EC-Council
CEH™ Certified Ethical Hacker
Version 10
Quick Review Guide

Matt Walker

New York Chicago San Francisco
Athens London Madrid Mexico City
Milan New Delhi Singapore Sydney Toronto

Welcome to the CEH Certified Ethical Hacker Version 10 (CEHv10) Quick Review Guide! Although no single resource can adequately prepare you for the exam, this is a good resource for a last-minute review just before attempting your exam. I've tried to summarize everything in a quick-and-easy format for you and hope you find this to be a valuable study resource. I certainly recommend you check out the full details in the *CEH Certified Ethical Hacker All-in-One Exam Guide* book I so lovingly put together for exam candidates because you may find that some of the things listed here require further explanation. Best of luck to you on your certification exam and your career as an *ethical* hacker!

Chapter 1 Getting Started: Essential Knowledge

This chapter is about definitions and rote memorization. When studying, try to find some key words in each definition you can associate with the term. Laws and standards questions can and will be maddening. My best advice is to concentrate on key words and remember that the process of elimination can sometimes be more helpful in narrowing the options down to the correct answer than trying to memorize everything in the first place.

Keep in mind that this certification is provided by an international organization. Therefore, you will sometimes see some fairly atrocious grammar on test questions here and there, especially in this section of the exam. Don't worry about it—just keep focused on the main point of the question and look for your key words. And finally, for goodness' sake, please try not to confuse the real world with the exam—trust what you get out of this book and your other study material, and don't read too much into the questions.

The OSI Reference Model

- The OSI Reference Model layers are the Application layer (holds all the protocols that allow a user to access information on and across a network), Presentation layer (designed to put the message into a format all systems can understand), Session layer (no real manipulation of the data itself; its job is to open, maintain, and close a session), Transport layer (reliable end-to-end delivery of the message is ensured, along with segmentation, error correction, and flow control), Network layer (routing of packets across networks), Data Link layer (physical address; encapsulates the packet with a header and a trailer), and Physical layer (encoding of bits to the media used for delivery).
- ASCII stands for American Standard Code for Information Interchange, and it works as a standard for representing text.

TCP/IP Overview

- The TCP/IP protocol stack is arranged in layers: Application layer (holds all the protocols and performs all the activities of the Application, Presentation, and Session layers of the OSI Reference Model), Transport layer (reliable end-to-end

delivery of the message is ensured, along with segmentation, error correction, and flow control), Internet layer (routing of packets across networks), and Network Interface layer (holds all the protocols and performs all the activities of the Data Link and Physical layers).

- In an Ethernet TCP/IP network, Transmission Control Protocol (TCP) works as the connection-oriented transport protocol. UDP is the connectionless version.
- TCP uses a three-step handshake to get things going. This handshake includes a Synchronize (SYN) segment, a Synchronize Acknowledgment (SYN/ACK) segment, and an Acknowledgment (ACK) segment.
- In packets or datagrams crossing a network, source and destination MAC addresses will change, but IP addresses never do.

Security Essentials

- Increasing security reduces functionality and usability.
- *Security controls* are the countermeasures security personnel put into place to minimize risk as much as possible. The three main control types are preventative, detective, and corrective. A *preventative* control is exactly what it sounds like: a security measure put into place to prevent errors or incidents from occurring in the first place. A *detective* control is one put into place to identify an incident has occurred or is in progress. A *corrective* control is designed for after the event to limit the extent of damage and aid swift recovery.
- Security controls can also be categorized as physical, technical, and administrative. Physical controls are exactly what they sound like and include things such as guards, lights, and cameras. Technical controls include things such as encryption, smartcards, and access control lists. Administrative controls include the training, awareness, and policy efforts that are well intentioned, comprehensive, and well thought out.

Security Policy

- A security policy can be defined as a document describing the security controls implemented in a business to accomplish a goal. The security policy defines exactly what your business believes is the best way to secure its resources.
- An information security policy identifies to employees what company systems may be used for, what they cannot be used for, and what the consequences are for breaking the rules. Generally employees are required to sign a copy before accessing resources. A version of this policy is also known as an acceptable use policy.
- An information protection policy defines information sensitivity levels and who has access to those levels. It also addresses how data is stored, transmitted, and destroyed.

- A password policy defines everything imaginable about passwords within the organization, including length, complexity, maximum and minimum ages, and reuse.
- An e-mail policy, sometimes also called the e-mail security policy, addresses proper use of the company e-mail system.
- An information audit policy 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.
- Policy can be promiscuous, permissive, prudent, or paranoid. A *promiscuous* policy is basically wide open, whereas a *permissive* policy blocks only things that are known to be suspicious or dangerous. The next step up is a *prudent* policy, which provides maximum security but allows some potentially and known dangerous services because of business needs. Finally, a *paranoid* policy locks everything down, not even allowing the user to open so much as an Internet browser.
- *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.

Introduction to Ethical Hacking

- *Confidentiality,* addressing the secrecy and privacy of information, refers to the measures taken to prevent the disclosure of information or data to unauthorized individuals or systems. The use of passwords within some form of authentication is by far the most common logical measure taken to ensure confidentiality.
- *Integrity* refers to the methods and actions taken to protect the information from unauthorized alteration or revision—whether the data is at rest or in transit. Integrity in information systems is often ensured through the use of a hash.
- *Availability* refers to the communications systems and data being ready for use when legitimate users need them. Attacks against availability all fall into the "denial of service" realm.
- The Security, Functionality, and Ease of Use triangle is simply a graphic representation of a catch-22 in computing—the more secure something is, the less usable and functional it becomes.

Defining the Ethical Hacker

- An *ethical hacker* is someone who employs the same tools and techniques a criminal might use, with the customer's full support and approval, in order to help secure a network or system. They do not proceed without a signed agreement with the customer.

- *White hats* are ethical hackers, hired by a customer for the specific goal of testing and improving security or for other defensive purposes.
- *Gray hats* are neither good nor bad; they are usually attackers who are curious about hacking tools and techniques or attackers who feel like it's their duty, with or without customer permission, to demonstrate security flaws in systems.
- *Black hats* are "crackers," illegally using their skills either for personal gain or for malicious intent. Black hats do *not* ask for permission or consent.
- *Hacktivists* use their knowledge and actions as hackers to promote a political agenda or other cause. These attackers are almost always "black hat" in nature.
- A *penetration test,* also known as a *pen 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. Pen tests have three phases: preparation, assessment, and conclusion.
- The five phases of an ethical attack are reconnaissance, scanning and enumeration, gaining access, maintaining access, and covering tracks.
- Passive reconnaissance does not touch any of the target's internal resources or put the attacker at great risk of discovery. Examples usually include crawling the public portions of the target's websites, browsing job boards, examining DNS records that are accessible from the outside, and dumpster diving.

Hacking Terminology

- In *black-box testing,* the ethical hacker has absolutely no knowledge of the target of evaluation (TOE). It's designed to simulate an outside, unknown attacker.
- In *white-box testing*, pen testers have full knowledge of the network, system, and infrastructure they are testing. It is designed to simulate a knowledgeable internal threat, such as a disgruntled network admin or other trusted user.
- In *gray-box testing*, the attacker has limited knowledge about the TOE. It is designed to simulate privilege escalation from a trusted employee.
- Attack types include operating system (OS) attacks, application-level attacks, shrink-wrap attacks, and misconfiguration attacks. OS and application-level attacks are self-explanatory. Shrink-wrap attacks exploit built-in code and scripts within the application itself. Misconfiguration attacks take advantage of systems that are, on purpose or by accident, not configured appropriately for security.
- An *inside attack* generates from inside the network boundary, whereas an *outside attack* comes from outside the network border (usually from a network across the Internet).
- An *asset* is an item of economic value owned by an organization or individual. A *threat* is any agent, circumstance, or situation that could potentiality cause harm or loss to an IT asset. A *vulnerability* is any weakness, such as a software flaw or logic design, that could be exploited by a threat to cause damage to an asset.

Network Security Zones

- **Internet** Outside the boundary and uncontrolled. You don't apply security policies to the Internet. Governments try to all the time, but your organization can't.
- **Internet DMZ** The acronym DMZ (for Demilitarized Zone) comes from the military and refers to a section of land between two adversarial parties where there are no weapons and fighting. The idea is you can see an adversary coming across the DMZ and have time to work up a defense. In networking, the idea is the same: it's 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.

Security Terminology

- Threat Modeling includes five sections: Identify Security Objectives, Application Overview, Decompose Application, Identify Threats, and Identify Vulnerabilities.
- Incident Response Teams identify, analyze, prioritize, and resolve security incidents. The incident management process includes a review of incident detection, and analysis of the exploitation, in order to notify appropriate stakeholders, and efforts to contain the exploitation, eradicate residual backdoors and such, and coordinate recovery for any lost data or services.
- A business impact analysis (BIA) is an effort to identify the systems and processes that critical for operations. A business continuity plan (BCP) is a set of plans and procedures to follow in the event of a failure or a disaster—security related or not—to get business services back up and running, and includes a disaster recovery plan (DRP).
- In determining system value, the annualized loss expectancy (ALE) is the product of the ARO (annual rate of occurrence) and the SLE (single loss expectancy). Additionally the exposure factor (EF) is the percentage of loss for an asset if a specific threat was actually realized.

Hacking Phases and the Pen Test

- The hacking phases include *reconnaissance, scanning and enumeration, gaining access, maintaining access,* and *covering tracks.*
- There are three main phases to a pen test—*preparation, assessment,* and *conclusion*—and they are fairly easy to define and understand. The *preparation* phase defines the time period during which the actual contract is agreed upon: the scope of the test, the types of attacks allowed, and the individuals assigned to perform the activity are all agreed upon in this phase. The *assessment* phase (sometimes also known as the *security evaluation* phase or the *conduct* phase) is when the actual assaults on the security controls are conducted. The *conclusion* (or post-assessment) phase defines the time when final reports are prepared for the customer, detailing the findings of the tests (including the types of tests performed), and many times even providing recommendations to improve security.

Laws and Standards

- The Trusted Computer System Evaluation Criteria (TCSEC) was a United States Government Department of Defense (DoD) standard, with a goal to set basic requirements for testing the effectiveness of computer security controls built into a computer system.
- TCSEC gave way to *Common Criteria for Information Technology Security Evaluation* (also known as Common Criteria, or CC). It provided a way for vendors to make claims about their in-place security by following a set standard of controls and testing methods, resulting in something called an *Evaluation Assurance Level (EAL)*. CC includes the target of evaluation (TOE) (what is being tested), the security target (ST) (the documentation describing the TOE and security requirements), and the protection profile (PP) (a set of security requirements specifically for the type of product being tested).
- The list of laws and standards available for test questioning is nearly endless. A few that may be looked at include FISMA, the Electronics Communications Privacy Act, PATRIOT Act, Privacy Act of 1974, Cyber Intelligence Sharing and Protection Act (CISPA), Consumer Data Security and Notification Act, and the Computer Security Act of 1987.
- Health Insurance Portability and Accountability Act (HIPAA), developed by the U.S. Department of Health and Human Services to address privacy standards with regard to medical information. The law sets privacy standards to protect patient medical records and health information, which, by design, is provided to and shared with doctors, hospitals, and insurance providers. HIPAA has five

subsections that are fairly self-explanatory (Electronic Transaction and Code Sets, Privacy Rule, Security Rule, National Identifier Requirements, and Enforcement).

- Sarbanes-Oxley (SOX) Act was created to make corporate disclosures more accurate and reliable in order to protect the public and investors from shady behavior. There are 11 titles within SOX that handle everything from what financials should be reported and what should go in them, to protecting against auditor conflicts of interest and enforcement for accountability.
- The Open Source Security Testing Methodology (OSSTM) Manual is a peer-reviewed formalized methodology of security testing and analysis that can "provide actionable information to measurably improve your operational security." It defines three types of compliance for testing: *legislative* (government regulations), *contractual* (industry or group requirements), and *standards based* (practices that must be followed in order to remain a member of a group or organization).
- Payment Card Industry Data Security Standard (PCI-DSS) is a security standard for organizations handling credit cards, ATM, and other point-of-sales cards. The standards apply to all groups and organizations involved in the entirety of the payment process—from card issuers, to merchants, to those storing and transmitting card information—and consist of 12 requirements.
- Control Objects for Information and Related Technology (COBIT) is a security standard created by the Information Systems Audit and Control Association (ISACA) and the IT Governance Institute (ITGI). COBIT is an IT governance framework and supporting toolset that allows managers to bridge the gap between control requirements, technical issues, and business risks. COBIT enables clear policy development, good practice, and emphasizes regulatory compliance. It does so in part by categorizing control objectives into four domains (Planning and Organization, Acquisition and Implementation, Delivery and Support, and Monitoring and Evaluation).
- ISO/IEC 27001:2013 provides requirements for creating, maintaining, and improving organizational IS (Information Security) systems. The standard addresses issues such as ensuring compliance with laws as well as formulating internal security requirements and objectives.

Chapter 2 Reconnaissance: Information Gathering for the Ethical Hacker

If you want to be a successful ethical hacker, you'll need to know how to gather information about your targets *before* you ever even try to attack them.

