Introduction

Sara Khanchi
INCS 745 – NYIT

Outline

- Security Definitions and Terms
- Framework
- Types of Threat Agents
- Types of Attacks

Security

- Security
  - Protection of a person, building, organization, or country against threats such as crime or attacks by foreign countries. The fact that something is not likely to fail or be lost. - *Cambridge English Dictionary*

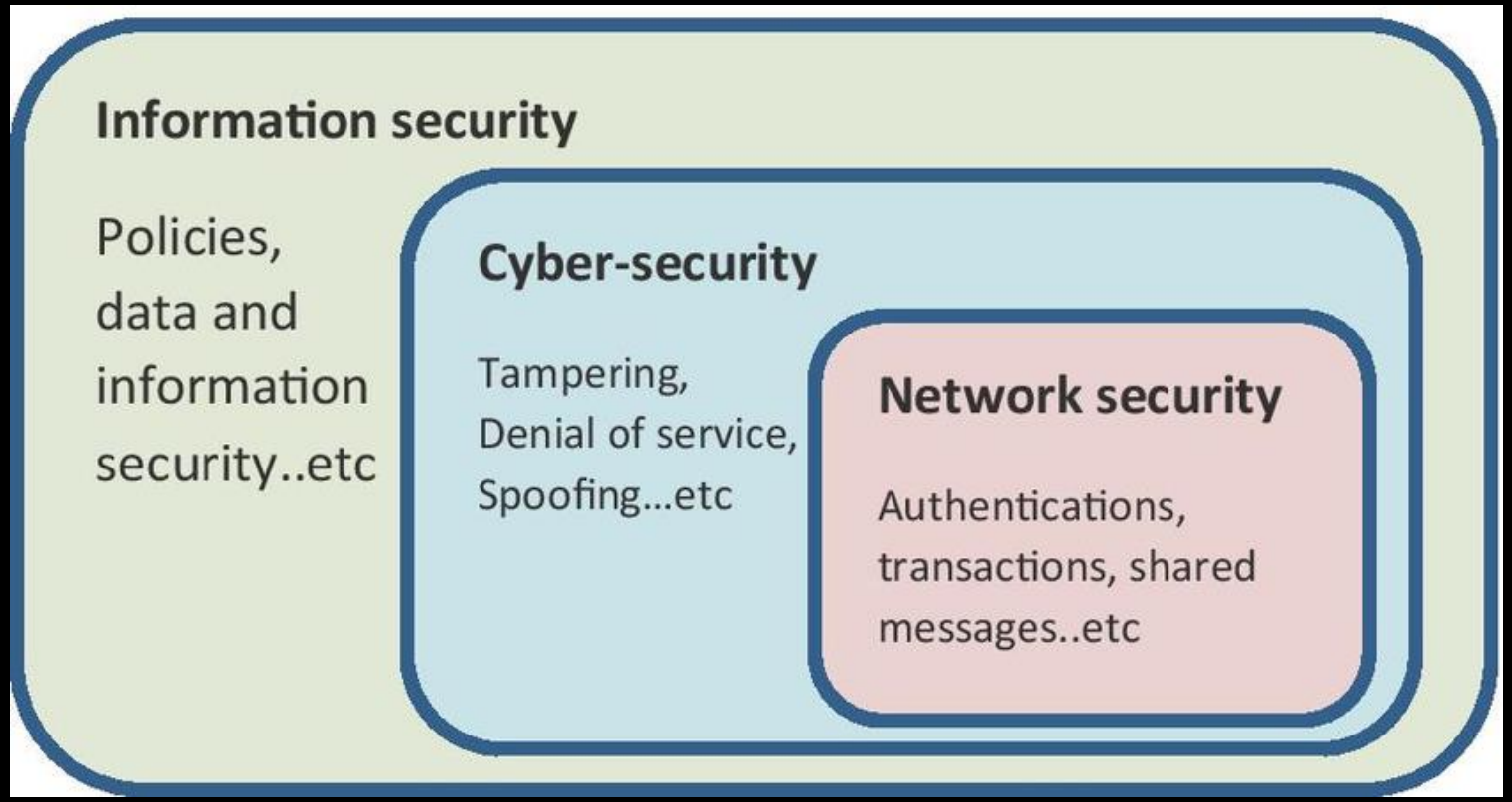
- Computer Security
  - The protection afforded to an automated information system in order to attain the applicable objectives of preserving the integrity, availability and confidentiality of information system resources (includes hardware, software, firmware, information/data, and telecommunications) - NIST 1995

