





Chapter 4 - Key Topics

Aa Description	≡ Element	▼ Page	≡ Summary
<u>Understanding passive vs. active reconnaissance</u>	Paragraph	154	Passive Reconnaissance - researching the victims public records, social media, DNS, & whois. Tools such as Shodan, Maltego, Recon-ng, The Harvester, Spiderfoot Active Reconnaissance - carried out by tools called scanners. Various application, port, & vulnerability scanners exist.
<u>Understanding Open-Source Intelligence (OSINT)</u>	Tip	156	A method of gathering publically available intelligence sources to collect and analyze information about a target. Open-source because collecting this info does not require any covert action.
<u>Different types of port-and network-scanning techniques</u>	List	157	Basic Port Scan - Scanning predetermined TCP/UDP ports by sending specially crafted packets TCP Connect Scan - Refers to Unix connect() sys call. If port open victim completes three-way handshake. TCP SYN Scan (Half-Open Scan) - Does not open full TCP connection, the attacker sends SYN and if victim responds with SYN/ACK port is considered open. TCP ACK Scan - Sends ACK to determine if port is filtered or unfiltered. Used to determine if firewalls are deployed and their rule-sets. TCP FIN packets may be used to bypass legacy firewalls. UDP Scan - Victim responds with ICMP "Port Unreachable" messages to determine if port is open. Affected by firewalls & ICMP rate limiting. Strobe Scan - Attackers use this scan to find ports they know how to exploit, execute on a more confined level. Stealth Scan - Designed to go undetected by network auditing tools

Aa Description	☰ Element	▼ Page	☰ Summary
<u>What are phishing, pharming, & malvertising?</u>	List	160	<p>Phishing - The attacker presents a link that looks like a valid, trusted resource to a user.</p> <p>Spear Phishing - Targets specific individuals or companies. Pharming - Term used to describe a threat actor redirecting a victim from a valid website or resource to a malicious one that could appear as the valid site. Malvertising - Act of incorporating malicious ads on trusted websites.</p>
<u>Privilege Escalation Attacks</u>	Section	162	Process of taking some level of access and achieving an even greater level of access.
<u>Backdoors</u>	Section	163	Threat actors may install backdoors on compromised systems to allow future access or collect information.
<u>Buffer Overflow & Code Execution</u>	Section	163	Remote Code Execution (RCE) allows an attacker to fully compromise the CIA of a system. Buffer Overflows can lead to RCE. Stack-based BO relies on overflowing a fixed-length buffer. A heap overflow relies on overwriting internal structures such as linked list pointers.
<u>Man-in-the-Middle attacks</u>	Section	165	Results when an attacker places themselves in the middle of two devices communicating with the intent of performing reconnaissance or manipulating data. ARP Poisoning - attacker spoofs Layer 2 MAC addresses to trick victim device into believing attacker is the default gateway. Rogue switches can be used to manipulate Spanning Tree Protocol (STP) to become the root switch. Rogue routers can be used to manipulate network routers into believing the attacker has a better route. Can occur by installing malware on a victim machine that can manipulate and send packets to an attacker. Safeguard data in motion by using encryption.

 Description	 Element	 Page	 Summary
<u>Identifying the different types of DDoS attacks</u>	List	166	Direct DDoS - an attack where the source of the attack generates the packets and sends them directly to the victim. Reflected DDoS, Amplification DDoS
<u>What are botnets?</u>	Paragraph	167	A collection of compromised machines that an attacker can manipulate from a command and control (C2 or CnC) system.
<u>Reflected DDoS attacks</u>	Paragraph	167	The source of attack is sent spoofed packets that appear to be from the victim and the source becomes attack pawns by sending response traffic to the victim.
<u>What are amplification attacks?</u>	Paragraph	168	A type of reflected attack where response traffic is made of packets that are much larger than those that were initially sent by the attacker. For example, DNS queries are sent and the DNS responses are much larger in packet size than the initial query packets.
<u>Attack Methods for Data Exfiltration</u>	Section	168	Many methods of data exfiltration of which DNS tunneling is very popular. Examples, DNS2TCP, DNScat-P, Iodine Protocol v5.00, Iodine Protocol v5.02, OzymanDNS, SplitBrain, TCP-Over-DNS, YourFreedom
<u>ARP Cache Poisoning</u>	Paragraph	169	Attackers can attack systems on a subnet by intercepting traffic intended for other systems on the subnet by spoofing the MAC address at Layer 2. Dynamic ARP inspection validates IP-to-MAC address bindings.
<u>Route Manipulation Attacks</u>	Paragraph	171	BGP hijacking attack - most popular route manipulation attack, attacker use a rogue router to announce prefixes that have not been assigned by the org, these contains routes to the attacker.

