CYBRARY

Chapter 1 CEHv9 STUDY GUIDE

"As security increases, ease of use and functionality decrease"

five major elements of InfoSec: confidentiality, integrity, availability, authenticity, and non-repudiation. IS has 3 types: network threats, host threats, and application threats

Confidentiality- the assurance that the information is accessible only to those authorized to have access and controls include data classification, data encryption, and proper equipment disposal.

Integrity -trustworthiness of data or resources in the prevention of improper and unauthorized changes—the assurance that information is sufficiently accurate for its purpose. Ensures information hasn't been altered. Hashing it used to ensure integrity. Bit flipping is one form of integrity attack

Availability- the assurance that systems responsible for delivering, storing, and processing information are accessible when required by authorized users.

Authentication- major role of authentication is to confirm that a user is who he or she claims to be or that information it genuine(authenticity). Digital signatures ensure the authenticity of the sender.

Non-repudiation -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.

Vulnerability- existence of a weakness, design, or implementation. Also called security loophole

Exploit-breach of a system via a vulnerability or malicious software or commands that can cause unanticipated behavior of legitimate software or hardware through attackers taking advantage of the vulnerabilities.

Doxing- publishing personally identifiable information PII

Phreaker manipulates telecommunications systems in order to make free calls.

Cyber-Terrorist-use skills to carry out a **political** agenda; motivated by **religious or political** beliefs

State Sponsored Hacker-work on the behalf of a government or military

Hacktivist-someone that uses their skills to impact a political agenda

Enterprise Information Security Architecture(EISA) -is a collection of requirements and processes that help determine how an organization's information systems are built and how they work

Incident handling includes triage, reporting and detection, analysis, and incident response. When an incident occurs, the handling process begins. Actual incident response occurs during the incident handling process.

Incident management includes vulnerability analysis, artifact handling, announcements, alerts, incident handling, and other incident management services.

****Incident response is part of incident handling, and incident handling is part of incident management. ****

Incident Response Plan

- Identify
- Analyze
- Prioritize
- Resolve
- Report

Incident Management Process- To restore all systems to normal operations asap.

- Review detection
- Analyze Exploitation
- Notify stakeholders
- Contain the exploitation
- Eradicate backdoors
- Coordinate recovery for lost data or services
- Provide reports and lessons learned

Incident Management Process-ECC and Transcender

- Prepare for incident handling and response
- Detect and analyze
- Classify and prioritize
- Notify
- Contain
- Investigate
- Eradicate and recover
- Perform post-incident activities

Security Controls

- Physical-guards, lights and cameras
- Technical-encryption, smart cards, and acls
- Administrative-training, awareness and policy efforts

Security Measures

- Preventative/Deterrent authentication or encryption, Smart Card, fence around building, attack dogs, firewall (technical preventative)
- Detective-bells, alerts, sirens, audits, etc. **Audit Trail!**
- Corrective-backups and restore options, OS upgrades, etc.

Hacking Phases:

- Reconnaissance-gathering information
  - Passive-finding information w/o touching the target. Dumpster diving, observing entry/exit policies, social engineering, network sniffing, etc.
  - Active- uses tools and techniques that may or may not be discovered but put your activities as a hacker at more risk of discovery. Active is that which purposefully puts packets, or specific communications, on a wire to your target.
- Scanning-probe the edge of the network, looking for entry points. Ping sweeps, network mapper, vulnerability scan. Actively applying tools and aggressive techniques to gather information. One of the most important phases used to discover exploitable communication channels, probe as many listeners as possible, and keep track of the one that are useful. Discovery and Port Scanning as well as Enumeration.
- Gaining Access-going active by starting an attack based on what was uncovered in recon and scanning. This is the most exciting true attack phase. Escalation of privileges and cracking passwords happens here
- Maintaining Access-keeping control and access available. Executing applications and Hiding files.
- Clearing/Covering Tracks-remove evidence of attack by removing/altering logs, or even using tunneling protocols to communicate with the system.

Attack Types

- **OS Attacks** – target OS vulnerabilities and default installation behavior
- **Application attacks** - attacks on the actual programming code and software logic of an application
- **Shrink-wrap attacks** - take advantage of the built-in code and scripts most off-the-shelf applications come with. These scripts and code pieces are designed to make installation and administration easier but can lead to vulnerabilities if not managed appropriately.
- **Misconfiguration attacks** - take advantage of systems that are not configured appropriately for security

Infowar is the use of offensive and defensive techniques to create advantage over your adversary.

Host Threats include: malware attacks, foot printing, password attacks, denial-of-service attacks, arbitrary code execution, unauthorized access, privilege escalation, and physical security threats.

Penetration Test is a clearly defined, full-scale test of the security controls of a system or network in order to identify security risks and vulnerabilities and has three major phases.

Pen Test Stages

1. **Preparation** – time it takes to put together the contract. Scope, type of tests, and individuals assigned
2. **Assessment** – also known as security evaluation or conduct phase is the actual assault on the targets
3. **Conclusion** – post assessment with detailed findings of the test and recommendations to improve security

Risk Assessment Activities

1. Threat identification- ID the threats
2. Vulnerability identification-ID the vulnerabilities
3. Control Analysis-evaluate the controls to put in place to address the vulnerabilities

NIST 800-30 Risk Assessment Steps

1. Purpose, scope, and source identification or system characterization
2. Threat identification – identify sources that could cause harm to the environment
3. Vulnerability identification – identify any flaws or weaknesses exist in systems, policies, or procedures
4. Control analysis
5. Likelihood determination
6. Impact analysis – determine extent of loss or degradation due to exploited risk
7. Risk determination – assign values to risk probabilities
8. Communicating and sharing risk assessment information
9. Maintaining the risk assessment

Risk Assessment Components

1. Administrative safeguards-security awareness training, data classification, and background checks
2. Logical safeguards-event logging and password management
3. Physical safeguards-facility access control and equipment inventory

* **Auditing can greatly impact the performance of a system. The act of collecting the audit information takes resources from the system, and storing the gathered information requires disk space.**

Handling Risk

- Accept the risk
- Mitigate the risk/apply controls
- Avoid the risk – cease the activity or process; **remove vulnerable software**
- Transfer the risk to 3rd party

Residual Risk – risk that still exists after security controls have been applied

- Accept the risk
- Apply additional controls
- Transfer to 3rd party

Security Zones

- **Internet** Outside the boundary and uncontrolled. You don't apply security policies to the Internet.
- **Internet DMZ** a controlled buffer network between you and the uncontrolled chaos of the Internet.
- **Production Network Zone** A very restricted zone that strictly controls direct access from uncontrolled zones. The PNZ doesn't hold users.
- **Intranet Zone** A controlled zone that has little-to-no heavy restrictions. This is not to say everything is wide open on the Intranet Zone, but communication requires fewer strict controls internally.
- **Management Network Zone** Usually an area you'd find rife with VLANs and maybe controlled via IPSec and such. This is a highly secured zone with very strict policies.

Threat Modeling

- Identify Security Objectives
- Application Overview
- Decompose Application
- Identify Threats

- Identify Vulnerabilities

Application Threat Model

- Understanding the adversary's view
- Characterizing the security of the system
- Determining threats

ALE = SLE X ARO

ALE - Annualized Loss Expectancy
SLE – Single Loss Expectancy
ARO – Annual Rate of Occurrence
EF – Exposure Factor
Asset value x EF = SLE

Common Criteria (CC) test standard designed to reduce or remove vulnerabilities from a product before release. Four parts are EAL, TOE, ST, and PP.

Protection profiles and **evaluation assurance levels** are the two key components of Common Criteria

Evaluation Assurance Level (EAL) – standard control and testing methods created by DoD level 1-7; how thorough the testing is. Functional testing ---→ Formally verified, designed, and tested

Target of Evaluation (TOE)- what is being tested, product itself

- Black Box – hacker has no knowledge of TOE and tests external type threats/hacks; hardest to perform
- Grey Box - partial knowledge test, but assumes higher privilege to mock insider threats
- White Box – full knowledge of network, system and infrastructure they are targeting also for insider threats with elevated privileges; easiest to perform

Security Target(ST)- documentation describing the TOE and security requirements

Protection Profile (PP)-set of security requirements for the type of product being tested, such as firewall

Mandatory access control (**MAC**) is a method of access control where security policy is controlled by a security administrator: **users can't set access controls themselves**. **Two-factor authentication that includes usernames, passwords, and smart cards implements a mandatory access control.**

Discretionary Access Control (DAC) allows users to set access controls on the resources they own or control.

- **Access Control Policy** This identifies the resources that need protection and the rules in place to control access to those resources.
- **Information Security Policy** This identifies to employees what company systems may be used for, what they cannot be used for, exceptions to the policy, reference documents, and what the consequences are for breaking the rules. Generally, employees are required to sign a copy before accessing resources. also known as an Acceptable Use Policy. **HR** is in charge of ensuring employees sign this.
- **Information Protection Policy** This defines information sensitivity levels and who has access to those levels. It also addresses how data is stored, transmitted, and destroyed.
- **Password Policy** This defines everything imaginable about passwords within the organization, including length, complexity, maximum and minimum age, and reuse.
- **E-mail Policy** Sometimes also called the E-mail Security Policy, this addresses the proper use of the company e-mail system.
- **Information Audit Policy** This defines the framework for auditing security within the organization. When, where, how, how often, and sometimes even who conducts information security audits are described here.
- A ***promiscuous*** **policy** is basically wide-open policy allowing everything
- A ***permissive*** **policy** blocks only things that are known to be naughty or dangerous.
- A ***prudent*** **policy** provides maximum security but allows some potentially and known dangerous services because of business needs.

- A ***paranoid* policy** locks everything down, not even allowing the user to open so much as an Internet browser.

The steps for creating security policies are as follows:

1. Perform a risk assessment.
2. Collect standard guidelines to use as guides.
3. Include senior management in the policy development.
4. Set clear penalties and enforce them.
5. Make the final version of the policies available to staff.
6. Ensure that every staff member reads, signs, and understands the policies.
7. Deploy tools to enforce the policies.
8. Train and educate users about the policies.
9. Review and update the policies on a regular basis.

Standards are mandatory rules used to achieve consistency. ***Baselines*** provide the minimum-security level necessary. ***Guidelines*** are flexible recommended actions users are to take in the event there is no standard to follow. And finally, ***Procedures*** are detailed step-by-step instructions for accomplishing a task or goal.

Business Impact Analysis (BIA) effort to identify the systems and processes that are critical for operations.

Business Continuity Plan (BCP) set of plans and procedures to follow in the event of a failure or a disaster to get business services back up and running

Disaster Recovery Plan (DRP) addresses exactly what to do to recover any lost data or services.

Laws and Standards

- **HIPAA** - sets privacy standards to protect patient medical records and health information consisting of 5 subsections: Electronic Transaction and Code Sets, Privacy Rule, Security Rule, National Identifier Requirements, and Enforcement
- **Sarbanes-Oxley (SOX)** to make corporate disclosures more accurate and reliable in order to protect the public and investors from shady behavior
- **Payment Card Industry Data Security Standard (PCI-DSS)** is a security standard for organizations handling credit cards, ATM cards, and other point-of-sales cards. Consists of 12 requirements:
    - 1: Install and maintain firewall configuration to protect data.
    - 2: Remove vendor-supplied default passwords and other default security features.
    - 3: Protect stored data.
    - 4: Encrypt transmission of cardholder data.
    - 5: Install, use, and update AV (antivirus).
    - 6: Develop secure systems and applications.
    - 7: Use “need to know” as a guideline to restrict access to data.
    - 8: Assign a unique ID to each stakeholder in the process (with computer access).
    - 9: Restrict any physical access to the data.
    - 10: Monitor all access to data and network resources holding, transmitting, or protecting it.
    - 11: Test security procedures and systems regularly.
    - 12: Create and maintain an information security policy.
- **COBIT** - an IT governance framework and supporting toolset that allows managers to bridge the gap between control requirements, technical issues and business risks by categorizing control objectives into these domains:
    - Planning and organization
    - Acquisition and implementation

  - Delivery and support
  - Monitoring and evaluation
- **ISO 27000**
  - 27006 describes audits and certifications for security management systems
  - 27001 describes how to perform a risk assessment
  - 27002 describes how to apply security controls after performing the risk assessment
  - 27005 describes how to best manage security risks using an organized and systematic approach

CHAPTER 2

Recon is a term for gathering information on targets, whereas footprinting is more of an effort to map out, at a high level, what the landscape looks like. They are interchangeable terms in CEH parlance, but if you **just remember that footprinting is part of reconnaissance, you'll be fine.**

Footprinting is defined as the process of gathering information on computer systems and networks. It is the **first step in information gathering** and provides a high-level blueprint of the target system or network. It **follows a logical flow**— investigating web resources and competitive intelligence, mapping out network ranges, mining whois and DNS, and finishing up with social engineering, e-mail tracking, and Google hacking.

