Course Notes

1 Definitions

1.1 Chapter 1: Introduction To Ethical Hacking

1.1.1 Information Security Overview

- Intelligence based warfare: A sensor-based technology that directly corrupts technological systems. "Warfare that consists of the design, protection, and denial of systems that seek sufficient knowledge to dominate the battle space.
-

1.1.2 Cyber Kill Chain Concepts

- Reconnaissance: An Adversary performs reconnaissance to collect as much information about the target as possible to probe for weak points before attacking.
- Installation: Adversary downloads and intalls more malicious software on the target system to maintain access to the target network for an extended period.
- Command and control: The adversary creates a command and control channel, which establishes two-way communication between the victim's system and adverary-controlled servers to communicate and pass data back and forth.
- Weaponization: Adversary selects or creates a tailored deliverable malicious payload (remote access malware weapon) using an exploit and a backdoor to send it to the victim.
-

1.1.3 Hacking and Ethical Hacking Concepts

1.1.4 Information security controls, laws and standards

- SOX Titles:
  - Title 3: Corpoate Responsability, eight sections and mandates that senior executives take individual responsability for the accuracy and completeness of corporate financial reports.

- Title 5: Analyst Conflicts of Intrest: One section that discusses the measures designed to help restore investor confidence in the reporting of securities analyst. Defines the code of conduct for securities analysts and requires that they disclose any knowable conflicts of interest.
- Title 6: Commission Resources and Authority: four sections defining practices to restore investor confidence in securities analysts. Defines the SEC's authority to censure or bar securities professionals from practice and defines the conditions to bar a person from practicing as a broker, advisor, or dealer.
- Title 7: Studies and Reports: five sections, requires the Comptroller General and the Securities and Exchange Commission (SEC) to perform various studies and to report their findings.

1.2 Chapter 2: Footprinting and Reconnaissance

1.2.1 Footprinting Concepts

- Sherlock: To search a vast number of social networking sites for a target username. This tool helps the attacker to locate the target user on various social networking sites along with the complete URL.
- BeRoot: BeRoot is a post-exploitation tool to check for common misconfigurations which can allow an attacker to escalate their privileges.
- OpUtils: SNMP enumeration protocol that helps to monitor, diagnose and trouble shoot the IT resources.
- Sublist3r: Sublist3r is a Python script designed to enumerate the subdomains of websites using OSINT. It enables you to enumerate subdomains across multiple sources at once.
- Passive footprinting: no direct interaction, archived and stored information from publically accessible sources.
  - Finding information through search engines
  - Finding the Top-level Domains (TLDs) and sub-domains of a target network through web services.
  - Collecting information on the target through web services.
  - Performing people search using social networking sites and people search engines.
  - Gathering financial information about the target through financial services.

  - Gathering infrastructure details of the target organization through job sites.
  - Monitoring target using alert services.
- Active footprinting, direct interaction with the target network:
  - Querying published name servers of the target.
  - Extracting metadata of published documents and files.
  - Gathering website information using web spiderin and mirroring tools.
  - Gathering information through email tracking.
  - Performing Whois lookup
  - Extracting DNS Information
  - Performing traceroute analysis
  - Performing social engineering.

1.2.2 Footprinting Methodology

1.2.3 Footprinting Tools and Countermeasures

1.3 Chapter 3: Scanning Networks

1.3.1 Network Scanning Concepts and Tools

1.3.2 Host, Port and Service Discovery

1.3.3 OS Discovery and Scanning Beyond IDS/Firewall

1.4 Chapter 4: Enumeration

1.4.1 Enumeration Concepts

1.4.2 NetBIOS and SNMP Enumeration

- Border Gateway Protocol (BGP) is a standardized exterior gateway protocol designed to exchange routing and reachability information among autonomous systems on the internet. Used by ISPs to maintain large routing tables. Utilizes port 179

1.4.3 LDAP, NTP, NFS, and SMTP Enumeration

- LDAP - Lightweight Directory Access Protocol

1.5 Chapter 5: Vulnerability Assessment

1.5.1 Vulnerability Assessment Concepts

- Vulnerability management lifecycle:
  - Risk assessment: All serious uncertanties that are associated with the system are assessed and prioritized, and remediation is planned to permanently eliminate system flaws.
  - Remediation: The process of applying fixes on vulnerable systems in order to reduce the impact and severity of vulnerabilities.
  - Verification: Provides clear visibility into the firm and allows the security team to check whether all the previous phases have been perfectly employed or not.
  - Monitoring: Organizations need to perform regular monitoring to maintain system security. Continuous monitoring identifies potential threats and any new vulnerabilities.
- The Common Vulnerability Scoring System (CVSS) provides an open framework for communicating the characteristics and impacts of IT vulnerabilities.
  - Base metric group
    - Exploitability Metrics
      - Attack Vector
      - Attack Complexity
      - Privileges Required
      - User Interaction
      - Scope
    - Impact Metrics
      - Compatibility Impact
      - Integrity Impact
      - Availability impact
      - Scope
- Temporal Metric group

  - Exploit Code maturity
  - Remediation level
  - Report confidence
- Environmental Metric group
  - Confidentiality Requirement
  - Integrity Requirement
  - Availability Requirement
  - modified Base Metrics