Cybersecurity[1]

- "cybersecurity" vs "information security"
  - Used interchangeably
  - cybersecurity is a part of information security

- Protection of information assets by addressing threats to information processed, stored and transported by internetworked information systems.

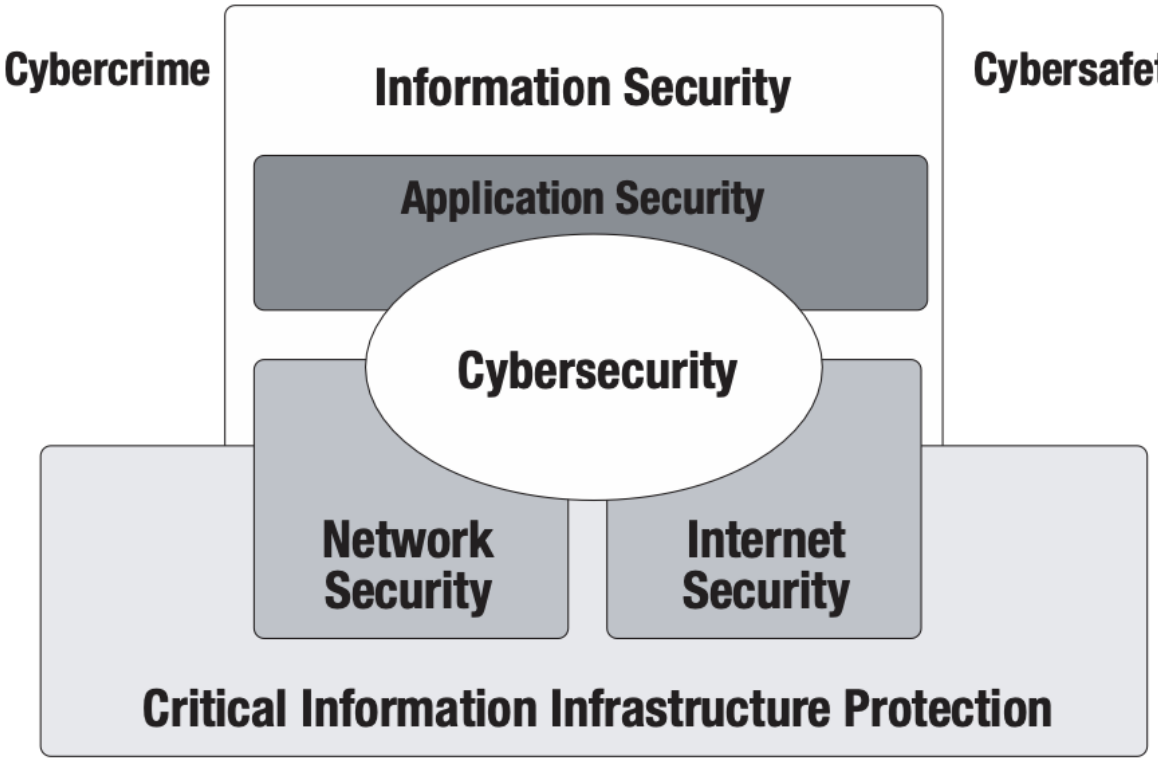
Cybersecurity



Solms, B.V. and Solms, R.V. (2018) Cybersecurity and Information Security—What Goes Where? Information and Computer Security, 26, 2-9.

