**Fast Ethernet** An Ethernet networking system transmitting data at 100 million bits per second(Mbps), ten times the speed of an earlier Ethernet standard. Derived from the Ethernet 802.3 standard, it is also known as 100BaseT.

**Fiber Distributed Data Interface (FDDI)** LAN standard, defined by ANSI X3T9.5, specifying a 100-Mbps token-passing network using fiber-optic cable and a dual-ring architecture for redundancy, with transmission distances of up to 2 kilometers.

**File Allocation Table (FAT)** A computer file system architecture used in Windows, OS/2, and most memory cards.

**File Transfer Protocol (FTP)** An Application layer protocol, using TCP, for transporting files across an Internet connection. FTP transmits in clear text.

**filter** A set of rules defined to screen network packets based on source address, destination address, or protocol. These rules determine whether the packet will be forwarded or discarded.

**Finger** An early network application that provides information on users currently logged on to a machine.

**firewalking** The process of systematically testing each port on a firewall to map rules and determine accessible ports.

**firewall** Software or hardware components that restrict access between a protected network and the Internet, or between other sets of networks, to block unwanted use or attacks.

**flood** Traffic-passing technique used by bridges and switches in which traffic received on an interface is sent out all interfaces on the device except the interface on which the information was originally received. Traffic on a switch is flooded when it is broadcast in nature (intended for a broadcast address, as with ARP or other protocols) or if the switch does not have an entry in the CAM table for the destination MAC.

**footprinting** All measures and techniques taken to gather information about an intended target. Footprinting can be passive or active.

**forwarding** The process of sending a packet or frame toward the destination. In a switch, messages are forwarded only to the port to which they are addressed.

**fragmentation** Process of breaking a packet into smaller units when it is being transmitted over a network medium that’s unable to support a transmission unit the original size of the packet.

**FreeBSD** A free and popular version of the Unix operating system.

**fully qualified domain name (FQDN)** A fully qualified domain name consists of a host and domain name, including a top-level domain such as .com, .net, .mil, .edu, and so on.

**gap analysis** A tool that helps a company compare its actual performance with its potential performance.

**gateway** A device that provides access between two or more networks. Gateways are typically used to connect dissimilar networks.

**GET** A command used in HTTP and FTP to retrieve a file from a server.

**Government Access to Keys (GAK)** An attempt through key disclosure laws to have software companies provide copies of all keys to the government, which will be used only when a warrant is provided during law enforcement efforts.

**gray hat** A skilled hacker who straddles the line between white hat (hacking only with permission and within guidelines) and black hat (malicious hacking for personal gain). Gray hats sometime perform illegal acts to exploit technology with the intent of achieving better security.

**gray-box testing** A penetration test in which the ethical hacker has limited knowledge of the intended target(s). Designed to simulate an internal but non-system-administrator-level attack.

**hack value** The idea a hacker holds about the perceived worth or interest in attacking a target.

**hacktivism** The act or actions of a hacker to put forward a cause or a political agenda, to affect some societal change, or to shed light on something he feels to be a political injustice. These activities are usually illegal in nature.

**halo effect** A well-known and well-studied phenomenon of human nature, whereby a single trait influences the perception of other traits.

**hardware keystroke logger** A hardware device used to log keystrokes covertly. Hardware keystroke loggers are dangerous because they cannot be detected through regular software/anti-malware scanning.

**hash** A unique numerical string, created by a hashing algorithm on a given piece of data, used to verify data integrity. Generally hashes are used to verify the integrity of files after download (comparison to the hash value on the site before download) and/or to store password values.

**hashing algorithm** A one-way mathematical function that generates a fixed-length numerical string (hash) from a given data input. MD5 and SHA-1 are hashing algorithms.

**heuristic scanning** Method used by antivirus software to detect new, unknown viruses that have not yet been identified; based on a piece-by-piece examination of a program, *heuristic scanning* looks for a sequence or sequences of instructions that differentiate the virus from “normal” programs.

**HIDS** Host-based IDS. An IDS that resides on the host, protecting against file and folder manipulation and other host-based attacks and actions.

**Hierarchical File System (HFS)** A file system used by macOS.

**honeynet** A network deployed as a trap to detect, deflect, or deter unauthorized use of information systems.

**honeypot** A host designed to collect data on suspicious activity.

**hot site** A fully operational off-site data-processing facility equipped with hardware and system software to be used in the event of a disaster.

**HTTP tunneling** A firewall-evasion technique whereby packets are wrapped in HTTP, as a covert channel to the target.

**human-based social engineering** Using conversation or some other interaction between people to gather useful information.

**hybrid attack** An attack that combines a brute-force attack with a dictionary attack.

**hybrid cloud** A cloud model that is a composite of two or more cloud deployment models (public, private, or community).

**Hypertext Transfer Protocol (HTTP)** A communications protocol used for browsing the Internet.

**Hypertext Transfer Protocol Secure (HTTPS)** A hybrid of the HTTP and SSL/TLS protocols that provides encrypted communication and secure identification of a web server.

**IaaS** Infrastructure as a Service. A cloud computing type providing virtualized computing resources over the Internet.

**identity theft** A form of fraud in which someone pretends to be someone else by assuming that person’s identity, typically in order to access resources or obtain credit and other benefits in that person’s name.

**impersonation** A social engineering effort in which the attacker pretends to be an employee, a valid user, or even an executive to elicit information or access.

**inference attack** An attack in which the hacker can derive information from the cipher text without actually decoding it. Sensitive information can be considered compromised if an adversary can infer its real value with a high level of confidence.

**information technology (IT) asset criticality** The level of importance assigned to an IT asset.

**information technology (IT) asset valuation** The monetary value assigned to an IT asset.

**information technology (IT) infrastructure** The combination of all IT assets, resources, components, and systems.

**information technology (IT) security architecture and framework** A document describing information security guidelines, policies, procedures, and standards.

**Information Technology Security Evaluation Criteria (ITSEC)** A structured set of criteria for evaluating computer security within products and systems produced by European countries; it has been largely replaced by the Common Criteria.

**infrastructure mode** A wireless networking mode where all clients connect to the wireless network through a central access point.

**initial sequence number (ISN)** A number assigned during TCP startup sessions that tracks how much information has been moved. This number is used by hackers when hijacking sessions.

**insider affiliate** A spouse, friend, or client of an employee who uses the employee’s credentials to gain physical or logical access to organizational resources.

**insider associate** A person with limited authorized access to the organization; contractors, guards, and cleaning services are all examples.

**Institute of Electrical and Electronics Engineers (IEEE)** An organization composed of engineers, scientists, and students who issue standards related to electrical, electronic, and computer engineering.

**integrity** The security property that data is not modified in an unauthorized and undetected manner. Also, this is the principle of taking measures to ensure that data received is in the same condition and state as when it was originally transmitted.

**Interior Gateway Protocol (IGP)** An Internet routing protocol used to exchange routing information within an autonomous system.

**International Organization for Standardization (ISO)** An international organization composed of national standards bodies from more than 75 countries. ISO developed the OSI reference model.

**Internet Assigned Number Authority (IANA)** The organization that governs the Internet’s top-level domains, IP address allocation, and port number assignments.

**Internet Control Message Protocol (ICMP)** A protocol used to pass control and error messages between nodes on the Internet.

**Internet of Things (IoT)** The collection of devices using sensors, software, storage, and electronics to collect, analyze, store, and share data among themselves or to a user, with or without human intervention or action.

**Internet Protocol (IP)** A protocol for transporting data packets across a packet-switched internetwork (such as the Internet). IP is a routed protocol.

**Internet Protocol Security (IPSec) architecture** A suite of protocols used for securing Internet Protocol (IP) communications by authenticating and encrypting each IP packet of a communication session. This suite includes protocols for establishing mutual authentication between agents at session establishment and for negotiating the cryptographic keys to be used throughout the session.

**Internet service provider (ISP)** A business, government agency, or educational institution thatprovides access to the Internet.

**intranet** A self-contained network with a limited number of participants who extend limited trust to one another in order to accomplish an agreed-upon goal.

**intrusion detection system (IDS)** A security tool designed to protect a system or network against attacks by comparing traffic patterns against a list of both known attack signatures and general characteristics of how attacks may be carried out. Threats are rated and reported.

**intrusion prevention system (IPS)** A security tool designed to protect a system or network against attacks by comparing traffic patterns against a list of both known attack signatures and general characteristics of how attacks may be carried out. Threats are rated and protective measures taken to prevent the more significant threats.

**IoT Gateway** A device designed to send collected data from IoT devices to the user or to data storage (the cloud) for use later.

**iris scanner** A biometric device that uses pattern-recognition techniques based on images of the irises of an individual’s eyes.

**ISO 17799** A standard that provides best-practice recommendations on information security management for use by those responsible for initiating, implementing, or maintaining Information Security Management Systems (ISMS). Information security is defined within the standard in the context of the CIA triad.

**Kerberos** A widely used authentication protocol developed at the Massachusetts Institute of Technology (MIT). Kerberos authentication uses tickets, a ticket granting service, and a key distribution center.

**key exchange protocol** A method in cryptography by which cryptographic keys are exchanged between users, thus allowing use of a cryptographic algorithm (for example, the Diffie-Hellman key exchange).

**keylogger** A software application or hardware device that captures user keystrokes.

**last in first out (LIFO)** A programming principle whereby the last piece of data added to the stack is the first piece of data taken off.

**Level I assessment** An evaluation consisting of a document review, interviews, and demonstrations. No hands-on testing is performed.

**Level II assessment** An evaluation consisting of a document review, interviews, and demonstrations, as well as vulnerability scans and hands-on testing.

**Level III assessment** An evaluation in which testers attempt to penetrate the network.

**Lightweight Directory Access Protocol (LDAP)** An industry-standard protocol used for accessing and managing information within a directory service; an application protocol for querying and modifying data using directory services running over TCP/IP.

**limitation of liability and remedies** A legal limit on the amount of financial liability and remedies the organization is responsible for taking on.

**local area network (LAN)** A computer network confined to a relatively small area, such as a single building or campus.

**logic bomb** A piece of code intentionally inserted into a software system that will perform a malicious function when specified conditions are met at some future point.

**MAC filtering** A method of permitting only MAC addresses in a preapproved list of network access. Addresses not matching are blocked.

**macro virus** A virus written in a macro language and usually embedded in document or spreadsheet files.

**malicious code** Software or firmware intended to perform an unauthorized process that will have an adverse impact on the confidentiality, integrity, or availability of an information system. A virus, worm, Trojan horse, or other code-based entity that infects a host.

**malware** A program or piece of code inserted into a system, usually covertly, with the intent of compromising the confidentiality, integrity, or availability of the victim’s data, applications, or operating system. Malware consists of viruses, worms, and other malicious code.

**mandatory access control (MAC)** A means of restricting access to system resources based on the sensitivity (as represented by a label) of the information contained in the system resource and the formal authorization (that is, clearance) of users to access information of such sensitivity.

**man-in-the-middle attack** An attack where the hacker positions himself between the client and the server to intercept (and sometimes alter) data traveling between the two.

**mantrap** A small space having two sets of interlocking doors; the first set of doors must close before the second set opens. Typically authentication is required for each door, often using different factors. For example, a smartcard may open the first door, and a personal identification number entered on a number pad opens the second.

**master boot record infector** A virus designed to infect the master boot record.

**maximum tolerable downtime (MTD)** A measurement of the potential cost due to a particular asset being unavailable, used as a means to prioritize the recovery of assets should the worst occur.

**MD5** A hashing algorithm that results in a 128-bit output.

**Media Access Control (MAC)** A sublayer of Layer 2 of the OSI model, the Data Link layer. It provides addressing and channel access control mechanisms that enable several terminals or network nodes to communicate within a multipoint network.

**methodology** A documented process for a procedure designed to be consistent, repeatable, and accountable.

**minimum acceptable level of risk** An organization’s threshold for the seven areas of information security responsibility. This level is established based on the objectives for maintaining the confidentiality, integrity, and availability of the organization’s IT assets and infrastructure and will determine the resources expended for information security.

**multipartite virus** A computer virus that infects and spreads in multiple ways.

**Multipurpose Internet Mail Extensions (MIME)** An extensible mechanism for e-mail. A variety of MIME types exist for sending content such as audio, binary, or video using the Simple Mail Transfer Protocol (SMTP).

**National Security Agency (NSA) INFOSEC Assessment Methodology (IAM)** A systematic process for the assessment of security vulnerabilities.

**NetBSD** A free, open source version of the Berkeley Software Distribution of Unix, often used in embedded systems.

**NetBus** A software program for remotely controlling a Microsoft Windows computer system over a network. Generally it is considered malware.

**network access server** A device providing temporary, on-demand, point-to-point network access to users.

**Network Address Translation (NAT)** A technology where you advertise one IP address externally and data packets are rerouted to the appropriate IP address inside your network by a device providing translation services. In this way, IP addresses of machines on your internal network are hidden from external users.

**Network Basic Input/Output System (NetBIOS)** An API that provides services related to the OSI model’s Session layer, allowing applications on separate computers to communicate over a LAN.

**network interface card (NIC)** An adapter that provides the physical connection to send and receive data between the computer and the network media.

**network operations center (NOC)** One or more locations from which control is exercised over a computer, television broadcast, or telecommunications network.

**network tap** Any kind of connection that allows you to see all traffic passing by. Generally used in reference to a network-based IDS (NIDS) to monitor all traffic.

**Nmap** An open source scanning utility used to discover hosts and services on a network.

**node** A device on a network.

**nonrepudiation** The means by which a recipient of a message can ensure the identity of the sender and that neither party can deny having sent or received the message. The most common method is through digital certificates.

**NOP** A command that instructs the system processor to do nothing. Many overflow attacks involve stringing several NOP operations together (known as a NOP sled).

**nslookup** A network administration command-line tool available for many operating systems for querying the Domain Name System (DNS) to obtain domain name or IP address mappings or any other specific DNS record.

**NT LAN Manager (NTLM)** The default network authentication suite of protocols for Windows NT 4.0—retained in later versions for backward compatibility. NTLM is considered insecure and was replaced by NTLMv2.

**null session** An anonymous connection to an administrative share (IPC$) on a Windows machine. Null sessions allow for enumeration of Windows machines, among other attacks.

**open source** Describes practices in production and development that promote access to the end product’s source materials.

**Open Source Security Testing Methodology Manual (OSSTMM)** A peer-reviewed, formalized methodology of security testing and analysis.

**Open System Interconnection (OSI) reference model** A network architecture framework developed by ISO that describes the communications process between two systems across the Internet in seven distinct layers.

**OpenBSD** A Unix-like computer operating system descending from the BSD. OpenBSD includes a number of security features absent or optional in other operating systems.

**operating system attack** An attack that exploits the common mistake many people make when installing operating systems—that is, accepting and leaving all the defaults.

**out-of-band signaling** Transmission using channels or frequencies outside those normally used for data transfer; often used for error reporting.

**outsider associate** A untrusted outsider using open, or illicitly gained, access to an organization’s resources.

**overt channel** A communications path, such as the Internet, authorized for data transmission within a computer system or network.

**PaaS** Platform as a Service. A cloud computing type geared toward software development, providing a platform that allows subscribers to develop applications without building the infrastructure it would normally take to develop and launch software.

**packer** A crypter that uses compression to pack malware executables into smaller sizes to avoid detection.

**packet** A unit of information formatted according to specific protocols, generally regarded as being used in OSI Layer 3, that allows precise transmittal of data from one network node to another. Also called a *datagram* or *data packet,* a packet contains a header (container) and a payload (contents). Any IP message larger than 1500 bytes will be fragmented into packets for transmission.

**packet filtering** Controlling access to a network by analyzing the headers of incoming and outgoing packets and letting them pass or discarding them based on rule sets created by a network administrator. A packet filter allows or denies packets based on destination, source, and/or port.

**Packet Internet Groper (ping)** A utility that sends an ICMP Echo message to determine whether a specific IP address is accessible; if the message receives a reply, the address is reachable.

**parameter tampering** An attack where the hacker manipulates parameters within the URL string in hopes of modifying data.

**passive attack** An attack against an authentication protocol in which the attacker intercepts data in transit along the network between the claimant and verifier but does not alter the data (in other words, eavesdropping).

**Password Authentication Protocol (PAP)** A simple PPP authentication mechanism in which the user name and password are transmitted in clear text to prove identity. PAP compares the user name and password to a table listing authorized users.

**patch** A piece of software, provided by the vendor, intended to update or fix known, discovered problems in a computer program or its supporting data.

**pattern matching** The act of checking some sequence of tokens for the presence of the constituents of some pattern.

**payload** The contents of a packet. A system attack requires the attacker to deliver a malicious payload that is acted upon and executed by the system.

**Payment Card Industry Data Security Standard (PCI-DSS)** 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.

**penetration testing** A method of evaluating the security of a computer system or network by simulating an attack from a malicious source.

**personal identification number (PIN)** A secret, typically consisting of only decimal digits, that a claimant memorizes and uses to authenticate his identity.

**phishing** The use of deceptive computer-based means to trick individuals into disclosing sensitive personal information—usually via a carefully crafted e-mail message.

**physical security** Security measures, such as a locked door, perimeter fence, or security guard, to prevent or deter physical access to a facility, resource, or information stored on physical media.

**piggybacking** When an authorized person allows (intentionally or unintentionally) someone to pass through a secure door, despite the intruder not having a badge.

**ping sweep** The process of pinging each address within a subnet to map potential targets. Ping sweeps are unreliable and easily detectable but very fast.

**polymorphic virus** Malicious code that uses a polymorphic engine to mutate while keeping the original algorithm intact; the code changes itself each time it runs, but the function of the code will not change.

**Point-to-Point Protocol (PPP)** Provides router-to-router or host-to-network connections over asynchronous and synchronous circuits.

**Point-to-Point Tunneling Protocol (PPTP)** A VPN tunneling protocol with encryption. PPTP connects two nodes in a VPN by using one TCP port for negotiation and authentication and one IP protocol for data transfer.

**Port Address Translation (PAT)** A NAT method in which multiple internal hosts, using private IP addressing, can be mapped through a single public IP address using the session IDs and port numbers. An internal global IP address can support in excess of 65,000 concurrent TCP and UDP connections.

**port knocking** Another term for *firewalking*—the method of externally testing ports on a firewall by generating a connection attempt on each port, one by one.

**port redirection** The process of directing a protocol from one port to another.

**port scanning** The process of using an application to remotely identify open ports on a system (for example, whether systems allow connections through those ports).

**POST** An HTTP command to transmit text to a web server for processing. This is the opposite of an HTTP GET.

**Post Office Protocol 3 (POP3)** An Application layer protocol used by local e-mail clients to retrieve e-mail from a remote server over a TCP/IP connection.

**Presentation layer** Layer 6 of the OSI reference model. The Presentation layer ensures information sent by the Application layer of the sending system will be readable by the Application layer of the receiving system.

**Pretty Good Privacy (PGP)** A data encryption/decryption program often used for e-mail and file storage.

**private cloud** A cloud model operated solely for a single organization (a.k.a. single-tenant environment) and is usually not pay-as-you-go.

**private key** The secret portion of an asymmetric key pair typically used to decrypt or digitally sign data. The private key is never shared and is always used for decryption, with one notable exception: the private key is used to encrypt the digital signature.

**private network address** A nonroutable IP address range intended for use only within the confines of a single organization, falling within the predefined range of 10.0.0.0, 172.16–31.0.0, or 192.168.0.0.

**promiscuous mode** A configuration of a network card that makes the card pass all traffic it receives to the central processing unit rather than just frames addressed to it—a feature normally used for packet sniffing and bridged networking for hardware virtualization. Windows machines use WinPcap for this; Linux uses libcap.

**protocol** A formal set of rules describing data transmission, especially across a network. A protocol determines the type of error checking, the data compression method, how the sending device will indicate completion, how the receiving device will indicate the message was received, and so on.

**protocol stack** A set of related communications protocols operating together as a group to address communication at some or all of the seven layers of the OSI reference model.

**proxy server** A device set up to send a response on behalf of an end node to the requesting host. Proxies are generally used to obfuscate the host from the Internet.

**public cloud** A cloud model where services are provided over a network that is open for public use (such as the Internet).

**public key** The public portion of an asymmetric key pair typically used to encrypt data or verify signatures. Public keys are shared and are used to encrypt messages.

**public key infrastructure (PKI)** A set of hardware, software, people, policies, and procedures needed to create, manage, distribute, use, store, and revoke digital certificates.

**pure insider** An employee with all the rights and access associated with being employed by the company.

**purple team** A single team of security professionals who perform cooperative vulnerability and penetration assessments (CVPA).

**qualitative analysis** A nonnumerical, subjective risk evaluation. This is used with qualitative assessment (an evaluation of risk that results in ratings of none, low, medium, or high for the probability).

**quality of service (QoS)** A defined measure of service within a network system—administrators may assign a higher QoS to one host, segment, or type of traffic.

**quantitative risk assessment** Calculations of two components of risk (R): the magnitude of the potential loss (L), and the probability (P) that the loss will occur.

**queue** A backlog of packets stored in buffers and waiting to be forwarded over an interface.

**RAID (Redundant Array of Independent Disks)** Formerly *Redundant Array of Inexpensive Disks,* RAID is a technology that provides increased storage functions and reliability through redundancy. This is achieved by combining multiple disk drive components into a logical unit, where data is distributed across the drives in one of several ways, called RAID levels.

**reconnaissance** The steps taken to gather evidence and information on the targets you want to attack.

**remote access** Access by information systems (or users) communicating from outside the information system security perimeter.

**remote procedure call (RPC)** A protocol that allows a client computer to request services from a server and the server to return the results.

**replay attack** An attack where the hacker repeats a portion of a cryptographic exchange in hopes of fooling the system into setting up a communications channel.

**request for comments (RFC)** A series of documents and notes on standards used or proposed for use on the Internet; each is identified by a number.

**reverse lookup; reverse DNS lookup** Used to find the domain name associated with an IP address; the opposite of a DNS lookup.

**reverse social engineering** A social engineering attack that manipulates the victim into calling the attacker for help.

**RID** Resource identifier. This is the last portion of the SID that identifies the user to the system in Windows. An RID of 500 identifies the administrator account.

**Rijndael** An encryption standard designed by Joan Daemen and Vincent Rijmen. This was chosen by a NIST contest to be the Advanced Encryption Standard (AES).

**ring topology** A networking configuration where all nodes are connected in a circle with no terminated ends on the cable.

**risk** The potential for damage to or loss of an IT asset.

**risk acceptance** An informed decision to accept the potential for damage to or loss of an IT asset.

**risk assessment** An evaluation conducted to determine the potential for damage to or loss of an IT asset.

**risk avoidance** A decision to reduce the potential for damage to or loss of an IT asset by taking some type of action.

**risk transference** Shifting responsibility from one party to another—for example, through purchasing an insurance policy.

**rogue access point** A wireless access point that either has been installed on a secure company network without explicit authorization from a local network administrator or has been created to allow a hacker to conduct a man-in-the-middle attack.