Vulnerability Research

- A *zero-day* threat is an attack or exploit on a vulnerability that the vendor, developer, system owner, and security community didn't even know existed.

- The U.S. Computer Security Incident Response Team (CSIRT; www.csirt.org) provides an incident response service to enable a reliable and trusted single point of contact for reporting computer security incidents worldwide and provides incident response services to any user, company, government agency, or organization in partnership with the Department of Homeland Security.

Footprinting

- An *active footprinting* effort is one that requires the attacker to touch the device or network or places the attacker at great risk of being discovered. Running scans against network segments is a prime example of active footprinting.
- A *passive footprinting* effort takes advantage of readily available information and does not put the attacker at risk of discovery. Examples within the exam include perusing company websites, searching job boards, and dumpster diving.
- *Competitive intelligence* refers to the information gathered by a business entity about their competitor's customers, products, and marketing. This information is readily available, is perfectly legal to obtain, and can be acquired through a host of different means. Competitive intelligence gathering is considered passive.
- *Anonymous footprinting* refers to footprinting efforts that can't be traced back to you. *Pseudonymous footprinting* refers to having any trace of efforts lead to a different person.
- The Computer Fraud and Abuse Act (1986) makes conspiracy to commit hacking a crime. Therefore, it's important the ethical hacker get an ironclad agreement in place *before even attempting* basic footprinting.
- The Wayback Machine (www.archive.org) keeps snapshots of sites from the past, allowing you to go back in time to search for lost information (for example, if the company erroneously had a phone list available for a long while but has since taken it down, you may be able to retrieve it from a "wayback" copy).

DNS Footprinting and Network Range

- DNS uses port 53 on both TCP and UDP. Name lookups generally use UDP, whereas zone transfers use TCP.
- Record types within a DNS namespace include SRV, SOA, PTR, NS, A, MX, and CNAME. SRV provides a listing for specific services. SOA is the Start of Authority record for the primary name server and provides basic properties of the entire domain. PTR is a pointer record, mapping an IP to a name (for reverse lookups). NS is for name server, and it lists the name servers within the namespace. Type A records provide name-to-IP-address mappings for lookups within a domain. MX is for mail exchanger, and it lists e-mail servers within the domain. CNAME (canonical name) provides for domain name aliases within the zone.

- The weirdest record type you'll be asked about is the HINFO type. The HINFO record type is old and outdated, but it allowed administrators the option of entering host information, specifically the CPU type and operating system, when creating the record.
- The process of replicating all DNS records between servers is known as a *zone transfer.*
- The SOA record includes the source host, contact e-mail, serial number (increments each time the zone file changes), refresh time (amount of time a secondary DNS server will wait before asking for updates), retry time (amount of time a secondary server will wait to retry if the zone transfer fails), expire time (maximum amount of time a secondary server will spend trying to complete a zone transfer), and TTL (minimum time to live for all records in the zone if not updated by a zone transfer).
- There are five regional registries for registering a public IP address space: the American Registry for Internet Numbers (ARIN) for North and South America and sub-Saharan Africa; the Asia Pacific Network Information Centre (APNIC) for Asia and the Pacific; Réseaux IP Européens (RIPE NCC) for Europe, Middle East, and parts of Central Asia/Northern Africa; the Latin America and Caribbean Network Information Centre (LACNIC) for Latin America and the Caribbean; and the African Network Information Center (AfriNIC) for Africa.
- *Whois* queries registries and returns information on domain ownership, addresses, locations, and phone numbers.
- *Nslookup* is a command that provides a means to query DNS servers for information. The syntax for the tool is

  `nslookup [-options] {hostname | [-server]}`

  The command can run as a single instance, providing information based on the options you choose, or you can run it in interactive mode, where the command runs as a tool, awaiting input. Zone transfers can be accomplished within the nslookup tool in interactive mode with this syntax:

  `ls -d domainname.com`

  where *domainname.com* is the name of the zone.
- *Traceroute* is a command-line tool that tracks a packet across the Internet and provides route path and transit times. The syntax on Windows systems is

  `tracert hostname`

  It accomplishes this by incrementing the ICMP TTL by 1 after each "hop" and using the resulting ECHO packets to report information on each hop (router) from the source to destination.
- There can be significant differences in traceroute from a Windows machine to a Linux box. Windows uses the command tracert, whereas Linux uses traceroute. Also keep in mind Windows is ICMP only, whereas Linux can use other options (UDP and TCP).

- DNS poisoning occurs when an attacker changes the cache on a name server to answer requests with bogus addresses.
- The Domain Name System Security Extensions (DNSSEC) is a suite of IETF specifications for securing certain kinds of information provided by DNS.

Google Hacking

- *Google hacking* refers to manipulating a search string with additional specific operators to search for vulnerabilities. The basic syntax is

  ```
  operator: "string"
  ```

- The Google operator intitle:*string* searches for web pages that contain *string* in the title.
- The Google operator inurl:*string* displays pages with *string* in the URL.
- The Google operator site:*domain or web page string* displays pages for a specific website or domain holding the search term.
- The Google operator index of:*string* displays pages with directory browsing enabled and is usually used with another operator.

Other Tips and Tools

- Web spiders are applications that crawl through a website, reporting information on what they find.
- The robots.txt file defines which pages are available for crawling by search engines and which are not.
- Tools such as Black Widow can be used to pull full copies of a website to a local machine for later examination.
- Archive.org (also known as the Wayback Machine) provides access to archived copies of websites, in the event you're looking for information that may have been recently removed from the site in question.
- Maltego (https://www.paterva.com/web7/) is an open source intelligence and forensics application designed explicitly to demonstrate social engineering (and other) weaknesses for your environment.
- Social Engineering Framework (SEF) (http://spl0it.org/projects/sef.html) has some 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.
- Shodan (https://www.shodan.io) is a search engine designed to help you find specific types of computers (routers, servers, and so on) connected to the Internet.

Chapter 3 Scanning and Enumeration

After footprinting, you'll need to scan for basics—the equivalent of knocking on the virtual doors on your target's machines to see who is home and what they look like. Then, when you find a machine up and about, you'll need to get to know it really well, asking some rather personal questions. You'll need to know port numbers, protocols, and communications handshakes as well as routing/switching basics and how they can affect your efforts. You're going to be quizzed on the use, output, and syntax of all scanning tools and methods.

Scanning Fundamentals

- Scanning methodology includes several phases: check for live systems, check for open ports, scan beyond IDS, perform banner grabbing, scan for vulnerabilities, draw network diagrams, and prepare proxies.
- All TCP communications begin with a three-way handshake: SYN, SYN/ACK, and ACK.
- Six flags are available within a TCP header: Synchronize (SYN), Acknowledgment (ACK), Reset (RST), Finish (FIN), Push (PSH), and Urgent (URG). The SYN flag is set during initial communication establishment. It indicates negotiation of parameters and sequence numbers. The ACK flag is set as an acknowledgment to SYN flags. This flag is set on all segments after the initial SYN flag. The RST flag forces a termination of communications in both directions. The FIN flag signifies an ordered close to communications. The PSH flag forces delivery of data without concern for any buffering. When the URG flag is set, it indicates the data inside is being sent out of band.
- A port number, inside the Transport layer protocol header (TCP or UDP), identifies which upper-layer protocol should receive the information contained within. Systems use port numbers to map communications to specific applications.
- Port numbers range from 0 to 65,535 and are split into three groups: well known (0–1023), registered (1024–49151), and dynamic (49152–65535).
- Well-known port numbers must be committed to memory. A few include FTP (21, TCP), SMTP (25, TCP), DNS (53, both TCP and UDP), DHCP (67, UDP), HTTP (80, TCP), and SNMP (161 and 162, UDP).
- Ports can be in several *states.* If an application is running on a computer and is waiting for another system to connect to it, the port number the application is set to use is said to be in a *listening* state. Once a remote system establishes a session over that open port, the port is said to be in an *established* state. In short, a listening port is one that is waiting for a connection, while an established port is one that is connected to a remote computer.

- Netstat is a command-line tool that can be used to view the port status on your system. The command *netstat -an*, for example, will display all connections and listening ports, with addresses and port numbers in numerical form.
- ICMP messages have a type and code. Type 3 messages represent Destination Unreachable, and Code 13 represents Administratively Prohibited (which lets you know a poorly configured firewall is not only preventing the delivery ICMP packets but also notifying you of it).
- ICMP Type 8 is an ECHO request, whereas Type 0 is an ECHO reply. Type 11 is for Time Exceeded.
- Combining pings to each and every address within a subnet range is known as a *ping sweep* (or *ICMP ECHO Sweep*). Ping sweeps are one of the easiest methods available to identify active machines on the network but are easily detected and usually blocked.
- Scan types include a Full Connect (most reliable, but most noisy), Stealth (also known as half-open or SYN), ACK (setting the ACK flag), IDLE (using a spoofed address and an idle zombie system), XMAS (setting all flags), and Inverse TCP (setting the FIN, URG, or PSH flag, or no flags at all; does not work on Windows systems).
- If an ACK is sent and there is no response, this indicates a stateful firewall is between the attacker and the host. If a RST comes back, there is not.
- Subnetting is the process of defining which portions of the IP address belong to the network ID, and which are Host bits. A subnet mask is a binary pattern that is matched against any IP address to determine which bits belong to the network side of the address, with the binary starting from left to right, turning on all the 1's until the mask is done. Three main rules apply in IPv4 subnetting: (1) If all the bits in the host field are 1's, the address is a broadcast (that is, anything sent to that address will go to everything on that network). (2) If all the bits in the host field are set to 0's, that's the network address. and (3) Any combination other than these two present the usable range of addresses in that network.
- IPv4 broadcast addressing has two main types. *Limited* broadcast addresses are delivered to every system inside the broadcast domain, and they use IP address 255.255.255.255 (destination MAC FF:FF:FF:FF:FF:FF). Routers ignore all limited broadcasts and do not even open the packets on receipt. *Directed* broadcasts are sent to all devices on a subnet, and they use the subnet's broadcast address (for example, the direct broadcast address for 192.168.17.0/24 would be 192.168.17.255). Routers may actually take action on these packets, depending on what's involved.

- A *routed* protocol is one that is actually being packaged up and moved around. IPv4 and IPv6, for instance, are routed protocols. A routing protocol is the one that decides the best way to get to the destination (for example, BGP, OSPF, or RIP).
- *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—examining things like Time-to-Live (TTL), window sizes, Don't Fragment (DF) flags, and Type of Service (ToS) fields from the capture.

Tools

- *Nmap* is one of the most common scanners available. The syntax for the tool is

  ```
  nmap <scan options> <target>
  ```

- Nmap has numerous switches for setting scan options. A few to remember are -sA (ACK scan), -sT (TCP Connect scan), -oN (normal output), -T0 (paranoid, slowest), and -T5 (insane, fastest).
- A response to a scan indicates whether the port is open. A quick-and-easy tip to remember is that all scans return a RST on a closed port, with the exception of the ACK scan, which returns no response.
- Port sweeping and enumeration on a machine are also known as *fingerprinting,* although the term is normally associated with examining the OS itself. You can fingerprint operating systems with tools such as SolarWinds, Queso, and Cheops.
- *Hping* is another powerful scanning tool. It works on Windows and Linux versions, can act as a packet builder, and runs nearly any scan nmap can put out. The syntax is

  ```
  hping3 <options> <IPAddress>
  ```

- *NESSUS* is a well-known and popular vulnerability assessment scanner. It is continually updated and has thousands of "plug-ins" available for almost any usage you can think of.
- *Retina* is a vulnerability scanning application. Owned by eEye, Retina is a popular choice on Department of Defense (DoD) and government networks.

Other Scanning Tips and Tools

- A *proxy* is a system set up to act as an intermediary between you and your targets. Attackers send commands and requests to a proxy and then let the proxy relay them to the targets, thus effectively hiding their tracks. Proxying can be done from a single location or spread across multiple proxies, to further disguise the original source.

- Hping3, Scapy, and Komodia are tools used for IP address spoofing. Spoofing an IP address means that any data coming back to the fake address will not be seen by the attacker.
- *Source routing* was designed to allow applications to specify the route a packet takes to a destination, regardless of what the route tables between the two systems say. It can be co-opted for use by attackers.
- *Anonymizers* are services on the Internet that make use of a web proxy to hide your identity.

