

## CEH Certification Notes

### Table of Contents

Module 1: Introduction to Ethical Hacking  
Module 2: Footprinting and Reconnaissance  
Module 3: Scanning Networks  
Module 4: Enumeration  
Module 5: System Hacking  
Module 6: Malware Threats  
Module 7: Sniffing  
Module 8: Social Engineering  
Module 9: Denial of Service  
Module 10: Session Hijacking  
Module 11: Hacking Web Servers  
Module 12: Hacking Web Applications  
Module 13: SQL Injection  
Module 14: Hacking Wireless Networks  
Module 15: Hacking Mobile Platforms  
Module 16: Evading IDS, Firewalls, and Honeybots  
Module 17: Cloud Computing  
Module 18: Cryptography  
Post Module: Extra Resources

---

### Module 1: Introduction to Ethical Hacking

#### Information Security Overview

- Terminology
  - Hack Value: Notion among hackers that something is worth doing or interesting
  - Vulnerability: Existence of a weakness, design, or implementation error that can lead to an expected event compromising the security of the system
  - Exploit: A breach of IT system security through vulnerabilities
  - Payload: Part of an exploit code that perform the intended malicious action
  - Zero-Day Attack: An attack that exploits computer app vulnerabilities before the software developer releases a patch for the vulnerability
  - Daisy Chaining: Gaining access to one network and/or computer and then using the same info to gain access to multiple networks and computer that contains desirable info
  - Doxing: Publishing personally identifiable information
  - Bot: software app that can be controlled remotely to execute or automate pre-defined tasks
- Elements of Information Security
  - Non-Repudiation: Sender of a message cannot later deny having sent the message
  - Confidentiality: Only authorized users able to view content
  - Integrity: Trustworthiness of data or resource in prevention of unauthorized changes
  - Availability: assurance systems are accessible
  - Authenticity: The quality of being genuine

#### Information Security Threats and Attack Vectors

- Cloud computing: is an on-demand delivery of IT capabilities, and stores data. Must be secure
- Advanced Persistent Threats: APT focus on stealing info from victim machine w/o user aware
- Viruses and Worms: Capable of infecting a network within seconds
- Mobile Threats: Many attackers see mobile phone as a way to gain access
- Botnet: huge network of compromised systems
- Insider Attack: an attack performed on a corporate network by an entrusted person w/ access
  
- Threat categories: Network Threats, Host Threats, App Threats
- Types of Attacks: OS Attacks, Mis-Config attacks, App Level Attacks, Shrink Wrap Code Attacks

#### Hacking Concepts, Types, and Phases

- Hacking: Exploiting system vulnerabilities and compromising security
- Five Phases of Hacking: Reconnaissance, Scanning, Gaining Access, Maintaining Access, Clearing Tracks
- Reconnaissance: Preparation phase when an attacker seeks to gather information. Does not directly interact with the system, and relies on social engineering and public info
- Scanning: Identify specific vulnerabilities (in-depth probing). Using Port scanners to detect listening ports (companies should shut down ports that are not required)
- Gaining Access: Using vulnerabilities identified during reconnaissance [DoS, Logic/Time Exploit, reconfiguring/crashing system]
- Maintaining Access: Keeping a low profile, keeping system as a launch pad, etc.
- Clearing Tracks: Hiding malicious acts while continuing to have access, avoiding suspicion

### Ethical Hacking Concepts and Scope

Ethical Hacking: Using tools and techniques to identify vulnerabilities w/ permission

### Information Security Controls

- Information Assurance: Assurance for integrity, availability, confidentiality, and authenticity of info
- Threat Modeling: Risk Assessment approach for analyzing security. 1) Identify Security Objectives 2) Application overview 3) Decompose Application 4) Identify Threats 5) Identify Vulnerabilities
- Network Security Zoning (High to Low): Internet Zone - Internet DMZ - Production Network Zone - Intranet Zone - Management Network Zone
- Security Policies are the foundation of security infrastructure
- Info security policy defines basic requirements and rules to be implemented in order to protect and secure organizations information systems
- 4 types of security policies
  - Promiscuous Policy
  - Permissive Policy
  - Prudent Policy
  - Paranoid Policy
- Incident Management: set of defined processes to identify, analyze, prioritize, and resolve security incidents
- Types of Vulnerability Assessments:
  - Active Assessments
  - Passive Assessments
  - Host-Based assessment
  - Internal Assessment
  - External Assessment
  - Application Assessments
  - Network Assessments
  - Wireless Network Assessments
- Methodology of Assessment: - Acquisition - Identification - Analyzing - Evaluation - Reports
- Penetration Testing: Simulating an attack to find out vulnerabilities
- Blue Team: Detect and Mitigate
  - Red Team: Attack w/ limited access w/ or w/o warning

- Types of Pen Test:
  - black-box (no prior knowledge)
  - white-box (complete knowledge)
  - grey-box(limited knowledge)
- Lots of open source security testing methodologies (OWASP, NIST , etc)

#### Information Security Laws & Standards

- Payment card Industry Data Security Standard (PCI-DSS) - Payment Systems
- Sarbanes Oxley Act (SOX) - Protect investors and public by increasing reliability of corporate disclosures

### **Module 2: Footprinting and Reconnaissance**

#### Sections

1. Footprinting Concepts
2. Footprinting Methodology
3. Footprinting Tools
4. Footprinting Countermeasures
5. Footprinting Penetration Testing

#### Footprinting Concepts

- Footprinting is process of collecting as much information as possible about a target network
- Footprinting Threats: social engineering, system and network attacks, information leakage, privacy loss, corporate espionage, business loss

#### Footprinting Methodology

1. Footprinting through search engines
  - a. Google, Netcraft (restricted URL's, Determine OS), SHODAN Search Engine,GMAPS, Google Finance, etc
2. Footprinting using advanced Google Hacking Techniques
  - a. Using technique to locate specific strings of text within search results using an advanced operator in the search engine (finding vulnerable targets), Google Operators to locate specific strings of text, GHDB
3. Footprinting through social networking sites
  - a. Fake identifies of co-workers, finding personal info, tracking their groups, etc, Facebook, Twitter, LinkedIn etc
4. Website Footprinting
  - a. Looking at system information from websites, personal information, examining HTML source comments, Web Spiders, archive.org, mirroring sites etc
5. Email Footprinting
  - a. Can get recipient's IP address, Geolocation, Email Received and Read, Read Duration, Proxy Detection, Links, OS and Browser info, Forward Email
6. Competitive Intelligence
  - a. Competitive Intelligence gathering is the process of identifying, gathering, analyzing, and verifying, and using the information about your competitors from sources such as the internet. Monitoring web traffic etc.
  - b. Non-interfering and subtle in nature
  - c. This method is legal
7. WHOIS Footprinting
  - a. WHOIS databases are maintained by regional internet registries and contain PI of domain owners
8. DNS Footprinting
  - a. Attacker can gather DNS information to determine key hosts in the network
9. Network Footprinting
  - a. Network range information assists attackers to create a map of the target network
  - b. Find the range of IP addresses using ARIN whois database search
  - c. Traceroute programs work on the concept of ICMP protocol and use the TTL field in the header of ICMP packets to discover on the path to a target host
10. Footprinting through Social Engineering
  - a. Art in exploiting human behaviour to extract confidential information

- b. Social engineers depend on the fact that people are unaware

#### Footprinting Tools

- a. Maltego, Recon-NG (Web Reconnaissance Framework)

#### Footprinting Countermeasures

- a. Restrict the employees to access social networking sites
- b. Configure web servers to avoid information leakage
- c. Educate employees to use pseudonyms
- d. Limit the amount of information that you are publishing
- e. Use footprinting techniques to discover and remove sensitive information
- f. Use anonymous registration services
- g. Enforce security policies

#### Footprinting penetration testing

- a. Footprinting pen testing is used to determine organization's public available information
- b. Tester attempts to gather as much information as possible from the internet and other publicly accessible sources
- c. Define scope and then use footprint search engines
- d. Report Templates

### **Module 3: Scanning Networks**

- Overview of Network Scanning
- Understanding different techniques to check for live systems
- Understanding different techniques to check for open ports
- Understanding various scanning techniques
- Understanding various IDS evasion techniques
- Understanding banner grabbing
- Overview of vulnerability scanning
- Drawing Network Diagrams
- Using proxies and anonymizers for attack
- Understanding IP spoofing and various detection techniques
- Overview of Scanning Pen Testing

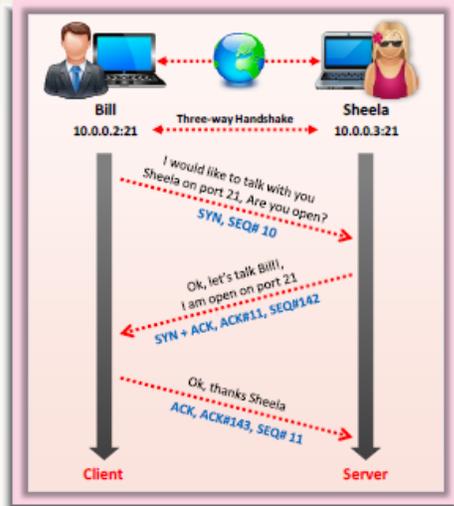
#### Overview of Network Scanning

- Network scanning refers to a set of procedures for identifying hosts, ports, and services in a network
- Network scanning is one of the components of intelligence gathering and attacker uses to create a profile of the target organization
- Types of scanning
  - i. Port scanning (list the open ports and services)
  - ii. Network Scanning (lists IP addresses)
  - iii. Vulnerability Scanning (shows presence of known weaknesses)
- TCP communication Flags (controls transmission of data)
  - 1. URG(urgent): Data contained in packet should be processed immediately
  - 2. PSH(push): Sends all buffered data immediately
  - 3. FIN(Finish): There will be no more transmissions
  - 4. ACK(Acknowledgement): Acknowledges receipts of a packet
  - 5. RST(Reset): Resets a connection
  - 6. SYN(Synchronization): Initiates a connection between hosts

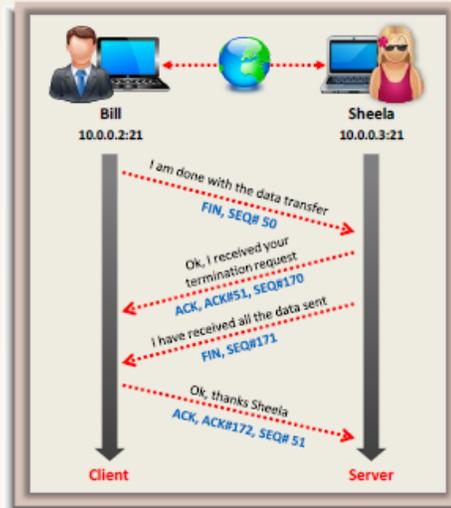
# TCP/IP Communication

CEH  
Certified Ethical Hacker

## TCP Session Establishment (Three-way Handshake)



## TCP Session Termination



## CEH Scanning Methodology

1. Check for live systems
  - a. ICMP Scanning: Ping scans involves ICMP ECHO requests to a host. If the host is live, it will return an ICMP ECHO reply
  - b. Useful for locating active devices and if ICMP is passing through firewall
  - c. Ping sweep is used to determine the live hosts from a range of IP addresses
  - d. Attackers calculate subnet masks using Subnet Mask Calculators
  - e. Attackers then use the Ping Sweep to create an inventory of live systems in the subnet
2. Check for Open Ports
  - a. Simple Service Discovery protocol (SSDP) works in conjunction with UPnP to detect plug and play devices on a networks
  - b. Vulnerabilities in UPnP may allow attackers to launch Buffer overflow or DoS attacks
  - c. Scanning IPv6 networks are computationally less feasible due to larger search space (128 bits)
  - d. Network admins can use Nmap for network inventory, managing service upgrade schedules, and monitoring host or service uptime
  - e. Attacker uses Nmap to extract info such as live hosts on the network, services, type of packet filters/firewalls, operating systems and OS versions
  - f. Hping2/Hping3: command line network scanning and packet crafting tools for the TCP/IP protocol
    - i. It can be used for network security auditing , firewall testing
  - g. TCP connect scan detects when a port is open by completing the three-way handshake
    - i. TCP connect scan establishes a full connection and tears it down sending a RST packet
    - ii. It does not require superuser privileges
  - h. Attackers send TCP probe packets with a TCP flags (FIN,URG,PSH) set or with no flags. No responses means port is open, RST means the port is closed
  - i. In Xmas scan, attackers send a TCP frame to a remote device with FIN, URG, and PUSH flags set
    - i. Won't work against any current version of Microsoft Windows
  - j. Attackers can an ACK probe packet with random sequence number, no responses means the port is filtered (stateful firewall is present) and RST response means the port is not filtered
  - k. A port is considered open if an application is listening on the port
    - i. Most web servers are on port 80 and mail servers on 25
    - ii. One way to determine whether a port is open is to send a "SYN" (session establishment) packet to the port

