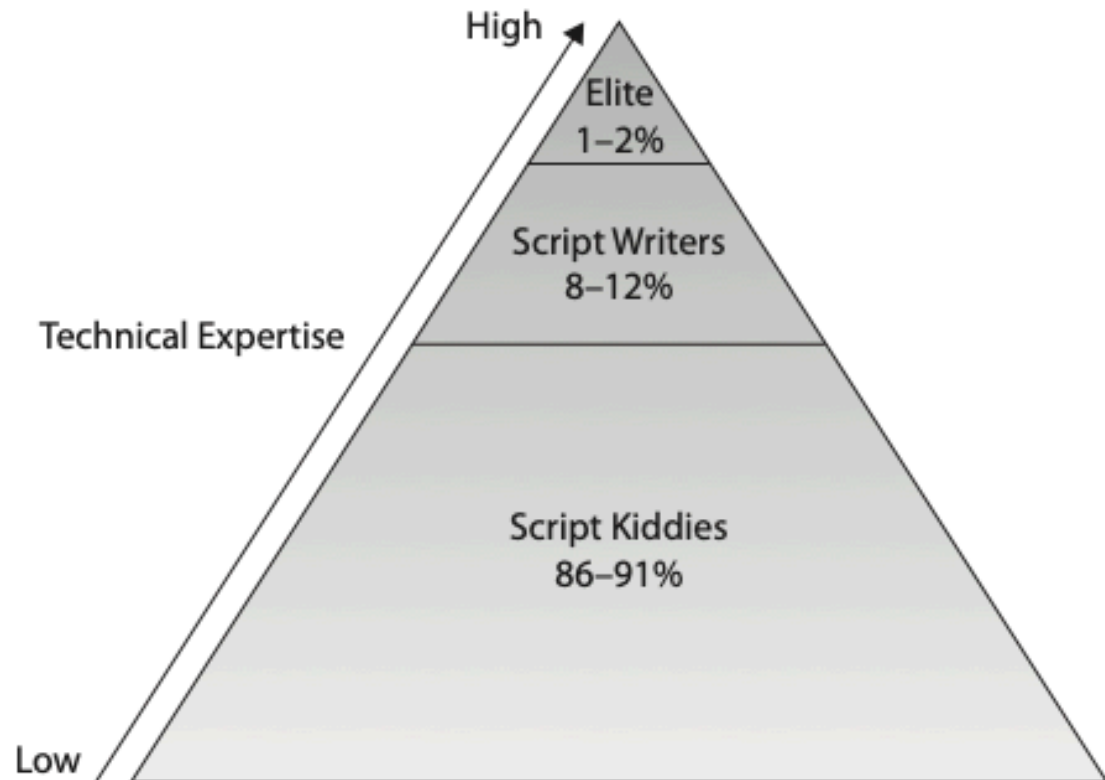
Attributes of Actors cont.

- **Available resources play a huge part of determining the type of attacker and their capabilities**
- **Motivations range from learning, notoriety, good causes, money, revenge, war, etc.**
- **Level of sophistication plays a major role in identifying actors**
 - **The skillset of an attacker could be an indicator of what type of groups they are working for**



Attacker Skill Level

Figure 3-1
Distribution of
attacker skill
levels



Open Source Intelligence

- **Open source intelligence is data collected from public sources**
- **Cybersecurity is a game of resource management**
 - **Firms won't be able to protect against all threats**
 - **Requires prioritization on what business needs are most important**
- **Threat intelligence is the gathering of information from a variety of sources to prepare for most likely attacks**
 - **Groups that do that:**
 - **Information Sharing and Analysis Organizations (ISAOs)**
 - **Information Sharing Analysis Centers (IASCs)**



OSINT Malicious Usage

- **OSINT represents a constant threat to any organization or mission, and can account for up to 80% of actionable intelligence, which is generally not protected and not classified**
- **In most cases, it's legal to obtain information in this way. This means that despite the high potential for harm, this critical information may be obtained at little or no risk to the intruder**

OSINT: Open Source Intelligence; publicly available information. i.e., information that any member of the public could lawfully obtain by request or observation, as well as other unclassified information that has limited public distribution or access.



