CEH Chapter One: Getting Started

TYPES OF HACKERS

White-Hat (Ethical): Penetration testers -- have contracts to prove they are legally attempting to infiltrate a network
Grey-Hat: Hackers who practice in both black and white hat capacities
Black-Hat: Hackers who use computers to intentionally commit illegal acts
Suicide: Hackers intending to be caught.
Script Kiddie: Hackers with limited or no training. Scope limited to basic tools and techniques
Contracts provide *proof* for white hat hackers

The more *secure* a network is, the less *convenient* it is to access.

SECURITY ←-------------------------→ CONVENIENCE

The more *convenient* a network is, the less *secure* it is against attacks.

White Box: Full knowledge -- internal attack simulation or audit.	Gray Box: Limited Knowledge -- attacker may know IP addresses, OS, & environment.	Black Box: No Knowledge -- simulates an outside attack from a third party.

CONFIDENTIALITY
ACCOUNTABILITY
CIA
TRIAD
INTEGRITY

Confidentiality - Keeping info away from unauthorized users.	Integrity - Keeping info in format that is true and correct to original purposes.	Availability - Keeping info available to those who are authorized to possess it.
Disclosure - inadvertent, accidental, or malicious revealing of information	Alteration - unauthorized modification.	Disruption (loss) - access to information is lost when it should not be.

HACKING METHODOLOGIES

Step by step approach to attack a target or computer network. (7 phases)

Footprinting	Primarily passive recon to gain information. Whois, Google, job boards and discussion forums
Scanning	Use info from footprinting to do more strategic research. Ping Sweeps, Port Scans, facility observations, etc… (NMAP)

Enumeration	Analyzing network components you discovered scanning. Compile lists of users, settings, groups, apps, and auditing this information.
System Hacking	Target specific accounts, groups, or applications and design specific attacks to gain access to a network.
Escalation of Privilege	Reassess the network once you have access and continue to gain access to or create more powerful accounts.
Covering Tracks	Remove evidence of your presence in a system. Purge server logs, etc...
Planting Backdoors	Leave behind software or accounts that allow you to return.

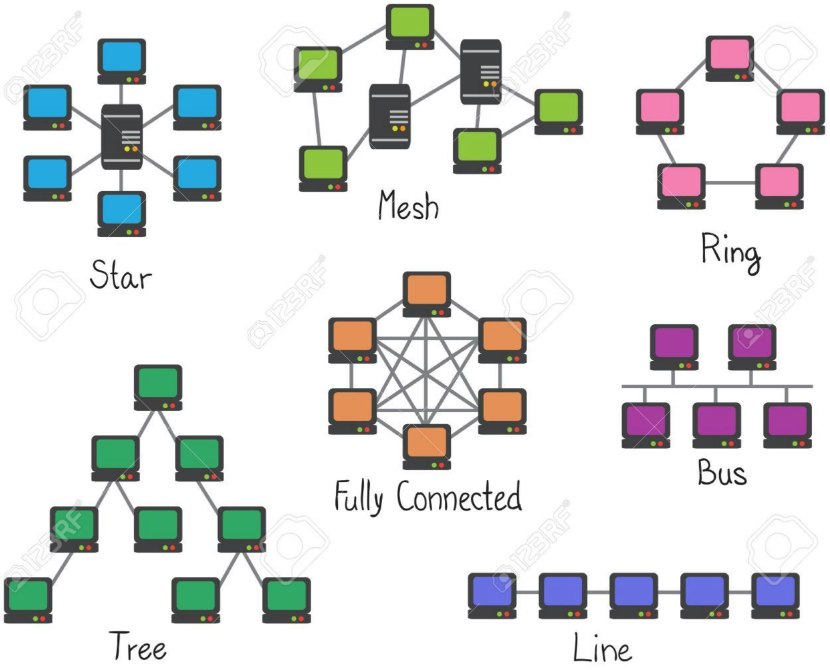
TYPES OF PEN TESTS

Insider Attack - mimic attack from authorized system user
Outsider Attack - mimic attack from outsider
Stolen Equipment Attack - mimics attack from a stolen computer
Social Engineering Attack - pen test targeting users

CEH Chapter Two: System Fundamentals

PHYSICAL TOPOLOGIES

Physical Topologies are the tangible layout of system and network hardware.



Hybrid is now the most common and may include elements of any of the above topologies.

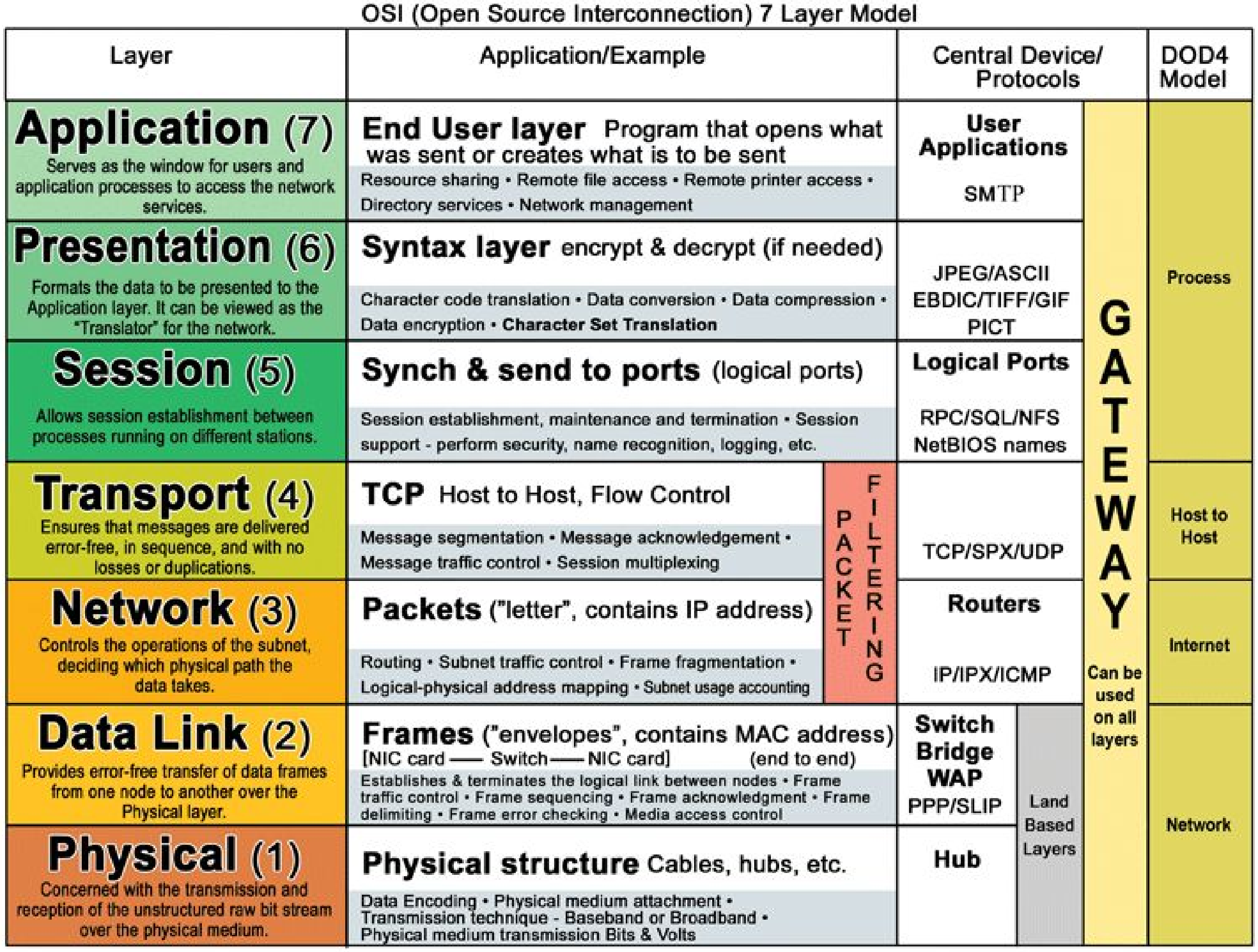
A token can be passed around for permission to transmit, or a shared media strategy can be used in which nodes listen for an opening.

Token Ring: Data Link Layer (OSI level two) network structure that uses a special three-byte frame called a token that travels around the ring. Token-possession grants the possessor permission to transmit on the medium. Token ring frames travel completely around the loop.

Shared Media: All the systems have the ability to access the physical layout whenever they need it. The main advantage in a shared media topology is that the systems have unrestricted access to the physical media. Of course, the main disadvantage to this topology is collisions.

OPEN SYSTEMS INTERCONNECTION (OSI) MODEL

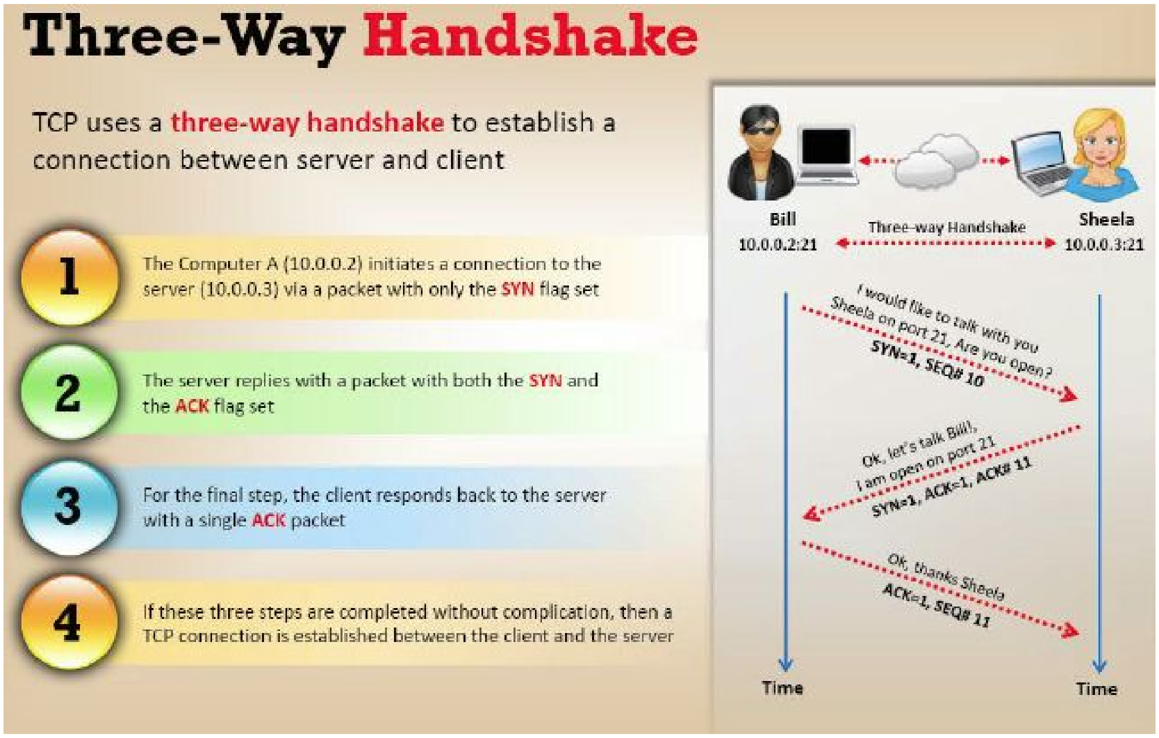
Please Do Not Teach Stupid People Acronyms



OSI (Open Source Interconnection) 7 Layer Model

Layer	Application/Example		Central Device/ Protocols			DOD4 Model
Application (7) Serves as the window for users and application processes to access the network services.	**End User layer** Program that opens what was sent or creates what is to be sent Resource sharing • Remote file access • Remote printer access • Directory services • Network management		**User Applications** SMTP		**GATEWAY** Can be used on all layers	Process
Presentation (6) Formats the data to be presented to the Application layer. It can be viewed as the "Translator" for the network.	**Syntax layer** encrypt & decrypt (if needed) Character code translation • Data conversion • Data compression • Data encryption • **Character Set Translation**		JPEG/ASCII EBDIC/TIFF/GIF PICT			
Session (5) Allows session establishment between processes running on different stations.	**Synch & send to ports** (logical ports) Session establishment, maintenance and termination • Session support - perform security, name recognition, logging, etc.		**Logical Ports** RPC/SQL/NFS NetBIOS names			
Transport (4) Ensures that messages are delivered error-free, in sequence, and with no losses or duplications.	**TCP** Host to Host, Flow Control Message segmentation • Message acknowledgement • Message traffic control • Session multiplexing	PACKET FILTERING	TCP/SPX/UDP			Host to Host
Network (3) Controls the operations of the subnet, deciding which physical path the data takes.	**Packets** ("letter", contains IP address) Routing • Subnet traffic control • Frame fragmentation • Logical-physical address mapping • Subnet usage accounting		**Routers** IP/IPX/ICMP			Internet
Data Link (2) Provides error-free transfer of data frames from one node to another over the Physical layer.	**Frames** ("envelopes", contains MAC address) [NIC card —— Switch —— NIC card] (end to end) Establishes & terminates the logical link between nodes • Frame traffic control • Frame sequencing • Frame acknowledgment • Frame delimiting • Frame error checking • Media access control		**Switch** **Bridge** **WAP** PPP/SLIP	Land Based Layers		Network
Physical (1) Concerned with the transmission and reception of the unstructured raw bit stream over the physical medium.	**Physical structure** Cables, hubs, etc. Data Encoding • Physical medium attachment • Transmission technique - Baseband or Broadband • Physical medium transmission Bits & Volts		**Hub**			

TCP/IP SUITE



Three-Way Handshake

TCP uses a three-way handshake to establish a connection between server and client

1 The Computer A (10.0.0.2) initiates a connection to the server (10.0.0.3) via a packet with only the SYN flag set

2 The server replies with a packet with both the SYN and the ACK flag set

3 For the final step, the client responds back to the server with a single ACK packet

4 If these three steps are completed without complication, then a TCP connection is established between the client and the server

IP SUBNETTING

Name	Range	Slash / CIDR
A Network	0.0.0.0-127.255.255.255	/8
B Network	128.0.0.0-255.255.255	/16
C Network	192.0.0.0-223.255.255.255	/24
Netmask for single host	255.255.255.255	/32

CLASSLESS INTER DOMAIN ROUTING TABLE

	128	**64**	**32**	**16**	**8**	**4**	**2**	**1**
	128	**192**	**224**	**240**	**248**	**252**	**254**	**255**
(A) /8	**/9**	**/10**	**/11**	**/12**	**/13**	**/14**	**/15**	**/16**
(B) /16	**/17**	**/18**	**/19**	**/20**	**/21**	**/22**	**/23**	**/24**
(C) /24	**/25**	**/26**	**/27**	**/28**	**/29**	**/30**	**/31**	**/32**

Study Subnetting info and CIDR notation here: https://quizlet.com/6869728/cidr-flash-cards/

HEX, BINARY, & DECIMAL

Decimal	Hexadecimal	Binary
0	0	0000
1	1	0001
2	2	0010
3	3	0011
4	4	0100
5	5	0101
6	6	0110
7	7	0111
8	8	1000
9	9	1001
10	A	1010
11	B	1011
12	C	1100
13	D	1101
14	E	1110
15	F	1111

PORTING

Well Known Port (1-1024)	Use	Well Known Port	Use
20-21	FTP	123	NTP
22	SSH	135	RPC - DCOM
23	Telnet	139	SMB
25	SMTP	143	IMAP
42	WINS	161-162	SNMP
53	DNS	389	LDAP
80, 8080	HTTP	445	CIFS
88	Kerberos	514	Syslog
110	POP3	636	Secure LDAP
111	Portmapper - Linux		

Registered Ports - 1025 to 49151 (Identified as usable by application running outside the user's present purview)

Port of Interest	Use	Port of Interest	Use
1080	Socks5	1521	Oracle Listener
1241	Nessus Server	2512-2513	Citrix Management
1433-1434	SQL Server	3389	RDP
1494-2598	Citrix Applications	6662-6663	IRC