**role-based access control** An approach to restricting system access to authorized users in which roles are created for various job functions. The permissions to perform certain operations are assigned to specific roles. Members of staff (or other system users) are assigned particular roles, and through those role assignments they acquire the permissions to perform particular system functions.

**rolling code** The code used by a key fob to unlock (and, in some cases, start) a car is called a rolling (or hopping) code. Stealing this code and reusing it is referred to as a rolling code attack.

**rootkit** A set of tools (applications or code) that enables administrator-level access to a computer or computer network and is designed to obscure the fact that the system has been compromised. Rootkits are dangerous malware entities that provide administrator control of machines to attackers and are difficult to detect and remove.

**roots of trust (RoT)** A set of functions within the trusted computing module that are always trusted by the computer’s operating system (OS).

**route** 1. The path a packet travels to reach the intended destination. Each individual device along the path traveled is called a *hop.* 2. Information contained on a device containing instructions for reaching other nodes on the network. This information can be entered dynamically or statically.

**routed protocol** A protocol defining packets that are able to be routed by a router.

**router** A device that receives and sends data packets between two or more networks; the packet headers and a forwarding table provide the router with the information necessary for deciding which interface to use to forward packets.

**Routing Information Protocol (RIP)** A distance-vector routing protocol that employs the hop count as a routing metric. The “hold down time,” used to define how long a route is held in memory, is 180 seconds. RIP prevents routing loops by implementing a limit on the number of hops allowed in a path from the source to a destination. The maximum number of hops allowed for RIP is 15. This hop limit, however, also limits the size of networks that RIP can support. A hop count of 16 is considered an infinite distance and is used to deprecate inaccessible, inoperable, or otherwise undesirable routes in the selection process.

**Routing Protocol** A standard developed to enable routers to exchange messages containing information about routes to reach subnets in the network.

**rule-based access control** A set of rules defined by a system administrator that indicates whether access is allowed or denied to resource objects.

**RxBoot** A limited-function version of the Internetworking Operating System (IOS), held in read-only memory in some earlier models of Cisco devices, capable of performing several seldom-needed low-level functions such as loading a new IOS into Flash memory to recover Flash if corrupted or deleted.

**SaaS** Software as a Service. A type of cloud computing used as a software distribution model.

**SAM** The Security Accounts Manager file in Windows stores all the password hashes for the system.

**Sarbanes-Oxley Act (SOX)** SOX 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.

**scope creep** The change or growth of a project’s scope.

**script kiddie** A derogatory term used to describe an attacker, usually new to the field, who uses simple, easy-to-follow scripts or programs developed by others to attack computer systems and networks and deface websites.

**secure channel** A means of exchanging information from one entity to another using a process that does not provide an attacker the opportunity to reorder, delete, insert, or read information.

**Secure Multipurpose Mail Extension (S/MIME)** A standard for encrypting and authenticating MIME data; used primarily for Internet e-mail.

**Secure Sockets Layer (SSL)** A protocol that uses a private key to encrypt data before transmitting confidential documents over the Internet; widely used on e-commerce, banking, and other sites requiring privacy.

**security breach or security incident** The exploitation of a security vulnerability.

**security bulletins** An announcement, typically from a software vendor, of a known security vulnerability in a program; often the bulletin contains instructions for the application of a software patch.

**security by obscurity** A principle in security engineering that attempts to use anonymity and secrecy (of design, implementation, and so on) to provide security; the footprint of the organization, entity, network, or system is kept as small as possible to avoid interest by hackers. The danger is that a system relying on security by obscurity may have theoretical or actual security vulnerabilities, but its owners or designers believe the flaws are not known.

**security controls** Safeguards or countermeasures to avoid, counteract, or minimize security risks.

**security defect** An unknown deficiency in software or some other product that results in a security vulnerability being identified.

**security incident response team (SIRT)** A group of experts that handles computer security incidents.

**security kernel** The central part of a computer or communications system hardware, firmware, and software that implements the basic security procedures for controlling access to system resources.

**segment** A section or subset of the network. Often a router or other routing device provides the endpoint of the segment.

**separation of duties** The concept of having more than one person required to complete a task.

**Serial Line Internet Protocol (SLIP)** A protocol for exchanging packets over a serial line.

**Service Oriented Architecture (SOA)** 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.

**service set identifier (SSID)** A value assigned to uniquely identify a single wide area network (WAN) in wireless LANs. SSIDs are broadcast by default and are sent in the header of every packet. SSIDs provide no encryption or security.

**service level agreements (SLAs)** A part of a service contract where the level of service is formally defined; may be required as part of the initial pen test agreements.

**session hijacking** An attack in which a hacker steps between two ends of an already established communication session and uses specialized tools to guess sequence numbers to take over the channel.

**session splicing** A method used to prevent IDS detection by dividing the request into multiple parts that are sent in different packets.

**sheepdip** A stand-alone computer, kept off the network, that is used for scanning potentially malicious media or software.

**shoulder surfing** Looking over an authorized user’s shoulder in order to steal information (such as authentication information).

**shrink-wrap code attacks** Attacks that take advantage of the built-in code and scripts most off-the-shelf applications come with.

**SID** Security identifier. The method by which Windows identifies user, group, and computer accounts for rights and permissions.

**sidejacking** A hacking method for stealing the cookies used during a session build and replaying them for unauthorized connection purposes.

**signature scanning** A method for detecting malicious code on a computer where the files are compared to signatures of known viruses stored in a database.

**sign-in seal** An e-mail protection method using a secret message or image that can be referenced on any official communication with the site; if an e-mail is received without the image or message, the recipient knows it is not legitimate.

**Simple Mail Transfer Protocol (SMTP)** An Application layer protocol for sending electronic mail between servers.

**Simple Network Management Protocol (SNMP)** An Application layer protocol for managing devices on an IP network.

**Simple Object Access Protocol (SOAP)** Used for exchanging structured information, such as XML-based messages, in the implementation of web services.

**single loss expectancy (SLE)** The monetary value expected from the occurrence of a risk on an asset. It is mathematically expressed as

single loss expectancy (SLE) = asset value (AV) × exposure factor (EF)

where EF is represented in the impact of the risk over the asset, or percentage of asset lost. As an example, if the AV is reduced by two-thirds, the exposure factor value is 0.66. If the asset is completely lost, the EF is 1.0. The result is a monetary value in the same unit as the SLE is expressed.

**site survey** An inspection of a place where a company or individual proposes to work, to gather the necessary information for a design or risk assessment.

**smartcard** A card with a built-in microprocessor and memory used for identification or financial transactions. The card transfers data to and from a central computer when inserted into a reader.

**smishing** An attack using text messaging, where a user is tricked into downloading malware onto his cellular phone or other mobile device.

**Smurf attack** A denial-of-service attack where the attacker sends a ping to the network’s broadcast address from the spoofed IP address of the target. All systems in the subnet then respond to the spoofed address, eventually flooding the device.

**sniffer** Computer software or hardware that can intercept and log traffic passing over a digital network.

**SOA record** Start of Authority record. This record identifies the primary name server for the zone. The SOA record contains the hostname of the server responsible for all DNS records within the namespace, as well as the basic properties of the domain.

**social engineering** A nontechnical method of hacking. Social engineering is the art of manipulating people, whether in person (human based) or via computing methods (computer based), into providing sensitive information.

**source routing** A network traffic management technique designed to allow applications to specify the route a packet will take to a destination, regardless of what the route tables between the two systems say.

**spam** An electronic version of junk mail. Unsolicited commercial e-mail sent to numerous recipients.

**spoofing** A method of falsely identifying the source of data packets; often used by hackers to make it difficult to trace where an attack originated.

**spyware** A type of malware that covertly collects information about a user.

**stateful packet filtering** A method of network traffic filtering that monitors the entire communications process, including the originator of the session and from which direction it started.

**steganography** The art and science of creating a covert message or image within another message, image, audio, or video file.

**stream cipher** A symmetric key cipher where plain-text bits are combined with a pseudorandom cipher bit stream (keystream), typically by an exclusive-or (XOR) operation. In a stream cipher, the plain-text digits are encrypted one at a time, and the transformation of successive digits varies during the encryption.

**suicide hacker** A hacker who aims to bring down critical infrastructure for a “cause” and does not worry about the penalties associated with his actions.

**sybil attack** An IoT DoS attack using multiple forged identities to create the illusion of traffic congestion, which affects everyone else in the local IoT network.

**symmetric algorithm** A class of algorithms for cryptography that use the same cryptographic key for both decryption and encryption.

**symmetric encryption** A type of encryption where the same key is used to encrypt and decrypt the message.

**SYN attack** A type of denial-of-service attack where a hacker sends thousands of SYN packets to the target with spoofed IP addresses.

**SYN flood attack** A type of attack used to deny service to legitimate users of a network resource by intentionally overloading the network with illegitimate TCP connection requests. SYN packets are sent repeatedly to the target, but the corresponding SYN/ACK responses are ignored.

**syslog** A protocol used for sending and receiving log information for nodes on a network.

**TACACS** Terminal Access Controller Access-Control System. A remote authentication protocol that is used to communicate with an authentication server commonly used in Unix networks.

**target of engagement (TOE)** The software product or system that is the subject of an evaluation.

**telnet** A protocol used in networking to provide bidirectional, interactive, text-oriented communication facility using a virtual terminal connection. Commands entered locally are executed on the remote system.

**Temporal Key Integrity Protocol (TKIP)** A security protocol used in IEEE 802.11i to replace WEP without the requirement to replace legacy hardware.

**third party** A person or entity indirectly involved in a relationship between two principals.

**threat** Any circumstance or event with the potential to adversely impact organizational operations, organizational assets, or individuals through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service.

**three-way (TCP) handshake** A three-step process computers execute to negotiate a connection with one another. The three steps are SYN, SYN/ACK, and ACK.

**tiger team** A group of people, gathered together by a business entity, working to address a specific problem or goal.

**time bomb** A program designed to execute at a specific time to release malicious code onto the computer system or network.

**time to live (TTL)** A limit on the amount of time or number of iterations or transmissions in computer and network technology a packet can experience before it will be discarded.

**timestamping** Recording the time, normally in a log file, when an event happens or when information is created or modified.

**Tini** A small Trojan program that listens on port 777.

**traceroute** A utility that traces a packet from your computer to an Internet host, showing how many hops the packet takes to reach the host and how long the packet requires to complete the hop.

**Transmission Control Protocol (TCP)** A connection-oriented, Layer 4 protocol for transporting data over network segments. TCP is considered reliable because it guarantees delivery and the proper reordering of transmitted packets. This protocol is used for most long-haul traffic on the Internet.

**Transport Layer Security (TLS)** A standard for encrypting e-mail, web pages, and other stream-oriented information transmitted over the Internet.

**trapdoor function** A function that is easy to compute in one direction yet believed to be difficult to compute in the opposite direction (finding its inverse) without special information, called the *trapdoor.* This function is widely used in cryptography.

**Trojan horse** A non-self-replicating program that appears to have a useful purpose but in reality has a different, malicious purpose.

**trusted computer base (TCB)** The set of all hardware, firmware, and/or software components critical to IT security. Bugs or vulnerabilities occurring inside the TCB might jeopardize the security properties of the entire system.

**Trusted Computer System Evaluation Criteria (TCSEC)** A U.S. Department of Defense (DoD) standard that sets basic requirements for assessing the effectiveness of computer security controls built into a computer system.

**tumbling** The act of using numerous electronic serial numbers on a cell phone until a valid number is located.

**tunnel** A point-to-point connection between two endpoints created to exchange data. Typically a tunnel is either an encrypted connection or a connection using a protocol in a method for which it was not designed. An encrypted connection forms a point-to-point connection between sites in which only the sender and the receiver of the data see it in a clear state.

**tunneling** Transmitting one protocol encapsulated inside another protocol.

**tunneling virus** A self-replicating malicious program that attempts installation beneath antivirus software by directly intercepting the interrupt handlers of the operating system to evade detection.

**Unicode** An international encoding standard, working within multiple languages and scripts, that represents each letter, digit, or symbol with a unique numeric value that applies across different platforms.

**Uniform Resource Locator (URL)** A string that represents the location of a web resource—most often a website.

**User Datagram Protocol (UDP)** A connectionless, Layer 4 transport protocol. UDP is faster than TCP but offers no reliability. A best effort is made to deliver the data, but no checks and verifications are performed to guarantee delivery. Therefore, UDP is termed a *connectionless* protocol. UDP is simpler to implement and is used where a small amount of packet loss is acceptable, such as for streaming video and audio.

**Vehicle Ad Hoc Network (VANET)** The communications network used by IoT-enabled vehicles; refers to the spontaneous creation of a wireless network for vehicle-to-vehicle (V2V) data exchange.

**Videocipher II Satellite Encryption System** The brand name of analog scrambling and de-scrambling equipment for cable and satellite television, invented primarily to keep consumer television receive-only (TVRO) satellite equipment from receiving TV programming except on a subscription basis.

**virtual local area network (VLAN)** Devices, connected to one or more switches, grouped logically into a single broadcast domain. Administrators can divide the devices connected to the switches into multiple VLANs without requiring separate physical switches.

**virtual private network (VPN)** A technology that establishes a tunnel to create a private, dedicated, leased-line network over the Internet. The data is encrypted so it’s readable only by the sender and receiver. Companies commonly use VPNs to allow employees to connect securely to the company network from remote locations.

**virtualization** A practice whereby the physical aspects of the hardware are virtually presented to operating systems in a way that allows one or more virtual machines (with their own operating systems) to run *simultaneously* on the same physical box.

**virus** A malicious computer program with self-replication capabilities that attaches to another file and moves with the host from one computer to another.

**virus hoax** An e-mail message that warns users of a nonexistent virus and encourages them to pass on the message to other users.

**vishing** Social engineering attacks using a phone.

**vulnerability** Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source.

**vulnerability assessment** Formal description and evaluation of the vulnerabilities in an information system.

**vulnerability management** The cyclical practice of identifying, classifying, remediating, and mitigating vulnerabilities.

**vulnerability scanning** Sending packets or requests to another system to gain information to be used to identify weaknesses and protect the system from attacks.

**war chalking** Drawing symbols in public places to alert others to an open Wi-Fi network. War chalking can include the SSIDs, administrative passwords to APs, and other information.

**war dialing** The act of dialing all numbers within an organization to discover open modems.

**war driving** The act of searching for Wi-Fi wireless networks by a person in a moving vehicle, using a portable device.

**warm site** An environmentally conditioned workspace partially equipped with IT and telecommunications equipment to support relocated IT operations in the event of a significant disruption.

**web spider** A program designed to browse websites in an automated, methodical manner. Sometimes these programs are used to harvest information from websites, such as e-mail addresses.

**white-box testing** A pen testing method where the attacker knows all information about the internal network. It is designed to simulate an attack by a disgruntled systems administrator or similar level.

**Whois** A query and response protocol widely used for querying databases that store the registered users or assignees of an Internet resource, such as a domain name, an IP address, or an autonomous system.

**wide area network (WAN)** Two or more LANs connected by a high-speed line across a large geographical area.

**Wi-Fi** A term trademarked by the Wi-Fi Alliance, used to define a standard for devices to use to connect to a wireless network.

**Wi-Fi Protected Access (WPA)** Provides data encryption for IEEE 802.11 wireless networks so data can be decrypted only by the intended recipients.

**Wired Equivalent Privacy (WEP)** A security protocol for wireless local area networks defined in the 802.11b standard; intended to provide the same level of security as a wired LAN. WEP is not considered strong security, although it does authenticate clients to access points, encrypt information transmitted between clients and access points, and check the integrity of each packet exchanged.

**wiretapping** The monitoring of telephone or Internet conversations, typically by covert means.

**worm** A self-replicating, self-propagating, self-contained program that uses networking mechanisms to spread itself.

**wrapper** Software used to bind a Trojan and a legitimate program together so the Trojan will be installed when the legitimate program is executed.

**XOR operation** A mathematical operation requiring two binary inputs: if the inputs match, the output is a 0; otherwise, it is a 1.

**Zenmap** A Windows-based GUI version of Nmap.

**zero subnet** In a classful IPv4 subnet, this is the network number with all binary 0s in the subnet part of the number. When written in decimal, the zero subnet has the same number as the classful network number.

**zero-day attack** An attack carried out on a system or application before the vendor becomes aware and before a patch or fix action is available to correct the underlying vulnerability.

**zombie** A computer system that performs tasks dictated by an attacker from a remote location. Zombies may be active or idle, and owners of the systems generally do not know their systems are compromised.

**zone transfer** A type of DNS transfer where all records from an SOA are transmitted to the requestor. Zone transfers have two options: full (opcode AXFR) and incremental (IXFR).

**hardware keystroke logger** A hardware device used to log keystrokes covertly. Hardware keystroke loggers are dangerous because they cannot be detected through regular software/anti-malware scanning.

**hash** A unique numerical string, created by a hashing algorithm on a given piece of data, used to verify data integrity. Generally hashes are used to verify the integrity of files after download (comparison to the hash value on the site before download) and/or to store password values.

**hashing algorithm** A one-way mathematical function that generates a fixed-length numerical string (hash) from a given data input. MD5 and SHA-1 are hashing algorithms.

**heuristic scanning** Method used by antivirus software to detect new, unknown viruses that have not yet been identified; based on a piece-by-piece examination of a program, *heuristic scanning* looks for a sequence or sequences of instructions that differentiate the virus from “normal” programs.

**HIDS** Host-based IDS. An IDS that resides on the host, protecting against file and folder manipulation and other host-based attacks and actions.

**Hierarchical File System (HFS)** A file system used by macOS.

**honeynet** A network deployed as a trap to detect, deflect, or deter unauthorized use of information systems.

**honeypot** A host designed to collect data on suspicious activity.

**hot site** A fully operational off-site data-processing facility equipped with hardware and system software to be used in the event of a disaster.

**HTTP tunneling** A firewall-evasion technique whereby packets are wrapped in HTTP, as a covert channel to the target.

**human-based social engineering** Using conversation or some other interaction between people to gather useful information.

**hybrid attack** An attack that combines a brute-force attack with a dictionary attack.

**hybrid cloud** A cloud model that is a composite of two or more cloud deployment models (public, private, or community).

**Hypertext Transfer Protocol (HTTP)** A communications protocol used for browsing the Internet.

**Hypertext Transfer Protocol Secure (HTTPS)** A hybrid of the HTTP and SSL/TLS protocols that provides encrypted communication and secure identification of a web server.

**IaaS** Infrastructure as a Service. A cloud computing type providing virtualized computing resources over the Internet.

**identity theft** A form of fraud in which someone pretends to be someone else by assuming that person’s identity, typically in order to access resources or obtain credit and other benefits in that person’s name.

**impersonation** A social engineering effort in which the attacker pretends to be an employee, a valid user, or even an executive to elicit information or access.

**inference attack** An attack in which the hacker can derive information from the cipher text without actually decoding it. Sensitive information can be considered compromised if an adversary can infer its real value with a high level of confidence.

**information technology (IT) asset criticality** The level of importance assigned to an IT asset.

**information technology (IT) asset valuation** The monetary value assigned to an IT asset.

**information technology (IT) infrastructure** The combination of all IT assets, resources, components, and systems.

**information technology (IT) security architecture and framework** A document describing information security guidelines, policies, procedures, and standards.

**Information Technology Security Evaluation Criteria (ITSEC)** A structured set of criteria for evaluating computer security within products and systems produced by European countries; it has been largely replaced by the Common Criteria.

**infrastructure mode** A wireless networking mode where all clients connect to the wireless network through a central access point.

**initial sequence number (ISN)** A number assigned during TCP startup sessions that tracks how much information has been moved. This number is used by hackers when hijacking sessions.

**insider affiliate** A spouse, friend, or client of an employee who uses the employee’s credentials to gain physical or logical access to organizational resources.

**insider associate** A person with limited authorized access to the organization; contractors, guards, and cleaning services are all examples.

**Institute of Electrical and Electronics Engineers (IEEE)** An organization composed of engineers, scientists, and students who issue standards related to electrical, electronic, and computer engineering.

**integrity** The security property that data is not modified in an unauthorized and undetected manner. Also, this is the principle of taking measures to ensure that data received is in the same condition and state as when it was originally transmitted.

**Interior Gateway Protocol (IGP)** An Internet routing protocol used to exchange routing information within an autonomous system.

**International Organization for Standardization (ISO)** An international organization composed of national standards bodies from more than 75 countries. ISO developed the OSI reference model.

**Internet Assigned Number Authority (IANA)** The organization that governs the Internet’s top-level domains, IP address allocation, and port number assignments.

**Internet Control Message Protocol (ICMP)** A protocol used to pass control and error messages between nodes on the Internet.

**Internet of Things (IoT)** The collection of devices using sensors, software, storage, and electronics to collect, analyze, store, and share data among themselves or to a user, with or without human intervention or action.

**Internet Protocol (IP)** A protocol for transporting data packets across a packet-switched internetwork (such as the Internet). IP is a routed protocol.

**Internet Protocol Security (IPSec) architecture** A suite of protocols used for securing Internet Protocol (IP) communications by authenticating and encrypting each IP packet of a communication session. This suite includes protocols for establishing mutual authentication between agents at session establishment and for negotiating the cryptographic keys to be used throughout the session.

**Internet service provider (ISP)** A business, government agency, or educational institution thatprovides access to the Internet.

**intranet** A self-contained network with a limited number of participants who extend limited trust to one another in order to accomplish an agreed-upon goal.

**intrusion detection system (IDS)** A security tool designed to protect a system or network against attacks by comparing traffic patterns against a list of both known attack signatures and general characteristics of how attacks may be carried out. Threats are rated and reported.

**intrusion prevention system (IPS)** A security tool designed to protect a system or network against attacks by comparing traffic patterns against a list of both known attack signatures and general characteristics of how attacks may be carried out. Threats are rated and protective measures taken to prevent the more significant threats.

**IoT Gateway** A device designed to send collected data from IoT devices to the user or to data storage (the cloud) for use later.

**iris scanner** A biometric device that uses pattern-recognition techniques based on images of the irises of an individual’s eyes.

**ISO 17799** A standard that provides best-practice recommendations on information security management for use by those responsible for initiating, implementing, or maintaining Information Security Management Systems (ISMS). Information security is defined within the standard in the context of the CIA triad.

**Kerberos** A widely used authentication protocol developed at the Massachusetts Institute of Technology (MIT). Kerberos authentication uses tickets, a ticket granting service, and a key distribution center.

**key exchange protocol** A method in cryptography by which cryptographic keys are exchanged between users, thus allowing use of a cryptographic algorithm (for example, the Diffie-Hellman key exchange).

**keylogger** A software application or hardware device that captures user keystrokes.

**last in first out (LIFO)** A programming principle whereby the last piece of data added to the stack is the first piece of data taken off.

**Level I assessment** An evaluation consisting of a document review, interviews, and demonstrations. No hands-on testing is performed.

