

Cybersecurity Fundamentals

Lecture 3: Hackers and Cyber Crime

CYB 670

Cybersecurity Fundamentals

Presented by

Dr. Mohammad Alkhatib



Outline

The module covers the basics of cybersecurity including:

- Difference Between Information security and Cybersecurity.
- Protecting Digital Assets.
- Risk management terms, concepts and frameworks.
- The Types of Hackers, and Crackers.
- Attack Attributes.
- Generalized Attack Process.

Difference Between Information security and cybersecurity

- The terms “**cybersecurity**” and “information security” are often used interchangeably. Some use the term cybersecurity as a synonym for information security, IT security and information risk management.
- Others, particularly in government circles, have adopted more technical definitions related to national defense, including **cyberwarfare** and protection of critical infrastructure.
- Although different groups tend to adapt terminology for their own purposes, there are some important distinctions between **cybersecurity** and **information security**.
- **Information security** deals with information, regardless of its format—it encompasses paper documents, digital and intellectual property in people’s minds, and verbal or visual communications.

Difference Between Information security and cybersecurity

- **Cybersecurity**, on the other hand, is concerned with protecting digital assets—everything from networks to hardware and information that is processed, stored or transported by internetworked information systems.
- **Therefore, to eliminate confusion:**
 - The term **cybersecurity** will be defined in this guide as protecting information assets by addressing threats to information processed, stored and transported by internetworked information systems.

Difference Between Information security and cybersecurity

Cyber security is about keeping computer systems and networks safe from bad people who try to break in or cause harm online. It deals with things like stopping hackers, fixing computer problems, and making sure websites work properly. **Information security**, on the other hand, is about keeping all kinds of information safe, whether it's on computers or not. This includes protecting paper files, keeping secrets, and making sure only the right people can see or use important information. **While cyber security focuses on the internet and computers, information security covers a wider range of ways to keep information safe in all forms.**

Protecting Digital Assets

- In **cybersecurity** frameworks, both the National Institute of Standards and Technology (NIST) and the European Union Agency for Network and Information Security (ENISA) have identified five key functions necessary for the protection of digital assets.
- These functions coincide with incident management methodologies and include the following activities:
- **Identify**: Use organizational understanding to minimize risk to systems, assets, data and capabilities.
- **protect**: Design safeguards to limit the impact of potential events on critical services and infrastructure.
- **Detect**: Implement activities to identify the occurrence of a cybersecurity event.
- **Respond**: Take appropriate action after learning of a security event.
- **Recover**: Plan for resilience and the timely repair of compromised capabilities and services.

➤ Risk

- The core duty of **cybersecurity** is to identify, mitigate and manage **cyberrisk** to an organization's digital assets.:
- **Assessing risk** is one of the most critical functions of a cybersecurity organization.
- Effective policies, security implementations, resource allocation and incident response preparedness are all dependent on → understanding the risk and threats an organization faces.
- Using a **risk-based approach** to cybersecurity allows more informed decision-making to protect the organization and to apply limited budgets and resources effectively.

➤ Approaches to cybersecurity

Generally, there are three different approaches to implementing cybersecurity:

- 1) **Compliance-based**—Also known as standards-based security, this approach relies on regulations or standards to determine security implementations. **Controls** are implemented regardless of their applicability or necessity, which often leads to a “checklist” attitude toward security.
- 1) **Risk-based**—Risk-based security relies on identifying the unique risk a particular organization faces and designing and implementing security controls to address that risk above and beyond the entity’s risk tolerance and business needs.

➤ Approaches to cybersecurity

Generally, there are three different approaches to implementing cybersecurity:

- 3) Ad hoc**—An ad hoc approach simply implements security with no particular rationale or criteria. Ad hoc implementations may be driven by vendor marketing, or they may reflect insufficient subject matter expertise, knowledge or training when designing and implementing safeguards.

➤ key terms and definitions

There are many potential definitions of risk—some general and others more technical. Additionally, it is important to distinguish between a risk and a threat. Although many people use the words threat and risk synonymously, they have two very different meanings:

- ❖ **Risk**—The combination of the probability of an event and its consequence (International Organization for Standardization/International Electrotechnical Commission [ISO/IEC] 73).
- ❖ Risk is mitigated through the use of controls or safeguards.