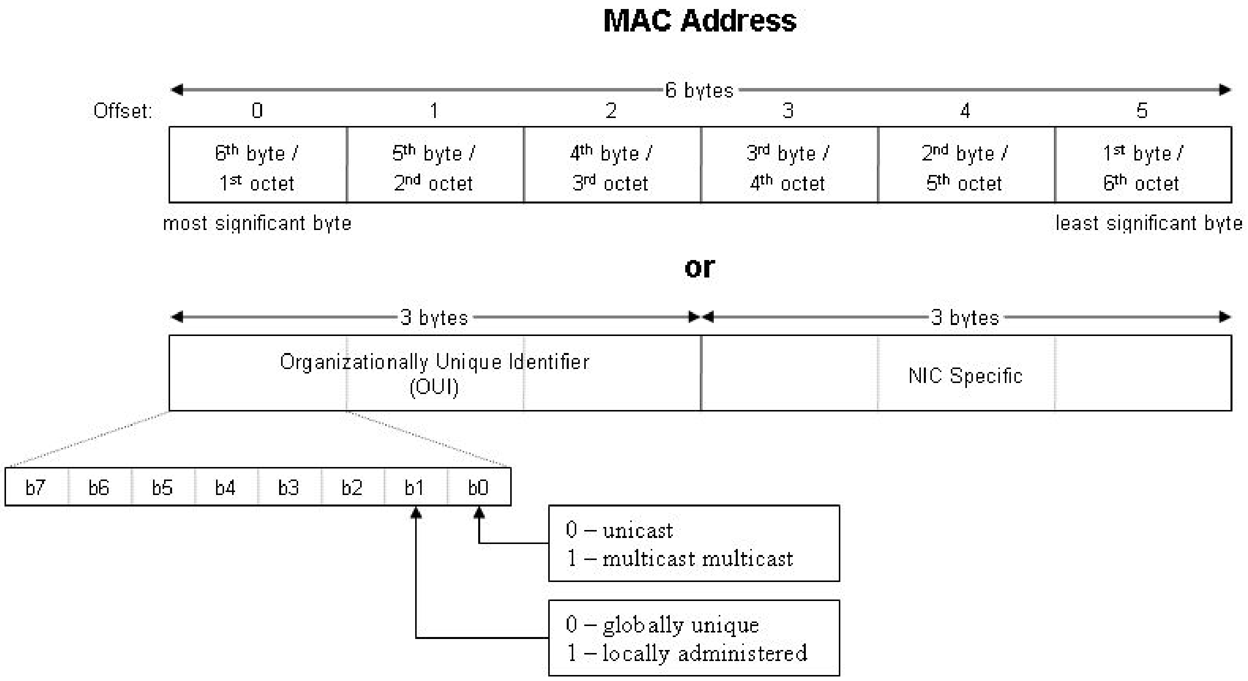
Dynamic Ports - 49152 to 65535 (Available to any TCP or UDP request made by an application)

DEVICES

Routers: Routers connect networks
A router's main function is to direct packets (layer 3 traffic) to the appropriate location based on network addressing. Routers allow different protocols on different networks to communicate and basically have in internal and external interface. Routers are responsible for Network Address Translation (NAT). This allows the internal network to be configured in any number of ways and still share a single external IP address. Routers function at level three of the OSI model, the network layer.

Switches: Switches create multiple broadcast domains
A switch's main function is to deliver data (frames) based on the media access control (MAC) address of the destination computers or devices. Switches function at level two of the OSI model, the data link layer.

Address Resolution Protocol (ARP): ARP is used to convert a network address (e.g. IP Address) to a physical address such as an ethernet address (aka MAC address). ARP has been implemented with many combinations of network and data link layer technologies. IPv4 (internet protocol version 4) over IEEE 802.3 and IEEE 802.11 is the most common case. **IEEE** stands for Institute of Electronics and Electrical Engineers. In Internet Protocol Version 6 (IPv6) networks, the functionality of ARP is provided by the Neighbor Discovery Protocol (NDP).
*Systems keep an ARP look-up table where they store information about what IP addresses are associated with what MAC addresses. When trying to send a packet to an IP address, the system will first consult this table to see if it already knows the MAC address. *If there is a value cached, ARP is not used*.
If the IP address is not found in the ARP table, the system will then send a broadcast packet to the network using the ARP protocol to ask "who has 192.168.1.1". Because it is a broadcast packet, it is sent to a special MAC address that causes all machines on the network to receive it. Any machine with the requested IP address will reply with an ARP packet that says "I am 192.168.1.1", and this includes the MAC address which can receive packets for that IP.



BROADCAST V. COLLISION DOMAINS

Broadcast Domain: Information sent across a Broadcast Domain will be broadcast to every node or device on the network.
Collision Domain: A set of LAN devices whose frames could collide with one another. This could cause packet loss or damage and require packages to be resent.
**It is possible in some cases to convert a switch into a giant hub (one huge collision domain)*

PROXIES AND FIREWALLS

Firewalls can block ports and programs that try to gain unauthorized access to your computer, while proxy servers basically hide your internal network from the Internet. A firewall essentially blocks communication, while a proxy server simply redirects it. (Firewalls can be a form of IDS)

Proxy: Proxies are intermediaries between a network and external resources, they are the only point of exposure to the open internet and are capable of filtering packets at the application (layer seven) layer.
Firewall: Three main categories

- Packet Filtering - Examine headers to determine legitimate traffic. [3]
- Stateful Packet Filtering - Determine legitimacy of traffic based on the state of the connection from which the traffic originated. [4]
- Application Proxies (See above). [7]

INTRUSION PREVENTION & DETECTION SYSTEMS

Intrusion Detection System (IDS) - Detects suspicious network activity
Intrusion Prevention System (IPS) - Reacts to threats in real time to protect network

BACKUPS AND ARCHIVING

Full backup is a method of backup where all the files and folders selected for the backup will be backed up. When subsequent backups are run, the entire list of files and will be backed up again. The advantage of this backup is restoration is fast and easy as the complete list of files are stored each time. The disadvantage is that each backup run is time consuming as the entire list of files is copied again. Also, full backups take up a lot more storage space when compared to incremental or differential backups.

Incremental backup is a backup of all changes made since the *last backup*. With incremental backups, one full backup is done first and subsequent backup runs are just the changes made since the last backup. The result is a much faster backup then a full backup for each backup run. Storage space used is much less than a full backup and less than with differential backups. Restores are slower than with a full backup and a differential backup.

Differential backup is a backup of all changes made since the last *full backup*. With differential backups, one full backup is done first and subsequent backup runs are the changes made since the last full backup. The result is a much faster backup then a full backup for each backup run. Storage space used is much less than a full backup but more than with Incremental backups. Restores are slower than with a full backup but usually faster than with Incremental backups.

REVIEW

Routers work at layer 3 by directing packets and connecting different networks.
Switches create a **collision domain** for each port; **broadcast domains** allow traffic to be broadcast to all connected nodes. **Proxies** work at ath application layer and can be used for caching and filtering of web content. **Proxy firewalls** can be detailed in what they filter.
A **packet filtering firewall** looks only at the header of the packet. A **stateful firewall** verifies legitimacy between client and server. **IPSs** are active and responsive, **IDS** detect and report.

RELATED TOOLS

tcpdump : list all packages on network (similar to wireshark)
arp -a : list all registered mac addresses on network
ifconfig : interface configuration. The utility is a command line interface tool and is also used in the system startup scripts of many operating systems. It has features for configuring, controlling, and querying TCP/IP network interface parameters.

CEH Chapter Three: Cryptography

Cryptography relates to protection of information in all of its forms. Safeguard *confidentiality* and *integrity* of information.

CONFIDENTIALITY
ACCOUNTABILITY
CIA
TRIAD
INTEGRITY

Confidentiality is the primary goal of cryptography and is achieved through *encryption.*
Integrity is another goal of cryptography as it can help detect changes in information through *hashing.*
Authentication allows a person or device to be positively identified. Authentication allows the ability to validate that a particular message originated from a source that is a known entity which, by extension can be trusted.
Nonrepudiation means to ensure that a transferred message has been sent and received by the parties claiming to have sent and received the message. Nonrepudiation is a way to guarantee that the sender of a message cannot later deny having sent the message and that the recipient cannot deny having received the message.This is accomplished most commonly with digital signatures.
Key Distribution Keys represent the specific combination or code used to encrypt or decrypt data.

APPLIED CRYPTOGRAPHY

Public Key Infrastructure (PKI)	a set of hardware, software, people, policies, and procedures needed to create, manage, distribute, use, store, and revoke digital certificates and manage public-key encryption.
Digital Certificates	are also called public key certificates and are electronic document used to prove ownership of a public key.
Authentication	the process of determining whether someone or something is, in fact, who or what it is declared to be
E-Commerce	Cryptography used to protect and verify financial transactions online
RSA	an algorithm used by modern computers to encrypt and decrypt messages. It is an asymmetric (public key) cryptographic algorithm. Built into most current operating systems.
MD-5	message-digest algorithm is a widely used cryptographic hash function producing a 128-bit (16-byte) hash value, typically expressed in text format as a 32 digit hexadecimal number. MD5 has been utilized in a wide variety of cryptographic applications, and is also commonly used to verify data integrity.
Secure Hash Algorithm (SHA)	The Secure Hash Algorithm is a family of cryptographic hash functions published by the National Institute of Standards and Technology (NIST) as a U.S. Federal Information Processing Standard (FIPS), including sha-0, sha-1, sha-2, sha-3
Secure Socket Layer (SSL)	a standard security technology for establishing an encrypted link between a server and a client—typically a web server (website) and a browser; or a mail server and a mail client (e.g., Outlook).

Pretty Good Privacy (PGP)	a data encryption and decryption computer program that provides cryptographic privacy and authentication for data communication. PGP is often used for signing, encrypting, and decrypting texts, e-mails, files, directories, and whole disk partitions and to increase the security of e-mail communications. It was created by Phil Zimmermann in 1991.
Secure Shell (SSH)	a cryptographic (encrypted) network protocol for initiating text-based shell sessions on remote machines in a secure way. This allows a user to run commands on a machine's command prompt without them being physically present near the machine. It also allows a user to establish a secure channel over an insecure network in a client-server architecture, connecting an SSH client application with an SSH server. Common applications include remote command-line login and remote command execution, but any network service can be secured with SSH.

TERMS

Plaintext - the original message passed as is
Ciphertext - data that has been transformed into a different format using an algorithm
Algorithm (**cipher**) - a formula that includes discrete steps that describe how the encryption and decryption process is to be performed in a given instance
Keys - discrete piece of information that is used to determine the result or output of a given cryptographic operation.

CRYPTOGRAPHY Types

Symmetric cryptography refers to any system which uses a single key to encrypt and decrypt.
Common Examples:

Data Encryption Standard (DES)	56 bit key algorithm used by US gov in 77. Key is too short to be useful today.
Triple DES (3DES)	168 bit key, 3 times more powerful than DES
Blowfish	448 bit key optimized for 32 bit and 64 bit processors. (DES is not). Designed by Bruce Schneier.
International Data Encryption Algorithm (IDEA)	Swiss; used in PGP.
MARS*	128-256 bit keys, AES finalist, built by IBM
RC2	1-2048 bit keys, developed by RSA labs, public in 1996. Exports limited to 40 bits so NSA could spy foreign communications
RC4	1-2048 bit keys. Another RSA project revealed in ‘94.
RC5	User defined key length
RC6*	128-256 bit keys, RSA labs AES finalist

Advanced Encryption Standard (AES) [Rijndael]	128, 192, 256 bit keys. Successor to DES chosen by NIST as new US standard
Serpent	128-256 bit keys, AES finalist
Twofish	128-256 bit keys, AES candidate by Bruce Schneider

***Advanced Encryption Standard (AES)**: a competition organized by the National Institute of Standards and Technology (NIST) to specify an unclassified, publicly disclosed encryption algorithm capable of protecting sensitive government information well into the next century.

Asymmetric (public key) cryptography - added benefits of nonrepudiation and key distribution. Each person who participates has two keys assigned to them, a public and private key. Public key may be published but private keys will only be available to respective assigned users.
Both public and private keys can be used to encrypt a message, but only the key's inverse can be used to decrypt. Theoretically, with PKI anyone with access to the public key can send an encrypted message, and only the holder of the private key could decrypt the message. The opposite also applies, a private key holder's identity can be verified because only the public key associated with the private key will decrypt the message.

Hash Function - any function that can be used to map digital data of arbitrary size to digital data of fixed size. The values returned by a hash function are called hash values, hash codes, hash sums, or simply hashes. Verification is completed when a message is received by the intended party and the hashing process is repeated. If the sender hash matches the recipient hash, the document has not been altered in any way.

But, how do you know who has a key?

Certification Authority - entity that issues digital certificates (public keys). A digital certificate certifies the ownership of a public key by the named subject of the certificate. A CA is a trusted third party that is responsible for issuing, managing, identifying and revoking certificates as well as enrolling parties for their own certificates. CAs verify identity of any cert holder. A CA issues credential to banks, web mail, VPNs, smart cards, etc…

Digital Certificates - A cryptographically sealed object containing various information that binds a key pair with a particular subscriber. Cert may include Version, Serial Number, Algorithm ID, Issuer, Validity, Not Before (initiation), Not After (expiration), Subject, Public Key, Public Key Info and Algorithm
Certificates are signed by generating a hash value and encrypting it with the issuer's private key. If the public key is altered, the certificate is rendered invalid. Else if the client has the issuer's public key, the certificate's (and therefore sender's) authenticity is verified. In this way a certificate allows you to associate the public key with a particular service, such as an e-commerce web server.

Steps for CA to issue Certificate:

1. Request is received
2. Background info is requested by CA and validated
3. Requester info is applied to certificate
4. CA hashes Certificate
5. Issuing CA signs certificate with their private key
6. The Requester is informed that the key is ready for pickup
7. Requester installs certificate on their computer or device

CERTIFICATE AUTHORITY ROLES

Generation of Key Pair - Creates and distributes public key and gives private key to requesting party

Generation of Certificates - Verification of identity and generation of certificate

Publication of Public Key - Each certificate is bound to a public key. Anyone who trusts the CA or requests the public Key will receive it

Validation of Certificates - When one party presents certificate to another, third party validates identity

Revocation of Certificates - Revoked at expiration or earlier if requested

Root CA - Initiates all trust paths. Root CA is at the top and must be protected, if it is compromised, all other systems are invalid

Trusted Root CA - a CA which is added to an application such as a browser by the software vendor. It means the software vendor who made the browser trusts the CA.

Peer CA - Provides a self-signed certificate that is distributed to its certificate holders and used by them to initiate certification paths.

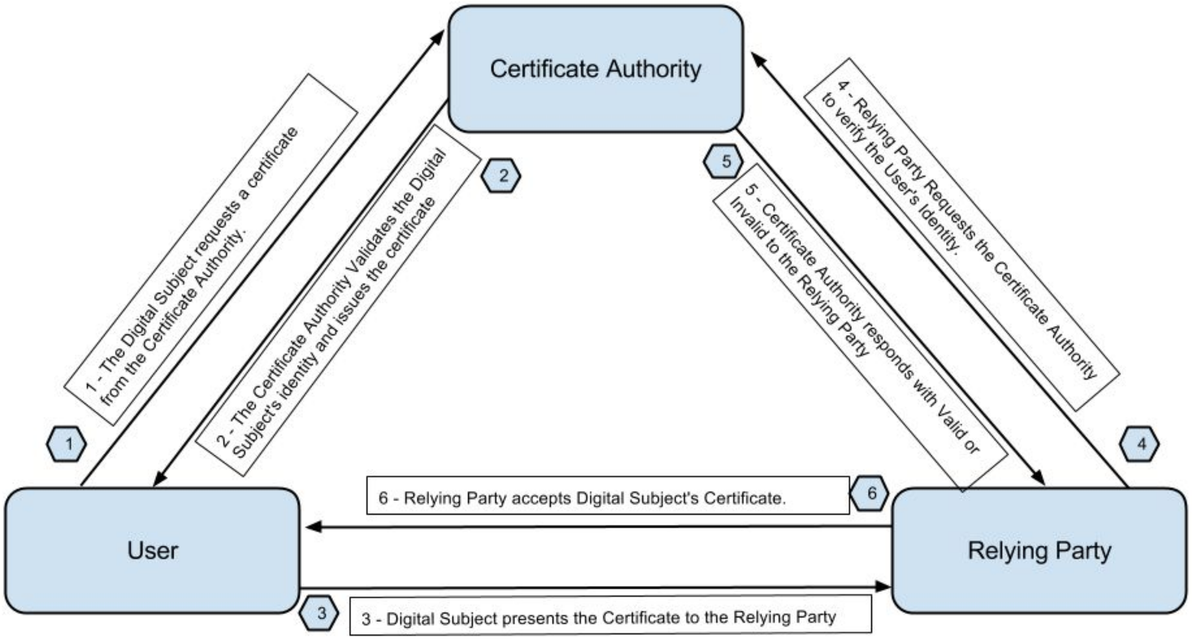
Subordinate CA (Child CA) - CAs that are not root CAs are considered subordinate. The first subordinate CA in a hierarchy obtains its CA certificate from the root CA. This first subordinate CA can, in turn, use this key to issue certificates that verify the integrity of another subordinate CA. These higher subordinate CAs are referred to as intermediate CAs or policy CAs. An intermediate CA is subordinate to a root CA, but also serves as a higher certifying authority to one or more subordinate CAs.