**Level II assessment** An evaluation consisting of a document review, interviews, and demonstrations, as well as vulnerability scans and hands-on testing.

**Level III assessment** An evaluation in which testers attempt to penetrate the network.

**Lightweight Directory Access Protocol (LDAP)** An industry-standard protocol used for accessing and managing information within a directory service; an application protocol for querying and modifying data using directory services running over TCP/IP.

**limitation of liability and remedies** A legal limit on the amount of financial liability and remedies the organization is responsible for taking on.

**local area network (LAN)** A computer network confined to a relatively small area, such as a single building or campus.

**logic bomb** A piece of code intentionally inserted into a software system that will perform a malicious function when specified conditions are met at some future point.

**MAC filtering** A method of permitting only MAC addresses in a preapproved list of network access. Addresses not matching are blocked.

**macro virus** A virus written in a macro language and usually embedded in document or spreadsheet files.

**malicious code** Software or firmware intended to perform an unauthorized process that will have an adverse impact on the confidentiality, integrity, or availability of an information system. A virus, worm, Trojan horse, or other code-based entity that infects a host.

**malware** A program or piece of code inserted into a system, usually covertly, with the intent of compromising the confidentiality, integrity, or availability of the victim’s data, applications, or operating system. Malware consists of viruses, worms, and other malicious code.

**mandatory access control (MAC)** A means of restricting access to system resources based on the sensitivity (as represented by a label) of the information contained in the system resource and the formal authorization (that is, clearance) of users to access information of such sensitivity.

**man-in-the-middle attack** An attack where the hacker positions himself between the client and the server to intercept (and sometimes alter) data traveling between the two.

**mantrap** A small space having two sets of interlocking doors; the first set of doors must close before the second set opens. Typically authentication is required for each door, often using different factors. For example, a smartcard may open the first door, and a personal identification number entered on a number pad opens the second.

**master boot record infector** A virus designed to infect the master boot record.

**maximum tolerable downtime (MTD)** A measurement of the potential cost due to a particular asset being unavailable, used as a means to prioritize the recovery of assets should the worst occur.

**MD5** A hashing algorithm that results in a 128-bit output.

**Media Access Control (MAC)** A sublayer of Layer 2 of the OSI model, the Data Link layer. It provides addressing and channel access control mechanisms that enable several terminals or network nodes to communicate within a multipoint network.

**methodology** A documented process for a procedure designed to be consistent, repeatable, and accountable.

**minimum acceptable level of risk** An organization’s threshold for the seven areas of information security responsibility. This level is established based on the objectives for maintaining the confidentiality, integrity, and availability of the organization’s IT assets and infrastructure and will determine the resources expended for information security.

**multipartite virus** A computer virus that infects and spreads in multiple ways.

**Multipurpose Internet Mail Extensions (MIME)** An extensible mechanism for e-mail. A variety of MIME types exist for sending content such as audio, binary, or video using the Simple Mail Transfer Protocol (SMTP).

**National Security Agency (NSA) INFOSEC Assessment Methodology (IAM)** A systematic process for the assessment of security vulnerabilities.

**NetBSD** A free, open source version of the Berkeley Software Distribution of Unix, often used in embedded systems.

**NetBus** A software program for remotely controlling a Microsoft Windows computer system over a network. Generally it is considered malware.

**network access server** A device providing temporary, on-demand, point-to-point network access to users.

**Network Address Translation (NAT)** A technology where you advertise one IP address externally and data packets are rerouted to the appropriate IP address inside your network by a device providing translation services. In this way, IP addresses of machines on your internal network are hidden from external users.

**Network Basic Input/Output System (NetBIOS)** An API that provides services related to the OSI model’s Session layer, allowing applications on separate computers to communicate over a LAN.

**network interface card (NIC)** An adapter that provides the physical connection to send and receive data between the computer and the network media.

**network operations center (NOC)** One or more locations from which control is exercised over a computer, television broadcast, or telecommunications network.

**network tap** Any kind of connection that allows you to see all traffic passing by. Generally used in reference to a network-based IDS (NIDS) to monitor all traffic.

**Nmap** An open source scanning utility used to discover hosts and services on a network.

**node** A device on a network.

**nonrepudiation** The means by which a recipient of a message can ensure the identity of the sender and that neither party can deny having sent or received the message. The most common method is through digital certificates.

**NOP** A command that instructs the system processor to do nothing. Many overflow attacks involve stringing several NOP operations together (known as a NOP sled).

**nslookup** A network administration command-line tool available for many operating systems for querying the Domain Name System (DNS) to obtain domain name or IP address mappings or any other specific DNS record.

**NT LAN Manager (NTLM)** The default network authentication suite of protocols for Windows NT 4.0—retained in later versions for backward compatibility. NTLM is considered insecure and was replaced by NTLMv2.

**null session** An anonymous connection to an administrative share (IPC$) on a Windows machine. Null sessions allow for enumeration of Windows machines, among other attacks.

**open source** Describes practices in production and development that promote access to the end product’s source materials.

**Open Source Security Testing Methodology Manual (OSSTMM)** A peer-reviewed, formalized methodology of security testing and analysis.

**Open System Interconnection (OSI) reference model** A network architecture framework developed by ISO that describes the communications process between two systems across the Internet in seven distinct layers.

**OpenBSD** A Unix-like computer operating system descending from the BSD. OpenBSD includes a number of security features absent or optional in other operating systems.

**operating system attack** An attack that exploits the common mistake many people make when installing operating systems—that is, accepting and leaving all the defaults.

**out-of-band signaling** Transmission using channels or frequencies outside those normally used for data transfer; often used for error reporting.

**outsider associate** A untrusted outsider using open, or illicitly gained, access to an organization’s resources.

**overt channel** A communications path, such as the Internet, authorized for data transmission within a computer system or network.

**PaaS** Platform as a Service. A cloud computing type geared toward software development, providing a platform that allows subscribers to develop applications without building the infrastructure it would normally take to develop and launch software.

**packer** A crypter that uses compression to pack malware executables into smaller sizes to avoid detection.

**packet** A unit of information formatted according to specific protocols, generally regarded as being used in OSI Layer 3, that allows precise transmittal of data from one network node to another. Also called a *datagram* or *data packet,* a packet contains a header (container) and a payload (contents). Any IP message larger than 1500 bytes will be fragmented into packets for transmission.

**packet filtering** Controlling access to a network by analyzing the headers of incoming and outgoing packets and letting them pass or discarding them based on rule sets created by a network administrator. A packet filter allows or denies packets based on destination, source, and/or port.

**Packet Internet Groper (ping)** A utility that sends an ICMP Echo message to determine whether a specific IP address is accessible; if the message receives a reply, the address is reachable.

**parameter tampering** An attack where the hacker manipulates parameters within the URL string in hopes of modifying data.

**passive attack** An attack against an authentication protocol in which the attacker intercepts data in transit along the network between the claimant and verifier but does not alter the data (in other words, eavesdropping).

**Password Authentication Protocol (PAP)** A simple PPP authentication mechanism in which the user name and password are transmitted in clear text to prove identity. PAP compares the user name and password to a table listing authorized users.

**patch** A piece of software, provided by the vendor, intended to update or fix known, discovered problems in a computer program or its supporting data.

**pattern matching** The act of checking some sequence of tokens for the presence of the constituents of some pattern.

**payload** The contents of a packet. A system attack requires the attacker to deliver a malicious payload that is acted upon and executed by the system.

**Payment Card Industry Data Security Standard (PCI-DSS)** 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.

**penetration testing** A method of evaluating the security of a computer system or network by simulating an attack from a malicious source.

**personal identification number (PIN)** A secret, typically consisting of only decimal digits, that a claimant memorizes and uses to authenticate his identity.

**phishing** The use of deceptive computer-based means to trick individuals into disclosing sensitive personal information—usually via a carefully crafted e-mail message.

**physical security** Security measures, such as a locked door, perimeter fence, or security guard, to prevent or deter physical access to a facility, resource, or information stored on physical media.

**piggybacking** When an authorized person allows (intentionally or unintentionally) someone to pass through a secure door, despite the intruder not having a badge.

**ping sweep** The process of pinging each address within a subnet to map potential targets. Ping sweeps are unreliable and easily detectable but very fast.

**polymorphic virus** Malicious code that uses a polymorphic engine to mutate while keeping the original algorithm intact; the code changes itself each time it runs, but the function of the code will not change.

**Point-to-Point Protocol (PPP)** Provides router-to-router or host-to-network connections over asynchronous and synchronous circuits.

**Point-to-Point Tunneling Protocol (PPTP)** A VPN tunneling protocol with encryption. PPTP connects two nodes in a VPN by using one TCP port for negotiation and authentication and one IP protocol for data transfer.

**Port Address Translation (PAT)** A NAT method in which multiple internal hosts, using private IP addressing, can be mapped through a single public IP address using the session IDs and port numbers. An internal global IP address can support in excess of 65,000 concurrent TCP and UDP connections.

**port knocking** Another term for *firewalking*—the method of externally testing ports on a firewall by generating a connection attempt on each port, one by one.

**port redirection** The process of directing a protocol from one port to another.

**port scanning** The process of using an application to remotely identify open ports on a system (for example, whether systems allow connections through those ports).

**POST** An HTTP command to transmit text to a web server for processing. This is the opposite of an HTTP GET.

**Post Office Protocol 3 (POP3)** An Application layer protocol used by local e-mail clients to retrieve e-mail from a remote server over a TCP/IP connection.

**Presentation layer** Layer 6 of the OSI reference model. The Presentation layer ensures information sent by the Application layer of the sending system will be readable by the Application layer of the receiving system.

**Pretty Good Privacy (PGP)** A data encryption/decryption program often used for e-mail and file storage.

**private cloud** A cloud model operated solely for a single organization (a.k.a. single-tenant environment) and is usually not pay-as-you-go.

**private key** The secret portion of an asymmetric key pair typically used to decrypt or digitally sign data. The private key is never shared and is always used for decryption, with one notable exception: the private key is used to encrypt the digital signature.

**private network address** A nonroutable IP address range intended for use only within the confines of a single organization, falling within the predefined range of 10.0.0.0, 172.16–31.0.0, or 192.168.0.0.

**promiscuous mode** A configuration of a network card that makes the card pass all traffic it receives to the central processing unit rather than just frames addressed to it—a feature normally used for packet sniffing and bridged networking for hardware virtualization. Windows machines use WinPcap for this; Linux uses libcap.

**protocol** A formal set of rules describing data transmission, especially across a network. A protocol determines the type of error checking, the data compression method, how the sending device will indicate completion, how the receiving device will indicate the message was received, and so on.

**protocol stack** A set of related communications protocols operating together as a group to address communication at some or all of the seven layers of the OSI reference model.

**proxy server** A device set up to send a response on behalf of an end node to the requesting host. Proxies are generally used to obfuscate the host from the Internet.

**public cloud** A cloud model where services are provided over a network that is open for public use (such as the Internet).

**public key** The public portion of an asymmetric key pair typically used to encrypt data or verify signatures. Public keys are shared and are used to encrypt messages.

**public key infrastructure (PKI)** A set of hardware, software, people, policies, and procedures needed to create, manage, distribute, use, store, and revoke digital certificates.

**pure insider** An employee with all the rights and access associated with being employed by the company.

**purple team** A single team of security professionals who perform cooperative vulnerability and penetration assessments (CVPA).

**qualitative analysis** A nonnumerical, subjective risk evaluation. This is used with qualitative assessment (an evaluation of risk that results in ratings of none, low, medium, or high for the probability).

**quality of service (QoS)** A defined measure of service within a network system—administrators may assign a higher QoS to one host, segment, or type of traffic.

**quantitative risk assessment** Calculations of two components of risk (R): the magnitude of the potential loss (L), and the probability (P) that the loss will occur.

**queue** A backlog of packets stored in buffers and waiting to be forwarded over an interface.

**RAID (Redundant Array of Independent Disks)** Formerly *Redundant Array of Inexpensive Disks,* RAID is a technology that provides increased storage functions and reliability through redundancy. This is achieved by combining multiple disk drive components into a logical unit, where data is distributed across the drives in one of several ways, called RAID levels.

**reconnaissance** The steps taken to gather evidence and information on the targets you want to attack.

**remote access** Access by information systems (or users) communicating from outside the information system security perimeter.

**remote procedure call (RPC)** A protocol that allows a client computer to request services from a server and the server to return the results.

**replay attack** An attack where the hacker repeats a portion of a cryptographic exchange in hopes of fooling the system into setting up a communications channel.

**request for comments (RFC)** A series of documents and notes on standards used or proposed for use on the Internet; each is identified by a number.

**reverse lookup; reverse DNS lookup** Used to find the domain name associated with an IP address; the opposite of a DNS lookup.

**reverse social engineering** A social engineering attack that manipulates the victim into calling the attacker for help.

**RID** Resource identifier. This is the last portion of the SID that identifies the user to the system in Windows. An RID of 500 identifies the administrator account.

**Rijndael** An encryption standard designed by Joan Daemen and Vincent Rijmen. This was chosen by a NIST contest to be the Advanced Encryption Standard (AES).

**ring topology** A networking configuration where all nodes are connected in a circle with no terminated ends on the cable.

**risk** The potential for damage to or loss of an IT asset.

**risk acceptance** An informed decision to accept the potential for damage to or loss of an IT asset.

**risk assessment** An evaluation conducted to determine the potential for damage to or loss of an IT asset.

**risk avoidance** A decision to reduce the potential for damage to or loss of an IT asset by taking some type of action.

**risk transference** Shifting responsibility from one party to another—for example, through purchasing an insurance policy.

**rogue access point** A wireless access point that either has been installed on a secure company network without explicit authorization from a local network administrator or has been created to allow a hacker to conduct a man-in-the-middle attack.

**role-based access control** An approach to restricting system access to authorized users in which roles are created for various job functions. The permissions to perform certain operations are assigned to specific roles. Members of staff (or other system users) are assigned particular roles, and through those role assignments they acquire the permissions to perform particular system functions.

**rolling code** The code used by a key fob to unlock (and, in some cases, start) a car is called a rolling (or hopping) code. Stealing this code and reusing it is referred to as a rolling code attack.

**rootkit** A set of tools (applications or code) that enables administrator-level access to a computer or computer network and is designed to obscure the fact that the system has been compromised. Rootkits are dangerous malware entities that provide administrator control of machines to attackers and are difficult to detect and remove.

**roots of trust (RoT)** A set of functions within the trusted computing module that are always trusted by the computer’s operating system (OS).

**route** 1. The path a packet travels to reach the intended destination. Each individual device along the path traveled is called a *hop.* 2. Information contained on a device containing instructions for reaching other nodes on the network. This information can be entered dynamically or statically.

**routed protocol** A protocol defining packets that are able to be routed by a router.

**router** A device that receives and sends data packets between two or more networks; the packet headers and a forwarding table provide the router with the information necessary for deciding which interface to use to forward packets.

**Routing Information Protocol (RIP)** A distance-vector routing protocol that employs the hop count as a routing metric. The “hold down time,” used to define how long a route is held in memory, is 180 seconds. RIP prevents routing loops by implementing a limit on the number of hops allowed in a path from the source to a destination. The maximum number of hops allowed for RIP is 15. This hop limit, however, also limits the size of networks that RIP can support. A hop count of 16 is considered an infinite distance and is used to deprecate inaccessible, inoperable, or otherwise undesirable routes in the selection process.

**Routing Protocol** A standard developed to enable routers to exchange messages containing information about routes to reach subnets in the network.

**rule-based access control** A set of rules defined by a system administrator that indicates whether access is allowed or denied to resource objects.

**RxBoot** A limited-function version of the Internetworking Operating System (IOS), held in read-only memory in some earlier models of Cisco devices, capable of performing several seldom-needed low-level functions such as loading a new IOS into Flash memory to recover Flash if corrupted or deleted.

**SaaS** Software as a Service. A type of cloud computing used as a software distribution model.

**SAM** The Security Accounts Manager file in Windows stores all the password hashes for the system.

**Sarbanes-Oxley Act (SOX)** SOX 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.

**scope creep** The change or growth of a project’s scope.

**script kiddie** A derogatory term used to describe an attacker, usually new to the field, who uses simple, easy-to-follow scripts or programs developed by others to attack computer systems and networks and deface websites.

**secure channel** A means of exchanging information from one entity to another using a process that does not provide an attacker the opportunity to reorder, delete, insert, or read information.

**Secure Multipurpose Mail Extension (S/MIME)** A standard for encrypting and authenticating MIME data; used primarily for Internet e-mail.

**Secure Sockets Layer (SSL)** A protocol that uses a private key to encrypt data before transmitting confidential documents over the Internet; widely used on e-commerce, banking, and other sites requiring privacy.

**security breach or security incident** The exploitation of a security vulnerability.

**security bulletins** An announcement, typically from a software vendor, of a known security vulnerability in a program; often the bulletin contains instructions for the application of a software patch.

**security by obscurity** A principle in security engineering that attempts to use anonymity and secrecy (of design, implementation, and so on) to provide security; the footprint of the organization, entity, network, or system is kept as small as possible to avoid interest by hackers. The danger is that a system relying on security by obscurity may have theoretical or actual security vulnerabilities, but its owners or designers believe the flaws are not known.

**security controls** Safeguards or countermeasures to avoid, counteract, or minimize security risks.

**security defect** An unknown deficiency in software or some other product that results in a security vulnerability being identified.

**security incident response team (SIRT)** A group of experts that handles computer security incidents.

**security kernel** The central part of a computer or communications system hardware, firmware, and software that implements the basic security procedures for controlling access to system resources.

**segment** A section or subset of the network. Often a router or other routing device provides the endpoint of the segment.

**separation of duties** The concept of having more than one person required to complete a task.

**Serial Line Internet Protocol (SLIP)** A protocol for exchanging packets over a serial line.

**Service Oriented Architecture (SOA)** 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.

**service set identifier (SSID)** A value assigned to uniquely identify a single wide area network (WAN) in wireless LANs. SSIDs are broadcast by default and are sent in the header of every packet. SSIDs provide no encryption or security.

**service level agreements (SLAs)** A part of a service contract where the level of service is formally defined; may be required as part of the initial pen test agreements.

**session hijacking** An attack in which a hacker steps between two ends of an already established communication session and uses specialized tools to guess sequence numbers to take over the channel.

**session splicing** A method used to prevent IDS detection by dividing the request into multiple parts that are sent in different packets.

**sheepdip** A stand-alone computer, kept off the network, that is used for scanning potentially malicious media or software.

**shoulder surfing** Looking over an authorized user’s shoulder in order to steal information (such as authentication information).

**shrink-wrap code attacks** Attacks that take advantage of the built-in code and scripts most off-the-shelf applications come with.

**SID** Security identifier. The method by which Windows identifies user, group, and computer accounts for rights and permissions.

**sidejacking** A hacking method for stealing the cookies used during a session build and replaying them for unauthorized connection purposes.

**signature scanning** A method for detecting malicious code on a computer where the files are compared to signatures of known viruses stored in a database.

**sign-in seal** An e-mail protection method using a secret message or image that can be referenced on any official communication with the site; if an e-mail is received without the image or message, the recipient knows it is not legitimate.

**Simple Mail Transfer Protocol (SMTP)** An Application layer protocol for sending electronic mail between servers.

**Simple Network Management Protocol (SNMP)** An Application layer protocol for managing devices on an IP network.

**Simple Object Access Protocol (SOAP)** Used for exchanging structured information, such as XML-based messages, in the implementation of web services.

**single loss expectancy (SLE)** The monetary value expected from the occurrence of a risk on an asset. It is mathematically expressed as

single loss expectancy (SLE) = asset value (AV) × exposure factor (EF)

where EF is represented in the impact of the risk over the asset, or percentage of asset lost. As an example, if the AV is reduced by two-thirds, the exposure factor value is 0.66. If the asset is completely lost, the EF is 1.0. The result is a monetary value in the same unit as the SLE is expressed.

**site survey** An inspection of a place where a company or individual proposes to work, to gather the necessary information for a design or risk assessment.

**smartcard** A card with a built-in microprocessor and memory used for identification or financial transactions. The card transfers data to and from a central computer when inserted into a reader.

**smishing** An attack using text messaging, where a user is tricked into downloading malware onto his cellular phone or other mobile device.

**Smurf attack** A denial-of-service attack where the attacker sends a ping to the network’s broadcast address from the spoofed IP address of the target. All systems in the subnet then respond to the spoofed address, eventually flooding the device.

**sniffer** Computer software or hardware that can intercept and log traffic passing over a digital network.

**SOA record** Start of Authority record. This record identifies the primary name server for the zone. The SOA record contains the hostname of the server responsible for all DNS records within the namespace, as well as the basic properties of the domain.

**social engineering** A nontechnical method of hacking. Social engineering is the art of manipulating people, whether in person (human based) or via computing methods (computer based), into providing sensitive information.

**source routing** A network traffic management technique designed to allow applications to specify the route a packet will take to a destination, regardless of what the route tables between the two systems say.

**spam** An electronic version of junk mail. Unsolicited commercial e-mail sent to numerous recipients.

**spoofing** A method of falsely identifying the source of data packets; often used by hackers to make it difficult to trace where an attack originated.

**spyware** A type of malware that covertly collects information about a user.

**stateful packet filtering** A method of network traffic filtering that monitors the entire communications process, including the originator of the session and from which direction it started.

**steganography** The art and science of creating a covert message or image within another message, image, audio, or video file.

**stream cipher** A symmetric key cipher where plain-text bits are combined with a pseudorandom cipher bit stream (keystream), typically by an exclusive-or (XOR) operation. In a stream cipher, the plain-text digits are encrypted one at a time, and the transformation of successive digits varies during the encryption.

**suicide hacker** A hacker who aims to bring down critical infrastructure for a “cause” and does not worry about the penalties associated with his actions.

**sybil attack** An IoT DoS attack using multiple forged identities to create the illusion of traffic congestion, which affects everyone else in the local IoT network.

**symmetric algorithm** A class of algorithms for cryptography that use the same cryptographic key for both decryption and encryption.

**symmetric encryption** A type of encryption where the same key is used to encrypt and decrypt the message.

**SYN attack** A type of denial-of-service attack where a hacker sends thousands of SYN packets to the target with spoofed IP addresses.

**SYN flood attack** A type of attack used to deny service to legitimate users of a network resource by intentionally overloading the network with illegitimate TCP connection requests. SYN packets are sent repeatedly to the target, but the corresponding SYN/ACK responses are ignored.

**syslog** A protocol used for sending and receiving log information for nodes on a network.

**TACACS** Terminal Access Controller Access-Control System. A remote authentication protocol that is used to communicate with an authentication server commonly used in Unix networks.

**target of engagement (TOE)** The software product or system that is the subject of an evaluation.

**telnet** A protocol used in networking to provide bidirectional, interactive, text-oriented communication facility using a virtual terminal connection. Commands entered locally are executed on the remote system.