Anonymous footprinting where you try to obscure the source of all this information gathering

Pseudonymous footprinting making someone else take the blame for your actions

Four main focuses and benefits of footprinting:

1. Know the security posture (footprinting helps make this clear).
2. Reduce the focus area (network range, number of targets, and so on).
3. Identify vulnerabilities (self-explanatory).
4. Draw a network map.

Active Footprinting requires the attacker to touch the device, network, or resource. For example, running a scan on different IPs in a network or actively performing social engineering on employees; anything requiring the hacker to interact with the organization.

Passive Footprinting refers to measures to collect information from publicly accessible sources. For example, perusing websites or looking up public records. Gathering competitive info or ***Competitive Intelligence***, using social media, search engines, **dumpster diving**, IP address and DNS lookups are all examples of passive footprinting.

Computer Fraud and Abuse Act (1986) makes conspiracy to commit hacking a crime.

Some operators for **Google hacking** are as follows: (use google.com/advanced_search)

- **filetype** Syntax: filetype:*type.* This searches only for files of a specific type (DOC, XLS, and so on).
- **index of** Syntax: index of */string*. This displays pages with directory browsing enabled, generally used with another operator.
- **intitle** Syntax: intitle:*string*. This searches for pages that contain a string in the title. For multiple string searches, use the allintitle operator (allintitle:login password, for example).
- **inurl** Syntax: inurl:*string*. This displays pages with a string in the URL. For multiple string searches, use allinurl (allinurl:etc/passwd, for example).
- **link** Syntax: link:*string*. This displays linked pages based on a search term.
- **site** Syntax: site:*domain_or_web_ page string*. This displays pages for a specific website or domain holding the search term.

Web Mirroring Tools

- HTTrack (www.httrack.com)
- Black Widow (http://softbytelabs.com)
- WebRipper (www.calluna-software.com)
- Teleport Pro (www.tenmax.com)
- GNU Wget (www.gnu.org)

- Backstreet Browser (http://spadixbd.com)

EXAM TIP Website Watcher (http://aignes.com) can be used to check web pages for changes, automatically notifying you when there's an update.

EXAM TIP The cacls.exe utility is a Windows command-line tool that can be used to assign, display, or modify access control lists (ACLs) to files or folders. **Taking ownership** from the command line can be done with the **xacls.exe** tool.

Examples of tools for e-mail tracking include GetNotify, Contact- Monkey, Yesware, Read Notify, WhoReadMe, MSGTAG, Trace Email, and Zendio.

DNS Records

- **SRV (Service)** Defines the hostname and port number of servers providing specific services, such as a Directory Services server.
- **SOA (Start of Authority)** Identifies the primary name server for the zone. The SOA record contains the hostname of the server responsible for all DNS records within the namespace, as well as the basic properties of the domain.
- **PTR (Pointer)** Maps an IP address to a hostname (providing for reverse DNS lookups).
- **NS (Name Server)** Defines the name servers within your namespace.
- **MX (Mail Exchange)** Identifies the e-mail servers within your domain.
- **CNAME (Canonical Name)** Provides for domain name aliases within your zone.
- **A (Address)** Maps an IP address to a hostname and is used most often for DNS lookups.

EXAM TIP Know the DNS records well and be able to pick them out of a lineup. You will definitely see a **DNS zone transfer TCP/53** on your exam and will be asked to identify information about the target from it.

NOTE When it comes to DNS, it's important to remember there are two real servers in play within your system. ***Name resolvers*** simply answer requests. ***Authoritative servers*** hold the records for a namespace, given from an administrative source, and answer accordingly.

SOA records provide loads of information, from the hostname of the primary server in the DNS namespace (zone) to the amount of time name servers should retain records in cache. The record contains the following information (all default values are from Microsoft DNS server settings):

- **Source host** Hostname of the primary DNS server for the zone (there should be an NS record for this as well).
- **Contact e-mail** E-mail address of the person responsible for the zone file.
- **Serial number** Revision number of the zone file. This number increments each time the zone file changes and is used by a secondary server to know when to update its copy (if the SN is higher than that of the secondary, it's time to update!).
- **Refresh time** amount of time a secondary DNS server will wait before asking for updates. The default value is 3,600 seconds (1 hour).
- **Retry time** time a secondary server will wait to retry if the zone transfers fails. Default value is 600 seconds.
- **Expire time** maximum amount of time a secondary server will spend trying to complete a zone transfer. The default value is 86,400 seconds (1 day).
- **TTL** minimum "time to live" for all records in the zone. If not updated by a zone transfer, the records will perish. The default value is 3,600 seconds (1 hour).

DIG is another tool you can use to test DNS queries **dig @*server name type.* Use "dig axfr domain.com @ 192.1.1.1" to perform zone transfer of said domain.**

The five regional Internet registries (RIRs) are as follows:

- **American Registry for Internet Numbers (ARIN)** Canada, many Caribbean and North Atlantic islands, and US
- **Asia-Pacific Network Information Center (APNIC)** Asia and the Pacific.
- **Réseaux IP Européens (RIPE) NCC** Europe, Middle East, and parts of Central Asia/Northern Africa.
- **Latin America and Caribbean Network Information Center (LACNIC)** Latin America and the Caribbean.
- **African Network Information Center (AfriNIC)** Africa.

EXAM TIP You need to know nslookup syntax and output very well. Be sure you know how to get into interactive mode with nslookup and how to look for specific information once there.

nslookup [**-option**] [name | -] [server]

INTERACTIVE COMMANDS

host [server]

Look up information for host using the current default server or using server, if specified. If host is an Internet address and the query type is A or PTR, the name of the host is returned. If host is a name and does not have a trailing period, the search list is used to qualify the name.

To look up a host not in the current domain, append a period to the name.

server domain

lserver domain

Change the default server to domain; **lserver** uses the initial server to look up information about domain, while **server** uses the current default server. If an authoritative answer can't be found, the names of servers that might have the answer are returned.

exit

Exits the program.

set keyword[=value]

This command is used to change state information that affects the lookups. Valid keywords are:

all

Prints the current values of the frequently used options to **set**. Information about the current default server and host is also printed.

class=value

Change the query class to one of:

IN the Internet class

CH the Chaos class

HS the Hesiod class

ANY wildcard

The class specifies the protocol group of the information.

(Default = IN; abbreviation = cl)

[no]**debug**

Turn on or off the display of the full response packet and any intermediate response packets when searching.

(Default = nodebug; abbreviation = [no]deb)

[no]**d2**

Turn debugging mode on or off. This displays more about what nslookup is doing.

(Default = nod2)

domain=name

Sets the search list to name.

[no]**search**

If the lookup request contains at least one period but doesn't end with a trailing period, append the domain names in the domain search list to the request until an answer is received.

(Default = search)

port=value

Change the default TCP/UDP name server port to value.

(Default = 53; abbreviation = po)

querytype=value

type=value

Change the type of the information query.

(Default = A; abbreviations = q, ty)

[no]**recurse**

Tell the name server to query other servers if it does not

have the information.
(Default = recurse; abbreviation = [no]rec)

retry=number
Set the number of retries to number.

timeout=number
Change the initial timeout interval for waiting for a reply
to number seconds.

[no]**vc**
Always use a virtual circuit when sending requests to the
server.
(Default = novc)

Traceroute Tools

- McAfee Visual Trace/NeoTrace
- Trout
- VisualRoute
- Magic NetTrace
- Network Pinger
- GEO Spider
- Ping Plotter

Traceroute Windows uses tracert and **ICMP**, Linux uses traceroute and **UDP** (or other options).
When using traceroute to map the path a packet travels over a network, the **host decrements the TTL by one** and **forwards the packets to the next host**. Conversely, traceroute will continue to **increment the TTL for each hop discovered** until the destination is reached or it times out.
Web spiders are applications that crawl through a website, reporting information on what they find.
Two tools in any discussion on social engineering and general footprinting are Maltego and SEF
Maltego "an open source intelligence and forensics application" designed explicitly to demonstrate social engineering (and other) weaknesses for your environment.
SEF great tools that can automate things such as extracting e-mail addresses out of websites and general preparation for social engineering. SEF also has ties into Metasploit payloads for easy phishing attacks.
Research tools available for new exploits or outbreaks are the

CHAPTER 3

Scanning is the next step after footprinting and is the process of discovering systems on the network to see what ports are open and which applications are running.
MPLS Label - comprised of the label, traffic class (TC), bottom-of-stack (S) and time-to-live (TTL) fields

The TCP header flags are as follows:

SYN (Synchronize) This flag is set during initial communication establishment. It indicates negotiation of parameters and sequence numbers.
ACK (Acknowledgment) This flag is set as an acknowledgment to SYN flags. This flag is set on all segments after the initial SYN flag.
RST (Reset) This flag forces a termination of communications (in both directions).
FIN (Finish) This flag signifies an ordered close to communications.
PSH (Push) This flag forces the delivery of data without concern for any buffering. In other words, the receiving device need not wait for the buffer to fill up before processing the data.
URG (Urgent) When this flag is set, it indicates the data inside is being sent out of band. Cancelling a message mid-stream is one example.
EXAM TIP Know the TCP flags and the three-way handshake well. You'll be asked questions on what flags are set at different points in the process, what responses a system provides given a particular flag receipt, and what the sequence numbers look like during a data exchange.

IDS Evasion - Packet builders like Colasoft can be used to create fragmented packets to **bypass IDS** (and possibly firewalls) in your target network**.** Another option is **sending large amounts of traffic** to hide the attack traffic.

SYN/FIN scanning using IP fragments to **avoid false positives** generated by other scans because of a **packet-filtering device** on the target system.

Well-known ports 0–1023

Registered ports 1024–49,151

Dynamic ports 49152–65,535

Port Number	Protocol	Transport Protocol	Port Number	Protocol	Transport Protocol
20/21	FTP	TCP	110	POP3	TCP
22	SSH	TCP	135	RPC	TCP
23	Telnet	TCP	137–139	NetBIOS	TCP and UDP
25	SMTP	TCP	143	IMAP	TCP
53	DNS	TCP and UDP	161/162	SNMP	UDP
67	DHCP	UDP	389	LDAP	TCP and UDP
69	TFTP	UDP	443	HTTPS	TCP
80	HTTP	TCP	445	SMB	TCP

EXAM TIP CurrPorts is a tool you'll definitely want to play with when it comes to ports. It displays a list of all currently opened TCP/IP and UDP ports on your local computer, including information about the process that opened the port, the process name, full path, version information, the time it created, and the user who created it.

CLOSE_WAIT shows that the remote side of your connection has closed the connection

TIME_WAIT state indicates that your side has closed the connection

EC-Council's Scanning Methodology Phases:

1. *Check for live systems.* Ping can provide this. This gives you a list of what's actually alive on your network

2. *Check for open ports.* Once you know which IP addresses are active, find what ports they're listening on.

3. *Scan beyond IDS.* Sometimes your scanning efforts need to be altered to avoid IDS

4. *Perform banner grabbing.* Banner grabbing and OS fingerprinting will tell you what operating system is on the machines and which services they are running. Externally you can use www.netcraft.com to scan servers to get restricted URLs and OS.

5. *Scan for vulnerabilities.* focused look at the vulnerabilities these machines haven't been patched for yet.

6. *Draw network diagrams.* network diagram will display logical and physical links to targets you might like.

7. *Prepare proxies.* This obscures your efforts to keep you hidden.

A **ping sweep** is the easiest method for identifying active machines on the network. An ICMP Echo Request (Type 8) message is sent to each address on the subnet. Live hosts reply with an ICMP Echo Reply (Type 0)

ICMP Type 3 Code 13 will show that the traffic is being blocked (filtered) by a firewall (or router).

An **ICMP Type 3 Code 3** will tell you the client *itself* has the port closed

ICMP Message Type	Description and Important Codes
0: Echo Reply	Answer to a Type 8 Echo Request.

3: Destination Unreachable	Error message indicating the host or network cannot be reached. The codes follow: **0**—Destination network unreachable **1**—Destination host unreachable **3**—Port unreachable **4**—Fragmentation needed and DF-bit was set **6**—Network unknown **7**—Host unknown **9**—Network administratively prohibited **10**—Host administratively prohibited **13**—Communication administratively prohibited
4: Source Quench	A congestion control message.
5: Redirect	Sent when there are two or more gateways available for the sender to use and the best route available to the destination is not the configured default gateway. The codes follow: **0**—Redirect datagram for the network **1**—Redirect datagram for the host
8: Echo Request	A ping message, requesting an Echo reply.
11: Time Exceeded	The packet took too long to be routed to the destination (Code 0 is TTL expired).

EXAM TIP In another brilliant move, ECC also calls ping sweeps or ICMP sweeps or **"ICMP Echo scanning."** Additionally, another option for identifying machines not alive now is called a "list scan"—basically just run a reverse DNS lookup on all IPs in the subnet.