Registration Authority - CA Assistant -- does not generate certificates but verifies ID and collects information for CA.

PKI STRUCTURE

A PKI is a group of technologies designed to validate , issue, and manage certificates on a large scale. Ultimately a PKI is a security architecture that you can use to provide an increased level of confidence for exchanging information over an insecure medium. Components:

Public/Private Key Encryption	Digital Certificates	Hashing


Certificate Authority
User
Relying Party
1
1 - The Digital Subject requests a certificate from the Certificate Authority.
2
2 - The Certificate Authority Validates the Digital Subject's identity and issues the certificate
3
3 - Digital Subject presents the Certificate to the Relying Party
4
4 - Relying Party Requests the Certificate Authority to verify the User's Identity.
5
5 - Certificate Authority responds with Valid or Invalid to the Relying Party
6
6 - Relying Party accepts Digital Subject's Certificate.

The first step of validating a certificate is to first verify the certificate's integrity. This is done by first creating a one way hash of the certificate contents (using the hash algorithm indicated in the certificate). This hash is stored temporarily in memory. Next, the digital signature embedded in the certificate is decrypted using the public key included in the certificate (or, for Certificate Authority issued certificates using the Public Key from the Certificate Authority root certificate). The decrypted Digital Signature (which is again a hash of the certificate contents) is then compared to the hash that was computed locally. If the hashes match, then the user knows that the certificate has not been altered since it was created.

HASHING

Hashing is the transformation of a string of characters into a usually shorter fixed-length value or key that represents the original string.

Message Digest 2 (MD2)	One way hash function used in privacy-enhanced mail (PEM)
Message Digest 4 (MD4)	One way hash used for PGP -- largely replaced by MD5
Message Digest 5 (MD5)	Improved MD4 generates 128 bit hash -- largely replaced by SHA2

Message Digest 6 (MD6)	Hashing Algorithm by Ron Rivest
HAVAL	Variable length one-way modification of MD5
Whirlpool	Hashing Algorithm designed by creators of AES
Tiger	Hash designed for 64 bit systems
RIPE-MD	Common European hashing algorithm
Secure Hash Algorithm - 0 (SHA-0)	Used before SHA-1
Secure Hash Algorithm - 1 (SHA-1)	Common hashing Algorithm - has been broken
Secure Hash Algorithm - 2 (SHA-2)	Upgraded SHA-1

CRYPTOGRAPHY VULNERABILITIES & ATTACKS

Brute Force - attempt every possible combination of characters
Ciphertext Only Attack - Attacker has ciphertext, but no plain text. Low success.
Known Plaintext - Attacker has plaintext and ciphertext for one or more messages. Similar to brute force but slightly better informed.
Chosen Plaintext Attack - Attacker can generate corresponding ciphertext for acquired plaintext. May not know secret key or algorithm.

APPLICATIONS

Internet Protocol Security (**IPSec**) is an end-to-end security scheme operating in the Internet Layer (network, OSI level 3) of the Internet Protocol Suite, while some other Internet security systems in widespread use, such as Transport Layer Security (TLS) and Secure Shell (SSH), operate in the upper layers at Application layer.

Two mechanisms:

- Authentication Header (AH) - Authenticates sender of data
- Encapsulating Security Payload (ESP) - Authentication info and encrypt data

CEH Chapter 4: Footprinting and Reconnaissance

STEPS OF ETHICAL HACKING

1. Footprinting: collecting data about the TOE that is exposed
    a. IP Address Ranges
    b. Namespaces
    c. Employee Information
    d. Phone Numbers
    e. Facility Information
    f. Job Information

2. Scanning (chapter 5): Actively engaging the target to obtain more information. Common tools include the following.
    a. **Pings** - query (another computer on a network) to determine whether there is a connection to it. Ping operates by sending Internet Control Message Protocol (ICMP) echo request packets to the target host and waiting for an ICMP echo reply.
    b. **Ping Sweeps** - (aka ICMP sweep) is a basic network scanning technique used to determine which of a range of IP addresses map to live hosts (computers).
    c. **Port Scan** - probing a server or host for open ports. This is often used by administrators to verify security policies of their networks and by attackers to identify running services on a host with the view to compromise it.
    d. **Traceroute** - a computer network diagnostic tool for displaying the route (path) and measuring transit delays of packets across an Internet Protocol (IP) network.
3. Enumeration (chapter 6): Systematic probing of a target with the goal of obtaining user lists, routing tables, and protocols from the system. Info like shares, users, groups, applications, protocols, and banners are all useful moving forward into the attack phase. Information includes the following:
    a.

Usernames	Group Info	Passwords	Hidden Shares	Device Info
Network Layout	Protocol Info	Server Data	Service Info	And More...

4. System Hacking (chapter 7: Using the information you have gathered to gain access to a system. Includes cracking passwords, escalating privileges, executing applications, hiding files, covering tracks, concealing evidence, and building backdoors for a complex attack.

FOOTPRINTING

Footprinting is reconnaissance: a method of observing and collecting information about potential targets with the intention of finding a way to attack the target. Footprinting looks for information and later analyzes it, looking for weaknesses or potential vulnerabilities. Footprinting is about gathering information and formulating a hacking strategy.

Steps:

1. Collect publicly available info like hosting and network.
2. Ascertain the OS in the environment -- especially server and application data
3. Use Whois, DNS, network and organizational queries
4. Locate vulnerabilities

Targets:

1. Network Information:
    a. Internal and external domain names, IP addresses, Unmonitored websites, Private Websites, TCP/UDP services, Access Control Systems, Firewalls, Virtual

Private Networks (VPN), Intrusion detection and prevention information, Telephone Numbers, Voice Over IP (VOIP), Authentication Systems

2. Operating Systems Info: Determine as much as possible about the OS, updates and version. Things to compile:
    a. Group Info and Names
    b. Banner grabbing is an enumeration technique used to glean information about a computer system on a network and the services running on its open ports.
    c. Routing Tables: A routing table is a set of rules, often viewed in table format, that is used to determine where data packets traveling over an Internet Protocol (IP) network will be directed. All IP-enabled devices, including routers and switches, use routing tables.
    d. SNMP: Simple Network Management Protocol (SNMP) is a popular protocol for network management. It is used for collecting information from, and configuring, network devices, such as servers, printers, hubs, switches, and routers on an Internet Protocol (IP) network.
    e. System Architecture: conceptual model that defines the structure, behavior, and views of a system.
    f. Remote System Data
    g. System Names and Passwords
3. Organization Data: Learn about employees, operations, projects, and other ongoings at the organization
    a. Employee details, organization's website, company directory, location details, address and phone numbers, comments in HTML, security policies, relevant server links, background, articles and news.

TERMINOLOGY

Passive (**open source**) **Information Gathering**: OS, network, public IP, web server, TCP/UDP
Active Information Gathering: Actively (usually through social engineering) discovering more about the TOE. Calling recruiters to ask about job openings, hiring managers, interviews and people at the bar.

FOOTPRINTING THREATS

Social Engineering: Request or manipulate people for information
Network and System Attack: Gather info related to an environment's system configuration and operating system.
Information Leakage:
Privacy Loss: Hackers disclosing information on a system to others
Revenue Loss: Loss of trust can easily cost large amounts of money

subdomain.domainname.topleveldomain
example.site.com

TOOLS

NETCRAFT: Suite of tools to find IP, server version, subnet data, OS, and subdomains
Link Extractor: Tool to extract internal and external links for a given location
EDGAR: Electronic Data-Gathering Analysis and Retrieval System at http://www.sec.gov/edgar/searchedgar/webusers.htm: info on publicly traded companies.
LexisNexis: Publicly record info database.

Google Hacking

site:	Get results from certain sites or domains. Examples: olympics site:nbc.com and olympics site:.gov
link:	Find pages that link to a certain page. Example: link:youtube.com
related:	Find sites that are similar to a web address you already know. Example: related:time.com
OR	Find pages that might use one of several words. Example: marathon OR race
info:	Get information about a web address, including the cached version of the page, similar pages, and pages that link to the site. Example: info:google.com
cache:	See what a page looks like the last time Google visited the site. Example: cache:washington.edu

https://www.exploit-db.com/google-hacking-database/ <-Great resource on Google Hacking

Chapter Five: Scanning Networks

PRIMARY OBJECTIVES

- List IP Addresses and open/closed ports
- Information on the OS and the System Architecture
- Services or processes on live hosts

MAIN TYPES OF SCANNING

1. **Port Scanning**: send specific packets to a TOE with the intention of learning more about it. Typically these scans target ports 0-1024. Generally, the idea is to map out different assets like mail servers, domain controllers, and web servers and distinguish between the two.
    a. NMAP - main port scanning software

2. **Network Scanning**: locate all live hosts on a network. Generally the goal is to targets for later attack or further evaluation.
3. **Vulnerability Scan**: identify weaknesses or vulnerabilities on a target system.

FIND LIVE SYSTEMS

War-Dialing: Dialing a block of phone numbers to find live hosts. Good way to target backup systems to gain access to systems, firewalls, routers, and fax machines.

- ToneLoc: randomly dial numbers in a range.
- THC-SCAN: DOS based program that can use a modem to dial ranges in search of carrier functions for fax or modem.
- NIKSUN's PhoneSweep: Commercial wardialing.

PROS	CONS
People pay no attention to these devices, they are typically completely off the radar.	Rarely used, much less for anything important these days.

War-Driving: Driving around with a laptop looking for wireless access points (WAP).

- AirSnort: Wireless Cracking Tool.
- AirSnare: and IDS that monitors your wireless networks. Notifications for unapproved devices.
- Kismet: Wireless network detector, sniffer, and IDS primarily found on Linux
- NetStumbler: Wireless network detector.
- inSSIDer: Wireless Network Director and access point mapper.

Pinging (**Ping Sweep**): Send an Internet Control Message Protocol (ICMP) message to detect whether a system is live or not. No response to a ping on a hostname could indicate a DNS issue, while pings to an IP will always determine a live host.
See Also: Common NMAP Commands, Nmap 6: Network Exploration and Security Auditing Cookbook, nmap cheat sheet

TCP Flags:

SYN	Initiate connection between hosts
ACK	Acknowledge receipt of a packet
URG	Indicate packet contains important information and should be processed immediately
PSH	Send all buffered data immediately
FIN	Close connection / indicate that no more data will be sent
RST	Reset the connection

Port Scanner: software application designed to probe a server or host for open ports. This is often used by administrators to verify security policies of their networks and by attackers to identify running services on a host with the view to compromise it

Packet Crafter: utility designed to create packet with flags you specify HPING2 and HPING3 allow you to do this. hping is a command-line oriented TCP/IP packet assembler/analyzer. The interface is inspired to the ping(8) unix command, but hping isn't only able to send ICMP echo requests. It supports TCP, UDP, ICMP and RAW-IP protocols, has a traceroute mode, the ability to send files between a covered channel, and many other features.

Fragmenting: breaking a packet into multiple pieces which will not be recognized by an IDS.
Nmap fragmenting flags:

- -sS: SYN Scan (Default)
- -A: Enable OS detection, version detection, script scanning, and traceroute
- -f: Scan most common ports (Fast)

See also: **Fragtest** and **Fragroute**

TYPES OF SCANS

Full Open Scan: systems involved initiate and complete a three-way handshake. Gives proof that the system is live, but also documents you scanning it.

Stealth / Half Open Scan: (1)Attacker sends a SYN packet, if a SYN-ACK packet is received in return, the port is open and the attacker sends a RST packet to terminate the connection. (2) if the victim port is closed, it sends the attacker a RST packet to indicate that it is not taking connections. This is less likely to be detected, but may have false positives because confirmation is not received.

Xmas Tree Scan: Scan that sends all packet flags except PSH. Send packet with ACK, SYN, URG, RST and FIN all flagged. This is an illegal/illogical combination. The server will either drop the packet or ignore it; this could indicate an open port. A single RST in response tells you the port is closed. (-sX)

FIN Scan: Attacker sends packet with FIN flag. Results are similar to Xmas Tree; closed ports return RST packets. (-sF)

NULL Scan: Attacker sends packet with no flags. Closed ports return RST. Open may vary as in Xmas and FIN scans.

ACK Scan: Test whether any filtering is being done on the port. Filtering indicates the presence of a stateful firewall. (-sA -P0)

UDP Scan: If TCP is not being used. (-sU)

UDP Scan results in open and closed ports

Open	No Response
Closed	ICMP Port Unreachable Message

OS FINGERPRINTING

Active V. Passive Fingerprinting

	Active	Passive
How it Works	Uses specially crafted packets.	Sniffs packets coming from the system.
Analysis	Responses are compared with DB of known responses.	Responses are analyzed looking for OS details.
Chance of Detection	High, introduces new traffic.	Low, examines existing traffic.

BANNER GRABBING

A *banner* is what a service returns to the requesting program to give information about the service itself. HTTP banners usually include type of server software, version number, and date of last modification.

Banner Grabbing: an enumeration technique used to glean information about a computer system on a network and the services running on its open ports. Administrators can use this to take inventory of the systems and services on their network.

Tools: Netcraft, Xprobe, p0f

COUNTERMEASURES

Disable or change information exposed in the banner with IIS Lockdown, ServerMask, etc…

Hide file extensions on web pages (.asp, .php, .jsp, etc…). Conceal the technology used to generate the page.

SUMMARY

Scanning is designed to reveal the nature of system networks as well as the vulnerabilities that are present in the environment.

Targets may have vulnerable resources based on OS, network design, and environment.

Countermeasures may be taken to protect systems from disclosing information.

Tools are extremely important for scanning, know how to use them, especially NMAP.

CEH Chapter Six: Enumeration of Services

Enumeration: the process of extracting information from a target system in an organized and methodical manner.

Enumeration Targets:

- Network resources and Shares
- Users and Groups
- Routing Tables
- Auditing and Service Settings
- Machine Names
- Applications and Banners
- SNMP and DNS Details

Common Approaches:

- Extract info from E-mail IDs: Username and Domain Names
- Use Default Passwords
- Brute - Force Attacks on Directory Services - Directory service is a database that contains information used to administer the network. Many directories are vulnerable to input verification deficiencies as well as other holes that may be exploited to discover and compromise user accounts.
- Exploiting SNMP - Simple Network Management Protocol (SNMP) can be exploited by an attacker who can guess the strings and use them to extract usernames.
- Working with DNS Zone Transfers - DNS zone transfer, also sometimes known by the inducing DNS query type AXFR, is a type of DNS transaction. A zone transfer uses the Transmission Control Protocol (TCP) for transport, and takes the form of a client–server transaction. The client requesting a zone transfer may be a slave server or secondary server, requesting data from a master server, sometimes called a primary server. The portion of the database that is replicated is a zone. Capturing the zone allows insight to network mapping.
- Capturing User Groups - extracting user accounts from specified groups, storing the results, and determining whether the session accounts are in the group.

WINDOWS RUNDOWN

Users: the item most responsible for controlling access to the system is the user object. Processes in Windows are run under one of the following user contexts:

- Local Service: A user account with higher than normal access to the local system but only limited access to the network.
- Network Service: A user account with normal access to the network but only limited access to the local system.
- System: A Super-User (sudo) style account that has nearly unlimited access to the local system.
- Current User: The currently logged-in user who can run applications and tasks but is still subject to restriction that other users are not subject to. These restrictions hold true even in the case of admin account use.

Each is used for specific reasons. In a typical session, each is running different processes behind the scenes to keep the system performing.

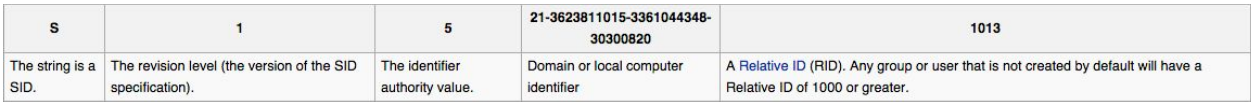
Groups: Groups are used to grant access to resources and simplify management by enabling management of multiple users.

- Anonymous Logon: Allows anonymous access to resources, typically used when accessing web server or web application.
- Batch: Batch jobs or scheduled tasks like deleting temp files
- Creator Group: grants access to users who are members of the same groups as the creator of a file or directory
- Creator Owner: Person who created the file or directory

- Everyone: All interactive, network, dial-up, and authenticated users. Group provides wide access to resources.
- Interactive: Any user logged on to the local system, allows only local users to access a resource.
- Network: Any user accessing the system through a network has the Network Identity, which allows only remote users to access a resource.
- Restricted: Users and computers with restricted capabilities have the restricted identity. A local user who is a member of the Users Group (rather than the Power Users Group) has this identity.
- Self: refers to the object and allows the object to modify itself.
- Service: Any service accessing the system. Grants access to processes being run by Windows.
- System: Used when the OS needs to perform a system level function.
- Terminal Server Use: Allow Terminal Server users to access Terminal Server applications.