➤ key terms and definitions

- ❖ **Threat**—Anything (e.g., object, substance, human) that is capable of acting against an asset in a manner that can result in harm.
 - ISO/IEC 13335 defines a threat broadly as a potential cause of an unwanted incident.
 - Some organizations make a further distinction between a threat source and a threat event, classifying a threat source as the actual process or agent attempting to cause harm, and a threat event as the result or outcome of a threat agent's malicious activity.
- ❖ **Asset**—Something of either tangible or intangible value that is worth protecting, including people, information, infrastructure, finances and reputation.

➤ key terms and definitions

- ❖ **Vulnerability**—A weakness in the design, implementation, operation or internal control of a process that could expose the system to adverse threats from threat events
 - Although much of cybersecurity is focused on the design, implementation and management of controls to mitigate risk, it is critical for security practitioners to understand that risk can never be completely eliminated.

➤ key terms and definitions

- ❖ **Residual risk**—Even after safeguards are in place, there will always be residual risk, defined as the remaining risk after management has implemented a risk response.
- ❖ **Inherent risk**—The risk level or exposure without taking into account the actions that management has taken or might take (e.g., implementing controls)

➤ Approaches to Risk

There are a number of methodologies available to measure risk.

Different industries and professions have adopted various tactics based upon the following criteria:

- ❖ Risk tolerance
- ❖ Size and scope of the environment in question
- ❖ Amount of data available

➤ Third-party Risk

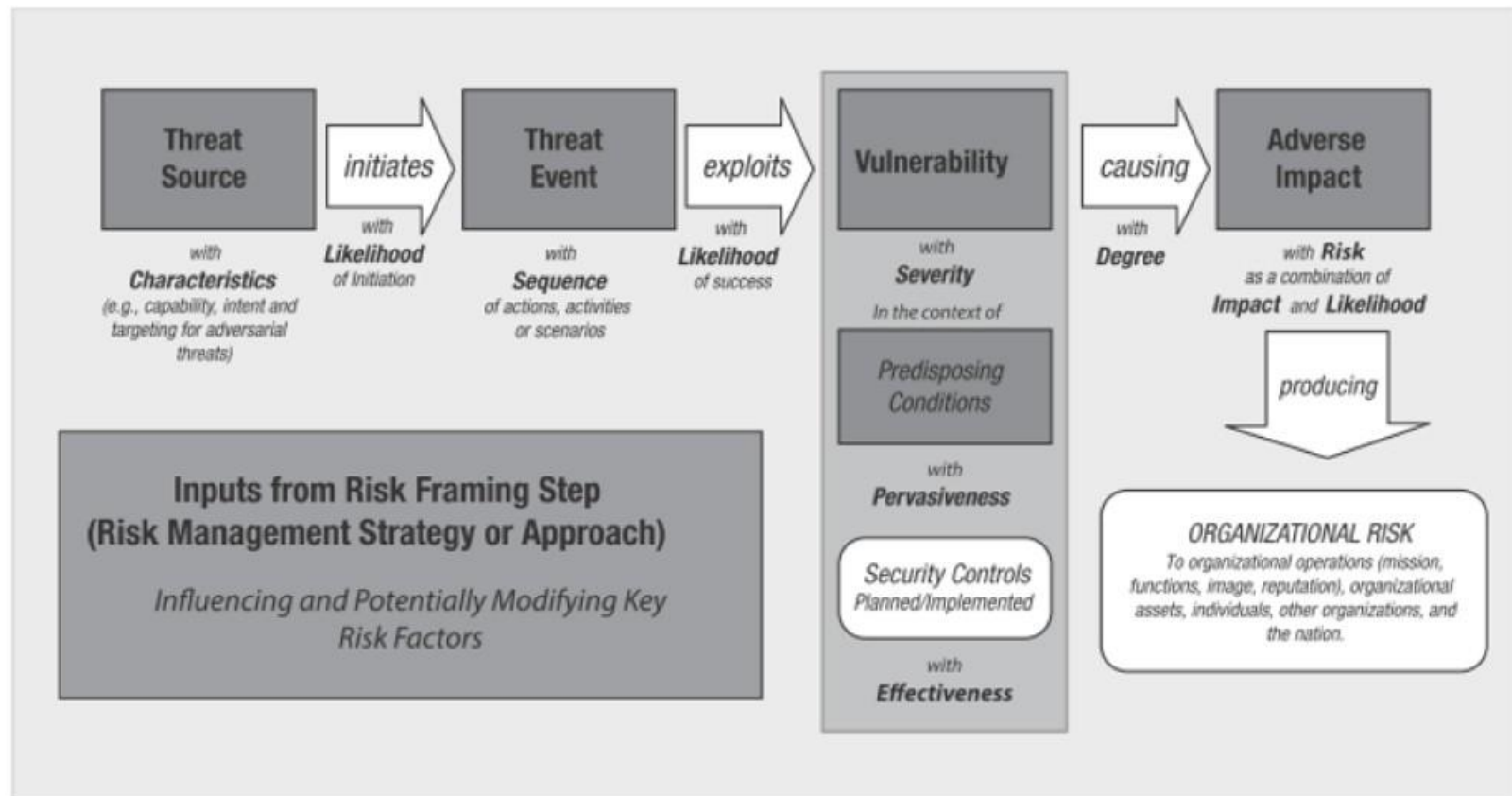
- ✓ *Cybersecurity can be more difficult to control when third parties are involved, especially when different entities have different security cultures and risk tolerances.*
- ✓ *No organization exists in a vacuum, and information must be shared with other individuals or organizations, often referred to as third parties.*
- ✓ *It is important to understand third-party risk, such as information sharing and network access, as it relates to cybersecurity.*