1. The target machine will then send back a SYN|ACK packet if the port is open, and a RST (reset) packet if the port is closed
    - iii. IDLE Scan
      1. Attack a zombie computer. A zombie machine is one that assigns IPID packets incrementally.
      2. Can retrieve IPID number for IP address spoofing
  - l. UDP Scanning: When UDP port is open ---There is not three-way TCP handshake for UDP scan. System does not respond with a message. The system does not respond with a message when the port is open. When UDP port is closed -- the system responds with ICMP port unreachable message. Spywares, Trojan Horses, and other apps use UDP ports
  - m. There are port scanners for mobile as well
  - n. Port scanning counter measures
    - i. Configure firewall, IDS rules to detect/block probes
    - ii. Run port scanning tools against hosts to determine if firewall properly detects port scanning activity
    - iii. Ensure mechanism used for routing and filtering at the routers and firewalls respectively cannot be bypassed
    - iv. Ensure sure the router, IDS, and firewall firmware are updated
    - v. Use custom rule set to lock down the network and block unwanted ports
    - vi. Filter all ICMP message at the firewalls and routers
    - vii. Perform TCP and UDP scanning
    - viii. Ensure that anti scanning and anti spoofing rules are configured
3. Scanning Beyond IDS
- a. Evasion techniques: fragmented IP packets, spoofing IP address, source routing, connect to proxy servers
  - b. Lower the frequency of packets, split into parts
4. Banner Grabbing
- a. An attacker uses banner grabbing techniques to identify network hosts running versions of applications and OSs with known exploits.
  - b. Banner grabbing or OS fingerprinting is the method to determine the operating system running on a remote target system. There are two types
    - i. Active Banner Grabbing: specifically crafted packets are sent to remote OS and responses are noted, then compared with a database to determine OS.
    - ii. Passive Banner Grabbing: Sniffing the network traffic. Banner grabbing from error message, and banner grabbing from page extensions (stealthy)
  - c. Identifying OS's allow an attack to figure out the vulnerabilities running on a remote target system
  - d. An attacker uses banner grabbing to identify the OS used on the target host and thus determine the system vulnerabilities
  - e. Tools like Netcat reads and writes data across network connections
  - f. Countermeasures for banner grabbing
    - i. Display False Banners
    - ii. Turn off unnecessary services
    - iii. Use ServerMask
  - g. Hiding file extensions from web pages
5. Scan for Vulnerability
- a. Vulnerability scanning identifies vulnerabilities and weaknesses of a system
  - b. Nessus is the vulnerability and configuration assessment product
6. Draw Network Diagrams
- a. A network diagrams helps in analyzing complete network topology.
  - b. Drawing target's network diagram shows logical or physical path to a potential target. Shows network and its architecture to attacker
7. Prepare Proxies
- a. Proxy servers serves as an intermediary for connecting with other computers
    - i. Hides the source IP
    - ii. Chain multiple proxies to avoid detection
  - b. Many hackers use proxies to hide his/her identity so they cannot be traced. Logs record proxy's address rather than the attacker's
  - c. Burp suite includes an intercepting proxy, which lets you inspect and modify traffic between your browser and target app. Popular.
  - d. Anonymizers removes all identifying information from a user's computer while user surfs internet
  - e. Tails is a live operating system, that user can start on any computer from a DVD, USB stick, or SD card
  - f. Can use HPING2 to IPspoof
  - g. IP spoofing counter measures

- i. Encrypt all network traffic
  - ii. Use multiple firewalls
  - iii. Do not rely on IP-based authentication
  - iv. Use random initial sequence number
  - v. Ingress filtering: use routers and firewalls at network perimeter to filter incoming packets that appear to come from an internal IP address
  - vi. Egress filtering: Filter all outgoing packets with an invalid local IP address as source address
8. Scanning Pen Testing
  - a. Pen testing a network determines the network's security posture by identifying live systems, discovering open ports, associating services and grabbing system banners to simulate a network hacking attempt
  - b. Here's how to conduct a pen-test of a target network
    - i. Host Discovery: detect live hosts on the target network. It is difficult to detect live hosts behind a firewall (Nmap, Angry IP scanner, colasoft)
    - ii. Port Scanning: Check for open ports (Nmap, Netscan)
    - iii. Banner Grabbing or OS fingerprinting: determine the OS running on the target host
    - iv. Scan the network for vulnerabilities (nessus)
    - v. Draw Network Diagrams that help you understand the logical connection
    - vi. Prepare Proxies: Hides yourself from detection
    - vii. Document all findings

#### **Module 4: Enumeration**

##### Module Objectives

- Understanding Enumeration Concepts
- Understanding different techniques for NetBIOS enumeration
- Understanding Different Techniques for SNMP enumeration
- Understanding different techniques for LDAP enumeration
- Understanding different techniques for NTP enumeration
- Understanding different techniques for SMTP and DNS Enumeration
- Enumeration countermeasures
- Overview of enumeration pen testing

##### Enumeration Concepts

- In the enumeration phase, attacker creates active connections to system and performs directed queries to gain more information. Uses this information to identify system attack points and perform password attacks
  - Conducted in an intranet environment
- Techniques for Enumeration
  - Extract user names using email IDs
  - Extract user names using SNMP
  - Extract user groups from windows
  - Extract information using the default passwords
  - Brute force active directions
  - Extract information using DNS Zone Transfer
- Popular Ports to Enumerate
  - TCP/UDP 53 - DNS Zone Transfer
  - TCP/UDP 135 - Microsoft EPC Endpoint Manager
  - UDP 137 - NetBIOS Name Service (NBNS)
  - TCP 139 - SMB over NetBIOS
  - TCP/UDP 445 - SMB over TCP (direct host)
  - UDP 161 - Simple Network Management Protocol (SNMP)
  - TCP/UDP 389 - Lightweight Directory Access Protocol (LDAP)
  - TCP/UDP 3268 - Global Catalog Service
  - TCP 25 - Simple Mail Transfer Protocol (SMTP)
  - TCP/UDP 162 - SNMP Trap

##### NetBIOS Enumeration

- NetBIOS name is a unique 16 ASCII string used to identify the network devices (15 of it are device name, 16 is reserved for service or name record type)
- Nbtstat utility displays NetBIOS over TCP/IP protocol statistics, NetBIOS name tables/cache
- Net View utility is used to obtain a list of all the shared resources of remote hosts or workgroup

### SNMP Enumeration (simple network Management protocol enumeration)

- SNMP enumeration is a process of enumerating user accounts and devices on a target system using SNMP
- SNMP contains a manager and agent. Agents are embedded on every network, manager installed on a separate computer
- SNMP has two passwords
  - Attacker uses default community strings to extract info
  - Uses it to extract information about network resources such as hosts, routers, devices, shares
- Management Information Base (MIB)
  - MIB is a virtual database containing formal description of all the network objects managed using SNMP

### LDAP Enumeration

- LDAP is an internet protocol for accessing distributed directory services
- Attacker queries LDAP service to gather information such as valid user names, addresses, departmental details, etc

### NTP Enumeration

- Network Time Protocol (NTP) is designed to synchronize clocks of networked computers
- Uses UDP port 123
- Can use it to find important information on a network
- Can use Nmap, Wireshark

### SMTP and DNS Enumeration

- SMTP has 3 built-in commands
  - VRFY - Validates users
  - EXPN - Tells actual delivery addresses of aliases and mailing lists
  - RCPT TO - Defines the recipients of the message
- SMTP servers respond differently to these commands
- Attackers can directly interact with SMTP via the telnet prompt and collect a list of valid users on the SMTP Server

### Enumeration Countermeasures

- SNMP countermeasures
  - Remove SNMP agent or turn off the SNMP service (block 161)
  - Change default community string name
  - Upgrade to SNMPv3, which encrypts passwords/messages
  - Implement additional security option called "additional restrictions for anonymous connections"
  - Ensure that the access to null session pipes, null session shares, and IPsec filtering are restricted
- DNS countermeasures
  - Disable DNS zone transfers to the untrusted hosts
  - Make sure private hosts and their IP addresses are not published into DNS zone files of public DNS server
  - Use premium DNS registration services to hide sensitive information
  - Use standard network admin contacts for dns registrations in order to avoid social engineering attacks
- SMTP countermeasures
  - Ignore email messages to unknown recipients
  - Disable open relay features
  - Do not include sensitive mail server and local host information in mail responses
- LDAP countermeasures
  - Restrict access to active directory by using software such as Citrix
  - Enable account lockout
  - Use SSL technology for LDAP traffic
- Enumeration Pen Testing
  - Used to identify valid user accounts or poorly protected resource shares
  - Information can be users and groups, network resources
  - Used in combination with data collected in reconnaissance phase
  - Steps in Enumeration Pen Testing
    - Find the network range
    - Calculate the subnet mask
    - Undergo host discovery

- Perform port scanning
  - Perform NetBIOS enumeration
  - Perform SNMP enumeration
  - Perform LDAP enumeration
  - Perform NTP enumeration
  - Perform SMTP enumeration
  - Perform DNS enumeration
  - Document all findings
- Remember OneSixtyOne application, used for scanning SNMP port 161

## **Module 5: System Hacking**

### Module Objectives

- Overview of CEH Hacking Methodology
- Understanding Techniques to gain access to the system
- Understanding privilege escalation techniques
- Understanding Techniques to create and maintain remote access to the system
- Overview of different types of rootkits
- Overview of steganography and steganalysis techniques
- Understanding Techniques to hide the evidence on compromise
- Overview of system hacking penetration testing

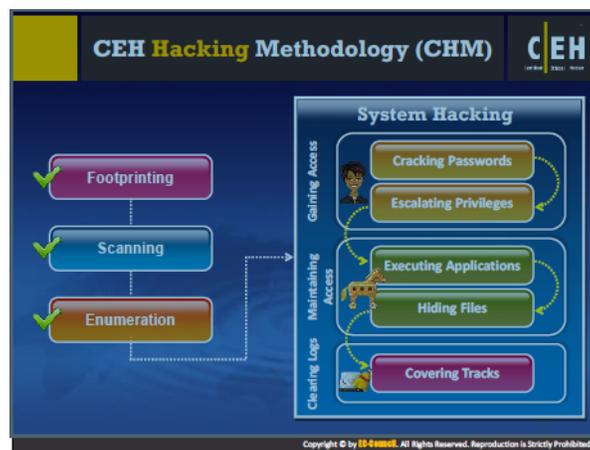
System hacking is one of the most important and sometimes ultimate goal of an attacker.

Information at hand before system hacking stage

1. Footprinting: IP range, Namespace, Employees
2. Scanning module: target assessment, identified systems, identified services
3. Enumeration: Intrusive probing, user lists, security flaws

System Hacking Goals:

1. Gaining Access - password cracking, social engineering
2. Escalating Privileges (get other passwords) - exploiting known system vulnerabilities
3. Executing Applications (backdoors) - Trojans, Spywares, Backdoors, Keyloggers
4. Hiding Files - Rootkits, Steganography
5. Covering Tracks - Clearing logs



### Cracking Passwords

- Password cracking techniques are used to recover passwords from computer systems
- Attackers use password cracking techniques to gain unauthorized access
- Most cracks are successful due to guessable passwords
- Types of password attacks
  - Non-electronic attacks: Attacker does not need technical knowledge to crack password (looking at keyboard/screen, convincing people, trash bins etc)

- Active Online Attacks: Attacker performs cracking by directly communicating with the victim machine (dictionary, brute force, rule based - some info known)
  - Passive Online Attacks: Performs cracking without communicating with party
  - Offline Attack: attacker copies password file and tried to crack it
- Default passwords are set by the manufacturer
- Trojans can collect usernames and passwords and send to attacker, run in background
- Can use USB drive for a physical approach
- Hash Injection Attack: attacker injects compromised hash into local session then use it to validate network resource. Finds and extracts a logged on domain admin account hash
- Passive Online Attack: Wire Sniffing
  - Packet Sniffer tools on LAN
  - Capture data may include sensitive information such as passwords
  - Sniffed credentials are used to gain unauthorized access
- Rainbow table attack
  - Precomputed table which contains word lists like dictionary files, brute force lists, and their hash values
  - Compare the hashes
  - Easy to recover passwords by comparing captured password hashes to precomputed tables
- Offline Attack: Distributed Network Attack (DNA)
  - A DNA technique is used for recovering passwords from hashes or password protected files using the unused processing power of machines across the network to decrypt passwords
- Microsoft Authentication
  - Windows stores passwords in the Security Accounts Manager (SAM) Database, or in the Active Directory database in domains. They are hashed.
  - NTLM Authentication
    - NTLM authentication protocol types
    - LM authentication protocol
    - These protocols stores user's password in the SAM database using different hashing methods
  - Kerberos Authentication
    - Microsoft has upgraded its default authentication protocol
  - Password Salting
    - Random strings of characters are added to the password before calculating their hashes
      - Advantage: salting makes it more difficult to reverse hashes
- Use password crackers like L0phtCrack, Cain&Abel, RainbowCrack
- Enable SYSKEY with strong password to encrypt and protect the SAM database

### Escalating Privileges

- An attacker can gain access to the network using a non-admin user account, next step is to gain admin privileges
- Privilege Escalation Using DLL Hijacking
  - If attackers place a malicious DLL in the application directory, it will be executed in place of the real DLL
- Resetting passwords using command prompt
  - An admin can reset passwords while an administrator
- Countermeasures: restrict interactive login privileges, use least privilege policy, implement multi-factor, run services as unprivileged accounts, patch systems regularly, use encryption technique, reduce amount of code, perform debugging