SECURITY IDENTIFIERS (SID)

SID: a unique, unalterable identifier of a user, user group, or other security *principal. A security principal has a single SID for life, and all properties of the principal, including its name, are associated with the SID. This design allows a principal to be renamed (for example, from "John" to "Jane") without affecting the security attributes of objects that refer to the principal.
***Principal**: individual people, computers, services, computational entities such as processes and threads, or any group of such things.
Think of a SID as a primary key in a database, it remains the same even if a username changes. The SID is used in every situation where permissions need to be checked.
Example format of a SID: "S-1-5-21-3623811015-3361044348-30300820-1013"



S	1	5	21-3623811015-3361044348-30300820	1013
The string is a SID.	The revision level (the version of the SID specification).	The identifier authority value.	Domain or local computer identifier	A Relative ID (RID). Any group or user that is not created by default will have a Relative ID of 1000 or greater.

SERVICES AND PORTS OF INTEREST

Ports to pay close attention to:

TCP 53	DNS Zone Transfers that keep servers up to date with the latest zone data
TCP 135	Facilitates communication for client-server applications like allowing Microsoft Outlook and Microsoft Exchange
TCP 137	NetBIOS Name Service (NBNS) - provides name resolution involving NetBIOS protocol. Allows NetBIOS to associate names and IP addresses of individual systems and services. i.e. Easy Target
TCP 139	NetBIOS Session Service (SMB over NetBIOS) allows management of connections between NetBIOS-enabled clients and applications. Used by NetBIOS to create and tear down connections.
TCP 445	SMB over TCP, or Direct Host improves network access and bypasses NetBIOS.

UDP 161 and 162	SNMP is a protocol used to manage and monitor network devices and hosts. Facilitates messaging, monitoring, auditing, etc… Listening (161). Traps Received (162).
TCP/UDP 389	Lightweight Directory Access Protocol (LDAP) is used to exchange info between two parties. Common examples are Exchange and Active Directory.
TCP/UDP 3268	Global Catalog System is used to locate information in Microsoft's Active Directory
TCP 25	Simple Mail Transfer Protocol (SMTP) used for the transmission of messages in the form of email across networks.

COMMON EXPLOITS

During normal operation, a service in windows know as NetBIOS over TCP/IP will resolve NetBIOS names to IP addresses. **nbtstat** is designed to locate problems with this service. The utility also can return names registered with the Windows Internet Naming Service (WINS).

nbtstat flags

-a	Returns NetBIOS name table and mandatory access control (MAC) address of the card for the computer name specified
-A	-a info but accepts IP address as input
-c	List the contents of the NetBIOS name cache
-n	Names: display names registered locally by NetBIOS applications such as the server and redirector
-r	Resolved: Displays count of all names resolved by broadcast or the WINS server
-s	Sessions: Lists the NetBIOS sessions table and converts destination IP addresses to computer NetBIOS names
-S	Sessions: Lists the current NetBIOS sessions and their status, along with the IP address

NULL Session - an anonymous connection to a freely accessible network share called IPC$ on Windows-based servers. It allows immediate read and write access with Windows NT/2000 and read-access with Windows XP and 2003.
Basically a NULL session is something that occurs when a connection is made to a Windows system that allows information about system shares or user accounts without credentials like username and password being provided.
NULL sessions can only be made to an **interprocess communication** (**IPC**) - a set of programming interfaces that allow a programmer to coordinate activities among different program processes that can run concurrently in an operating system.
Commonly enumerated information from this process:

- List of Users and Groups
- List of Machines
- List of Shares
- Users and host SIDs

Use NULL session exploit assuming hostname “zelda”:
net use \\zelda/ipc$ “/user:”
net view \\zelda -- view shares available on the system
net use s: \\zelda/(shared folder name) -- view the contents of the folder by browsing the S: drive

SuperScan - Windows based utility to scan NetBIOS name table, NULL session, MAC addresses, Workstation types, Users, Groups, Remote Procedure call (RPC) endpoint dump, Account policies, Shares, Domains, Logon sessions, Trusted domains, Services
http://www.mcafee.com/us/downloads/free-tools/superscan.aspx

PsTools - Modeled after unix based ps cli tool to manage remote and local systems
PsExec - execute processes remotely
PsFile - shows files opened remotely
PsGetSid - display the SID of a computer or a user
PsInfo - list information about a system
PsPing - measure network performance
PsKill - kill processes by name or process ID
PsList - list detailed information about processes
PsLoggedOn - see who's logged on locally and via resource sharing (full source is included)
PsLogList - dump event log records
PsPasswd - changes account passwords
PsService - view and control services
PsShutdown - shuts down and optionally reboots a computer
PsSuspend - suspends processes
PsUptime - shows you how long a system has been running since its last reboot (PsUptime's functionality has been incorporated into PsInfo)

SNMP ENUMERATION

Simple Network Management Protocol (SNMP) is a popular protocol for network management. It is used for collecting information from, and configuring, network devices, such as servers, printers, hubs, switches, and routers on an Internet Protocol (IP) network. Application layer (OSI layer 7) operating on UDP. There are three versions:
SNMPv1 - first standardized protocol to manage networked devices. Low Security
SNMPv2 - introduced new management functions and security. Backwards compatible.
SNMPv3 - latest version, security focused

- *Authentication* - ensure traps are only read by intended recipient
- *Privacy* - encrypt payload of SNMP message

Can be accessed on most OS including Linux, Unix, & Windows. Requires TCP/IP.

The SNMP system has two components, the *agent* (located on the managed/monitored device) and the *management station* (which communicates with the agent).

Process:

1. SNMP management station sends request to agent.
2. Agent receives request and sends back reply with traps on occurrences.

Management Information Base (**MIB**) - Database that contains descriptions of the network objects that can be managed through SNMP. MIB elements are recognized with object identifiers.

- *Scalar* - single object instance
- *Tabular* - groups of related object instances

Typically there are two passwords to interact with information from an agent:

- Read Community String
  - Configuration of device can be *read* with this password
  - These are public
- Read/Write Community String
  - Configuration of device can be *changed* with this password
  - These are private

With SNMP, one can find: Network Resources like hosts, routers, and devices, shares, ARP tables, Routing Tables, Device Specifics, and Traffic Stats.

Tools: SolarWind’s IP Network Browser and SNMPUtil

SNScan - utility designed to detect devices on a network enabled for SNMP.

UNIX AND LINUX ENUMERATION

Common tools:

finger: finger command returns info about a user on a given system. Returns home directory, login time, idle times, office location, and last time they read/received mail

finger <switches> username

rpcinfo: enumerates info exposed over the Remote Procedure Call (RPC) protocol

rpcinfo <switches> hostname

showmount: lists and identifies the shared directories present on a given system. showmount displays a list of all clients that have remotely mounted a file system.

/usr/sbin/showmount [- ade] [hostname]

enum4linux: enum4linux is a tool for enumerating information from Windows and Samba systems. More information available at: https://labs.portcullis.co.uk/tools/enum4linux/

LDAP & DIRECTORY SERVICE ENUMERATION

Lightweight Directory Access Protocol (LDAP) is used to interact with and organize databases. LDAP is used in Active Directory, Novell eDirectory, OpenLDAP, Open Directory, Oracle iPlanet

NTP ENUMERATION

Network Time Protocol (NTP) - (UDP port 123) syncs clocks across hosts on a network. Very important for logging into directory services. Commands:

- ntpdate - deprecated computer program used to quickly synchronize and set computers' date and time by querying a Network Time Protocol (NTP) server
- ntptrace - trace ntp back to primary
- ntpq - The ntpq utility program is used to query NTP servers which implement the recommended NTP mode 6 control message format about current state and to request changes in that state. ntpq can also obtain and print a list of peers in a common format by sending multiple queries to the server

SMTP ENUMERATION

SMTP sends messages between servers that send and receive email.

*Versions of Windows after XP do not include telnet client, it must be downloaded.

VRFY and EXPN ask the server for information about an address. They are inherently unusable through firewalls, gateways, mail exchangers for part-time hosts, etc.

VRFY

A VRFY request asks the server to verify an address. Its parameter may be an encoded address or a user name in a server-defined format.
If the server accepts the request (required code 250, 251, or 252), it may provide information about the address in a server-defined format. 250 typically means that the address is valid, 251 typically means that mail to the address is forwarded, and 252 means that the server doesn't know whether the address is valid.

EXPN

EXPN asks the server for the membership of a mailing list. Its parameter may be an encoded address or a list name in a server-defined format. If the server accepts the request (required code 250), its response text shows each subscriber to the mailing list, one per line, in a server-defined format.

RCPT TO

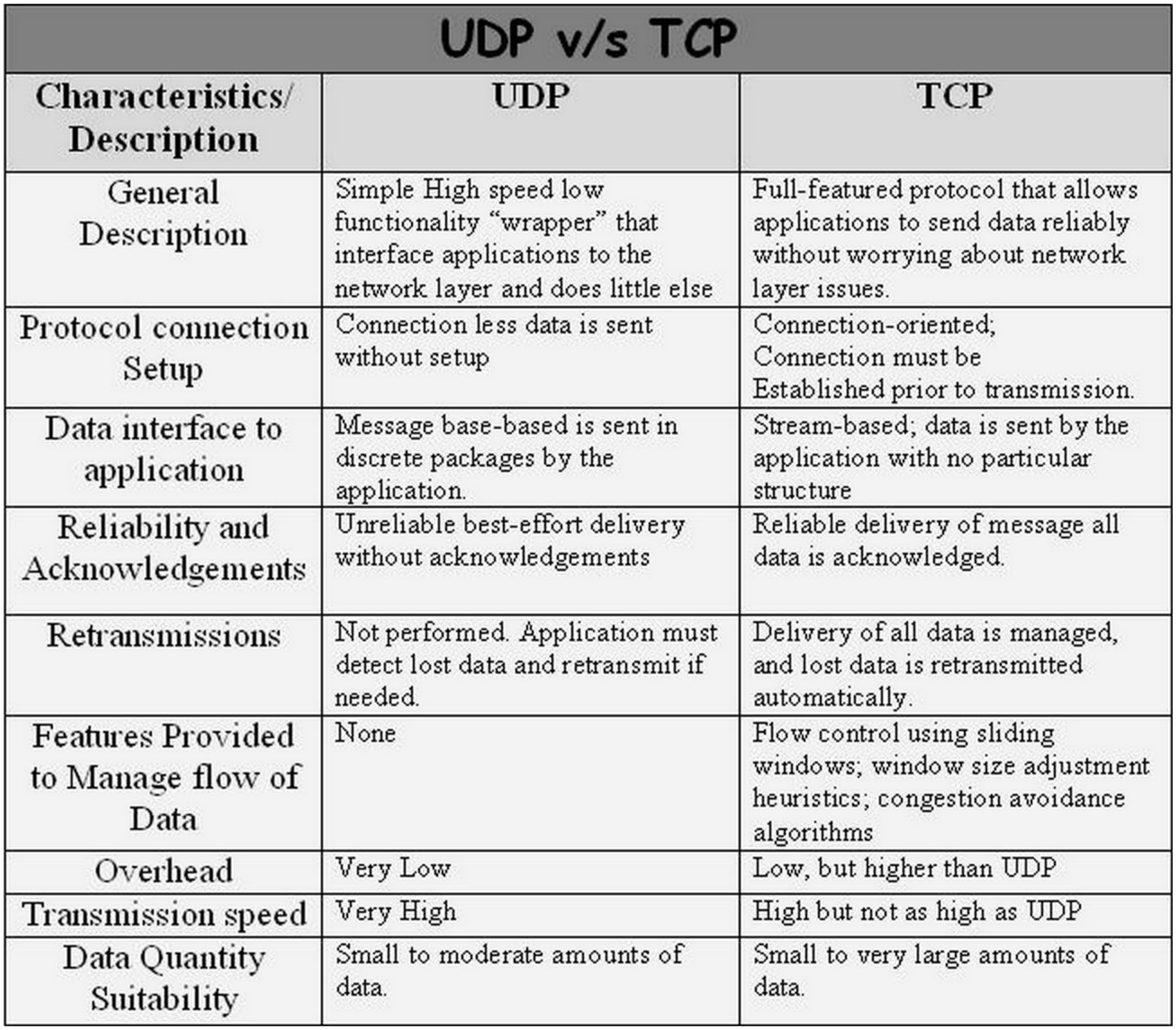
Identifies the recipient of an e-mail message.

SMTP Relay

Lets users send email through external servers. Spammers and hackers use e-mail servers to send spam or malware through e-mail under the guise of unsuspecting open relay owners.

SUMMARY

Know ports and protocols mentioned in this chapter really well. Understand enumeration and remember that most of the stuff before chapter six is typically legal. We are now interacting directly with a target with the intention of gaining access. This requires permission.



UDP v/s TCP

Characteristics/ Description	UDP	TCP
General Description	Simple High speed low functionality "wrapper" that interface applications to the network layer and does little else	Full-featured protocol that allows applications to send data reliably without worrying about network layer issues.
Protocol connection Setup	Connection less data is sent without setup	Connection-oriented; Connection must be Established prior to transmission.
Data interface to application	Message base-based is sent in discrete packages by the application.	Stream-based; data is sent by the application with no particular structure
Reliability and Acknowledgements	Unreliable best-effort delivery without acknowledgements	Reliable delivery of message all data is acknowledged.
Retransmissions	Not performed. Application must detect lost data and retransmit if needed.	Delivery of all data is managed, and lost data is retransmitted automatically.
Features Provided to Manage flow of Data	None	Flow control using sliding windows; window size adjustment heuristics; congestion avoidance algorithms
Overhead	Very Low	Low, but higher than UDP
Transmission speed	Very High	High but not as high as UDP
Data Quantity Suitability	Small to moderate amounts of data.	Small to very large amounts of data.

CEH Chapter Seven: Gaining Access to a System

SYSTEM HACKING

Password Cracking: recovering passwords from transmitted or stored data

Categories:

- Dictionary Attacks: Password cracking application that has a dictionary file loaded into it
- Brute-force Attacks: Trying every possible combination of characters programmatically
- Hybrid Attack: Like dictionary attack but with special characters substituted
- Syllable Attack: Brute force/dictionary hybrid; used to crack non standard word or phrase

- Rule-Based Attack: Utilize some known phrase or letter combination

Types:

1. Passive Online Attack: Listening based attack with Wireshark or MITM attacks
2. Active Online Attack: Interacting with target, guessing, Trojan/Spyware/Keylogger, hash injection, and phishing
3. Offline Attack: Attack preying on weakness of stored passwords. Precomputed hashes, distributed network attack, and rainbow attacks
4. Non-Technical Attack: Attack taking place in physical reality through theft, deception, or other means. Shoulder Surfing, Social Engineering, and dumpster diving

Passive Online Attacks:

- Packet Sniffing: limited to a single collision domain. You can only sniff hosts that are not connected by a switch or bridge in the selected network segment.
- Man in the Middle (MITM): Third party spying/interfering with a connection. Targets Telnet and FTP, can results in invalid traffic.
- Replay Attack: capture packets and place them back on the network later. The goal is to inject captured info such as passwords back to the server and gain access.

Active Online Attack:

- Password Guessing: use a program to crack simple passwords
- Trojans, Spyware, and Keyloggers: easy way to grab passwords (and other info) as it's typed.
- Hash Injection: four steps
  a. Compromise a work station
  b. When connected, attempt to extract hashes from the system for admins
  c. Use extracted hash to log onto server like a domain controler
  d. Attempt to extract hashers from system with intention of exploiting other accounts

*Password Hashing: verification from hashing password on client side and sending hash to the server where the stored hash and transmitted hash are compared, if they match, the user is authenticated.