**Temporal Key Integrity Protocol (TKIP)** A security protocol used in IEEE 802.11i to replace WEP without the requirement to replace legacy hardware.

**third party** A person or entity indirectly involved in a relationship between two principals.

**threat** Any circumstance or event with the potential to adversely impact organizational operations, organizational assets, or individuals through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service.

**three-way (TCP) handshake** A three-step process computers execute to negotiate a connection with one another. The three steps are SYN, SYN/ACK, and ACK.

**tiger team** A group of people, gathered together by a business entity, working to address a specific problem or goal.

**time bomb** A program designed to execute at a specific time to release malicious code onto the computer system or network.

**time to live (TTL)** A limit on the amount of time or number of iterations or transmissions in computer and network technology a packet can experience before it will be discarded.

**timestamping** Recording the time, normally in a log file, when an event happens or when information is created or modified.

**Tini** A small Trojan program that listens on port 777.

**traceroute** A utility that traces a packet from your computer to an Internet host, showing how many hops the packet takes to reach the host and how long the packet requires to complete the hop.

**Transmission Control Protocol (TCP)** A connection-oriented, Layer 4 protocol for transporting data over network segments. TCP is considered reliable because it guarantees delivery and the proper reordering of transmitted packets. This protocol is used for most long-haul traffic on the Internet.

**Transport Layer Security (TLS)** A standard for encrypting e-mail, web pages, and other stream-oriented information transmitted over the Internet.

**trapdoor function** A function that is easy to compute in one direction yet believed to be difficult to compute in the opposite direction (finding its inverse) without special information, called the *trapdoor.* This function is widely used in cryptography.

**Trojan horse** A non-self-replicating program that appears to have a useful purpose but in reality has a different, malicious purpose.

**trusted computer base (TCB)** The set of all hardware, firmware, and/or software components critical to IT security. Bugs or vulnerabilities occurring inside the TCB might jeopardize the security properties of the entire system.

**Trusted Computer System Evaluation Criteria (TCSEC)** A U.S. Department of Defense (DoD) standard that sets basic requirements for assessing the effectiveness of computer security controls built into a computer system.

**tumbling** The act of using numerous electronic serial numbers on a cell phone until a valid number is located.

**tunnel** A point-to-point connection between two endpoints created to exchange data. Typically a tunnel is either an encrypted connection or a connection using a protocol in a method for which it was not designed. An encrypted connection forms a point-to-point connection between sites in which only the sender and the receiver of the data see it in a clear state.

**tunneling** Transmitting one protocol encapsulated inside another protocol.

**tunneling virus** A self-replicating malicious program that attempts installation beneath antivirus software by directly intercepting the interrupt handlers of the operating system to evade detection.

**Unicode** An international encoding standard, working within multiple languages and scripts, that represents each letter, digit, or symbol with a unique numeric value that applies across different platforms.

**Uniform Resource Locator (URL)** A string that represents the location of a web resource—most often a website.

**User Datagram Protocol (UDP)** A connectionless, Layer 4 transport protocol. UDP is faster than TCP but offers no reliability. A best effort is made to deliver the data, but no checks and verifications are performed to guarantee delivery. Therefore, UDP is termed a *connectionless* protocol. UDP is simpler to implement and is used where a small amount of packet loss is acceptable, such as for streaming video and audio.

**Vehicle Ad Hoc Network (VANET)** The communications network used by IoT-enabled vehicles; refers to the spontaneous creation of a wireless network for vehicle-to-vehicle (V2V) data exchange.

**Videocipher II Satellite Encryption System** The brand name of analog scrambling and de-scrambling equipment for cable and satellite television, invented primarily to keep consumer television receive-only (TVRO) satellite equipment from receiving TV programming except on a subscription basis.

**virtual local area network (VLAN)** Devices, connected to one or more switches, grouped logically into a single broadcast domain. Administrators can divide the devices connected to the switches into multiple VLANs without requiring separate physical switches.

**virtual private network (VPN)** A technology that establishes a tunnel to create a private, dedicated, leased-line network over the Internet. The data is encrypted so it’s readable only by the sender and receiver. Companies commonly use VPNs to allow employees to connect securely to the company network from remote locations.

**virtualization** A practice whereby the physical aspects of the hardware are virtually presented to operating systems in a way that allows one or more virtual machines (with their own operating systems) to run *simultaneously* on the same physical box.

**virus** A malicious computer program with self-replication capabilities that attaches to another file and moves with the host from one computer to another.

**virus hoax** An e-mail message that warns users of a nonexistent virus and encourages them to pass on the message to other users.

**vishing** Social engineering attacks using a phone.

**vulnerability** Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source.

**vulnerability assessment** Formal description and evaluation of the vulnerabilities in an information system.

**vulnerability management** The cyclical practice of identifying, classifying, remediating, and mitigating vulnerabilities.

**vulnerability scanning** Sending packets or requests to another system to gain information to be used to identify weaknesses and protect the system from attacks.

**war chalking** Drawing symbols in public places to alert others to an open Wi-Fi network. War chalking can include the SSIDs, administrative passwords to APs, and other information.

**war dialing** The act of dialing all numbers within an organization to discover open modems.

**war driving** The act of searching for Wi-Fi wireless networks by a person in a moving vehicle, using a portable device.

**warm site** An environmentally conditioned workspace partially equipped with IT and telecommunications equipment to support relocated IT operations in the event of a significant disruption.

**web spider** A program designed to browse websites in an automated, methodical manner. Sometimes these programs are used to harvest information from websites, such as e-mail addresses.

**white-box testing** A pen testing method where the attacker knows all information about the internal network. It is designed to simulate an attack by a disgruntled systems administrator or similar level.

**Whois** A query and response protocol widely used for querying databases that store the registered users or assignees of an Internet resource, such as a domain name, an IP address, or an autonomous system.

**wide area network (WAN)** Two or more LANs connected by a high-speed line across a large geographical area.

**Wi-Fi** A term trademarked by the Wi-Fi Alliance, used to define a standard for devices to use to connect to a wireless network.

**Wi-Fi Protected Access (WPA)** Provides data encryption for IEEE 802.11 wireless networks so data can be decrypted only by the intended recipients.

**Wired Equivalent Privacy (WEP)** A security protocol for wireless local area networks defined in the 802.11b standard; intended to provide the same level of security as a wired LAN. WEP is not considered strong security, although it does authenticate clients to access points, encrypt information transmitted between clients and access points, and check the integrity of each packet exchanged.

**wiretapping** The monitoring of telephone or Internet conversations, typically by covert means.

**worm** A self-replicating, self-propagating, self-contained program that uses networking mechanisms to spread itself.

**wrapper** Software used to bind a Trojan and a legitimate program together so the Trojan will be installed when the legitimate program is executed.

**XOR operation** A mathematical operation requiring two binary inputs: if the inputs match, the output is a 0; otherwise, it is a 1.

**Zenmap** A Windows-based GUI version of Nmap.

**zero subnet** In a classful IPv4 subnet, this is the network number with all binary 0s in the subnet part of the number. When written in decimal, the zero subnet has the same number as the classful network number.

**zero-day attack** An attack carried out on a system or application before the vendor becomes aware and before a patch or fix action is available to correct the underlying vulnerability.

**zombie** A computer system that performs tasks dictated by an attacker from a remote location. Zombies may be active or idle, and owners of the systems generally do not know their systems are compromised.

**zone transfer** A type of DNS transfer where all records from an SOA are transmitted to the requestor. Zone transfers have two options: full (opcode AXFR) and incremental (IXFR).

## INDEX

*Please note that index links point to page beginnings from the print edition. Locations are approximate in e-readers, and you may need to page down one or more times after clicking a link to get to the indexed material*.

3D printing, [170](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch4.xhtml#page_170)–171

3DES encryption, [389](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch11.xhtml#page_389)

3G standard, [307](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch8.xhtml#page_307)

4G standard, [286](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch7.xhtml#page_286), [307](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch8.xhtml#page_307)

802.11 standards, [272](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch7.xhtml#page_272)–273

**A**

Absinthe, [259](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch6.xhtml#page_259)

access

covering tracks, [29](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_29)

gaining, [28](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_28), [197](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch5.xhtml#page_197)–198

government access to keys, [396](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch11.xhtml#page_396)–397

maintaining, [29](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_29)

access card attacks, [429](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch12.xhtml#page_429)

access control lists (ACLs), [118](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch3.xhtml#page_118), [165](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch4.xhtml#page_165), [166](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch4.xhtml#page_166)

Access Control Policy, [23](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_23)

access control systems, [21](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_21)–22

access controls, [21](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_21)–22, [230](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch6.xhtml#page_230), [445](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch12.xhtml#page_445)–448

access points (APs)

Cisco, [285](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch7.xhtml#page_285)

considerations, [274](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch7.xhtml#page_274)

detecting, [283](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch7.xhtml#page_283)

multiple, [274](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch7.xhtml#page_274)

open, [281](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch7.xhtml#page_281)

rogue, [274](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch7.xhtml#page_274), [283](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch7.xhtml#page_283), [284](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch7.xhtml#page_284)–285

wireless, [274](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch7.xhtml#page_274), [278](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch7.xhtml#page_278), [281](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch7.xhtml#page_281), [284](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch7.xhtml#page_284)–285

ACK (acknowledgment), [9](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_9), [10](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_10)

ACK flag, [86](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch3.xhtml#page_86), [87](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch3.xhtml#page_87), [102](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch3.xhtml#page_102)

ACK scans, [102](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch3.xhtml#page_102)

acknowledgment. *See* ACK

ACLs (access control lists), [118](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch3.xhtml#page_118), [165](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch4.xhtml#page_165), [166](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch4.xhtml#page_166)

Active Directory Explorer, [124](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch3.xhtml#page_124)

active footprinting, [49](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch2.xhtml#page_49), [52](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch2.xhtml#page_52)

active sniffing, [150](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch4.xhtml#page_150)–153

ad hoc connection attack, [285](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch7.xhtml#page_285)

ad hoc networks, [273](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch7.xhtml#page_273), [274](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch7.xhtml#page_274)

adaptive chosen plain-text attack, [415](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch11.xhtml#page_415)

Address Resolution Protocol. *See* ARP

address space layout randomization (ASLR), [251](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch6.xhtml#page_251)

administrative controls, [16](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_16)

administrators

changing account name, [204](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch5.xhtml#page_204)

enforcing password restrictions, [187](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch5.xhtml#page_187)

network monitoring, [160](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch4.xhtml#page_160)–161, [162](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch4.xhtml#page_162)

patches/software deployment, [211](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch5.xhtml#page_211)

privileges, [209](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch5.xhtml#page_209)–210

zone transfers, [71](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch2.xhtml#page_71)

ADMmutate tool, [168](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch4.xhtml#page_168)

ADS (alternate data stream), [212](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch5.xhtml#page_212)–214

Advanced Encryption Standard (AES), [279](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch7.xhtml#page_279), [280](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch7.xhtml#page_280), [390](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch11.xhtml#page_390)

AES (Advanced Encryption Standard), [279](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch7.xhtml#page_279), [280](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch7.xhtml#page_280), [390](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch11.xhtml#page_390)

African Network Information Center (AfriNIC), [68](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch2.xhtml#page_68)

AfriNIC (African Network Information Center), [68](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch2.xhtml#page_68)

AH (authentication header), [373](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch10.xhtml#page_373), [410](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch11.xhtml#page_410)

air quality, [444](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch12.xhtml#page_444)

Aircrack, [280](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch7.xhtml#page_280), [288](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch7.xhtml#page_288)

AirMagnet WiFi Analyzer, [289](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch7.xhtml#page_289)

AirPcap card, [283](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch7.xhtml#page_283)

AirPcap dongle, [282](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch7.xhtml#page_282)

ALE (annualized loss expectancy), [17](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_17)

alexa.com, [51](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch2.xhtml#page_51)

algorithms, [387](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch11.xhtml#page_387)

alternate data stream (ADS), [212](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch5.xhtml#page_212)–214

Amazon, [336](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch9.xhtml#page_336), [338](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch9.xhtml#page_338)

Amazon Web Services. *See* AWS

“ambering out,” 155

American Registry for Internet Numbers (ARIN), [68](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch2.xhtml#page_68), [72](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch2.xhtml#page_72), [73](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch2.xhtml#page_73)

American Standard Code for Information Interchange (ASCII), [6](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_6)–7

Android phones. *See also* mobile devices

applications, [300](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch8.xhtml#page_300), [303](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch8.xhtml#page_303), [305](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch8.xhtml#page_305), [306](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch8.xhtml#page_306)

Device Administration API, [305](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch8.xhtml#page_305)

rooting, [303](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch8.xhtml#page_303), [305](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch8.xhtml#page_305)

Stagefright bugs, [308](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch8.xhtml#page_308)

ZitMo malware, [442](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch12.xhtml#page_442)

Angry IP Scanner, [99](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch3.xhtml#page_99)–101

annual rate of occurrence (ARO), [17](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_17)

annualized loss expectancy (ALE), [17](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_17)

anonymizers, [114](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch3.xhtml#page_114)–115

anonymous footprinting, [49](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch2.xhtml#page_49)

Anonymous hackers, [369](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch10.xhtml#page_369)–370

antennas, wireless, [274](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch7.xhtml#page_274)–276

antivirus. *See* AV

anycast, [146](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch4.xhtml#page_146), [147](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch4.xhtml#page_147)

Apache servers, [235](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch6.xhtml#page_235), [236](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch6.xhtml#page_236)–237

APIs (application program interfaces), [305](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch8.xhtml#page_305), [341](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch9.xhtml#page_341)

APNIC (Asia-Pacific Network Information Center), [68](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch2.xhtml#page_68)

Apple HFS file system, [212](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch5.xhtml#page_212)

Apple iOS, [303](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch8.xhtml#page_303)–304, [305](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch8.xhtml#page_305). *See also* mobile devices

Apple TV, [303](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch8.xhtml#page_303)

application flaws, [13](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_13)

Application layer, [6](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_6)–7, [141](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch4.xhtml#page_141)–142

application level rootkits, [217](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch5.xhtml#page_217)

application logs, [215](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch5.xhtml#page_215)

application program interfaces (APIs), [305](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch8.xhtml#page_305), [341](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch9.xhtml#page_341)

application servers, [235](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch6.xhtml#page_235)

application-level attacks

buffer overflows, [251](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch6.xhtml#page_251)–253

cookies, [252](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch6.xhtml#page_252), [253](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch6.xhtml#page_253)–254

cross-site scripting, [251](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch6.xhtml#page_251)–253

described, [26](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_26), [366](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch10.xhtml#page_366), [367](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch10.xhtml#page_367)

executable code, [210](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch5.xhtml#page_210)–211

LDAP injection attacks, [249](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch6.xhtml#page_249)–250

mobile platform, [441](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch12.xhtml#page_441)–443

SQL injection, [254](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch6.xhtml#page_254)–259

web applications, [247](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch6.xhtml#page_247)–261

application-level rootkits, [217](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch5.xhtml#page_217)

applications

attacks on. *See* application-level attacks

executing, [210](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch5.xhtml#page_210)–211

fake security apps, [442](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch12.xhtml#page_442)

malicious, [442](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch12.xhtml#page_442)

mobile devices, [300](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch8.xhtml#page_300), [303](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch8.xhtml#page_303), [305](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch8.xhtml#page_305), [306](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch8.xhtml#page_306)

repackaging, [442](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch12.xhtml#page_442)

security, [229](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch6.xhtml#page_229)–231

APs. *See* access points

ARIN (American Registry for Internet Numbers), [68](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch2.xhtml#page_68), [72](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch2.xhtml#page_72), [73](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch2.xhtml#page_73)

Armitage, [210](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch5.xhtml#page_210)

ARO (annual rate of occurrence), [17](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_17)

ARP (Address Resolution Protocol), [10](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_10), [142](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch4.xhtml#page_142)–145, [278](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch7.xhtml#page_278)

ARP cache, [143](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch4.xhtml#page_143)–145

ARP entries, [144](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch4.xhtml#page_144)–145

ARP poisoning, [152](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch4.xhtml#page_152)–153, [205](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch5.xhtml#page_205)

ARP requests, [143](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch4.xhtml#page_143), [144](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch4.xhtml#page_144)–145

ARP spoofing, [152](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch4.xhtml#page_152)–153

ARPspoof tool, [153](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch4.xhtml#page_153)

AS (authentication service), [187](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch5.xhtml#page_187)

ASCII (American Standard Code for Information Interchange), [6](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_6)–7

Asia-Pacific Network Information Center (APNIC), [68](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch2.xhtml#page_68)

ASLR (address space layout randomization), [251](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch6.xhtml#page_251)

assets, [16](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_16), [443](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch12.xhtml#page_443)

association, [276](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch7.xhtml#page_276)

asymmetric encryption, [391](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch11.xhtml#page_391)–392

AtomSync, [124](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch3.xhtml#page_124)

attacks. *See also specific attacks*

access card attacks, [429](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch12.xhtml#page_429)

on applications. *See* application-level attacks

authentication, [18](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_18)

Bluetooth, [308](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch8.xhtml#page_308)–309

brute-force, [207](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch5.xhtml#page_207)–208, [416](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch11.xhtml#page_416), [417](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch11.xhtml#page_417)

categories, [26](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_26)–27

cipher-based, [416](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch11.xhtml#page_416)

collision, [395](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch11.xhtml#page_395)

cross-guest VM breach, [342](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch9.xhtml#page_342)

cross-site scripting, [251](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch6.xhtml#page_251)–253

cryptography, [415](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch11.xhtml#page_415)–417

DDoS, [260](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch6.xhtml#page_260), [365](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch10.xhtml#page_365)–368, [370](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch10.xhtml#page_370)

DNS, [64](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch2.xhtml#page_64)–66, [70](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch2.xhtml#page_70), [71](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch2.xhtml#page_71)

DoS, [20](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_20), [285](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch7.xhtml#page_285), [286](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch7.xhtml#page_286), [365](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch10.xhtml#page_365)–369

evil twin, [284](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch7.xhtml#page_284)–285

fraggle, [367](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch10.xhtml#page_367)

honeypots and, [171](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch4.xhtml#page_171)–173

injection, [229](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch6.xhtml#page_229), [249](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch6.xhtml#page_249)–250

interference, [416](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch11.xhtml#page_416)

IoT devices, [298](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch8.xhtml#page_298), [313](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch8.xhtml#page_313)–316

malware. *See* malware attacks

man-in-the-browser, [372](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch10.xhtml#page_372)

man-in-the-middle, [205](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch5.xhtml#page_205), [416](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch11.xhtml#page_416)

misconfiguration, [26](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_26)

mobile devices, [299](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch8.xhtml#page_299), [302](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch8.xhtml#page_302), [303](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch8.xhtml#page_303)–309

mobile platform, [281](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch7.xhtml#page_281), [441](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch12.xhtml#page_441)–443

on operating system, [26](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_26)

password. *See* password cracking

phishing. *See* phishing

plain-text, [415](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch11.xhtml#page_415)

replay, [416](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch11.xhtml#page_416)

session hijacking, [369](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch10.xhtml#page_369)–374

session riding, [342](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch9.xhtml#page_342)

shrink-wrap code, [26](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_26)

side-channel, [342](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch9.xhtml#page_342), [416](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch11.xhtml#page_416)

Smurf, [367](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch10.xhtml#page_367)

social engineering. *See* social engineering

source-routing, [112](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch3.xhtml#page_112)

stealth, [211](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch5.xhtml#page_211)–212, [216](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch5.xhtml#page_216)

SYN, [367](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch10.xhtml#page_367)

system. *See* system attacks

teardrop, [367](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch10.xhtml#page_367)

Trojan. *See* Trojans

viruses, [357](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch10.xhtml#page_357)–361, [363](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch10.xhtml#page_363)

web applications, [247](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch6.xhtml#page_247)–261

web servers, [233](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch6.xhtml#page_233)–235, [241](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch6.xhtml#page_241)–247

wireless. *See* wireless hacking

worms, [357](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch10.xhtml#page_357)–361

wrapping, [342](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch9.xhtml#page_342)

Attention Meter, [51](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch2.xhtml#page_51)

Auditpol tool, [216](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch5.xhtml#page_216)

authentication, [199](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch5.xhtml#page_199)–208

badges, [200](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch5.xhtml#page_200)

biometric, [199](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch5.xhtml#page_199)–200

*vs.* confidentiality, [18](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_18)

DES, [185](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch5.xhtml#page_185)

described, [276](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch7.xhtml#page_276)

IoT devices, [314](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch8.xhtml#page_314)

Kerberos, [185](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch5.xhtml#page_185), [187](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch5.xhtml#page_187)–189

LM, [187](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch5.xhtml#page_187)

mobile computing, [300](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch8.xhtml#page_300)

NTLM, [185](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch5.xhtml#page_185), [187](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch5.xhtml#page_187)

one-factor, [200](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch5.xhtml#page_200)

overview, [199](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch5.xhtml#page_199)–200

pre-boot, [408](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch11.xhtml#page_408)

three-factor, [200](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch5.xhtml#page_200)

two-factor, [200](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch5.xhtml#page_200)

web servers, [229](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch6.xhtml#page_229)

wireless networks, [276](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch7.xhtml#page_276)–277

authentication attacks, [18](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_18)

authentication header (AH), [373](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch10.xhtml#page_373), [410](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch11.xhtml#page_410)

authentication service (AS), [187](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch5.xhtml#page_187)

authenticity, [20](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_20)

authoritative servers, [64](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch2.xhtml#page_64)

authority support social engineering, [429](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch12.xhtml#page_429)

authorization, [301](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch8.xhtml#page_301), [314](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch8.xhtml#page_314), [335](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch9.xhtml#page_335)

AutoRuns, [356](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch10.xhtml#page_356)–357

AV (antivirus) programs. *See also virus entries*

fake AVprograms, [358](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch10.xhtml#page_358), [437](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch12.xhtml#page_437), [438](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch12.xhtml#page_438)–439

importance of, [363](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch10.xhtml#page_363)–364

malware attacks and, [350](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch10.xhtml#page_350)–352

AV signatures, [351](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch10.xhtml#page_351)

availability, [20](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_20)

AWS (Amazon Web Services), [72](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch2.xhtml#page_72), [330](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch9.xhtml#page_330), [331](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch9.xhtml#page_331), [332](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch9.xhtml#page_332)

AWS Greengrass, [332](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch9.xhtml#page_332)