### Executing Applications

- Attackers execute malicious programs remotely in the victim's machine to gather information
  - Backdoors
  - Crackers
  - Keyloggers
  - Spyware
- Software like RemoteExec can remotely install software, execute programs/scripts
- There are hardware and software keystroke loggers (USB vs App)
- Spyware
  - Records user's interaction
  - Hides its process
  - Hidden component of freeware program
  - Gather info about victim or organization
- GPS spyware also exists
- Countermeasures for Keyloggers

- Pop-up blocker
- anti-spyware/virus
- Firewall software
- Anti-keylogging software
- Recognize phishing emails and delete
- Choose new passwords for different online accounts
- Avoid opening junk emails
- There are Anti-keyloggers out there
- Rootkits are programs that hide their presence and an attacker's malicious activities, granting them full access to the server or host at the time or in future
  - Typical Rootkit has backdoor programs, DDos programs, packet sniffers, log-wiping utilities, IRC bots, etc
- 6 Types of Rootkits
  - Hypervisor Level Rootkit: Acts as hypervisor and modifies boot sequence of the computer to load the host OS as a virtual machine.
  - Boot Loader level rootkit: replaces original boot loader with one controlled by attacker
  - Hardware/Firmware Rootkit: Hides in hardware devices or platform firmware which is not inspected for code integrity
  - Application level rootkit: replaces regular application binaries with fake trojan, or modifies the behavior of existing applications
  - Kernel Level Rootkit: Adds malicious code or replaces original OS kernel and device driver codes
  - Library Level Rootkits: Replaces original system calls with fake ones to hide information about attacker
- Detecting Rootkits
  - Integrity-Based detection: compares a snapshot of the filesystem, boot records, or memory
  - Signature-based technology: compares characteristics of all system processes and executable files with a database of known rootkit fingerprints
  - Heuristic/Behavior based detection: any deviations in the systems normal activity
  - Runtime Execution path profiling: compares runtime execution paths of all system processes before and after rootkit infection
  - Cross View-Based detection: enumerates key elements in the computer system such as system files, processes, and registry keys and compares them to an algorithm to generate a similar data set that does not rely on common APIs
- NTFS Data Stream
  - NTFS alternate data stream (ADS) is a windows hidden stream which contains metadata for the file such as attributes, word count, author name, access and modification time of files
  - Using NTFS stream, an attacker can almost completely hide files within the system.
  - You can hide a file side another file (trojan in a readme.txt)
  - Countermeasures: use a third party file integrity checker
- Steganography
  - Steganography is a technique of hiding a secret message within an ordinary message and extracting it at the destination
  - Utilizing a graphic image as a cover is the most popular method to conceal the data in files
  - Attackers can use steganography to hide messages such as list of compromised servers, source code for the hacking tools, plans for future attacks, etc
  - Technical Steganography: invisible ink/microdots, physical methods to hide
  - Linguistic Steganography: Type that hides the message in another file
    - Semagrams: use of symbols to hide information
  - Least Significant bit insertion: The rightmost bit of a pixel is called the LSB
  - Masking and Filtering: Making technique hides data similar to watermarks on actual paper. Can be detection with simple statistical analysis. Mostly in grayscale images.
  - Algorithms and Transformation
    - Hide data in mathematical functions used in compression algorithms
    - Data is embedded by changing the coefficients of a transform of an image
  - Audio steganography - information in hidden frequency
- Steganalysis
  - Art of discovering and rendering covert messages using steganography. It attacks steganography efforts

### Covering Tracks

- Techniques used for covering tracks

- Disable Auditing: disabling audit features of target system
- Clearing logs: attacker clears/delete the system log entries for their activities
- Manipulating logs: Manipulates logs in a way they won't be caught in legal actions
- If system is exploited with metasploit, attacker uses meterpreter shell to wipe logs

#### Penetration Testing

- Password Cracking
- Privilege Escalation
- Execute Applications
- Hiding Files
- Covering Tracks

#### **Module 6: Malware Threats**

##### Module Objectives

- Introduction to Malware and Malware propagation techniques
- Overview of Trojans, their types, how to infect systems
- Overview of Viruses, their types, and how they infect files
- Introduction to the Computer Worm
- Understanding the Malware Analysis process
- Understanding Different techniques to detect malware
- Malware countermeasures
- Overview of Malware penetration testing

#### Introduction to Malware

- Malware is a malicious software that damages or disables computer systems and give limited control or full control of the systems to the attacker for the purpose of theft or fraud
- Examples of Malware: Trojan Horse, Backdoor, Rootkit, Ransomware, Adware, Virus, Worms, Spyware, Botnet, Crypter
- Common techniques attackers use to distribute malware: Blackhat SEO, Social Engineer Clickjacking, Spear Phishing sites, Malvertising, Compromised legitimate websites, Drive by downloads on browser vulnerabilities

#### Trojan Concepts

- A trojan is a program which the malicious or harmful code is contained inside an apparently harmless program or in such a way it can get control and cause damage, such as ruining a file allocation table on your hard disk
- Trojans get activated upon user's certain predefined actions, and conduct abnormal activities on the system
- When a trojan is installed, they attacker can basically do anything to your computer

Common Ports used by Trojans				CEH Certified Ethical Hacker	
Port	Trojan	Port	Trojan	Port	Trojan
2	Death	1492	FTP99CMP	5559	Robo-Hack
30	Senna Spy	1800	Shiva-Barba	6870-71	DeepThroat
21	Blade Runner, Doly Trojan, Fore, Invisible FTP, WebEx, WinCrash	1807	SpySender	6969	GateCrasher, Priority
22	Shaft	1981	Shockwave	7000	Remote Grab
23	Tiny Telnet Server	1999	BackDoor 1.00-1.03	7300-08	NetMonitor
25	Antigen, Email Password Sender, Terminator, WinPC, WinDsp	2001	Trojan Cow	7789	ICKiller
31	Hackers Paradise	2023	Ripper	8787	BackOffice 2000
80	Executor	2115	Bugs	9872-9875	Portal of Doom
421	TCP Wrappers Trojan	2160	The Invoker	9989	INI-Killer
456	Hackers Paradise	2155	Illusion Moler, Nirvana	10607	Corn 1.0.0
555	INI-Killer, Phase Zero, Stealth Spy	3129	Masters Paradise	11000	Senna Spy
666	Satanz Backdoor	3150	The Invoker	11223	Progenc Trojan
1005	Silencer, WebEx	4092	WinCrash		
1011	Doly Trojan	4567	File Nail 1	12223	Hack '99 KeyLogger
1095-98	BAT	4590	ICQ Trojan	12345-68	GabanBus, NetBus
1170	Psyber Stream Server, Voice	5000	Bubbel	12361, 12362	Whack-a-mole
1234	Ultors Trojan	5001	Sockets de Troie	16989	Priority
1240	SubSeven 1.0 - 1.8	5121	Firehotcker	20001	Millennium
1245	VooDoo Doll	5400-01	Blade Runner	20034	NetBus 2.0, Beta-NetBus 2.01
				21546	Griffind 1.0, Beta-1.35
				22222	Proxiak
				23456	Evil FTP, Ugly FTP
				30274	Delta
				30300-02	NetSphere 1.27a
				31327-38	Back Office, DeepBO
				31330	NetSpy DK
				31666	BOWhack
				31333	Proxiak
				34524	BigGluck, TN
				40412	The Spy
				40421-28	Masters Paradise
				47262	Delta
				50506	Sockets de Troie
				50796	Fore
				53001	Remote Windows Shutdown
				54321	SchoolBus_6.0-1.11
				61666	Telecommando
				65000	Devil

Copyright © by SP-000008. All Rights Reserved. Reproduction is Strictly Prohibited.

- How to infect systems using a trojan
  - Create a new trojan packet using a trojan horse construction kit
  - Create a dropper, which is part in a trojanized packet that installs the malicious code on the target system
- A wrapper binds a trojan executable with an innocent looking .EXE application such as games or office applications. When an EXE is executed, it first installs the trojan in the background.
- Attackers use crypters to hide viruses, spyware, keyloggers to make them undetectable by antivirus
- Attackers can deploy a trojan by creating a malicious link/email attachments
- Exploit kit: Platform to deliver exploits and payloads such as trojans, backdoors, bots, buffer overflow scripts, etc
- Evading Anti-Virus Techniques:
  - Break the trojan file into multiple pieces and zip them as a single file
  - ALWAYS write your own Trojan, and embed it into an application
  - Change the Trojans Syntax
    - Convert EXE to VB script
  - Change the content of the Trojan using Hex Editor and also change the checksum and encrypt the file
  - Never use trojans downloaded from the web (antivirus can detect these easily)

## Common Ports used by Trojans



Port	Trojan	Port	Trojan	Port	Trojan	Port	Trojan
1	Death	1492	FTP99COMP	5569	Robo-Hack	21544	Girlfriend 1.0, Beta-1.35
20	Senna Spy	1600	Shivka-Burka	6670-71	DeepThroat	22222	Prosiak
21	Blade Runner, Doly Trojan, Fork, Invisible FTP, WebEx, WinCrash	1807	SpySender	6969	GateCrasher, Priority	23456	Evil FTP, Ugly FTP
22	Shut	1961	Shockwave	7000	Remote Grab	26274	Delta
23	Tiny Telnet Server	1999	BackDoor 1.00-1.03	7300-08	NetMonitor	30300-02	NetSphere 1.27a
25	Antigen, Email Password Sender, Terminator, WinPC, WinSpy	2001	Trojan Cow	7789	IOKiller	31337-38	Back Office, DeepBO
31	Hackers Paradise	2023	Ripper	8787	BackOffice 2000	31338	NetSpy DK
80	Executer	2113	Bugs	9872-9875	Portal of Doom	31666	BOWhack
421	TCP Wrappers Trojan	2140	The Inveisor	9989	INI-Killer	33333	Prosiak
456	Hackers Paradise	2155	Illusion Mailer, Nirvana	10407	Come 1.0.9	34324	BigGluck, TN
555	INI-Killer, Phase Zero, Stealth Spy	3129	Masters Paradise	11000	Senna Spy	40412	The Spy
666	Satanz Backdoor	3150	The Inveisor	11223	Progenitrojan	40421-26	Masters Paradise
1001	Silencer, WebEx	4092	WinCrash			47262	Delta
1011	Doly Trojan	4567	File Nail 1	12223	Hack '99 KeyLogger	50505	Sockets de Troie
1095-98	RAT	4590	IOCI Trojan	12345-46	GabenBus, NetBus	50786	Fone
1170	Psyber Stream Server, Voice	5000	Bubbel	12361, 12362	Whack-a-mole	53001	Remote Windows Shutdown
1234	Ultors Trojan	5001	Sockets de Troie	16969	Priority	54321	SchoolBus.69-1.11
1243	SubSeven 1.0 - 1.8	5321	Firehotcker	20001	Millennium	61466	Telecommando
1245	VooDoo Doll	5400-02	Blade Runner	20094	NetBus 2.0, Beta-NetBus 2.01	65000	Devil

Copyright © by **ES-COMM**. All Rights Reserved. Reproduction is Strictly Prohibited.

- Command shell trojans give remote control of a command shell
- Trojan server is installed on the victim's machine, which opens a port for attacker to connect.
- Defacement Trojans: Can destroy or change entire content present in a database. Much more dangerous when attackers target websites
- Botnet Trojans: infect a large number of computers to create a network of bots(chewbacca)
- Proxy Server Trojans: Converts user's computer into proxy servers, thus making them accessible to specific attackers.
- VNC Trojan: VNC trojan starts a VNC server daemon in the infected systems. Attacker can connect to the victim using any VNC viewer
- HTTP/HTTPS Trojans: bypass firewall, spawn a child program and child program appears to be a user to the firewall
- ICMP Tunneling
  - Covert channels are methods in which an attacker can hide the data in a protocol that is undetectable
  - They rely on techniques called tunneling, which allow on protocol be carried over to another protocol . very stealthy
- Remote Access Trojans: provide attackers with full control over the victim's system
- E Banking Trojans - intercept a victim's account information before it is encrypted
  - Steals victim's data such as credit card information
- Notification Trojans: Sends the location of the victim's IP address to attacker
- Whenever victim's computer connected to the internet, the attacker receives the notification

### Viruses and Worm Concepts

- Virus: A self replicating program that produces its own copy by attacking itself to another program, computer boot sector or document
  - Transmitted through downloads, infected flash drives, email attachments
- Stages of Virus Life
  - Design: creating the virus
  - Replication: Replicating the virus on target system
  - Launch: launching/running the virus (.exe file)
  - Detection: Target system identifies virus
  - Incorporation : Anti-virus softwares update
  - Elimination: users install anti-virus update to eliminate virus
- Indications of a virus attack: abnormal activities (slow, anti virus alerts, folders missing, etc)
- There are many Fake Anti-Viruses that are actually viruses
- Ransomware restrict computer files until a sum is paid
- Boot Sector Viruses: moves MBR to another location on hard disk