Risk management terms, concepts and frameworks

➤ Risk management

- ✓ Exhibit 2.1 illustrates how many of these key terms come into play when framing an approach to risk management.

Exhibit 2.1: Framing Risk Management



The Hackers, and Crackers – Definition



Hacking:

Hacking may be defined as the technique or planning which is done to get an access to unauthorized systems. Simply we can say to gaining access to a network or a computer for illegal purposes. The person who does that are very intelligent and skilled in computers.

The person who are skilled in Hacking are divided into 2 categories:

1. Hackers

- Hackers are kind of good peoples who does hacking for the good purpose and to obtain more knowledge from it.
- They generally find loop holes in the system and help them to cover the loop holes.
- Hackers are generally programmers who obtain advance knowledge about operating systems and programming languages.
- These people never damage or harm any kind of data.

The Hackers, and Crackers – Definition



Hacking:

Hacking may be defined as the technique or planning which is done to get an access to unauthorized systems. Simply we can say to gaining access to a network or a computer for illegal purposes. The person who does that are very intelligent and skilled in computers.

The person who are skilled in Hacking are divided into 2 categories:

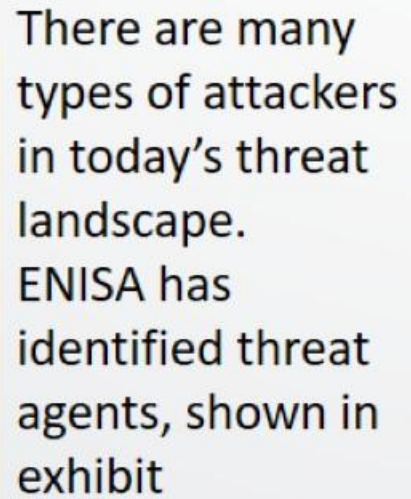
2. Crackers

- Crackers are kind of bad people who breaks or violates the system or a computer remotely with bad intentions to harm the data and steal it.
- Crackers destroy data by gaining an unauthorized access to the network.
- Their works are always hidden as they are doing illegal stuff.
- Bypasses passwords of computers and social media websites, can steal your bank details and transfer money from bank.

Difference between Hackers and Crackers :



Hacker	Cracker
The good people who hack for knowledge purposes.	The evil person who breaks into a system for benefits.
They are skilled and have a advance knowledge of computers OS and programming languages.	They may or may not be skilled, some of crackers just knows a few tricks to steal data.
They work in an organization to help protecting there data and giving them expertise on internet security.	These are the person from which hackers protect organizations .
Hackers share the knowledge and never damages the data.	If they found any loop hole they just delete the data or damages the data.
Hackers are the ethical professionals.	Crackers are unethical and want to benefit themselves from illegal tasks.
Hackers program or hacks to check the integrity and vulnerability strength of a network.	Crackers do not make new tools but use someone else tools for there cause and harm the network.
Hackers have legal certificates with them e.g CEH certificates.	Crackers may or may not have certificates, as there motive is to stay anonymous.



