Cyber Attacks & Defense

Lesson 1: Attacks and Attackers

CIS377

Dr. Atul Rawal

References:

Learning Outcomes

TOWSON UNIVERSITY

Upon completion of this lesson, students will be able to:

- Analyze a cybersecurity attack case study in order to determine the vulnerability, threat, exploits and the attackers.
- Draw conclusions and reflect on a cybersecurity attack case study using adversarial thinking.

Attacks

Vocabulary

- Define the following terms in your own words:
    - Threats
    - Vulnerabilities
    - Attacks
    - Exploits

Threats

A threat is the likelihood that something harmful could occur.

- If you shop online, there is a **threat** of Identity theft.
- If you use a computer online, there is a **threat** of getting a virus.
- For more details see https://csrc.nist.gov/glossary/term/threat

What are some examples of threats to you (individual), your organization (Industries and companies) and this nation?

- https://www.owasp.org/index.php/Category:Threat

Threat

- Object, person, or other entity that presents an ongoing danger to an asset.
- External threat increases when an organization connects to the internet.
- 65% of the world’s 8 billion people are connected to the internet.

Category of threats

- Compromise to intellectual property
- Software attacks – virus, worms, macros, dos
- Espionage or trespass
- Forces of nature
- Human error or failure
- Information extortion
- Sabotage or vandalism
- Theft
- Technical hardware failure or errors
- Technical software failure or errors
- Technological obsolescence

Compromise to intellectual property (IP)

- IP – ownership of ideas and control over the tangible or virtual representation of those ideas.
- Trade secrets
- Copyrights
- Trademarks
- Patents
- Software piracy

Vulnerability

- A vulnerability is a hole or a weakness that could be exploited to attack a specific target.
- Examples
  - If I leave my door open, it makes me susceptible to a burglar.
  - Unsecure ports running on a network e.g. Telnet
- What are some examples of vulnerabilities to an individual, organization and Nation?
- https://www.owasp.org/index.php/Category:Vulnerability

Attacks and Exploits

- An attack occurs when you take advantage of a vulnerability in a system.
- An exploit is a piece of software that takes advantage of a vulnerability in the target system.
- Sometimes the word attacks and exploits are used interchangeably, depending on the context.
  - Example – A system has been exploited or A system has been attacked.

- Activity
- What are some examples of attacks/exploits that have occurred recently?
- What is the threat and/or vulnerability that was exploited?

ATTACKERS

Section 1.2

Purpose of an Attack

- What are some reasons for an attack?
  - Malicious
  - Financial
  - Competition
- What are some examples of attacks that may have occurred for some of the reasons listed above?
- Are there other reasons for attacks?

Vocabulary

- Define the following terms in your own words:
  - Black Hat Hacker
  - White Hat Hacker
  - Grey Hat Hacker
  - Ethical Hacker
  - Hacktivist
  - Nation State Hacker
  - Insider Threat
  - Advanced Persistent Threat (APT)

White, Black or Grey Hat?

White Hat Hackers – Hack with permission from a specific entity.

- Example - An organization may hire a white hat hacker to find all the vulnerabilities in their system so that it can be patched before someone takes advantage of it.

Black Hat Hackers – Hack for malicious reasons or personal gain. They do not have permission from the entity.

- Example – If you use public WIFI and someone gets your email password and logs into your email. That individual is a Black Hat Hacker

Grey Hat Hackers – Hack without permission but not for malicious reasons.

- Example – An individual hacks into a company's network and provides the company the information so that they can fix the vulnerability.

Insider Threat and Advanced Persistent Threat(APT)

- Insider Threat

  A member of an organization or an employee who uses his or her access as a member of the organization to attack the specific organization

- Advanced Persistent Threat (APT)

  An attacker who has sophisticated tools and expertise to perform different forms of attacks in order to gain access to a system and remain in the system undetected for as long as possible.

Categorize the terms above as Black, White or Grey. Could any one of them belong to more than one category?

Group Activity

Categorize the following as **Black, White or Grey Hat**. Will any of these fall into more than one group? Why or Why not?

Ethical Hackers – Hacking for good.

Hacktivist – Hacking to push an agenda or protest against certain political issues.

Nation-State Hacker – Hacking sponsored by a nation-state to gather information about an organization or nation.

What is Adversarial Thinking?

- In your groups discuss what you understand by adversarial thinking?

Adversarial Thinking Defined

- Adversarial thinking is the ability to embody the technological capabilities, the unconventional perspectives, and the strategic reasoning of hackers.
  - https://clark.center/details/shamman/Adversarial%20Thinking
- In simple terms, you need to know yourself and your enemy (attackers). You need to understand how they think and develop the same skills (or better) that they have in order to adequately keep yourself, organization and nation safe.

ATTACKS AND DEFENSE

Lesson 2 – Categorizing Attacks

Dr. Atul Rawal

Learning Outcomes

Upon completion of this lesson, students will be able to:

- Compare different types of attacks and determine the appropriate mitigation technique for each one

What is a Cyber Attack?

"An attack, via cyberspace, targeting an enterprise's use of cyberspace for the purpose of disrupting, disabling, destroying, or maliciously controlling a computing environment/infrastructure; or destroying the integrity of the data or stealing controlled information."

Source: NIST Glossary
https://csrc.nist.gov/glossary/term/Cyber-Attack

Who can be attacked?

