|  | **OFFENSIVE** | **DEFENSIVE** |
| --- | --- | --- |
| **Skills** | Ethical hacking skills:   * SQL injection   + ‘ or 1=1 –   + Bypassing login credentials * Exploit broken anti-automation vulnerabilities   + Bypass CAPTCHA   + Submit multiple HTTP requests     - Positions, Payloads * Brute force attack   + Modifying code in HTTP POST requests * Privilege escalation   + Modifying in HTTP requests * Sensitive data exposure * Directory transversal attack * Broken access control * Null byte injection   + %00, %2500   Attack mitigation techniques:   * Encrypt data both at rest and in transit using a secure protocol * Implement access control mechanisms   + Restrict access to certain directories and files with Access Control Lists * Use multi-factor authentication * Validate, filter, and sanitize all client-provided data * Define data types and strict patterns for all string parameters | Analyze network traffic packets   * Trace source(s) and path of infection   + IP and MAC addresses   + Domain and Host names   + Windows user account   + Ports and protocols involved * Identify instances of malicious traffic   + Suspicious file attributes, source addresses, and communication flags * Investigate cause of security alerts * Apply static and dynamic analysis techniques   Recognize and identify characteristics of malware, including malicious email attachments and downloaded internet content   * Exploit Kits (EK) * Encryption types * Points of network entry * Identifiers   + SHA1, SHA256, MD5   + File extensions   + Executed commands   Audit CLI logs   * Identify malicious command executions   + Keylogging scripts   + Linux-based security exploits     - i.e. enumeration, privilege escalation |
| **Tasks** | Log into unknown admin, user accounts  Access confidential documents, data  Escalate user privileges  Edit website content | Analyze PCAP files  Identify malware type, source  Trace path of system infection  Audit security alert logs |
| **Tools** | Burp Suite   * Intercept * Repeater * Intruder   OWASP Juice Shop | Wireshark  VirusTotal  VirtualBox  Sysinternals  Powershell, Terminal  PeStudio  dotPeek  Regshot  Process Hacker |