Azure, [331](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch9.xhtml#page_331)

**B**

baby monitors, [315](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch8.xhtml#page_315)–316

backdoors. *See also* Trojans

leaving open, [29](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_29)

mobile computing, [301](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch8.xhtml#page_301)

Trojans and, [352](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch10.xhtml#page_352)–357

worms and, [362](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch10.xhtml#page_362)

backtracking, [242](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch6.xhtml#page_242)

backups, [16](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_16), [203](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch5.xhtml#page_203)

badges, [200](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch5.xhtml#page_200)

bandwidth, [366](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch10.xhtml#page_366)

banner grabbing, [96](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch3.xhtml#page_96), [120](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch3.xhtml#page_120)–121, [168](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch4.xhtml#page_168)

baselines, [23](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_23)

Bash, [247](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch6.xhtml#page_247)

Bashdoor, [247](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch6.xhtml#page_247)

Basic Encoding Rules (BER), [124](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch3.xhtml#page_124)

basic service area (BSA), [274](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch7.xhtml#page_274)

basic service set (BSS), [274](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch7.xhtml#page_274)

basic service set identifier (BSSID), [274](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch7.xhtml#page_274)

bastion hosts, [166](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch4.xhtml#page_166)

BBProxy, [309](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch8.xhtml#page_309)

BCP (business continuity plan), [17](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_17)

BER (Basic Encoding Rules), [124](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch3.xhtml#page_124)

beSTORM, [318](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch8.xhtml#page_318)

Beyond Trust tools, [318](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch8.xhtml#page_318)

BIA (business impact analysis), [17](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_17)

“big brother,” 396–397

binText tool, [363](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch10.xhtml#page_363)

biometric authentication, [199](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch5.xhtml#page_199)–200

biometric identifiers, [445](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch12.xhtml#page_445)–447

biometric passports, [200](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch5.xhtml#page_200)

biometrics, [445](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch12.xhtml#page_445)–447

BIOS rootkit, [217](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch5.xhtml#page_217), [218](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch5.xhtml#page_218)

bit flipping, [20](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_20)

bitcoin, [393](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch11.xhtml#page_393)

BitLocker, [408](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch11.xhtml#page_408)

bits

encrypted, [387](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch11.xhtml#page_387)–390

frames, [8](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_8)

salt, [396](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch11.xhtml#page_396)

subnetting and, [92](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch3.xhtml#page_92)–96

black hats, [25](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_25)

Black Widow tool, [234](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch6.xhtml#page_234)

Blackberry phones, [303](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch8.xhtml#page_303), [309](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch8.xhtml#page_309). *See also* mobile devices

black-box testing, [32](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_32)

Blackhole Exploit Kit, [352](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch10.xhtml#page_352)

blackjacking, [309](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch8.xhtml#page_309)

Bleeding Life, [352](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch10.xhtml#page_352)

blind/inferential injection, [259](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch6.xhtml#page_259)

block ciphers, [387](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch11.xhtml#page_387), [388](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch11.xhtml#page_388), [389](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch11.xhtml#page_389)–390

blockchain, [393](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch11.xhtml#page_393)–394

Bloover, [309](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch8.xhtml#page_309)

Blowfish encryption, [390](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch11.xhtml#page_390)

Blueborne attack, [316](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch8.xhtml#page_316)

Bluebugging, [309](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch8.xhtml#page_309)

Bluejacking, [309](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch8.xhtml#page_309)

Blueprinting, [309](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch8.xhtml#page_309)

BlueScanner, [309](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch8.xhtml#page_309)

Bluesmacking, [309](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch8.xhtml#page_309)

Bluesnarfing, [309](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch8.xhtml#page_309)

Bluesniffing, [309](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch8.xhtml#page_309)

Bluetooth

attacks, [308](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch8.xhtml#page_308)–309

devices, [307](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch8.xhtml#page_307), [308](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch8.xhtml#page_308)–309

hacking, [308](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch8.xhtml#page_308)–309

standard, [272](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch7.xhtml#page_272)

technology, [307](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch8.xhtml#page_307)

tools, [309](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch8.xhtml#page_309)

boot loader level rootkits, [217](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch5.xhtml#page_217)

boot sector viruses, [360](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch10.xhtml#page_360)

boot-n-root attack, [408](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch11.xhtml#page_408)

BootROM exploit, [304](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch8.xhtml#page_304)

botnets, [15](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_15), [260](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch6.xhtml#page_260)–261, [366](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch10.xhtml#page_366), [439](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch12.xhtml#page_439)

Brandon, John, [336](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch9.xhtml#page_336)

“bricking,” 367

Bring Your Own Device (BYOD), [299](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch8.xhtml#page_299), [302](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch8.xhtml#page_302), [305](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch8.xhtml#page_305)–306

broadcast, [146](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch4.xhtml#page_146), [147](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch4.xhtml#page_147)

broadcast addressing, [94](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch3.xhtml#page_94)

broadcast messages, [138](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch4.xhtml#page_138), [139](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch4.xhtml#page_139)

brute-force attacks, [207](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch5.xhtml#page_207)–208, [416](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch11.xhtml#page_416), [417](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch11.xhtml#page_417)

Brutus tool, [245](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch6.xhtml#page_245)

BSA (basic service area), [274](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch7.xhtml#page_274)

BSS (basic service set), [274](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch7.xhtml#page_274)

BSSID (basic service set identifier), [274](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch7.xhtml#page_274)

BT Browser, [309](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch8.xhtml#page_309)

btCrawler, [309](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch8.xhtml#page_309)

buffer overflows, [13](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_13), [251](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch6.xhtml#page_251)–253

Bug Bear worm, [361](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch10.xhtml#page_361)

bump key, [449](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch12.xhtml#page_449)

Burp Suite, [234](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch6.xhtml#page_234)

Buscador, [76](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch2.xhtml#page_76)

business continuity plan (BCP), [17](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_17)

business impact analysis (BIA), [17](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_17)

Business Wire, [51](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch2.xhtml#page_51)

BYOD (Bring Your Own Device), [299](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch8.xhtml#page_299), [302](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch8.xhtml#page_302), [305](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch8.xhtml#page_305)–306

**C**

CA (certificate authority), [391](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch11.xhtml#page_391), [400](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch11.xhtml#page_400)–402, [405](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch11.xhtml#page_405)–406

CAC (Common Access Card), [400](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch11.xhtml#page_400)

cache

ARP, [143](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch4.xhtml#page_143)–145

DNS, [65](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch2.xhtml#page_65), [66](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch2.xhtml#page_66), [67](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch2.xhtml#page_67), [71](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch2.xhtml#page_71)

Google Cache, [61](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch2.xhtml#page_61)

web cache poisoning, [244](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch6.xhtml#page_244)

Cain and Abel tool

ARP flooding, [153](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch4.xhtml#page_153)

MAC address spoofing, [153](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch4.xhtml#page_153)

sniffing passwords, [205](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch5.xhtml#page_205), [207](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch5.xhtml#page_207), [288](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch7.xhtml#page_288)

WEP attacks, [288](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch7.xhtml#page_288)

caller ID, [70](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch2.xhtml#page_70)

CAM (content addressable memory) table, [152](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch4.xhtml#page_152)

canaries, [251](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch6.xhtml#page_251)

canary words, [251](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch6.xhtml#page_251)

cantennas, [275](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch7.xhtml#page_275)

CAPTCHAs, [254](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch6.xhtml#page_254)

Carrier Sense Multiple Access/Collision Detection (CSMA/CD), [139](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch4.xhtml#page_139)–141

cars. *See* vehicles

cavity viruses, [361](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch10.xhtml#page_361)

CBC-MAC (cipher block chaining message authentication code), [279](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch7.xhtml#page_279)

CC (Common Criteria), [21](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_21)–22

CCMP (Cipher Block Chaining Message Authentication Code Protocol), [279](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch7.xhtml#page_279)

CCTT (Covert Channel Tunneling Trojan), [353](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch10.xhtml#page_353)

CEH (Certified Ethical Hacker) certification, [3](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_3), [29](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_29)

cell phones. *See* smartphones

Censys tool, [318](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch8.xhtml#page_318)

Centralized Authentication, [276](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch7.xhtml#page_276)

CER (crossover error rate), [200](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch5.xhtml#page_200), [446](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch12.xhtml#page_446)–447

certificate authority (CA), [391](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch11.xhtml#page_391), [400](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch11.xhtml#page_400)–402, [405](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch11.xhtml#page_405)–406

certificate revocation list (CRL), [400](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch11.xhtml#page_400)

certification tests, [29](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_29)

certification-level exams, [3](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_3)–5

Certified Ethical Hacker (CEH) certification, [3](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_3), [29](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_29)

chat channels, [439](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch12.xhtml#page_439)

chosen-cipher attacks, [415](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch11.xhtml#page_415), [416](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch11.xhtml#page_416)

chosen-plain text attacks, [415](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch11.xhtml#page_415)

Christmas scan, [102](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch3.xhtml#page_102), [105](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch3.xhtml#page_105), [106](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch3.xhtml#page_106)

Chrome browser, [414](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch11.xhtml#page_414)

CIA (Confidentiality, Integrity, and Availability), 18–20

cipher block chaining message authentication code (CBC-MAC), [279](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch7.xhtml#page_279)

Cipher Block Chaining Message Authentication Code Protocol (CCMP), [279](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch7.xhtml#page_279)

cipher text, [386](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch11.xhtml#page_386)

cipher types, [387](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch11.xhtml#page_387)–388

ciphers, [388](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch11.xhtml#page_388), [389](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch11.xhtml#page_389)

cipher-text-only attacks, [416](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch11.xhtml#page_416)

Cisco, [285](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch7.xhtml#page_285)

clients, [272](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch7.xhtml#page_272), [274](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch7.xhtml#page_274), [276](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch7.xhtml#page_276), [277](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch7.xhtml#page_277)

Cline, Ernest, [59](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch2.xhtml#page_59)

cloud auditors, [335](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch9.xhtml#page_335)

cloud brokers, [334](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch9.xhtml#page_334)

cloud carriers, [334](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch9.xhtml#page_334)

cloud computing, [329](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch9.xhtml#page_329)–348

architecture, [334](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch9.xhtml#page_334)–335

attacks/threats, [339](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch9.xhtml#page_339)–342

community clouds, [333](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch9.xhtml#page_333)

data breach/loss, [339](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch9.xhtml#page_339)

horror stories, [336](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch9.xhtml#page_336)–337

hybrid clouds, [333](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch9.xhtml#page_333)

IoT and, [314](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch8.xhtml#page_314)

overview, [330](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch9.xhtml#page_330)–332

public *vs.* private clouds, [333](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch9.xhtml#page_333)

regulatory efforts, [335](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch9.xhtml#page_335)

roles in, [334](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch9.xhtml#page_334)–335

security, [335](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch9.xhtml#page_335)–339

tools, [338](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch9.xhtml#page_338)–339

*Cloud Computing Guidelines,* 335

cloud consumers, [334](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch9.xhtml#page_334)

cloud, defined, [329](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch9.xhtml#page_329), [330](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch9.xhtml#page_330)

cloud models, [333](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch9.xhtml#page_333)–334

cloud providers, [331](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch9.xhtml#page_331)–332, [334](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch9.xhtml#page_334)

Cloud Security Alliance (CSA), [335](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch9.xhtml#page_335)

cloud services, [72](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch2.xhtml#page_72), [341](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch9.xhtml#page_341)

CloudInspect, [338](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch9.xhtml#page_338)

CloudPassage Halo, [338](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch9.xhtml#page_338)

Cloudshark, [320](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch8.xhtml#page_320)

cluster viruses, [360](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch10.xhtml#page_360)

COBIT (Control Objects for Information and Related Technology), [35](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_35), [36](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_36)

Code Red worm, [361](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch10.xhtml#page_361)

code/coding, [13](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_13), [243](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch6.xhtml#page_243), [301](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch8.xhtml#page_301)

Codenomicon, [413](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch11.xhtml#page_413)

collision attacks, [395](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch11.xhtml#page_395), [397](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch11.xhtml#page_397)

collision domains, [139](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch4.xhtml#page_139)–141, [150](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch4.xhtml#page_150)

collisions, [139](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch4.xhtml#page_139)–141, [395](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch11.xhtml#page_395)

command injection, [249](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch6.xhtml#page_249)

command shell Trojan, [353](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch10.xhtml#page_353)

Common Access Card (CAC), [400](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch11.xhtml#page_400)

Common Criteria (CC), [21](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_21)–22

Common Vulnerability Scoring System (CVSS), [12](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_12)

Communication Act of 1934, [286](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch7.xhtml#page_286)

Communications Decency Act, [37](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_37)–38

community cloud model, [333](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch9.xhtml#page_333)

community strings, [124](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch3.xhtml#page_124)

companies

competitive intelligence, [51](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch2.xhtml#page_51)–52, [76](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch2.xhtml#page_76)–77

financial information, [52](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch2.xhtml#page_52)

compliance, [35](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_35)

computer contaminant, [351](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch10.xhtml#page_351)

Computer Fraud and Abuse Act, [55](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch2.xhtml#page_55)

computer-based social engineering, [434](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch12.xhtml#page_434)–441

Conficker worm, [361](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch10.xhtml#page_361)

confidentiality, [18](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_18), [387](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch11.xhtml#page_387), [409](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch11.xhtml#page_409)

Confidentiality, Integrity, and Availability (CIA), [18](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_18)–20

CONNECT method, [240](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch6.xhtml#page_240)

connection string parameter pollution (CSPP), [245](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch6.xhtml#page_245)

connectionless communication, [85](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch3.xhtml#page_85)

connection-oriented communication, [84](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch3.xhtml#page_84)–88

content addressable memory (CAM) table, [152](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch4.xhtml#page_152)

Control Objects for Information and Related Technology (COBIT), [35](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_35), [36](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_36)

cookies, [60](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch2.xhtml#page_60), [115](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch3.xhtml#page_115), [205](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch5.xhtml#page_205), [252](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch6.xhtml#page_252), [253](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch6.xhtml#page_253)–254

copyrights, [37](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_37)–38

corrective controls, [16](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_16)

Covert Channel Tunneling Trojan (CCTT), [353](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch10.xhtml#page_353)

covert channels, [351](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch10.xhtml#page_351)

crackers, [25](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_25), [30](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_30)

cracking passwords. *See* password cracking

Crimepack, [352](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch10.xhtml#page_352)

criminal activity, [49](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch2.xhtml#page_49)

CRL (certificate revocation list), [400](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch11.xhtml#page_400)

cross-certification, [402](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch11.xhtml#page_402)

cross-guest VM breach, [342](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch9.xhtml#page_342)

crossover error rate (CER), [200](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch5.xhtml#page_200), [446](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch12.xhtml#page_446)–447

cross-site request forgery (CSRF), [253](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch6.xhtml#page_253)

cross-site scripting (XSS), [230](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch6.xhtml#page_230)

cryptanalysis, [386](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch11.xhtml#page_386)–387

crypters, [352](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch10.xhtml#page_352)

Cryptobench, [417](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch11.xhtml#page_417)

cryptographic systems, [387](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch11.xhtml#page_387)

cryptography, [385](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch11.xhtml#page_385)–424. *See also* encryption

algorithms/techniques, [387](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch11.xhtml#page_387)–399

defined, [386](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch11.xhtml#page_386)

digital certificates, [402](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch11.xhtml#page_402)–406

digital signatures, [391](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch11.xhtml#page_391), [406](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch11.xhtml#page_406)–407

encrypted communication, [407](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch11.xhtml#page_407)–415

history, [385](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch11.xhtml#page_385)–387

mobile devices, [300](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch8.xhtml#page_300)

overview, [386](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch11.xhtml#page_386)–399

PKI system, [399](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch11.xhtml#page_399)–407

cryptography attacks, [415](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch11.xhtml#page_415)–417

CrypTool, [388](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch11.xhtml#page_388), [417](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch11.xhtml#page_417)

CSA (Cloud Security Alliance), [335](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch9.xhtml#page_335)

CSMA/CD (Carrier Sense Multiple Access/Collision Detection), [139](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch4.xhtml#page_139)–141

CSPP (connection string parameter pollution), [245](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch6.xhtml#page_245)

CSRF (cross-site request forgery), [253](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch6.xhtml#page_253)

Currports tool, [90](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch3.xhtml#page_90)

CVSS (Common Vulnerability Scoring System), [12](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_12)

cyberterrorists, [26](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_26)

**D**

DAC (discretionary access control), [22](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_22)

daisy-chaining networks, [15](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_15)

DameWare Remote Support, [211](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch5.xhtml#page_211)

DAR (data at rest), [408](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch11.xhtml#page_408), [409](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch11.xhtml#page_409)

Dark Reading, [12](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_12)

Darlloz worm, [362](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch10.xhtml#page_362)

DAST (Dynamic Application Security Testing), [230](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch6.xhtml#page_230)

data. *See also* information

availability, [20](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_20)

backups, [16](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_16), [203](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch5.xhtml#page_203)

considerations, [6](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_6)–7

described, [7](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_7)

disclosure, [18](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_18)

encrypted. *See* encryption

handling of, [23](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_23)

at rest, [408](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch11.xhtml#page_408), [409](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch11.xhtml#page_409)

sensitive, [65](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch2.xhtml#page_65), [229](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch6.xhtml#page_229)

storage, [300](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch8.xhtml#page_300), [312](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch8.xhtml#page_312)

transfer/exchange, [85](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch3.xhtml#page_85)–87

data at rest (DAR), [408](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch11.xhtml#page_408), [409](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch11.xhtml#page_409)

data breach/loss, [339](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch9.xhtml#page_339)

Data Encryption Standard. *See* DES

data execution prevention (DEP), [251](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch6.xhtml#page_251)

data layers, [7](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_7)

Data Link layer, [6](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_6), [7](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_7), [138](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch4.xhtml#page_138), [142](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch4.xhtml#page_142)

database servers, [235](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch6.xhtml#page_235)

databases, [189](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch5.xhtml#page_189), [254](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch6.xhtml#page_254)–259

datagrams, [10](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_10), [85](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch3.xhtml#page_85)

DDoS attacks, [260](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch6.xhtml#page_260), [365](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch10.xhtml#page_365)–368, [370](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch10.xhtml#page_370)

Decrypting RSA with Obsolete and Weakened eNcryption (DROWN), [415](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch11.xhtml#page_415)

decryption, [278](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch7.xhtml#page_278), [282](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch7.xhtml#page_282), [386](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch11.xhtml#page_386), [388](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch11.xhtml#page_388)–392. *See also* encryption

decryption keys. *See* private keys

default vulnerabilities, [13](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_13)

defense in depth, [280](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch7.xhtml#page_280), [448](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch12.xhtml#page_448)

DELETE method, [240](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch6.xhtml#page_240)

demilitarized zone (DMZ), [11](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_11), [166](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch4.xhtml#page_166)

denial-of-service attacks (DoS), [20](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_20), [285](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch7.xhtml#page_285), [286](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch7.xhtml#page_286), [365](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch10.xhtml#page_365)–369

DEP (data execution prevention), [251](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch6.xhtml#page_251)

Department of Defense (DoD), [21](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_21), [22](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_22), [160](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch4.xhtml#page_160)

DES (Data Encryption Standard), [389](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch11.xhtml#page_389)

DES authentication, [185](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch5.xhtml#page_185)

deserialization flaws, [230](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch6.xhtml#page_230)

design flaws, [13](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_13)

detective controls, [16](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_16)

DHCP (Dynamic Host Configuration Protocol), [153](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch4.xhtml#page_153)–154

DHCP starvation, [153](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch4.xhtml#page_153)–154

dictionary attacks, [206](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch5.xhtml#page_206)–207

Diffie-Hellman algorithm, [373](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch10.xhtml#page_373), [392](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch11.xhtml#page_392)

dig command, [72](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch2.xhtml#page_72)

digital certificates, [402](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch11.xhtml#page_402)–406

Digital Signature Algorithm (DSA), [407](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch11.xhtml#page_407)

digital signatures, [391](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch11.xhtml#page_391), [406](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch11.xhtml#page_406)–407

digital watermarks, [398](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch11.xhtml#page_398)

dipole antenna, [275](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch7.xhtml#page_275)

directional antenna, [275](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch7.xhtml#page_275), [276](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch7.xhtml#page_276)

Directory System Agent (DSA), [124](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch3.xhtml#page_124)

directory traversal, [241](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch6.xhtml#page_241)–243

direct-sequence spread spectrum (DSSS), [273](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch7.xhtml#page_273)

disaster recovery, [17](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_17)

disaster recovery plan (DRP), [17](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_17)

disasters, [17](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_17), [448](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch12.xhtml#page_448)

discovery, [281](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch7.xhtml#page_281)–284

discretionary access control (DAC), [22](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_22)

disgruntled employees, [55](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch2.xhtml#page_55), [432](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch12.xhtml#page_432)–434

distributed reflection denial-of-service (DRDoS) attack, [366](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch10.xhtml#page_366)

distributed-denial-of-service attacks. *See* DDoS attacks

DLL hijacking, [209](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch5.xhtml#page_209)

DMZ (demilitarized zone), [11](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_11), [166](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch4.xhtml#page_166)

DNS (Domain Naming System)

basics, [63](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch2.xhtml#page_63)–72

cache, [63](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch2.xhtml#page_63)–66, [69](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch2.xhtml#page_69), [71](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch2.xhtml#page_71)

considerations, [9](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_9), [10](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_10)

for footprinting, [62](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch2.xhtml#page_62)–72

tools for, [62](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch2.xhtml#page_62)–72

DNS amplification, [241](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch6.xhtml#page_241)

DNS attacks, [64](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch2.xhtml#page_64)–66, [70](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch2.xhtml#page_70), [71](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch2.xhtml#page_71)

DNS lookups, [64](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch2.xhtml#page_64)–65, [66](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch2.xhtml#page_66)

DNS namespace, [63](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch2.xhtml#page_63)–66, [69](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch2.xhtml#page_69), [71](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch2.xhtml#page_71)

DNS poisoning, [65](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch2.xhtml#page_65), [66](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch2.xhtml#page_66), [71](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch2.xhtml#page_71), [155](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch4.xhtml#page_155)