- Individuals
- Organizations/Companies
- Nations/Countries

Attacks on Individuals

- These are some of the items that an attacker may be interested in:
  - Personal records - medical records, personal information, intellectual property, credit card information etc.
  - Devices - cellphone, laptops, tablets, etc. (Essentially anything that stores your personal data)

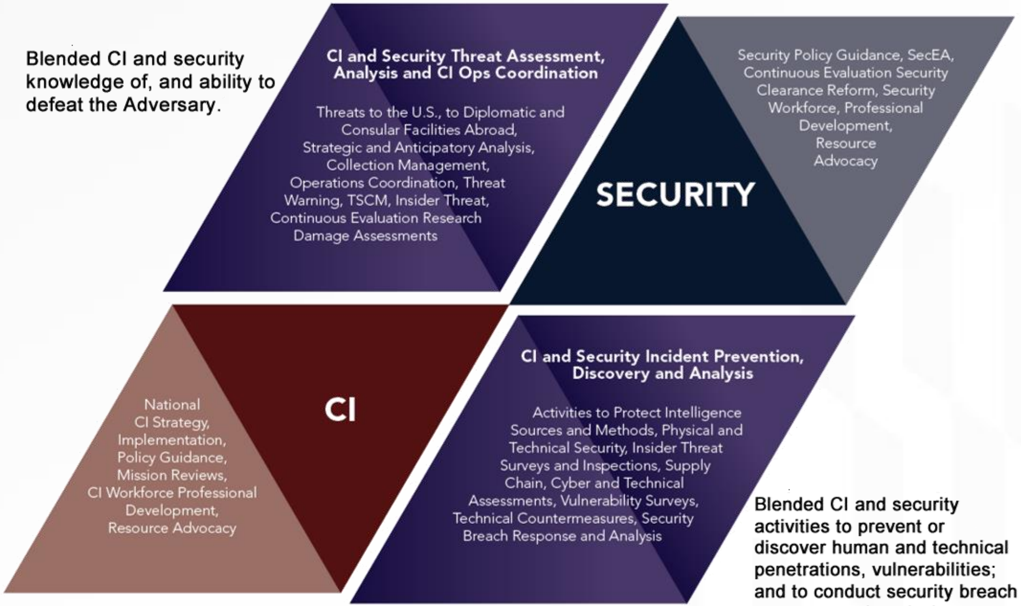
Attacks on Organizations/Companies

- Companies and Organizations are susceptible to similar attacks
  - Company Records – Intellectual property, employee records, financial information
  - Network systems - Servers, Routers etc.

Attacks on Nations/Countries

- Countries may be attacked by other countries or individuals to get
  - National secrets
  - Intelligence
  - Military information etc.

NCSC blends CI and security expertise to lead and support CI and security activities across the US Government, the Intelligence Community and US private sector entities at risk of intelligence collection, penetration or attack by foreign and other adversaries.



Blended CI and security knowledge of, and ability to defeat the Adversary.

CI and Security Threat Assessment, Analysis and CI Ops Coordination

Threats to the U.S., to Diplomatic and Consular Facilities Abroad, Strategic and Anticipatory Analysis, Collection Management, Operations Coordination, Threat Warning, TSCM, Insider Threat, Continuous Evaluation Research Damage Assessments

SECURITY

Security Policy Guidance, SecEA, Continuous Evaluation Security Clearance Reform, Security Workforce, Professional Development, Resource Advocacy

National CI Strategy, Implementation, Policy Guidance, Mission Reviews, CI Workforce Professional Development, Resource Advocacy

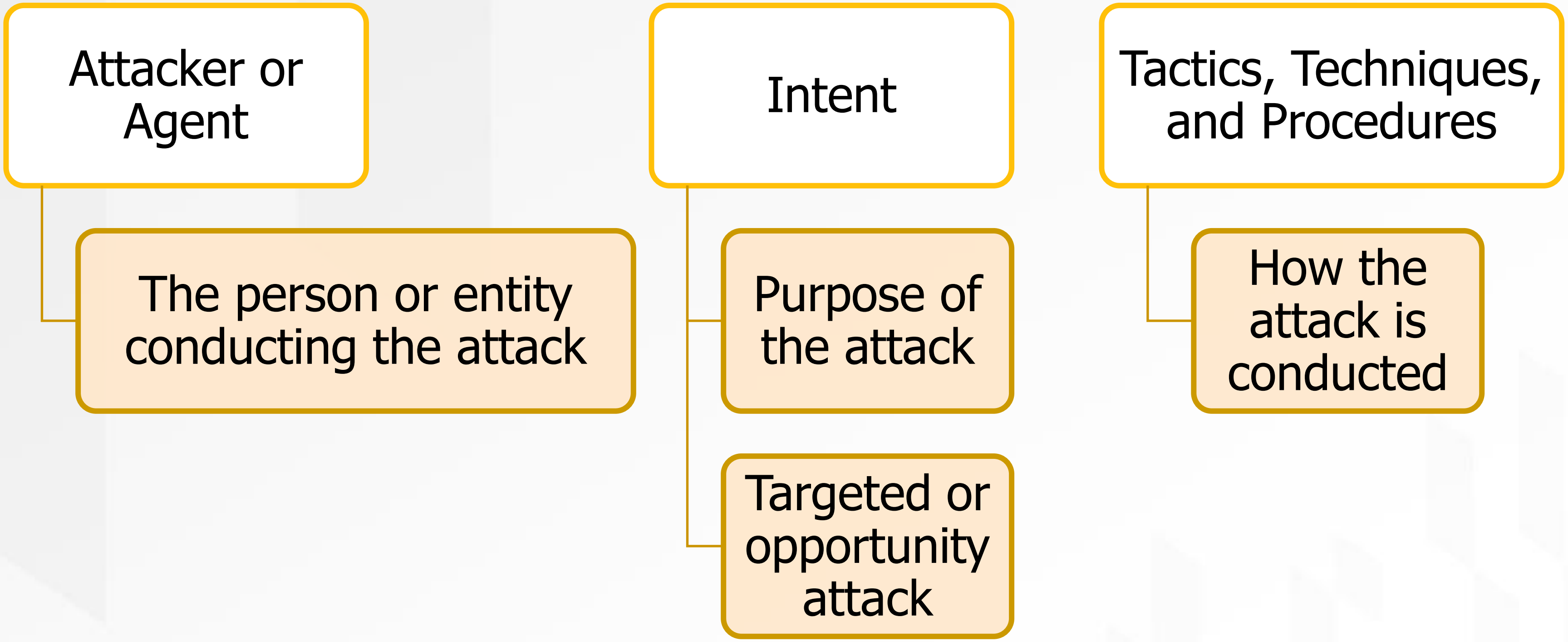
CI

CI and Security Incident Prevention, Discovery and Analysis

Activities to Protect Intelligence Sources and Methods, Physical and Technical Security, Insider Threat Surveys and Inspections, Supply Chain, Cyber and Technical Assessments, Vulnerability Surveys, Technical Countermeasures, Security Breach Response and Analysis

