Module : Intro to Cybersecurity

Offensive Security

🔍 Purpose

- Identify and exploit weaknesses in systems
- Understand hacker mindset to improve defenses

Key Roles :

Red Teamer

- Emulates real adversaries
- Avoids detection, maintains persistence
- Tests detection and response capabilities

Penetration Tester (Ethical Hacker)

- Tests system security via simulated attacks
- Finds vulnerabilities and reports risk levels
- Helps in patching flaws before real attacks occur

Exploit Developer

- Creates custom exploits for vulnerabilities
- Works closely with vulnerability researchers
- Helps Red Teams and pentesters with advanced payloads

Social Engineer

- Uses psychological manipulation to trick users
- Executes phishing, pretexting, baiting, and tailgating
- Tests human layer of security

Malware Developer (Offensive)

- Crafts custom malware or payloads for testing security posture
- Often writes droppers, backdoors, or ransomware simulators
- Helps simulate sophisticated APT-style attacks

Wireless Attacker

- Focuses on exploiting Wi-Fi and Bluetooth protocols
- Attacks include Evil Twin, Deauthentication, and WPA cracking
- Tests wireless network segmentation and client isolation

Voice/VoIP Attacker

- Exploits telecommunication systems like VoIP infrastructure
- Common attacks include vishing, spoofing, and SIP flooding
- Evaluates the resilience of communication systems

Web Application Attacker

- Specializes in exploiting web applications
- Uses techniques like SQL Injection, XSS, RCE, etc.
- Often overlaps with bug bounty hunters and app pentesters

Bug Bounty Hunter

- Independently finds vulnerabilities in public applications
- Reports to vendors via responsible disclosure programs
- Paid based on severity of the bug (bug bounty programs like HackerOne, Bugcrowd)

Network Attacker

- Performs deep assessments of internal and external networks
- Uses scanning, sniffing, spoofing, and man-in-the-middle attacks
- Evaluates segmentation, firewall rules, and exposed services

Defensive Security

Purpose

- Prevent intrusions
- Detect and respond to attacks

Key Team: Blue Team

Responsibilities

- User cybersecurity awareness training
- Asset inventory and documentation
- System updates & patch management
- Deployment of firewalls & Intrusion Prevention Systems (IPS)
- Setup of logging and monitoring tools

Blue Teamer

- Defends against real-time cyberattacks
- Monitors systems, analyzes behavior, and responds to threats
- Improves detection, response, and recovery processes

Security Analyst

- Monitors logs, alerts, and incidents
- Correlates data to identify potential threats
- Reports on vulnerabilities and trends to inform security policies

Security Engineer

- Designs and implements security infrastructure (firewalls, IDS/IPS, VPNs)
- Patches systems and mitigates vulnerabilities
- Supports prevention through secure network architecture

Incident Responder

Phases:

1. Preparation: Team readiness and policies
2. Detection & Analysis: Identifying threats
3. Containment, Eradication & Recovery: Stop spread, remove threats, restore services
4. Post-Incident Activity: Reporting, lessons learned

- Reacts to security breaches in real time
- Investigates incidents, contains damage, and restores systems
- Prepares and maintains incident response plans and playbooks

Digital Forensics Expert

- Investigate evidence from:
    - File Systems (deleted/created files)
    - Memory dumps (RAM-based malware)
    - System Logs (event trails)
    - Network Logs (traffic analysis)
- Collects and analyzes digital evidence
- Traces attacker activity using memory dumps, logs, and disk images
- Supports legal cases or internal investigations

Malware Analyst (Defensive)

- Dissects malicious code to understand how it works
- Identifies Indicators of Compromise (IOCs)
- Assists in developing antivirus signatures and threat detection rules
- **Types of Malware:**
    - Virus: Self-replicates, damages files
    - Trojan Horse: Malicious program hidden in a legitimate one
    - Ransomware: Encrypts files; demands payment

- **Analysis Methods:**
- Static Analysis: Inspect without running code
- Dynamic Analysis: Run in sandbox to observe behavior

Threat Intelligence Analyst

Purpose

- Collect and analyze data to anticipate attacker behavior
- Build threat-informed defense

Intelligence Process

1. Data Collection: Local (logs), public (forums)
2. Processing: Structure for analysis
3. Analysis: Identify adversaries, motives, and techniques
4. Outcome: Mitigation plans and proactive response strategies

- Gathers and analyzes data on adversaries
- Tracks TTPs (Tactics, Techniques, Procedures) of threat actors
- Delivers threat-informed insights to security teams

SOC Analyst (Security Operations Center)

Function

A centralized team monitoring systems and networks to detect threats.

SOC Focus Areas

- Vulnerabilities: Patch or mitigate weaknesses
- Policy Violations: Detect breaches of internal rules
- Unauthorized Activity: Detect login misuse, data exfiltration
- Intrusions: Immediate detection and mitigation of attacks
- Monitors dashboards and SIEM tools (e.g., Splunk, ELK, QRadar)
- Investigates suspicious activity and triages alerts
- Escalates high-risk incidents to senior defenders

Firewall / IDS/IPS Administrator

- Configures and monitors firewalls and intrusion detection/prevention systems
- Tunes signatures and rules to avoid false positives/negatives
- Ensures perimeter defenses are up-to-date and effective

Compliance & Risk Officer

- Ensures organizational security meets regulations (GDPR, HIPAA, ISO 27001)
- Conducts audits and risk assessments
- Develops policy and governance frameworks

Access Control / Identity Management Specialist

- Manages user privileges and identity systems (IAM)
- Implements role-based access, MFA, and zero-trust principles
- Prevents unauthorized access to sensitive data and systems

Cybersecurity Careers Overview

Role	Key Focus	Responsibilities
Security Analyst	Analysis & reporting	Monitor networks, draft security plans
Security Engineer	Build protections	Design, implement, and test controls
Incident Responder	Real-time action	Respond to threats, minimize damage
Digital Forensics Expert	Investigate incidents	Gather legal evidence, report findings
Malware Analyst	Reverse-engineer malware	Perform static/dynamic analysis, document behavior
Penetration Tester	Ethical hacking	Find and report vulnerabilities
Red Teamer	Simulated adversary	Test detection/response via stealth attacks