Cybersecurity [1]

Figure 1.2—Relationship Among Cybersecurity and Other Security Domains

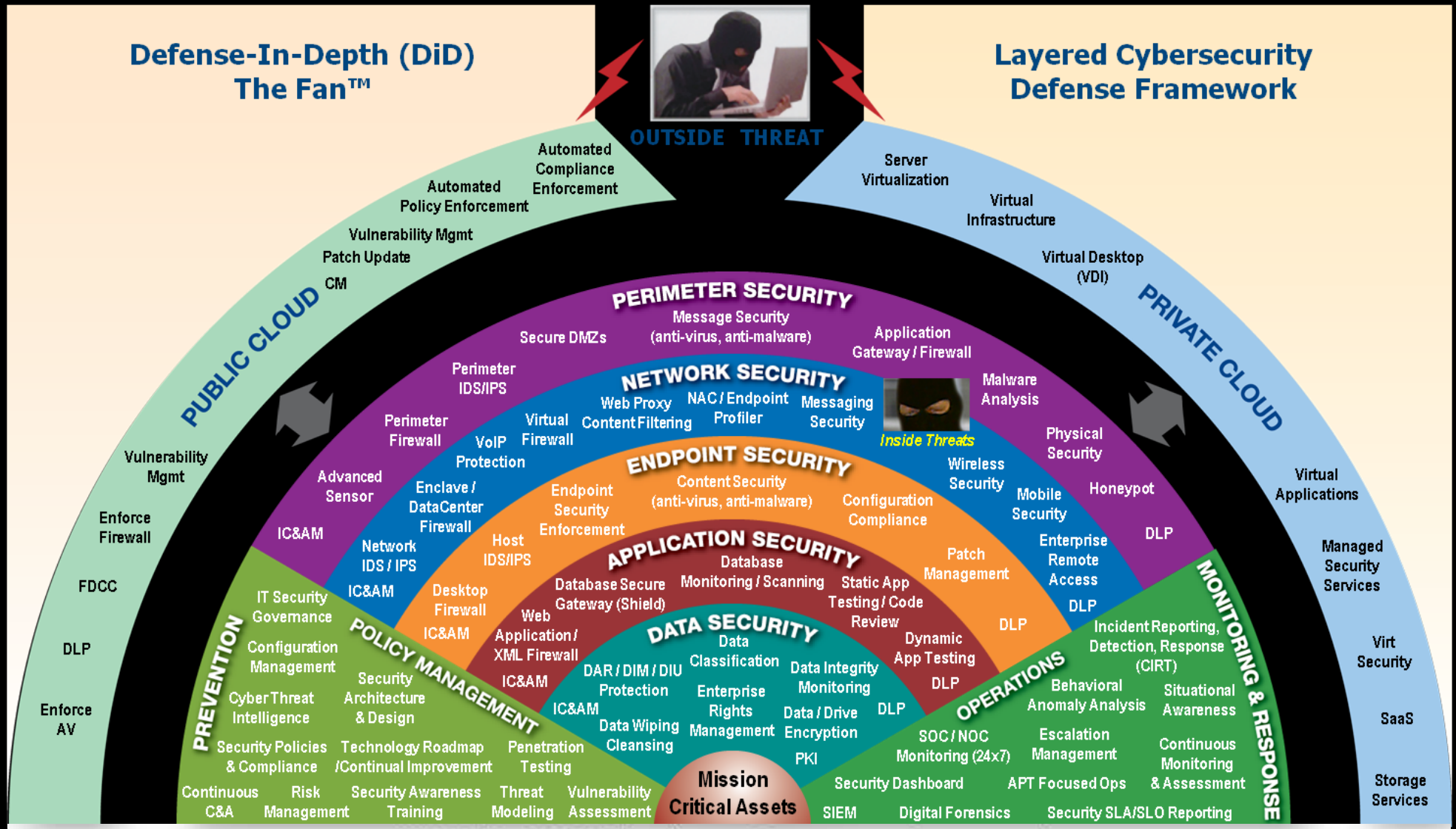


Source: International Organization for Standardization, *ISO/IEC 27032:2012: Information technology—Security techniques—Guidelines for cybersecurity*, Switzerland, 2012

Cybersecurity Terms [1]

- **Risk**
  - The combination of the probability of an event and its consequence (ISO/IEC 73).
- **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.
- **Asset**
  - Something of either tangible or intangible value that is worth protecting, including people, information, infrastructure, finances and reputation
- **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.