OSINT Sources

- Intelligence can be gathered from a broad range of publicly available sources
- Media
 - Television, radio, newspaper, magazines
- Internet
 - Search engines
 - Google, DuckDuckGo, Bing, Yahoo
 - User-generated content
 - Blogs, forums, social-networking, wikis
 - RSS feeds
 - Peer to Peer (P2P)
- Geographic
 - Maps and environmental and navigational data
- Observation
 - Camera, video recorder, reporting



Chapter 3:

<https://forms.gle/RFEfskVkt16Citfc6>



Vulnerability Scanning & Penetration Testing

Threats, Attacks & Vulnerabilities

Reference:

Drew Hamilton Lecture Notes

Christopher I. G. Lanclos & DeMarcus Thomas

Security+ Exam Guide, 5th ed.

Conklin, White, Cothren, Davis and Williams



Vulnerability Scanning Concepts

- **This chapter will cover the following**
 - **Penetration Test Concepts**
 - **White Box**
 - **Black Box**
 - **Etc.**
 - **Vulnerability Scanning Concepts**
 - **Identify Vulnerability**
 - **Etc.**
 - **Example Questions**



Penetration Testing

- **Penetration testing is simulating attacks from malicious outsiders by probing your network and system**
 - **Testing employees**
 - **Testing vulnerabilities**
- **Essentially penetration testers are acting like malicious attackers**



Types of Reconnaissance

- **Active Reconnaissance**
 - **Testing that involves tools that interact with the network.**
 - **Checking for active system on a network**
 - **Checking for open ports on a system**
- **Passive Reconnaissance is the use of tools that do not provide information to the network or system under investigation**
 - **Google**
 - **Shodan**



Active and Passive Security Threats

Passive Threats

Traffic Analysis

Compromise of
Message Contents

Active Threats

Masquerade

Replay

Denial of
Service

Msg Content
Modification



Passive vs. Active Tools

- **Passive Tools**
 - Receive traffic only and do nothing to the traffic flow.
 - Ex. Wireshark
- **Active Tools**
 - Active tools modify or send traffic and are thus discoverable by their traffic patterns.
 - Ex. Nmap (Network Mapper)



Penetration Testing Concepts

- **Pivot is a key method used by a pen tester or attacker to move across to a network**
 - They must gain access to one computer on network and use it to access others.
- **Initial exploitation is used to show that a vulnerability is present and exploitable**
- **Persistence is part of very high level attacks**
 - APTs, which focus on invisibility and persistence
 - Penetration testers seek to determine if this is possible



Black, White and Gray Box Testing

- **Black Box Testing is testing a system without having any prior information**
- **White Box Testing is testing based on the information you know about the system**
- **Gray Box Testing is having some knowledge of the system but not much, helps to narrow testing**



Difference Between Penetration Testing and Vulnerability Scanning

- **Vulnerability scanning is the scanning of a system for vulnerabilities, whether they are exploitable or not**
- **Penetration testing is the examination of a system for vulnerabilities that can be exploited**



Vulnerability Scanning Concepts

- **Vulnerability scanners are designed to help administrators discover vulnerabilities**
 - **Nessus**
 - **Nmap**
 - **Zmap**
- **While performing a vulnerability scan access controls are tested**
 - **This is called passive testing**
 - **Target of the vulnerability scanner is the system, not the controls**
- **Vulnerability scanners can only scan for identified vulnerabilities**



Vulnerability Scanning Concepts Cont.