Offline Attacks:

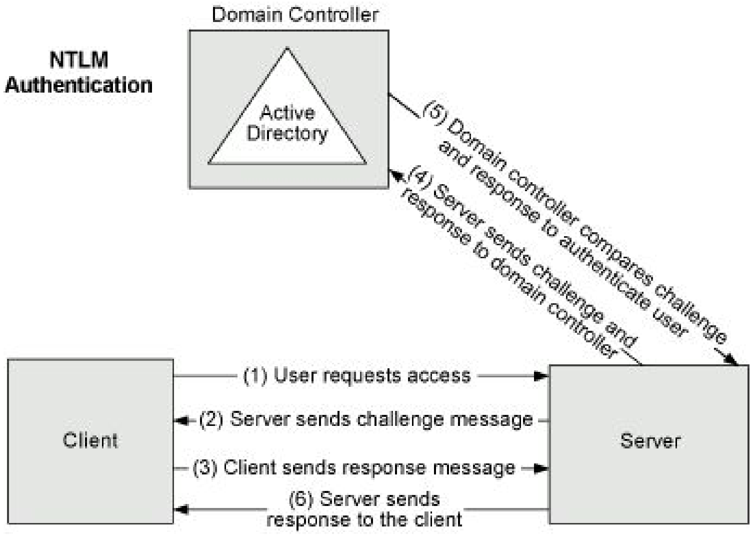
Tool: pwdump7.exe

- Precomputed Hashes and Rainbow Tables: Rainbow tables compute every possible combination of characters prior to capturing a password. Compare captured hashes for a match and you have the password.
  - Tool: winrtgen
  - *note: salted hashes are more entropic to make pattern detection more difficult
- Distributed Network Attacks (DNA): Create a bot-net and use the extra computing power to crack passwords.
- Default Passwords: easy to look up online
- Guessing: Pretty basic
- USB Password Theft: Embedded software on USB steals passwords saved locally on the machine. Can be circumvented by turning off autoplay USB (on by default)

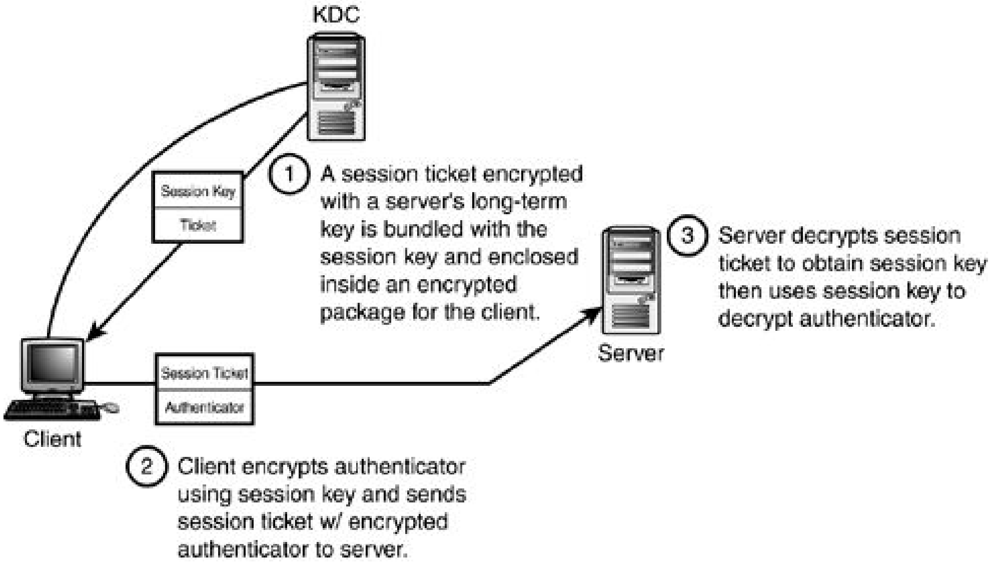
AUTHENTICATION IN THE MICROSOFT ENVIRONMENT

Security Accounts Manager (SAM) - Local database housing security principles (accounts which can be authenticated). Passwords are stored in a hashed format. This database on disk remains locked while the system is active, but it also resides in RAM and can be accessed.
SYSKEY - encryption key used to protect SAM, defaults true on all recent systems but can be manually overridden.
XP and later SAM stores passwords in a hashed format LM/NTLM C:\windows\system32\SAM
Newer hashes are salted, so offline and precomputed attacks are much more difficult to execute.

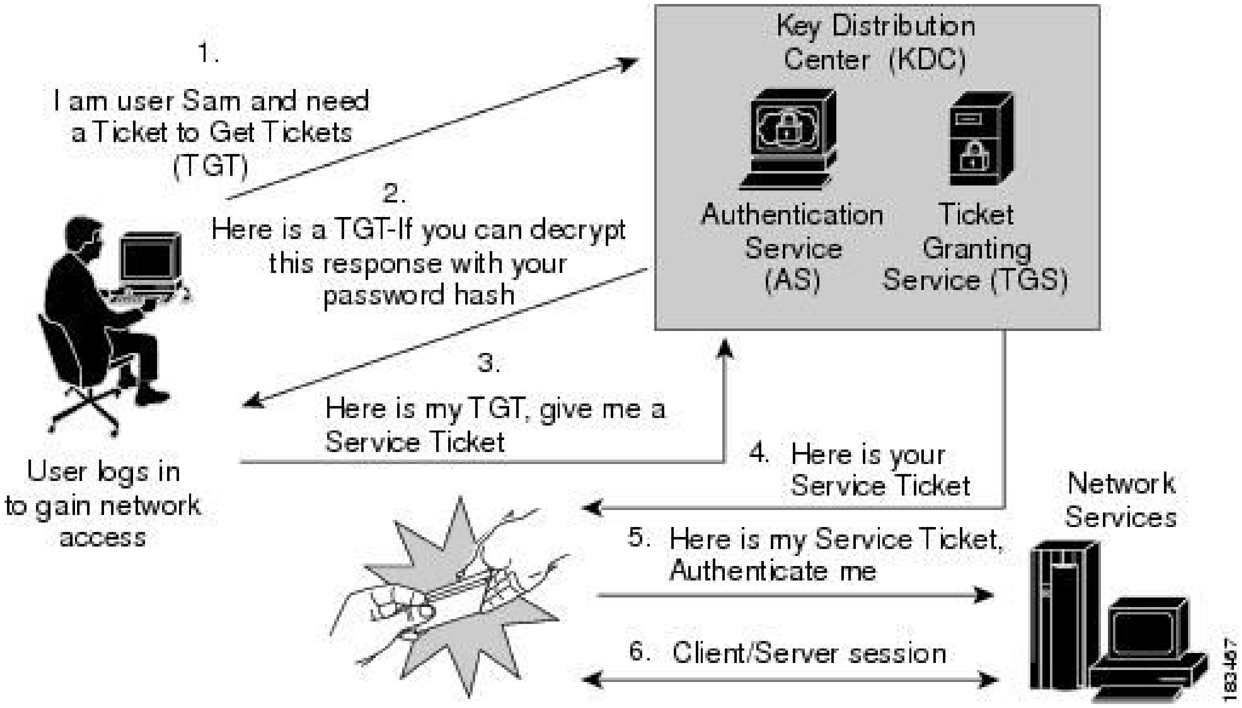
NTLM Authentication - NT LAN Manager is a proprietary Microsoft protocol.
NTLMv1 - Still supported but largely replaced with v2
NTLMv2 - Better, but still relatively insecure
Security Support Provider (SSP) - combines with NTLM for additional security


NTLM Authentication
Domain Controller
Active Directory
(5) Domain controller compares challenge and response to authenticate user
(4) Server sends challenge and response to domain controller
Client
Server
(1) User requests access
(2) Server sends challenge message
(3) Client sends response message
(6) Server sends response to the client

Kerberos:
A computer network authentication protocol which works on the basis of 'tickets' to allow nodes communicating over a non-secure network to prove their identity to one another in a secure manner.


KDC
Session Key
Ticket
1 A session ticket encrypted with a server's long-term key is bundled with the session key and enclosed inside an encrypted package for the client.
3 Server decrypts session ticket to obtain session key then uses session key to decrypt authenticator.
Server
Session Ticket
Authenticator
Client
2 Client encrypts authenticator using session key and sends session ticket w/ encrypted authenticator to server.

Kerberos offers a robust authentication framework through the use of strong cryptographic mechanisms such as secret key cryptography. The components and auth process look like this:


Key Distribution Center (KDC)
Authentication Service (AS)
Ticket Granting Service (TGS)
1. I am user Sam and need a Ticket to Get Tickets (TGT)
2. Here is a TGT-If you can decrypt this response with your password hash
3. Here is my TGT, give me a Service Ticket
4. Here is your Service Ticket
5. Here is my Service Ticket, Authenticate me
6. Client/Server session
User logs in to gain network access
Network Services
183467

Privilege Escalation

Horizontal Escalation	Attacker attempts to take over the rights and privileges of another user who has the same privileges as the current user.
Vertical Escalation	Attacker gains access to account and tries to elevate privileges or use the new position to gain access to more privileged accounts.

Tools: Active@ Password Changer, Trinity Rescue Kit (TRK), ERD Commander, Windows Recovery Environment (WinRE), Password Resetter
Detailed instructions for Vertical Privilege Escalation on p.168 with TRK.

Executing Applications
Once an attacker has permissions to execute programs, he *owns* the system. Several applications include:

- Backdoors: Allows later access to the system. Common Tools:
  - PsTools Suite: (PsExec is designed to run commands on a remote system)
  - PDQ Deploy: Designed to deploy software across network
  - RemoteExec: Like PsExec, but allows restart, reboot, and folder manipulation
  - DameWare: OSX, Linux, and Windows compatible, remote admin and control
- Crackers: crack encryption or gain passwords
- Keyloggers: Hard/Software that logs user input from the keyboard

- Malware: Capture into, alter, or compromise the system

Disable auditing wherever possible to leave no trace. Also clear logs with Dumpel, Elsave, WinZapper, CCleaner, Wipe, MRU-Blaster, Tracks Eraser Pro, Clear My History

Data Hiding

Alternate Data Streams (ADS) - strictly a feature of the NTFS file system and may not be supported in future file systems. However, NTFS will be supported in future versions of Windows NT. ADS is the ability to fork file data into existing files without affecting their functionality, size, or display to traditional file browsing utilities like dir or Windows Explorer. Found in all version of NTFS, ADS capabilities where originally conceived to allow for compatibility with the Macintosh Hierarchical File System, HFS; where file information is sometimes forked into separate resources. When launched, the ADS executable will appear to run as the original file - looking undetectable to process viewers like Windows Task Manager. Using this method, it is not only possible to hide a file, but to also hide the execution of an illegitimate process.

Tools to discover ADS: SFind, LNS, and Tripwire

CEH Chapter Eight: Trojans, Viruses, Worms & Covert Channels

MALWARE

Malware - Malicious software; anything that steals resources, time, identity, or anything else while in operation.

Common Malware Laws

The Computer Fraud and Abuse Act - Law to protect federal computer systems, extends to FDIC regulated financial institutions and interstate crime.

The Patriot Act - Greatly expanded Computer Fraud and Abuse Act. Law provides penalties of up to ten years for the first offense and twenty for the second. Assesses damage to multiple systems or damages > $5,000.

CAN-SPAM Act - Designed to thwart the spread of spam.

Types of Malware:

Viruses	Self replicating program typically initiated by user action
Worms	Ruthless self replicating software, used in forming rogue botnets
Trojan Horse	Relies on social engineering as useful, positive software
Rootkits	Malware residing in core components of a system; hard to detect and remove
Spyware	Malware designed to gain information in a stealthy manner
Adware	Malware that may replace homepages in browsers, place pop-up ads on a desktop, or install items on a victim's system designed to advertise products or services.

Viruses

1. Design: Conception and production by author
2. Replication: Initiate the spreading to different systems
3. Launch: Virus starts to carry out the task for which it was created, activating through user interaction or predetermined action
4. Detection: Virus is recognized after infection and reported to anti-virus makers
5. Incorporation: Antivirus makers determine a way to identify virus and incorporate removal in products and services
6. Elimination: Users of the antivirus products incorporate the antivirus
7. Go to step one

System/**Boot Sector Virus** - infects and places code in the master boot record (MBR)
Macro Viruses - takes advantage of embedded languages like Visual Basic for Apps (VBA)
Cluster Viruses - alters file - allocation tables on a storage device, causing file entries to point to the virus instead of a real file. So the virus runs before the application executes.
Stealth/**Tunneling** Virus - designed to avoid detection. May intercept system OS calls and send bogus responses.
Encryption Viruses - payload is decrypted, executed, and encrypted with a new key before being passed on. Very difficult to detect.
Cavity or **File Overwriting Virus** - hide in host file without making any changes
Sparse-infector viruses - only carries out mission periodically to avoid detection
Companion/**Camouflage** Virus - compromises feature of OS that enables software with the same name, but different extensions, to operate with different priorities
Logic Bomb - designed to lay in wait until a predetermined event or action occurs. Contains both a payload and a trigger. Both look innocuous until activated
File or **Multiparty Viruses** - infect systems in multiple ways using multiple attack vectors. Usually contains components on the hard drive and boot sector. Challenging to remove because you must remove all components
Shell Viruses - software infects a target application and alters it. Virus makes the app into a subroutine that runs after the virus itself
Cryptoviruses - Viruses that hunt for specific information on a system and encrypt it. Then require the victim to pay a ransom to restore access

Viruses are simple to program, and even easier to create with applications like JPS Virus Maker
Sheep-Dip System: a dedicated computer which is used to test files on removable media for viruses before they are allowed to be used with other computers.

Worms

The distinction between viruses and worms is that viruses require interaction and worms are entirely self replicating without interaction.
Common Worm Applications and Points of Interest:

- Transmit info from a victim system back to another location specified by the designer
- Carry a payload (like a virus) to multiple computers quickly

- Does not typically bind to other software applications
- Worms spread through networks automatically if the host is vulnerable, viruses do no

Spyware
Collects information about a system's activities and forwards it to interested parties
Can be installed in any number of ways: P2P, IM, Internet Relay Chat, E-mail attachments, Physical Access, Browser Vulnerabilities, Freeware, Websites, and Software

Adware
Annoying software that displays ads, popups, nag screens and may alter the browser default home page.

Scareware
Similar to a trojan horse, software triggers some error message that entices a user to download something or enter credit card information.

Trojans
Generally a non-self-replicating type of malware program containing malicious code that, when executed, carries out actions determined by the nature of the Trojan, typically causing loss or theft of data, and possible system harm. Malicious programs are classified as Trojans if they do not attempt to inject themselves into other files (computer virus) or otherwise propagate themselves (worm). Trojans rely on Covert and Overt channels.

- Overt Channel - communication path or channel that is used to send info or perform other actions. HTTP & TCP/IP, for example.
- Covert Channel - path that is used to transmit or convey info but does so in a way that is illegitimate or supposed to be impossible. Covert channels violate security on a system.

Common Covert Channels:

Loki	Passes info through an ICMP echo packet.
ICMP backdoor	Like Loki but with ICMP response packets.
007Shell	Uses ICMP packets but formats them to be normal size.
B0CK	Like Loki but with Internet Group Management Protocol (IGMP)
Reverse WWW Tunneling Shell	Creates covert channels through firewalls and proxies by masquerading as normal web traffic.
AckCmd	Provides a command shell on Windows Systems.

Types of Trojans:

Remote Access Trojans (RAT)	Allow remote control over victim’s system.
Data Sending	Collects data like keystrokes or files and transmits data back to attacker.
Destructive	Corrupt, erase or otherwise destroy data on victim system.
Proxy	Allows attacker to use infected computer as a proxy
FTP	Sets up infected system as an FTP server to distribute (illegal) information or media
Security Software Disablers	Turns off security software

*Detect Trojans by looking for open ports with Nmap (Linux) or netstat (Windows) or TCPView

Use *wrappers* to install trojans. **Wrappers** take the intended payload and merge it with a harmless executable to create a single executable file for both.
Tools: EliteWrap, Saran Wrap, Trojan Man, Teflon Oil Patch, Restorator, Firekiller 2000 (disables firewalls)

Trojan Construction Kits:
Trojan Construction Kit - CLI based tool to create trojans capable of destroying partition tables, master boot records, and hard drives.
Senna Spy - provides custom options such as file transfers, executing DOS commands, keyboard control, and list control processes
Stealth Tool - Program not to create Trojans, but assist in hiding them. Move bytes, change headers, splitting files, and combining files.

Common Keyloggers:
IKS Software Keylogger: Windows based keylogger that runs in the background at a very low level. Does not show up in process lists or through normal detection.
Ghost Keylogger: Windows based keylogger like IKS but with additional functionality. Can encrypt logs and email them to the attacker.
Spector Pro: Designed to capture keystrokes, email passwords, chat conversations, logs and instant messengers.
Fakegina: Designed specifically to capture usernames and passwords from a windows system. Intercepts info between the Winlogon process and logon GUI in windows.