- File Virus: Infects files which are executed or interpreted on the system such as (COM, EXE, SYL, OVL, OBJ, MNU and BAT files)
- Multipartite Virus: Infect the system boot sector and the executable files at the same time (hybrid, top 2 combined))
- Macro Viruses: Infect files created by Microsoft Word or Excel. Most of these are written in macro language Visual Basic for Applications (VBA)
  - Infect Templates, convert infected documents into template files
- Cluster Viruses: These modify directory table contents so that it points users to system processes to the virus code instead of the actual program
  - There is only one copy of the virus on the disk infecting all the programs in the computer system
  - Will launch itself first when any program on the computer system is started
- Stealth/Tunneling Virus: This virus evades anti-virus software by intercepting its requests to the operating system
  - Virus can return an uninfected version of the file to the anti-virus software, so it appears as if the file is “clean”
- Encryption Viruses: uses simple encryption to encipher the code. Virus is encrypted with different key for each infected file. AV Scanner cannot directly detect these types fo viruses using signature detection methods
- Polymorphic Code: Code that mutates while keeping the original algorithm intact. Well written polymorphic code has no parts that stay the same on each infection
- Metamorphic Viruses: Rewrite themselves completely each they are to infect new executable
  - Can Reprogram itself by translating its own code into a temporary representation and then back to the normal code again
- File Overwriting or Cavity Virus: Overwrites a part of the host file that is constant (usually nulls), without increasing the length of the file and preserving its functionality
- Sparse Infector Viruses: Infects only occasionally, or only files whose length falls within a narrow range. By infection less often, they try to minimize the probability of being discovered
- Companion/camouflage Viruses: Creates a companion file for each executable file the viruses infects. Therefor, a companion virus may save itself as notepad.com and every time the user executes notepad.exe (good program), the computer will load the virus notepad.com and infect
- Shell Viruses: Virus code forms a shell around the target host program’s code, making itself the original program and host code as its sub-routine. Almost all boot program are shell viruses
- File Extension Viruses: changes the extensions of files. Ex. .TXT is a safe file. Virus file is BAD.TXT.VBS but will only show up as bad.txt . When opened a script executes.
- Add-on Virus: adds on their code to the host code without making any changes to the latter or relocate the host code to insert their own code at the beginning
- Intrusive Viruses: Overwrite the host code partly or completely with the viral code
- Transient/Direct Action Virus: Transfers all the controls of the host code to where it resides in the memory. Virus runs when the host code is run and terminates itself or exits memory as soon as host code execution ends
- Terminate and Stay Resident Virus: remains permanently in the memory during entire work session even after the host’s program is executed and terminated. Removed only by rebooting system.
- Computer Worms: Malicious programs that replicate, execute, and spread across network connections independently without human interaction. Most are created only to replicate and spread, but some have payloads
  - Attackers use payloads to install backdoors which turns them into a zombie for a botnet
  - A worm is a special type of malware that can replicate itself and use memory, but cannot attach itself to other programs
  - A worm takes advantage of file or information transport features on a computer and spreads through the infected network

Virus	Worm
Virus infects a system by inserting itself into a file or executable program	Worm infects a system by exploiting a vulnerability in an OS or application by replicating itself
It might delete or alter content in files, or change the location of files in the system	Typically, a worm does not modify any stored programs. It only exploits the CPU and memory
It alters the way a computer system operates, without the knowledge or consent of a user	It consumes network bandwidth, system memory, etc., excessively overloading servers and computer systems
A virus cannot be spread to other computers unless an infected file is replicated and actually sent to the other computer	A worm, after being installed in a system, can replicate itself and spread by using IRC, Outlook, or other applicable mailing programs
A virus is spread at a uniform speed, as programmed	A worm spreads more rapidly than a virus.
Viruses are hard to remove from infected machines	As compared with a virus, a worm can be easily removed from a system

- Sheep Dipping refers to the analysis of suspect files, incoming messages, for malware
  - A sheep dip computer is installed with port monitors, file monitors, network monitors and antivirus software and connects to a network only under strictly controlled conditions
- Anti-Virus Sensor Systems: Collection of computer software that detects and analyzes malicious code threats
- Malware Analysis Procedure:
  - Perform static analysis when the malware is inactive
  - Collect info of string values found in binary with tools
  - Setup network connection and check there are no errors
  - Run the virus and monitor the process actions and system information with help of process monitor/explorer
  - Record network traffic information using monitoring tools (TCP view, netResident)
  - Determine the files added, processes spawn, and changes to registry with tools
  - Collect Service requests and DNS tables information, attempts for incoming and outgoing connections using tools

### Malware Detection

- Trojans open unused ports in victims machine to connect back to Trojan handlers
- Look for connection established to unknown or suspicious IP addresses
  - You can use a port monitoring tool
- Scanning for Suspicious Processes
  - Trojans camouflage themselves as genuine Windows services
  - Some trojans use Portable Executable to inject into various processes
  - Processes are visible but may look like a legitimate processes and helps bypass desktop firewalls
  - Trojans can also use rootkit methods to hide their processes
  - Use process monitoring tools to detect hidden trojans and backdoors
- Trojans are installed along with device drivers downloaded from untrusted sources
  - Scan suspicious drivers and verify they are genuine and downloaded from publishers original site
- Trojans normally modify system's files and folders. Use these tools to detect changes
  - SIGVERIF: checks integrity of critical files digitally signed by microsoft
  - FCIV - Computes MD5 or SHA-1 cryptographic hashes for files
  - TRIPWIRE: system integrity verifier that scan and reports critical system file for changes
- Scanning for suspicious network activities
  - Trojans connect back to handlers and send confidential info to attackers
  - Use network scanners
- Virus Detection Methods
  - Anti-virus executes the malicious code to simulate. Effective for dealing with encrypted and polymorphic viruses
  - Heuristic Analysis: Can be static or dynamic. In static, anti-virus analyzes the file format and code structure to determine is code is viral. In dynamic, the AV performs a code emulation

### Counter-Measures

- Trojan Countermeasures
  - Avoid opening email attachments from unknown senders
  - Block unnecessary ports
  - Avoid accepting programs transferred by instant messaging
  - Hard weak default configs and unused functionality including protocols/services
  - Monitor internal network traffic for odd ports
  - Avoid downloading and executing apps from untrusted sources
  - Install security updates
  - Scan CD's and DVD's w/ antivirus software
  - Restrict permissions within desktop environment
  - Manage local workstation file integrity
  - Run Host-Based Antivirus
- Backdoor Countermeasures
  - Anti-viruses
  - Educate users not to download from untrusted sites

### Anti-Malware Software

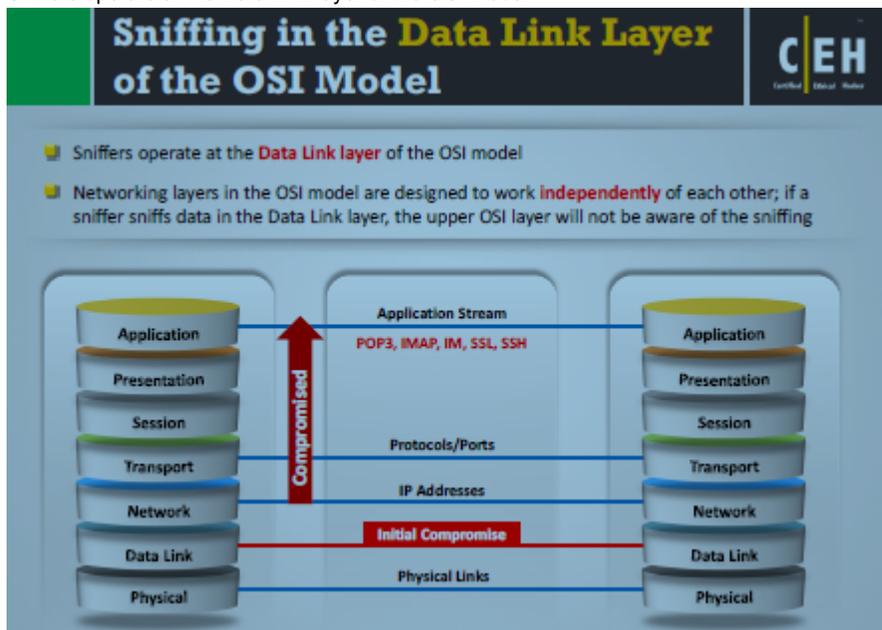
Norton, McAfee, Nessus etc.

## Module 7: Sniffing

Objectives: Overview of sniffing concepts, understanding MAC attacks, Understanding DHCP attacks, understanding ARP poisoning, Understanding MAC spoofing attacks, Understanding DNS poisoning, Sniffing tools, Sniffing countermeasures, Understanding various techniques to detect sniffing, overview of sniffing pen testing

### Sniffing Concepts

- Sniffing is a process of monitoring and capturing all data packets passing through a given network using sniffing tools (form of wire tap)
  - Many enterprises switch ports are open
  - Anyone in same physical location can plug into network with ethernet
- How a sniffer works
  - Sniffer turns on the NIC of a system to the promiscuous mode that it listens to all the data transmitted on its segment
- Each computer has a MAC address and an IP address
- Passive sniffing means through a hub (involves sending no packets), on a hub traffic is sent to all ports
  - Most modern networks use switches
- Active Sniffing: Searches for traffic on a switched LAN by actively injecting traffic into the LAN. Involves injecting address resolution packets (ARP) into the network
- Protocols vulnerable to sniffing:
  - HTTP, Telnet and Rlogin, POP, IMAP, SMTP and NNTP
- Sniffers operate at the Data Link layer of the OSI model



- Hardware Protocol Analyzer: equipment that captures signals without altering the traffic in a cable segment
  - Can be used to monitor traffic. Allows attacker to see individual data bytes
- Span Port: A port which is configured to receive a copy of every packet that passing through a switch
- Wiretapping: Process of monitoring telephone and internet convo's by third party
  - Via connecting a listening device (hardware or software) to the circuit
  - Active Wiretapping: Monitors, records, and injects something into the communication or traffic
  - Passive Wiretapping: It only monitors and records the traffic and gain knowledge of the data it contains
  - Lawful interception: legally intercepting data communication

### MAC Attacks

- Each switch has a fixed size dynamic content addressable memory (CAM table)

- CAM table stores information such as MAC address available on physical ports
- If CAM table is flooded with more MAC address it can hold, then the switch turns into a HUB
  - Attackers exploit this
- Switch Port Stealing: uses mac flooding to sniff the packets
- How to defend against MAC attacks: use a port security to restrict inbound traffic from only a selected set of mac addresses and limit MAC flooding attacks

### DHCP Attacks

- DHCP servers maintain TCP/IP configuration information (provides leases)
- DHCP starvation attack: attacker broadcasts forged DHCP requests and tries to lease all DHCP addresses available in the DHCP scope
  - As a result, legitimate user is unable to obtain or renew an IP address
- Rogue DHCP: rogue DHCP server in network and responds to DHCP requests with bogus IP addresses
- How to defend against DHCP starvation and Rogue Server Attack: Enable port security for DHCP starvation, and enable DHCP snooping that allows switch to accept DHCP transactions from a trusted port

### ARP Poisoning

- Address Resolution Protocol (ARP) is a stateless protocol used for resolving IP address to machine (MAC) addresses
- All network devices broadcasts ARP queries in the network to find machine's MAC address
- When one machine needs to communicate with another, it looks up to the ARP table. If it's not there, the ARP\_REQUEST is broadcasted over the network
- ARP packets can be forged
- ARP spoofing involves constructing large number of forged ARP requests
- Switch is set in 'forwarding mode' after the ARP table is flooded with spoofed ARP replies
- Attackers flood a target computer's ARP cache with forged entries, which is also known as poisoning
- ARP spoofing is a method of attacking an ethernet LAN
- Using Fake ARP messages, an attacker can divert all communications between two machines so that all traffic is exchanged via his/her PC
- ARP Tools: Cain & Abel, WinArpAttacker
- How to defend: Implement dynamic ARP inspection, DHCP Snooping, XArp spoofing detection

### Spoofing

- Attacker can sniff network for MAC addresses, then spoof them to receive all the traffic destined for the user. Allows attacker to gain access to the network
- IRDP spoofing: ICMP Router discovery protocol allows host to discover the IP address of active routers.
  - Attacker sends spoofed IRDP router advertisement message to the host on the subnet, causing it to change its default router
- How to defend: DHCP snooping, Dynamic ARP inspection, IP source guard

### DNS Poisoning

- DNS poisoning is a technique that tricks a DNS server into believing that it has received authentication when it really has not
  - Results in substitution of a false IP address
  - Attacker can create fake DNS entries
- Intranet DNS spoofing: must be connected to LAN and able to sniff. Works well against switches with ARP poisoning the router.
  - Intranet DNS spoofing attacker infects machine with trojan and changes DNS IP to that of attacker
- Proxy Server DNS poisoning: attacker sends a trojan to machine that changes hosts proxy server settings in internet explorer to that of the attacker's and redirect to fake website
- DNS Cache Poisoning: Refers to altering or adding forged DNS records into DNS resolver cache so that a DNS query is redirected to a malicious site
- How to defend: resolve all DNS queries to local DNS server, Block DNS requests from going to external servers, configure firewall to restrict external DNS lookup, Implement IDS and deploy correct, Implement DNSSEC