Enumeration

- In Windows operating systems, a *security identifier (SID)* identifies user, group, and computer accounts and follows a specific format. A *relative ID (RID)* is a portion of the overall SID identifying a specific user, computer, or domain. SIDs are composed of an *S,* followed by a revision number, an authority value, a domain or computer indicator, and an RID. The RID portion of the identifier starts at 500 for the administrator account. The next account on the system, Guest, is RID 501. All users created for the system start at 1000 and increment from that point forward—even if their user name is re-created later.
- Linux uses a user ID (UID) and a group ID (GID) in much the same way as Windows uses SIDs and RIDs. On a Linux machine, groups are typically found in /etc/groups, and the mapping of a user to a group can be found in the /etc/passwd file.
- In Windows, passwords are stored in C:\Windows\System 32\Config\SAM. The SAM database holds (in encrypted format, of course) all the local passwords for accounts on the machine. For those machines that are part of a domain, the passwords are stored and handled by the domain controller. You may be able to pull a copy of the SAM file from the repair volume as well.
- Some Linux enumeration commands include finger (provides information on the user and host machine), rpcinfo and rpcclient (providing information on RPC in the environment), and showmount (displays all the shared directories on the machine).
- A null session is sometimes an effective method to enumerate a Windows system. A null session occurs when you log into a system with no user ID and password at all. The syntax for a null session is as follows:

  ```
  net use \\<target>\IPC$ "" /u:""
  ```

  Null sessions require TCP ports 135, 137, 139, and 445 to work.
- Nbtstat is a command-line tool that is useful in enumerating NetBIOS. NetBIOS enumeration questions will generally be about identifying the suffix. Pay special attention to the server identifiers: 1B is the master browser for the subnet, 1C is a domain controller, and 1D is the domain master browser.

- Some tools that make use of the null session are SuperScan, User2SID, and SID2User. User2SID and SID2User allow you to enumerate the SID given the user name or allow you to enumerate the user name given the SID.
- *Banner grabbing* is one of the easiest enumerating methods and involves sending an unsolicited request to an open port to see what, if any, default message (banner) is returned. A common method for banner grabbing is to use Telnet.

  ```
  telnet <IPAddress> <port_Number>
  ```

- Known as the "Swiss Army knife of hacking tools," netcat is a command-line networking utility that reads and writes data across network connections using TCP/IP. It's also a tunneling protocol, a scanner, and an advanced hacking tool. You can accomplish banner grabbing with this tool as well with the following syntax:

  ```
  nc <IPaddress or FQDN> <port number>
  ```

- SNMP uses a community string as a form of a password. The read-only version of the community string allows a requester to read virtually anything SNMP can drag out of the device, whereas the read-write version is used to control access for the SNMP SET requests. The default read string is public, and the default write string is private. Tools you can use to enumerate with SNMP include SNMPUtil, OpUtils 5, and IP Network Browser (SolarWinds).
- Lightweight Directory Access Protocol (LDAP) is *designed* to be queried, so it presents a perfect enumeration option. LDAP sessions are started by a client on TCP port 389 connecting to a Directory System Agent (DSA). The request queries the hierarchical/logical structure within LDAP and returns an answer using Basic Encryption Rules (BER). Tools like JXplorer, Lex, softerra, and the built-in Active Directory Explorer can make LDAP information gathering quick and easy.
- 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. Their responses can tell us which are valid and which are invalid user names.

Chapter 4 Sniffing and Evasion

Data exchanges over a network are a lot like conversations between people: If the conversation happens somewhere that is accessible by others, it can be overheard. In networking, if you have the right tools and are in the right place at the right time, you can pick up information just as easily as eavesdropping on a conversation. This section is about the tools and methods used in this endeavor.

Communication Basics

- Regardless of OS, the NIC still has to be told to behave promiscuously. On Windows, the de facto driver/library choice is *winpcap*. On Linux, it's *libpcap*.

- Collision domains are composed of all the machines *sharing* any given transport medium. Hobs extend collisions domains; switches segment them.
- *Sniffing* is the art of capturing packets as they pass on a wire, or over the airwaves, to review for interesting information.
- Examples of Application layer protocols include SMTP (e-mail; uses TCP, sends in clear text, and carries only ASCII), FTP (file transfer; uses TCP and sends in clear text), HTTP (transfers HTML files and uses TCP), and SNMP (network management; uses UDP).
- SMTP, FTP, TFTP, SNMP, POP3, and HTTP send information in clear text, making them susceptible to sniffing.
- Transport layer protocols include TCP (connection oriented, three-way handshake, slower) and UDP (connectionless, fire and forget, faster).
- The MAC address (a.k.a. physical address) that is burned onto a NIC is made of two sections. The first half of the address (3 bytes, or 24 bits) is known as the organizational unique identifier and is used to identify the card manufacturer. The second half is a unique number burned in at manufacturing to ensure no two cards on any given subnet will have the same address.
- The Address Resolution Protocol (ARP) is used to map IP addresses to MAC addresses. ARP is broadcast based and updates a cache on the local system. The process of maliciously changing an ARP cache on a machine to inject faulty entries is known as *ARP poisoning* (a.k.a. *gratuitous ARP*).
- The three types of frames within TCP/IP networking are unicast, multicast, and broadcast. Unicast frames have a MAC address in the destination field intended for a single machine (only this machine will open the frame). Multicast frames have a MAC address in the destination field intended for any machines that need the information (only machines looking for that multicast address will open the frame). Broadcast frames have a MAC address in the destination field intended for every machine on the subnet (all machines open this frame).
- Broadcast MAC addresses have all bits turned on and appear as all Fs (that is, FF:FF:FF:FF:FF:FF).
- Switches flood all broadcast and multicast frames to all ports. Switches filter unicast frames only to the port with the intended recipient attached.
- IPv6 uses a 128-bit address instead of the 32-bit IPv4 version and is represented as eight groups of four hexadecimal digits separated by colons. Leading zeroes from any groups of hexadecimal digits can be removed, and consecutive sections of zeroes can be replaced with a double colon (::). This is usually done to either all or none of the leading zeroes.
- The IPv6 loopback address is 0000:0000:0000:0000:0000:0000:0000:0001 and may be edited all the way down to ::1.

- In IPv6, the address block fe80::/10 has been reserved 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.
- The packets in DHCPv6 have different names than those of DHCPv4. DHCPDISCOVER, DHCPOFFER, DHCPREQUEST, and DHCPACK are known as Solicit, Advertise, Request (or Confirm/Renew), and Reply, respectively.

Sniffing

- Machines running a sniffer must have the NIC in *promiscuous mode,* which allows the NIC to accept and open all frames, regardless of address. A special driver is required for the NIC to behave in this way. WinPcap is an example of a driver that allows the operating system to provide low-level network access and is used by a lot of sniffers on Windows machines' NICs.
- Wireshark is one of the most popular sniffers and can capture packets from wired or wireless networks, providing an easy-to-use interface. The top portion of the display is called the packet list and shows all the captured packets. The middle portion, called the packet detail, displays the sections within the frame and packet headers. The bottom portion displays the actual hex entries in the highlighted section.
- Following a TCP stream in Wireshark (by choosing that option on a selected packet) is a great way to see an entire conversation, which can lead to the discovery of passwords in the clear.
- Wireshark filters are used to display only the information you want to see in the packet capture. The expressions builder within the application can put them together. There are multiple syntax methods for an expression. As another important study tip, watch for the period (.) between *ip* and *src* because on the exam they'll drop it or change it to a dash (-) to trick you.
- There are innumerable filter combinations in Wireshark. Make very sure you are familiar with what the *equal to*, *and*, and *or* conjunctions mean. *Equal to* (==) means exactly what it says—the packet will display if the argument appears in the packet. *And* (&&) means the packet will display only if *both* arguments appear. *Or* (or) means the packet will display if either argument appears.
- Wireshark also 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.
- The command-line tool tcpdump is another classic, well-known sniffer. At one time, it was Unix-based only (a Windows version is now available). The syntax for this tool is simple:

```
tcpdump flag(s) interface
```

Multiple available flags and Boolean combinations can make for some pretty elegant search strings. For example, the following will show all data packets (no SYN, FIN, or ACK only) to and from port 80:

```
tcpdump 'tcp port 80 and (((ip[2:2] - ((ip[0]&0xf)<<2)) -
((tcp[12]&0xf0)>>2)) != 0)'
```

- Within a lawful intercept, the components used are a tap (usually the service provider allows a port opening for this), something to process all the data (the mediation device), and a collection area where the data is stored and parsed/processed further.
- Sniffing can be active or passive in nature. If you are not injecting packets into the stream, it's a passive exercise.

Flooding and Spoofing

- The process of sending lots of broadcast traffic to a switch in order to force it out to all recipients is called *flooding*. Tools that make ARP flooding easy are Cain and Abel (Windows hacking tool) and dsniff (a collection of Linux tools holding a tool called ARPspoof).
- Adding a MAC address permanently into the ARP cache on each device can be done with the ARP command *arp -s*.
- A *MAC flood* is defined as the practice of sending thousands of unsolicited MACs to the switch and thus filling up the content addressable memory (CAM) table. The CAM is finite in size; when it fills up, the switch is effectively turned into a hub—flooding all incoming packets out all ports.
- *Port security* refers to a security feature on switches that allows an administrator to manually assign MAC addresses to a specific port; if the machine connecting to the port does not use that particular MAC, it isn't allowed to connect.
- *Port spanning* (also called *port mirroring*) is a method of configuring a port on a switch to receive a copy of all frames being sent out other ports. A span port may span a single port, multiple ports, or all ports on a switch. Span ports do not transmit data; they are used for monitoring only.
- DHCP starvation is an attack whereby the malicious agent attempts to exhaust all available addresses from the server.
- ECC defines some versions of MAC flooding as "switch port stealing." The idea is the same—flood the CAM with unsolicited ARPs. But instead of attempting to 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.

Intrusion Detection

- *Intrusion detection systems* (IDSs) are hardware and/or software devices that examine streams of packets for unusual or malicious behavior. An IDS is signature based (matching packets to a signature file) or anomaly based (learning traffic patterns over time). A signature-based system is only as good as the signature list itself. An anomaly-based system may be better at picking up the latest attacks because they would definitely be out of the norm, but such systems are also known to have excessive false positives, especially during setup.
- A *false negative* occurs when the IDS reports a particular stream of traffic is just fine, with no corresponding alarm or alert, when in fact an intrusion attempt did occur. False negatives are considered far worse than false positives.
- Snort is a popular IDS and runs in three different modes. Sniffer mode is exactly what it sounds like and lets you watch packets in real time as they come across your network tap. Packet Logger mode saves packets to disk for review at a later time. Network Intrusion Detection System mode analyzes network traffic against various rule sets you pick from, depending on your network's situation.
- The Snort configuration file resides in /etc/snort on Unix/Linux and c:\snort\etc\ on most Windows installations. Snort can be started using a command such as this:

```
snort -l c:\snort\log\ -c c:\snort\etc\snort.conf
```

- Snort rules are composed of an action, a protocol, a source address/port, a destination address/port, and message parameters.
- IDS evasion tactics include slowing down traffic, flooding massive amounts of traffic, session splicing (fragmentation), Unicode, and encryption.
- libwhisker (https://sourceforge.net) is a full-featured Perl library used for HTTP-related functions, including vulnerability scanning, exploitation, and, of course, IDS evasion.

Firewalls and Honeypots

- A *firewall* is an appliance within a network that is designed to protect internal resources from unauthorized external access using a set of rules *explicitly* stating what is allowed to pass from one side of the firewall to the other. Most firewalls work with an *implicit deny* principle, which means if there is no rule defined to allow the packet to pass, it is blocked—there is no need to create a rule to deny packets.
- A *stateful inspection* firewall has the means to track the entire status of a connection. A *packet-filtering* firewall matches packets to a signature file.
- The process of "walking" through every port against a firewall to determine what is open is known as *firewalking*.
- A *honeypot* is a system set up as a decoy to entice attackers.

- HTTP tunneling is a firewall evasion technique you'll definitely see on the exam.
- 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: they're called bastions because they can withstand Internet traffic attacks. 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 firewall has two or more interfaces, it is referred to as *multi-homed.*

Chapter 5 Attacking a System

Preparation with background knowledge, system architecture, and basic network and communication knowledge is essential before attacking a system. This section deals with the actual attacks and the system architecture goodies you'll need to know to be successful.

Methodology

- The system hacking stages are gaining access, escalating privileges, executing applications, hiding files, and covering tracks. These can be further defined by five steps: cracking passwords, escalating privileges, executing applications, hiding files, and covering tracks.

Password Attacks

- Password strength is usually determined by two major functions: length and complexity. On the exam, complexity will trump length. Per EC-Council, the password must not contain any part of the user's name, must have a minimum of eight characters, and must contain characters from at least three of the four major components of complexity.
- Four main attack types are defined within CEH: passive online (sniffing a wire in the hopes of either intercepting a password in clear text or attempting a replay or man-in-the-middle attack), active online (the attacker begins guessing passwords), offline (the hacker steals a copy of the password file and works the cracking efforts on a separate system), and nonelectronic (social engineering).
- *Sidejacking* is an attack whereby the hacker steals cookies exchanged between two systems and discovers which one to use as a replay-style attack.
- Some tools for passive online password hacking include Cain and Abel, Ettercap, ScoopLM, and KerbCrack. Ettercap can ARP poison and sniff traffic. ScoopLM has a built-in password cracker and specifically looks for Windows authentication traffic on the wire to pull passwords from. KerbCrack is designed

to crack Kerberos authentication and has a built-in sniffer and password cracker, specifically looking for port 88 Kerberos traffic.