EXAM TIP Know ICMP well. Pay particular attention to **Type 3** messages and the associated codes, especially **Code 13,** which lets you know a **poorly configured firewall** is preventing the delivery of ICMP packets.

Scanning techniques are split into two categories – Scanning TCP Services & Scanning UDP Services

Port Scan Types

A scan type will be defined by three things: what flags are set in the packets before delivery, what responses you expect from ports, and how stealthily the scan works.

Full connect Also known as a *TCP connect or full open scan,* this runs through a full connection (three-way handshake) on all ports, tearing it down with an RST at the end. It is the easiest to detect but it's possibly the most reliable. Open ports will respond with a SYN/ACK, and closed ports will respond with an RST.

Stealth Also known as a *half-open scan* (and also as a SYN scan). Only SYN packets are sent to ports (no completion of the three-way handshake ever takes place; meaning SYN/ACK is not answered). Responses from ports are the same as they are for a TCP connect scan. This technique is useful in hiding your scanning efforts, possibly bypassing firewalls and monitoring efforts by hiding as normal traffic.

Inverse TCP flag; also FIN or NULL uses the FIN, URG, or PSH flag or no flags at all to poke at system ports. If the **port is open, there will be no response**. If the **port is closed, an RST/ACK** will be sent in response. Doesn't work on Windows either.

XMAS A Christmas scan is so named because all flags are turned on (FIN, URG, and PUSH), so the packet is "lit up" like a Christmas tree. **Open port = No Response Closed Port=RST/ACK**. XMAS scans do not work against Microsoft Windows Machines as they are not RFC 793 compliant.

ACK flag probe attacker sends the ACK flag and looks at the return header (TTL or Window fields) to determine the port status. In TTL version, if **TTL of the returned RST packet is less than 64, the port is open**. In Window version, if the **WINDOW size on the RST packet has anything other than zero, the port is open**.

IDLE This uses a spoofed IP address to elicit port responses during a scan. Designed for stealth, this scan uses a SYN flag and monitors responses as with a SYN scan. It also uses an inactive zombie system and IPID numbers. If the IPID increments, the zombie is not truly idle.

EXAM TIP ACK flag probes can be used to check filtering at the remote end. If an ACK is sent and there is no response, this **indicates** a stateful firewall is between the attacker and the host and the port was filtered. If an RST comes back, the port is not filtered and there is not a stateful firewall in place.

Scan Type	Initial Flags Set	Open Port Response	Closed Port Response	Notes
Full (TCP connect)	SYN	SYN/ACK	RST	Noisiest but most reliable.*
Stealth	SYN	SYN/ACK	RST	No completion of three-way handshake; designed for stealth but may be picked up on IDS sensors.
XMAS	FIN/URG/PSH	No response	RST	Doesn't work on Windows
Inverse TCP/Null	FIN, URG, or PSH (or no flags at all)	No response	RST/ACK	Doesn't work on Windows

NMAP

to scan a single IP

nmap 192.168.1.100

scanning multiple IPs

nmap 192.168.1.100 192.168.1.101

scanning an entire subnet

nmap 192.168.1.0/24

- The **"s"** commands determine the **type of scan** to perform, the **"P"** commands set up **ping sweep options**, and the **"o"** commands deal with **output.** The **"T"** commands deal with **speed and stealth**, with the serial methods taking the longest amount of time. **Parallel methods (T3-T5)** are much faster because they run multiple scans at once. The **–A switch** turns on **OS detection, version detection, script scanning, and traceroute**, just as the **–O, -sV, -sC, and –traceroute** switches do in conjunctions with each other.
- **Nmap –script http-methods –script-args one.two.sample.com** will list port, state, service, reason and supported methods of GET PUT HEAD POST, etc.. **PUT, DELETE, TRACE, and CONNECT** are considered risky
- **–sn**(probe only, host discovery not port scan) and **–Pn**(port scan only, no discovery)
- **-sC** to automate and customize the scan. It activates the NSE (Nmap scripting engine) and allows Lua scripts to be use
- **-sU** specifies UDP scan
- **-sV** service versioning for each port
- **-sO** specifies IP Protocol scan
- **-sA** ACK scan, if ports come back as "unfiltered" means there is NO stateful firewall in the path. RST would indicate a stateful firewall. ACK scan, we **cannot tell which ports are open**, just if we can access them.

Nmap Switch	Description	Nmap Switch	Description
-sA	ACK scan	-PI	ICMP ping
-sF	FIN scan	-Po	No ping
-sI	IDLE scan	-PS	SYN ping
-sL	DNS scan (a.k.a. list scan)	-PT	TCP ping
-sN	NULL scan	-oN	Normal output
-sO	Protocol scan	-oX	XML output

-sP	Ping scan	-T0	Serial, slowest scan
-sR	RPC scan	-T1	Serial, slowest scan
-sS	SYN scan	-T2	Serial, normal speed scan
-sT	TCP connect scan	-T3	Parallel, normal speed scan
-sW	Windows scan	-T4	Parallel, fast scan
-sX	XMAS scan		

Hping

Switch	Description
-1	Sets ICMP mode. For example, **hping3 -1 172.17.15.12** performs an ICMP ping.
-2	Sets UDP mode. For example, **hping3 -2 192.168.12.55 –p 80** performs a UDP scan on port 80 for 192.168.12.55.
-8	Sets scan mode, expecting an argument for the ports to be scanned (single, range [1–1000], or “all”). For example, **hping3 -8 20-100** scans ports 20 through 100.
-9	Sets Hping in listen mode, to trigger on a signature argument when it sees it come through. For example, **hping3 -9 HTTP –I eth0** looks for HTTP signature packets on eth0.
--flood	Will send packets as fast as possible, without taking care to show incoming replies. For example, a SYN flood from 192.168.10.10 against .22 could be kicked off with **hping3 –S 192.168.10.10 –a 192.168.10.22 –p 22 --flood**.
-Q *--seqnum*	This option can be used in order to collect sequence numbers generated by the target host. This can be useful when you need to analyze whether a TCP sequence number is predictable (for example, **hping3 172.17.15.12 –Q –p 139 -s**).
-F	Sets the FIN flag.
-S	Sets the SYN flag.
-R	Sets the RST flag.
-P	Sets the PSH flag.
-A	Sets the ACK flag.
-U	Sets the URG flag.
-X	Sets the XMAS scan flags.

EXAM TIP ***active* OS fingerprinting** involves sending crafted, nonstandard packets to a remote host and analyzing the replies. ***Passive* OS fingerprinting** involves sniffing packets without injecting any packets into the network

EXAM TIP spoofing an IP means any data coming back to the fake address will not be seen by the attacker

EXAM TIP It’s important to remember a proxy isn’t just a means for obfuscating source. Proxies are used for all sorts of things, so when those weird questions show up asking you what the proxy is for, use contextual clues. If you want to set up ***proxy chains,* where multiple proxies further hide your activities**, you can use tools such as Proxy Switcher, Proxy Workbench, ProxyChains, SoftCab’s Proxy Chain Builder, CyberGhost, and Proxifier

Gzapper-program to remove google tracking cookies

Vulnerability Scanners – can gather application configuration errors and network topology weaknesses. They also utilize automated processes, scan for open ports/services, and can operate proactively to locate issues.

- Nessus from Tenable
- GFI LanGuard-quality vuln and compliance scanning
- Qualys FreeScan – testing websites and applications for OWASP top risks/malware
- OpenVAS-basically free version of Nessus
- **Ecora Auditor Professional** - uses a non-agent architecture to discover, collect, analyze, and report configuration data across an enterprise infrastructure. Its features include centralized configuration

auditing, change management, compliance reporting for standards like SOX, PCI, GLBA, and HIPAA, and IT configuration analysis against industry standards like ITIL, CobiT, NIST, and ISO 17799

Enumeration-listing the items you find within a specific target; moving from passive information gathering to active gathering

security identifier (SID) identifies user, group, and computer accounts and follows a specific format.

resource identifier (RID) is a portion of the overall SID identifying a specific user, computer, or domain. Starts at **500 for the administrator account**, 501 for guest, and 1000 for users; so 1014 would be the 14th person added to the system.

Security accounts manager (SAM) **C:\Windows\System32\Config\SAM**- SAM file holds in encrypted format, all the local credential hashes for accounts on the machine

The **SSDP service** controls communication for the Universal Plug and Play feature **(uPnP)**

EXAM TIP Linux enumeration commands include, but are not limited to, finger (which provides information on the user and host machine), rpcinfo and rpcclient (which provide information on RPC in the environment), and showmount (which displays all the shared directories on the machine).

Banner Grabbing- sending an unsolicited request to an open port to see what, if any, default message (banner) is returned. Use telnet:ip:port to get a return. Also can use netcat nc:ip:port

EXAM TIP ECC defines two different categories of **banner grabbing—active and passive**. Active banner grabbing is sending specially crafted packets to remote systems and comparing responses to determine the OS. Passive banner grabbing involves reading error messages, sniffing traffic, or looking at page extensions.

NetBIOS Enumeration- provides the same three services on a network segment: name servicing, connection-less communication, and some Session layer stuff via CLI and API. NetBIOS name is a 16-character ASCII string used to identify network devices— 15 characters define the name, and the 16th character is reserved for the service or name record type.

Tools: Nbtstat, SuperScan, Hyena, Winfingerprint, NetBIOS Enumerator, and NSAuditor.

Code	Type	Meaning
<1B>	UNIQUE	Domain master browser
<1C>	UNIQUE	Domain controller
<1D>	GROUP	Master browser for the subnet
<00>	UNIQUE	Hostname
<00>	GROUP	Domain name
<03>	UNIQUE	Service running on the system
<20>	UNIQUE	Server service running

EXAM TIP NetBIOS enumeration questions will generally be about three things:

- Identifying the code and type
- The fact NetBIOS name resolution doesn't work at all on IPv6
- Which tools can be used to perform it

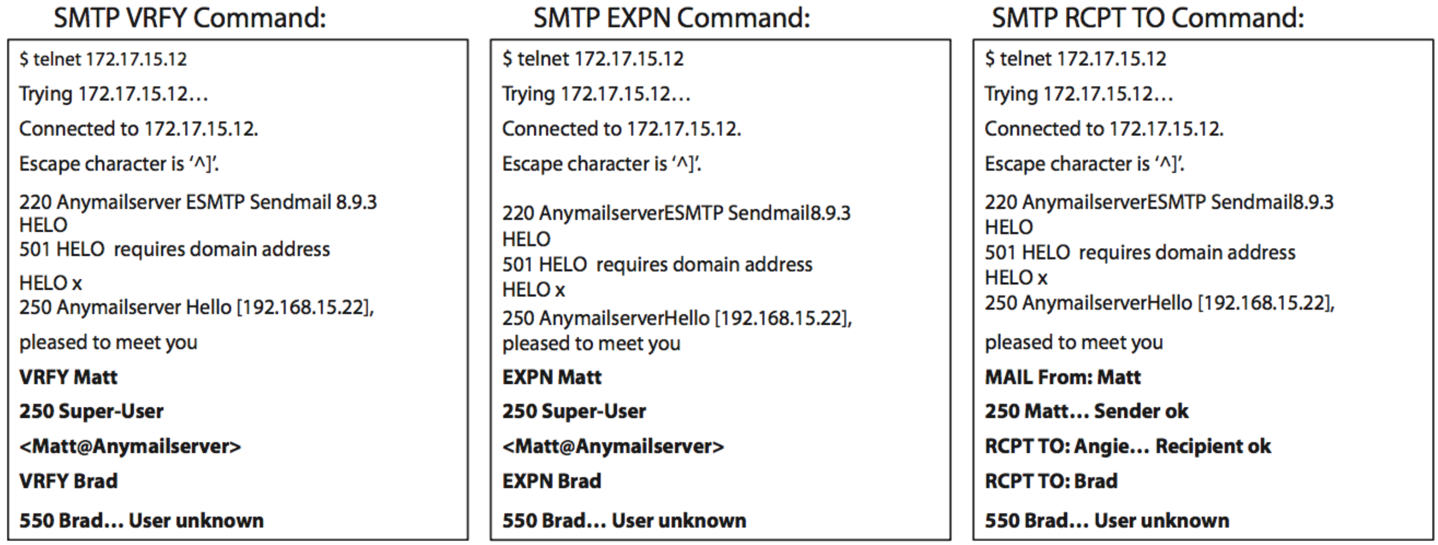
SNMP Enumeration- GET asks a device for information like a value and SET is used to make configuration changes. V1=community strings V2=community strings+acls V3=encrypts community strings

Tools: Engineer's Toolset(solarwinds), SNMPScanner, OpUtils 5 and SNScan.