Blended CI and security activities to prevent or discover human and technical penetrations, vulnerabilities; and to conduct security breach response and analysis.

Components of a Cyber Attack



Attacker or Agent

The person or entity conducting the attack

Intent

Purpose of the attack

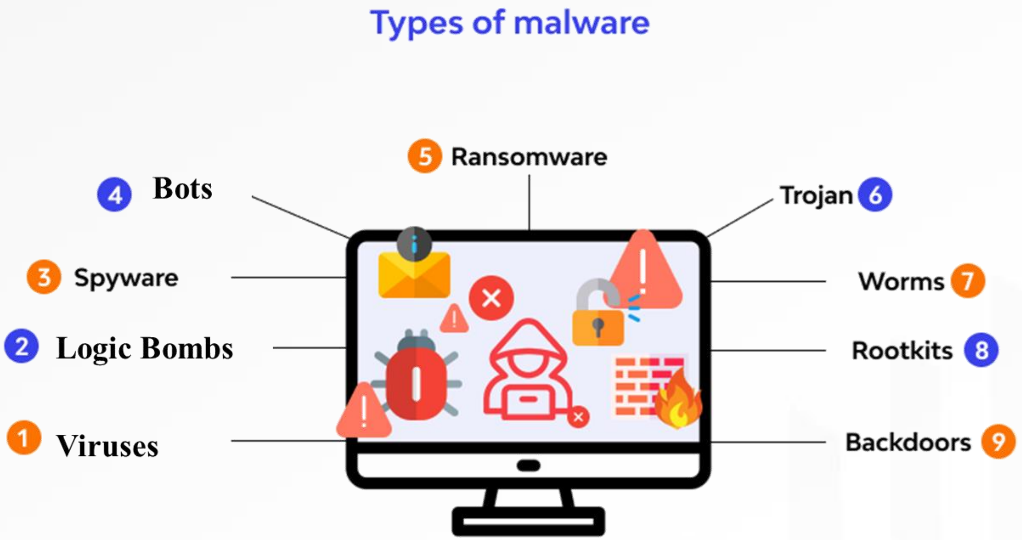
Targeted or opportunity attack

Tactics, Techniques, and Procedures

How the attack is conducted

Attack Techniques or Methods

- Several available methods.
- Five categories:
  1. Malware Attacks
  2. Network Attacks
  3. Application/Web based attacks
  4. Human Centered
  5. Wireless/Mobile Attacks
- Combo = Blended Attack.



Malware Attacks

TOWSON UNIVERSITY

- Malware stands for malicious software.
- Research the different types of Malware below, Which one do you think is the most dangerous, why?
- Describe one way to prevent yourself from them.

Viruses
Worms
Spyware
Logic Bombs
Trojan Horse
Ransomware

Botnets
Rootkit
Backdoor
Keylogger
Drive-by downloads

Malware Attacks Defined

- **Virus** – A malicious code that attaches itself to another program. It needs user intervention to run. (https://youtu.be/DF8Ka8Jh0BQ)
- **Worm** – A self-replicating program that propagates itself through a network without the need for user intervention.
- **Spyware** – A malicious code that is secretly installed on a system to gather information without the knowledge of the user, like keyloggers.
- **Logic Bomb** – A malicious code inserted into a software and is executed when certain conditions are met. (time, day or other conditions)
- **Trojan Horse** – A malicious code hidden in something that seems useful to trick you into clicking or downloading it. Remote Access Trojan (RAT) is a trojan attack used to gain remote access to a system.
- **Ransomware** – A type of malicious code that takes control of the information on a system and demands payment to release it. Some attackers will encrypt the data on the system and demand a ransom to decrypt it.

Malware Attacks Defined

- **Botnet** – A group of computers controlled from a server used to attack other systems. The computers (Bots) are added to the Botnet using a malicious code without the knowledge of the owner.
- **Rootkit** – A collection of tools used by an attacker operating on a system at the root (administrative control) level. The goal is to remain undetected while they operate.
- **Backdoor** – Malicious software used to gain access to a system remotely without the knowledge of the host system.
- **Keylogger** – Malicious software (can also be hardware) used to collect keystrokes on a target system.
- **Drive-by Downloads** – A malicious code that can be downloaded without the knowledge of the host by visiting a malicious site. It can be used to download other types of Malware to the host.

Network Attacks

The following are some common network attacks:

1. Denial of Service (DoS)
2. Distributed Denial of Service (DDoS)
3. Man in the Middle Attacks (MitM)
4. SYN Flood Attacks
5. Network Sniffing
6. Spoofing
7. Ping of Death

In your groups, research the term assigned to you. Be prepared to describe the term and how to mitigate against it.

Network Attacks Defined

- **Denial of Service (DoS)** – An attack that prevents legitimate users from accessing network resources.
- **Distributed Denial of Service (DDoS)** – A denial of service attack from multiple sources.
- **Man in the Middle (MitM)** – This occurs when an illegitimate user interrupts the communication between a server and a client in order to steal important information or redirect the traffic.
- **SYN Flood Attacks** – An attacker sends multiple SYN packets to a server and does not respond to the SYN/ACK sent by the server to complete the 3-way handshake. This attack keeps the server busy and prevents legitimate users from accessing the network.