Cybersecurity Layers



Cybersecurity Market

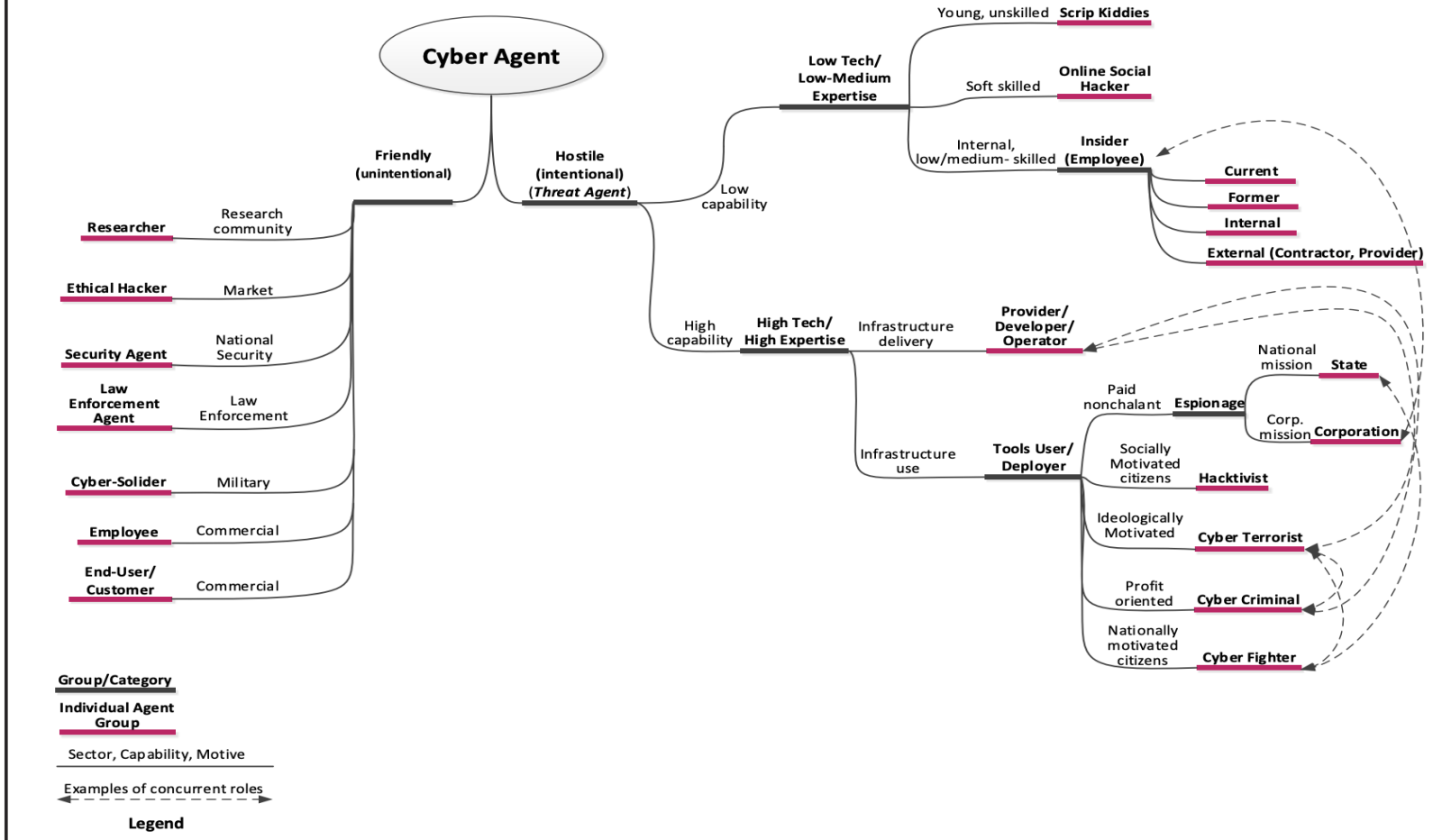
Source

Fortune Business Insight

Business Wire

Threat Agents [1]