LDAP Enumeration-LDAP is designed to be queried on tcp/389 to a directory system agent (DSA). LDAP structure is queried and returns an answer using Basic Encryption Rules (BER). Types of information we can glean from LDAP: valid user names, domain information, addresses and telephone numbers, system data, and organizational structure, among other items. Tools: Softerra, JXplorer, Lex, and LDAP Admin Tool

<u>NTP Enumeration</u>- udp/123; querying ntp server can provide: name/ip of systems using NTP, possibly internal ip addresses if this server is in the DMZ. Tools: NTP Server Scanner, NMAP, Wireshark, AtomSync. Commands: ntptrace, ntpdc, and ntpq.

<u>Email Enumeration</u>- SMTP holds three commands—VRFY (validates user), EXPN (provides the actual delivery addresses of mailing lists and aliases), and RCPT TO (defines recipients)—and servers respond differently to these commands



SMTP VRFY Command:

```
$ telnet 172.17.15.12
Trying 172.17.15.12...
Connected to 172.17.15.12.
Escape character is '^]'.
220 Anymailserver ESMTP Sendmail 8.9.3
HELO
501 HELO  requires domain address
HELO x
250 Anymailserver Hello [192.168.15.22],
pleased to meet you
VRFY Matt
250 Super-User
<Matt@Anymailserver>
VRFY Brad
550 Brad... User unknown
```

SMTP EXPN Command:

```
$ telnet 172.17.15.12
Trying 172.17.15.12...
Connected to 172.17.15.12.
Escape character is '^]'.
220 AnymailserverESMTP Sendmail8.9.3
HELO
501 HELO  requires domain address
HELO x
250 AnymailserverHello [192.168.15.22],
pleased to meet you
EXPN Matt
250 Super-User
<Matt@Anymailserver>
EXPN Brad
550 Brad... User unknown
```

SMTP RCPT TO Command:

```
$ telnet 172.17.15.12
Trying 172.17.15.12...
Connected to 172.17.15.12.
Escape character is '^]'.
220 AnymailserverESMTP Sendmail8.9.3
HELO
501 HELO  requires domain address
HELO x
250 AnymailserverHello [192.168.15.22],
pleased to meet you
MAIL From: Matt
250 Matt... Sender ok
RCPT TO: Angie... Recipient ok
RCPT TO: Brad
550 Brad... User unknown
```

EXAM TIP protocol encryption, authentication, and message integrity functions. NTPv3 and SMTPv3 both provide these.

<u>Anonymizers</u>- Guardstar, Psiphon, Ultrasurf, and Proxify. Tails is as well, but it is an OS

<u>CHAPTER 4</u>

Sniffing and Evasion

EXAM TIP In IPv6, fe80::/10 is for link- local addressing. The unique local address (the counterpart of IPv4 private addressing) is in the fc00::/7 block. Prefixes for site local addresses will always be FEC0::/10.

Wiretapping can be active or passive. Active wiretapping involves interjecting something into the communication (traffic), for whatever reason. Passive only monitors and records the data.

<u>Active Sniffing</u>-easier to detect than passive sniffing and is usually required in switched network. **ARP poisoning or mac flooding and utilizing a SPAN port** are three examples of sniffing on switched network

EXAM TIP MAC flooding is "switch port stealing." Flood the CAM with unsolicited ARPs, but don't fill the table, you're only interested in updating the information regarding a specific port, causing something called a "race condition," where the switch keeps flipping back and forth between the bad MAC and the real one.

ARP- Is prone to MiTM attacks and maps a 32-bit IP to 48-bit MAC

Process of maliciously changing an ARP cache on a machine to inject faulty entries is known as ***ARP poisoning*** or **ARP Spoofing,** a.k.a. gratuitous *ARP*

EXAM TIP *Equal to* (**==**) *And* (**&&**) *Or* (**or**) *Tcp contains facebook* would filter out all mention of facebook in packets captured

NOTE Wireshark has the ability to filter based on a decimal numbering system assigned to TCP flags. The assigned flag decimal numbers are FIN = 1, SYN = 2, RST = 4, PSH = 8, ACK = 16, and URG = 32. Adding these numbers together (for example, SYN + ACK = 18) allows you to simplify a Wireshark filter. Example: **tcp.flags == 0x2** looks for SYN packets, **tcp.flags == 0x16** looks for ACK packets, and **tcp.flags == 0x18** looks for both.

<u>Tcpdump</u> will perform packet captures in unix/linux.

Tcpdump –I eth1 –w output.pcap turn on eth1 to promiscuous mode

tcpdump -w /log command creates a binary log file in a specific folder, in this case /log.

tcpdump -r file_name command will read packets from a particular file

tcpdump -i int_name command will capture packets from the specified interface.
tcpdump host host_name command will capture packets from the specified host.
netsh firewall show config displays the Windows Firewall settings at a high level. The command is deprecated and replaced with similar command options under the *netsh advfirewall* context.
IDS can be signature based or anomaly/behavior based. To try and bypass one of these with a buffer overflow attack, you would target the signature-based version if possible.

snort -l c:\snort\log\ -c c:\snort\etc\snort.conf
Basically, this says, "Snort application, I'd like you to start logging to the directory c:\snort\log\. I'd also like you to go ahead and start monitoring traffic using the rule sets I've defined in your configuration file located in c:\snort\etc\snort.conf."
./snort –b –A fast –c snort.conf
Snort configuration file contains a number of Snort settings. You can specify the range of IP addresses you are trying to protect (internal) and other networks (external). You should open the Snort configuration file and comment out all of the rules you do not wish to use so they will not be loaded when Snort is run in network intrusion detection system (NIDS) mode. You can capture all packets by specifying promiscuous mode.
Snort Rules are processed in the order: **Pass, Drop, Alert, Log**

Snort Functions

- Intrusion detection - **./snort –c snort.conf (using snort.conf rule file)**
- Packet sniffing – sniffer mode: **./snort -v**
- Packet logging – packer logger: **./snort –l ./log**
- Log packets in binary - **./snort –b**
- Log timestamp, alert message, source IP and port and destination IP and port - **./snort –A fast**

EXAM TIP libwhisker It's a full-featured Perl library used for HTTP-related functions, including vulnerability scanning, exploitation, and, of course, IDS evasion.
Fragroute is used to intercept, modify, and rewrite egress traffic destined for the specified host in such a way that a NIDS cannot recognize the attack signatures due the manipulations performed on the payload, but a host-based IDS installed on the target system would be able to recognize the attack by monitoring at the application layer, and could report on entries created in the system or access logs.
Network Intrusion Detection System (NIDS) provides user behavior measurement and analysis. Network tunnels and encryption can defeat detection by NIDS. A NIDS experiences a large number of false positives. Also, new attack types will not be detected by a NIDS until the attack signature is captured.
EXAM TIP The *screened subnet* (a.k.a. *public zone*) of your DMZ is connected to the Internet and hosts all the public-facing servers and services your organization provides. These *bastion hosts* sit outside your internal firewall and are designed to protect internal network resources from attack. The *private zone* holds all the internal hosts that, other than responding to a request from inside that zone, no Internet host has any business dealing with. Lastly, because your FW has two or more interfaces, it is referred to as *multi-homed.*

Firewalls

packet-filtering look at the headers of packets coming through a port and decide whether to allow them based on the ACLs configured.
stateful inspection firewalls with the means to track the entire status of a connection. "stateful multilayer inspection" firewalls, with the capability from the Network layer up to the Application layer
circuit-level gateway firewall works at the Session layer and allows or prevents data streams
application-level firewall filters traffic much like a proxy, allowing specific applications (services) in and out of the network based on its rule set.
Linux Firewall ipfwadm was replaced by ipchains for versions 2.2x and in version 2.4x, ipchains was replaced by iptables.

EXAM TIP HTTP tunneling is a firewall evasion technique you'll probably see at least mentioned on the exam. HTTP beacons and HTTP tunnels are the de facto standard implant technology for hackers.

Firewalking process of "walking" through every port against a firewall to determine what is open

CHAPTER 5

Attacking a System

Kerberos makes use of both symmetric and asymmetric encryption technologies to securely transmit passwords and keys across a network. The entire process is made up of a **Key Distribution Center (KDC), an Authentication Service (AS), a Ticket Granting Service (TGS), and the Ticket Granting Ticket (TGT).**

NTLM – uses **DES** for encryption and creates two 7-character sections for up to 14-character password. These sections are padded with spaces and hashed as two sections. If the second section contains **AAD3B435B51404EE**; which is the hash for 7 spaces, we know from looking the pw is 7 characters or less.

Root Level Registry Keys

- **HKEY_LOCAL_MACHINE (HKLM)** hardware (processor type, bus architecture, video, disk I/O, and so on) and software (operating system, drivers, services, security, and installed applications).
- **HKEY_CLASSES_ROOT (HKCR)** file associations and Object Linking and Embedding (OLE) classes.
- **HKEY_CURRENT_USER (HKCU)** profile information for the user currently logged on. Information includes user-level preferences for the OS and applications.
- **HKEY_USERS (HKU)** specific user configuration information for all currently active users on the computer.
- **HKEY_CURRENT_CONFIG (HKCC)** Contains a pointer to HKEY_ LOCAL_MACHINE\SYSTEM\CurrentControlSet\CurrentControlSet\ Hardware Profiles\Current, designed to make accessing and editing this profile information easier.

Other Important key locations. **If malware is located here, it will run every time a user logs in.**

- HKLM\Software\Microsoft\Windows\CurrentVersion\ RunServicesOnce
- HKLM\Software\Microsoft\Windows\CurrentVersion\ RunServices
- HKLM\Software\Microsoft\Windows\CurrentVersion\ RunOnce
- HKLM\Software\Microsoft\Windows\CurrentVersion\Run
- HKCU\Software\Microsoft\Windows\ CurrentVersion\Explorer\RunMRU –recent commands used
- HKEY\USERSID\Software\Microsoft\ Windows\CurrentVersion\Explorer\RecentDoc –recent files accessed
- HKCU\Software\Microsoft\Windows\CurrentVersion\ Explorer\ComputerDescriptions – systems communicated with

Microsoft Management Consoles (MMCs)have been around for a long while and are basically small GUI containers for specific tools. **Compmgmt.msc** = computer management MMC **services.msc** = services MMC and **gpedit.msc** = group policy MMC

Linux Directory Structure

- **/** A forward slash represents the root directory.
- **/bin** directory holds all sorts Linux commands (a lot like the C:\Windows\System32 folder in Windows).
- **/dev** This folder contains the pointer locations to the various storage and input/output systems you will need to mount if you want to use them, such as optical drives and additional hard drives or partitions.
- **/home** This folder holds the user home directories.
- **/mnt** This folder holds the access locations you've actually mounted.
- **/etc** all the administration files and passwords. Both the password and shadow files are found here.
- **/sbin** system binaries folder holds more administrative commands and *daemons*
- **/usr** folder holds almost all of the information, commands, and files unique to the users.

Chmod – change file permissions or **ch**ange **mod**e. Up to 4 digits 0-7 defined by adding permission values
User (rwx) = 4+2+1 = **7**
Group(rx) = 4+1 = **5**
World (rx) = 4+1 = **5**
chmode mode = 0755; entered as ***chmod 755; omitted digits are considered zero***
Chmod 744 would give read, write, execute to user and read only to users in the group, and read only to all other users.

EXAM TIP Adding an ampersand **(&)** after process name indicates that process should run in the background. If you wish for the process to be persistent use the nohup command.
Shadow File stores and displays passwords in encrypted format; referenced by username:x the x tells us shadow file is in use.
Types of Authentication- What you know (password) what you have (token) and what you are (biometrics)
Biometric System Measurements
False Rejection Rate (FRR), is the % of time a biometric reader will deny access to a legitimate user.
False Acceptance Rate (FAR), is the percentage of unauthorized access given by the system. The two measurements are charted together, and where they intersect is known as the crossover error rate (CER), which becomes a ranking measurement of biometric systems (the lower the CER, the better the system).
Four main attack types for password cracking:
non-electronic-social engineering, shoulder surfing, dumpster diving
active online – directly communicating with the victim machine. Examples are dictionary/brute-force attacks, hash injections, phishing, Trojans, spyware, keyloggers, and password guessing
passive online – sniffing packets in hopes to intercept passwords in clear text or hashes for MITM
offline – attacker steals copy of password file to work on offline
EXAM TIP software keyloggers are easy to spot with antivirus and other scanning options, whereas hardware keyloggers are almost impossible to detect.
net view /domain:*domainname* Shows all systems in the domain name provided
net view \\*systemname* Provides a list of open shares on the system named
net use \\*target*\ipc$ "" /u: " Sets up a null session
EXAM TIP Just typing **net use** will show your list of **connected shared resources**. Typing **net use Z: \\*somename*\*fileshare*** will mount the folder *fileshare* on the remote machine *somename*. If you add a **/persistent:yes** switch to it, the mount will stay after a reboot. Change it to **no** and it won't. For example:
net use F: \\\\MATTBOX\BankFiles /persistent:yes | this will create a drive BankFiles (\\\\MATTBOX) (F:)
EXAM TIP Vertical privilege escalation occurs when a lower-level user executes code at a higher privilege level than they should have access to. Horizontal privilege escalation isn't really escalation at all but rather simply executing code at the same user level but from a location that should be protected from access.
alternate data stream (ADS) in the form of (NTFS) file streaming. For instance, **"echo bad stuff > good.txt:shh"** will "push" the text "bad stuff" into the good.txt file with an alternate stream named "shh". **Streams.exe, SFind, and ADS Spy** will help locate ADSs. **To Execute** start readme.txt:badfile.exe
EXAM TIP Another term used in regard to steganography is *semagram,* and there are two types. A visual semagram uses an everyday object to convey a message. Examples can include doodling. A text semagram obscures a message in text by using things such as font, size, type, or spacing.
Windows Logs-default location c:\system32\config, but also these can be moved or hidden in registry.