Network Attacks Defined

- **Network Sniffing** – Sniffing is when someone is listening to traffic on a network. While it is a good tool for network administrators to use in monitoring network traffic, it's a way for attackers to learn about a network in order to attack it.
- **Spoofing** – Spoofing is when an attacker impersonates a trusted user in order to get access to a network system.
- **Ping of Death** – (AKA malicious ping) when an attacker sends a request, such as an IP packet, that is ill-formed.

Web/Application Attacks

Common Web/ Application attacks could be performed by taking advantage of vulnerabilities in an application. Some common ones are listed below.

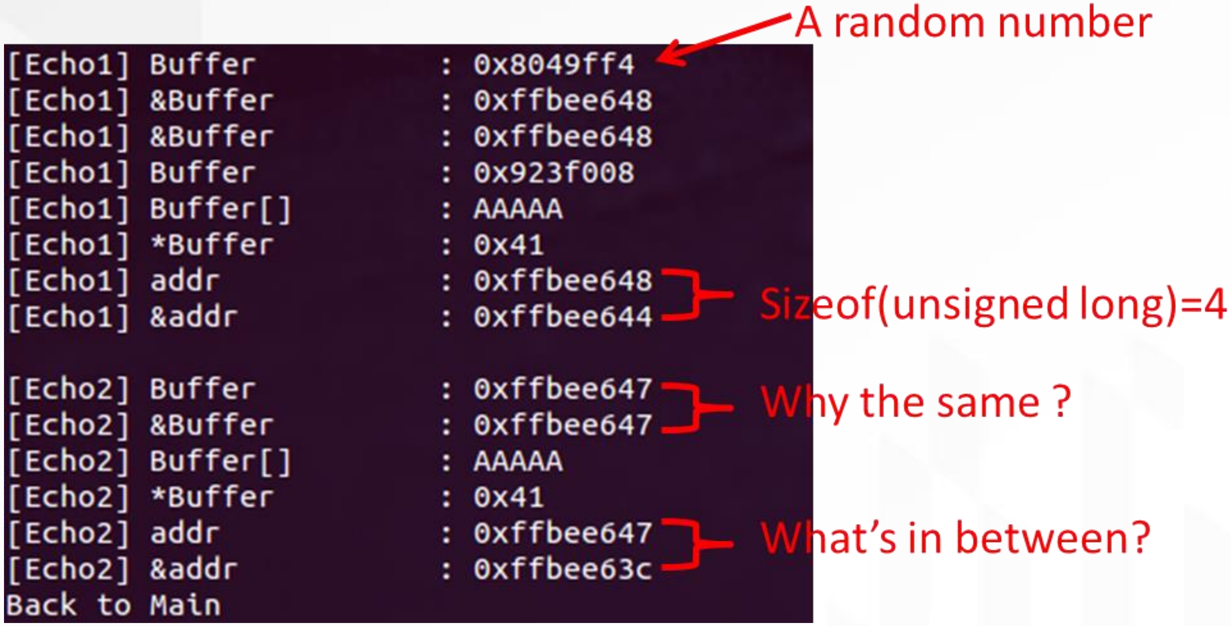
- Buffer Overflow
- Cross-site Scripting (XSS)
- SQL Injection
- XML injection
- Active X
- Java Applet and Javascript

Describe the term assigned to you. How can an attacker take advantage of this vulnerability? What can be done to mitigate against it?

Do you know of some other web/application attacks?

Buffer Overflow

Buffer Overflow – This occurs when an application receives more input than it can handle or a different input from what it is expecting. This may cause it to expose parts of the memory that the attacker may then use to attack the system or cause a system crash.



```
[Echo1] Buffer                : 0x8049ff4
[Echo1] &Buffer               : 0xffbee648
[Echo1] &Buffer               : 0xffbee648
[Echo1] Buffer                : 0x923f008
[Echo1] Buffer[]              : AAAAA
[Echo1] *Buffer               : 0x41
[Echo1] addr                  : 0xffbee648
[Echo1] &addr                 : 0xffbee644

[Echo2] Buffer                : 0xffbee647
[Echo2] &Buffer               : 0xffbee647
[Echo2] Buffer[]              : AAAAA
[Echo2] *Buffer               : 0x41
[Echo2] addr                  : 0xffbee647
[Echo2] &addr                 : 0xffbee63c
Back to Main
```

A random number

Sizeof(unsigned long)=4

Why the same ?