Cyber Agent

- Friendly**
 - Researcher (Research Community)
 - Ethical Hacker (Market)
 - Security Agent (National Security)
 - Law Enforcement Agent (Law Enforcement)
 - Cyber-Soldier (Military)
- Hostile (Threat Agent)**
 - Low Capability**
 - Low Tech/Low-Medium Expertise**
 - Young, Unskilled: Script Kiddies
 - Soft Skilled: Online Social Hacker
 - Internal, Low-Medium Skilled: Employee
 - High Capability**
 - High Tech/High Expertise**
 - Infrastructure Delivery
 - Provider/Developer/Operator
 - Infrastructure Use
 - Tools User/Deployer
 - Paid Nonchalant: Espionage
 - National Mission: State
 - Corp. Mission: Corporation
 - Socially Motivated Citizens: Hacktivist
 - Ideologically Motivated: Cyber Terrorist
 - Profit Oriented: Cyber Criminal
 - Nationally Motivated Citizations: Cyber Fighter

Legend:

- Group/Category
- Individual Agent
- Sector, Capability, Motive
- Examples of Concurrent Roles

The Types of Hackers, and Crackers

❖ Threat Agents:

➤ **Corporations:-**

- Corporations have been known to breach security boundaries and perform malicious acts to gain a competitive advantage.

➤ **Nation States:-**

- Nation states often target government and private entities with a high level of sophistication to obtain intelligence or carry out other destructive activities.

The Types of Hackers, and Crackers

❖ Threat Agents:

➤ **Hacktivists:-**

- Although they often act independently, politically motivated hackers may target specific individuals or organizations to achieve various ideological ends.

➤ **Cyberterrorists:-**

- Characterized by their willingness to use violence to achieve their goals, cyberterrorists frequently target critical infrastructures and government groups.

The Types of Hackers, and Crackers

❖ Threat Agents:

➤ **Cybercriminals:-**

- Motivated by the desire for profit, these individuals are involved in fraudulent financial transactions.

➤ **Cyberwarriors:-**

- Often likened to hacktivists, cyberwarriors, also referred to as cyberfighters, are nationally motivated citizens who may act on behalf of a political party or against another political party that threatens them.

The Types of Hackers, and Crackers



❖ Threat Agents:

➤ **Script kiddies:-**

- Script kiddies are young individuals who are learning to hack; they may work alone or with others and are primarily involved in code injections and distributed denial-of-service (DDoS) attacks.

➤ **Online Social hackers:-**

- Skilled in social engineering, these attackers are frequently involved in cyberbullying, identity theft and collection of other confidential information or credentials.

The Types of Hackers, and Crackers

❖ *Hackers can be classified into different categories such as **white hat, black hat, and grey hat**, based on their intent of hacking a system.*



1) White Hat Hackers

- White Hat hackers are also known as **Ethical Hackers**.
- They never intent to harm a system, rather they try to find out weaknesses in a computer or a network system as a part of penetration testing and vulnerability assessments.
- Ethical hacking is not illegal and it is one of the demanding jobs available in the IT industry.
- There are numerous companies that hire ethical hackers for penetration testing and vulnerability assessments.

The Types of Hackers, and Crackers

❖ *Hackers can be classified into different categories such as white hat, black hat, and grey hat, based on their intent of hacking a system.*



2) Black Hat Hackers

- Black Hat hackers, also known as **crackers**, are those who hack in order to gain unauthorized access to a system and harm its operations or steal sensitive information.
- Black Hat hacking is always illegal because of its bad intent which includes:
 - stealing corporate data,
 - violating privacy,
 - damaging the system,
 - blocking network communication, etc.

The Types of Hackers, and Crackers

❖ *Hackers can be classified into different categories such as white hat, black hat, and grey hat, based on their intent of hacking a system.*



3) Grey Hat Hackers

- Grey hat hackers are a blend of both black hat and white hat hackers.
- They act without malicious intent but for their fun,
- They exploit a security weakness in a computer system or network without the owner's permission or knowledge.
- Their intent is to bring the weakness to the attention of the owners and getting appreciation or a little bounty from the owners.

The Types of Hackers, and Crackers

❖ *Hackers can be classified into different categories such as white hat, black hat, and grey hat, based on their intent of hacking a system.*



4) Red Hat Hackers

- Red hat hackers are again a blend of both black hat and white hat hackers.
- They are usually on the level of hacking government agencies, top-secret information hubs, and generally anything that falls under the category of sensitive information.