- **Application** – entries related to applications
- **System**- registers system events like startup/shutdown, drivers failing, etc..
- **Security** – records login attempts, access and activities regarding resources
- **Registry entry:** HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\EventLog

Rootkits- software designed to obscure compromise. Examples are Azazel, Avatar, Necurs, and ZeroAccess.
Types of Rootkits

- **Hypervisor level** These rootkits modify the boot sequence of a host system to load a vm as the host OS.
- **Hardware (firmware)** These rootkits hide in hardware devices or firmware.
- **Boot loader level** These rootkits replace the boot loader with one controlled by the hacker.
- **Application level** these replace valid application files with Trojan binaries. These kits work inside an application and use various means to change the application's behavior, user rights level, and actions.
- **Kernel level** These rootkits attack the boot sectors and kernel level of the operating systems themselves, replacing kernel code with backdoor code. These rootkits are by far the **most dangerous and are difficult** to detect and remove. If this happens, **restore from local backup media**
- **Library level** These rootkits basically use system-level calls to hide their existence.

protection rings refer to concentric, hierarchical rings from the kernel out to the applications, each with its own fault tolerance and security requirements. The kernel is referred to as Ring 0, while drivers (Ring 1), libraries (Ring 2), and applications (Ring 3, also known as user mode)

EXAM TIP "Steps for Detecting Rootkits." First, run the *dir /s /b /ah* command and the *dir /s /b /a-h* command in the potentially infected operating system and save the results. Next, boot a clean CD version
and run the same commands for the same drive again. Last, use WinDiff (https://support.microsoft.com/en-us/kb/159214) on both results to see any hidden malware.

CHAPTER 6

Web Hacking: Servers and Applications

Organizations:

Internet Engineering Task Force (IETF) IETF creates engineering documents to help make the Internet work better from an engineering point of view. The IETF's official documents are published free of charge as Requests For Comments (RFCs)

Open Source Security Testing Methodology Manual (OSSTMM) focuses operational security. It is about knowing and measuring how well security works by examining the controls that have been put in place

Process controls for OSSTMM:

- non-repudiation – participants can't deny the actions they take
- confidentiality – only participants have knowledge of an asset
- privacy – ensures only participants have access to the asset
- integrity – ensures participants know when processes or assets change
- alarm

Types of Compliance for OSSTMM: Contractual deals with **industry** requirements like PCI-DSS. **Legislative** deals with government regulations. **Standards based** addresses compliance to obtain or keep certification from an organization or group.

Open Web Application Security Project (OWASP) focused on improving the security of software. OWASP also maintains **WebGoat** . The provide "top tens" like Proactive Controls and Most Critical Web Application Risks

The OWASP Top Ten Proactive Controls:

- Verify for security early and often.
- Parameterize queries.
- Encode data.
- Validate all inputs.
- Implement identity and authentication controls. – **passwords, encryption keys, and session tokens. Broken Authentication and Session Management**
- Implement appropriate access controls.
- Protect data.
- Implement logging and intrusion detection.

- Leverage security frameworks and libraries.
- Implement error and exception handling.

The OWASP Top Ten Most Critical Web Application Security Risks

1. **Injection**
2. **Broken Authentication and Session Management**
3. **Cross-Site Scripting (XSS)**
4. Insecure Direct Object References
5. Security Misconfiguration
6. Sensitive Data Exposure
7. Missing Function Level Access Control
8. Cross-Site Request Forgery (CSRF)
9. Using Components with Known Vulnerabilities
10. Unvalidated Redirects and Forwards

Web Application Architecture

- Client or presentation layer - this is the top-most tier of the application that the user sees.
- Business logic layer - this tier controls how the application works.
- Database layer - this tier handles and stores all the data required for the application.

6 stages in web server attack methodology:

- information gathering
- footprinting
- mirroring websites
- vulnerability scanning
- session hijacking
- password cracking

Security Development Lifecycle Phases:

- Training – core security training for developers
- Requirements – level of security desired is defined and set
- Design – requirements, attack surface analysis, and threat modeling
- Implementation – using approved tools and static analysis; also turning off unsafe functions
- Verification – dynamic analysis, **fuzz testing**, and attack surface reviews are performed
- Release – incident response plan, final security review and certification
- Response

Fuzz Testing - using large amounts of data or "fuzz" to discover coding errors and security loopholes.

EXAM TIP Apache httpd.conf file controls who can view the server status page. The php.ini file is one you want to look at for the verbose error messaging setting.

EXAM TIP DNS amplification manipulates recursive DNS to DoS a target. The bad guy uses a botnet to amplify DNS answers to the target until it can't do anything else.

EXAM TIP URL tampering. In short, you just manipulate parameters within the URL string in hopes of modifying data such as permissions and elevation of privileges, prices and quantities of goods, and credentials.

EXAM TIP This ../dot-dot-slash attack %2E%2E%2F is a variant of Unicode or unvalidated input attack. *Unvalidated input* means the server has not been configured to accept only specific input during an HTTP GET, so an attacker can craft the request to ask for command prompts, to try administrative passwords, and so on.

```
http://www.verigon.com/script.ext?template=%2e%2e%2f%2e%2e%2f%2e%2e%2f%65%
74%63%2f%70%61%73%73%77%64 %0D%70%61%73%73%77%64 = passwd
```

DECODED is:

```
http://www.verigon.com/script.ext?template=../../../etc/passwd passwd =
passwd
```

Carriage Return/Line Feed (CRLF) attack describes when characters for a carriage return (<CR>) and line feed (<LF>) are inserted into a stream reading by an application.

```
Email is not working&lt;CR&gt;&lt;LF&gt;Bcc: user@sneaknet.com
```

CSPP (Connection String Parameter Pollution) is an injection attack that takes advantage of web applications that communicate with databases by **using semicolons** to separate each parameter. This attack can be used to steal user identities and hijack web credentials

Metasploit framework contains:

- Interfaces
- Libraries
- Modules
- Plug-ins
- Web Services

Pivoting – using a compromised system as jumping off point to compromise other systems. Can add routes in metasploit to access network(s) behind the compromised system.

Metasploit Modules

- Exploits-hold the actual exploit; which you can modify
- Payloads-combines the arbitrary code executed if the exploit is successful
- Auxiliary- used to run one-off actions like scans
- NOPS-used for buffer overflow like this IDS entry. Uses module **x86/opty2**
    - Mar 30 10:31:07 [1123}: IDS1661/**NOPS-x86**: 64.118.55.64:1146-> 192.168.119.56:53
- REX library for most tasks

Core Impact Pro Probably the best-known all-inclusive automated pen testing framework

CANVAS another automated pen test tool

LDAP Injection the attacker changes what's entered into the form field by adding the characters **)(&)** after the username and then providing any password.

(&(USER=Matt)**(&)**(PASSWORD=Anything))

Canary Words- are known values placed between the buffer and control data. When a buffer overflow occurs, the canary words are the first to be corrupted; which will create an alert.

XSS Attacks- occurs when the bad guys take advantage of scripting on a site and have it perform something other than the intended response. An attacker inputs the following into the Search text box on an entry form:

```
<script type="text/javascript">
        Alert ("It Worked");
</script>
```

The attacker then clicks the Search button and a pop-up appears stating, "It Worked."

JavaScript XSS

The two most important object methods for **JavaScript XSS defacement** attacks are ***getElementById()*** and ***getElementsByTagName().*** The Id method retrieves an element node based on its identifier, such as the field name, like username or password. The Tag Name method retrieves an array of element nodes based on the tag name like h1 or a. Using these two methods, an attacker can easily deface the website as follows:

```
function defaceFirstHeader(){
   document.getElementsByTagName("h1")[0].innerHTML =
    "YOU'VE BEEN HACKED!";
}
```

EXAM TIP XSS attempt: **http://IPADDRESS/";!- -"<XSS>=&{()}.**

Prevent XSS attacks on cookies is to set the **HttpOnly flag** in an HTTP response header, the cookie cannot be accessed through client side script.

Injection Attacks

file injection the attacker injects a pointer in the web form input to an exploit hosted on a remote site
command injection the attacker injects commands into the form fields instead of the expected test entry
shell injection the attacker attempts to gain shell access using Java or other functions
Simple Object Access Protocol (SOAP) is designed to exchange structured information in web services and uses XML to format information. SOAP is compatible with HTTP and SMTP, and **messages are typically "one way"** in nature. **SOAP is slower than CORBA** since binary parses faster than XML. SOAP is platform-independent, simplifies communications, and leverages multiple transport protocols.
Session Fixation Attack The attacker logs in to a legitimate site and pulls a session ID, then sends an e-mail with a link containing the fix session ID. When the user clicks it and logs into the same legitimate site, the hacker can now log in and run with the user's credentials. **Defend with random challenge tokens**
Cross-Site Request Forgery (CSRF): user is tricked to visiting malicious website. While the user has an active, authenticated session with a trusted website, the malicious website then instructs the user's browser to send a request to the target/trusted website.

SQL Injection

- **Single Quote (') is best character to start SQL injection attempt**
- **Union query** ECC, in previous versions, concentrated on the use of this with separate databases, but in practice it has nothing to do with that. The UNION command allows you to join together SELECT queries. For example, **SELECT *fname,lname* FROM *users* WHERE *id=$id* UNION ALL SELECT *socialsecuritynumber*,1 FROM *secretstuff***; combines a relatively harmless query with one that's a little more...useful.
- **Tautology** Because user IDs and passwords are often compared and the "true" value allows access, if you trick the db by providing something that is already true then you can sneak by.
- **Blind SQL injection** This occurs when the attacker knows the database is susceptible to injection, but the error messages and screen returns don't come back to the attacker. Takes a long time to pull off.
- **Error-based SQL injection** enumeration technique. The objective is to enter poorly constructed statements in an effort to get the database to respond with table names and other information in its error messages.
- **Mole tool** automates SQL injection attacks
- SQL Injection of **' *or 1=1* --** The single quote (') will terminate the string for the username field, while the OR condition (1=1) automatically forces a true value. The double-dash (--) indicates a T-SQL comment. If the web application returns a SQL error message, then you can add another SQL query after the comment.

CHAPTER 7

Wireless Network Hacking

Wireless Standard	Operating Speed (Mbps)	Frequency (GHz)	Modulation Type
802.11a	54	5	OFDM
802.11b	11	2.4	DSSS
802.11g	54	2.4	OFDM and DSSS
802.11n	100 +	2.4–5	OFDM
802.11ac	1000	5	QAM (Quadrature amplitude modulation)

EXAM TIP 802.11i WPA/WPA2 802.16 ="WiMax," it speeds up to 40 Mbps and is moving toward gigabit speed.
WEP "encryption" options *wired equivalent privacy*
64-bit version uses a 40-bit key
128-bit version uses a 104-bit key
256-bit version uses a 232-bit key
To crack WEP, all you need is SSID and MAC of AP
WPA makes use of something called Temporal Key Integrity Protocol (TKIP), a 128-bit key, and the client's MAC address to accomplish much stronger encryption. The key is changed every 10k packets and they are exchanged back and forth during EAP

WPA-2 *Enterprise*, you can tie EAP or a RADIUS server into the authentication side of WPA2, allowing you to make use of **Kerberos tickets. AES for encryption, ensuring FIPS 140-2 compliance**. As for **integrity** TKIP had some irregularities originally. **WPA2** addresses these by using Cipher Block Chaining Message Authentication Code Protocol (CCMP). CCMP calls them message integrity codes (MICs), and the whole thing is done through cipher block chaining message authentication code (CBC-MAC). To crack WPA2 you must capture the authentication traffic and crack the key, but it is virtually impossible. **MICs** prevent MiTM attacks in WPA. **CCMP provides the integrity method for WPA2; not WPA**

Wireless Standard	Encryption Used	IV Size (bits)	Key Length (bits)	Integrity Check
WEP	RC4	24	40/104	CRC-32
WPA	RC4 + TKIP	48	128	Michael Algorithm + CRC-32
WPA2	AES-CCMP	48	128	CBC-MAC (CCMP)

Kismet works by "channel hopping," to discover as many networks as possible. Second, it has the ability to **passively sniff** packets and save them to a log file, readable by Wireshark or tcpdump. Lastly, Kismet can **find wireless networks** even **when beaconing is turned off.**

"evil twin" SSID on the rogue box is set similar to the legitimate one may also be called **mis-association attack**. Faking a well-known hotspot on a rogue AP is referred to as a **"honeyspot"** attack.