### Sniffing Tools

**Display Filters in Wireshark**

Display filters are used to **change the view of packets** in the captured files

- 1 Display Filtering by Protocol**  
Example: Type the protocol in the filter box; arp, http, tcp, udp, dns, ip
- 2 Monitoring the Specific Ports**  

```
tcp.port==23
ip.addr==192.168.1.100 machine
ip.addr==192.168.1.100 && tcp.port==23
```
- 3 Filtering by Multiple IP Addresses**  

```
ip.addr == 10.0.0.4 or
ip.addr == 10.0.0.5
```
- 4 Filtering by IP Address**  

```
ip.addr == 10.0.0.4
```
- 5 Other Filters**  

```
ip.dst == 10.0.1.50 && frame.pkt_len > 400
ip.addr == 10.0.1.12 && icmp && frame.number > 15 && frame.number < 30
ip.src==205.153.63.30 or ip.dst==205.153.63.30
```

#### Counter-Measures

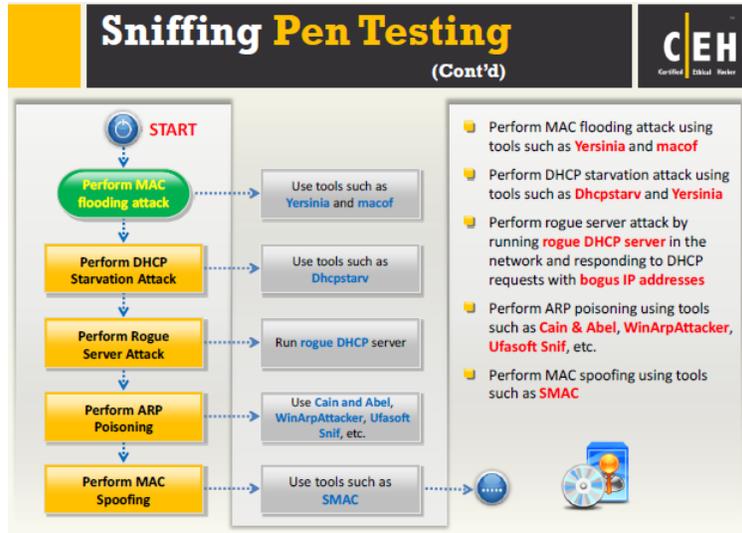
- Restrict physical access
- Use encryption
- Permanent add MAC address to the gateway to the ARP cache
- Use static IP addresses
- Turn off network ID broadcasts
- Use IPV6
- Use HTTPS instead of HTTP
- Use switch than Hub
- Use SFTP instead of FTP

#### Sniffing Detection Techniques

- Runs IDS and notice if mac address of certain machines have changed
- Check which machines are running in the promiscuous mode
  - Promiscuous mode allows a network device to intercept and read each network packet
- Only a machine in promiscuous mode cache the ARP information
  - A machine in promiscuous mode replies to the ping message as it has correct information about the host sending a ping request

#### Sniffing Pen Testing

- Sniffing pen test is used to check if the data transmission from an org is secure from sniffing and interception attacks



## Module 8: Social Engineering

Objectives: overview of social engineering concepts, understanding various social engineering techniques, understanding insider threats, understanding impersonation on social networking sites, understanding identity theft, social engineering countermeasures, identify theft countermeasures, overview of social engineering pen testing

### Social Engineering Concepts

- Social engineering is the art of convincing people to reveal confidential information
  - Depends on the fact people are unaware of their valuable info and careless about protecting it

### Social Engineering Techniques

- Human-based social engineering, Computer-Based social engineering, Mobile-based social engineering
- Human Based Social Engineering
  - Reverse social engineering (attacker presents as authority)
  - Piggybacking ("I forgot my ID badge, please help)
  - Tailgating (walking directly behind someone for entrance)
- Computer Based Social Engineering
  - Hoax Letters, free gifts, etc
- Mobile-based social engineering
  - Repackaging legitimate apps
  - Fake security applications
- Insider attack
  - Disgruntled employee
  - Prevention: separation and rotation of duties, least privilege, controlled access, logging and auditing, legal policies, archive critical data

### Impersonation on Social Networking Sites

- Social engineering on facebook, twitter, linkedin etc

### Identify Theft

- When someone steals your PI

### Social Engineering countermeasures

- Periodic password change, good policies, etc.

## Module 9: Denial of Service

Objectives: Overview of DOS attacks and DDoS attacks, understanding the techniques of DoS/DDoS Attack Techniques, Understanding the Botnet Network, Understanding Various DoS and DDoS attack tools, DoS/DDoS countermeasures, Overview of DoS attack penetration testing

### DoS/DDoS Concepts

- Denial of Service (DoS) is an attack on a computer or network that reduces, restricts or prevents accessibility of system resource to its legitimate users
  - Attackers flood a victim system with non-legitimate service requests
- DDoS attack involves a multitude of compromised systems attacking a single targeted system (botnet)

### DoS/DDoS Attack Techniques

- Basic categories of the attacks
  - Volumetric Attacks: consumes the bandwidth of the target network or service
  - Fragmentation: overwhelms target's ability of reassembling fragmented packets
  - TCP state-exhaustion attack: consumes connection state table present such as load balancers, firewalls, app servers
  - Application layer attack: consumes app resources or service making it unavailable to other legitimate users
- SYN Attack
  - Attacker sends a large number of SYN request to target server
    - Target machine sends back a SYN ACK in response to the request waiting for the ACK to complete session
    - Attacker never sends ack
- ICMP flood attack: type of DoS where perpetrators send a large number of ICMP packets causing the system to stop responding to legitimate TCP/IP requests
  - To protect yourself: set a threshold limit that invokes a ICMP protection feature
- Peer to Peer Attack: attackers instruct clients of p2p file sharing hubs to disconnect for their p2p network and connect to victims fake website. Attackers can launch massive DoS attacks and compromise websites
- Permanent Denial-of-Service Attack: Also known as phlashing, refers to attacks that cause irreversible damage to system hardware
  - Unlike other DoS attacks,, it sabotages the system hardware
- Application-Level Flood Attack: Application-level flood attacks results in the loss of services
  - Using this attack , attackers exploit weaknesses in programming source code to prevent in the application from processing legitimate requests
- Distributed Reflection Denial of Service (DRDoS)
  - Also known as a spoofed attack, involves the use of multiple intermediary and secondary machines that contribute to the actual DDoS attack against the target machine or application

### Botnets

- Bots are software applications that run-automated tasks over the internet
  - A botnet is a huge network of compromised systems and can be used by an attacker to launch a DoS attack
- Scanning Methods for Finding Vulnerable Machines: Random Scanning, Hit-list scanning, topological scanning, local subnet scanning, permutation scanning
- DoS and DDoS attack tools
  - LOIC, GoldenEye

### Countermeasures

- Techniques
  - Activity Profiling
    - Increases in activity levels, distinct clusters, average packet rate etc
  - Changepoint detection
    - Filters network traffic by IP addresses, targeted port numbers, stores traffic flow data in a graph that shows the traffic flow rate vs time
  - Wavelet-based signal analysis



- A session token can be compromised in various ways
  - Session sniffing
    - Sniff to capture valid session token or ID
  - Predictable session token
    - Predict a session ID generated by a weak algorithm
    - Guesses unique session value or deduce session ID
  - Man-in-middle attack
    - Intruding an existing connection and intercept
    - Attackers use different techniques and split the TCP connection
  - Man-in-browser attack
    - Uses a trojan horse to intercept calls between browser and its security mechanisms
      - Can be a malicious extension
  - Cross-site script attack
    - XSS enables attackers to inject malicious client side scripts into web pages
    - Malicious Javascript code
    - Trojan horse can change proxy settings in user's browser
  - Cross-site request forgery attack (CSRF)
    - A CSRF attack exploits victim's active session with a trusted site in order to perform malicious activities
  - Session replay attack
    - In session reply, the attacker listens to the conversation between the user and the server and captures the authentication token of the user
    - Once authentication token is captured, the attacker replays the request to the server with the authentication token
  - Session fixation
    - Session fixation is an attack that allows an attacker to hijack a valid user session
    - Attack tries to lure a user to authenticate himself with a known session ID and then hijacks the user-validated session
    - Attacker has to provide a legitimate web app session ID and try to lure the victim browser to use it
- CSRF Cross site request forgery:
  - User visits banking site. Attacker has user somehow visit his site. His site infects and adds onto her session and insert more commands into her session and do things she did not authorize.

#### Network Level Session Hijacking

- The 3-way handshake: if the attacker can anticipate the next sequence and ACK number , they can spoof bobs address and start a communication with the server
- TCP/IP Hijacking:
- Blind Hijacking
  - Attacker injects malicious data or commands into the intercepted communication in the TCP session even if the source-routing is disabled
  - The attacker can send the data or comments but has no access to see the response
    - You might be able to see the effects however
- UDP Hijacking
  - Manipulating the packet

#### Session Hijacking Tools

- ZAP (zed attack proxy by OWASP) is an integrated penetration testing tool
- BURP Suite: inspect and modify traffic. Analyzes all kinds of content. Is an interception proxy

#### Countermeasures

## Approaches Vulnerable to Session Hijacking and their Preventative Solutions



Issue	Solution	Notes
Telnet, rlogin	OpenSSH or ssh (Secure Shell)	It sends encrypted data and makes it difficult for attacker to send the correctly encrypted data if session is hijacked
FTP	sFTP	It reduces the chances of successful hijacking
HTTP	SSL (Secure Socket Layer)	It reduces the chances of successful hijacking
IP	IPSec	It prevents hijacking by securing IP communications
Any Remote Connection	VPN	Implementing encrypted VPN such as PPTP, L2PT, IPSec, etc. for remote connection prevents session hijacking
SMB (Server Message Block)	SMB signing	It improves the security of the SMB protocol and reduces the chances of session hijacking
Hub Network	Switch Network	It mitigates the risk of ARP spoofing and other session hijacking attacks

- IPSec: protocol suite for securing IP communications by authenticating and encrypting each IP packet of a communication session
  - Deployed widely to implement virtual private networks (VPNs) and for remote user access through dial up connection to private networks
  - Transport Mode: Authenticates two connected computers. Option to encrypt data transfer. Compatible with NAT
  - Tunnel Mode: Encapsulates packets being transferred. Option to encrypt data. Not compatible with NAT.

### Module 11: Hacking Webservers

Objectives: Understanding web server concepts, understanding web server attacks, understanding webserver attack methodology, webserver attack tools, countermeasures against web server attacks, overview of patch management, webserver security tools, overview of web server penetration testing

#### Web server Concepts

- A web server is a program that hosts websites, attackers usually target software vulnerabilities and config errors to compromise the servers
  - Nowadays, network and OS level attacks can be well defended using proper network security measures such as firewalls, IDS, etc. Web servers are more vulnerable to attack since they are available on the web
- Why are web servers compromised
  - Improper file/directory permissions
  - Installing the server with default settings
  - Unnecessary services enabled
  - Security conflicts
  - Lack of proper security policy
  - Improper Authentication
  - Default Accounts
  - Misconfigs
  - Bugs in OS
  - Misconfigured SSL certificates
  - Use of self-signed certs
- IIS (internet information service) is a webserver application developed by Microsoft for Windows.

#### Webserver Attacks

- DoS/DDoS Attacks: Attackers may send numerous fake requests to the web server which results in the web server crash or become unavailable
  - May target high-profile web servers

- DNS Server Hijacking: Attacker compromises DNS server and changes the DNS settings so that all requests coming towards the target web server is redirected to another malicious server
- DNS Amplification Attack: Attacker takes advantage of DNS recursive method of DNS redirection to perform DNS amplification attack
  - Attacker uses compromised PCs with spoofed IPs to amplify the DDoS attack by exploiting the DNS recursive method
- Directory Traversal Attack: Attackers use ../ to sequence to access restricted directories outside of the web server root directory (trial and error)
- Man-in-the-middle Sniffing Attack: MITM attacks allow an attacker to access sensitive info by intercepting and altering communications
- Phishing Attacks: Attacker tricks user to submit login details for website that looks legit but it's not. Attempts to steal credentials
- Website Defacement: intruder maliciously alters visual appearance of a web page by inserting offending data. Variety of methods such as MYSQL injection
- Web Server Configuration: Refers configuration weaknesses in infrastructure such as directory traversal
- HTTP Responses Splitting Attack: involves adding header data into the input field so that the server split the response into two responses. The attack can control the second response to redirect user to malicious website whereas the other response will be discarded by browser
- Web Cache Poisoning: An attacker forces the web server's cache to flush its actual cache content and sends a specially crafted requests, which will be stored in cache
- SSH Bruteforce Attack: SSH protocols are used to create encrypted SSH Tunnel between two hosts. Attackers can brute force the SSH login credentials
- Webserver Password Cracking: An attacker tries to exploit the weaknesses to hack well-chosen passwords (social engineering, spoofing, phishing, etc).
- Web Application Attacks: Vulnerabilities in web apps running on a webserver provide a broad attack path for webserver compromise
  - SQL Injection, Directory Traversal, DoS, Cookie Tampering, XSS Attack, Buffer Overflow, CSRF attack,

#### Attack Methodology:

Information Gathering, Webserver Footprinting, Mirroring Website, Vulnerability Scanning, Session hijacking, Hacking webserver passwords