DNS records, [50](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch2.xhtml#page_50), [62](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch2.xhtml#page_62), [63](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch2.xhtml#page_63), [65](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch2.xhtml#page_65)

DNS servers, [62](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch2.xhtml#page_62)–72, [284](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch7.xhtml#page_284)

DNS zone transfers, [63](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch2.xhtml#page_63), [71](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch2.xhtml#page_71)

DNSSEC (Domain Name System Security Extensions), [66](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch2.xhtml#page_66), [69](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch2.xhtml#page_69)

[dnsstuff.com](http://dnsstuff.com/), [78](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch2.xhtml#page_78)

DoD (Department of Defense), [21](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_21), [22](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_22), [160](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch4.xhtml#page_160)

domain controller, [187](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch5.xhtml#page_187)

Domain Name System Security Extensions (DNSSEC), [66](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch2.xhtml#page_66), [69](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch2.xhtml#page_69)

domain names, [68](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch2.xhtml#page_68)

Domain Naming System. *See* DNS

DoS (denial-of-service attacks), [20](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_20), [285](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch7.xhtml#page_285), [286](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch7.xhtml#page_286), [365](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch10.xhtml#page_365)–369

dot-dot-slash attack, [241](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch6.xhtml#page_241)–243

doxing, [15](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_15)

DRDoS (distributed reflection denial-of-service) attack, [366](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch10.xhtml#page_366)

drivers, [282](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch7.xhtml#page_282)

DROWN (Decrypting RSA with Obsolete and Weakened eNcryption), [415](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch11.xhtml#page_415)

DRP (disaster recovery plan), [17](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_17)

DSA (Digital Signature Algorithm), [407](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch11.xhtml#page_407)

DSA (Directory System Agent), [124](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch3.xhtml#page_124)

dsniff tool, [153](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch4.xhtml#page_153)

DSSS (direct-sequence spread spectrum), [273](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch7.xhtml#page_273)

DUHK attack, [395](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch11.xhtml#page_395)

dumpster diving, [50](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch2.xhtml#page_50), [51](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch2.xhtml#page_51), [52](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch2.xhtml#page_52), [201](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch5.xhtml#page_201), [428](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch12.xhtml#page_428)

dust, [444](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch12.xhtml#page_444)

DYLIB hijacking, [209](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch5.xhtml#page_209)

Dyn, [260](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch6.xhtml#page_260)

Dyn attack, [315](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch8.xhtml#page_315)–316

Dynamic Application Security Testing (DAST), [230](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch6.xhtml#page_230)

Dynamic Host Configuration Protocol. *See* DHCP

dynamic web pages, [248](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch6.xhtml#page_248)

**E**

EAL (Evaluation Assurance Level), [21](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_21)

EAP (Extensible Authentication Protocol), [278](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch7.xhtml#page_278)

Easter eggs, [59](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch2.xhtml#page_59)

eavesdropping, [137](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch4.xhtml#page_137), [138](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch4.xhtml#page_138). *See also* sniffing

ECC (Elliptic Curve Cryptosystem), [392](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch11.xhtml#page_392)

EC-Council (ECC), [4](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_4), [22](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_22), [23](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_23), [48](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch2.xhtml#page_48), [231](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch6.xhtml#page_231), [236](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch6.xhtml#page_236)

EDGAR Database, [51](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch2.xhtml#page_51)

edge computing networks, [331](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch9.xhtml#page_331)

EF (exposure factor), [17](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_17)

Effland, Charlie, [340](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch9.xhtml#page_340)

EFS (Encrypted File Systems), [410](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch11.xhtml#page_410)

EISA (Enterprise Information Security Architecture), [15](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_15)

El Gamal algorithm, [392](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch11.xhtml#page_392)

EliteWrap, [351](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch10.xhtml#page_351)

Elliptic Curve Cryptosystem (ECC), [392](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch11.xhtml#page_392)

e-mail

contact, [66](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch2.xhtml#page_66)

executable code in, [210](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch5.xhtml#page_210)

footprinting, [60](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch2.xhtml#page_60), [61](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch2.xhtml#page_61)–62

phishing, [202](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch5.xhtml#page_202), [435](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch12.xhtml#page_435)–438, [439](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch12.xhtml#page_439)

S/MIME and, [411](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch11.xhtml#page_411)

tracking tools, [61](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch2.xhtml#page_61)

e-mail headers, [61](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch2.xhtml#page_61), [62](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch2.xhtml#page_62)

e-mail policy, [23](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_23)

e-mail servers, [71](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch2.xhtml#page_71)

employees

disgruntled, [55](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch2.xhtml#page_55), [432](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch12.xhtml#page_432)–434

privilege escalation and, [33](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_33)

security policies, [23](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_23)

social engineering and, [427](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch12.xhtml#page_427)–434

Encapsulating Security Payload (ESP), [373](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch10.xhtml#page_373), [410](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch11.xhtml#page_410)

encrypted communication, [407](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch11.xhtml#page_407)–417

Encrypted File Systems (EFS), [410](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch11.xhtml#page_410)

encryption. *See also* cryptography

3DES, [389](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch11.xhtml#page_389)

AES, [390](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch11.xhtml#page_390)

algorithms, [387](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch11.xhtml#page_387)–398

asymmetric, [391](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch11.xhtml#page_391)–392

Blowfish, [390](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch11.xhtml#page_390)

cipher types, [387](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch11.xhtml#page_387)–388

data at rest, [408](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch11.xhtml#page_408), [409](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch11.xhtml#page_409)

data while communicating, [407](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch11.xhtml#page_407)–417

decryption, [278](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch7.xhtml#page_278), [282](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch7.xhtml#page_282), [386](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch11.xhtml#page_386), [388](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch11.xhtml#page_388)–392

DES, [389](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch11.xhtml#page_389)

digital certificates, [402](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch11.xhtml#page_402)–406

digital signatures, [406](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch11.xhtml#page_406)–407

Endpoint Encryption, [408](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch11.xhtml#page_408)

hash algorithms, [392](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch11.xhtml#page_392)–398

IDEA, [390](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch11.xhtml#page_390)

IoT devices, [314](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch8.xhtml#page_314)

key, [387](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch11.xhtml#page_387)–392

laptops, [408](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch11.xhtml#page_408)

mobile devices, [408](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch11.xhtml#page_408)

overview, [386](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch11.xhtml#page_386)–399

PKI system, [402](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch11.xhtml#page_402)

RC, [390](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch11.xhtml#page_390)

shared key, [389](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch11.xhtml#page_389)–390

single key, [389](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch11.xhtml#page_389), [391](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch11.xhtml#page_391)

steganography, [398](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch11.xhtml#page_398)–399

symmetric, [389](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch11.xhtml#page_389)–390

techniques, [387](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch11.xhtml#page_387)–399

tools for, [396](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch11.xhtml#page_396)

Twofish, [390](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch11.xhtml#page_390)

wireless networks, [277](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch7.xhtml#page_277)–280, [287](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch7.xhtml#page_287)–289

encryption keys. *See* public keys

encryption viruses, [360](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch10.xhtml#page_360)

Endpoint Encryption, [408](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch11.xhtml#page_408)

Enterprise Information Security Architecture (EISA), [15](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_15)

enumeration, [117](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch3.xhtml#page_117)–125

banner grabbing, [120](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch3.xhtml#page_120)–121

considerations, [117](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch3.xhtml#page_117)–125

described, [117](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch3.xhtml#page_117)

examples of, [28](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_28)

Linux systems, [119](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch3.xhtml#page_119)

NetBIOS, [121](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch3.xhtml#page_121)–123

other options, [124](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch3.xhtml#page_124)–125

SNMP, [123](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch3.xhtml#page_123)–124

techniques, [120](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch3.xhtml#page_120)–125

Windows systems, [117](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch3.xhtml#page_117)–119

e-passports, [200](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch5.xhtml#page_200)

escalation of privileges, [29](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_29), [33](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_33), [208](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch5.xhtml#page_208)–210

ESP (Encapsulating Security Payload), [373](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch10.xhtml#page_373), [410](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch11.xhtml#page_410)

ESS (extended service set), [274](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch7.xhtml#page_274)

Ethernet frames, [8](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_8)–11

ethical hackers, [18](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_18), [25](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_25), [30](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_30)–38

ethical hacking, [24](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_24)–38. *See also* hacking

attack types, [26](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_26)–27

classifications, [24](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_24)–26

considerations, [108](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch3.xhtml#page_108)

hacking phases, [27](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_27)–30

laws/standards, [33](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_33)–38

overview, [24](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_24)

terminology, [15](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_15), [24](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_24)–30

white hats, [25](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_25)

Ettercap sniffer, [159](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch4.xhtml#page_159), [205](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch5.xhtml#page_205)–206, [372](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch10.xhtml#page_372)

Euromonitor, [51](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch2.xhtml#page_51)

Evaluation Assurance Level (EAL), [21](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_21)

evasion, [159](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch4.xhtml#page_159)–173

firewalls, [165](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch4.xhtml#page_165)–167

intrusion detection systems. *See* IDS

overview, [159](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch4.xhtml#page_159)

via fragmentation, [168](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch4.xhtml#page_168)

event logs, [215](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch5.xhtml#page_215), [216](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch5.xhtml#page_216)

evil twin attack, [284](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch7.xhtml#page_284)–285

exam, [3](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_3)–5

exam tips, [4](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_4)–5

exclusive-or. *See* XOR

Experian, [51](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch2.xhtml#page_51)

Exploit Database, [12](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_12)

exploit kits, [352](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch10.xhtml#page_352)

exploits, [15](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_15)

exposure factor (EF), [17](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_17)

extended service set (ESS), [274](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch7.xhtml#page_274)

Extensible Authentication Protocol (EAP), [278](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch7.xhtml#page_278)

Extensible Markup Language (XML), [108](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch3.xhtml#page_108), [239](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch6.xhtml#page_239)

External Blue exploit, [358](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch10.xhtml#page_358), [360](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch10.xhtml#page_360)

**F**

FAA (Federal Aviation Administration), [286](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch7.xhtml#page_286)

Facebook, [52](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch2.xhtml#page_52), [55](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch2.xhtml#page_55), [434](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch12.xhtml#page_434)

Factoring Attack on RSA-EXPORT Keys (FREAK), [413](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch11.xhtml#page_413)

false acceptance rate (FAR), [200](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch5.xhtml#page_200), [446](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch12.xhtml#page_446)

false negatives, [160](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch4.xhtml#page_160)

false positives, [160](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch4.xhtml#page_160)

false rejection rate (FRR), [200](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch5.xhtml#page_200), [446](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch12.xhtml#page_446)

FAR (false acceptance rate), [200](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch5.xhtml#page_200), [446](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch12.xhtml#page_446)

FCC (Federal Communications Commission), [279](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch7.xhtml#page_279), [286](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch7.xhtml#page_286), [287](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch7.xhtml#page_287)

FCC ID, [287](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch7.xhtml#page_287)

FDE (full disk encryption), [408](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch11.xhtml#page_408)

Federal Aviation Administration (FAA), [286](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch7.xhtml#page_286)

Federal Communications Commission (FCC), [279](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch7.xhtml#page_279), [286](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch7.xhtml#page_286), [287](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch7.xhtml#page_287)

Federal Risk and Authorization Management Program (FedRAMP), [335](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch9.xhtml#page_335)

FedRAMP (Federal Risk and Authorization Management Program), [335](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch9.xhtml#page_335)

file extension viruses, [361](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch10.xhtml#page_361)

file injection, [249](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch6.xhtml#page_249)

file streaming, [212](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch5.xhtml#page_212)–213, [214](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch5.xhtml#page_214)

file system, [193](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch5.xhtml#page_193), [212](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch5.xhtml#page_212)–213, [410](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch11.xhtml#page_410)

File Transfer Protocol (FTP), [141](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch4.xhtml#page_141), [410](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch11.xhtml#page_410)

files

activity, [211](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch5.xhtml#page_211)–216

hiding, [211](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch5.xhtml#page_211)–214

hosts, [67](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch2.xhtml#page_67)

HTML, [239](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch6.xhtml#page_239)

log. *See* log files

SAM, [184](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch5.xhtml#page_184)–187, [188](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch5.xhtml#page_188)

shadow, [194](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch5.xhtml#page_194), [195](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch5.xhtml#page_195)–196

signature, [363](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch10.xhtml#page_363)–364

steganographic, [398](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch11.xhtml#page_398)–399

verifying integrity of, [356](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch10.xhtml#page_356)–357

filters, [157](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch4.xhtml#page_157)–158

FIN flag, [86](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch3.xhtml#page_86)

FIN scans, [102](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch3.xhtml#page_102)

finger tool, [119](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch3.xhtml#page_119)

fingerprinting, [96](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch3.xhtml#page_96), [107](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch3.xhtml#page_107)

Firewalk tool, [170](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch4.xhtml#page_170)

firewalking, [168](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch4.xhtml#page_168)–170

Firewall Informer, [168](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch4.xhtml#page_168)

firewalls

application-level, [167](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch4.xhtml#page_167)

banner grabbing and, [168](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch4.xhtml#page_168)

bastion hosts, [166](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch4.xhtml#page_166)

circuit-level, [167](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch4.xhtml#page_167)

evasion, [168](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch4.xhtml#page_168)–169

hacking tools, [168](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch4.xhtml#page_168)–170

implicit deny principle, [165](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch4.xhtml#page_165)

multi-homed, [166](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch4.xhtml#page_166)

overview, [165](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch4.xhtml#page_165)–167

packet-filtering, [166](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch4.xhtml#page_166)–167

rules, [165](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch4.xhtml#page_165)

Firmalyzer, [320](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch8.xhtml#page_320)

firmware, [217](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch5.xhtml#page_217), [218](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch5.xhtml#page_218), [315](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch8.xhtml#page_315)

firmware rootkits, [217](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch5.xhtml#page_217)

flow control, [6](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_6)

footprinting, [48](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch2.xhtml#page_48)–77

active, [49](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch2.xhtml#page_49), [52](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch2.xhtml#page_52)

anonymous, [49](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch2.xhtml#page_49)

benefits of, [49](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch2.xhtml#page_49)

considerations, [48](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch2.xhtml#page_48), [50](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch2.xhtml#page_50), [54](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch2.xhtml#page_54)–55

DNS, [62](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch2.xhtml#page_62)–72

dumpster diving, [428](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch12.xhtml#page_428)

e-mail, [60](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch2.xhtml#page_60), [61](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch2.xhtml#page_61)–62

methods/tools, [53](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch2.xhtml#page_53)–77

network, [72](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch2.xhtml#page_72)–75

overview, [48](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch2.xhtml#page_48)–50

passive, [49](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch2.xhtml#page_49), [50](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch2.xhtml#page_50)–52

pseudonymous, [49](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch2.xhtml#page_49)

*vs.* reconnaissance, [48](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch2.xhtml#page_48)

*vs.* scanning, [84](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch3.xhtml#page_84)

search engines, [53](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch2.xhtml#page_53)–60

social engineering and, [51](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch2.xhtml#page_51), [52](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch2.xhtml#page_52)

web mirroring, [60](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch2.xhtml#page_60)

web servers, [233](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch6.xhtml#page_233)–234

web spiders, [54](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch2.xhtml#page_54), [76](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch2.xhtml#page_76)

website, [60](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch2.xhtml#page_60)–61

Fport tool, [356](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch10.xhtml#page_356)

fraggle attacks, [367](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch10.xhtml#page_367)

fragmentation, [103](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch3.xhtml#page_103), [111](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch3.xhtml#page_111), [168](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch4.xhtml#page_168)

fragmentation attacks, [366](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch10.xhtml#page_366)

fragmented packets, [111](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch3.xhtml#page_111)–112, [366](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch10.xhtml#page_366)

frames, [6](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_6), [10](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_10), [84](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch3.xhtml#page_84)

FREAK (Factoring Attack on RSA-EXPORT Keys), [413](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch11.xhtml#page_413)

FreeScan, [116](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch3.xhtml#page_116)–117

FRR (false rejection rate), [200](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch5.xhtml#page_200), [446](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch12.xhtml#page_446)

FTP (File Transfer Protocol), [141](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch4.xhtml#page_141), [410](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch11.xhtml#page_410)

fud (fully undetectable), [352](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch10.xhtml#page_352)

full connect scan, [101](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch3.xhtml#page_101), [105](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch3.xhtml#page_105)

full disk encryption (FDE), [408](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch11.xhtml#page_408)

full open scan, [101](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch3.xhtml#page_101)

functionality, [14](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_14)

fuzz testing, [257](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch6.xhtml#page_257)

**G**

GAK (government access to keys), [397](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch11.xhtml#page_397)

GET method, [240](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch6.xhtml#page_240)

GFI Languard, [14](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_14)

Ghost Eye Worm, [361](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch10.xhtml#page_361)

GIDs (group IDs), [119](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch3.xhtml#page_119)

Gigabit Wi-Fi, [279](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch7.xhtml#page_279)

Gilisoft Full Disk Encryption, [408](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch11.xhtml#page_408)

Gizmodo, [319](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch8.xhtml#page_319)

Google

Chrome browser, [414](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch11.xhtml#page_414)

cookies, [115](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch3.xhtml#page_115)

growth of, [331](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch9.xhtml#page_331)

Heartbleed exploit, [412](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch11.xhtml#page_412), [413](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch11.xhtml#page_413)

IoT hacking and, [317](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch8.xhtml#page_317)

OpenSSL and, [412](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch11.xhtml#page_412)

Google Cache, [61](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch2.xhtml#page_61)

Google CAPTCHA, [58](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch2.xhtml#page_58)

Google hacking, [55](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch2.xhtml#page_55)–60

Google search queries, [59](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch2.xhtml#page_59)–60

Google servers, [414](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch11.xhtml#page_414)

government access to keys (GAK), [397](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch11.xhtml#page_397)

GPS devices, [283](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch7.xhtml#page_283), [284](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch7.xhtml#page_284)

gray hats, [25](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_25)

gray-box testing, [33](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_33)

Grayfish rootkit, [217](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch5.xhtml#page_217)

the Great Firewall, [114](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch3.xhtml#page_114)

group IDs (GIDs), [119](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch3.xhtml#page_119)

Guardster, [115](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch3.xhtml#page_115)

guidelines, [23](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_23)

Gzapper, [115](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch3.xhtml#page_115)

**H**

hack value, [14](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_14)

hackers. *See also* pen testers

Anonymous, [369](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch10.xhtml#page_369)–370

black hats, [25](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_25)

classifications, [24](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_24)–26

considerations, [29](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_29), [30](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_30)

crackers, [25](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_25), [30](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_30)

described, [24](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_24)

ethical. *See* ethical hackers

favorite tools, [77](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch2.xhtml#page_77)

good *vs.* bad, [30](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_30)

gray hats, [25](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_25)

honeypots, [171](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch4.xhtml#page_171)–173

IDS evasion, [161](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch4.xhtml#page_161)

interview with, [161](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch4.xhtml#page_161)–162

malicious, [30](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_30)

*vs.* pen testers, [29](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_29)

script kiddies, [24](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_24), [26](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_26)

state-sponsored, [26](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_26)

suicide hackers, [25](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_25)

tips on, [161](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch4.xhtml#page_161)–162

white hats, [25](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_25)

Hackerstorm, [12](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_12)

hacking, [199](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch5.xhtml#page_199)–218. *See also* pen testing

Bluetooth, [308](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch8.xhtml#page_308)–309

Computer Fraud and Abuse Act, [55](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch2.xhtml#page_55)

considerations, [24](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_24), [25](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_25)

covering tracks, [29](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_29)

covering/clearing tracks, [198](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch5.xhtml#page_198), [199](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch5.xhtml#page_199), [215](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch5.xhtml#page_215)–216

ethical. *See* ethical hacking

gaining access, [28](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_28), [197](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch5.xhtml#page_197)–198

good *vs.* bad, [24](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_24), [25](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_25)

Google hacking, [55](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch2.xhtml#page_55)–60

IoT devices, [317](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch8.xhtml#page_317)–320

learning about, [232](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch6.xhtml#page_232)–233

Linux. *See* Linux systems

maintaining access, [29](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_29), [197](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch5.xhtml#page_197), [198](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch5.xhtml#page_198), [199](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch5.xhtml#page_199)

mobile devices, [299](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch8.xhtml#page_299), [302](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch8.xhtml#page_302), [307](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch8.xhtml#page_307)–309

*vs.* pen testing, [53](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch2.xhtml#page_53)

phases of, [27](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_27)–30, [197](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch5.xhtml#page_197)–199

privilege escalation, [29](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_29), [33](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_33), [208](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch5.xhtml#page_208)–210

reconnaissance. *See* reconnaissance

system. *See* system attacks

terminology, [15](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_15), [24](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_24)–30

web-based. *See* web-based hacking

Windows. *See* Windows systems

wireless. *See* wireless hacking

HackRF. *See* vehicles

hacktivists/hacktivism, [25](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_25), [370](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch10.xhtml#page_370)

half-open scan, [102](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch3.xhtml#page_102)

halo effect, [430](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch12.xhtml#page_430)

hardware protocol analyzers, [141](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch4.xhtml#page_141)

hardware rootkits, [217](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch5.xhtml#page_217)

hash algorithms, [392](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch11.xhtml#page_392)–398

hash functions, [20](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_20)

hash injection attacks, [202](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch5.xhtml#page_202)

hash values, [20](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_20), [185](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch5.xhtml#page_185), [186](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch5.xhtml#page_186), [187](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch5.xhtml#page_187)

hashes, [20](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_20), [447](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch12.xhtml#page_447)

hashing passwords, [185](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch5.xhtml#page_185)–189

Havij scanner, [259](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch6.xhtml#page_259)

HBSS (Host Based Security System), [160](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch4.xhtml#page_160)

HEAD method, [240](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch6.xhtml#page_240)

headers, [60](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch2.xhtml#page_60)

Health Insurance Portability and Accountability Act (HIPAA), [35](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_35)

heap overflow, [251](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch6.xhtml#page_251)

Heartbleed exploit, [411](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch11.xhtml#page_411), [412](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch11.xhtml#page_412)–413, [414](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch11.xhtml#page_414)