5) Blue Hat Hackers

- A blue hat hacker is someone outside computer security consulting firms who is used to bug-test a system prior to its launch.
- They look for loopholes that can be exploited and try to close these gaps.
- Microsoft also uses the term **BlueHat** to represent a series of security briefing events.

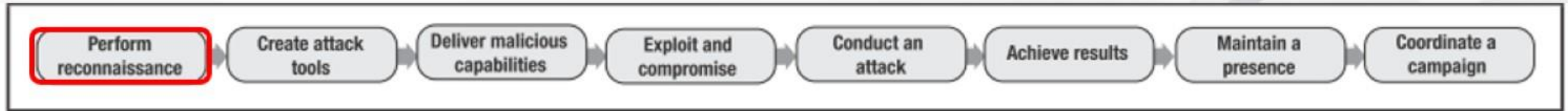
Attack Attributes

- The attacker must defeat any controls in place and/or use an exploit to take advantage of a vulnerability.
- Another attribute of an attack is the attack mechanism, or the method used to deliver the exploit.
- Unless the attacker is personally performing the attack, the attack mechanism may involve a payload, or container, that delivers the exploit to the target.



Generalized Attack Process

❖ While each attack is different, most adversarial threat events follow a common process.

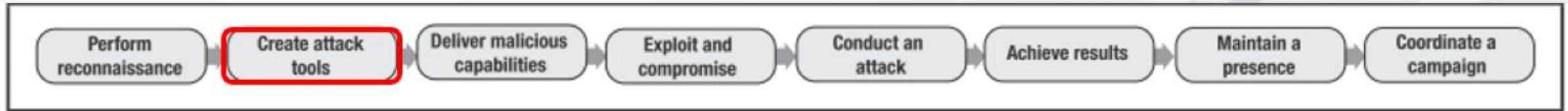


1. perform reconnaissance: The adversary gathers information using a variety of techniques, which may include:

- Sniffing or scanning the network perimeter
- Using open source discovery of organizational information
- Running malware to identify potential targets

Generalized Attack Process

❖ While each attack is different, most adversarial threat events follow a common process.

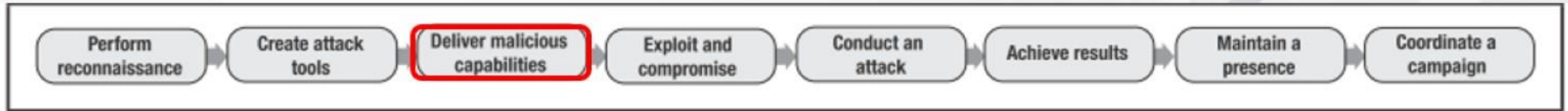


2. Create attack tools: The adversary crafts the tools needed to carry out a future attack, which may include:

- Phishing or spear phishing attacks
- Crafting counterfeit web sites or certificates
- Creating and operating false front organizations to inject malicious components into the supply chain

Generalized Attack Process

❖ While each attack is different, most adversarial threat events follow a common process.

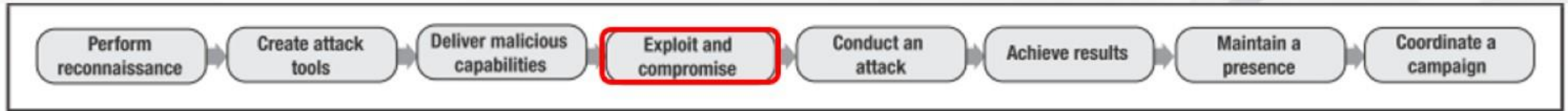


3. Deliver malicious capabilities: The adversary inserts or installs whatever is needed to carry out the attack, which may include the following tactics:

- Introducing malware into organizational information systems
- Placing subverted individuals into privileged positions within the organization
- Installing sniffers or scanning devices on targeted networks and systems
- Inserting tampered hardware or critical components into organizational systems or supply chains

Generalized Attack Process

❖ While each attack is different, most adversarial threat events follow a common process.

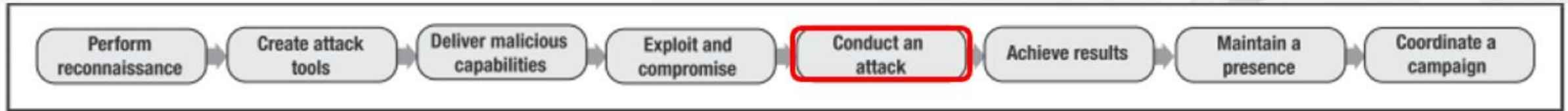


4. Exploit and compromise: The adversary takes advantage of information and systems in order to compromise them, which may involve the following actions:

- Split tunneling or gaining physical access to organizational facilities
- Exfiltrating data or sensitive information
- Exploiting multitenancy in a cloud environment
- Launching zero-day exploits

Generalized Attack Process

❖ While each attack is different, most adversarial threat events follow a common process.