- Some net commands to remember in Windows include *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), and *net use \\target\ipc$ "" /u:"* (sets up a null session).
- Three major offline password-cracking methods are available: dictionary attack, hybrid attack, and brute-force attack. A *dictionary attack* uses a list of passwords in a text file, which is then hashed by the same algorithm/process the original password was put through (the easiest and fastest attack available). A *hybrid attack* takes words from a dictionary list and substitutes numbers and symbols for alpha characters (hybrid attacks may also append numbers and symbols to the end of dictionary file passwords). A *brute-force attack* attempts every conceivable combination of letters, numbers, and special characters against the password hash to determine a match (takes the longest amount of time).
- *Rainbow tables* are large text files containing the hash of almost every password imaginable for a given algorithm. A rainbow table greatly speeds up offline password cracking.
- *John the Ripper* is an offline password-cracking Linux tool that can crack Unix, NT, and Kerberos passwords.
- *LC5,* the next generation of the old L0phtCrack tool, is a Windows-based password cracker.
- *Keylogging* is the process of using a hardware device or software application to capture the keystrokes a user types. Keyloggers can be hardware devices—usually small devices connected between the keyboard cable and the computer—or software applications installed and running in the background. Software keyloggers are easy to spot with antivirus software and other scanning options; however, hardware keyloggers are almost impossible to detect and are almost always very effective.

Windows Essentials

- LM hashing (in LAN Manager and then NT LAN Manager) creates hashed Windows passwords by converting the password to all uppercase, splitting it into two seven-character strings, and hashing each portion. If a password is less than 14 characters, it simply appends spaces to the end to reach 14. Therefore, if the password is seven characters or less, the second half of the password hash will always be AAD3B435B51404EE.
- LM authentication (DES) was used with Windows 95/98 machines. NTLM (DES and MD$) was used with NT machines until SP3. NTLM v2 (MD5) was used after that. Kerberos came about with Windows 2000. LM authentication has six different levels available: 0 is the XP default, and 2 is the 2003 default.

- Kerberos makes use of both symmetric and asymmetric encryption technologies to securely transmit passwords and keys across a network. The entire process consists of a key distribution center (KDC), an authentication service (AS), a ticket-granting service (TGS), and a ticket-granting ticket (TGT).
- A Kerberos authentication effort follows a set pattern. The client first asks the KDC, which holds the AS and TGS, for a ticket, which will be used to authenticate throughout the network. This request is in clear text. The server will respond with a secret key, which is hashed by the password copy kept on the server (in Active Directory). This is known as the TGT. If the client can decrypt the message, the TGT is sent back to the server requesting a TGS service ticket. The server responds with the service ticket, and the client is allowed to log on and access network resources.
- Registry hives include HKEY_LOCAL_MACHINE (HKLM: contains information on hardware and software), HKEY_CLASSES_ROOT (HKCR: contains information on file associations and OLE classes), HKEY_CURRENT_USER (HKCU: contains profile information for the user currently logged on, such as user-level preferences for the OS and applications), HKEY_USERS (HKU: contains specific user configuration information for all currently active users on the computer), and HKEY_CURRENT_CONFIG (HKCC: a pointer to HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\CurrentControlSet\Hardware Profiles\Current, designed to make accessing and editing this profile information easier).
- Microsoft Management Consoles (MMCs) are basically small GUI containers in Windows systems for specific tools. Each MMC holds an administrative tool for a given task, added in the console as a "snap-in," and is named for that task. For example, there is an MMC named "Group Policy Editor" that allows an admin to edit the group policy. Other MMCs include Computer Management, Event Viewer, and Services, along with many more.
- 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.

Escalating Privileges

- Obtaining administrator (root) privileges on a machine can be accomplished by cracking the password of an administrator or root account, or taking advantage of a vulnerability found in the OS (or application), that will allow you access as a privileged user. You can also use tools specifically designed for escalation or use social engineering to have the currently logged-on user perform actions for you.

- Metasploit is an entire hacking suite in one and is a great exploit-testing tool that can also be of value in escalating privileges.
- Examples of tools used for privilege escalation are Billybastard.c (useful on 2003 and XP Windows machines) and GetAD (XP). Older tools (for 2000 and NT devices) are GetAdmin and HK.exe.
- 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.
- DLL hijacking can prove very useful in privilege escalation. Most Windows applications don't bother with a full path when loading external DLLs. If you can somehow replace DLLs in the same application directory with your own nefarious versions, you might be in business.

Stealth

- Stealth in hacking comes down to patience (spend enough time, move slow enough, and chances are better than not you'll go unnoticed), hiding files, covering your tracks, and maintaining access on the machine.
- Alternate Data Streams (ADS) is a feature of the Windows-native NTFS file systems that ensures compatibility with Apple file systems (called HFS). It can be used to hide files in the form of NTFS file streaming. NTFS file steaming allows you to hide virtually any file behind any other file, rendering it invisible to directory searches. A sample syntax for NTFS file streaming would look like this:

  ```
  type wanttohide.txt > original.txt:hidden.txt
  ```

  In this example, the wantohide.txt file is being hidden behind the original.txt file.
- Several applications, such as LNS and Sfind, were created specifically to hunt down ADS. Additionally, the *dir /r* directory command in Windows Vista will display all file streams in the directory. Lastly, copying files to and from a FAT partition removes any residual file streams in the directory.
- The *hidden* file attribute sets the file to not display during file searches or folder browsing (unless the admin changes the view to force all hidden files to show). In Windows, you can hide a file by right-clicking, choosing Properties, and checking the Hidden Attribute check box at the bottom of the dialog box. This can also be done by issuing the attrib command: *attrib +h filename*.
- Hiding a file on a Windows machine from a cursory search can also be accomplished by marking it as a system file. The *attrib -s* command can accomplish this.

- Steganography is a good method to hide information. Tools for hiding files include ImageHide, Snow, Mp3Stego, Blindside, S-tools, WbStego, and Stealth.
- Another term used in regard to steganography is *semagram*. There are two types: visual and text. A visual semagram uses an everyday object to convey a message. Examples can include doodling as well as the way items are laid out on a desk. A text semagram obscures a message in text by using things such as font, size, type, or spacing.
- In Windows, three main logs must be scrubbed to cover tracks: the application, system, and security logs. The application log holds entries specifically related to the applications themselves, and only entries programmed by the developers get in. The system log registers system events, such as drivers failing and startup/shutdown times. The security log records the login attempts, access, and activities regarding resources, and so on.
- The security log will not record anything unless expressly configured to do so with auditing. You must have administrative privileges on the machine to set up auditing.
- Corrupting log files is often an effective method to cover tracks, as opposed to deleting or editing them.
- Log files in Windows are kept in the %systemroot%\System32\Config folder by default (each will have an .evt extension). Updating the individual file entries in the appropriate registry key (that is, HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\EventLog) allows you to place them wherever you'd like.
- In Control Panel | Administrative Tools | Local Security Policy, you can set up and change the audit policy for the system. The top-level settings are found under Local Policies | Audit Policy. Other settings of note are found in the Advanced Audit Policy Configuration at the bottom of the listings under Security Settings.
- Elsave, WinZapper, and Evidence Eliminator are all Windows log file tools.
- Auditpol is a tool included in the old NT Resource Kit that can be used to disable event logs on other machines. Here's the syntax:

```
c:\auditpol \\targetIPaddress /disable
```

Rootkits

- A *rootkit* is a collection of software put in place by an attacker that is designed to obscure system compromise. Rootkits are designed to provide backdoors for the attacker to use later and include measures to remove and hide evidence of any activity.

- Rootkits are notoriously difficult to remove and usually require a complete wipe and reload of the system.
- Per the CEH objectives, there are three types of rootkits: application level (directed at replacing valid application files with Trojan binaries), kernel level (attacks the boot sectors and kernel level of the operating systems themselves, replacing kernel code with backdoor code—by far the most dangerous and difficult to detect and remove), and library level (makes use of system-level calls to hide their existence).
- Tripwire is a file and service integrity verification tool that can be useful in detecting rootkits and their behavior on a system.
- Sigverif can find unsigned drivers and verify device drivers in Windows XP.

Linux Essentials

- Linux starts with a root directory just like Windows does. the Windows root is (usually) C:\, whereas the Linux root is just a slash (/). It also has folders holding specific information for specific purposes.
- The basic file structure for Linux includes these important folders you should memorize: / (a forward slash; represents the root directory), /bin (holds basic Linux commands, like the C:\Windows\System32 folder in Windows), /dev (contains 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), /etc (contains all the administration files and passwords; both the password and shadow file are found here), /home (user home directories), /mnt (holds the access locations you've actually mounted), /sbin (holds more administrative commands and is the repository for most of the routines Linux runs), and /usr (holds most of the information, commands, and files unique to the users).
- Security on files and folders is managed through your user account, your user's group membership, and three security options that can be assigned to each for any resource: read, write, and execute. These security rights can be assigned only by the owner of the object. Typing the command *ls -l* will display the current security settings for the contents of the directory you're in.
- Permissions are assigned via the chmod command and the use of the binary equivalent for each rwx group: Read is equivalent to 4, write is 2, and execute is 1. For example, the command *chmod 464 file1* would set the permissions "r--rw-r--" for file1.
- Adding an ampersand (&) after a process name indicates that the process should run in the background. If you wish for the process to remain after user logout (that is, stay persistent) use the nohup command.

- All users and groups are organized via a unique user ID (UID) and a group ID (GUID). Information for both can be found within the /etc/passwd file. Running a cat command on the file displays the information, as in

  ```
  matt:x:500:500:Matt:/home/mat:/bin/csh
  ```

  where UID and GID are set to 500 and the *x* indicates the use of the shadow file for passwords.
- Passwords in Linux can be stored the *passwd* file (all passwords will be displayed in clear text) or the *shadow* file (passwords are stored and displayed encrypted). The shadow file is accessible only by root. Some Linux distributions do not shadow passwords by default (an example is HPUX 11.11).
- Most install files will come in the form of a *tar* file, which is basically a zipped file. The application most commonly used to unzip to the raw files is gzip. There are generally three commands to compile most programs in Linux: ./configure, make, and make install.
- GNU Compiler Collection (GCC) can compile and execute from several languages, such as C, C++, and FORTRAN. For example, if you had a C++ source file (sample.cpp) and wanted to compile it in Linux, the command might look something like this:

  ```
  g++ sample.cpp newapp.exe
  ```

Vulnerability Scanners

- *Nessus* is well known and has an excellent reputation (an older version of Nessus is Newt, or Nessus Windows Technology). Nessus can be used to run a vulnerability scan across your entire subnet, or it can be aimed at a single machine. Nessus used to be open source and freely available but is now a commercial entity.
- *Retina* is a commercial vulnerability assessment scanner by eEye. Retina is used widely in DoD networks. Mostly a GUI interface, Retina runs natively on a Windows machine and can scan subnets or individual systems.
- *Core Impact* is much more than a simple vulnerability scanner. It is a point-and-shoot comprehensive penetration testing product. It's expensive but is used widely within the federal government and as part of many commercial pen test teams.
- Much like Nessus, *SAINT* used to be open source but is now a commercial entity. SAINT runs natively on Unix.
- A biometric passport (also known as an *e-passport*) is a token you carry with you that holds biometric information identifying you. Even though it sounds like a two-factor measure, because it's a single token, its use is considered just something you *have.*

Chapter 6 Web-Based Hacking: Servers and Applications

Whereas most of your targets are nestled away comfortably behind network security defenses, firewalls, and a host of protection efforts, web servers and applications are purposefully left out in the open. After all, if they're not publicly accessible, no one would be able to read about the company's services or take part in their e-commerce offerings. Web servers and web applications are going to be one of your best bets in gaining access.

Web Organizations and Standards

- The Internet Engineering Task Force (IEFT; https://www.ietf.org/) 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 Request For Comments (RFCs).
- World Wide Web Consortium (W3C; https://www.w3.org) is an international community where member organizations, a full-time staff, and the public work together to develop web standards.
- The Open Web Application Security Project (OWASP; https://www.owasp.org) is a 501(c)(3) worldwide not-for-profit charitable organization focused on improving the security of software. Their mission is to make software security visible so that individuals and organizations worldwide can make informed decisions about true software security risks. The OWASP Top Ten is a powerful awareness document for web application security. The OWASP Top Ten represents a broad consensus about what the most critical web application security flaws are.
- WebGoat (https://www.owasp.org/index.php/Category:OWASP_WebGoat_Project) is a deliberately insecure web application maintained by OWASP that is designed to teach web application security lessons.

Web Server Architecture

- Apache configuration is almost always done as part of a module within special files (http.conf, for instance, can be used to set server status), and the modules are appropriately named (mod_negotiation, for instance).
- IIS will spawn all shells as LOCAL_SYSTEM.
- HTML entities include   (for a blank, nonbreaking space), " (“), ' (‘), & (&), < (<), and > (>).
- An HTTP GET requests data from a resource, such as “Please send me the HTML for the web page located at _insert-URL-here_.” The problem with it is HTTP GET can also be used to *send* data, and when sending data, the GET method adds the data to the URL. A POST, on the other hand, is a much better

method of submitting data to a resource for processing. It can also be used to elicit a response, but its primary purpose is to provide data for the server to work with. POST is generally considered safer than GET because it is not stored in browser history or in the server logs, and it doesn't display returned data in the URL.