- Information Gathering: Robots.txt file contains list of web server directory and files that website owner wants to hide from web crawlers
- .Use tools such as burp suite to automate session hijacking

#### Webserver Attack Tools

- Metasploit: Encapsulates an exploit.
  - Payload module: carries a backpack into the system to unload
  - Metasploit Aux Module: Performing arbitrary, one-off actions such as port scanning, DoS, and fuzzing
  - NOPS module: generate a no-operation instructions used for blocking out buffers
- Password Cracking: THC Hydra, Cain & Abel

#### Countermeasures

- An ideal web hosting network should be designed with at least three segments namely: The internet segment, secure server security segment (DMZ), internal network
  - Placed the web server in DMZ of the network isolated from the public network as well as internal network
  - Firewalls should be placed for internal network as well as internet traffic going towards DMZ
- Patches and Updates: Ensure service packs, hotfixes, and security patch levels are consistent on all domain controllers
- Protocols: block all unnecessary ports, ICMPs, and unnecessary protocols such as NetBIOS and SMB. Disable WebDav if not used
- Files and Directories: delete unnecessary files, disable serving of directory listings, disable serving certain file types , avoid virtual directories
- Detecting Hacking Attempts: Run scripts on the server that detects any changes made in the existing executable file. Compare hash values of files on server to detect changes in codebase. Alert user upon any change in detection
- Secure the SAM (stand-alone servers only)

- Defending against DNS hijacking: choose ICANN accredited registrar. Install anti-virus

### Patch Management

- Hotfixes are an update to fix a specific customer issue
- A patch is a small piece of software designed to fix problems
  - Hotfixes and Patches are sometimes combined for server packs
- Patch Management is a process used to ensure that the appropriate patches are installed on a system to help fix known vulnerabilities
  - Before installing a patch, verify the source.
- Patch Management Tools: MBSA (Microsoft baseline Security Analyzer) - checks for available updates to OS, SQL Server, .NET framework etc

### Webserver Security Tools

- Syhunt helps automate web app security testing and guards. N Stalker is a scanner to search vulnerabilities

### Webserver Pen Testing

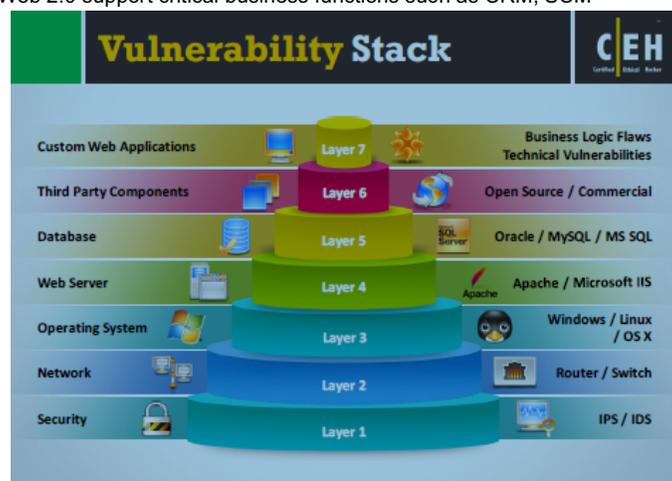
- Used to identify, analyze, and report vulnerabilities

## **Module 12: Hacking Web Applications**

Module Objectives: Understanding Web Application concepts, understanding web app threats, understanding web app hacking methodology, web app hacking tools, understanding web app countermeasures, web app security tools, overview of web app pen testing

### Web App Concepts

- Web apps provide an interface between end users and web servers through a set of pages
- Web tech such as Web 2.0 support critical business functions such as CRM, SCM



### Web App Threats

- Cookie Poisoning: by changing info in a cookie, attackers can bypass authentication process
- Directory Traversal: Gives access to unrestricted directories
- Unvalidated Input: Tempering http requests, form field, hidden fields, query strings, so on. Example of these attacks include SQL injection, XSS, buffer overflows
- Cross Site Scripting: Bypassing client-ID mechanisms to gain privileges, injecting malicious scripts into web pages
- Injection Flaws: Injecting malicious code, commands, scripts into input gates of flawed apps
- SQL Injection: type of attack where attackers inject SQL commands via input data, and then tamper with the data
  - LDAP Injection to obtain direct access to databases behind LDAP tree

- Parameter/Form tampering: Manipulates the parameters exchanged between client and server to modify app data such as user cred and permissions.
- DoS: intended to terminate operations
- Broken Access Control: method in which attacker identifies a flaw related to access control and bypasses the authentication, then compromises the network
- Cross-Site Request Forgery: attack in which an authenticated user is made to perform certain tasks on the web app that an attacker chooses.
- Information Leakage: can cause great losses to company.
- Improper Error Handling : important to define how a system or network should behave when an error occurs. Otherwise, error may provide a chance for an attacker to break into the system. Improper error can lead to DoS attack
- Log Tampering: Attackers can inject, delete, or tamper with app logs to hide their identities
- Buffer Overflow: Occurs when app fails to guard its buffer property and allows writing beyond its maximum size
- Broken Session management: When credentials such as passwords are not properly secured
- Security Misconfigurations
- Broken Account Management: account update, forgotten/lost password recovery/reset
- Insecure Storage: Users must maintain the proper security of their storage locations
- Platform Exploits: Each platform (BEA WEBLOGIC, COLD FUSION) has its own various vulnerabilities
- Insecure Direct Object References: When developers expose objects such as files, records, result is insecure direct object reference
- Insecure Cryptographic Storage: Sensitive data should be properly encrypted using cryptographic. Some cryptographic techniques have inherent weaknesses however
- Authentication Hijacking: Once an attacker compromises a system, user impersonation can occur
- Network Access attacks: can allow levels of access that standard HTTP app methods could not grant
- Cookie Snooping
- Web Services Attack: Web services are based on XML protocols such SOAP (simple object access protocol) for communication between web services
- Insufficient Transport layer protection
- Hidden Manipulation
- DMZ protocol attacks
- Unvalidated redirects and forwards
- Failure to restrict URL access
- Obfuscation Application
- Security Management Exploits
- Session Fixation Attack: Attacker tricks user to access a genuine web server using an explicit session ID value. Attacker assumes identity of the victim and exploits credentials on the server
- Malicious File Execution

### Hacking Methodology

- Hackers first footprint the web infrastructure
  - Server discovery, location
- Service Discovery: Scan Ports
- Banner grabbing: footprinting technique to obtain sensitive info about target. They can analyze the server response to certain requests (server identification)
- Detecting Web App Firewalls and Proxies on target site
  - Use Trace method for proxy, and cookie response for a firewall
- Hidden Content discovery: Web spidering automatically finds hidden content
- Launch web server attack to exploit identified vulnerabilities, launch DoS
- Attacking authentication mechanism
  - Username enumeration
    - Verbose failure messages. Predictable user names
  - Cookie Exploitation
    - Poisoning(tampering), Sniffing Replay
  - Session Attack
    - Session prediction, brute forcing, poisoning
  - Password Attack:
    - Guessing, brute force
- Authorization attack: finds legitimate accounts then slowly escalates privileges
- Attack Session Management Mechanism: involves exchanging sensitive info between server and clients. If session management is insecure, attacker can take advantage of flawed session management session
  - Bypassing authentication controls

- Perform injection attacks: exploiting vulnerable input validation mechanism implement
- Attack Data connectivity: attacking database connection that forms link between a database server and its client software
  - Connection string injection: attacker injects parameters in a connection string. CSPP attacks (Connection String Parameter Attacks).
  - Connection Pool DoS: Attacker examines connection pooling settings and constructs large SQL query, and runs multiple queries simultaneously to consume all connections

#### Countermeasures

- Encoding Schemes: employing encoding schemes for data to safely handle unusual characters and binary data in the way you intent
  - Ex. unicode editing
- How to defend against SQL Injection Attacks
  - Limit length of user input
  - Perform input validation
- How to defend against xss
  - Validate all headers, cookies, strings, form fields. Use firewall
- How to configure against DoS
  - Configure firewall to deny ICMP traffic access
  - Perform thorough input validation
- How to defend against web services attack
  - Multiple layer protection

#### Tools

- N-Stalker is effective suite of web security assessment tools

#### Pen Testing

1. Info Gathering
2. Config Management Testing
3. Authentication Testing
4. Session Management testing
5. Authorization Testings
6. Data Validation Testing
7. DoS Testing
8. Web Services Testing
9. AJAX Testing
10. Use Kali Linux tools
  - a. Metasploit

#### **Module 13: SQL Injection**

- Understanding SQL injection concepts, understanding various types of SQL injection attacks, understanding SQL injection methodology, SQL injection tools, understanding different IDS evasion techniques, SQL injection countermeasures, SQL injection detection tools

#### SQL Injection Concepts

- SQL injection is a technique used to take advantage of non-validated input vulnerabilities to pass SQL commands through a web app for execution by the backend database
  - Usually to retrieve information
  - This is a flaw in web apps
- Attacker can deface a web page with this attack
- They can add info to your website, extract data, and insert new data

#### Types of SQL Injection

- Error based SQL Injection: Attacker puts intentional bad input into app to see the database-level error messages. Uses this to create carefully designed SQL Injections

- Blind SQL Injection: Attacker has no error messages from the system with which to work. Instead, attack simply sends a malicious SQL query to the database
- Whenever you see SELECT, it is probably a SQL command
- Union SQL command, joining a forged query to the original query
- Time-Based SQL Injection: evaluates time delay in response to true-false queries

#### SQL Injection Methodology

- Information gathering and SQL vulnerability detection
  - Attackers analyze web GET and POST requests to identify all input fields
  - Afterwards, launch attack
  - Advanced SQL injections
- SQL Injection Black Box Pen Testing
  - Send single quotes and input data to see where the user input is not sanitized
  - Send long strings of junk data to detect buffer overruns
  - Used right square bracket as input data

#### Evasion Techniques

- Evading IDS
  - Obscure input strings
  - Hex Encoding
  - Manipulating whitespace
  - Inline Comment
  - Char encoding

#### Countermeasures

- Use Firewalls on SQL server
- Make no assumptions about size, type, or content of the data that is received by the application
- Avoid constructing dynamic SQL with concatenated input values

#### **Module 14: Hacking Wireless Networks**

- Understanding Wireless Concepts, understanding wireless encryption algorithms, understanding wireless threats, understanding wireless hacking methodology, wireless hacking tools, understanding bluetooth hacking techniques, understanding wireless hacking countermeasures, overview of wireless penetration testing

#### Wireless Concepts

- GSM: universal system used for mobile transportation for wireless network worldwide
- Bandwidth: Describes amount of information that may be broadcasted over a connection
- BSSID: The MAC address of an access point that has set up a basic service set
- ISM band: a set of frequency for the international industrial, scientific, and medical communities
- Access Point: Used to connect wireless devices to a wireless network
- Hotspot: Places where wireless network is available for public use
- Association: Process of connecting a wireless device to an access point
- Orthogonal Frequency Division Multiplexing: method of encoding digital data on multiple carrier frequencies
- Direct-Sequence Spread Spectrum: original data signal is multiplied with a pseudo random noise spreading code
- Frequency-hopping spread spectrum (FHSS): Method of transmitting radio signals rapidly switching a carrier among many frequency channels
- Wireless Networks
  - WiFi refers to IEEE 802.11 standard

Amendments	Freq. (GHz)	Modulation	Speed (Mbps)	Range (ft)
802.11a	5	OFDM	54	25 – 75
802.11b	2.4	DSSS	11	150 – 150
802.11g	2.4	OFDM, DSSS	54	150 – 150
802.11i	Defines WPA2-Enterprise/WPA2-Personal for Wi-Fi			
802.11n	2.4, 5	OFDM	54	~100
802.16 (WiMAX)	10 - 66		70 – 1000	30 miles
Bluetooth	2.4		1 - 3	25

- 
- SSID (service set identifier)
- Open System Authentication Process: in open system, any wireless client that wants to access a WiFi networks sends a request to the wireless AP for authentication.
- Shared Key Authentication Process: in this process, each wireless station receives a shared secret key over a secure channel that is distinct from the 802.11 comm channels.
- Centralized Authentication server (RADIUS)
- WiFi Chalking
  - WarChalking: draw symbols in public places to advertise open Wi-Fi networks
- Types of Wireless Antennas
  - Directional Antennas: Used to broadcast and obtain radio waves from a single direction
  - Omni-Directional Antennas: provides 360 degrees horizontal broadcasts, used in wireless base stations
  - Parabolic Grid Antenna: Based on the idea of a satellite dish. Can pick up Wi-Fi signals ten miles or more
  - Yagi Antenna: unidirectional antenna
  - Dipole Antenna: Bi-Directional Antenna, used to support client connection rather than site-to-site applications
- Parabolic grid antennas let attackers attack from from farther away (10 miles!)