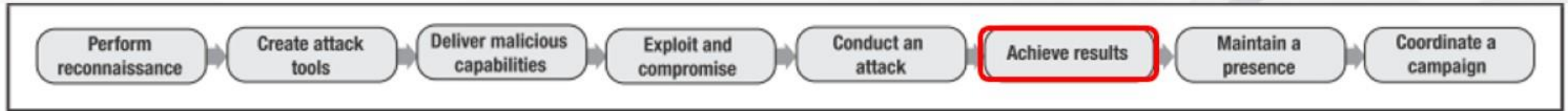


5. Conduct an attack: The adversary coordinates attack tools or performs activities that interfere with organizational functions. Potential methods of attack include:

- Communication interception or wireless jamming attacks
- Denial-of-service (DoS) or distributed denial-of-service (DDoS) attacks
- Remote interference with or physical attacks on organizational facilities or infrastructures
- Session-hijacking or man-in-the-middle attacks

Generalized Attack Process

❖ While each attack is different, most adversarial threat events follow a common process.

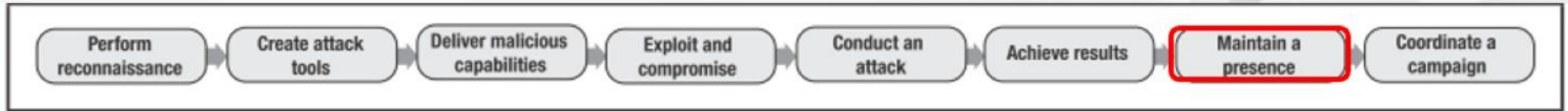


6. Achieve results: The adversary causes an adverse impact, which may include:

- Obtaining unauthorized access to systems and/or sensitive information
- Degrading organizational services or capabilities
- Creating, corrupting or deleting critical data

Generalized Attack Process

❖ While each attack is different, most adversarial threat events follow a common process.

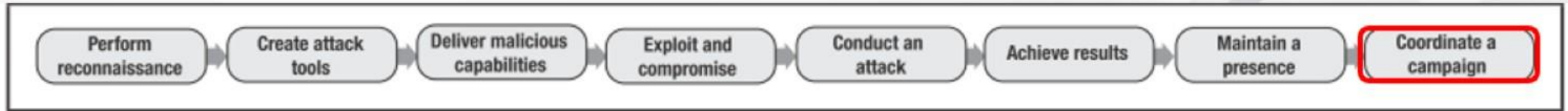


7. Maintain a presence or set of capabilities: The adversary continues to exploit and compromise the system using the following techniques:

- Obfuscating adversary actions or interfering with intrusion detection systems (IDSs)
- Adapting cyberattacks in response to organizational security measures

Generalized Attack Process

❖ While each attack is different, most adversarial threat events follow a common process.



8. Coordinate a campaign: The adversary coordinates a campaign against the organization that may involve the following measures:

- Multi-staged attacks
- Internal and external attacks
- Widespread and adaptive attacks

Generalized Attack Process

Nonadversarial Threat Events

Although most attacks are the result of a coordinated effort, there are other events that can pose various risk to an organization. Some of the most common

nonadversarial threat events are:

- Mishandling of critical or sensitive information by authorized users
- Incorrect privilege settings
- Fire, flood, hurricane, windstorm or earthquake at primary or backup facilities
- Introduction of vulnerabilities into software products
- Pervasive disk errors or other problems caused by aging equipment

Malwares and attack Types

❖ **Malware**, also called malicious code, is software designed to:

- gain access to targeted computer systems,
- steal information or
- disrupt computer operations.



Next
Lecture

❖ **Malware and malicious files inside a computer system can:**

- Deny access to the critical components of the network
- Obtain information by retrieving data from the hard drive
- Disrupt the system or even render it inoperable

Self Assignment

Case Study:

- Stuxnet attack components
- Internet of Things (IoT) Attacks

The END 😊



Thank You