CEH Chapter Nine: Sniffers

A **packet analyzer** (also known as a **network analyzer**, **protocol analyzer** or **packet sniffer—**or, for particular types of networks, an **Ethernet sniffer** or **wireless sniffer**) is a computer program or piece of computer hardware that can intercept and log traffic that passes over a digital network or part of a network.
Passive Sniffing: Traffic is observed but not altered
Active Sniffing: Traffic may be altered by the sniffing party

Targeted Protocols for Sniffing:

Telnet/rlogin	Keystrokes can be easily sniffed
HTTP	Designed to send information in the open
Simple Mail Transfer Protocol (SMTP)	Used to transfer email, no protection against sniffing
Network News Transfer Protocol (NNTP)	All communication in the clear
Post Office Protocol (POP)	Retrieves email from servers, no sniffing protection
File Transfer Protocol (FTP)	Optimized for speed, not security, wide open
Internet Message Access Protocol (IMAP)	Similar to SMTP, unprotected as well

Wireshark is the industry leader and the CLI version is called tshark.
Secondary options include TCPdump (Linux) and Windump (Windows)

MAC FLOODING

Mac Flooding: a technique employed to compromise the security of network switches. Switches maintain a MAC Table that maps individual MAC addresses on the network to the physical ports on the switch.
Tool: macof (part of the dsniff suite) [linux based]
In terminal window:

```
root@kali: ~# aptitude install dsniff
root@kali: ~#macof
```

Control - Z to stop attack

ARP POISONING

ARP spoofing, ARP cache poisoning, or ARP poison routing, is a technique by which an attacker sends (spoofed) Address Resolution Protocol (ARP) messages onto a local area network. Generally, the aim is to associate the attacker's MAC address with the IP address of another host, such as the default gateway, causing any traffic meant for that IP address to be sent to the attacker instead.
Tools: Ettercap, Cain and Able, and Arpspoof

MAC SPOOFING

MAC spoofing is a technique for changing a factory-assigned Media Access Control (MAC) address of a network interface on a networked device. The MAC address is hard-coded on a network interface controller (NIC) and cannot be changed. However, there are tools which can make an operating system believe that the NIC has the MAC address of a user's choosing. The process of masking a MAC address is known as MAC spoofing. Essentially, MAC spoofing entails changing a computer's identity, for any reason, and it is relatively easy.

PORT MIRROR OR SPAN PORT

Port Mirroring, also known as SPAN (Switched Port Analyzer), is a method of monitoring network traffic. With port mirroring enabled, the switch sends a copy of all network packets seen on one port (or an entire VLAN) to another port, where the packet can be analyzed.

DEFENSE STRATEGY

- Use hardware switched network for sensitive portions of your network to isolate traffic to one collision domain.
- Implement IP *DHCP Snooping on switches to prevent ARP Cache Poisoning and spoofing attacks
- Implement policies preventing promiscuous mode on network adapters
- Be careful deploying Wireless Access Points, all traffic is subject to sniffing
- Encrypt sensitive traffic with IPSec or SSH
- Use static ARP entries - preconfigure device for MAC addresses of connecting devices
- Port Security allow only certain MAC addresses on specific ports
- IPv6 > IPv4
- SSH > FTP and Telnet
- VPNs offer encryption solutions
- Use SSL and IPSec

*Dynamic Host Configuration Protocol (DHCP) is a network protocol that enables a server to automatically assign an IP address to a computer from a defined range of numbers (i.e., a scope) configured for a given network. DHCP assigns an IP address when a system is started.

SUMMARY

Sniffing is a technique used to gather info as it flows across a network. Sniffing can be performed using software-based systems or through the use of hardware devices called protocol analyzers. Sniffing is possible with physical access to a network where data is sent in the open. IPSec, SSL, SSH, and VPNs provide effective countermeasures against sniffing.

CEH Chapter 10: Social Engineering

Social engineering is a non-technical method of intrusion hackers use that relies heavily on human interaction and often involves tricking people into breaking normal security procedures. It is one of the greatest threats that organizations today encounter.

Strategies:

Moral Obligation	Manipulate victim’s desire to provide assistance or sense of duty.
Trust	Illustrate prior knowledge to build trust.
Threats	Utilize intimidation or threatening behavior.
Something for Nothing	Promise rewards for little effort.
Ignorance	Many people don’t recognize the threat.

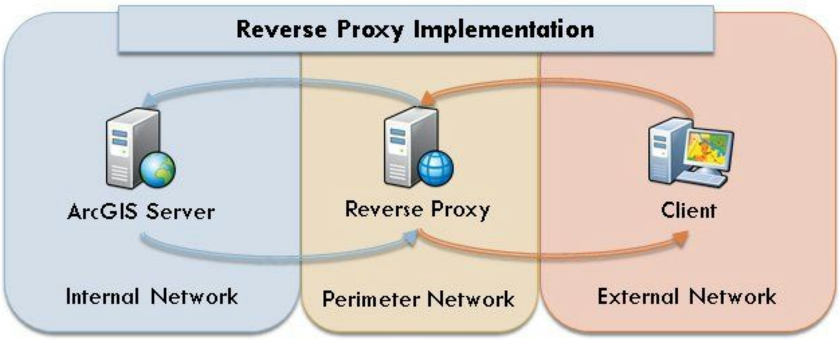
Three Phases of Social Engineering:
Research: Gather information and details through research and observation. Dumpster dive, phish, network, tour company, etc...
Development: Find a target that is frustrated, overconfident, or arrogant and willing to provide information. Build a relationship.
Exploitation: Extract desired information.

Commonly Employed Threats:
Malware: All kinds can be useful in the research phase.
Shoulder Surfing: Look over someone’s shoulder or spy on their screen.
Eavesdropping: Listen in on calls, conversations, videos, or emails.
Dumpster Diving: Attacker intercepting information physically.
Phishing: Legitimate looking emails that link to phony websites.

Defense:

- Use the latest browser and keep it up to date
- Use a pop-up blocker
- Heed Unsafe Site Warnings
- Use Antivirus Software
- Enable Automatic Updates
- Use Private Browsing
- Don’t do stupid things on the internet

A **reverse proxy** is a type of proxy server that retrieves resources on behalf of a client from one or more servers. These resources are then returned to the client as though they originated from the proxy server itself.



Egress filtering is the practice of monitoring and potentially restricting the flow of information outbound from one network to another. Typically it is information from a private TCP/IP computer network to the Internet that is controlled.
Ingress filtering is a technique used to make sure that incoming packets are actually from the networks that they claim to be from.

CEH Chapter Eleven: Denial of Service

A **denial-of-service (DoS)** or distributed denial-of-service (DDoS) attack is an attempt to make a machine or network resource unavailable to its intended users. A DoS attack generally consists of efforts to temporarily or indefinitely interrupt or suspend services of a host connected to the Internet.

DOS TARGETS

Web Server Compromise: Wides public exposure. Usually results in loss of uptime.
Back-end Resources: DOS attack on back end resources that power a website, like a SQL server.
Network or Computer Specific: Attack launched from within a LAN.

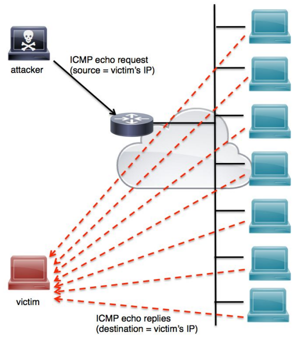
TYPES OF ATTACKS

Service Request Floods: Service like web server or application is flooded with requests until all resources are used. Typically carried out with TCP connections.

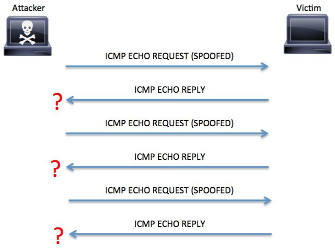
SYN Attack/Flood: a form of denial-of-service attack in which an attacker sends a succession of SYN requests to a target's system in an attempt to consume enough server resources to make the system unresponsive to legitimate traffic. Attacker sends forged SYN packets with a bogus source address. Victim system sends SYN-ACK to bogus address and waits for an ACK that never comes. This waiting period ties up the connection.

ICMP Flood Attack:

- Smurf Attacks: a distributed denial-of-service attack in which large numbers of Internet Control Message Protocol (ICMP) packets with the *intended victim's* spoofed source IP are broadcast to a computer network using an IP Broadcast address.



- Ping/ICMP Floods: a simple denial-of-service attack where the attacker overwhelms the victim with ICMP Echo Request (ping) packets. This is most effective by using the flood option of ping which sends ICMP packets as fast as possible without waiting for replies.


Attacker
Victim
ICMP ECHO REQUEST (SPOOFED)
ICMP ECHO REPLY
?
ICMP ECHO REQUEST (SPOOFED)
ICMP ECHO REPLY
?
ICMP ECHO REQUEST (SPOOFED)
ICMP ECHO REPLY
?

Ping of Death:
a type of attack on a computer system that involves sending a malformed or otherwise malicious ping to a computer. A correctly-formed ping packet is typically *56 bytes* in size, or *84 bytes* when the Internet Protocol header is considered. However, any IPv4 packet (including pings) may be as large as 65,535 bytes. Some computer systems were never designed to properly handle a ping packet larger than the maximum packet size because it violates the Internet Protocol documented in RFC 791. Like other large but well-formed packets, a ping of death is fragmented into groups of 8 octets before transmission. However, when the target computer reassembles the malformed packet, a buffer overflow can occur, causing a system crash and potentially allowing the injection of malicious code. OS patches, ping blocking and general awareness have lead to the downfall of this type of attack.

Teardrop:
A denial-of-service (DoS) attack that involves sending fragmented packets to a target machine. Since the machine receiving such packets cannot reassemble them due to a bug in TCP/IP fragmentation reassembly, the packets overlap one another, crashing the target network device.

Fraggle:
A denial-of-service (DoS) attack that involves sending a large amount of spoofed UDP traffic to a router's broadcast address within a network. It is very similar to a Smurf Attack, which uses spoofed ICMP traffic rather than UDP traffic to achieve the same goal.

Land:
A DOS attack wherein the attacker sends traffic to a target machine with self addressed sourcing. The victim attempts to acknowledge the request repeatedly with no end.

Phlashing:
A permanent denial of service (PDoS) attack that exploits a vulnerability in network-based firmware updates. Such an attack is currently theoretical but if carried out could render the target device inoperable

BUFFER OVERFLOW

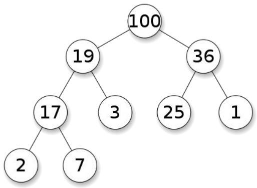
A buffer overflow, or buffer overrun, is an anomaly where a program, while writing data to a buffer (block of allocated memory), overruns the buffer's boundary and overwrites adjacent memory locations. This is a special case of the violation of memory safety.

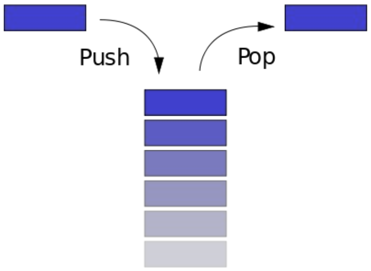
Buffer overflows can be triggered by inputs that are designed to execute code, or alter the way the program operates. This may result in erratic program behavior, including memory access errors, incorrect results, a crash, or a breach of system security. Thus, they are the basis of many software vulnerabilities and can be maliciously exploited.

C and C++ offer no built in protection against this type of attack.

Heap and Stack: two areas of memory a program uses for storage. Heap is dynamic, stack is linear.

- **Heap**: dynamic storage location that does not have sequential constraints or an organizational scheme. Considered the larger pool of free storage for programs to use as needed. Once the space is no longer needed, it’s freed for future use.
- **Stack**: Refers to a smaller pool of free storage: memory allocated for short-term processing. Where program variables are temporarily stored, added, and removed as needed. Last in first out (LIFO).
    - Push: Add something to the top of the stack.
    - Pop: Remove something from the top of the stack.





NOP Sled:
NOP slide, NOP sled or NOP ramp is a sequence of NOP (no-operation) instructions meant to "slide" the CPU's instruction execution flow to its final, desired, destination whenever the program branches to a memory address anywhere on the sled.
0x90 is the hex code for no operation for Intel processors and is used to create padding in the stack to insert malicious code. 0x90 instructs an intel processor to perform one *clock cycle on an empty process.
*The **clock cycle** is the time between two adjacent pulses of the oscillator that sets the tempo of the computer processor.

Buffer overflow overfills the heap, exceeding memory boundaries. This creates an unpredictable condition where the OS sees the program operating outside it’s allocated memory space.

- The OS will terminate the program
- The address of the hacker’s malicious code, which is now in the overflowed stack, winds up in the Extended Instruction Pointer, and that code gets executed.

UNDERSTANDING DDOS

Distributed Denial of Service Attacks use a distributed group of computers to attack a single target. This group of computers is referred to as a botnet. A botnet refers to a type of bot running on an IRC network that has been created with a trojan. When an infected computer is on the Internet the bot can then start up an IRC client and connect to an IRC server. The Trojan will also have been coded to make the bot join a certain chat room once it has connected.
Botnet Tools: Shark, Plugbot, Poison Ivy, Low Orbit Ion Cannon (LOIC)

DoS Tools:

- DoSHTTP: HTTP flood tool capable of targeting URLs s/ port designation.
- UDP Flood: Generates UDP packets at specific rate to certain target.
- Jolt2: IP Fragmentation DoS tool sends fragmented packets to Windows host
- Targa: 8in1 tool for various DoS attacks

DDoS Tools:

- Trinoo: UDP flooding for single or multiple IPs
- LOIC: Simple user interface for DoS attacks
- TFN2K: Based on Tribe Flood Network (TFN) capable of SYN, UDP, and UDP flood
- Stacheldraht: Similar to TFN2K, specific duration to specific ports

DDOS DEFENSIVE STRATEGIES

Disable Unnecessary Services: Harden individual systems and block ports that are not in use.
Use Anti-Malware: Prevent bot installations by keeping anti-malware up to date.
Enable Router Throttling: Traffic saturation attacks and be thwarted or slowed by throttling traffic on gateway router. Creates automated control and allows admin to respond before networks go offline.
Use a **Reverse Proxy**: Destination resource redirects approved traffic. Middleman can take proactive measures.
Enable Ingress and Egress Filtering:

- **Ingress Filtering**: prevents DoS and DDoS attacks by filtering for Spoofed IP Addresses
- **Egress Filtering**: blocks outbound traffic from relaying info to attacking party

Degrading Services: Throttle down or shut off services in response to an attack
Absorb the **Attack**: Have more resources than an attacker can consume

BOTNET-SPECIFIC DEFENSES

RFC 3704 Filtering - Block or stop packets from addresses that are unused or reserved in any given range. Ideally filtering is done at the IP level prior to reaching the main network.
Black Hole Filtering - Creates essentially a black hole on the network where offensive packets are forwarded and dropped.
Source IP Reputation Filtering - Cisco (IPS solutions) filter based on history of traffic attacks and behavior.

SUMMARY

DoS overloads a system with traffic, DDoS does the same thing using multiple attacking systems. Heaps are dynamic, stacks are linear, LIFO. EIP is the point of execution in a stack and it gets shifted during an overflow. Buffer overflow occurs when data gets pushed beyond stack memory allocation. Stack smashing is causing a stack in a computer application or operating system to overflow. Buffer overflow occurs when a program or process tries to store more data in a buffer (temporary data storage area) than it was intended to hold. C contains dangerous function because they don't check for overflows: gets(), scanf(), strcpy(), and strcat(). NOP means "No Operation" and is a dry fire command on an Intel processor which tells the CPU to do nothing for one clock cycle.

CEH Chapter 12: Session Hijacking

Session Hijacking is sometimes also known as *cookie hijacking* and is the exploitation of a valid computer session—sometimes also called a session key—to gain unauthorized access to information or services in a computer system.

Primary session hijacking techniques: Need session ID or Session *token*
Brute-Forcing and ID: Guessing and ID, maybe with the help of HTTP referrers, sniffing, cross-site scripting, or malware.
Stealing an ID: Pilfering an ID through sniffing or other means.
Calculating an ID: Look at an existing ID and looking up the sequence.

Process:

1. Sniffing: Observing network traffic to watch for session IDs
2. Monitoring: Observe traffic between the two points with an eye toward predicting the sequence numbers of the packets.
3. Session Desynchronization: Breaking the session between the two parties.
4. Session ID prediction: Predict session ID to take over the session.
5. Command Injection: Inject commands into the session at the target (usually a server or resource).

Active v. Passive:
Active Session Hijacking: attacker assumes the session as their own, thereby taking over the legitimate client's connection to the resource. In an active attack the attacker is actively manipulating and/or serving the client connection and fooling the server into thinking they are the authenticated user.
Passive Session Hijacking: monitor traffic between victim and server.