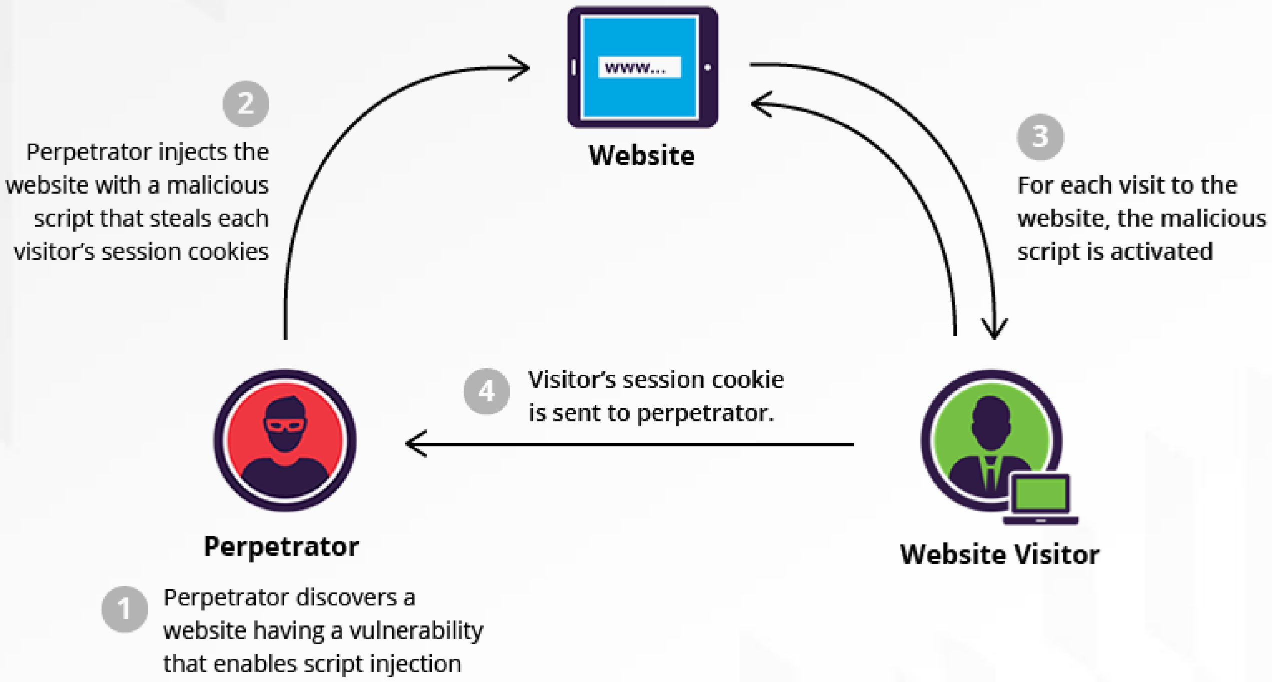
What's in between?

This Photo by Unknown Author is licensed under CC BY-SA

Cross- Site Scripting (XSS) Attacks

Cross-site Scripting (XSS) - Is a web based attack that allows an attacker to inject scripts into a webpage viewed by a user. This could contain malicious codes or access cookies with sensitive information.

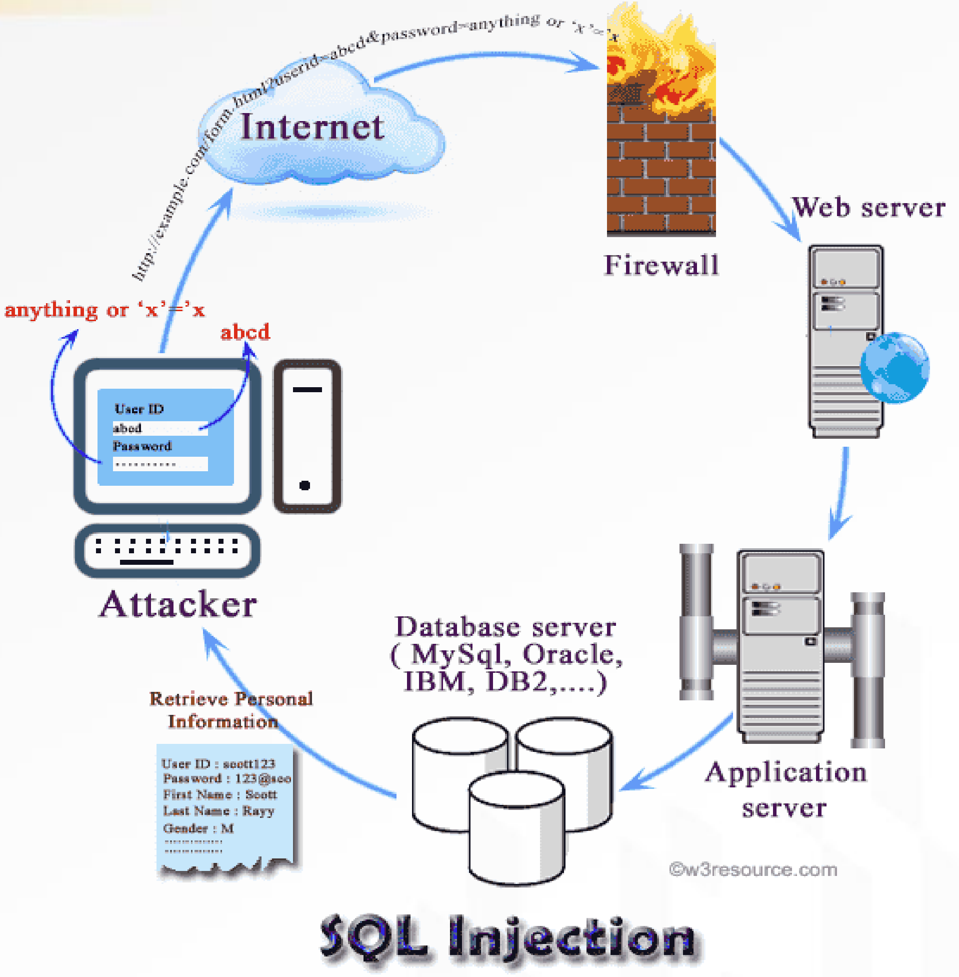
There are two types – Reflected XSS and Stored XSS.



www...
Website
2
Perpetrator injects the website with a malicious script that steals each visitor's session cookies
3
For each visit to the website, the malicious script is activated
4
Visitor's session cookie is sent to perpetrator.
Perpetrator
Website Visitor
1
Perpetrator discovers a website having a vulnerability that enables script injection

XML/SQL Injection

A type of database attack that could occur if an attacker manipulates a query entered into a database through a web page. If the input is improperly validated by the database it could result in the attacker getting access to sensitive information on the database.