Figure —2.5 Cybersecurity Threat Agents



Source: Marinos, Louis, A. Belmonte, E. Rekleitis, "ENISA Threat Landscape 2015," ENISA, January 2016, Greece

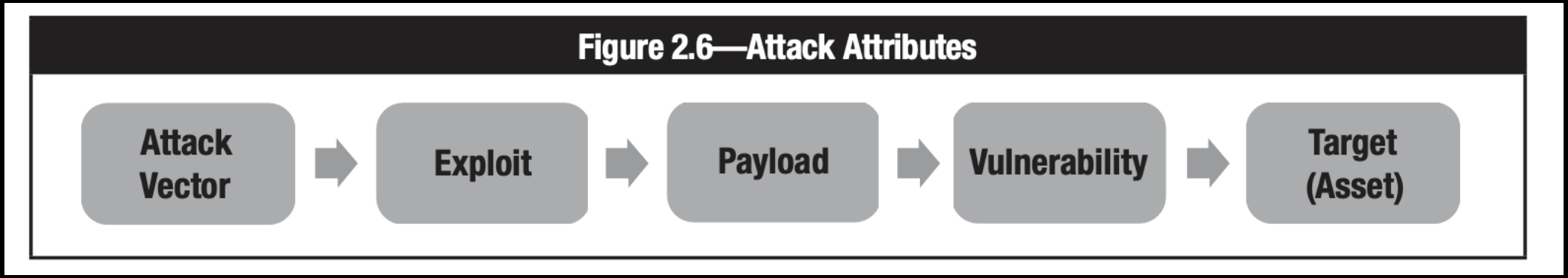
Threat Agents [1]

- **Corporations**
  - Corporations have been known to breach security boundaries and perform malicious acts to gain a competitive advantage
- **Cybercriminals**
  - Individuals or members of an organized crime group with a goal of financial reward
  - They meet in underground forums to trade tips and data and coordinate attacks
  - Motivated by the desire for profit
- **Cyberterrorists**
  - Characterized by their willingness to use violence to achieve their goals
- **Cyberwarriors**
  - Nationally motivated citizens who may act on behalf of a political party or against another political party that threatens them.
- **Employees**
  - Dissatisfied current or former employees represent a clear cybersecurity risk

Threat Agents [1]

- **Hacktivists**
  - Although they often act independently, politically motivated hackers may target specific individuals or organizations to achieve various ideological ends
  - Aim of their attacks is often to promote and publicize their cause
- **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.
  - Stuxnet Worm
- **Online social hackers**
  - Skilled in social engineering, these attackers are frequently involved in cyberbullying, identity theft and collection of other confidential information or credentials.
- **Script kiddies**
  - Script kiddies are individuals who are learning to hack
  - Code injections and distributed denial-of-service (DDoS) attacks.

Attack Attributes



ENISA Threat Landscape (ETL) report (2022)

- Prime threats:
  1. Ransomware
  2. Malware
  3. Social Engineering threats
  4. Threats against data
  5. Threats against availability: Denial of Service
  6. Threats against availability: Internet threats
  7. Disinformation – misinformation
  8. Supply-chain attacks

MALWARE

- Malicious code
- Software designed to gain access to targeted computer systems, steal information or disrupt computer operations
- **Types:**
  - Viruses
  - Network worm
  - Trojan horses
  - Botnets
  - Spyware
  - Adware
  - Ransomware
  - Keylogger
  - Rootkit