Session ID Types:

1. Embedded in a URL: A web app uses a GET request to follow links embedded in a web page. Attacker can just check browser history to find this.

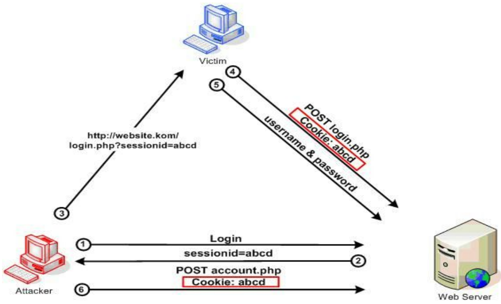
2. Embedded as a hidden file: Utilizes a POST command when the info is submitted.
3. Cookies: Find session ID in software embedded on a user’s machine.

APPLICATION LEVEL SESSION HIJACKING

Session Sniffing: Sniff to find the token / session ID and then use it to access the server.
Predicting Session Tokens: Examine past valid session IDs and make an educated guess at what a future one will be.
Man in the Middle: In cryptography and computer security, aman-in-the-middle attack (often abbreviated to MITM, MitM, MIM, MiM or MITMA) is anattack where the attacker secretly relays and possibly alters the communication between two parties who believe they are directly communicating with each other.
Man in the Browser:

1. Cross Site Scripting(XSS): A type of attack that can occur in many forms, but generally when data enters a web app through an untrusted source (usually a web request).
    a. Stored XSS Attacks: Attacks where the hacker will place code on a target server where the victims they wish to target will access the content. When the victim makes a request on the server, the code will execute.
    b. Reflected XSS Attacks: injected code is bounced or reflected off a web server in the form of something else like an error message or other result. Email or a different server may be involved but the user may be tricked into clicking a link in a web page or message. The link executes code.
2. Trojans:
3. Javascript:

The **session fixation** attack is a class of Session Hijacking, which steals the established session between the client and the Web Server after the user logs in. Instead, the Session Fixation attack fixes an established session on the victim's browser, so the attack starts before the user logs in.



Blind Hijacking: a type of session hijack where the attacker cannot capture return traffic from the host connection. So the attacker is blindly injecting malicious packets without any indication of whether they are successful.

IP Spoofing: IP spoofing, also known as IP address forgery or a host file hijack, is a hijacking technique in which a cracker masquerades as a trusted host to conceal his identity, spoof a Web site, hijack browsers, or gain access to a network. IP spoofing is not session hijacking, but both aim at using an existing authentication session to gain access to an otherwise inaccessible system.

Source Routing is a technique whereby the sender of a packet can specify the route that a packet should take through the network. In strict source routing, the sender specifies the exact route the packet must take. This is virtually never used.

DNS spoofing (or DNS cache poisoning) is a computer hacking attack, whereby data is introduced into a Domain Name System (DNS) resolver's cache, causing the name server to return an incorrect IP address, diverting traffic to the attacker's computer (or any other computer).

ARP spoofing, ARP cache poisoning, or ARP poison routing, is a technique by which an attacker sends (spoofed) Address Resolution Protocol (ARP) messages onto a local area network. Generally, the aim is to associate the attacker's MAC address with the IP address of another host, such as the default gateway, causing any traffic meant for that IP address to be sent to the attacker instead.

Desynchronization: TCP connections begin their sequencing of the packets with what is know as an initial sequence number (ISN). The ISN is basically a starting point on which all following packets can increment and sequence themselves accordingly. Desynchronizing the connection involves breaking the sequence between the victim and the host, thereby giving the attacker the opportunity to jump in and take over the connection to the host.

NETWORK SESSION HIJACKING

A hijacking method that focuses on exploiting a TCP/IP connection after initialization or authentication has occurred.

TCP/IP Session Hijacking

The attacker infiltrates a TCP session by attempting to predict the sequence numbers of the packets flowing from the victim's machine to the connected resource. Then attacker can inject packets that are in sequence with legit user's traffic.

UDP Session Hijacking

Trick the victim into thinking the attacker's computer is the server. This is done by the attacking computer by responding before the server. UDP is simpler because it does not establish a connection.

CEH Chapter 13: Web Servers and Web Applications

Server Administrators: The Server Administrator's role is to design, install, administer, and optimize company servers and related components to achieve high performance of the various business functions supported by the servers as necessary. This includes ensuring the availability of client/server applications, configuring all new implementations, and developing processes and procedures for ongoing management of the server environment. Where applicable, the Server Administrator will assist in overseeing the physical security, integrity, and safety of the data center/server farm.

Network Administrators: responsible for the maintenance of computer hardware and software systems that make up a computer network including the maintenance and monitoring of active data network or converged infrastructure and related network equipment.

Network administrators are generally mid-level support staff within an organization and do not typically get involved directly with users. Network administrators focus on network components within a company's LAN/WAN infrastructure ensuring integrity. Depending on the company and its size, the network administrator may also design and deploy networks.

End Users: Those who interact with the server and app as a user and consumer of information.

WEB APPLICATION LAYERS

Presentation Layer: Responsible for display and presenting information to the user on the client side.

Logic Layer: Used to transform, query, edit, and otherwise manipulate information to and from the forms it needs to be stored or presented in.

Data Layer: Responsible for holding the data and information for the application as a whole.

Stateless: a protocol is said to be stateless when it does not keep track of session information from one connection to the next. Each communication in HTTP is treated as a separate connection.

Web Application Components:

Login	Username and password authentication
Web Server	Combination of hard and software used to host the app itself. Capabilities vary by server.
Session Tracking	Allows web application to store info about a client pertaining to the current visit.
Permissions	Based on authentication category and success, permissions afforded to a user.
Application Content	Info that the user is interacting with by providing requests to the server.
Data Access	Web pages in a web app are attached to a library that provides data access.
Data Store	Where valuable information for the application is contained.
Logic	Component responsible for interacting with the user and providing means for the correct information to be extracted from the database.
Logout	Usually a separate function that terminates connection with web app.

SERVER AND APPLICATION VULNERABILITIES

Flawed Web Design: Poor coding can reveal form data.
Buffer Overflow: Buffers can be overwritten to cause data to lose its integrity.
Denial-of-Service or Distributed Denial-of-Service (DoS/DDoS):

- Ping Flood
- Smurf Attack
- Syn Flood
- IP Fragmentation

Banner Information: telnet <servername>.com 80
Error Messages: Descriptive Error messages outside development.

COMMON ATTACK METHODS

Input Validation: verifying information as it is entered into an application. Failure to sanitize inputs and escape outputs can result in:

- Database Manipulation
- Database Corruption
- Buffer Overflows
- Inconsistent Data

Cross Site Scripting: a type of computer security vulnerability typically found in Web applications. XSS enables attackers to inject client-side script into Web pages viewed by other users. A cross-site scripting vulnerability may be used by attackers to bypass access controls such as the same-origin policy.

Insecure Logon Systems: Applications should be designed to return generic information that does not reveal info such as correct usernames.

Scripting Errors: Common Gateway Interface (CGI), ASP.NET, and JavaServer Pages(JSP) are common scripting languages and include their own issues. Common strategies:

- Upload Bombing: Uploads massive files to a server with the goal of filling up the hard drive on the server.
- Poison Null Byte Attack: passes special characters that scripts may not be designed to handle properly.
- Default Scripts: Generic scripts that are uploaded by designers and developers who do not know what they do.
- Sample Scripts: Examples of how certain scripts are configured that are left out in the open.
- Poor scripting: leaving sensitive info out in the open.

Encryption Weaknesses:

- OpenSSL: www.openssl.org
- OWASP: www.owasp.org
- Nessus Vulnerability Scanner: www.nessus.org <-lists ciphers in use by a web server.

- WinSSLMim: HTTPS man in the middle attacks www.securiteinfo.com/outils/WinSSLMiM.shtml
- Stunnel, a program that allows encryption of Non-SSL-aware protocols

Directory Traversal Attacks:

- Access control lists (ACL): Indicate which users and groups are allowed to access files and directories on a server as well as what level of interaction is allowed.
- Root Directory: directory on server to which users are specifically restricted should act as the highest directory that users have access to.

e.g. http.examples.com/index.php/../../../..

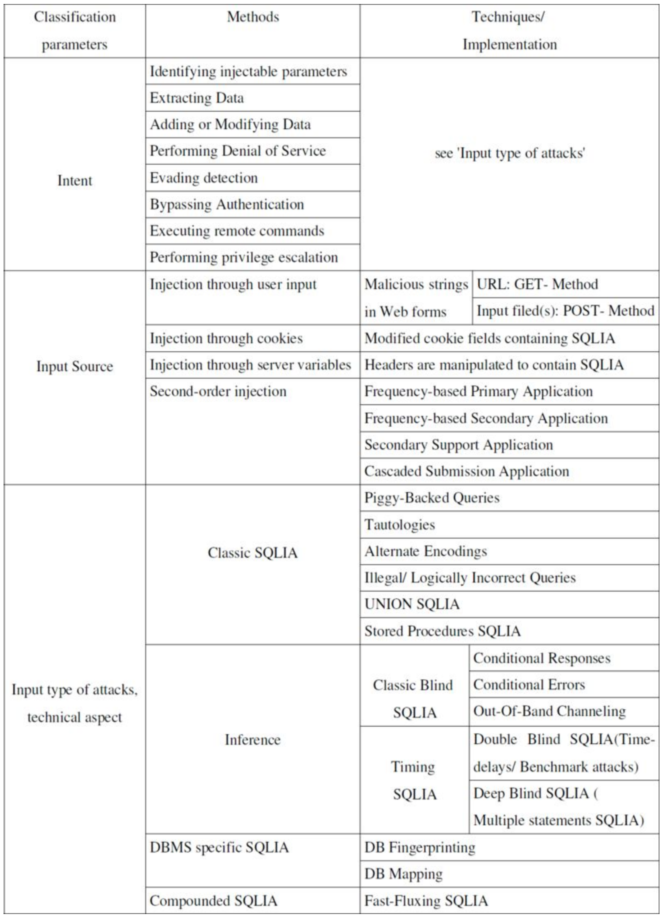
SUMMARY

Web Applications are designed to run on the server and have results transmitted to the client. Directory traversal may allow for access to information outside the public_html file, and that's a problem. Client side applications happen in the *browser* not the *server*.

CEH Chapter 14: SQL Injection

SQL injection is a code injection technique, used to attack data-driven applications, in which malicious SQL statements are inserted into an entry field for execution (e.g. to dump the database contents to the attacker). SQL injection must exploit a security vulnerability in an application's software, for example, when user input is either incorrectly filtered for string literal escape characters embedded in SQL statements or user input is not strongly typed and unexpectedly executed. SQL injection is mostly known as an attack vector for websites but can be used to attack any type of SQL database.

- SQL injection is typically a result of flaws in the web application or website and is not an issue with the database.
- Source of many high level attacks online.
- Goal is to submit commands through a web application in order to retrieve or manipulate data.
- Typically caused by improper or absent input validation, allows unverified code into database.



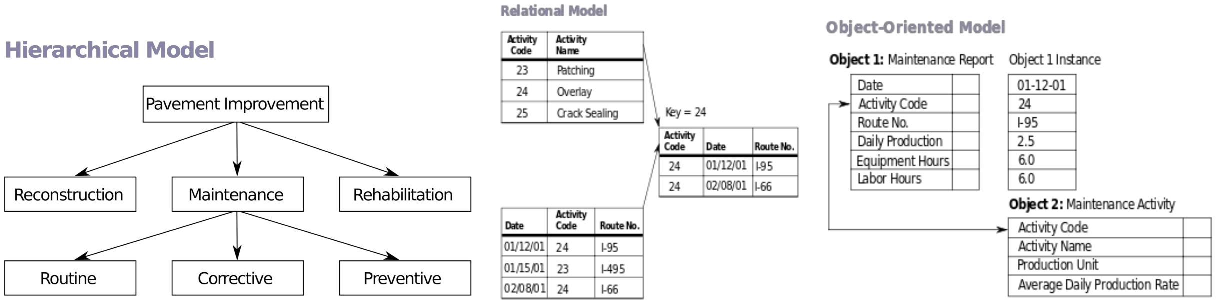
Classification parameters	Methods	Techniques/ Implementation	
Intent	Identifying injectable parameters	see 'Input type of attacks'	
	Extracting Data		
	Adding or Modifying Data		
	Performing Denial of Service		
	Evading detection		
	Bypassing Authentication		
	Executing remote commands		
	Performing privilege escalation		
Input Source	Injection through user input	Malicious strings in Web forms	URL: GET- Method
			Input filed(s): POST- Method
	Injection through cookies	Modified cookie fields containing SQLIA	
	Injection through server variables	Headers are manipulated to contain SQLIA	
	Second-order injection	Frequency-based Primary Application	
		Frequency-based Secondary Application	
		Secondary Support Application	
		Cascaded Submission Application	
Input type of attacks, technical aspect	Classic SQLIA	Piggy-Backed Queries	
		Tautologies	
		Alternate Encodings	
		Illegal/ Logically Incorrect Queries	
		UNION SQLIA	
		Stored Procedures SQLIA	
	Inference	Classic Blind SQLIA	Conditional Responses
			Conditional Errors
			Out-Of-Band Channeling
		Timing SQLIA	Double Blind SQLIA(Time-delays/ Benchmark attacks)
			Deep Blind SQLIA (Multiple statements SQLIA)
	DBMS specific SQLIA	DB Fingerprinting	
		DB Mapping	
	Compounded SQLIA	Fast-Fluxing SQLIA	

SERVER SIDE APPLICATION TECHNOLOGIES

ASP, .NET, ORACLE, PHP, JSP, SQL Server, IBM DB2, MySQL, RubyOnRails

DATABASES

Relational Databases: Data can be organized and accessed in different ways depending on the situation; a database structured to recognize relations among stored items of information.
Distributed Databases: Dispersed or replicated across network locations.
Object-oriented Programming Database: Built on object classes and subclasses.
Hierarchical Database - a data model in which the data is organized into a tree-like structure. The data is stored as records which are connected to one another through links. A record is a collection of fields, with each field containing only one value.



Record / Row: a collection of related data
Column: data category or type

Tools to find vulnerable databases:
SQLPing3: Performs both active and passive scans to identify all SQL Server / MSDE installations. http://www.vulnerabilityassessment.co.uk/
SQLRecon: Similar to SQL Ping3 but has added features to discover hidden DBs
*Once you locate databases you can try to crack the password.

You can find targets with Google hacking - list of suggestions on page 336.

Test to see if a website is vulnerable to SQL injection attacks by adding an apostrophe to the end of the URL. Example: http://examplesite.com/default.php?id=1'
If the site returns an SQL error, it's probably vulnerable.

Once you find a target use order by 1 to increment through records until you hit an error. Then use union select to grab all the non-error records.
@@version

Validate: Sanitize inputs, escape outputs

- Don't use dynamic SQL to generate queries based on user input
- Maintain the server and watch for red flags
- Use a well configured IDS to monitor interaction at the Database Level
- Harden the system and disable the xp_cmdshell commands
- Exercise least privilege and eliminate superfluous connections
- Test your apps
- Don't use default settings
- Disable error messages in production

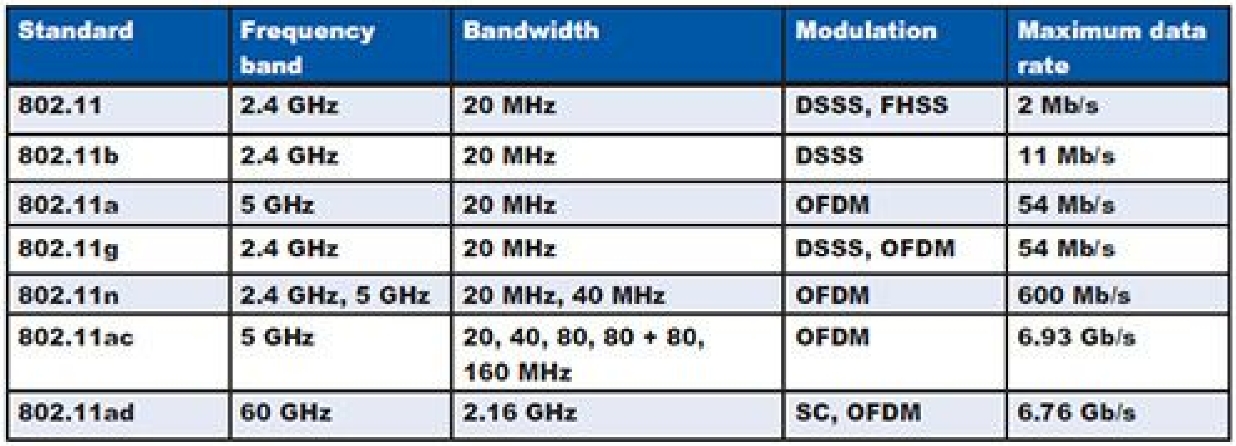
CEH Chapter 15: Wireless Networking

IEEE 802.11 is a set of media access control (MAC) and physical layer (PHY) specifications for implementing wireless local area network (WLAN) computer communication in the 2.4, 3.6, 5, and 60 GHz frequency bands. They are created and maintained by the IEEE LAN/MAN Standards Committee (IEEE 802). The base version of the standard was released in 1997, and has had subsequent amendments.