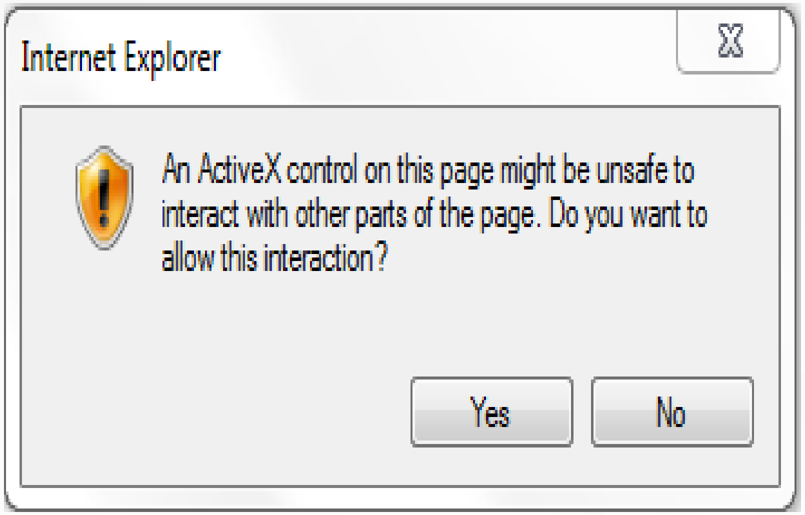


User ID : scott123
Password : 123@sco
First Name : Scott
Last Name : Rayy
Gender : M

This Photo by Unknown Author is licensed under CC BY-SA-NC

ActiveX

- **ActiveX** was developed by Microsoft to allow users play multimedia content directly from a browser.
- One main security issue with ActiveX is that it is downloaded to the user's hard drive and could potentially be accessed again by an active process.
    - The use of ActiveX can be disabled with browser security settings. ActiveX is not supported by default on many browsers.



Internet Explorer

An ActiveX control on this page might be unsafe to interact with other parts of the page. Do you want to allow this interaction?

This Photo by Unknown Author is licensed under CC BY-SA

Java Applet/Javascript Attacks

- **Java applet** is a code that runs from the browser. This applet may be used to perform malicious operations like executing malicious codes on a vulnerable system.
- **Javascript** is a programming language that allows you to create dynamic webpages. This can also allow an attacker to execute malicious code through a website. XSS attacks can be carried out using Javascript.

Port Scanning & Zero-Day Attacks

TOWSON UNIVERSITY

- **Port Scanning** - an **attack** that scans servers on a network to see which communication channels / ports are being used to exploit known vulnerabilities.
    - Most common types of scans:
        - Ping scan – block ICMP port 53.
        - Connect scan – common but easily detected.
        - SYN scan – stealthy only send SYN/ACK and don't respond.
        - FIN scan – Connection finished flagset.
- **Zero-Day Attacks** - (AKA 0-day)

  Vulnerability/flaw in software, hardware, or firware that is unknown by vendor responsible for patching; first attack.

Try some pings to see who allows you to communicate that way.

Rootkit Malware

- **Rootkit** – a collection of tools used to cover-up an intrusion that gains administrative (root level) access with utilities to:
  - Monitor traffic and keystrokes.
  - Create a back-door into the system for the hacker's use.
  - Alter log files.
  - Attack other machines on the network.
  - Alter existing system tools to circumvent detection.

Human Centered

- These types of attacks have something to do with human interaction.
  - Social Engineering
  - Email Attacks
    - Phishing
      - ❑ Spear Phishing
      - ❑ Whaling
    - Spam
  - Tailgating
  - Dumpster Diving
  - Shoulder surfing

What are some reasons why social engineering is a very successful method for perpetuating an attack? Select one category listed. Explain what the term means and how to prevent it.

Social Engineering

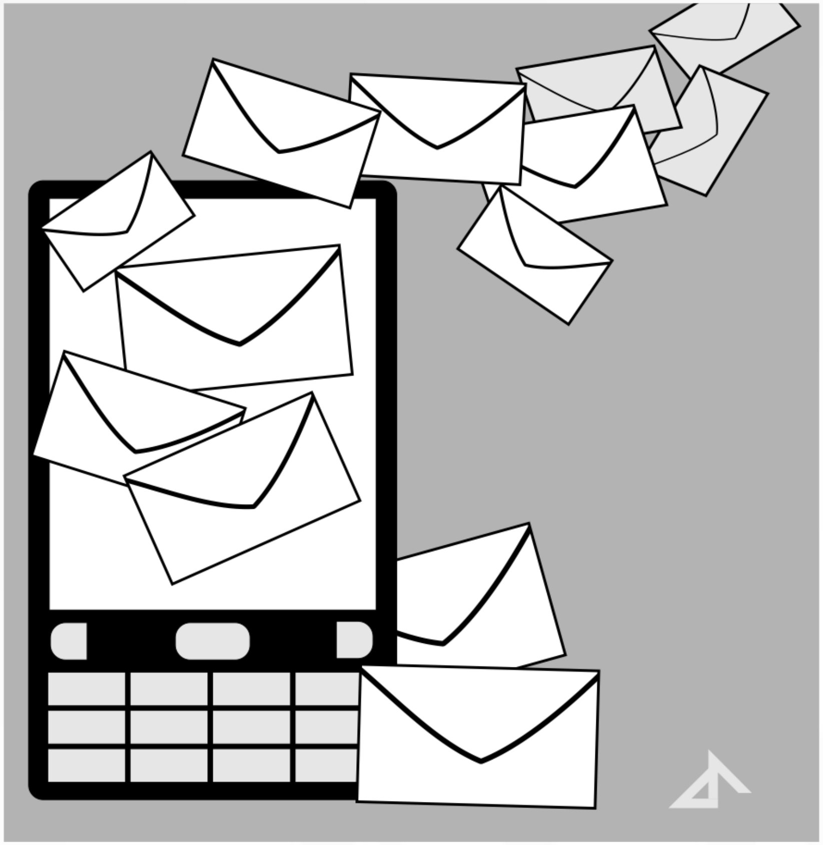
- People are the weakest link.
- **Social engineering** is the art of manipulating people so they give up confidential information.
- Examples at https://resources.infosecinstitute.com/common-social-engineering-attacks/#gref

SOCIAL ENGINEERING
The clever manipulation of the natural human tendency to trust.