Aa Description	☰ Element	▼ Page	☰ Summary
<u>Different types of password attacks</u>	List	171	<p>Password-guessing attack - Most common, some methods are brute-force attack (combinations of characters) & dictionary attack (whole words). Tools include Hydra, John the Ripper, Cain & Abel. Password-resetting attack - Easier to simply reset the password, most tools contain bootable version of Linux that can mount NTFS volumes to help locate and reset Admin password. Password Cracking - Take a password hash and attempt to convert it to it's plaintext. Possible hashes put in lookup table called Rainbow Table, hashes can be looked up in rainbow table. Password Sniffing - Attacker sniffs authentication packets between server and client to help in cracking. Password Capturing - With keyloggers or Trojan horses.</p>
<u>The most common attacks against wireless networks</u>	List	172	<p>Installing a rogue access point - Attacker installs access point as a backdoor to obtain network access. Jamming wireless signals and causing interference - Create a DoS condition within the wireless network. War Driving - Used to find access points wherever they may be, attackers can drive around and gather large amounts of info. Bluejacking - Attacker sends unsolicited messages to another device via Bluetooth. Evil twin attack - Done when creating rogue access points, attacker configures the access point exactly the same as on the network. IV attack - Attacker can cause modification to the IV (Initialization Vector) of an encrypted wireless packet to ultimately generate another key for use in decryption. WEP/attack - WEP should never be used, WPA 3 is the latest version of WPA specification. WPA 1 & 2 vulnerable to KRACK. WPS attack - WPS password-guessing tools used to gain WPS passwords.</p>

Aa Description	☰ Element	▼ Page	☰ Summary
<u>Defining & understanding different types of security vulnerabilities</u>	List	173	<p>API-based vulnerabilities - aimed at flaws in APIs</p> <p>Authentication & Authorization bypass vulnerabilities - Used to bypass authentication and authorization mechanisms of systems within the network.</p> <p>Buffer Overflow - Occurs when a program tries to write past the bounds of a memory buffer. This corruption of memory can lead to Code Execution.</p> <p>Cross-site scripting (XSS) vulnerability - Malicious scripts are injected into legitimate and trusted websites. Successful exploitation may lead to the execution of malicious code, account compromise, session hijacking, redirection, & modification of local files. Found in HTTP headers, input fields that echo user data, hidden form fields, & error messages that return user input.</p> <p>Cross-site request forgery (CSRF) vulnerability - Forces users to execute malicious steps on a web application, exploiting trust between a user and a web app.</p> <p>Cryptographic vulnerability - Flaw in a cryptographic protocol or its implementation.</p> <p>Deserialization of untrusted data vulnerability - Uses or causes malformed data or unexpected data to abuse application logic.</p> <p>Double Free - Occurs in C, C++ languages when free() is called more than once with the same memory address.</p> <p>Insufficient Entropy - When crypto applications lack entropy. Pseudo-random Number Generators (PRNGs) are susceptible to insufficient entropy vulnerabilities.</p> <p>SQL injection vulnerabilities - Attackers can exploit vulnerable web applications to interact with a database.</p>
<u>The Open Web Application Security Project (OWASP)</u>	Paragraph	174	<p>OWASP provides references to vulnerabilities as well as mitigations, training, tools, and general infosec material.</p>

Aa Description	:≡ Element	▼ Page	≡ Summary
<u>Accessing Omar's GitHub repository & WebSploit labs</u>	Tip	174	https://h4cker.org/github
<u>Untitled</u>			