Week 3 – Exploitation and detection  
CIS 450  
Krutarth Panchal

## Week 3- Exploitation and detection

**Concept 1:**

Cyber Security (CS) Analysts commonly conduct assessments and respond to incidents as a result of penetration tests or real-world exploitation. CS Engineers often build the solutions (tools) and implement the architecture that make it possible for analysts to monitor and detect activity within the environment. Information Security Analysts typically create, modify, and update organizational policy often used to establish standards.

**1.** What tasks do you think each role would complete once a pen test is complete and results have been handed to the organization? Explain your answer.

**Ans:** Once the Pentest is completed and results have been handed to the organization, Cyber Security Anaylst, CS Engineer and IS Analyst will do the following:  
  
**>** Cyber Security (CS) Analyst: Will analyze the pen test results, identifies vulnerabilities, assesses their risk, and prioritizes remediation efforts. Also will document the findings and communicate them to relevant stakeholders.

**>** CS Engineer: Will collaborate with the CS Analyst to understand the exploited vulnerabilities and implements security patches or configuration changes to address them. They will improve the security architecture based on the pen test findings.

**>** Information Security Analyst: Will reviews the pen test results to update or create security policies that can prevent similar vulnerabilities in the future. They may also work with CS Engineers to ensure new security measures align with organizational policies.

**Concept 2:**

The cumulative goal of a pen tester is to exploit or by-pass engineer's security controls and countermeasures that security engineers use to secure and provide visibility into the environment. Visibility is vital for detection. If you cannot see the activity, you cannot effectively defend or secure your environment.

**2.** What are two methods or tactics that can be leveraged to gather intelligence from the target network?

Social Engineering: Manipulating people into divulging confidential information or performing actions that compromise security. Pen testers may use social engineering techniques to gain access to systems or information that would be difficult to exploit technically (discussed in concept 4).

Open-Source Intelligence (OSINT): Gathering information about the target network from publicly available sources like websites, social media, and security reports. This can help identify potential vulnerabilities and weaknesses.

**Concept 3:**

Take a look at a basic architectural framework design.   ([Open Link](https://canvas.highline.edu/courses/2426355/files/238600759/download))

**3.** Which of the systems in Slide 3 is tasked with collecting and providing log analytics?

**Ans:** SIEM (Security Information and Event Management), the SIEM system in the diagram is responsible for collecting and analyzing logs from various security tools and network devices. It provides insights into security events and help identify potential threats.

**Concept 4:**

Thinking about the concepts in Chapter 3 and referencing the basic diagram in Concept 3, answer the following questions.

**4.** Which systems in the architecture security diagram would be considered a Countermeasure?

**Ans:** Firewalls, WAF (Web Application Firewall), EDR (Endpoint Detection and Response), and AV (Antivirus) are all security countermeasures in the diagram. They are designed to prevent, detect, and respond to security attacks.

**5.** Which systems might be targets of a Precision Strike, Customized Exploitation, Tailored Exploit, or a Zero Day Angle?

**Ans:** Attackers may target various systems in the architecture here are a few systems:

**>** Web Applications: Web servers and applications are targeted for exploiting vulnerabilities that will allow attackers to steal data, inject malicious code or deface the website in recent cases.

**>** Endpoints (Network Devices, Workstations): Unpatched vulnerabilities in device operating systems or applications will give attackers a foothold on the network.

**>** Security Tools: Attackers can target many security tools to disable or bypass their monitoring capabilities.

6. What is social engineering and how can it be applied in pen testing?

**Ans:** Social engineering is the art of manipulating or tricking techniques that exploits human weaknesses to gain access to confidential information, computer systems or data. For instance, a pen tester can use social engineering to trick an employee into giving them their login credentials or granting them access to a restricted area.