Four major environments:

Extensions	**Hardware Based Access points** (HAP) use a device like a router or dedicated WAP **Software Based Access points** (SAP) are possible through a wireless enabled system attached to a wired network, which shares the wireless adapter.
Multiple Access Points	Provides multiple overlapping access points that users can connect to and move across seamlessly.
LAN to LAN	Connects wired networks in different locations to be connected through wirelessly.
3G or 4G hotspot	Provides Wi-Fi access to Wi-Fi enabled devices.

Table 1: IEEE 802.11 Standards



Standard	Frequency band	Bandwidth	Modulation	Maximum data rate
802.11	2.4 GHz	20 MHz	DSSS, FHSS	2 Mb/s
802.11b	2.4 GHz	20 MHz	DSSS	11 Mb/s
802.11a	5 GHz	20 MHz	OFDM	54 Mb/s
802.11g	2.4 GHz	20 MHz	DSSS, OFDM	54 Mb/s
802.11n	2.4 GHz, 5 GHz	20 MHz, 40 MHz	OFDM	600 Mb/s
802.11ac	5 GHz	20, 40, 80, 80 + 80, 160 MHz	OFDM	6.93 Gb/s
802.11ad	60 GHz	2.16 GHz	SC, OFDM	6.76 Gb/s

Direct-Sequence Spread Spectrum (**DSSS**) is a transmission technology used in LAWN transmissions where a data signal at the sending station is combined with a higher data rate bit sequence, or chipping code, that divides the user data according to a spreading ratio.

Frequency Hopping Spread Spectrum (**FHSS**) is a method of transmitting radio signals by rapidly switching a carrier among many frequency channels, using a pseudorandom sequence known to both transmitter and receiver.

Orthogonal frequency-division multiplexing (**OFDM)** is a technology used to compress a large amount of data into a small amount of bandwidth. This is done by dividing a large amount of data into smaller chunks, then sending that data simultaneously over a number of frequencies.

Service Set Identifier (**SSID**): is a case sensitive, 32 alphanumeric character unique identifier attached to the header of packets sent over a wireless local-area network (WLAN).

VOCABULARY

GSM (Global System for Mobile Communications)	International standard for mobile wireless.
Association	Process of connecting client and access point
BSSID (basic SSID)	MAC address of an access point
Hotspot	Location that provides wireless to the public
Access point	Hard/Software construct that enables wireless access
ISM (Industrial, Scientific, and Medical)	Unlicensed band of frequencies
Bandwidth	Amount of speed available to devices

WIRELESS ANTENNAS

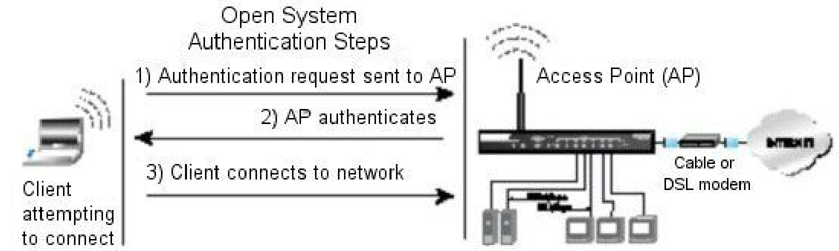
Yagi Antenna - a highly directional radio antenna made of several short rods mounted across an insulating support and transmitting or receiving a narrow band of frequencies.

Omnidirectional Antenna - a class of antenna which radiates radio wave power uniformly in all directions.

Parabolic Grid Antenna - dish shaped, directional antenna. It’s possible to hack a direct tv satellite into a long range antenna.

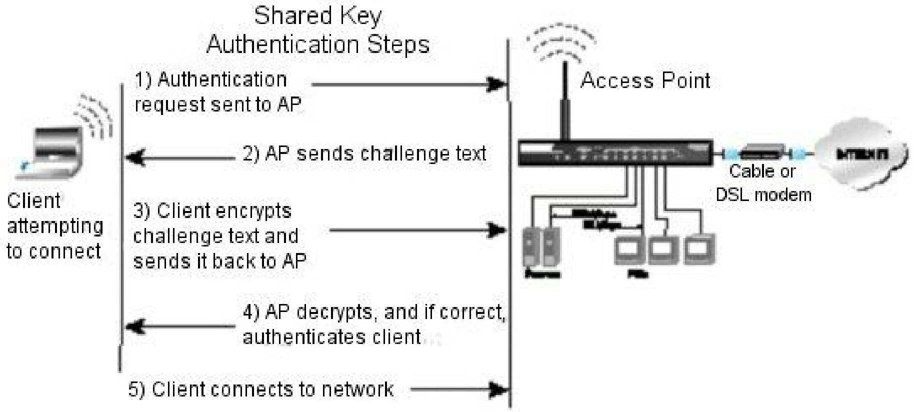
AUTHENTICATION

Open System Authentication:



Source: http://www.netgear.com/docs/refdocs/Wireless/wirelessBasics.htm

Shared Key Authentication:



Source: http://www.netgear.com/docs/refdocs/Wireless/wirelessBasics.htm

Shared Key Authentication (**SKA**) is a process by which a computer can gain access to a wireless network that uses the Wired Equivalent Privacy (WEP) protocol. With SKA, a computer equipped with a wireless modem can fully access any WEP network and exchange encrypted or unencrypted data.

ENCRYPTION PROTOCOLS

Wired Equivalent Privacy (**WEP**) - oldest, weakest, encryption protocol.
Wi-Fi Protected Access (**WPA**) - Designed to replace WEP. Uses Temporal Key Integrity Protocol (TKIP), message integrity code (MIC), and Advanced Encryption Standard (AES) as the main mechanism for securing info.
WPA2 - stronger version of WPA employing AES, Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (CCMP), Extensible Authentication Protocol (EAP), and TKIP. Can be expanded and is available for enterprises.
Temporal Key Integrity Protocol (**TKIP**) - enhances WPA and WEP.
Advanced Encryption Standard (**AES**) - symmetric key encryption, used in WPA 2 as a replacement for TKIP.
Lightweight Extensible Authentication Protocol (**LEAP**) - is a proprietary WLAN authentication protocol from Cisco.
Remote Authentication Dial-In User Services (**RADIUS**) - centralized authentication and authorization management.
802.11i - IEEE standard that specifies security mechanisms for 802.11 wireless networks.

CCMP - 128 bit keys with 48 bit initialization vector (IV) for replay detection.
*An **initialization vector** (**IV**) is an arbitrary number that can be used along with a secret key for data encryption. This number, also called a nonce, is employed only one time in any session.

WEP:

- IVs are only 24 bits in length, meaning they can be exhausted in less than 5 hours on a busy network.
- CRC32 Cyclic Redundancy Check is used to check integrity, slight packet modification can bypass this feature.
- Vulnerable to plaintext attacks through packet sniffing
- Easy to build decryption tables
- Susceptible to DOS attacks

How to break WEP:

1. Start a packet capture to monitor the target interface.
2. Determine if packet injection can be performed.
3. Use a tool like Aireplay-ng to spoof authentication requests.
4. Start sniffing Wi-Fi to capture IVs
5. Use Cain & Able to extract encryption layers from the IVs

WPA:

- Weak user keys
- Packet Spoofing
- Authentication issues with Microsoft Challenge Handshake Authentication Protocol v2.

Cracking WPA:

1. Use Reaver on Kali to crack WPA

WPA2: Available in both personal and enterprise versions.
Offline Attack: Capture the three way handshake that initiates the connection and crack the packets offline.
Deauthentication Attack: Observe the handshake between the client and the access point and force a reconnect.
Brute Force: Use Aircrack-ng to brute force your way through possible keys. Takes time and CPU cycles, but it works.

DEFENSE

- Complex passwords
- Use server validation on the client side to enable the client to have a positive ID
- Utilize WPA2 where available.
- Use Encryption like CCMP, AES, and TKIP

Wardriving Tools: KisMAC, NetStumbler, Kismet, WaveStumbler, and InSSIDer.

Installing a **Rogue Access Point** and either cloaking the SSID or making it appear benign may be the easiest way to gain access to a network. See also raspberry pi dropboxes that use reverse ssh tunneling from inside a network to establish a connection with the attacker.
MAC Spoofing can circumvent MAC address filtering SMAC, ifconfig, changemac.sh
A wireless **ad hoc network** (WANET) is a decentralized type of wireless network. The network is ad hoc because it does not rely on a pre existing infrastructure, such as routers in wired networks or access points in managed (infrastructure) wireless networks. Ad hoc networks do not allow the same security.
Misconfiguration: All the security features in the world won't help if they aren't used correctly.
Client Misassociation: Starts with a client attaching to network other than their own.
Promiscuous Client: Set up a router with a really strong signal to get people to connect to it.
Jamming Attack: Buy a jammer online and overload the WAP - some of these are in gray areas, but this one is not, it's totally illegal.
HoneySpot: bring your own router and have the strongest connection

Tools:
OpenSignal: app and website to map out WAPs on a map.
wefi www.wefi.com
JiWire www.jiwire.com
Wireshark to reveal the following:

- Broadcast SSID
- Presence of access points
- Possibly SSIDs
- Authentication method being used.
- WLAN encryption

Wireless traffic analysis tools: Kismet, AirMagnet, WIreshark with AirPcap, CommView

BLUETOOTH

Modes:
Discoverable: Allows device to be scanned by devices in range.
Limited Discoverable: Discoverable for a short period of time before it returns to nondiscoverable
Non-discoverable: can only be found if it has been found by the device before.

Bluejacking: send bluetooth messages at random to people in range.
Bluesnarfing: Remotely extract information from a device. Invasive and very dangerous.

CEH Chapter 16: Evading IDS, Firewalls, and Honeypots

HONEYPOTS, IDS, & FIREWALLS

Intrusion Detection System: an application or device used to gather and analyze information that passes across a network or host.

- Designed to detect malicious or nonstandard behavior
- Gathers information from within a network to detect violations of a security policy
- Reports violations and deviations to an administrator or system owner

Network IDS (NIDS) is a packet sniffer designed to report deviations from a set of rules.

FOUR TYPES OF IDSs

1. NIDS - designed to inspect every packet entering a network for the presence of malicious or damaging behavior and throw an alert when malicious activity is detected.
2. Host-Based Intrusion Detection Device (HIDS) - installed on a server or computer. HIDS monitors activities on a system.
3. Log File Monitors (LFMs) - Monitor log files created by network services to find logs of suspicious events. Example: swatch
4. File Integrity Checking (Tripwire) - programs that test files against original repos looking for modifications.

IDS DETECTION METHODS

Signature (Misuse) Detection - Compare traffic to known models and report matches.
Anomaly Detection - Any activity that matches something in the database is considered an anomaly. System must be set to detect normal network traffic as a baseline.
Protocol Anomaly Detection - system uses known specifications for a protocol and then uses that as a model to compare against.

Host System Intrusions - Indicated by new files, altered files, altered attributes, unknown extensions, cryptic filenames, double extensions, unknown or unexplained file extensions
Network Intrusions - Indicated by increased/unexplained use of bandwidth, probes against services on the network, connection requests from outside the local network, repeated login attempts from remote hosts, suspicious log files.
Nonspecific Signs of Intrusion - Modifications to system software and config files, missing or suspicious log files, crashes, gaps in accounting, logins during non-work hours, decreased performance.

FIREWALLS

Firewall: a hard or software part of a computer system or network that is designed to block unauthorized access while permitting outward communication. Ideally, only traffic that is explicitly allowed to pass will be able to do so.

- Firewalls are a form of IDS
- Firewall configuration is mandated by company security policy and will change to keep pace with the goals of the organization
- Firewalls are typically configured to allow only specific kinds of traffic such as email protocols, web protocols, or remote access points
- May act as a phone tap
- Uses rules to determine what traffic can move in and out of the network - one way traffic is possible
- For packets moving between networks, firewalls also act as routers

- Can filter based on virtually all criteria
- Alarms can be configured

Placing a firewall in front of a router reduces the stress on the router.

Firewall Configurations:
Bastion Host: intended to be the point where traffic enters and exits the network. This setup mandates two interfaces, one exterior facing interface and one interior facing interface.
Screened Subnet: Single firewall with three interfaces: the internet, DMZ, and intranet. All are separated and function on their own interface. A compromise in one area will not affect the others.
Multihomed Firewall: Two or more networks. Each interface connects to its own network segment logically and physically.

DEMILITARIZED ZONE (DMZ)

Buffer zone between public and private network. Also serves as a way to host services that a company wishes to make publicly available without allowing direct access to their internal network. Three interfaces are configured for the intranet, DMZ, and internet.

TYPES OF FIREWALLS

Packet Filtering Firewall: Network Layer of the OSI model. Firewall compares properties of a packet like source and destination address, protocol, and port. If the packet does not match a rule, it’s dropped.
Circuit Level Gateway: Session Layer of the OSI model. Detects valid sessions by inspecting TCP handshakes. Does not filter based on packets.
Application-Level Firewall: Analyze application information. Proxy based firewalls operate at this level. Content catching serves common (cached) content rather than calling the server.
Stateful Multilayer Inspection Firewall: Combines aspects of the other three types. Filters packets at the network layer and evaluate contents at the application layer.
Firewalls typically run on specific ports, so you can use port scanning and banner grabbing (telnet) to identify what firewall is running.
A **checksum** is a count of the number of bits in a transmission unit that is included with the unit so that the receiver can check to see whether the same number of bits arrived. If the counts match, it's assumed that the complete transmission was received.
Firewalking: utilizes traceroute techniques and TTL values to analyze IP packet responses in order to determine gateway ACL (Access Control List) filters and map networks. It is an active reconnaissance network security analysis technique that attempts to determine which layer 4 protocols a specific firewall will allow.
Requirements:
Firewalking Host: System outside the target that is sending packets.
Gateway Host: System on target network that is connected to the internet.
Destination Host: Target system on target network that data packets are addressed to.
Tools: firewalk (cli)

BASIC IDS EVASION

DoS: tie up IDS resources with a DoS attack
Obfuscation: obscuring of intended meaning in communication, making the message confusing, willfully ambiguous, or harder to understand
Crying Wolf: Simulate lots of attacks to desensitize admin to IDS
Session Splicing: One basic technique is to split the attack payload into multiple small packets, so that the IDS must reassemble the packet stream to detect the attack. A simple way of splitting packets is by fragmenting them, but an adversary can also simply craft packets with small payloads. The 'whisker' evasion tool calls crafting packets with small payloads 'session splicing'.
False Flags: URG or RST flags to disrupt traffic flow.
Encryption

EVADING FIREWALLS

IP Spoofing: Make traffic appear like it's coming from a trusted host.
Source Routing: Route traffic around the firewall.
Fragmentation: Break packets into smaller pieces so flags are not in first packet.
Proxy in or access site via IP address: Some firewalls block certain URLs
ICMP Tunneling: (also known as ICMPTX) establishes a covert connection between two remote computers (a client and proxy), using ICMP echo requests and reply packets. An example of this technique is tunneling complete TCP traffic over ping requests and replies.
loki, ncovert, 007shell
ACK Tunneling: exploit the fact that some firewalls do not check packets that have the ACK bit configured.
HTTP Tunneling: An obvious choice because HTTP ports are pretty much always open.
HTTPTunnel

CEH Chapter 17: Physical Security

USBs, external hard drives, flash drives and iPods all pose a threat because they can steal large amounts of information quickly and be easily hidden.

Sanitize Drives after Use:
Drive Wiping: Rewriting a drive 7 times
Zeroization: Overwriting all data with zeros
Degaussing: Basically hitting a hard drive with an extremely powerful electromagnet. This process bricks it.
Physical Destruction: Up to and including melting down the drives.

1. Finger Scanners: Popular on new laptops
2. Hand Geometry Systems: Measures unique distances in hand
3. Palm Scan Systems: Measure creases and ridges of users palm

4. Retina Pattern Systems: Very accurate
5. Iris Recognition: Matches blood vessels in the back of the eye
6. Voice Recognition: Voice analysis
7. Keyboard Dynamics: Analyzes the user's speed and pattern of typing