1.6 General / Unsorted

- CIA Triad:
  - Confidentiality: unauthorized access to information.
  - Integrity: Trustworthiness of data
  - Availability: accessible when required
  - (Other) Non-repudiation: Sender of a message cannot deny having sent the message, same for receiver.
  - (Other) Authenticity: quality of being genuine
- OSI model - Open System Interconnection model
- Local Area Network (LAN): Computer network that connects two or more computers within a limited area.
- Virtual Local Area Network (VLAN): Broadcast domain that is divided in a computer network at the data link layer (OSI layer 2).
- Wide Area Network (WAN): Covers larger area than a LAN, typically involves telecommunication circuits for a special purpose, ie: banking network. Nodes are more than 10 miles apart.
- Time to live (TTL): time period a message can live on the network before it is discarded. (8-bits). Number of seconds or number of hops?
- User Datagram Protocol (UDP): light weight communication protocol that gives no assurance of delivery. If the application receives out of order packets they are

destroyed rather than worrying about reordering them.

- Transmission Control Protocol (TCP):
- Internet of Things (IoT): Devices with embedded software and network access.
- Malware: software created to harm or infiltrate a computer system without the owners consent.
  - Virus: Create copies of themselves in other programs and activate from a trigger event.
  - Worm
  - Spyware
  - Trojan
- Information Security Policy: set of rules sanction by an organization to ensure that user of networks abide by the prescriptions regarding the security of data stored within the boundaries of the organization.
- Event: Something that happens that is detectable
- Incident: an event that violates policy.
- Certificate Authority: Organization that issues digital certificates.
- Vulnerability Scanner: Computer program designed to assess computer systems, network or applications for known weaknesses.
- Uniform Resource Locator (URL): reference to a web resource. Is a specific type of URI.
- Uniform Resource Identifier (URI): Unique sequence of characters that identifies a logical or physical resource used by web technologies. the `http://` part of the url.
- DNS Zone transfer: Used to duplicate or make copies of DNS data across a number of DNS servers or to back up DNS files.
- Open-source intelligence: to describe identifying information about a target using freely available sources.
- Defence in breadth: planned, systematic set of multi-disciplinary activities that seek to identify, manage, and reduce risk of exploitable vulnerabilities at every stage of the system, network, or sub-component lifecycle.

- Defence in depth (DiD): Information security approach in which a series of security mechanisms and controls are layered throughout a computer network.
- Lawful Interception: Process of legally intercepting communications betwen two or more parties for surveillance on telecommunications, VoIP, data, and multiservice networks.
- Internet Zones
  - Internet (uncontrolled zone): outside the boundary of your organization.
  - Internet DMZ (controlled zone): Internet-facing controlled zone that contains components in which clients may directly communicate with. Usually buffered by two firewalls one from internet to DMZ and one from DMZ to the internal network.
  - Production network (restricted zone): A restricted zone supports functions to which access must be strictly controlled; direct access from an uncontrolled network should not be permitted. In a large enterprise, several network zones might be designated as restricted. As with an internet DMZ, a restricted zone is typically bounded by one or more firewalls that filter incoming and outgoing traffic.
  - Intranet (controlled zone): is not heavily restricted in use, but an appropriate span of control is in place to assure that network traffic does not compromise the operation of critical business functions.
  - Management network (secured zone): In a secured zone, access is tightly controlled and available to only to a small number of authorized users. Access to one area of the zone does not necessarily apply to another area of the zone.

1.7 Attacks

- SQL Injection:
  - In-band SQL Injection: Attacker uses the same communication channel to launch the attack and gather results. (error-based and union-based SQL injection).
- Bluetooth
  - Bluesnarfing: Theft of information from a target device using a bluetooth connection.
  - Bluejacking: Transmission of data to a target device using a bluetooth connection.

- Operating System Attacks
- Application-Level Attacks
- Shrink Wrap Code Attacks
- Misconfiguration Attacks
- DHCP starvation attack: Broadcasting DHCP requests with spoofed MAC addresses to expend the available address pool, denying access to new users.
- MAC flooding attack: Attacker floods the switch MAC table to push legitimate MAC addresses out of the switch. This causes significant amounts of frames to be broadcasted to all ports.

1.8 Organizations

- Open Web Application Security Project (OWASP): International non-profit organization focused on web application security.
- Federal Risk and Authorization Management Program (FedRAMP): Cloud computing regulatory effort, government-wide, delivers systemized approach to security assessment, authorization, and continuous monitoring of cloud products and services.

1.9 Cloud computing

- Platform as a service (PaaS): Third-party provider delivers hardware and software tools to users over the internet. PaaS frees developers from having to install in-house hardware and software to develop or run a new application.
- Infrastructure as a Service (IaaS):
- Hardware as a Service (HaaS):
- Software as a Service (SaaS):
- Models:
  - Private
  - Public
  - Community: Infrastructure is shared by several organizations, usually with the same policy and compliance considerations.
  - Hybrid

1.10 Cryptography

- Ciphers
  - Symmetric Ciphers: Single key is used for encryption and decryption
    - Data Encryption Standard (DES): Symmetric-key block cipher with key size of 56-bits
    - Triple Data Encryption Algorithm (3DES, TDES, TDEA): Applies the DES algorithm 3 times to each data block. Key length of $56 \times 3 = 168$ bits when 3 independent keys are used, or 112 when two keys are independent.
  - Asymmetric Ciphers (Public key cryptography): One key can encrypt and one key can decrypt.
    -