This Photo by Unknown Author is licensed under CC BY-ND

Email Attacks - Spam

- Unsolicited email
- Productivity drain
- Sometimes illegitimate
- Resources bogged down
- TIME!



This Photo by Unknown Author is licensed under CC BY-NC-ND

Watering Hole attack

- Injecting malicious code into the public Web pages of a site that the targets used to visit
- Attackers compromise websites within a specific sector that are ordinary visited by specific individuals of interest for the attacks.
- Once a victim visits the page on the compromised website a **backdoor trojan** is installed on his computer.
- Watering Hole method of attacks is very common for cyber espionage operation or state-sponsored attacks.

Mobile/Wireless Attacks

- Wireless Replay Attack
- WPS attacks
- Wireless jamming
- Rogue Access points/ Evil Twin
- War Driving/ War Chalking – see https://wigle.net/
- Bluetooth attacks
  - Bluesnarfing – theft through intercepting Bluetooth connection
  - Bluejacking – sending unwanted messages over Bluetooth
- Mobile Phone Attacks
  - Vishing – phone form of phishing
  - Smishing – uses text messages to lure people with phone # or URL

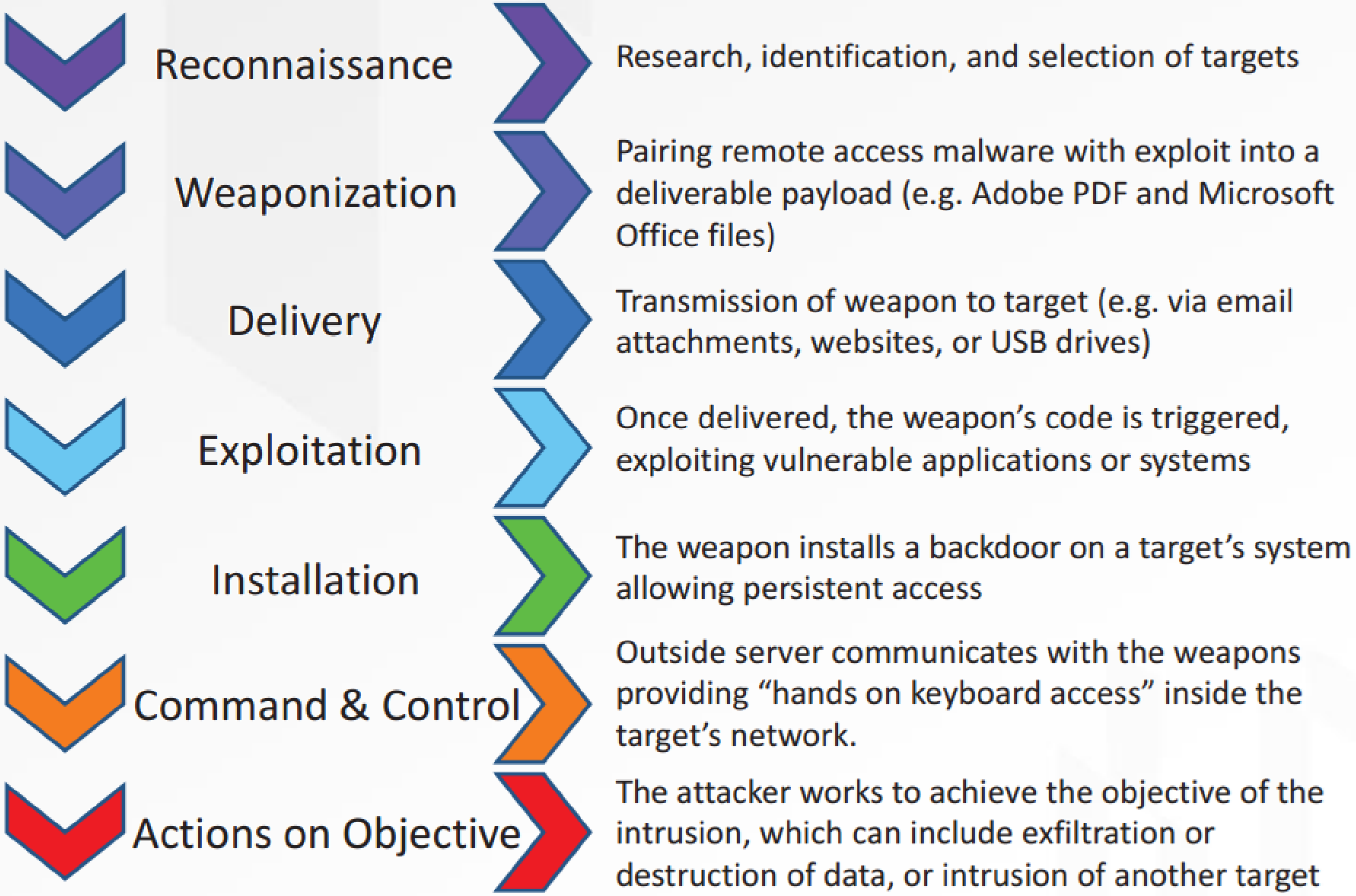
Cyber-Kill Chain

TOWSON UNIVERSITY

Cyber Kill Chain

TOWSON UNIVERSITY

Phases of the Intrusion Kill Chain



Reconnaissance	Research, identification, and selection of targets
Weaponization	Pairing remote access malware with exploit into a deliverable payload (e.g. Adobe PDF and Microsoft Office files)
Delivery	Transmission of weapon to target (e.g. via email attachments, websites, or USB drives)
Exploitation	Once delivered, the weapon's code is triggered, exploiting vulnerable applications or systems
Installation	The weapon installs a backdoor on a target's system allowing persistent access
Command & Control	Outside server communicates with the weapons providing "hands on keyboard access" inside the target's network.
Actions on Objective	The attacker works to achieve the objective of the intrusion, which can include exfiltration or destruction of data, or intrusion of another target

Created by Lockheed Martin

The Cyber Kill-Chain framework

- Originally published by Lockheed Martin as part of the Intelligence Driven Defense model.
- For the identification and prevention of cyber intrusions activity.
- Identifies what the adversaries must complete in order to achieve their objective, by targeting the network, exfiltration data and maintaining persistence in the organization.