#### Wireless Encryption

- WEP (wired equivalent privacy): weakest encryption. Uses 24-bit initialization vector. A 64 bit WEP uses a 40 bit key etc
  - Can use Cain & Abel to crack
- WPA (Wifi Protected Access): Stronger encryption with TKIP.
  - You can brute force the keys offline
  - You can defend by using stronger passphrases
- WPA2: Stronger data protection with AES
  - WPA-2 personal uses a pre-shared key to protect access
  - WPA-2 Enterprise includes EAP or RADIUS for centralized authentication w/kerberos etc

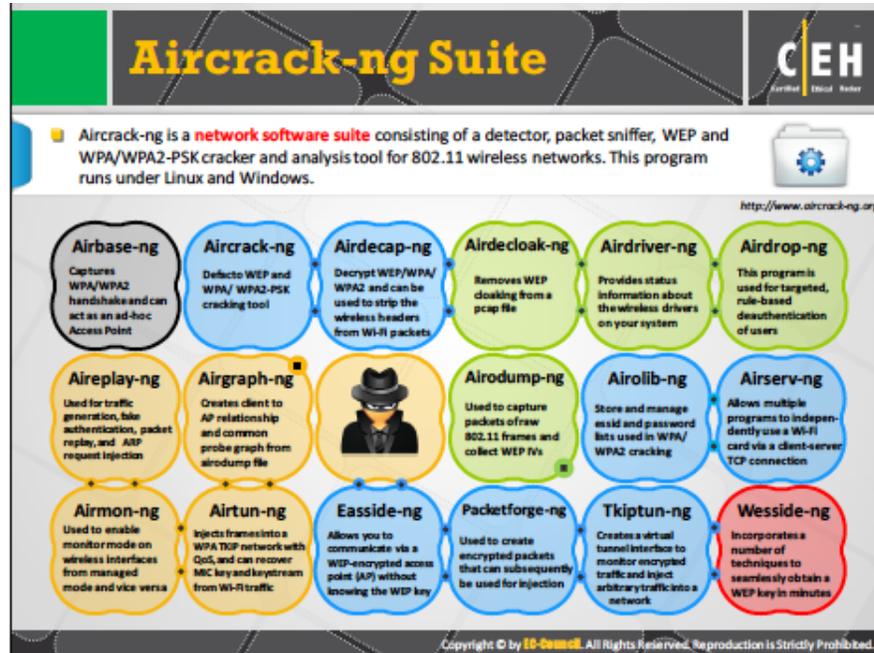
#### Wireless Threats

- Access Control Attacks: Aims to penetrate a network by evading WLAN access control measures, such as AP MAC filters and Wi-Fi port access controls
- Integrity Attacks: Sending forged control management or data frames over a wireless network
- Confidentiality Attacks: attempt to intercept confidential information sent over wireless associations
- Availability Attacks: DoS
- Authentication Attacks: Steal the identity of Wi-Fi clients, their PI, logins, etc. to unauthorized access of network resources
- Rogue Access Point Attack: Hijacking connections and acting as a middle man sniffing
- Client Mis-Association: Attacker sets up a rogue access point outside of the corporate perimeter and lures the employees of the organization to connect with it
- Misconfigured Access Point Attack: Accidents for configurations that you can exploit

- AD Hoc connection attack: Wifi Clients communicate directly in ad-hoc and do not require AP to relay packet. Attack can attack OS direct since the encryption is weak
- Honeypot Access Point Attack: Attacker takes advantage of multiple WLAN's in area and use same SID
- AP MAC Spoofing: Hacker spoofs the MAC address of the WLAN client equipment to mask an authorized client
- Jamming Signal Attack: High gain amplifier

### Wireless Hacking Methodology

1. WiFi Discovery: discovers the WiFi network
2. GPS Mapping: Attackers create a map of discovered Wi-Fi network and create a database
3. Wireless Traffic Analysis: identify vulnerabilities, WiFi reconnaissance, Tools for Packet Capture & Analysis
4. Launch Wireless Attacks



- a. Fragmentation Attack: can obtain 1500 bytes of PRGA data that can be used for injection attacks
  - b. Mac Spoofing: attackers change MAC address to that of an authenticated user to bypass the MAC filtering configured in an access point
  - c. Denial of Service: Deauthentication and Disassociation attacks
  - d. Man in the middle attack MITM : Attacker spoofs his MAC, sends a deAuth requests and then puts himself in the middle
  - e. Wireless ARP poisoning attack:
  - f. Rogue Access Point: Wireless APs attacker installs on a network without authorization and are not under management of the network administrator. Are not configured with any security
  - g. Evil Twin: Replicates another wireless APs name via common SSID
5. Crack Wi-Fi encryption
    - a. Crack WEP using Aircrack
    - b. Crack WPA-PSK using aircrack
    - c. WEP cracking using Cain & Abel
  6. Compromise the Wi-Fi Network
    - What is spectrum analysis
      - RF spectrum analyzers examine Wi-Fi radio transmissions and measure power (amplitude)
      - Employ statistical analysis to plot spectral usage
      - Can be used for DoS attack

### Bluetooth Hacking

- Exploitation of Bluetooth Stack implementation vulnerabilities
  - Bluesmacking: DoS attack which overflows Bluetooth-enabled devices with random packets causing device to crash
  - Bluejacking: sending unsolicited messages over bluetooth to bluetooth-enabled devices such as mobile phones, laptops, etc
  - Bluesnarfing: Theft of information from a wireless device through a bluetooth connection
  - Blue Sniff: Proof of concept code for a bluetooth wardriving utility
  - Bluebugging: remotely accessing the bluetooth-enabled devices and using its features
  - BluePrinting: collecting information about bluetooth enabled devices such as manufacturer, device model, firmware
  - MAC spoofing attack: intercepting data intended for other bluetooth enabled devices
  - MITM: Modifying data between bluetooth enabled devices communication on a piconet
- Bluetooth Modes:
  - Discoverable, Limited Discoverable (timed), Non-discoverable
- Pairing Modes
  - Non-pairable models: rejects every pairing request
  - Pairable mode: will pair upon request

#### Countermeasures

- How to defend against bluetooth hacking
  - Use non-regular patterns such as PIN keys
  - Keep device in non-discoverable mode
  - Keep a check of all paired devices
  - Always enable encryptions

#### Wireless Security Tools

- Wireless Intrusion Prevention Systems

### **Module 15: Hacking Mobile Platforms**

- Understanding Mobile platform attack vectors, understanding various Android Threats and Attacks, Understanding various iOS threats and attacks, understanding various Windows Phone OS Threats and Attacks, Understanding various blackberry threats as attacks, understanding mobile device management (MDM), Mobile Security Guidelines and Security Tools, Overview of Mobile Pen Testing

#### Mobile Platform Attack Vectors

- OWASP Mobile Top 10 Risks
  - Insecure Data Storage
    - Assumption malware won't enter system. Jailbreaking bypasses encryption
  - Unintended Data Leakage
    - When a user places sensitive data in a location accessible to other apps
  - Broken Cryptography
    - Weak encryption algorithms. Users should use AES or 3DES algorithms
  - Security Decision via Untrusted Inputs
    - Apps use protection mechanisms dependent on input values (cookies, environmental variables, hidden form fields), but these input values can be altered by an attacker to bypass protection mechanism
  - Lack of Binary Protections: Lack of binary protections in a mobile app exposes it and owner to wide variety of technical and business risks if insecure. Must use countermeasures such as
    - Secure coding techniques
    - Jailbreak detection controls
    - Checksum controls
    - Certificate Pinning Controls

- Anatomy of a Mobile Attack
  - The device -> the network > the data center
  - Clicking Jacking: tricking users to click something different than what they think they are clicking. Attackers obtain sensitive info or take control of device
  - Framing: a webpage integrated into another webpage using iFrame elements in HTML
  - Drive By Downloading: unintended download of software from the internet. Android is affected by this attack
  - Man in the Middle: Attacker implants malicious code on victim's mobile device
  - Buffer Overflows: writing data to buffer suites ,
  - Data Caching: Caching in mobile devices used to interact with web apps, attackers attempt to exploit the data caches
- Phone/SMS-Based attacks
  - Baseband attacks: exploiting vulnerabilities in phone's GSM/3GPP baseband processor, which sends/receives signals to towers
  - SMiShing - Type of phishing where attacker uses SMS text message to link to malicious site
  - RF (radio frequency) attacks: exploit vulnerabilities found on different peripheral communication channels normally used in nearby device-device communications
- Application-based attacks
  - Sensitive Data Storage: Some apps employ weak security in their database architecture, which make them targets for attacker to hack and steal sensitive user information stored on them
  - No encryption/weak encryption: apps transmit data unencrypted or weakly encrypted are susceptible to attack such as session hijacking
  - Improper SSL validation: Security Loopholes in apps SSL validation process may allow attackers to circumvent the data security
  - Config Manipulation: Apps may use external files and libraries, modifying those entities or affecting apps' capability of using those results in a config manipulation attack
  - Dynamic Runtime Injection: attackers manipulate and abuse the runtime of an app to circumvent security locks, logic checks, access privileges parts of an app, and steal data
  - Unintended Permissions: Misconfigured apps can at times open doors to attackers by providing unintended permissions
  - Escalated privileges: Attackers engage in privilege escalation attacks , which take advantage of design flaws, programming errors, bugs, or config oversights to gain access to resources
- OS Based Attacks
  - iOS Jailbreaking: removing security mechanisms set by apple to prevent malicious code
  - Android Rooting: allows users to attain privileged control (root access) within android's subsystem.
  - Passwords and data accessible
  - Carrier-loaded software: pre installed software or apps on devices may contain vulnerabilities that an attacker can exploit to perform malicious activities such as delete, modify, or steal data on the device, eavesdrop on calls
  - Zero-day exploits: launch an attack by exploiting a previously unknown vulnerability in a mobile OS or app.
- The Network based point of attacks
  - WiFi (weak encryption or no encryption)
  - Rogue Access Points: attackers install illicit wireless access point by physical means, which allows them to access a protected network by hijacking the connections of network users
  - Man in the Middle (MITM): attackers eaves on existing network connections between two systems
  - SSLStrip: Type of MITM attack which exploits vulnerabilities in the SSL/TLS implementation
  - Session Hijacking: Attacker steal valid session ID's
  - DNS Poisoning: Attackers exploit DNS servers, redirect website users to another website of the attacker's choice
  - Fake SSL certificates: Fake SSL certs represent another kind of MITM attacks. Attacker issues a fake SSL cert to intercept traffic on a supposedly secure HTTPS connection
- The Data Center
  - Two main point of entry: web server and a database
  - Web server-based attacks
    - Platform vulnerabilities: Exploiting vulnerabilities in the OS, Server software, or app modules running on the web server
    - Server Misconfiguration
    - XSS
    - CSRF
    - Weak Input Validation
    - Brute-Force Attacks
- Database Attacks

- SQL Injection
  - Data Dumping
  - OS command execution
  - Privilege Escalation
- Sandboxing: helps protect systems and users by limiting the resources the app can access in the mobile platform; however, malicious apps may exploit vulnerabilities

### Hacking Android OS

- The device administration API provides device administration features at the system level
- Rooting allows android users to attain privileged control (root access)
  - Involves exploiting security vulnerabilities in the device firmware
- Securing Android Devices:
  - Enable screen locks
  - Don't root your device
  - Download apps only from android market
  - Keep device updated with google software
  - Do not directly download APK files
  - Update OS regularly
  - Use free protector app
- Google Apps device policy: allows domain admin to set security policies for your android device

### Hacking iOS

- Layers of the OS
  - Cocoa Touch: key framework that help in building iOS app. Defines appearance, basic services such as touch
  - Media: contains graphics, audio, and video technology experienced in apps
  - Core Services: contains fundamental system services for apps
  - Core OS: low level feature on which most on which most other technologies are built
- Tethered (kernel will be patched upon restart) and untethered

### Hacking Windows Phone

### Hacking Blackberry

- Malicious Code Signing: Blackberry apps must be signed by RIM. Attacker can obtain code-signing keys for a malicious app and post it in the store
- JAD file exploits: A jad file allows a user to go through app details and decide whether to download the app. However, attackers created spoofed .jad files to trick user
- PIM Data Attacks: PIM (personal information manager) includes address , books, calendars, tasks
  - Malicious apps can delete or modify this data
- TCP/IP Connections Vulnerabilities: If the device firewall is off, signed apps can open TCP connections without the user being prompted.
  - Malicious apps create a reverse connection with the attacker enabling him to use the infected device as a TCP proxy and gain access to organization's internal resources

### Mobile Device Management (MDM)

- MDM provides platforms for over the air or wired distribution of application, data and configuration settings for all types of mobile devices, smartphones, tablets, etc.
  - Helps implementing enterprise-wide policies to reduce support cost s
  - Can manage both company-owned and BYOD devices

### Mobile Security Guidelines and Tools

- General Guidelines
  - Do not load too many apps and avoid auto-upload of photos to social networks
  - Perform a security assessment of the Application Architecture
  - Maintain configuration control and management
  - Install apps from trusted app stores
  - Securely wipe or delete the data disposing of the device

- Ensure bluetooth is off by default
- Do not share location within GPS enabled apps
- Never connect two separate networks such as Wi-Fi and Bluetooth simultaneously

## **Module 16: Evading IDS, Firewalls, and Honeypots**

- Understanding IDS, Firewall, and Honeypot Concept : IDS, Firewall and Honeypot Solutions: Understanding different techniques to bypass IDS : Understanding different techniques to bypass firewalls, IDS/Firewall Evading Tools : Understanding different techniques to detect honeypots : Overview of IDS and Firewall Penetration Testing