HFS file system, [212](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch5.xhtml#page_212)

hidden field, [243](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch6.xhtml#page_243)–244

HIDS (host-based IDS), [98](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch3.xhtml#page_98)–99, [160](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch4.xhtml#page_160)

hierarchical trust system, [402](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch11.xhtml#page_402)

hijacking, [369](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch10.xhtml#page_369)

hijacking sessions, [369](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch10.xhtml#page_369)–374

HIPAA (Health Insurance Portability and Accountability Act), [35](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_35)

Hoare, Greg, [341](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch9.xhtml#page_341)

Honeynet, [260](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch6.xhtml#page_260)

honeypots, [171](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch4.xhtml#page_171)–173, [232](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch6.xhtml#page_232), [260](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch6.xhtml#page_260)

honeyspot attacks, [285](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch7.xhtml#page_285)

Hoovers, [51](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch2.xhtml#page_51)

Horsepill rootkit, [217](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch5.xhtml#page_217)

Host Based Security System (HBSS), [160](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch4.xhtml#page_160)

host ID, [92](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch3.xhtml#page_92), [93](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch3.xhtml#page_93)

host-based IDS (HIDS), [98](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch3.xhtml#page_98)–99, [160](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch4.xhtml#page_160)

hosts file, [67](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch2.xhtml#page_67)

hotspots, [285](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch7.xhtml#page_285)

Hping, [109](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch3.xhtml#page_109), [110](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch3.xhtml#page_110)

HTML code, [60](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch2.xhtml#page_60), [235](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch6.xhtml#page_235), [239](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch6.xhtml#page_239), [243](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch6.xhtml#page_243)

HTML entities, [239](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch6.xhtml#page_239), [252](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch6.xhtml#page_252)

HTML files, [239](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch6.xhtml#page_239)

HTTP (Hypertext Transfer Protocol), [142](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch4.xhtml#page_142), [238](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch6.xhtml#page_238)–241

HTTP attacks, [259](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch6.xhtml#page_259)

HTTP beacons, [167](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch4.xhtml#page_167)

HTTP requests, [9](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_9), [238](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch6.xhtml#page_238)–240, [242](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch6.xhtml#page_242), [244](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch6.xhtml#page_244)

HTTP response messages, [241](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch6.xhtml#page_241)

HTTP response splitting, [259](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch6.xhtml#page_259)

HTTP shell, [167](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch4.xhtml#page_167)

HTTP tunneling, [167](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch4.xhtml#page_167)

HTTPRecon, [233](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch6.xhtml#page_233)

HTTPrint, [233](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch6.xhtml#page_233)

HTTPS servers, [415](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch11.xhtml#page_415)

hubs, [141](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch4.xhtml#page_141), [150](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch4.xhtml#page_150), [151](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch4.xhtml#page_151), [278](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch7.xhtml#page_278)

human-based social engineering, [427](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch12.xhtml#page_427)–434

humidity, [444](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch12.xhtml#page_444)

Hunt tool, [372](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch10.xhtml#page_372)

Hutchins, Marcus, [359](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch10.xhtml#page_359)

HVAC attacks, [316](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch8.xhtml#page_316)

hybrid cloud model, [333](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch9.xhtml#page_333)

Hyena, [123](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch3.xhtml#page_123)

hyperlinks, [238](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch6.xhtml#page_238)

hypertext, [238](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch6.xhtml#page_238)

Hypertext Transfer Protocol. *See* HTTP

hypervisor level rootkits, [217](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch5.xhtml#page_217)

hypervisors, [332](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch9.xhtml#page_332), [337](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch9.xhtml#page_337)

**I**

IaaS (Infrastructure as a Service), [332](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch9.xhtml#page_332)

IANA (Internet Assigned Number Authority), [68](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch2.xhtml#page_68), [89](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch3.xhtml#page_89)

iBoot exploit, [304](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch8.xhtml#page_304)

ICANN (Internet Corporation for Assigned Names and Numbers), [68](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch2.xhtml#page_68)

ICMP (Internet Control Message Protocol), [97](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch3.xhtml#page_97)–98, [99](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch3.xhtml#page_99)

ICMP Echo scanning, [98](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch3.xhtml#page_98)

ICMP floods, [367](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch10.xhtml#page_367)

ICMP message types, [97](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch3.xhtml#page_97)–98

ICMP packets, [98](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch3.xhtml#page_98), [99](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch3.xhtml#page_99), [100](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch3.xhtml#page_100), [367](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch10.xhtml#page_367)

ICMP requests, [74](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch2.xhtml#page_74), [75](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch2.xhtml#page_75)

ICQ (Internet Chat Query), [366](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch10.xhtml#page_366)

ICV (integrity check value), [278](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch7.xhtml#page_278)

ID badges, [429](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch12.xhtml#page_429)

ID Serve, [233](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch6.xhtml#page_233)

IDA Pro, [363](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch10.xhtml#page_363)

IDEA (International Data Encryption Algorithm), [390](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch11.xhtml#page_390)

identity theft, [429](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch12.xhtml#page_429)–430, [440](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch12.xhtml#page_440)–441

IDLE scan, [102](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch3.xhtml#page_102), [103](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch3.xhtml#page_103)–104

IDSInformer tool, [168](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch4.xhtml#page_168)

IDSs (intrusion detection systems), [159](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch4.xhtml#page_159)–168

anomaly-based, [160](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch4.xhtml#page_160)

behavior-based, [17](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_17), [160](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch4.xhtml#page_160)

considerations, [160](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch4.xhtml#page_160)–161

evasion issues, [96](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch3.xhtml#page_96), [161](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch4.xhtml#page_161)

evasion techniques, [167](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch4.xhtml#page_167)–173

host-based, [98](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch3.xhtml#page_98)–99, [160](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch4.xhtml#page_160)

network-based, [98](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch3.xhtml#page_98)–99, [160](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch4.xhtml#page_160)–161, [162](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch4.xhtml#page_162)

overview, [159](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch4.xhtml#page_159)–161

signature-based, [160](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch4.xhtml#page_160)

Snort, [161](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch4.xhtml#page_161)–165

Unicode characters and, [168](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch4.xhtml#page_168)

IEFT (Internet Engineering Task Force), [228](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch6.xhtml#page_228)

IIS (Internet Information Services) servers, [235](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch6.xhtml#page_235)–236, [237](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch6.xhtml#page_237), [238](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch6.xhtml#page_238)

IKE (Internet Key Exchange), [373](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch10.xhtml#page_373)

IMAP, [142](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch4.xhtml#page_142)

impersonation, [428](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch12.xhtml#page_428)–429

implicit deny principle, [165](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch4.xhtml#page_165)

in-band SQL injection, [258](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch6.xhtml#page_258)

incident management, [15](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_15)

incident response team (IRT), [15](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_15)

Infinity, [352](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch10.xhtml#page_352)

information. *See* data

Information Audit Policy, [23](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_23)

information gathering

company websites, [51](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch2.xhtml#page_51)–52

competitive intelligence, [51](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch2.xhtml#page_51)–52, [76](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch2.xhtml#page_76)–77

dumpster diving, [428](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch12.xhtml#page_428)

job boards, [54](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch2.xhtml#page_54)

shredded documents, [428](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch12.xhtml#page_428)

social networking sites, [52](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch2.xhtml#page_52), [55](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch2.xhtml#page_55)

web-based hacking, [233](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch6.xhtml#page_233)–234

Information Protection Policy, [23](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_23)

Information Security Policy, [23](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_23)

Information Systems Audit and Control Association (ISACA), [36](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_36)

information technology. *See* IT

infowar, [27](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_27)

Infrastructure as a Service (IaaS), [332](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch9.xhtml#page_332)

infrastructure mode, [274](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch7.xhtml#page_274)

initial sequence number (ISN), [371](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch10.xhtml#page_371)

initialization vector (IV), [278](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch7.xhtml#page_278)

injection attacks, [229](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch6.xhtml#page_229), [245](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch6.xhtml#page_245), [249](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch6.xhtml#page_249)–250

insider threats, [432](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch12.xhtml#page_432)–434

installation vulnerabilities, [13](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_13)

integrity, [20](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_20), [314](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch8.xhtml#page_314)

integrity check value (ICV), [278](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch7.xhtml#page_278)

interference attacks, [416](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch11.xhtml#page_416)

International Data Encryption Algorithm (IDEA), [390](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch11.xhtml#page_390)

International Telecommunications Union (ITU), [280](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch7.xhtml#page_280), [313](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch8.xhtml#page_313)

Internet Assigned Number Authority (IANA), [68](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch2.xhtml#page_68), [89](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch3.xhtml#page_89)

Internet Chat Query (ICQ), [366](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch10.xhtml#page_366)

Internet Control Message Protocol. *See* ICMP

Internet Corporation for Assigned Names and Numbers (ICANN), [68](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch2.xhtml#page_68)

Internet DMZ zone, [11](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_11)

Internet Engineering Task Force (IEFT), [228](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch6.xhtml#page_228)

Internet Information Services (IIS) servers, [235](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch6.xhtml#page_235)–236, [237](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch6.xhtml#page_237), [238](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch6.xhtml#page_238)

Internet Key Exchange (IKE), [373](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch10.xhtml#page_373)

Internet of Things. *See* IoT

The Internet of Useless Things, [319](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch8.xhtml#page_319)

Internet Protocol. *See* IP

Internet Protocol Security (IPSec), [410](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch11.xhtml#page_410)

Internet Relay Chat. *See* IRC

Internet Security Association Key Management Protocol, [373](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch10.xhtml#page_373)

Internet service providers (ISPs), [37](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_37), [369](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch10.xhtml#page_369)

Internet zone, [10](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_10)

intranet zone, [12](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_12)

intrusion detection systems. *See* IDSs

inverse TCP flag, [102](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch3.xhtml#page_102)

iOS, [303](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch8.xhtml#page_303)–304, [305](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch8.xhtml#page_305). *See also* mobile devices

IoT (Internet of Things), [309](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch8.xhtml#page_309)–320

architecture, [310](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch8.xhtml#page_310)–313

authorization/authentication, [314](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch8.xhtml#page_314)

communication models, [312](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch8.xhtml#page_312)

considerations, [310](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch8.xhtml#page_310), [311](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch8.xhtml#page_311), [313](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch8.xhtml#page_313), [319](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch8.xhtml#page_319)

data storage, [312](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch8.xhtml#page_312)

encryption, [314](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch8.xhtml#page_314)

hacking methodology, [317](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch8.xhtml#page_317)–320

HVAC attacks, [316](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch8.xhtml#page_316)

insecure communication, [314](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch8.xhtml#page_314)

overview, [297](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch8.xhtml#page_297)–298, [309](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch8.xhtml#page_309)–310

privacy issues, [314](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch8.xhtml#page_314)

security issues, [313](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch8.xhtml#page_313)–316

software/firmware issues, [315](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch8.xhtml#page_315)

vehicles, [312](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch8.xhtml#page_312), [316](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch8.xhtml#page_316)

vulnerabilities/attacks, [298](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch8.xhtml#page_298), [313](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch8.xhtml#page_313)–316

vulnerability scanning, [318](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch8.xhtml#page_318)–320

IoT devices, [316](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch8.xhtml#page_316)–320

attacks on, [298](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch8.xhtml#page_298), [313](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch8.xhtml#page_313)–316

baby monitors, [315](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch8.xhtml#page_315)–316

hacking, [317](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch8.xhtml#page_317)–320

overview, [309](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch8.xhtml#page_309)–310

requirements for, [311](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch8.xhtml#page_311)–312

thermostats, [311](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch8.xhtml#page_311)

vulnerabilities, [298](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch8.xhtml#page_298), [313](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch8.xhtml#page_313)–316

IoT gateway, [312](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch8.xhtml#page_312)

IoT networks, [310](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch8.xhtml#page_310), [314](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch8.xhtml#page_314), [316](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch8.xhtml#page_316)

IP (Internet Protocol), [142](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch4.xhtml#page_142)

IP Address Decoy, [112](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch3.xhtml#page_112)

IP addresses

broadcast, [92](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch3.xhtml#page_92)

described, [92](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch3.xhtml#page_92)

directed broadcast, [94](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch3.xhtml#page_94)

DNS and, [9](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_9), [10](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_10), [68](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch2.xhtml#page_68)

fragmented, [103](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch3.xhtml#page_103)

limited broadcast, [94](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch3.xhtml#page_94)

multicast, [92](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch3.xhtml#page_92)

network range, [72](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch2.xhtml#page_72)–73

rules, [93](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch3.xhtml#page_93)

spoofing, [103](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch3.xhtml#page_103), [112](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch3.xhtml#page_112)

unicast, [92](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch3.xhtml#page_92)

IP communication, [373](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch10.xhtml#page_373)

IP identifier (IPID), [103](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch3.xhtml#page_103)

IP packet header, [142](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch4.xhtml#page_142)

IP packets, [9](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_9)–10, [103](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch3.xhtml#page_103)

IP version 4. *See* IPv4

IP version 6 (IPv6), [145](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch4.xhtml#page_145)–147

iPhones. *See also* mobile devices

applications, [300](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch8.xhtml#page_300), [303](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch8.xhtml#page_303), [305](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch8.xhtml#page_305), [306](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch8.xhtml#page_306)

iOS, [303](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch8.xhtml#page_303)–304, [305](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch8.xhtml#page_305). *See also* mobile devices

jailbreaking, [303](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch8.xhtml#page_303)–304, [305](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch8.xhtml#page_305)

IPID (IP identifier), [103](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch3.xhtml#page_103)

iPods, [303](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch8.xhtml#page_303)

IPSec (Internet Protocol Security), [373](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch10.xhtml#page_373), [410](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch11.xhtml#page_410)

IPSec shell, [373](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch10.xhtml#page_373)

IPv4 (IP version 4), [145](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch4.xhtml#page_145)–147

IPv4 address depletion, [145](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch4.xhtml#page_145)

IPv4 addresses, [92](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch3.xhtml#page_92)

IPv4 loopback address, [138](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch4.xhtml#page_138)

IPv6 (IP version 6), [143](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch4.xhtml#page_143)–145

Iran nuclear worm, [362](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch10.xhtml#page_362)–363

IRC (Internet Relay Chat), [362](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch10.xhtml#page_362), [366](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch10.xhtml#page_366), [439](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch12.xhtml#page_439)

IRC channel, [351](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch10.xhtml#page_351)

IRDP spoofing, [155](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch4.xhtml#page_155)

IRT (incident response team), [15](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_15)

ISACA (Information Systems Audit and Control Association), [36](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_36)

ISN (initial sequence number), [371](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch10.xhtml#page_371)

ISO/IEC, [35](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_35)

ISPs (Internet service providers), [37](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_37), [369](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch10.xhtml#page_369)

IT Governance Institute (ITGI), [36](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_36)

ITGI (IT Governance Institute), [36](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_36)

ITU (International Telecommunications Union), [280](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch7.xhtml#page_280), [313](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch8.xhtml#page_313)

IV (initialization vector), [278](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch7.xhtml#page_278)

**J**

jailbreaking, [303](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch8.xhtml#page_303)–304, [305](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch8.xhtml#page_305)

jamming devices, [285](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch7.xhtml#page_285)–287

Java, [438](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch12.xhtml#page_438)–439

JavaScript, [252](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch6.xhtml#page_252)

job boards, [54](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch2.xhtml#page_54)

John the Ripper, [197](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch5.xhtml#page_197), [208](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch5.xhtml#page_208)

JTAGulator, [320](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch8.xhtml#page_320)

JXplorer, [124](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch3.xhtml#page_124)

**K**

Kaminsky, Dan, [66](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch2.xhtml#page_66)

KDC (key distribution center), [187](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch5.xhtml#page_187)

KerbCrack, [206](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch5.xhtml#page_206)

Kerberos authentication, [185](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch5.xhtml#page_185), [187](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch5.xhtml#page_187)–189

kernel-level rootkits, [217](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch5.xhtml#page_217)

key distribution, [389](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch11.xhtml#page_389), [390](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch11.xhtml#page_390), [392](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch11.xhtml#page_392)

network, [276](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch7.xhtml#page_276)–280

key distribution center (KDC), [187](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch5.xhtml#page_187)

key encryption, [387](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch11.xhtml#page_387)–392

key escrow, [397](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch11.xhtml#page_397)

key generation, [399](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch11.xhtml#page_399)

key pairs, [389](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch11.xhtml#page_389), [391](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch11.xhtml#page_391), [400](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch11.xhtml#page_400)

Key Reinstallation Attack (KRACK), [288](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch7.xhtml#page_288)–289

key sets, [399](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch11.xhtml#page_399)

keyboard walks, [201](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch5.xhtml#page_201)

keyloggers, [202](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch5.xhtml#page_202)

keylogging, [202](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch5.xhtml#page_202)

keys

government access to, [396](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch11.xhtml#page_396)–397

length, [389](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch11.xhtml#page_389), [390](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch11.xhtml#page_390), [392](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch11.xhtml#page_392), [413](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch11.xhtml#page_413)

private. *See* private keys

public. *See* public keys

registry, [189](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch5.xhtml#page_189)–190

shared, [276](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch7.xhtml#page_276)–277

symmetric encryption, [389](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch11.xhtml#page_389)–390

temporal, [288](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch7.xhtml#page_288)

WEP, [277](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch7.xhtml#page_277), [278](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch7.xhtml#page_278)

WPA2, [288](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch7.xhtml#page_288)–289

keystream, [278](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch7.xhtml#page_278)

KicMAC, [280](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch7.xhtml#page_280)

KillerBee, [320](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch8.xhtml#page_320)

KisMAC, [288](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch7.xhtml#page_288)

Kismet, [283](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch7.xhtml#page_283), [289](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch7.xhtml#page_289)

KRACK (Key Reinstallation Attack), [288](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch7.xhtml#page_288)–289

**L**

L0phtcrack tool, [208](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch5.xhtml#page_208)

LACNIC (Latin America and Caribbean Network Information Center), [68](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch2.xhtml#page_68)

LAND attack, [367](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch10.xhtml#page_367)

laptop computers, [408](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch11.xhtml#page_408)

Latin America and Caribbean Network Information Center (LACNIC), [68](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch2.xhtml#page_68)

lawful interception, [148](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch4.xhtml#page_148)

laws/standards, [33](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_33)–38

LC5 tool, [208](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch5.xhtml#page_208)

LDAP (Lightweight Directory Access Protocol), [124](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch3.xhtml#page_124)

LDAP Admin Tool, [124](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch3.xhtml#page_124)

LDAP injection attacks, [249](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch6.xhtml#page_249)–250

Legion tool, [204](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch5.xhtml#page_204)

LexisNexis, [51](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch2.xhtml#page_51)

libpcap, [139](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch4.xhtml#page_139)

library-level rootkits, [217](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch5.xhtml#page_217)

libwhisker, [160](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch4.xhtml#page_160)

Licklider, J.C.R., [330](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch9.xhtml#page_330)

Lightweight Directory Access Protocol. *See* LDAP

LinkedIn, [53](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch2.xhtml#page_53), [55](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch2.xhtml#page_55), [434](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch12.xhtml#page_434)

Linux root, [193](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch5.xhtml#page_193)

Linux servers, [193](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch5.xhtml#page_193)

Linux systems

basic commands, [195](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch5.xhtml#page_195)

enumeration, [119](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch3.xhtml#page_119)

file structure, [193](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch5.xhtml#page_193)–194

file system, [193](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch5.xhtml#page_193)

hacking, [195](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch5.xhtml#page_195)–197

navigating, [195](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch5.xhtml#page_195)

passwords, [194](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch5.xhtml#page_194), [195](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch5.xhtml#page_195), [196](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch5.xhtml#page_196)–197

security, [193](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch5.xhtml#page_193)–197

users/groups, [119](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch3.xhtml#page_119)

*vs.* Windows systems, [191](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch5.xhtml#page_191)–192

list scans, [98](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch3.xhtml#page_98)

“live” systems, [96](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch3.xhtml#page_96)

LLMNR attacks, [203](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch5.xhtml#page_203), [204](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch5.xhtml#page_204)

Lloyd, Kris, [341](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch9.xhtml#page_341)

LM authentication, [187](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch5.xhtml#page_187)

LM hashing, [186](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch5.xhtml#page_186)

locks, [443](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch12.xhtml#page_443), [445](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch12.xhtml#page_445), [447](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch12.xhtml#page_447), [449](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch12.xhtml#page_449)

Locky, [360](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch10.xhtml#page_360)

log files

application logs, [215](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch5.xhtml#page_215)

considerations, [29](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_29), [215](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch5.xhtml#page_215)

corrupting, [29](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_29), [215](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch5.xhtml#page_215)

covering/clearing tracks, [198](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch5.xhtml#page_198), [199](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch5.xhtml#page_199), [215](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch5.xhtml#page_215)–216

deleting, [29](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_29)

event logs, [215](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch5.xhtml#page_215), [216](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch5.xhtml#page_216)

location of, [215](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch5.xhtml#page_215)–216

monitoring, [215](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch5.xhtml#page_215)

security logs, [215](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch5.xhtml#page_215)

SIGVERIF, [357](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch10.xhtml#page_357)

system logs, [215](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch5.xhtml#page_215)

logging/log files

web-based hacking, [231](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch6.xhtml#page_231)

LOIC (Low Orbit Ion Cannon), [367](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch10.xhtml#page_367)–368

Long, Johnny, [55](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch2.xhtml#page_55)–57

loop antenna, [276](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch7.xhtml#page_276)

lovebugs, [53](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch2.xhtml#page_53)

Low Orbit Ion Cannon (LOIC), [367](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch10.xhtml#page_367)–368

“low-hanging fruit,” 417

LTE networks, [286](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch7.xhtml#page_286)

**M**

MAC (mandatory access control), [22](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_22)

MAC (Media Access Control), [138](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch4.xhtml#page_138)