- **Many vulnerabilities come from misconfiguration of a system**
- **Intrusive vs. Non-intrusive**
 - **Intrusive scanners perform tests that change the state of the system.**
 - **Non-intrusive methods do not directly interact with the vulnerability, less accurate than intrusive**
- **Credential vs. Non-credentialed is the difference between scanning with or without credentials.**
 - **Credentials that will be more accurate in determining whether the vulnerabilities exist.**



False Positive and Negative

- **False positive is an incorrect finding.**
 - Type I Error
- **False negative is when the scanner fails to report a vulnerability that does exist.**
 - Type II Error

		Reality	
		True	False
Measured or Perceived	True	Correct 😊	Type 1 error False Positive
	False	Type 2 error False Negative	Correct 😊



Chapter 4 Quiz

<https://forms.gle/a9iqoVMkmCihwv6A7>



Vulnerabilities and Impacts Threats, Attacks & Vulnerabilities

Reference:

Drew Hamilton Lecture Notes

Christopher I. G. Lanclos & DeMarcus Thomas

Security+ Exam Guide, 5th ed.

Conklin, White, Cothren, Davis and Williams



Vulnerabilities and Impacts

- **This chapter will cover the following**
 - **Race Conditions**
 - **System Vulnerabilities**
 - **Improper Input Handling**
 - **Improper Error Handling**
 - **Misconfiguration/Weak Configuration**
 - **Etc.**
 - **Example Questions**



Vulnerabilities

- **Vulnerabilities are specific characteristics of a system that an attacker exploits to violate the system**
- **Vulnerabilities are the source of virtually all security concerns.**



Race Conditions

- **Race Conditions** are an error condition that occurs when the output of a function is dependent on the sequence or time of the inputs
- **Problem:** The issue is when the sequence of events does not happen in the order that is intended
- **Where:** Multithreaded or distributed programs
- **Effect:** Crashing System (Denial-of-Service), Elevated Privilege
- **Prevention:** Reference counters, kernel locks and thread synchronization.



Race Condition Example



Process P1

count
5



Process P2

End-of-life systems (System Vulnerabilities)

- **End-of-life is defined as when the system has reached a point where it can no longer function as intended.**
- **Problem: Lack of vendor support, a failure to instantiate on new hardware and incompatibility with other aspects of system.**
- **Where: Total system**
- **Effect: Leaves computer vulnerable to attacks or possibly unusable.**
- **Prevention: Upgrade or change vendors.**

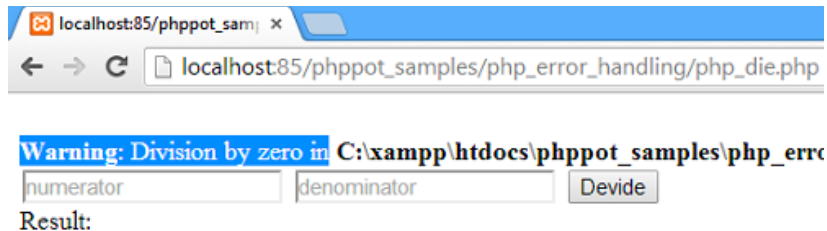
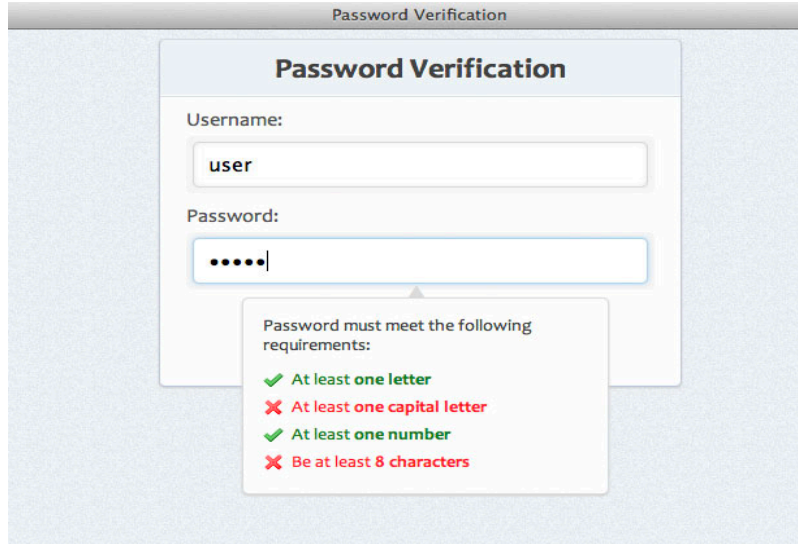