- Other HTTP methods include HEAD (identical to GET except that the server MUST NOT return a message-body in the response; often used for testing hypertext links for validity, accessibility, and recent modification, and requesting headers and metadata), PUT (requests that the enclosed entity be stored under the supplied Request-URI), DELETE (requests that the origin server delete the resource identified by the Request-URI), TRACE (used to invoke a remote, application-layer loop-back of the request message), and CONNECT (reserved for use with a proxy that can dynamically switch to being a tunnel; e.g., SSL tunneling).
- The first digit of an HTTP Status-Code defines the class of response. The last two digits do not have any categorization role, but more thoroughly define the response intent. There are five values for the first digit: 1xx: Informational (request received, continuing process), 2xx: Success (action was successfully received, understood, and accepted), 3xx: Redirection (further action must be taken in order to complete the request), 4xx: Client Error (request contains bad syntax or cannot be fulfilled), and 5xx: Server Error (server failed to fulfill an apparently valid request).

Web Attacks

- EC-Council defines six different stages in web server attack methodology: information gathering, footprinting, mirroring websites, vulnerability scanning, session hijacking, and password cracking.
- *Directory traversal,* also known as the *dot slash attack,* is a common, and sometimes successful, attack whereby an attacker uses the URL to navigate through the directory structure on the web server to execute commands. An example of a directory traversal attack might look like this:

  `www.example.com/../../../../directory_of_choice/command.exe`
- Directory traversal can also be accomplished using Unicode (the dot-dot-slash appears as %2e%2e%2f in Unicode). Unicode is a standard for ensuring consistent encoding and text representation and can be accepted by servers for malicious purposes. 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 access passwords, and so on.
- Parameter tampering is an attack where the URL parameters are changed to accomplish a specific goal, execute code, or gain access to hidden areas. Another version of parameter tampering involves manipulating the hidden field on the source code (copying the source code to the local system and changing *hidden* field entries).

- LDAP injection is an attack that exploits applications that construct LDAP statements based on user input. To be more specific, it exploits nonvalidated web input that passes LDAP queries.
- SOAP injection is another web attack. Simple Object Access Protocol (SOAP) is designed to exchange structured information in web services in computer networks and uses XML to format information.

Web Application Attacks

- *SQL injection* is the most common and most successful web application attack technique in the world and involves entering SQL queries and commands into a web front end to manipulate the database being accessed by the website. SQL injection occurs when the attacker injects SQL queries directly into the input form. Properly constructed, the SQL command bypasses the intent of the front end and executes directly on the SQL database.
- *Structured Query Language (SQL)* is a computer "language" designed for managing data in a relational database system. The relational database itself is simply a collection of tables (consisting of rows that hold individual fields containing data) tied together using some common field (key) that you can update and query. Each table has a name given to it that is referenced when you perform queries or updates. Common commands seen on the exam include SELECT, DROP TABLE, and INSERT.
- An easy test to see whether an application is vulnerable to SQL injection is to enter a single quote (another common example is entering ***anything***' or **1=1--**).
- *Blind SQL injection* 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. Because there's a lot of guesswork and trial and error, this attack takes a long while to pull off.
- Some SQL injection tools include SQLMap, SQLNinja, Havij, SQL Brute, Pangolin, SQLExec, Absinthe, and BobCat.
- *Cross-site scripting (XSS)* is another common attack dealing with web design and dynamic content. In XSS, a script is inserted into a form field, URL, or link for a user to click—the code is executed instead of the "normal" processing done by the server for that web application.
- A URL such as http://IPADDRESS/";!- -"<XSS>=&{()} is an indicator of an XSS attempt. Additionally, entering JavaScript or other scripting into a form field is an indicator of XSS attempts.
- Buffer overflow attacks attempt to write more data into an application's prebuilt buffer area in order to overwrite adjacent memory, execute code, or crash a system (application).

- Buffer overflow attack categories are stack, heap, and NOP sled. *Stack buffer overflows* take advantage of program calls being kept in a stack and executed in order. They affect the stack with a buffer overflow and change a function pointer or variable to allow code execution. *Heap buffer overflows* take advantage of the memory "on top" of the application, which is allocated dynamically at run time. *NOP sleds* make use of a machine instruction called no-op. In the attack, a hacker sends a large number of NOP instructions into the buffer, appending command code instruction at the end.
- *Canary words* are known values placed between the buffer and control data. If a buffer overflow occurs, the canary word will be altered first, triggering a halt to the system. Tools such as StackGuard make use of this for stack protection.
- A *cookie* is a small text-based file that is stored on your system for use by the web server the next time you log in, containing information such as authentication details, site preferences, shopping cart contents, and session details. Cookies are sent in the header of an HTTP response from a web server and may or may not have an expiration date.
- Tools that search for vulnerabilities on web applications and sites include Netcraft, HttpRecon, ID Serve (identifying, reliably, the web server architecture and OS), httPrint, BurpSuite (insight into content on the site the owner probably didn't want disclosed), Black Widow, and Httrack (to make a copy of the website on your system for your review).
- Nikto is a vulnerability scanner more suited specifically for web servers.
- A cross-site request forgery (CSRF) is a fun attack that forces an end user to execute unwanted actions on a web application in which they're currently authenticated. CSRF attacks can be mitigated by configuring a web server to send random challenge tokens. If every user request includes the challenge token, it becomes easy to spot illegitimate requests not initiated by the user.
- A session fixation attack is somewhat similar to CSRF. 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.

Chapter 7 Wireless Network Hacking

Wireless computing is here to stay, and what a benefit it is to the world. The freedom and ease of use it offers are wonderful and, truly, are changing our society day by day. However, along with that we have to use a little caution. If data is sent over the airwaves, it can be received over the airwaves—by anyone (maybe not in clear text, and maybe not easily discernable, but it can be received). Therefore, we need to explore the means of

securing our data and preventing accidental spillage. And that, dear reader, is what this chapter is all about.

Wireless Standards and Architecture

- 802.11a operates on the 5GHz frequency range and can run at speeds up to 54 Mbps. This standard doesn't provide as wide a range as others and isn't used as commonly as others.
- 802.11b operates on the 2.4GHz frequency range and can run at speeds up to 11 Mbps.
- 802.11g operates on the 2.4GHz frequency range and can run at speeds up to 54 Mbps. It is backward compatible with 802.11b.
- 802.11n operates on the 2.4GHz through 5GHz frequency range and can run at speeds up to 100 Mbps.
- When you have a single access point, its "footprint" is called a *basic service area* (BSA). Communications between this *single* AP and its clients is known as a *basic service set* (BSS). An *extended service set* (ESS) is created with multiple APs serving a single network. As a client moves from one AP in your subnet to another, as long as you've configured everything correctly, they'll disassociate from one AP and re-associate with another seamlessly. This movement across multiple APs within a single ESS is known as *roaming*.
- An omnidirectional antenna provides connectivity in a 360-degree range radiating from the antenna. A directional antenna (sometimes called a Yagi antenna, after the inventor of the technology and a term now used interchangeably with this antenna type) focuses the signal in one direction. This results in much better use of signal strength but greatly extends the range at which the signal can be picked up.
- Dipole antennas have two signal "towers" and work omnidirectionally. Parabolic grid antennas work a lot like satellite dishes and can have a phenomenal range (up to 10 miles).
- The service set identifier (SSID) is not a password and is not designed for security purposes at all. SSIDs are 32-character-or-less labels that identify your wireless network from others. SSIDs are broadcast by default and are easily obtainable even if you try to turn off the broadcast. Turning off SSID broadcasting is known as *SSID cloaking*. The SSID is part of the header on every packet, so its discovery by a determined attacker is a given—broadcast or not.
- There is a difference between association and authentication. *Association* is the action of a client connecting to an AP, whereas *authentication* actually identifies the client before it can access anything on the network.

Wireless Security

- Wired Equivalent Privacy (WEP) is designed to give people using a wireless network the same level of protection that someone surfing over an Ethernet wired hub would expect. Encryption is weak and easily cracked. WEP uses 40-bit to 232-bit keys and RC4 as an encryption algorithm.
- An initialization vector (IV) provides for confidentiality and integrity in wireless encryption. IVs in WEP are relatively short (24 bits) and are reused often. An attacker simply needs to generate enough packets in order to analyze the IVs and come up with the key used. This allows them to decrypt the WEP shared key on the fly, in real time, which renders the encryption useless.
- A better choice in encryption technology is Wi-Fi Protected Access (WPA) or WPA2. WPA makes use of Temporal Key Integrity Protocol (TKIP), a 48-bit IV, a 128-bit encryption key, and the client's MAC address to accomplish much stronger encryption. WPA changes out the key every 10,000 packets or so, instead of sticking with one (and reusing it, as occurred in WEP). Additionally, the keys are transferred back and forth during an Extensible Authentication Protocol (EAP) authentication session, which makes use of a four-step handshake process in proving the client belongs to the AP, and vice versa.
- WPA2 was designed with the government and the enterprise in mind. In something called WPA2 Enterprise, you can tie EAP or a RADIUS server into the authentication side of WPA2, allowing you to make use of Kerberos tickets. (If you just want to use it at home or on your small network and don't want to bother with all those additional, and costly, authentication measures, use WPA2 Personal). WPA2 uses AES for encryption, ensuring FIPS 140-2 compliance, and Cipher Block Chaining Message Authentication Code Protocol (CCMP) for integrity.

Wireless Attacks

- *NetStumbler* is a wireless tool that can be used for identifying poor coverage locations within an ESS, detecting interference causes, and finding any rogue access points in the network.
- *Kismet* is a wireless packet analyzer/sniffer that can also be used to discover wireless networks. Kismet is Linux based and works passively. It detects access points and clients without actually sending or interjecting any packets. It can detect access points that have not been configured and will determine which type of encryption is in use. It works by "channel hopping" to discover as many networks as possible and has the ability to sniff packets and save them to a log file, readable by Wireshark or tcpdump.
- *Netsurveyor* is a free, easy-to-use, Windows-based tool that provides many of the same features as NetStumbler and Kismet. It supports almost all wireless adapters without any significant additional configuration and acts as a great tool for troubleshooting and during the installation of wireless networks.

- Other wireless sniffing tools include OmniPeek, AirMagnet WiFi Analyzer Pro, and WiFi Pilot. OmniPeek provides network activity status and monitoring in a nice dashboard for up-to-the minute viewing. AirMagnet's WiFi Analyzer, from Fluke Networks, can be used to resolve performance problems and automatically detect security threats and vulnerabilities.
- Setting up a rogue access point, in an attack sometimes referred to as the *evil twin*, allows an attacker to trick users into authenticating onto the fake AP and transferring data. Rogue APs (evil twins) may also be referenced as a *misassociation* attack.
- SMAC and TMAC are both MAC spoofing tools.
- The standard WEP attack follows four steps: Start a compatible wireless adapter on your attack machine and ensure it can both inject and sniff packets, start a sniffer to capture packets, use some method to force the creation of thousands and thousands of packets (generally by using "deauth" packets), and analyze these captured packets (either in real time or on the side) with a cracking tool.
- *Aircrack* is a tool used for cracking wireless encryption. It makes use of "KoreK implementation."
- *Aireplay* is used to generate deauthentication packets for wireless sniffing purposes. Here's an example of the syntax used:

```
aireplay -ng -0 0 -a 0A:00:2B:40:70:80 -c mon0
```

- *Airsnarf* is a simple rogue wireless access point setup utility designed to demonstrate how a rogue AP can steal user names and passwords from public wireless hotspots.
- Cain, Aircrack, KisMac, WEPCrack, chopchop, and Elcomsoft's Wireless Security Auditor are all useful tools in wireless hacking.

Chapter 8 Mobile Communications and the IoT

While the same attack types, ethical hacking procedures, and other security principles that we've covered also apply to the mobile world, the Internet of Things (IoT) adds a whole new dimension to look at. The vulnerabilities introduced by networking virtually everything in our homes and offices are staggering, and efforts to secure those devices are just as monumental. EC-Council added an entire new chapter to address IoT, and we'll take a look here.

Mobile Computing

- BYOD (Bring Your Own Device) refers to a wireless model allowing employees to bring their personal devices to work and make use of the business network.
- Mobile Device Management (MDM) is an effort to add some control to enterprise mobile devices. Much like group policy and such in the Microsoft Windows world, MDM helps in pushing security policies, application deployment, and monitoring of mobile devices. Some solutions include XenMobile, MaaS360, AirWatch, and MobiControl.

