Cybersecurity Kill Chain™ Glossary

Created by: Andrea Rebora, Teaching Assistant

1. **Backdoor** – A backdoor is a means to access a computer system or encrypted data that bypasses the system's security mechanisms.
2. **Cyber Kill Chain** – Kill chain is a term originally used by the military to define the steps an enemy uses to attack a target. Similar in concept to the military's model, the Cyber Kill Chain defines the steps used by cyber attackers in cyber-based attacks.
3. **F2T2EA** – Find, Fix, Track, Target, Engage, and Assess.
4. **Network Scanner** – A network scanner is a tool used to find and categorize devices running on a network. The user inputs a range of IP addresses into the tool and the scanner determines if there is an active device present on each given IP address. One of the most famous network scanners is Nmap, the Network Mapper.
5. **Payload** – A payload is the carrying capacity of a packet or other transmission data unit. In the context of malware, the payload refers to malicious code that causes harm to the target.
6. **Penetration Testing** – It is the practice of testing a computer system, network, or web application to find security vulnerabilities that an attacker could exploit. It can be automated with software applications or performed manually. The process involves analyzing and assessing the target, and reporting back the findings.
7. **Port Scanner** – A port scanner is used for determining which ports on a network are open. Using a port scanner on a network or server reveals which ports are open and listening (receiving information), as well as revealing the presence of security devices such as firewalls.
8. **Reconnaissance** – In this phase, the attacker finds out the information he needs to breach the system, such as what traffic the firewall lets through, what hosts are in the network, what services are running, etc.
9. **Vulnerability** – A vulnerability is a mistake in software code that provides an attacker with direct access to a system or network. For instance, a vulnerability may allow an attacker to pose as a system administrator who has full access privileges.
10. **Vulnerability Scan** – A vulnerability scan is the inspection of potential points of exploit on a computer or network to identify possible vulnerabilities.

References:

1. https://searchsecurity.techtarget.com/definition/back-door
2. https://www.sans.org/security-awareness-training/blog/applying-security-awareness-cyber-kill-chain
4. https://study.com/academy/lesson/what-is-a-network-scanner-definition-use.html
5. https://searchsecurity.techtarget.com/definition/payload
6. https://searchsecurity.techtarget.com/definition/penetration-testing
7. https://www.techopedia.com/definition/13076/port-scanner
8. https://www.usna.edu/CyberDept/sy110/lec/cyberRecon/lec.html
9. https://www.rapid7.com/fundamentals/vulnerabilities-exploits-threats/
10. https://www.beyondtrust.com/resources/glossary/vulnerability-scanning