### **IDS, Firewall, and Honeypot Concepts**

- An IDS inspects all inbound and outbound network traffic for suspicious patterns that may indicate a network security breach
  - Checks traffic for signatures that match known intrusion patterns
  - Anomaly Detection (behavior detection)
  - Protocol Anomaly Detection
- Indications of Intrusions
  - System Intrusions
    - Presence of new files/programs
    - Changes in file permissions
    - Unexplained changes in file size
    - Rogue Files
    - Unfamiliar file names in directories
    - Missing files
  - Network Intrusions
    - Repeated probes of the available services on your machines
    - Connections from unusual locations
    - Repeated login attempts from remote hosts
    - Arbitrary data in log files
- Firewall Architecture
  - Bastion Host
    - Computer system designed and configured to protect network resources from attack
  - Screened Subnet
    - Also known as the DMZ contains hosts that offer public services. DMZ zone only responds to public requests, and has no hosts accessed by the private network
  - Multi-homed Firewall
    - A firewall with two or more interfaces
- DeMilitarized Zone (DMZ)
  - A network that serves as a buffer between the internal secure network and insecure internet
  - Can be created using firewall with three or more main network interfaces
- Types of Firewall
  - Packet Filters: works on the network layers of OSI. Can drop packets if needed
  - Circuit Level Gateways: Works at the sessions layer. Information passed to a remote computer through a circuit-level gateway appear to have originated from the gateway. They monitor requests to create sessions, and determines if the session will be allowed. They allow or prevent data streams
  - Application Level Gateways: App-level proxies can filter packets at the application later of the OSI
  - Stateful Multilayer Inspection Firewalls: combines the aspects of the other three types of firewalls
- Honeypot
  - Information system resource that is expressly set up to attract and trap people who attempt to penetrate an organization's network
    - Honeypot can log port access attempts, monitor attacker's keystrokes, show early signs etc
  - 2 Types of Honeypots
    - Low-interaction Honeypots: simulate only a limited number of services and apps. Cannot be compromised
    - High-interaction Honeypots: simulates all services and apps. Can be completely compromised by attackers.
      - Captures complete information about an attack vector such attack techniques

### **IDS Tools**

- Snort

### Evading IDS

- Insertion Attack: IDS blindly believes and accepts the packet
- Evasion: End system accepts a packet that an IDS rejects. Attacker is exploiting the host computer
- DoS Attack: Attackers intrusion attempts will not be logged
- Obfuscating: encoding the attack payload in a way that the target computer understands but the IDS will not (polymorphic code, etc)
- False Positive Generation: Attackers w/ knowledge of the target IDS, craft packets just to generate alerts. Causes IDS to generate large number of false positive alerts. Then use it to hide real attack traffic
- Session Splicing
- Unicode Evasion Technique: Attackers can convert attack strings to unicode characters to avoid pattern and signature matching at the IDS
- Fragmentation Attack: Attackers will keep sending fragments with 15 second delays until all attack payload is reassembled at the target system
- TTL attacks require attacker to have a prior knowledge of the topology of the victim's network
- Invalid RST Packets
  - Uses a checksum to communicate with host even though the IDS thinks that communication has ended
- Urgency Flag
  - A URG flag in the TCP header is used to mark the data that requires urgent processing
    - Many IDS do not address the URG pointer
- Polymorphic Shellcode: Most IDSs contains signatures for commonly used strings within shellcode. This can be bypassed by using encoded shellcode containing a stub that decodes the shell code
- App Layer Attacks: IDS cannot verify signature of a compressed file

### Evading Firewalls

- Port Scanning is used to identify open ports and services running on these ports
  - Open ports can be further probed to identify the version of services, which helps in finding vulnerabilities in these services
- Firewalking: A technique that uses TTL values to determine gateway ACL filters
  - Attacker sends a TCP or UDP packet to the targeted firewall with a TTL set to one hop greater
- Banner Grabbing: Banners are service announcements provided by services in response to connection requests, and often carry vendor version information
- IP address spoofing to a trusted machine
- Source Routing: Allows sender of a packet to partially or completely specify the route of a packet through a network, going around a firewall
- Tiny Fragments: Forcing some of the TCP packet's header info into the next fragment
- ICMP Tunneling: Allows tunneling a backdoor shell in the data portion of ICMP echo packets
- Ack Tunneling: Allows tunneling a backdoor application with TCP packets with the ACK bit set
- HTTP Tunneling Method: allows attackers to perform various internet tasks despite restrictions imposed by firewalls. Method can be implemented if the target company has a public web server with port 80 used for HTTP traffic

### Detecting Honeypots

- Attackers craft malicious probe packets to scan for services such as HTTP over SSL, SMTP over SSL, and IMAP
- Ports that show a particular service running but deny a three-way handshake indicate the presence of a honeypot

### Countermeasures

- Shut down switch ports associated with the known attack hosts
- Reset (RST) malicious TCP sessions

### **Module 17: Cloud Computing**

- Understanding cloud computing concepts, understanding cloud computing threats, understanding cloud computing attacks, understanding cloud computing security, understanding cloud computing security tools, overview of cloud pen testing

## Introduction to Cloud Computing

- Cloud computing is an on-demand delivery of IT capabilities where IT infrastructure applications are provided to subscribers as a metered service
- Types of Cloud Computing Services:
  - IaaS: Provides virtual machines and other abstracted hardware and OSs which may be controlled through a service API
  - PaaS: Offers development tools, config management, and deployment platforms on-demand and can be used by subscribers to develop custom applications
  - SaaS: Offers software to subscribers on-demand over the internet
- Cloud Deployment Models
  - Private Cloud: Cloud Infrastructure operated solely for a single organization
  - Community Cloud: Shared Infrastructure between several organizations from a specific communications with common concerns
  - Hybrid Cloud: Composition of two or more cloud (private, community or public)
  - Public Cloud: Services are rendered over a network that is open for public use

## Cloud Computing Threats

- Data Breach/Loss, Abuse of Cloud Services, Insecure Interfaces and APIs, Insufficient due diligence, shared technology issues, unknown risk profile, Inadequate infrastructure design and planning, conflicts between client hardening procedures and cloud environment, malicious insiders, illegal access to the cloud, privilege Escalation via error

## **Module 18: Cryptography**

Heartbleed:: Security Flaw in OpenSSL

PoodleBleed: Security vulnerability in SSL 3.0

Understanding Cryptography Concepts, Overview of Encryption Algorithms, Cryptography, Cryptography Tools, Understanding Public key Infrastructure, Understanding Email Encryption, Understanding disk encryption, Understanding cryptographic attacks, cryptanalysis

## Cryptography Concepts

- The conversion of data into a scrambled code that is decrypted and sent over a private or public network
  - Used for email messages, chat sessions, web transactions, personal data, corporate data, e-commerce apps, etc.
- Types of Cryptography
  - Symmetric Encryption: Uses the same key for encryption as it does for decryption
  - Asymmetric Encryption: Uses different key for encryption for encryption and decryption
- Government Access to Keys (GAK)
  - Software companies will give copies of all keys
  - Government promises they will hold on to the keys in a secure will, and will only use them when a court issues a warrant to do so
    - Gives them ability to wiretap phones

## Encryption Algorithms

- Cipher is an algorithm for performing encryption and decryption
  - Classical Cipher: Most basic type, operates on the alphabet (A-Z)
  - Modern Ciphers: provide secrecy, integrity, and authentication of sender. Uses a one-way mathematical function capable of factoring large prime numbers
    - Block Ciphers: Deterministic algorithm operating on block of fixed size with an unvary transformation specified by a symmetric key.
    - Stream Ciphers: Symmetric key ciphers are plaintext digits combined with a key stream (random).
  - Data Encryption Standard (DES)

- Uses a secret key for both encryption and decryption (symmetric). 62 bit secret key.
    - Advanced Encryption Standard (AES): Symmetric key algorithm for securing sensitive but unclassified material by U.S. Government agencies (128 bit)
    - RC4 variable key size stream cipher
    - RC5: parameterized algorithm with variable block size, 128 bits
    - RC6: Symmetric key block cipher derived from RC5
    - Digital Signature Algorithm(DSA): Specifies algorithm to be used in the generation and verification of digital signatures for sensitive, unclassified application
    - Digital Signature: Computed using a set of rules (I.e, the DSA) and a set of parameters
    - RSA (Rivest Shamir Adleman)
      - RSA is an internet encryption and authentication system
      - Widely used and is one of the de facto encryption standard
      - Uses modular arithmetic and elementary number theories
    - Message Digest (one way Hash)
      - Hash functions calculate a unique fixed-size bit string
      - Every output bit has a 50% of changing
      - MD5, SHA 128/256
- Secure Hashing Algorithms
  - SHA-1: Produces 160 digest with maximum length 264-1, resembles MD5
  - SHA-2: comprised of SHA-256 and SHA-512(64 bit)
  - SHA-3: Uses sponge construction in which message block are XORed
- What is SSH (Secure Shell)
  - Replacement for telnet
  - Provides an encrypted channel
  - Provides strong host-to-host and user authentication

#### Public Key Infrastructure

- Public Key infrastructure (PKI): set of hardware, software, people, policies, and procedures required to create, manage, distribute, use, store, and revoke digital certificates
- Signed CA vs Self Signed: Signed is more trustworthy

#### Email Encryption

- Digital signature used asymmetric cryptography to simulate the security properties of a signature in digital, rather than written form
  - A digital signature may be further protection, by encrypting the signed email
- SSL (Secure Sockets Layer): SSL is an app protocol developed for netscape for managing the security of a message transmission on the internet
  - It uses RSA asymmetric (public key) encryption
- Transport Layer Security (TLS): Protocol to establish a secure connection between a client and a sever. Uses RSA algorithm with 1024 and 2048 bit strengths

#### Cryptographic Attacks

- Ciphertext only attack: goal of this attack to recover encryption key from cipher text
- Adaptive Chosen-plaintext attack: attacker makes a series of interactive queries
- Chosen-plaintext attack: attacker defines his own plaintext, feeds it into the cipher, and analyzes the resulting cipher text
- Chosen-plaintext Attack: Attacker defines his own plaintext, feeds it into the cipher, and analyzes the resulting ciphertext
- Known-plaintext Attack: Attacker has knowledge of some part of the plain text
- Code Breaking Methodologies:
  - Trickery and Deceit: Social Engineering techniques
  - Brute Force: trying every possible combination
  - One-Time pad: contains many non-repeating groups of letters or number keys which are randomly chosen
  - Frequency Analysis: Study the frequency of letters or groups of letters in a ciphertext
- MITM on digital sig schemes
  - Attack works by encrypting one end and decrypting from the other end, the meeting in the middle
    - Can be used for forging signatures even on digital signatures
- Side Channel Attack: Physical attack performed on a cryptographic device/cryptosystem to gain sensitive information

---

Extra Resources:

- MW AIO Chap 3: [https://quizlet.com/\\_3ldo8z](https://quizlet.com/_3ldo8z)
- MW AIO Chap 4: [https://quizlet.com/\\_3ldofz](https://quizlet.com/_3ldofz)
- MW AIO Chap 5: [https://quizlet.com/\\_3ldokt](https://quizlet.com/_3ldokt)
- MW AIO Chap 6: [https://quizlet.com/\\_3ldoqo](https://quizlet.com/_3ldoqo)
- MW AIO Chap 7: [https://quizlet.com/\\_3ldp6p](https://quizlet.com/_3ldp6p)
- MW AIO Chap 8: [https://quizlet.com/\\_3ldpbs](https://quizlet.com/_3ldpbs)
- MW AIO Chap 9: [https://quizlet.com/\\_3ldplh](https://quizlet.com/_3ldplh)
- MW AIO Chap 10: [https://quizlet.com/\\_3ldwzh](https://quizlet.com/_3ldwzh)
- MW AIO Chap 11: [https://quizlet.com/\\_3ldxls](https://quizlet.com/_3ldxls)
- MW AIO Chap 12: [https://quizlet.com/\\_3ldxue](https://quizlet.com/_3ldxue)
- Major Named Vulnerabilities: [https://quizlet.com/\\_3lc3is](https://quizlet.com/_3lc3is)
- Boson: [https://quizlet.com/\\_3l8qep](https://quizlet.com/_3l8qep)
- "Tools": [https://quizlet.com/\\_3la4dl](https://quizlet.com/_3la4dl)
- DoS attacks: [https://quizlet.com/\\_3la3o3](https://quizlet.com/_3la3o3)
- General CEH: [https://quizlet.com/\\_3la3wu](https://quizlet.com/_3la3wu)
- Workflowy: <https://workflowy.com/s/De7u.dMnMILnDcu>
- Workflowy (pastebin): <https://pastebin.com/HNewRQVf>
- NMAP Switches: <https://quizlet.com/138174963/ceh-v9-nmap-command-switches-flash-cards/>
- CEH Pre-Assesment: <https://www.eccouncil.org/programs/certified-ethical-hacker-ceh/ceh-assessment/>
- CEH v9 Questions (create a free account to view all questions): <https://www.exam-labs.com/exam/312-50v9#!>