- Android and iOS make up the vast majority of mobile device operating systems. Performing some action that grants you administrative (root) access to the device so you can do whatever you want with it is called rooting (for Android) or jailbreaking (iOS).
- Some tools for rooting Android include SuperOneClick, Superboot, OneClickRoot, Kingo, unrevoked, RescueRoot, and UnlockRootPro.
- Types of jailbreaking include Userland (user-level access but not admin), iBoot, and Bootrom (both granting admin-level privileges). Some jailbreaking tools include evasi0n7, GeekSn0w, Pangu, Redsn0w, Absinthe, and Cydia.
- Techniques for jailbreaking include *untethered jailbreaking* (the kernel will remain patched—that is, jailbroken—after reboot, with or without a system connection), *semi-tethered jailbreaking* (a reboot no longer retains the patched kernel; however, the software has already been added to the device. Therefore, if admin privileges are required, the installed jailbreaking tool can be used.), and *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).
- SMS phishing (also known as smishing) is a mobile attack making use of text and SMS messaging to fool the victim.

Bluetooth

- *Bluetooth* is a wireless standard for connecting devices and transferring data over short distances (usually 10 meters or less). Bluetooth works at 2.45GHz and can attach up to eight devices simultaneously. It makes use of spread-spectrum frequency hopping, which significantly reduces the chance that more than one device will use the same frequency in communicating.
- Bluetooth has two modes of operation: pairable and nonpairable. *Nonpairable* rejects every connection request, whereas *pairable* accepts all of them.
- There are four Bluetooth attacks: *Bluesmacking* is a denial-of-service attack against a device. *Bluejacking* consists of sending unsolicited messages to, and from, mobile devices. *Bluesniffing* involves sniffing traffic from a device. *Bluescarfing* is the actual theft of data from a mobile device.
- BlueScanner is a good tool for discovering devices nearby, as well as for attempting to extract and display as much information as possible. BTBrowser is a good tool for finding and enumerating nearby devices. Bluesniff and BTCrawler are other Bluetooth tools.

OWASP Top 10 Mobile Risks

- The Open Web Application Security Project (OWASP) has an arm dedicated specifically to mobile security (https://www.owasp.org/index.php/OWASP_Mobile_Security_Project) and publishes a list of Top 10 Mobile Risks.

- The current Top 10 (https://www.owasp.org/index.php/Mobile_Top_10_2016-Top_10) includes the following vulnerabilities:

  M1 – Improper Platform Usage, M2 – Insecure Data Storage, M3 – Insecure Communication, M4 – Insecure Authentication, M5 – Insufficient Cryptography, M6 – Insecure Authorization, M7 – Client Code Quality, M8 – Code Tampering, M9 – Reverse Engineering, and M10 – Extraneous Functionality.

IoT

- The IoT is a collection of devices using sensors, software, storage, and electronics to collect, analyze, store, and share data among themselves or to a user.
- The IoT is also defined as a network of devices with IP addresses that have the capability of sensing, collecting, and sending data *to each other*—basically a web of connected devices made possible by machine-to-machine communications, large availability of storage, and internetworked communications.
- Another definition of IoT is technologies extending Internet connectivity beyond "standard" devices, such as desktops, laptops, smartphones, and tablets, to any range of traditionally non-network-enabled physical devices and *everyday objects*.

IoT Architecture

- There are three basic components to IoT architecture—things using *sensing technology*, *IoT gateways*, and the *cloud* (or put another way, data storage availability). A *thing* inside the IoT is defined as any device implanted somewhere with the ability (and purpose) of communicating on the network.
- IoT devices, each embedded with some form of sensing technology, can communicate and interact over the Internet, and oftentimes can be remotely monitored and controlled. In other words, sensors are embedded in the device to measure and forward data.
- Operating systems for IoT devices include RIOT OS, ARM mbed OS, RealSense OS X, Nucleus RTOS, and others.
- IoT devices communicate primarily via wireless and generally follow one of these four IoT communication models—device to device, device to gateway, device to cloud, and back-end data sharing.
- The device to gateway model adds a collective *before* sending to cloud, which can be used to offer some security controls. The back-end data sharing model is almost exactly like device to cloud; however, it adds the ability for third parties to collect and use the data, which makes it the one outlier of the four models.
- The *IoT gateway* is designed to send collected data from devices to the user or to the third component, *data storage* (or cloud), for use later. The cloud stores and analyzes data, providing information back for future queries.

- Architecture layers inside IoT include EdgeTechnology Layer, Access Gateway Layer, Internet Layer, Middleware Layer, and Application Layer.

IoT Vulnerabilities and Attacks

- The OWASP Top 10 for IoT (https://www.owasp.org/index.php/Top_IoT_Vulnerabilities) list includes the following vulnerabilities:

  I1 – Insecure Web Interface, I2 – Insufficient Authentication/Authorization, I3 – Insecure Network Services, I4 – Lack of Transport Encryption/Integrity Verification, I5 – Privacy Concerns, I6 – Insecure Cloud Interface, I7 – Insecure Mobile Interface, I8 – Insufficient Security Configurability, I9 – Insecure Software/Firmware, and I10 – Poor Physical Security.

- DDoS (distributed denial of service) in IoT isn't any different from any other DDoS against or using "normal" devices. In one version of this, noted as the *Sybil* attack in EC-Council's curriculum, multiple forged identities are used to create the illusion of traffic congestion that affects everyone else in the local IoT network.
- An *HVAC attack* is exactly what it sounds like—hack IoT devices in order to shut down air conditioning services.
- A *rolling code* attack sniffs the code used by your key fob to unlock (and in some cases) start your car. A *BlueBorne* attack is basically an amalgamation of techniques and attacks against known, already existing Bluetooth vulnerabilities.
- Ransomware, side channel, man in the middle (MITM), and so on all still apply to IoT as they do everywhere else. IoT devices can also fall prey to malware. Mirai malware purposefully looks for and interjects itself onto IoT devices. After successful infiltration, it basically propagates and creates gigantic botnets—with the primary purpose of DDoS attacks thereafter.

IoT Hacking Methodology

- The first phase in IoT hacking methodology is information gathering—reconnaissance and footprinting for IoT devices.
- Shodan (https://www.shodan.io/) is often referred to as the search engine for *everything*. While Google and other search engines index the Web, Shodan indexes anything and everything imaginable that is, or once was (and many times probably shouldn't be) plugged into the Internet. Common Shodan search filters include *city, hostname, geo, port,* and *net.*
- Shodan requires a registration, but is free to use. It is highly recommended you take great pains to obscure your identity as much as possible before signing up and using it. For example, you might consider loading TOR on a USB, use that connection to create a fake e-mail account, and register with that.
- Some of the other tools to assist in information gathering are Censys (https://censys.io) and Thingful (www.thingful.net).

- The second phase in IoT hacking methodology is vulnerability scanning. There are several vulnerability scanners and assessment tools for IoT devices, including RIoT Vulnerability Scanner (https://www.beyondtrust.com/resources/data-sheet/retina-iot-riot-scanner/), beSTORM (https://www.beyondsecurity.com/bestorm.html), IoTsploit (https://iotsploit.com), and IoT Inspector (www.iot-inspector.com).
- The third phase in the methodology is launching attacks. Tools include Firmalyzer (https://firmalyzer.com, for performing active security assessments on IoT devices), KillerBee (https://github.com), JTAGulator (www.grandideastudio.com), and Attify Zigbee Framework (https://www.attify.com, providing a suite of tools for testing Zigbee devices).
- The last two phases in IoT hacking methodology are gaining access and maintaining access. Telnet is often leveraged in IoT devices and provides a rather easy means to gain access. Foren6 (http://cetic.github.io/foren6/) is a sniffer specially for IoT traffic.

Chapter 9 Security in Cloud Computing

Cloud computing is one of those terms thrown around a lot these days, yet not many people actually understand what it means. EC-Council added a brand-new chapter on the subject in their official courseware, and you can rest assured it will receive more and more attention on the exam as time passes. The information covered on the exam is sure to change over time, as this is a new focus area for ECC. EC-Council tends to focus on lists, categories, and in-the-weeds specificity in other topics, and cloud computing will be no different. Know the types and deployment models very well, and completely memorize NIST's reference architecture on cloud. Most of the attacks and threats in cloud computing are similar to everything else, but a couple are very specific, and those will likely find their way onto your exam. Lastly, there aren't a whole lot of cloud-specific tools to know, but you will definitely need to be familiar with them.

Cloud Computing Essentials

- Virtualization is the effort to run multiple operating systems on the same physical device simultaneously. Several virtual machine (VM) offerings are available, making use of a hypervisor (such as VMware, Oracle VirtualBox, Xen, or KVM) to create, manage, and run virtual machines on the host.
- There are three major types of cloud computing models: IaaS, PaaS, and SaaS.
- *Infrastructure as a Service (IaaS)* provides virtualized computing resources over the Internet. A third-party provider hosts infrastructure components, applications, and services on behalf of its subscribers, with a hypervisor running the virtual machines as guests. Collections of hypervisors within the cloud provider exponentially increase the virtualized resources available and provide scalability of service to subscribers. IaaS is a good choice for day-to-day infrastructure

service, as well as for temporary or experimental workloads that may change unexpectedly. IaaS subscribers typically pay on a per-use basis.

- *Platform as a Service (PaaS)* is geared toward software development, providing a development platform that allows subscribers to develop applications without building the infrastructure it would normally take to develop and launch software. PaaS doesn't usually replace an organization's actual infrastructure—instead it just offers key services the organization may not have onsite.
- *Software as a Service (SaaS)* is simply a software distribution model—the provider offers on-demand applications to subscribers over the Internet. SaaS benefits include easier administration, automated patch management, compatibility, and version control.
- There are four main deployment models for cloud: public, private, community, and hybrid.
- A *public cloud* model is one where services are provided over a network that is open for public use (like the Internet). Public cloud is generally used when security and compliance requirements found in large organizations isn't a major issue.
- A *private cloud* model is operated solely for a single organization (a.k.a. single-tenant environment) and is usually not a pay-as-you-go operation. Private clouds are usually preferred by larger organizations, because the hardware is dedicated and security and compliance requirements can be more easily met.
- A *community cloud* model is one where the infrastructure is shared by several organizations, usually with the same policy and compliance considerations.
- The *hybrid cloud* model is a composition of two or more cloud deployment models.

Cloud Regulatory Bodies

- NIST (National Institutes of Standards and Technology) *Special Publication 500-292: NIST Cloud Computing Reference Architecture* provides a fundamental reference point to describe an overall framework that can be used government wide. There are five major roles within NIST Cloud Architecture: Cloud carrier (the organization that has the responsibility of transferring the data; the intermediary for connectivity and transport between subscriber and provider), Cloud consumer (the individual or organization that acquires and uses cloud products and services), Cloud provider (the 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), and Cloud auditor (the independent assessor of cloud service and security controls).
- FedRAMP (https://www.fedramp.gov/) is the most recognized and referenced regulatory effort regarding cloud computing. The Federal Risk and Authorization Management Program is a government-wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services.

- PCI Data Security Standard (PCI DSS) Cloud Special Interest Group offers cloud computing guidelines as well (https://www.pcisecuritystandards.org/pdfs/PCI_DSS_v2_Cloud_Guidelines.pdf)
- Cloud Security Alliance (CSA) is the leading professional organization devoted to promoting cloud security best practices and organizing cloud security professionals.

Cloud Security and Tools

- *Trusted computing* refers to an attempt to resolve computer security problems through hardware enhancements and associated software modifications. The Trusted Computing Group (TCG) is made up of a bunch of hardware and software providers who cooperate to come up with specific plans. *Roots of Trust (RoT)* is a set of functions within the trusted computing module that are always trusted by the computer's operating system (OS).
- Core's CloudInspect is a tool that offers penetration testing as a service from Amazon Web Services for EC2 users (https://www.coresecurity.com/corelabs-research/projects/core-cloudinspect). It's designed for AWS cloud subscribers and runs as an automated, all-in-one testing suite specifically for their cloud subscription.
- CloudPassage's Halo provides instant visibility and continuous protection for servers in any combination of data centers, private clouds, and public clouds (https://www.cloudpassage.com/products/).
- 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. It's designed to allow software components to deliver information directly to other components over a network.
- Two specific cloud attacks mentioned by ECC include session riding and side channel. *Session riding* is, in effect, simply CSRF under a different name and deals with cloud services instead of traditional data centers. Side channel attacks, also known as *cross-guest VM breach,* deal 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, he may be able to pull off lots of malicious activities).

Chapter 10 Trojans and Other Attacks

Don't overlook the "seedier" side of hacking in your pen testing efforts. You'll be tested on viruses, worms, and all sorts of malware on the exam. Learn what they are and what you can do to stop their influence in the world.