Extensible Authentication Protocol (EAP) – can be used with token cards, Kerberos, one-time passwords, certificates, public key authentication, or **smart cards**

One defense wireless admins attempt to use is to enforce a **MAC filter.** MAC spoofing tools SMAC and TMAC.

Sniffers: Omnipeek, AirMagnet, Wireshark, NetStumbler(windows), Kismet, and Airsnarf

sniffers work at L2 and L3. Windows has issues collecting 802.11 management and control packets.

WiFi Discovery: NetStumbler (windows), WirelessMon, inSSIDer, Vistumbler, PrismStumbler

Aircrack-ng-a sniffer, a wireless network detector, a password cracker, and even a traffic analysis tool. When **targeting WPA2** keys, aircrack-ng can only use **a dictionary list.** When cracking **WEP** keys, aircrack can use **dictionary list, PTW, and Korek.**

Cain and Abel relies on statistical measures and the PTW technique to break WEP codes. It can also extract voice streams from VoIP captures.

Types of jailbreaking: Userland (user access, not admin), iBoot, and Bootrom (admin-level privileges)

Untethered jailbreaking - kernel remains patched/jailbroken after reboot, with or w/o a system connection.

Semi-tethered jailbreaking A reboot no longer retains the patched kernel; however, sw has already been added to the device. If admin privileges are required, the installed jailbreaking tool can be used.

Tethered jailbreaking A reboot removes all jailbreaking patches, and the phone may get stuck in a perpetual loop on startup, requiring a system connection (USB) to repair.

Jailbreaking tools include, but are not limited to, evasi0n7(iOS), GeekSn0w(iOS), Pangu(iOS), Redsn0w(iOS), Absinthe, Cydia(iOS), and SuperOneClick(Android)

Bluetooth devices have two modes: a **discovery mode** and a **pairing mode**. *Discovery mode* determines how the device reacts to inquiries from other devices looking to connect, and it has three actions. The *discoverable* action has the device answer all inquiries, *limited discoverable* restricts that action, and *nondiscoverable* tells the device to ignore all inquiries.

- **Bluesmacking** A simple denial-of-service attack against the device.
- **Bluejacking** Consists of **sending unsolicited messages** to, and from, mobile devices.
- **Bluesniffing** effort to discover Bluetooth-enabled devices—much like war driving in wireless hacking.
- **Bluebugging remotely taking full control** of BT device. **Blooover** is well-known tool
- **Bluesnarfing** actual **theft of data** from a mobile device.
- **BlueScanner** tool used to find BT devices as as well **BT Browser and btCrawler**

- **Blueprinting** footprinting for Bluetooth it involves collecting device information over Bluetooth.

BBProxy is a Blackberry-centric tool that's useful in an attack called blackjacking.

Blackjacking is using a mobile app to gain access to internal networks.

Attacks Only Targeting Mobile Devices

- **Bluebugging – remotely taking full control of mobile device Blooover** well-known tool
- **SMiShing – SMS phishing**
- **Jailbreaking/rooting – removing vendor's sandbox and malicious code protections from mobile**

ZitMo (ZeuS in the Middle) malware aimed at Android phones; taking advantage of two-factor auth; like in banking apps.

CHAPTER 8 Cloud Computing Security

Infrastructure as a Service (IaaS) virtualized computing resources over the Internet. IaaS is a good choice not just for day-to-day infrastructure service, but also for temporary workloads that may change unexpectedly.

Platform as a Service (PaaS) provides a development platform that allows subscribers to develop applications without building the infrastructure it would normally take to develop and launch software.

Software as a Service (SaaS) the provider offers on-demand applications to subscribers over the Internet. Sass benefits include easier administration, automated patch management, compatibility, and version control

public cloud model where services are provided over a network that is open for public use (like the Internet)

private cloud cloud is operated for a single organization (a.k.a. single-tenant environment)

community cloud shared by several organizations, usually with the same policy and compliance considerations

hybrid cloud composition of two or more cloud deployment models

Cloud Computing – also separates data ownership from data custodian duties; ultimate separation of duties.

- **Cloud carrier** has the responsibility of **transferring the data** and is the intermediary for connectivity and transport between subscriber and provider.
- **Cloud consumer** acquires and uses cloud products and services.
- **Cloud provider** purveyor of products and services.
- **Cloud broker** Acts to manage use, performance, and delivery of cloud services, as well as the relationships between providers and subscribers.
- **Cloud auditor** The auditor "provides a valuable inherent function for the government by conducting the independent performance and security monitoring of cloud services."

Federal Risk and Authorization Management Program (FedRAMP) government program that uses a standard approach to security assessment, authorization, and continuous monitoring for cloud products and services.

Cloud Security Alliance (CSA) leading professional organization devoted to promoting cloud security best practices and organizing cloud security professionals.

Trusted computing module **(TC)** an attempt to resolve computer security problems through hardware enhancements and associated software modifications.

Trusted Computing Group (TCG) hw and sw providers who cooperate to come up with specific plans.

Roots of Trust (RoT) set of functions within the TC module that are always trusted by the computer's OS

CloudInspect- tool that offers penetration- testing as a service from Amazon Web Services for EC2 users

CloudPassage Halo- provides instant visibility and continuous protection for servers in any combination of data centers, private clouds and public clouds

Cloud-specific tools include Dell Cloud Manager, Qualys Cloud Suite, Trend Micro's "Instant On" Cloud Security, and Panda Cloud Office Protection.

SOA (Service Oriented Architecture) is an API that makes it easier for application components to cooperate and exchange information on systems connected over a network. SOA vulnerability is an XML denial of service, in which the attacker crafts an XML message with very large payloads, recursive content, excessive nesting, malicious external entities, or with malicious DTDs (Data Type Definitions). It can be **mitigated by**

using XML filters and XML gateways, and by ensuring that the XML parser in use is robust and the XML parsing process is not processor intensive.

EXAM TIP Cloud computing is the ultimate in separation of duties. It also separates the role of data owner from the role of data custodian.

Wrapping Attack SOAP message is intercepted and the data in the envelope is changed and then replayed

Session riding simply CSRF and deals with cloud services instead of traditional data centers. Mitigate with random tokens with each request to the site.

Side channel attack aka ***cross-guest VM breach***, deals with the virtualization itself. If an attacker can somehow gain control of an existing VM (or place his own) on the same physical host as the target.

CHAPTER 9

Trojans and Other Attacks

Purpose of analyzing the interrupts within software? To ensure critical data is not changed on the system.

Malware sw designed/intended to harm or secretly access a system without the owner's informed consent.

wrappers are programs that allow you to bind an executable of your choice (Trojan) to an innocent file your target won't mind opening. *EliteWrap* Can use to hide malware in Windows winlogon.exe like so:

g++ endlessLoop.cpp -o trojanMalware.exe (then bind compilation file to winlogon.exe)

Crypters tools that use a combination of encryption and code manipulation to render malware undetectable to AV and other security monitoring products. Crypters encrypt binary code in executables to hide malware like viruses, keyloggers, and RATs. Some examples are: **SwayzCryptor**, Hidden Sight, Galaxy, and Criogenic.

Packers use compression to pack the malware executable into a smaller size. While this does reduce the file size, it also serves to make the malware harder to detect for some antivirus engines.

Exploit Kits- platforms from which you can deliver exploits and payloads. Examples include, but are not limited to, Infinity, Bleeding Life, Crimepack, and Blackhole Exploit Kit.

Trojan sw that appears to perform a desirable function for the user prior to running or installing it but instead performs a function, usually without the user's knowledge, that steals information or otherwise harms the system or data. Also, a method to gain, and maintain, access on a target machine. Trojan is the means of delivery, and the backdoor provides the open access. Types are defacement, proxy, and botnet like Chewbacca and Skynet. RATs like RAT, MoSucker, Optix Pro, and Blackhole or e-banking like Zeus and Spyeye.

Covert Channel Tunneling Trojan (CCTT) is one form of remote access Trojan that uses a variety of exploitation techniques to **create data transfer channels in previously authorized data streams**. It's designed to provide an external shell from within the internal environment.

Command shell Trojan is intended to provide a backdoor to the system that you connect to via CLI

CryptCat encrypted version of NetCat

Netcat - command-line access to the machine, **nc –e IPaddress Port#** Telnet, type the **–t** option. Backdoor access to a machine, when installed and executed on a remote machine, Netcat opens a listening port of your choice. From your attack machine, you connect using the open port **nc –l –p 5555** opens port 5555 in a listening state on the target machine. You can then type **nc IPAddress –p 5555** and connect to the target machine—a raw "telnet-like" connection. And, just for fun, do you think the following command might provide something interesting (assuming we're connecting to a Linux box)?

nc –l –p 5555 < /etc/passwd

connect to somewhere:

nc [-options] hostname port[s] [ports] ...

listen for inbound:

nc -l -p port [options] [hostname] [port]

options:

```
    -d          detach from console, background mode
    -e prog     inbound program to exec [cmd.exe?]
    -g gateway  source-routing hop point[s], up to 8
    -G num        source-routing pointer: 4, 8, 12, ...
    -h           this cruft
    -i secs       delay interval for lines sent, ports scanned
    -l           listen mode, for inbound connects
    -L           listen harder, re-listen on socket close
    -n           numeric-only IP addresses, no DNS
    -o file       hex dump of traffic
    -p port       local port number
    -r           randomize local and remote ports
    -s addr       local source address
    -t           answer TELNET negotiation
    -u           UDP mode
    -v           verbose [use twice to be more verbose]
    -w secs       timeout for connects and final net reads
    -z           zero-I/O mode [used for scanning]
```

Netcat used for outbound or inbound connections, over TCP or UDP, to or from any port on the machine. It offers DNS forwarding, port mapping and forwarding, and proxying. You can use it as a port scanner if you're really in a bind. By piping **the "yes" keyword** into netcat; two hosts will continue sending data until one or the other terminates the session.

Neverquest Trojan targets banking websites. It's designed to steal credentials and sensitive information and to set up VNC remote access to target systems

netstat –an will show you all the connections and listening ports in numerical form

netstat -b displays all active connections and the processes or applications that are using them

Registry Tools - SysAnalyzer, Tiny Watcher, Active Registry Monitor, and Regshot. Additionally, many antivirus and malware scanners will watch out for registry errors.

Tripwire is a well-respected System Integrity Verifier that can act as an HIDS in protection against Trojans.

SIGVERIF is built into Windows machines to help verify the integrity of critical files on the system. The log is, by default, overwritten each time the tool is run. Third-party drivers that are not signed are displayed as "Not Signed" and indicate a good spot to begin your search.

Virus is a self-replicating program that reproduces its code by attaching copies into other executable codes

Ransomware This malware locks you out of your own system resources and demands an online payment of some sort. examples such as Cryptorbit, CryptoLocker, CryptoDefense, and police-themed.

Boot sector virus Also known as a ***system virus,*** this virus type actually moves the boot sector to another location on the hard drive, forcing the virus code to be executed first. These viruses are almost impossible to get rid of once you get infected. You *can* re-create the boot record—old-school fdisk or mbr could do the trick.

Shell virus Working just like the boot sector virus, this virus type wraps itself around an application's code, inserting its own code before the application's. Every time the application is run, the virus code is run first.

Cluster virus This virus type modifies directory table entries so that user or system processes are pointed to the virus code itself instead of the application or action intended. A single copy of the virus "infects" everything by launching when any application is initiated.

Multipartite virus Attempts to infect both files and the boot sector at the same time. This generally refers to a virus with multiple infection vectors.

Macro virus Probably one of the most common malware types you'll see in today's world, this is usually written with Visual Basic for Applications (VBA). This virus type infects template files created by Microsoft Office, normally Word and Excel. The Melissa virus was a prime example of this.

Polymorphic code virus This virus mutates its code using a built-in polymorphic engine. This type of virus is difficult to find and remove because its signature constantly changes. No part of the virus stays the same from infection to infection.

Polymorphic shellcode hides shellcode by encoding commonly used strings with a simple technique like XOR, so the payload bypasses signature-based IDSes. This technique is polymorphic, because the payload also includes a stub that decodes and executes the hidden shellcode differently each time. Polymorphic shellcode is often used to hide NOP sleds/slides used by buffer overflow attacks.

Encryption virus uses encryption to hide the code from antivirus scanners.