The Cyber Kill-Chain framework

- Thanks to this model, we learned that stopping adversaries at any stage breaks the chain of attack.
- Adversaries must completely progress through all phases for success.
- We, the defenders, just need to block them at any stage for success
- The earlier the better
- A better understanding of adversaries and their trails allows for a more effective design of defenses.

Reconnaissance

- Target selection
- Identification of organization details
- Industry-vertical-legislative requirements
- Information on technology choices, social network activity or mailing lists.
- The adversary is essentially looking to answer these questions:
    - "Which attack methods will work with the highest degree of success?" And of those,
    - "which are the easiest to execute in terms of our investment of resources?"

A reconnaissance attack

- Efforts of threat actors to gain as much information about the network as possible before launching other more serious types of attacks.
- Much of the info is readily available
- What is the objective?
- “Who” will likely focus on privileged individuals (either for system access, or access to confidential data).
- “Network” will focus on architecture and layout; tools, devices and protocols; and critical infrastructure. It is like a robber understanding the behaviour of the victim and breaking into the victim’s house.

A reconnaissance attack

Types of reconnaissance attack:

- Passive reconnaissance: a hacker looks for information not related to victim domain. He just knows the registered domain to the target system so he can use commands (eg. Telephone directory) to fish information about the target
- Active reconnaissance: A hacker uses system information to gain unauthorized access to protected digital or electronic materials, and may go around routers or even firewalls to get it.

The goal of the reconnaissance phase is to identify weak points of the target.

Network Information	•IP addresses •subnet mask •network topology •domain names
Host Information	•user names •group names •architecture type (e.g. x86 vs SPARC) •operating system family and version •TCP and UDP services running with versions
Security Policies	•password complexity requirements •password change frequency •expired/disabled account retention •physical security (e.g. locks, ID badges, etc.) •firewalls •intrusion detection systems
Human Information	•home address •home telephone number •frequent hangouts •computer knowledge •dark secrets

RECONNAISSANCE Identify the Targets

ADVERSARY

- The adversaries are in the planning phase of their operation. They conduct research to understand which targets will enable them to meet their objectives.
  - Harvest email addresses
  - Identify employees on social media networks
  - Collect press releases, contract awards, conference attendee lists
  - Discover internet-facing servers

DEFENDER

- Detecting reconnaissance as it happens can be very difficult, but when defenders discover recon – even well after the fact – it can reveal the intent of the adversaries.
  - Collect website visitor logs for alerting and historical searching.
  - Collaborate with web administrators to utilize their existing browser analytics.
  - Build detections for browsing behaviors unique to reconnaissance.
  - Prioritize defenses around particular technologies or people based on recon activity.

Weaponization

- During weaponization, the threat actor develops malware specifically crafted to the vulnerabilities discovered during the reconnaissance phase of the cyber kill chain.
- Based on the intelligence gathered in the reconnaissance phase, the attacker will tailor their toolset to meet the specific requirements of the target network.

Delivery

- The third stage in the cyber kill chain, delivery, involves transmitting the APT code from the attacker to the target information system for exploitation. Based on current research and analysis from the 2018 Verizon Data Breach Investigation Report, a network attack is most likely to originate from a spear-phishing attack targeting an internal employee of the organization.
- A carefully researched and crafted spear-phishing campaign against an organization based on information gathered during the reconnaissance phase would result in the organization's employees executing the APT malware code on their information systems. The spear phishing message will most likely contain an attachment such as a Microsoft Word or an Adobe PDF document. The attachment would contain code that, when executed, would result in the APT gaining a foothold on the organizational network.

Exploitation

- During the exploitation phase, the APT malware code is executed on the target network through remote or local mechanisms, taking advantage of discovered vulnerabilities to gain superuser access to the targeted organizational information system.

Installation

- Once the exploitation of the system has been successful, the APT malware code will install itself onto the targeted information system. At this point, the APT malware will begin to download additional software if network access is available. This allows the delivery payload to remain small and undetectable.
- The small size of the malware in this example would have limited functionality. Therefore, the APT will download additional components to have better control of the exploited information systems and to penetrate further into the target organization's network.

Command and Control

Command and control is the sixth phase of the cyber kill chain. Command and control, also known as C2, is when the attacker has put in place their management and communication APT code onto to the target network. This software allows the attacker to fully manage the APT code in the environment and allows the attacker to move deeper into the network, exfiltrate data and conduct destruction or denial of service operations.

Actions on Objective

- The actions and objectives of the APT are dependent on its specific mission. The APT could be focused on data exfiltration, denial of service or destruction.
- In the case of data exfiltration, the APT may be interested in organizational proprietary data such as engineering designs or employee and customer Personally Identifiable Information (PII). In the case of a denial of service, like the Ukrainian power outage of December 2015, the APT may disable a key component of the organization's infrastructure to temporarily disrupt services.
- Finally, in the case of destruction, an APT like the Stuxnet worm may seek to operate industrial control systems outside of their manufacturer specifications, resulting in catastrophic failure.