Malware Attacks

- A *Trojan* is software that appears to perform a desirable function for the user prior to running or installing but instead performs a function, usually without the user's knowledge, that steals information or otherwise harms the system (or data).
- A worm does not require human intervention to spread.
- *Overt channels* are legitimate communication channels used by programs across a system or a network (the communication channel is being used in the method it was designed for), whereas *covert channels* are used to transport data in ways they were not intended.
- *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 is a tool used for wrapping Trojans.
- *Crypters* are software tools that use a combination of encryption and code manipulation to render malware undetectable to AV and other security monitoring products.
- *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.
- There are several Trojan types, including command shell, GUI (MoSucker, BioDox), e-mail (remotbyMail), defacement (Restorator), botnet, FTP (TinyFTP), VNC, and remote access (RAT, Apocalypse, netcat).
- Windows will automatically run everything located in Run, RunServices, RunOnce, and RunServicesOnce, and you'll find most questions center around, or show you, settings from HKEY_LOCAL_MACHINE.
- *Netcat* is a remote access tool sometimes classified as malware that is known as the "Swiss Army knife" of TCP/IP hacking. Netcat provides a lot of control over a remote shell on a target. When installed and executed on a remote machine, it opens a listening port of your choice. For example, *nc -l -p 5555* opens port 5555 in a listening state on the target machine, and typing **nc IPAddress -p 5555** on a separate machine would open a raw "Telnet-like" connection.
- Netcat can be 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 even use it as a port scanner.
- Here are some default malware port numbers for memorization: TCP Wrappers (421), Doom (666), Snipernet (667), Tini (7777), WinHole (1080–81), RAT (1095, 1097–98), SpySender (1807), Deep Throat (2140, 3150), NetBus (12345, 12346), Whack a Mole (12362, 12363), and BackOrifice (31337, 31338).

- Netstat is a built-in command on Windows machines useful for identifying running processes and open ports on a machine. A *netstat -an* command will show all connections and listening ports in numerical form.

Virus Types and Other Attacks

- A *boot sector virus* (also known as a *system virus*) actually moves the boot sector to another location on the hard drive, forcing the virus code to be executed first. It's almost impossible to get rid of once you get infected.
- Working just like the boot sector virus, a *shell virus* wraps itself around an application's code, inserting its own code before the application's code. Every time the application is run, the virus code is run first.
- A *multipartite virus* attempts to infect both files and the boot sector at the same time.
- A *macro virus*—usually written with Visual Basic for Applications (VBA)—infects template files created by Microsoft Office (normally Word and Excel). The Melissa virus was a prime example of this.
- A *polymorphic code 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.
- A *metamorphic virus* rewrites itself every time it infects a new file.
- *Ransomware* is a malware type that locks you out of your own system resources and demands an online payment of some sort in order to release them back to you. Usually the payment is smaller than the cost it would take to remove the malware and recover anything lost. The ransomware "family" includes examples such as Cryptorbit, CryptoLocker, CryptoDefense, and police-themed.
- *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.
- *Sparse infector virus* only infects occasionally. For example, maybe the virus only fires every tenth time a specific application is run.
- Windows will automatically run everything located in Run, RunServices, RunOnce, and RunServicesOnce, and you'll find that most questions on the exam are centered around or show you settings from HKEY_LOCAL_MACHINE.
- The distributed denial-of-service (DDoS) attack comes not from one system but many—and it's usually part of a botnet. A *botnet* is a network of zombie computers the hacker can use to start a distributed attack from (examples of botnet software/Trojans are Shark and Poison Ivy). These systems can sit idly by doing other work for months before being called into action.
- Normally the preferred communication channel used to signal the bots is Internet Relay Chat (IRC) or Internet Chat Query (ICQ).

DoS Attack Types

- **SYN attack** The hacker will send 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 (because the address is false). Eventually, all the machine's resources are engaged, and it becomes a giant paperweight.
- **SYN flood** In this attack, the hacker sends thousands of SYN packets to the target but never responds to any of the return SYN/ACK packets. Because 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 connections available.
- **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 eventually reaches a limit of packets per second sent.
- **Application level** This is a simple attack whereby the hacker simply sends more "legitimate" traffic to a web application than it can handle, causing the system to crash.
- **Smurf** The attacker sends a large amount 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, thus exhausting the resources there. A *fraggle* attack is similar but uses UDP for the same purpose.
- **Ping of Death** This isn't a valid attack with modern systems but is still a definition you may need to know. In the Ping of Death, an attacker fragments an ICMP message to send to a target. When the fragments are reassembled, the resulting ICMP packet is larger than the maximum size and crashes the system.
- **Distributed reflection denial-of-service (DRDoS)** Also known as a *spoof attack,* it uses multiple intermediary machines to pull off the denial of service, by having the secondary machines send the attack at the behest of the attacker. The attacker remains hidden because the attacks appear to originate from those secondary machines.

Session Hijacking

- In session hijacking, the attacker waits for the session to initialize between two parties and then interjects himself in the middle, knocking one party offline while the other continues to function and communicate normally—none the wiser.
- A key note to remember for testing purposes is how hijacking differs from spoofing. In *spoofing,* you're pretending to be someone else's address with the intent of sniffing their traffic while they work. *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.

- TCP session hijacking requires the attacker to monitor the sequence numbers of a communications session, disrupt the session with a RST or FIN packet (to one side), and then interject packets with predicted sequence numbers in order to pick up the communication channel in use. The sequence numbers must be guessed properly or the attack won't work.
- You will see sequence number prediction on a couple of exam questions. The sequence number comes from the following: An acknowledgment packet will recognize the agreed-upon sequence number and then acknowledge receipt of the previous packet by incrementing the acknowledgment number with the packet size of the receipt. For example, if the agreed-upon sequence number is 500 and a packet is received showing Seq=500, Ack=1448, then the response packet should show the sequence number as 500 and the acknowledgment as 1948 (500 + 1448).
- Other questions will interject window size in sequence prediction. For example, an acknowledgment of 105 with a window size of 200 means you could expect sequence numbering from 105 through 305.
- Ettercap, Hunt, and T-sight are probably the best-known session hijacking tools. Some other tools include Paros (more known as a proxy), BurpSuite, Juggernaut (a well-known Linux-based tool), Hamster, and Ferret.
- A man-in-browser (MIB) attack occurs when the hacker sends a Trojan to intercept browser calls. It basically sits between the browser and libraries, allowing a hacker to watch, and interact within, a browser session.
- Using unpredictable sequence numbers is a good defense against session hijacking.

Chapter 11 Cryptography 101

Cryptography is the science or study of protecting information, whether in transit or at rest, by using techniques to render the information unusable to anyone who does not possess the means to decrypt it. *Cryptanalysis* is the study and methods taken to crack encrypted communications and is the focus for most ethical hackers.

Encryption Overview

- *Plain text* refers to the data in its readable, open state. *Cipher text* refers to the data after it has been encrypted and is in an unreadable state.
- *Nonrepudiation* is the means by which a recipient can ensure the identity of the sender and that neither party can deny having sent or received the message.
- *Stream ciphers* encrypt data as a continuous stream of bits (one by one). Stream ciphers are very fast.
- *Block ciphers* split the data into blocks (usually 64 bits at a time) and encrypt each block. They are simpler and slower than stream. Most algorithms covered on the exam will be block ciphers.

- An XOR operation requires two inputs to generate an outcome: if the bits match, the output is a 0; if they don't, it's a 1.
- *Symmetric encryption,* also known as *single key* or *shared key,* uses a single key for both encryption and decryption. Symmetric is fast and a good choice for bulk encryption but does not scale well.
- The formula for determining the number of keys required in a symmetric system is

  $N(N-1)/2)$

  where N represents the number of hosts involved.
- *Asymmetric encryption* uses one key for encryption and another for decryption. It provides both confidentiality and nonrepudiation and solves the problems of key distribution and scalability. However, it is slower and uses more processing power.
- IPSec is used to secure IP communication by providing encryption and authentication services to each packet, and 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 used in network address translation (NAT) because the original packet is still routed in exactly the same manner as it would have been without IPSec. *Tunnel mode*, however, encrypts the whole thing, encapsulating the entire original packet in a new IPSec shell. This makes it incompatible with NAT.
- IPSec architecture includes the following protocols: *Authentication Header* (a protocol within IPSec that guarantees the integrity and authentication of the IP packet sender), *Encapsulating Security Payload* (a protocol that also provides origin authenticity and integrity, but it can take care of confidentiality as well; 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* (the protocol that produces the keys for the encryption process), *Oakley* (a protocol that uses Diffie-Hellman to create master and session keys), and *Internet Security Association Key Management Protocol* (software that facilitates encrypted communication between two endpoints).

Symmetric Encryption Algorithms

- *DES* is a block cipher that uses a 56-bit key (with 8 bits reserved for parity). Because of the small key size, this encryption standard became quickly outdated and is not considered a very secure encryption algorithm.
- *3DES* is 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 much more effective than DES but is much slower.
- *Advanced Encryption Standard (AES)* is a block cipher that uses a key length of 128, 192, or 256 bits and effectively replaces DES. It is much faster than DES or 3DES.

- *International Data Encryption Algorithm (IDEA)* is a block cipher that uses a 128-bit key and was also designed to replace DES. Originally used in Pretty Good Privacy (PGP) 2.0, IDEA was patented and used mainly in Europe.
- *Twofish* is a block cipher that uses a key size up to 256 bits.
- *Blowfish* is 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.
- *Rivest Cipher (RC)* encompasses several versions, from RC2 through RC6. It's a block cipher that uses a variable key length up to 2040 bits. RC6, the latest version, uses 128-bit blocks, whereas RC5 uses variable block sizes (32, 64, or 128).

Asymmetric Encryption Algorithms

- The *public* key is used for encryption. The *private* key is used for decryption.
- *Diffie-Hellman* was developed for use as a key exchange protocol and 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.
- *Elliptic Curve Cryptosystem (ECC)* uses points on an elliptical curve, in conjunction with logarithmic problems, for encryption and signatures. It uses less processing power than other methods, making it a good choice for mobile devices.
- *El Gamal,* which is not based on prime number factoring, uses the solving of discrete logarithm problems for encryption and digital signatures.
- *RSA* is an algorithm that achieves strong encryption through the use of two large prime numbers. Factoring these numbers creates key sizes up to 4096 bits. RSA can be used for encryption and digital signatures and is the modern de facto standard.

Hash Algorithms

- A hashing algorithm is 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.
- Hashes are generally used as an integrity check and do *not* encrypt data.
- *MD5 (Message Digest algorithm)* produces a 128-bit hash value output, expressed as a 32-digit hexadecimal. Serious flaws in the algorithm, and the advancement of other hashes, have resulted in this hash being rendered obsolete (U.S. CERT, August 2010).
- *SHA-1* was developed by the National Security Agency (NSA). It produces 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 after the year 2010 (see FIPS PUB 180-1).

- *SHA-2* actually holds four separate hash functions that produce outputs of 224, 256, 384, and 512 bits.
- *SHA-3* 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).
- A *hash collision* occurs when two or more files create the same output.

Steganography

- *Steganography* is the practice of concealing a message inside another medium (such as another file or an image) in such a way that only the sender and recipient even know of its existence.
- There are a few ways to 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.
- *Snow* is a steganography tool used to conceal messages in ASCII text by appending whitespace to the end of lines.
- *GifShuffle* is a steganography tool used to conceal messages in GIF images by shuffling bits in the color map.

Public Key Infrastructure (PKI)

- There are three *trust models* for a PKI system: *Web of trust* has multiple entities sign certificates for one another (users within this system 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 certs (users trust each other based on the CA itself), and *hierarchical trust system* has a CA at the top (root CA) but makes use of one or more intermediate CAs underneath it (known as RAs) to issue and manage certificates.
- A *digital certificate* is an electronic file that is used to verify a user's identity, providing nonrepudiation throughout the system.
- The *X.509 standard* defines what should and should not be in a digital certificate. Standard certificates include the following fields: Version, Serial Number, Subject, Algorithm ID (or Signature Algorithm), Issuer, Valid From and Valid To, Key Usage, Subject's Public Key, and Optional.
- A *digital signature* is an algorithmic output designed to ensure the authenticity (and integrity) of the sender. Digital signatures are encrypted with the user's *private* key.

Encrypted Communication

- Protocols providing encrypted communication include Secure Shell (SSH), Secure Sockets Layer (SSL), Transport Layer Security (TLS), Internet Protocol Security (IPSec), and Point-to-Point Tunneling Protocol (PPTP).
- Data at Rest (DAR) is encryption designed to protect against loss or theft or data in a resting state (data that is in a stored state and not currently accessible). This full disk encryption (FDE) uses pre-boot authentication (usually an account and password) to "unlock" the drive before the system can even boot up.
- SSH uses TCP port 22 and is an encrypted version of Telnet (port 23).
- SSL has six steps: (1) Client hello, (2) server hello and certificate, (3) server hello done message, (4) client verifies server identity and sends client key exchange message, (5) client sends change cipher spec and finish message, and (6) server responds with change cipher spec and finish message. The session key is created by the client after it verifies the server identity (using the certificate provided in step 2).
- Pretty Good Privacy (PGP) is used for signing, compression, and encrypting and decrypting e-mails, files, directories, and even whole disk partitions, mainly in an effort to increase the security of e-mail communications. PGP follows the OpenPGP standard (RFC 4880) for encrypting and decrypting data.