Metamorphic virus rewrites itself every time it infects a new file.

Stealth virus Also known as a "tunneling virus," this one attempts to evade antivirus (AV) applications by intercepting the AV's requests to the operating system (OS) and returning them to itself instead of the OS. The virus then alters the requests and sends them back to AV as uninfected, making the virus now appear "clean."

Cavity virus overwrite portions of host files so as not to increase the actual size of the file. This is done using the null content sections of the file and leaves the file's actual functionality intact.

Sparse infector virus infects occasionally when certain conditions are met. For example, maybe the virus only fires every tenth time a specific application is run.

File extension virus change the file extensions of files to take advantage of most people having file extension view turned off. For example, readme.txt.vbs might appear as readme.txt with extensions turned off.

Create Viruses - Sonic Bat, PoisonVirus Maker, Sam's Virus Generator, and JPS Virus Maker

Worm self-replicating malware that uses a network to send copies of itself to other systems

Code Red exploited indexing software on IIS servers in 2001. The worm used a buffer overflow and defaced hundreds of thousands of servers.

Darlloz Known as the worm for "the Internet of Things," darlloz is a Linux- based worm that targets running ARM, MIPS, and PowerPC architectures— which are usually routers, set-top boxes, and security cameras.

Slammer Also known as SQL Slammer, this was a denial-of-service worm attacking buffer overflow weaknesses in Microsoft SQL services. Also called Sapphire, SQL_HEL, and Helkern, it spread quickly using UDP, and its small size (the entire worm could fit inside a single packet) allowed it to bypass many sensors.

Nimda Nimda was a file infection virus that modified and touched nearly all web content on a machine. It spread so quickly it became the most widespread worm in history. Nimda spread through e-mail, open network shares, and websites, and it also took advantage of backdoors left by the Code Red worm.

Bug Bear Propagating over open network shares and e-mail, Bug Bear terminated AV applications and set up a backdoor for later use. It also contained keylogging capabilities.

Pretty Park Pretty Park spread via e-mail and took advantage of IRC to propagate stolen passwords and the like. Running the worm often displayed the 3D Pipe screensaver on Windows machines.

Tools that can help you with malware analysis IDA Pro, VirusTotal, Anubis, and Threat Analyzer

Sheepdip system is set up to check physical media, device drivers, and other files for malware before it is introduced to the network. Typically, this computer is used for nothing else and is isolated from the other computers, meaning it is not connected to the network at all and are usually configured with a couple of different AV programs, port monitors, registry monitors, and file integrity verifiers.

DoS is generally thought of as a last-resort attack.

Preferred communications channel used to **signal the bots is IRC or Internet Chat Query (ICQ).**

EXAM TIP "botnet" -- ***distributed reflection denial-of-service*** **(DRDoS)** attack, also known as a ***spoof attack***.

Fragmentation attacks take advantage of the system's lack of ability to reconstruct fragmented packets.

Volumetric attacks known as bandwidth attacks, these consume all available bw for the system or service.

Application attacks consume the resources for the app to run, effectively making it unavailable to others.

TCP state-exhaustion attacks These attacks go after load balancers, firewalls, and application servers by attempting to consume their connection state tables.

SYN attack thousands upon thousands of SYN packets to the machine with a *false source IP address*. The machine will attempt to respond with a SYN/ACK but will be unsuccessful. Eventually, all the machine's resources are engaged, and it becomes a giant paperweight.

SYN flood thousands of SYN packets to the target but never responds to any of the return SYN/ACK packets. There is a certain amount of time the target must wait to receive an answer to the SYN/ ACK, it will eventually bog down and run out of available connections.

ICMP flood Here, the attacker sends ICMP Echo packets to the target with a spoofed (fake) source address. The target continues to respond to an address that doesn't exist and reaches a limit of pps sent.

Application level hacker sends more "legitimate" traffic to a web application than it can handle, causing the system to crash. Usually these attacks are designed to exploit weak programming code.

Smurf large number of **pings to the broadcast address** of the subnet, with the source IP spoofed to that of the target. The entire subnet will then begin sending ping responses to the target, exhausting the resources there. A ***fraggle*** attack is similar but uses **UDP** for the same purpose.

Ping of death an attacker fragments an ICMP message to send to a target. When the fragments are reassembled, the resultant ICMP packet is larger than the maximum size and crashes the system.

Teardrop large number of garbled **IP fragments** with **overlapping, oversized payloads** are sent to the target

Peer to peer clients of a P2P file sharing hub are disconnected and directed to connect with the target system.

Permanent *Phlashing* a DoS attack that causes damage to the hw and can also be known as *bricking* a system.

LAND attack sends a SYN packet to the target with the source IP spoofed to the same as the target IP. If vulnerable, the target will loop endlessly and crash the OS

DDoS Tools

LOIC- Low Orbit Ion Cannon, simple to use and floods target with TCP, UDP, or HTTP requests

Trinity is a Linux-based DDoS tool much like LOIC.

Tribe Flood Network uses voluntary botnet systems to launch massive flood attacks on targets

R-U-Dead-Yet (known by its acronym RUDY) performs DoS with HTTP POST via long-form field submissions.

Slowloris TCP DoS tool that ties up open sockets and causes services to hang. It's useful against web servers and doesn't consume large amounts of bandwidth

Hijacking refers to the active attempt to steal the entire session from the client: the server isn't even aware of what happened, and the client simply connects again in a different session

Session Hijacking Steps

1. Sniff the traffic between the client and the server.

2. Monitor the traffic and predict the sequence numbering.

3. Desynchronize the session with the client.

4. Predict the session token and take over the session.

5. Inject packets to the target server.

Defending Session Hijacks

1. Use unpredictable session IDs
2. Limit incoming connections and remote access
3. Regenerate session key after authentication
4. Use encryption like IPSec

EXAM TIP You'll need to know, given an acknowledgment number and a window size, what sequence number would be acceptable to the system. For example, an acknowledgment of 105 with a window size of 200 means you could expect sequence numbering from 105 through 305.

- During a TCP data exchange, the client has offered a sequence number of 100, and the server has offered 500. During acknowledgments, the packet shows 101 and 501, respectively, as the agreed-upon sequence numbers. With a window size of 5, which sequence numbers would the server willingly accept as part of this session? **102 through 106**
- **The sequence number used in the reply packet will be the acknowledgment number in the captured packet, which is 87698415 (Ack no. 87698415). After the three-way handshake has competed in the**

exchange process, the devices start transmitting data from one to another. The sequence number in the response packet will be the acknowledgment number in the received packet.

```
Seq no. 26556942
(next seq no. 26557263)
Ack no. 87698415
Window 8700
LEN = 1656 bytes 0f data
```

Ettercap- packet sniffer on steroids. It's an excellent man-in-the-middle tool and can be run from a variety of platforms. **Hunt** and **T-sight** are probably the two best-known session hijacking tools. **Hunt** can **sniff, hijack, and reset connections** at will, **T-sight** can easily **hijack sessions as well as monitor additional network connections**. Other tools **Zaproxy** and **Paros**, **Burp Suite, Juggernaut**, **Hamster, and Ferret**.

IPSec used to secure IP communication by providing encryption and authentication services to each packet. IPSec works in two modes. In ***transport mode,*** the **payload and ESP trailer are encrypted**; however, the IP header of the original packet is not. Transport can be in NAT. ***Tunnel mode*** encrypts the whole thing, encapsulating the entire original packet in a new IPSec shell. This makes it incompatible with NAT

Authentication Header protocol that guarantees the integrity and authentication of the IP packet sender.

Encapsulating Security Payload ESP is a protocol that provides **origin authenticity and integrity**, but it can take care of confidentiality (through encryption) too. ESP **does not** provide integrity and authentication for the entire IP packet **in transport mode**, but in tunnel mode protection is provided to the entire IP packet.

Internet Key Exchange produces the keys for the encryption process. **IKE-Scan** is a tool **used to scan, fingerprint, and test IPSec VPN.**

Oakley A protocol that uses Diffie-Hellman to create master and session keys.

ISAKMP Sw that facilitates encrypted communication between two endpoints

CHAPTER 10

Cryptography 101

Cryptography- securing communication between two or more parties

Cryptanalysis - the study and methods used to crack encrypted communications.

Encryption algorithms—mathematical formulas used to encrypt and decrypt data; also called ciphers

Stream Ciphers –bits of data encrypted as a continuous stream. These are very fast and use an XOR operation. 0 XOR 0 = 0, 0 XOR 1 =1, 1 XOR 1 = 0. **Same values=0 Different values = 1**

Block Ciphers- bits are split up into blocks (64 bits at a time) and then encrypted with the key and algorithm. These are **simpler and slower than stream ciphers**. These algorithms use substitution and transposition.

Both **symmetric and asymmetric cryptography** are **affected by brute-force** attacks.

- **Symmetric Encryption** single key or shared key, symmetric encryption simply means one key is used both to encrypt and to decrypt the data. Total key pairs needed, N(N-1)/2. This is a great choice for bulk encryption because of speed, but key distribution is an issue because the delivery of the key for the secured channel must be done offline. Additionally, scalability is a concern because the larger the network gets, the number of keys that must be generated increases greatly. Provides confidentiality, but not nonrepudiation.

Symmetric Algorithms

DES A block cipher that uses a 56-bit key (with 8 bits reserved for parity, so 64) and 64-bit block size. Because of the small key size, it became quickly outdated and is not considered a very secure encryption algorithm.

3DES A block cipher that uses a 168-bit key. 3DES (called *triple* DES) can use up to three keys in a multiple-encryption method. It's more effective than DES but much slower. 56, 112, or 168-bit key w/64-bit block size

AES (Advanced Encryption Standard) A block cipher that uses a key length of 128, 192, or 256 bits, and effectively replaces DES. It's much faster than DES or 3DES. Block size is 128, 192, or 256 as well.

IDEA (International Data Encryption Algorithm) block cipher that uses a 128-bit key and was designed to replace DES. Used in Pretty Good Privacy (PGP) 2.0, IDEA was used mainly in Europe. 64-bit blocks

Twofish A block cipher that uses a key size 128, 192, or 256 bits. 128-bit block size

Blowfish A fast block cipher, largely replaced by AES, using a 64-bit block size and a key from 32 to 448 bits. Blowfish is considered public domain.

RC4 is a stream cipher, not a block cipher **and used in WEP;** so WEP uses symmetric encryption. **SysKey** also uses RC4. 40-2,048 bit keys

RC (Rivest Cipher) A block cipher that uses a variable key length up to 2048 bits. RC6, the latest version, uses 128-bit blocks and 4-bit working registers, whereas RC5 uses variable block sizes (32, 64, or 128) and 2-bit working registers.

- **Asymmetric Encryption** In this key-pair system, both are generated together, with one key used to encrypt a message and the other to decrypt it. The **encryption key, also known as the *public key*,** could be sent anywhere, to anyone. The decryption key, known as the *private key,* is kept secured on the system. Weakness includes speed/performance and requires more processing power. **Protects data and provides nonrepudiation**

EXAM TIP Asymmetric encryption comes down to this: what one key encrypts, the other key decrypts. Either can be used for encryption or decryption within the pair, but in general remember
public = encrypt, private = decrypt.

Asymmetric Algorithms

Diffie-Hellman Developed for use as a key exchange protocol, Diffie-Hellman is used in Secure Sockets Layer (SSL) and IPSec encryption. It can be vulnerable to man-in-the-middle attacks, however, if the use of digital signatures is waived. Whitfield Diffie and Martin Hellman effectively invented public key encryption. The algorithm **DOES NOT** provide compression, restorability, or encryption.

Elliptic Curve Cryptosystem (ECC) This uses points on an elliptical curve, in conjunction with logarithmic problems, for encryption and signatures. Less processing power than other methods, good for mobile devices.

El Gamal this method uses the solving of discrete logarithm problems for encryption and digital signatures.

RSA key sizes up to 4096 bits. modern de facto standard for **encryption** and **digital signatures**. It is a form of two-factor authentication and uses passwords only once. Current recommended **key length for PKI is 2048 bits**

- **Hash Algorithms -** a *one-way* mathematical function that takes an input and typically produces a fixed-length string (usually a number), or hash, based on the arrangement of the data bits in the input. Its sole purpose in life is to provide a means to **verify the integrity** of a piece of data There isn't a way for a hash to be reverse- engineered.

MD5 (Message Digest algorithm) This produces a 128-bit hash value output, expressed as a 32-digit hexadecimal. MD5 was originally popular for ensuring file integrity. Despite its past, MD5 is still used for file verification on downloads and, in many cases, to store passwords.

SHA-1 Developed by the NSA, SHA-1 produces a 512-bit block size with a 160-bit value output and was required by law for use in U.S. government applications. In late 2005, however, serious flaws became apparent and the U.S. government began recommending the replacement of SHA-1 with SHA-2

SHA-2 This hash algorithm actually holds four separate hash functions that produce outputs of 224, 256, 384, and 512 bits. Although it was designed as a replacement for SHA-1, SHA-2 is still not as widely used.