	Threat Agents								
	Cyber criminals	Insiders	Online social hackers	Nation States	Corporations	Hacktivists	Cyber Fighters	Cyber terrorists	Script kiddies
Malware	✓	✓	✓	✓	✓	✓	✓	✓	✓
Web-based attacks	✓			✓	✓	✓	✓	✓	✓
Web application attacks	✓			✓	✓	✓	✓	✓	✓
Botnets	✓			✓	✓	✓	✓	✓	✓
Denial of service	✓			✓	✓	✓	✓	✓	✓
Physical damage/ theft /loss	✓	✓		✓	✓			✓	
Insider threat	✓	✓		✓	✓			✓	
Phishing	✓	✓	✓	✓	✓	✓	✓	✓	✓
Spam	✓		✓	✓	✓	✓	✓	✓	✓
Exploit kits	✓			✓	✓	✓			✓
Data breaches	✓	✓		✓	✓	✓	✓	✓	✓
Identity theft	✓	✓		✓	✓	✓	✓	✓	✓
Information leakage	✓	✓	✓	✓	✓	✓	✓	✓	✓
Ransomware	✓		✓						✓
Cyber espionage		✓		✓	✓				

Legend:
Primary group for threat: ✓
Secondary group for threat: ✓

ENISA ETL 2015

OTHER ATTACK TYPES

- Advanced persistent threats (APTs)
- Backdoor
- Brute force attack
- Buffer overflow
- Cross-site scripting (XSS)
- DoS attack
- Man-in-the-middle attack
- Social engineering
- Phishing
- Spear phishing
- Spoofing
- Structure Query Language (SQL) injection
- Zero-day exploit

Advanced Persistent Threats (APTs)

- Complex and coordinated attacks directed at a specific entity or organization
- Require a substantial amount of research and time, often taking months or even years to fully execute
- APT is a term, indicating the class of complexity; however, it cannot be tested if a particular attack was APT or not.
  - Based on Fire Eye report on 2018, the average time to detect APT existence in the system is:
    - Americas: 71 days
    - EMEA: 177 days
    - APAC: 204 days

Backdoor

- A means of regaining access to a compromised system by installing software or configuring existing software to enable remote access under attacker-defined conditions
- Example: WordPress was spotted with multiple backdoors in 2014. These backdoors were WordPress plug-ins featuring an obfuscated JavaScript code.

Compromising Passwords

- Bypass access controls by guessing passwords
- Cracking
  - Attempting to guess a password
- Brute force attack
  - Application of computing and network resources to try every possible combination of options
- Dictionary attack
  - Variation on the brute force attack
  - Narrows the field by selecting specific target accounts and using a list of commonly used passwords

DoS and DDoS [3]

- Denial-of-service (DoS) attack
  - Attacker sends a large number of connection or information requests to a target
  - So many requests are made that the target system cannot handle them along with other, legitimate requests for service
- Distributed denial-of-service (DDoS)
  - Coordinated stream of requests against a target from many locations at the same time
- Any system connected to the Internet is a potential target for denial-of-service attacks

Social Engineering [3]

- Process of using social skills to convince people to reveal access credentials or other valuable information to the attacker

E-mail Attacks [3]

- E-mail
  - Vehicle for attacks rather than the attack itself
- Spam
  - Used as a means to make malicious code attacks more effective
- Mail bomb
  - Attacker routes large quantities of e-mail to the target system
- Phishing
  - Attempts to convince a user that the originator is genuine, but with the intention of obtaining information for use in social engineering
- Spear phishing
  - Social engineering techniques are used to masquerade as a trusted party to obtain important information such as passwords from the victim.

Zero-day Exploit

- A vulnerability that is exploited before the software creator/vendor is even aware of its existence

In-Class Activity

- **Attacks and Threat agents**
  - **Discussion Board: Module 1 - Attacks and Threat Agents**
- **What was the goal?**
- **Done by which threat agent?**

What to do next?

1. Create groups
2. Set up your machines for course labs
   - Follow the Lab 1 pre-requisite

Training

1. Join the CTF platforms:
    - Hack The Box (HTB)
    - TryHackMe
    - Introduction to Linux and Kali Linux
- Self-Paced Basic Linux course at Edx. @ https://courses.edx.org/courses/course-v1:LinuxFoundationX+LFS101x+3T2018/course/
- Learn Linux as a novice: https://overthewire.org/wargames/bandit/
- Kali Linux @ https://www.udemy.com/kali-linux-101/

References

1. CSX Cybersecurity Fundamentals Study Guide, 2nd Edition
   - Chapters 1, 2
2. ENISA Reports @ www.enisa.europa.eu