Encrypted Communication Attacks

- **Known plain-text attack** Attackers scan plain-text copies for repeatable sequences, which are then compared to the corresponding cipher-text versions. Over time, and with effort, this can be used to decipher the key.
- **Chosen plain-text attack** This is a variant of known plain text where the attacker encrypts multiple plain-text copies in order to gain the key.
- **Cipher text-only attack** Attackers gain copies of several messages encrypted in the same way (with the same algorithm). Statistical analysis can then be used to reveal, eventually, repeating code, which can be used to decode messages later.
- **Chosen-cipher attack** This is a variant of cipher text-only where the same process is followed (statistical analysis without a plain text version for comparison), but it's only for portions of gained cipher text.
- **Replay attack** Most often performed within the context of a man-in-the-middle attack, a replay attack repeats a portion of a cryptographic exchange in hopes of fooling the system into setting up a communication channel. Session tokens can be used in the communication process to combat this attack.
- **Inference attack** *Inference* means you can derive information from the cipher text without actually decoding it. For example, if you are monitoring the encrypted line a shipping company uses and the traffic suddenly increases, you could assume the company is getting ready for a big delivery.

- **Heartbleed** Heartbleed exploits the heartbeat feature in OpenSSL: During an open session to verify that data was received correctly, Open SSL echoes data back to the other system. Basically, one system tells the other "I received what you sent and it's all good. Go ahead and send more." In Heartbleed, an attacker sends a single byte of data while telling the server it sent 64Kb of data. The server will then send back 64Kb of data—64Kb of random data from its memory. Open SSL versions 1.0.1 and *1.0.1f* are vulnerable to Heartbleed.
- Factoring Attack on RSA-EXPORT Keys (FREAK) is a man-in-the-middle attack that forces a downgrade of an RSA key to a weaker length. The attacker forces the use of a weaker encryption key length, enabling successful brute-force attacks.
- POODLE (Padding Oracle On Downgraded Legacy Encryption) exploits the handshake feature in TLS that attempts to downgrade encryption down to SSL 3.0 for backwards compatibility with clients.
- DROWN (Decrypting RSA with Obsolete and Weakened eNcryption) is a serious vulnerability that affects HTTPS and other services that rely on SSL and TLS (essential cryptographic protocols for Internet security).

Chapter 12 Low Tech: Social Engineering and Physical Security

Users are the weakest link in your security chain, and social engineering is one of the best methods of hacking available to you as a pen tester. Social engineering is the art of manipulating a person, or a group of people, into providing information or a service they otherwise would never have given. Social engineers prey on people's natural desire to help one another, listen to authority, and trust of offices and entities. Physical security involves the plans, procedures, and steps taken to protect your assets from deliberate or accidental events that could cause damage or loss.

Human-Based Social Engineering Attacks

- The three types of social engineering attacks are human based, computer based, and mobile based. Human-based social engineering uses interaction in conversation or some other circumstance between people to gather useful information. Computer-based social engineering makes use of tools and techniques on a system to accomplish the goal. Mobile based uses mobile devices.
- *Dumpster diving* is a human-based attack whereby the attacker rifles through refuse, dumpsters, paper recycling bins, and office trash cans for useful information target users may have thrown away inadvertently.
- *Impersonation* is a human-based attack where the social engineer pretends to be an employee, a valid user, or even an executive (or other V.I.P.).
- *Technical support* is a human-based attack aimed at the technical support staff themselves. The attacker calls and poses as a user needing assistance.

- *Shoulder surfing* is a human-based attack whereby the attacker looks over the shoulder of the user to see their onscreen activity. Shoulder surfing can also be done "long distance," using telescopes and binoculars (referred to as *surveillance* in the real world).
- *Tailgating* is a human-based attack where an attacker has a fake badge and simply follows an authorized person through the opened security door.
- *Piggybacking* is a human-based attack where the attacker doesn't have a badge but asks for someone to let them in anyway. An authorized user holds the door open for them despite not having a badge visible.
- Potential targets for social engineering are known as Rebecca or Jessica. During communications with other attackers, these terms can provide information on whom to target. For example, "Rebecca, the receptionist, was very pleasant and easy to work with."
- In a *reverse social engineering* attack, the attacker will pose as someone in a position of authority or as technical support and set up a scenario whereby the user feels they must dial in for support. Three steps are taken in the attack: advertisement, sabotage, and support.
- Using a phone during a social engineering effort is known as "vishing" (short for *voice phishing*).

Computer-Based Social Engineering Attacks

- Computer-based attacks are those attacks carried out with the use of a computer or other data-processing device. Examples include specially crafted pop-up windows, SMS texts, spoofing entire websites, wireless access points, and a host of other entry points.
- A *phishing* attack is an e-mail crafted to appear legitimate but in fact contains links to fake websites or to download malicious content. The links contained within the e-mail lead the user to a fake web form in which information entered is saved for the hacker's use.
- Some indicators of a phishing e-mail include unknown, unexpected, or suspicious originators (if you don't know the person or entity sending the e-mail, it should be looked at suspiciously), vague addresses in the greeting line, bad spelling or grammar, and closely worded links (hover over a link to see its true destination).
- *Spear phishing* is a targeted attack against an individual or a small group of individuals within an organization. Spear phishing usually is a result of a little reconnaissance work that has churned up some useful information.
- *Sign-in seal* is an e-mail protection method in use at a variety of business locations. The practice is to use a secret message or image that can be referenced on any official communication with the site. If you receive an e-mail purportedly from the business but it does not include the sign-in seal image or message, you're aware it's a probably phishing attempt.

- The Netcraft Toolbar and the PhishTank Toolbar can help in identifying risky sites and phishing behavior.
- Fake AV or rogue security pop-ups will definitely be tested. The idea is a pop up or an e-mail that purports to have found multiple security infections on the system, and if the user would just "click here," they'd be cleaned off. Of course, clicking the link leads to malware and redirection.

Mobile Attacks

- **Publishing malicious applications** An attacker creates an app that looks like, acts like, and is named similarly to a legitimate application.
- **Repackaging legitimate applications** An 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** This one actually 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, infecting their mobile device.
- **SMS** An attacker sends SMS text messages crafted to appear as legitimate security notifications, with a phone number provided. The user unwittingly calls the number and provides sensitive data in response.

Physical Security

- Physical security measures come down to three major components: physical, technical, and operational. *Physical measures* include all the things you can touch, taste, smell, or get shocked by (lighting, locks, fences, and guards), *technical measures* are measures taken with technology in mind to protect explicitly at the physical level (smartcards and biometrics), and *operational measures* are the policies and procedures you set up to enforce a security-minded operation (background checks on employees, risk assessments on devices, and policies regarding key management and storage).
- Access controls are physical measures designed to prevent access to controlled areas. They include biometric controls, identification/entry cards, door locks, and man traps.
- Biometrics includes the measures taken for authentication that come from the "something you are" tenant. Biometrics can include fingerprint readers, face scanners, retina scanners, and voice recognition.

- Biometric systems are measured by two main factors. The first, *false rejection rate (FRR)*, is the percentage of time a biometric reader will deny access to a legitimate user. The percentage of time that an *unauthorized* user is granted access by the system, known as *false acceptance rate (FAR)*, is the second major factor. These are usually graphed on a chart, and the intercepting mark, known as *crossover error rate (CER)*, becomes a ranking method to determine how well the system functions overall (the lower the CER, the better the system).
- A *man trap* uses two doors to create a small space to hold a person until appropriate authentication has occurred. The user enters through the first door, which must shut and lock before the second door can be cleared. Once inside the enclosed room, which normally has clear walls, the user must authenticate through some means—biometric, token with PIN, password, and so on—to open the second door. Failure to authenticate "traps" the intruder.

Chapter 13 The Pen Test: Putting It All Together

This section is almost a catchall for the remainder of the information you need for the exam. Most of it is pure memorization, with some really crazy definitions involved.

Security Assessments

- A *security assessment* is any test that is performed in order to assess the level of security on a network or system. The security assessment can be one of two categories: a security audit (otherwise known as a *vulnerability assessment*) or a penetration test.
- A *security audit* (vulnerability scan) tests a system or network for existing vulnerabilities but does not intentionally exploit any of them. This vulnerability assessment is designed to uncover potential security holes in the system and report them to the client for their action. Penetration tests do exploit vulnerabilities—within the confines of an agreed-upon scope.
- Pen tests can be *external* (analyzing publicly available information and conducting network scanning, enumeration, and testing from the network perimeter—usually from the Internet) or *internal* (performed from within the organization, from various network access points).
- *Black-box testing* occurs when the attacker has no prior knowledge of the infrastructure at all (takes the longest to accomplish and simulates a true outside hacker). *White-box testing* simulates an internal user who has complete knowledge of the company's infrastructure (designed to simulate an internal system administrator–level attack). *Gray-box testing* provides limited information on the infrastructure.

- Automated pen test tools include Core Impact, Metasploit, and Canvas. Automated tools are designed to save time and money for an organization; however, they are susceptible to false positives and false negatives, don't necessarily care what your agreed-upon scope says is your stopping point, and don't provide as much clear information as a true pen test.
- Shellshock (a.k.a. Bashdoor, Bash Bug, and CVE-2014-6271) is a security vulnerability that affected the Unix Bash shell found in most versions of Linux and Unix operating systems, including Mac OS X. Bash can also be used to run commands passed to it by applications, and if a command is entered to set an environment variable (a dynamic, named value affecting the way a process is run), then an attacker could tack on malicious code that would run when the variable was received.
- *Meterpreter* is a Metasploit payload type that operates via DLL injection and is difficult for antivirus software to pick up. Inline payloads are single payloads that contain the full exploit and shell code for the designed task (may be more stable, but they're easier to detect). Staged payloads establish a connection between the attacking machine and the victim (then reading in a payload to execute on the remote machine).
- *Metasploit* is an open source framework designed in a modular fashion, with each library and component responsible for its own function. The most fundamental piece of the architecture is the *Rex (Ruby Extension)* library: It includes a wrapper socket subsystem, implementations of protocol clients and servers, a logging subsystem, exploitation utility classes, and a number of other useful classes. Rex provides critical services to the entire framework. *MSF Core* is responsible for implementing all of the required interfaces that allow for interacting with exploit modules, sessions, and plug-ins (it interfaces directly with Rex). *MSF Base* is designed to provide simpler wrapper routines for dealing with the framework core and is an extension of the core. *MSF interfaces* are the means by which the user interacts with the framework (including console, CLI, Web, and GUI).
- EC-Council defines a pen test as having three phases: pre-attack, attack, and post-attack. Exam questions regarding these will attempt to confuse you with comparisons to the steps for an attack—don't get them confused.
- The *pre-attack phase* is where teams perform all reconnaissance and data-gathering efforts. Competitive intelligence, identifying network ranges, and checking network filters for open ports are all carried out here. Whois, DNS enumeration, finding the network IP address range, and nmap network scanning all occur here. Other tasks you might consider here include, but aren't limited to, testing proxy servers, checking for default firewall or other network-filtering device installations or configurations, and looking at any remote login allowances.

- In the *attack phase,* you attempt to penetrate the network perimeter, acquire your targets, execute attacks, and elevate privileges. Some activities include verifying ACLs; checking to see whether you can use any covert tunnels inside the organization; executing XSS, buffer overflows, and SQL injections; password cracking; and privilege escalation.
- The *post-attack phase* consists of two major steps. First, teams must clean up after their efforts, removing anything that has been uploaded to the organization's systems, including tools, malware, backdoors, or other attack software, as well as any files and folders left on systems. Registry changes must also revert to the original settings.
- The *red team* is the offense-minded group, simulating the bad guys in the world, actively attacking and exploiting everything they can find in your environment. In a traditional war game scenario, the red team is attacking black-box style, given little to no information to start things off.
- The *blue team* is defensive in nature. They're not out attacking things—rather, they're focused on shoring up defenses and making things safe. Unlike red teams, since blue teams are responsible for defense against the bad guys, they usually operate with full knowledge of the internal environment.

Deliverables

- The initial in-brief to management for a pen test is important. It provides an introduction of the team members and an overview of the original agreement, including which tests will be performed, which team members will be performing specific tasks, and the timeline for your test. Points of contact, phone numbers, and so on, should all be presented to the clients before testing begins.
- A comprehensive report is due to the customer at the conclusion of the pen test. It should include the following items: (1) an executive summary of the organization's overall security posture (if testing under the auspices of FISMA, DIACAP, HIPAA, or another standard, this will be tailored to the standard), (2) the names of all participants and the dates of all tests, (3) a list of findings, usually presented in order of highest risk, (4) an analysis of each finding, and (5) recommended mitigation steps (if available).

Additional Information to Remember

- A *suicide hacker* is an attacker who is so wrapped up in promoting their cause they do not care about the consequences of their actions—even if it means jail time. In some instances (I've seen this in practice test exams before), the suicide hacker even *wants* to be caught to serve as a martyr for the cause.

- An *unannounced test* occurs when the organization's IT staff is not made aware of the pen test team's activities in advance. An *announced test* means the opposite; the IT staff is ready and waiting.
- OSSTM (pronounced "awestem" per the developers) is a peer-reviewed manual of security testing and analysis that results in fact-based actions that can be taken by an organization to improve security. Downloadable as a single, although massive, PDF file, OSSTM tests legislative-, contractual-, and standards-based compliance.
- Open Web Application Security Project (OWASP) provides security information, including vulnerabilities and fixes, on web servers and applications for free (https://www.owasp.org/index.php/Main_Page).