System Vulnerabilities

- **Embedded systems are systems that are inside other systems or a module or component of a larger system**
 - Usually, only providing one purpose not effected by other system
- **Lack of vendor support is a vulnerability when systems start to age or need to be integrated with other systems and vender is not working that side of the software**



Improper Input and Error Handling



- **Improper Input Handling**
 - When validation is not done correctly or thoroughly and allows input that it should not
- **Improper Error Handling**
 - When an error occurs it reveals some information to the user that it should not



Configuration Vulnerabilities

- **Misconfiguration and Weak Configuration causes vulnerabilities that would not exist if configured correctly**
- **Misconfiguration and Weak Configuration can happen to many different components in a network**
- **Misconfiguration or weak configuration can come from the default configuration of a system.**
 - **Default configuration may allow for desired functional outcome but lack security measures**



Other Vulnerabilities (2)

- **Resource Exhaustion**
 - State where a system does not have all the resources it needs to continue to function
- **Untrained Users**
 - User who does not know how to operate the system correctly
- **Improperly Configured Accounts**
 - Allows accounts to have the wrong access controls



Other Vulnerabilities (3)

- **Vulnerable Business Processes**
 - Usually an automated process that increase the speed to failure, usually doing something with no verification
 - A simple example would be paying an invoice without matching it to an approved purchase order. A common form of fraud is to send an invoice to an organization for goods or services that were not provided
- **Weak Cipher Suites**
 - Those that were considered secure but are no longer viable, but still are being used
 - Using older SSL versions with known vulnerabilities
- **Weak Implementations**
 - Security options that are known to have vulnerabilities that allow you to bypass them
 - Using WEP Wireless Security Algorithm



Memory and Buffer Vulnerability

- **Memory Leaks** are programming errors caused when a computer program does not properly handle memory resources
- **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
- **Buffer Overflow attacks** are input validation attacks, designed to take advantage of input routines that do not validate the length of inputs



Memory and Buffer Vulnerability (2)

- **Pointer Dereference** now changes the meaning of the object to the contents of the memory location, not the location as identified by the pointer

```
#include <stdio.h>

int main( int argc, char *argv[] ) {
    int x, y;
    int *p;

    x = 5;
    p = &x;
    y = *p; /* same as y = x */

    return 0;
}
```

Memory	Address
x = 5	0x0
y = 5	0x1
p = 0x0	0x2
	0x3
	0x4
	0x5
	0x6
	0x7
	0x8
	0x9



Memory and Buffer Vulnerability (3)

- **DLL Injection is the process of adding to a program at run time a DLL that has a specific vulnerability or function that can be capitalized upon by an attacker**



System Sprawl/Undocumented Assets

- **System Sprawl** is when a system expands over time, adding elements and functionality, and over time the growth and changes are not documented
 - This usually produces **Undocumented Assets**, which means that these specific assets are not necessarily included in plans for upgrades, security, etc.
 - This can lead to outdated system component that can then be exploited



Improper Certificate and Key Management

- **Improper Certificate Management is an issue because it is used to transfer and manage cryptographic keys**
 - A certificate is a digital document that provides a status on cryptographic keys
 - If certificates are not managed and kept up to date, expired or compromised keys could be used
- **Improper Key Management is an issue because allowing access to the keys gives the ability to use the keys improperly**



Chapter 5 Quiz

<https://forms.gle/YYZmMdmeQTqqoBHf7>



Chapter Summary

- **Chapter 1: Malware & Indicators of Compromise**
- **Chapter 2: Attacks**
- **Chapter 3: Threat Actors**
- **Chapter 4: Vulnerability Scanning & Penetration Testing**
- **Chapter 5: Vulnerabilities & Impacts**