SHA-3 This hash algorithm uses something called "sponge construction," where data is "absorbed" into the sponge (by XOR-ing the initial bits of the state) and then "squeezed" out (output blocks are read and alternated with state transformations).

Encrypted File System (EFS) Windows native encryption for files and folders. For drives, use BitLocker.

Collision Attack – mathematical attack used against hashing algorithms; there are only so many combinations

Salt is a collection of random bits that are used as a key in addition to the hashing algorithm

EXAM TIP even though hashes are one-way functions, a collision attack may break older versions (MD5).

EXAM TIP How can you tell if a file is a stego-file? For text, character positions are key (look for text patterns, unusual blank spaces, and language anomalies). Image files will be larger in size, and may show some weird color palette "faults." Audio and video files require some statistical analysis and specific tools.

Image steganography three main techniques, **least significant bit insertion, masking and filtering**, which is usually accomplished on grayscale images and **algorithmic transformation** hides data in the mathematical functions used in image compression.

GAK - government access to keys. Also referred to as *key escrow,* Companies provide their encryption keys to the government, and they promises to play nicely with them and use them only when it *really* needs to.

PKI a structure designed to verify and authenticate the identity of individuals within the enterprise taking part in a data exchange. It consists of hardware, software, and policies that create, manage, store, distribute, and revoke keys and digital certificates. Simply, **it provides public-key encryption and digital signatures**.

Hybrid PKI - both symmetric and asymmetric algorithms are used. The asymmetric algorithm is used to encrypt the keys that will be exchanged and symmetric encryption is used on the data being exchanged. The sole purpose of the symmetric algorithm is to encrypt the data.

Certificate Authority (CA) acts as a third party to the organization and its job is to create and issue digital certificates that can be used to verify identity. The CA also keeps track of all the certificates within the system (using a certificate management system) and maintains a *certificate revocation list (CRL)*, used to track which certificates have problems and which have been revoked.

Validation Authority (VA) is used to validate certificates via Online Certificate Status Protocol (OCSP).

Registration Authority (RA) responsible for receiving subject's request, verifying its identity, and issuing the request to the CA. Subordinate CAs handle things internally (as a matter of fact, most root CAs are removed from network access to protect the integrity of the system)

EXAM TIP A certificate authority can be set up to trust a CA in a completely different PKI through something called *cross-certification.* This allows both PKI CAs to validate certificates generated from either side.

Web of Trust multiple entities sign certificates for one another. Users trust each other based on certificates they receive from other users on the same system.

Single-Authority System has a CA at the top that creates and issues certificates. Users trust each other based on the CA.

Hierarchical trust system (most secure) also has a root CA at the top but makes use of one or more registration authorities (subordinate CAs) underneath it to issue and manage certificates

EXAM TIP Remember the **public key is sent with the certificate.** If you have a web server in **cloud provider** network, you would be required to provide a **Private Key** and **Digital Signature** for users.

Contents of a Digital Certificate:

Version This identifies the certificate format. The most common version in use is 1.

Serial Number Fairly self-explanatory, the serial number is used to uniquely identify the certificate.

Subject This is whoever or whatever is being identified by the certificate.

Algorithm ID (or Signature Algorithm) This shows the algorithm that was used to create the digital signature.

Issuer This shows the entity that creates and verifies the authenticity of the certificate.

Valid From and Valid To These fields show the dates the certificate is good through.

Key Usage This shows for what purpose the certificate was created.

Subject's Public Key copy of the public key is included in the digital certificate, for obvious purposes.

Optional fields These fields include Issuer Unique Identifier, Subject Alternative Name, and Extensions.

Self-Signed Certificate—signed and verified by the same entity

Signed Certificate- CA is involved and the signature validating the identity of the entity is confirmed via an external source—in some instances, a validation authority (VA). Signed certificates can be trusted: assuming the CA chain is validated and not corrupted.

Digital Signature

- Bob creates a text message to send to Joe.

- Bob **generates a hash** of his message
- Bob then **encrypts** the outcome of that hash with his ***private*** **key** and sends the message, along with the **encrypted hash**, to Joe.
- Joe receives the message and attempts to **decrypt** the hash with **Bob's *public* key**. If it works, he knows the message came from Bob because the only thing Bob's public key could ever decrypt is something that was encrypted using his private key in the first place. Since Bob is the only one with that private key—*voilà*!

More Info

- Keys are generated in pairs, and what one does, the other undoes
- In general, the public key is used for encryption, and the private key is used for decryption.
- Although the private key is created to decrypt messages sent to the owner, it is also used to prove authenticity through the digital signature (encrypting with the private key allows recipients to decrypt with the readily available public key).

NOTE FIPS 186-2 specifies that something called the **Digital Signature Algorithm (DSA)** be used in the generation and verification of digital signatures.

Secure Communications

Secure Shell (SSH) tcp/22 basically, a secured version of Telnet. SSH relies on public key cryptography for its encryption. It can be used as a tunneling protocol. SSH2 is the successor to SSH. It's more secure, efficient, and portable, and it includes a built-in encrypted version of FTP (SFTP).

Secure Sockets Layer (SSL) This encrypts data at or above the transport layer and uses RSA asymmetric encryption and digital certificates and can be used with a wide variety of upper-layer protocols. SSL is not an active encryption standard, not protected against CBC attacks, and encrypts the entire communication channel vs. each message. SSL encryption could **cause a security issue** when an **IDS** is in the path since SSL **encrypts the contents of the packets**, the IDS will be unable to examine them for malicious content. When **session keys** are being created, the client will **encrypt the key** with the **server's public key**.

Transport Layer Security (TLS) Using an RSA algorithm of 1024 and 2048 bits, TLS is the successor to SSL. The handshake portion (TLS Handshake Protocol) allows both the client and the server to authenticate to each other, and TLS Record Protocol provides the secured communication channel.

Internet Protocol Security (IPSec) This is a network layer tunneling protocol that is capable of carrying nearly any application. The Authentication Header (AH) protocol verifies an IP packet's integrity and determines the validity of its source: it provides authentication and integrity, but not confidentiality. Encapsulating Security Payload (ESP) encrypts each packet

PGP Pretty Good Privacy is used for signing, compression, and encrypting and decrypting e-mails, files, directories, and **even whole disk partitions**. PGP is known as a hybrid cryptosystem, because it uses features of conventional and public key cryptography. PGP requires **no management of server services** and is one method to defend against sniffing. It uses **asymmetric encryption and digitally signs emails.**

S/MIME (Secure/Multipurpose Internet Mail Extensions) protocol developed by RSA and is a standard for public key encryption and signing of MIME data.

nmap -d –script ssl-heartbleed –script-*args vulns.showall -sV [host]*

to search for the vulnerability: the return will say "State: NOT VULNERABLE" if you're good to go.

Factoring Attack on RSA-EXPORT Keys (FREAK) is a man-in-the- middle attack forces the use of a weaker encryption key length, enabling brute-force attacks.

Heartbleed OpenSSL versions *1.0.1* and *1.0.1f* are vulnerable to Heartbleed. Allows attacker to **pull 64KB of information from a server's memory at regular intervals**

POODLE – mitm interrupts all handshake attempts by TLS clients forcing a degradation to lower, more vulnerable SSL version

Cryptography Attack

Known plain-text attack hacker has both plain-text and corresponding cipher-text messages. The plain-text copies are scanned for repeatable sequences, which are then compared to the cipher-text versions.

Chosen plain-text attack attacker encrypts multiple plain-text copies himself in order to gain the key.

Adaptive chosen plain-text attack"the attacker makes a series of interactive queries, choosing subsequent plaintexts based on the information from the previous encryptions." What this really means is the attacker sends bunches of cipher texts to be decrypted and then uses the results of the decryptions to select different, closely related cipher texts.

Cipher-text-only attack hacker gains copies of several messages encrypted with same algorithm. Statistical analysis can then be used to reveal repeating code, which can be used to decode messages later.

Replay attack This is most often performed within the context of a man-in- the-middle attack. The hacker repeats a portion of a cryptographic exchange in hopes of fooling the system into setting up a communications channel. Session tokens can be used in the communications process to combat this attack.

Chosen cipher attack attacker chooses a particular cipher-text message and attempts to discern the key through comparative analysis with multiple keys and a plain-text version. RSA is particularly vulnerable to this attack.

EXAM TIP A side-channel attack isn't like the other traditional attacks mentioned. It is a physical attack that monitors environmental factors (like power consumption, timing, and delay) on the cryptosystem itself.

CHAPTER 11

Social Engineering

Most common form is impersonation. Others are shoulder-surfing and eavesdropping.

EXAM TIP Using a phone during a social engineering effort is known as "vishing" (short for *voice phishing*).

EXAM TIP If you see an exam question listing both tailgating and piggybacking, the difference between the two comes down to the presence of a fake ID badge (tailgaters have them, piggybackers don't).

Mitigation user education, anti-malware, and e-mail gateways.

Reverse Social Engineering

- Advertise your position as some sort of technical support
- Perform some sort of sabotage like pulling cables or a DoS attack
- Support the user you have setup by asking for credentials so you can help out

Mobile-based Social Engineering

- **Publishing malicious apps** app that looks like, acts like, and is namely similarly to a legitimate application.
- **Repackaging legitimate apps** attacker takes a legitimate app from an app store and modifies it to contain malware, posting it on a third-party app store for download.
- **Fake security applications** starts with a victimized PC: the attacker infects a PC with malware and then uploads a malicious app to an app store. Once the user logs in, a malware pop-up advises them to download bank security software to their phone. The user complies, thus infecting their mobile device.
- **SMS** attacker sends SMS text messages crafted to appear as legitimate security notifications, with a phone number provided. The user calls the number and provides sensitive data. **This is known as "SMiShing."**

Objective-C when used need to look out for **code injection, buffer overflow, string formatting, and thread racing vulnerabilities**

Physical Security

- *Physical* things you can touch, taste, smell, or get shocked by. **Bollards, locks, fences, guards**
- *Technical/Logical* authentication and permissions, think about them within the context of **smartcards, security tokens and biometrics**
- *Operational* policies and procedures you set up such as **background checks on employees, risk assessments on devices, and policies regarding key management and storage**

Biometrics

False rejection rate (FRR) is the percentage of time a biometric reader will deny access to a legitimate user.
False acceptance rate (FAR) the percentage of time that an *unauthorized* user is granted access by the system
Crossover error rate (CER) on a graph where FRR intercepts FAR becomes a ranking method to determine how well the system functions overall

CHAPTER 12

Pen Test

* You should verify that **negligence and liability** are covered in the legal language **before signing** the confidentiality agreement and NDA. Any potential disclosure by the testing provider's intent or negligence should hold the testing provider liable. You should also ensure they have insurance to cover any potential damages. The confidentiality agreement and NDA must be signed before penetration testing begins.

The **ROE (rules of engagement)** documentation provides an ethical hacker the scope of targets and allowed testing techniques and tools. The ROE is guideline documentation for performing the penetration test, including allowed activities like port scanning, social engineering, and network sniffing, and restricted activities like password cracking and SQL injection attacks. It also includes specific IP address ranges, testing periods, contact information for the team and affected systems and networks, prevention measures for alerting law enforcement, and how collected information will be handled after testing.

Security Assessment test that is performed in order to assess the level of security on a network or system

- Security Audit-policy and procedure focused. Are you following your own policy?
- Vulnerability Assessment-scans and tests systems for existing vulnerabilities, but doesn't exploit them
- Penetration Test-looks for vulnerabilities and actively seeks to exploit them

Attack Phases

- **Pre-attack Phase**- recon, data gathering, footprinting, scanning, NDA signing
- **Attack Phase**- you'll be attempting to penetrate the network perimeter, acquire your targets, execute attacks, and elevate privileges
- **Post-attack Phase**- Anything uploaded to systems in the way of files or folders needs to be removed. Any tools, malware, backdoors, or other attack software loaded on client systems need to be taken off. And don't forget the Registry—any changes made there need to be reset to the original settings. Lastly, findings, the impacts, and the analysis in the report or out-brief need to be delivered

Vulnerability Assessment Phases

- Acquisition
- Identification
- Analyzing
- Evaluation
- Generating Reports

Organizational Roles

Pure insider - an employee with all the rights and access associated with being employed by the company.
Insider affiliate - a spouse, friend, or even client of an employee who uses the employee's credentials to gain access. Even if credentials are stolen, this is considered affiliate of an insider.
Outside affiliate - non-trusted outsiders who use open access to gain access to an organization's resources. A great example of this is an outsider gaining unauthorized access to wireless access points.
Insider associate - someone with limited authorized access. Contractors, guards, and cleaning and plant services all fit under this category.
asynchronous referring to an implant or malware that does not require active interaction from the attacker.