MAC addresses

ARP and, [142](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch4.xhtml#page_142)–143, [143](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch4.xhtml#page_143)–144

broadcast messages, [138](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch4.xhtml#page_138), [139](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch4.xhtml#page_139)

considerations, [10](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_10)

filtering, [287](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch7.xhtml#page_287)

flooding, [151](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch4.xhtml#page_151)–152

multicast messages, [139](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch4.xhtml#page_139)

spoofing, [152](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch4.xhtml#page_152), [154](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch4.xhtml#page_154)–155, [287](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch7.xhtml#page_287)

WPA and, [278](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch7.xhtml#page_278)

MAC duplication, [155](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch4.xhtml#page_155)

MAC filtering, [287](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch7.xhtml#page_287)

macro viruses, [360](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch10.xhtml#page_360)

madwifi project, [282](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch7.xhtml#page_282)

malicious applications, [442](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch12.xhtml#page_442)

malicious hackers, [30](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_30)

Maltego tool, [76](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch2.xhtml#page_76)

malvertising, [351](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch10.xhtml#page_351)

malware, [350](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch10.xhtml#page_350), [363](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch10.xhtml#page_363)

malware attacks, [350](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch10.xhtml#page_350)–364

overview, [350](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch10.xhtml#page_350)–351

Trojans, [352](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch10.xhtml#page_352)–357

viruses, [357](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch10.xhtml#page_357)–361

worms, [357](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch10.xhtml#page_357)–361

malware authors, [232](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch6.xhtml#page_232)–233

Malwarebytes, [356](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch10.xhtml#page_356)

Management Information Base. *See* MIB

management network zone, [12](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_12)

mandatory access control (MAC), [22](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_22)

man-in-the-browser (MIB) attacks, [372](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch10.xhtml#page_372)

man-in-the-middle (MITM) attacks, [205](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch5.xhtml#page_205), [416](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch11.xhtml#page_416)

mantraps, [447](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch12.xhtml#page_447)–448

Market Watch, [51](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch2.xhtml#page_51)

masking, [398](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch11.xhtml#page_398)

*The Matrix,* 297

maximum tolerable downtime (MTD), [17](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_17)

MBSA (Microsoft Baseline Security Analyzer), [115](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch3.xhtml#page_115), [261](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch6.xhtml#page_261)

MD4 algorithm, [185](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch5.xhtml#page_185)

MD5 algorithm, [185](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch5.xhtml#page_185), [394](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch11.xhtml#page_394)

MDM (Mobile Device Management), [306](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch8.xhtml#page_306)

Media Access Control. *See* MAC

Melissa virus, [360](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch10.xhtml#page_360)

Meltdown attacks, [373](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch10.xhtml#page_373)–374

memorization, [441](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch12.xhtml#page_441)

message integrity codes (MICs), [279](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch7.xhtml#page_279)

messenger channels, [439](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch12.xhtml#page_439)

Metagoofil, [58](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch2.xhtml#page_58)

metamorphic viruses, [360](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch10.xhtml#page_360)

Metasploit, [203](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch5.xhtml#page_203), [209](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch5.xhtml#page_209)–210, [246](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch6.xhtml#page_246)–247

methodologies, [96](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch3.xhtml#page_96)

MIB (Management Information Base), [123](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch3.xhtml#page_123)

MIB (man-in-the-browser) attacks, [372](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch10.xhtml#page_372)

MIB entries, [123](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch3.xhtml#page_123)

Microsoft Baseline Security Analyzer (MBSA), [115](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch3.xhtml#page_115), [261](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch6.xhtml#page_261)

Microsoft Management Consoles (MMCs), [192](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch5.xhtml#page_192)–193

Microsoft Vulnerability Research, [12](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_12)

Microsoft Windows. *See* Windows systems

MICs (message integrity codes), [279](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch7.xhtml#page_279)

Mirai botnet, [260](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch6.xhtml#page_260), [315](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch8.xhtml#page_315)–316

mirroring websites, [234](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch6.xhtml#page_234), [248](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch6.xhtml#page_248)

mis-association attack, [285](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch7.xhtml#page_285)

misconfiguration attacks, [26](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_26), [245](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch6.xhtml#page_245)

misconfiguration vulnerabilities, [13](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_13)

MITM (man-in-the-middle) attacks, [205](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch5.xhtml#page_205), [416](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch11.xhtml#page_416)

MMCs (Microsoft Management Consoles), [192](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch5.xhtml#page_192)–193

mobile computing, [298](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch8.xhtml#page_298)–309

attacks, [299](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch8.xhtml#page_299), [302](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch8.xhtml#page_302), [303](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch8.xhtml#page_303)–309

authentication, [300](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch8.xhtml#page_300)

authorization, [301](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch8.xhtml#page_301)

backdoors, [301](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch8.xhtml#page_301)

code-level issues, [301](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch8.xhtml#page_301)

considerations, [272](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch7.xhtml#page_272), [298](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch8.xhtml#page_298)

data storage, [300](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch8.xhtml#page_300)

insecure communication, [300](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch8.xhtml#page_300), [314](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch8.xhtml#page_314)

overview, [298](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch8.xhtml#page_298)

OWASP top 10 risks, [299](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch8.xhtml#page_299)–302

platform issues/problems, [300](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch8.xhtml#page_300)

platforms, [303](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch8.xhtml#page_303)–307

rooting/jailbreaking, [303](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch8.xhtml#page_303)–304, [305](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch8.xhtml#page_305)

software bugs, [308](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch8.xhtml#page_308)

Mobile Device Management (MDM), [306](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch8.xhtml#page_306)

mobile devices

applications, [300](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch8.xhtml#page_300), [303](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch8.xhtml#page_303), [305](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch8.xhtml#page_305), [306](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch8.xhtml#page_306)

as attack platform, [308](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch8.xhtml#page_308)

attacks on, [299](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch8.xhtml#page_299), [302](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch8.xhtml#page_302), [303](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch8.xhtml#page_303)–309

Bluetooth, [307](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch8.xhtml#page_307), [308](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch8.xhtml#page_308)–309

BYOD, [299](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch8.xhtml#page_299), [302](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch8.xhtml#page_302), [305](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch8.xhtml#page_305)–306

cryptography, [300](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch8.xhtml#page_300)

data storage, [300](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch8.xhtml#page_300)

encryption, [408](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch11.xhtml#page_408)

operating systems, [303](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch8.xhtml#page_303)–307

phishing, [307](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch8.xhtml#page_307)–308

smartphones. *See* smartphones

Trojans, [308](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch8.xhtml#page_308)

vulnerabilities/risks, [299](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch8.xhtml#page_299)–305

Wi-Fi connections, [307](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch8.xhtml#page_307), [308](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch8.xhtml#page_308)

mobile platform

application-based attacks, [442](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch12.xhtml#page_442)

smartphones. *See* smartphones

social engineering attacks, [441](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch12.xhtml#page_441)–443

mobile platform attacks, [441](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch12.xhtml#page_441)–443

modulation, [273](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch7.xhtml#page_273)

msconfig tool, [356](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch10.xhtml#page_356), [357](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch10.xhtml#page_357)

MTD (maximum tolerable downtime), [17](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_17)

Mudge, Raphael, [372](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch10.xhtml#page_372)

multicast, [146](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch4.xhtml#page_146)

multicast messages, [139](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch4.xhtml#page_139)

multipartite viruses, [360](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch10.xhtml#page_360)

multitier architecture, [237](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch6.xhtml#page_237)

**N**

name lookups, [66](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch2.xhtml#page_66)

name resolvers, [64](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch2.xhtml#page_64)

name servers, [63](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch2.xhtml#page_63)–66, [68](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch2.xhtml#page_68), [72](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch2.xhtml#page_72)

namespace, [63](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch2.xhtml#page_63)–66, [69](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch2.xhtml#page_69), [71](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch2.xhtml#page_71)

NAT (NetBIOS Auditing tool), [204](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch5.xhtml#page_204)

NAT (network address translation), [166](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch4.xhtml#page_166), [373](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch10.xhtml#page_373)

National Computer Security Center (NCSC), [21](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_21)

National Institutes of Standards and Technology. *See* NIST

National Vulnerability Database (NVD), [12](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_12)–13

NBNSpoof, [203](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch5.xhtml#page_203)

NBT-NS, [203](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch5.xhtml#page_203)

nbtstat command, [122](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch3.xhtml#page_122)–123

NCSC (National Computer Security Center), [21](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_21)

NDA (nondisclosure agreement), [31](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_31)

NeoTrace tool, [74](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch2.xhtml#page_74)

Nessus, [13](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_13), [115](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch3.xhtml#page_115)–116, [234](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch6.xhtml#page_234), [320](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch8.xhtml#page_320)

Nest thermostat, [311](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch8.xhtml#page_311)

net commands, [204](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch5.xhtml#page_204)

NetBIOS Auditing tool (NAT), [204](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch5.xhtml#page_204)

NetBIOS enumeration, [121](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch3.xhtml#page_121)–123

NetBIOS traffic, [203](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch5.xhtml#page_203)

netcat tool, [121](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch3.xhtml#page_121), [350](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch10.xhtml#page_350), [353](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch10.xhtml#page_353)–354

Netcraft, [53](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch2.xhtml#page_53)–54, [233](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch6.xhtml#page_233)

Netcraft Toolbar, [438](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch12.xhtml#page_438)

NetCut, [308](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch8.xhtml#page_308)

netizens, [364](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch10.xhtml#page_364)

Netscan, [86](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch3.xhtml#page_86)

NetScanTools Pro, [108](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch3.xhtml#page_108)

netstat tool, [91](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch3.xhtml#page_91), [355](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch10.xhtml#page_355)–356

NetStumbler, [281](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch7.xhtml#page_281), [283](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch7.xhtml#page_283)

NetSurveyor, [283](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch7.xhtml#page_283)–284, [289](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch7.xhtml#page_289)

network address translation (NAT), [166](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch4.xhtml#page_166), [373](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch10.xhtml#page_373)

Network Basic Input/Output System. *See* NetBIOS

network diagrams, [96](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch3.xhtml#page_96)

network ID, [92](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch3.xhtml#page_92), [93](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch3.xhtml#page_93), [95](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch3.xhtml#page_95), [96](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch3.xhtml#page_96), [98](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch3.xhtml#page_98)

network interface cards (NICs), [138](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch4.xhtml#page_138)–139, [141](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch4.xhtml#page_141), [274](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch7.xhtml#page_274)

network intrusion detection systems. *See* NIDSs

Network layer, [7](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_7), [142](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch4.xhtml#page_142)

network tap, [162](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch4.xhtml#page_162)

Network Time Protocol, [124](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch3.xhtml#page_124)

networks

ad hoc, [273](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch7.xhtml#page_273), [274](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch7.xhtml#page_274), [285](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch7.xhtml#page_285)

basics, [2](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_2), [5](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_5)–14

daisy-chaining, [15](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_15)

edge computing, [331](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch9.xhtml#page_331)

footprinting, [72](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch2.xhtml#page_72)–75

IoT, [310](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch8.xhtml#page_310), [314](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch8.xhtml#page_314), [316](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch8.xhtml#page_316)

LTE, [286](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch7.xhtml#page_286)

monitoring, [160](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch4.xhtml#page_160)–161, [162](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch4.xhtml#page_162)

range, [72](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch2.xhtml#page_72)–73

security zones, [10](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_10)–12

switched, [84](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch3.xhtml#page_84)

TCP/IP, [5](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_5), [7](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_7)–12, [84](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch3.xhtml#page_84)–88

VANET, [312](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch8.xhtml#page_312)

wireless. *See* wireless networks

Neverquest Trojan, [353](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch10.xhtml#page_353)

New Technology File System. *See* NTFS

*New York Times,* 370

NgineX servers, [236](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch6.xhtml#page_236)

NICs (network interface cards), [138](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch4.xhtml#page_138)–139, [141](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch4.xhtml#page_141), [274](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch7.xhtml#page_274)

NIDSbench tool, [168](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch4.xhtml#page_168)

NIDSs (network intrusion detection systems), [98](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch3.xhtml#page_98)–99, [160](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch4.xhtml#page_160)–162, [368](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch10.xhtml#page_368)

Nikto scanner, [234](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch6.xhtml#page_234)

Nimda worm, [361](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch10.xhtml#page_361)

Nirvanix, [336](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch9.xhtml#page_336)

NIST (National Institute of Standards and Technology), [334](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch9.xhtml#page_334), [409](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch11.xhtml#page_409)

NIST reference architecture, [334](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch9.xhtml#page_334)–335

nmap command, [234](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch6.xhtml#page_234), [412](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch11.xhtml#page_412)

Nmap switches, [105](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch3.xhtml#page_105)–106, [107](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch3.xhtml#page_107), [124](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch3.xhtml#page_124)

Nmap tool, [98](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch3.xhtml#page_98), [99](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch3.xhtml#page_99), [101](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch3.xhtml#page_101), [104](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch3.xhtml#page_104)–109, [318](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch8.xhtml#page_318)

nonce, [289](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch7.xhtml#page_289)

nondisclosure agreement (NDA), [31](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_31)

non-electronic password attacks, [201](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch5.xhtml#page_201)

nonrepudiation, [387](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch11.xhtml#page_387), [391](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch11.xhtml#page_391), [399](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch11.xhtml#page_399)

noodling, [183](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch5.xhtml#page_183)–184

NOP sled, [251](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch6.xhtml#page_251)

NSAuditor, [123](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch3.xhtml#page_123)

nslookup command, [70](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch2.xhtml#page_70)–72

NT LAN Manager. *See* NTLM

NTFS (New Technology File System), [212](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch5.xhtml#page_212)–213

NTFS file streaming, [212](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch5.xhtml#page_212)–213

n-tier architecture, [237](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch6.xhtml#page_237)

NTLM authentication, [185](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch5.xhtml#page_185), [187](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch5.xhtml#page_187)

NTLM hash, [186](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch5.xhtml#page_186)

NTP server, [124](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch3.xhtml#page_124)

NTPv3, [124](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch3.xhtml#page_124)

nuclear worm, [362](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch10.xhtml#page_362)–363

NULL scan, [102](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch3.xhtml#page_102)

NVD (National Vulnerability Database), [12](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_12)–13

**O**

Oakley protocol, [373](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch10.xhtml#page_373)

object identifiers (OIDs), [123](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch3.xhtml#page_123)

OCSP (Online Certificate Status Protocol), [400](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch11.xhtml#page_400)

OFDM (orthogonal frequency-division multiplexing), [273](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch7.xhtml#page_273)

OIDs (object identifiers), [123](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch3.xhtml#page_123)

omnidirectional antenna, [274](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch7.xhtml#page_274)

OmniPeek sniffer, [289](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch7.xhtml#page_289)

one-factor authentication, [200](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch5.xhtml#page_200)

Online Certificate Status Protocol (OCSP), [400](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch11.xhtml#page_400)

open services, [13](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_13)

Open Source Intelligence (OSINT), [75](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch2.xhtml#page_75)

Open Source Security Testing Methodology Manual (OSSTMM), [35](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_35)

Open System Authentication, [276](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch7.xhtml#page_276)

Open System Interconnection (OSI) Reference Model, [5](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_5)–7

Open Web Application Security Project. *See* OWASP

OpenPGP standard, [411](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch11.xhtml#page_411)

OpenSignalMaps, [281](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch7.xhtml#page_281)

OpenSSL, [412](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch11.xhtml#page_412), [413](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch11.xhtml#page_413)

OpenVAS, [14](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_14), [117](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch3.xhtml#page_117)

OpUtils 5, [124](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch3.xhtml#page_124)

Orange Book, [21](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_21)

organizational unique identifier, [138](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch4.xhtml#page_138), [143](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch4.xhtml#page_143)

orthogonal frequency-division multiplexing (OFDM), [273](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch7.xhtml#page_273)

Orwell, George, [149](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch4.xhtml#page_149), [397](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch11.xhtml#page_397)

OS (operating system)

attacks, [26](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_26)

baseline, [13](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_13)

default installation, [13](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_13)

design flaws, [13](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_13)

fingerprinting, [96](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch3.xhtml#page_96)

misconfiguration, [13](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_13)

OSI (Open System Interconnection) Reference Model, [5](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_5)–7

OSINT (Open Source Intelligence), [75](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch2.xhtml#page_75)

OSRFramework, [75](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch2.xhtml#page_75)–76

OSSTMM (Open Source Security Testing Methodology Manual), [35](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_35)

Ostinato tool, [86](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch3.xhtml#page_86)

out-of-band SQL injection, [259](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch6.xhtml#page_259)

overt channels, [351](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch10.xhtml#page_351)

OWASP (Open Web Application Security Project), [229](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch6.xhtml#page_229), [299](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch8.xhtml#page_299)–302, [313](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch8.xhtml#page_313)–315

**P**

PaaS (Platform as a Service), [332](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch9.xhtml#page_332)

packers, [352](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch10.xhtml#page_352)

Packet, [331](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch9.xhtml#page_331)

packet capture, [156](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch4.xhtml#page_156)–158

packet generating tools, [168](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch4.xhtml#page_168)

Packet Generator, [168](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch4.xhtml#page_168), [169](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch4.xhtml#page_169), [170](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch4.xhtml#page_170)

packet header, [84](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch3.xhtml#page_84)

Packet Internet Groper. *See* ping

PacketBuilder, [86](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch3.xhtml#page_86)–87

packet-filtering firewalls, [166](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch4.xhtml#page_166)–167

PackETH, [86](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch3.xhtml#page_86), [168](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch4.xhtml#page_168), [169](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch4.xhtml#page_169), [170](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch4.xhtml#page_170)

packets

considerations, [9](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_9)

fragmented, [111](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch3.xhtml#page_111)–112, [366](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch10.xhtml#page_366)

ICMP, [98](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch3.xhtml#page_98), [99](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch3.xhtml#page_99), [100](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch3.xhtml#page_100), [367](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch10.xhtml#page_367)

identifying targets, [97](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch3.xhtml#page_97)–100

IP, [9](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_9)–10, [103](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch3.xhtml#page_103)

PING, [98](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch3.xhtml#page_98)

routing, [112](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch3.xhtml#page_112)

SYN, [367](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch10.xhtml#page_367)

SYN/ACK, [367](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch10.xhtml#page_367)

TCP, [371](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch10.xhtml#page_371)

Padding Oracle On Downgraded Legacy Encryption (POODLE), [411](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch11.xhtml#page_411), [413](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch11.xhtml#page_413)–414

pair master key (PMK), [280](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch7.xhtml#page_280)

parabolic grid antenna, [275](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch7.xhtml#page_275)

parameter tampering, [242](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch6.xhtml#page_242)

paranoid policy, [23](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_23)

pareidolia, [340](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch9.xhtml#page_340)

partial knowledge testing, [33](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_33)

passive footprinting, [49](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch2.xhtml#page_49), [50](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch2.xhtml#page_50)–52

passive sniffing, [150](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch4.xhtml#page_150), [151](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch4.xhtml#page_151), [159](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch4.xhtml#page_159)

pass-the-hash attack, [189](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch5.xhtml#page_189)

password cracking, [201](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch5.xhtml#page_201)–208

active online attacks, [202](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch5.xhtml#page_202)–204

brute-force attacks, [207](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch5.xhtml#page_207)–208, [417](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch11.xhtml#page_417)

Cain and Abel tool, [153](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch4.xhtml#page_153), [205](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch5.xhtml#page_205), [207](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch5.xhtml#page_207), [288](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch7.xhtml#page_288)

cracking WEP, [287](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch7.xhtml#page_287)–289

cracking WPA, [287](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch7.xhtml#page_287)–289

dictionary attacks, [206](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch5.xhtml#page_206)–207

Ettercap, [205](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch5.xhtml#page_205)–206

hybrid attacks, [207](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch5.xhtml#page_207)

John the Ripper, [197](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch5.xhtml#page_197), [208](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch5.xhtml#page_208)

keylogging, [202](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch5.xhtml#page_202)

non-electronic attacks, [201](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch5.xhtml#page_201)

offline attacks, [206](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch5.xhtml#page_206)–207

passive online attacks, [205](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch5.xhtml#page_205)–206

rainbow tables, [207](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch5.xhtml#page_207), [396](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch11.xhtml#page_396)

resources, [208](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch5.xhtml#page_208)

rule-based attacks, [202](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch5.xhtml#page_202)

shoulder surfing, [201](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch5.xhtml#page_201), [429](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch12.xhtml#page_429)

web servers, [245](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch6.xhtml#page_245)

Windows systems, [184](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch5.xhtml#page_184)–189, [203](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch5.xhtml#page_203), [207](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch5.xhtml#page_207)

password guessing, [202](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch5.xhtml#page_202)

Password Policy, [23](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_23)

passwords, [199](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch5.xhtml#page_199)–204

attacks. *See* password cracking

changing, [447](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch12.xhtml#page_447)

community string, [124](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch3.xhtml#page_124)

complexity, [188](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch5.xhtml#page_188), [201](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch5.xhtml#page_201)

considerations, [141](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch4.xhtml#page_141)–142, [200](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch5.xhtml#page_200), [448](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch12.xhtml#page_448)–449

cracking. *See* password cracking

death of, [446](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch12.xhtml#page_446)

default, [13](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_13), [26](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_26), [201](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch5.xhtml#page_201), [208](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch5.xhtml#page_208)

forgotten, [257](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch6.xhtml#page_257)–258

hash values, [185](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch5.xhtml#page_185)–187

hashed, [185](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch5.xhtml#page_185)–189, [395](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch11.xhtml#page_395)–396

keyboard walks, [201](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch5.xhtml#page_201)

length, [188](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch5.xhtml#page_188), [201](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch5.xhtml#page_201)

Linux systems, [194](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch5.xhtml#page_194), [195](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch5.xhtml#page_195), [196](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch5.xhtml#page_196)–197

obtaining by asking for, [427](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch12.xhtml#page_427)

sniffing, [141](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch4.xhtml#page_141)–142, [201](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch5.xhtml#page_201)–208

stored in cookies, [254](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch6.xhtml#page_254)

strength, [200](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch5.xhtml#page_200)

tips for, [186](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch5.xhtml#page_186)

Windows systems, [184](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch5.xhtml#page_184)–189, [204](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch5.xhtml#page_204), [207](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch5.xhtml#page_207)

patches, [13](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_13), [211](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch5.xhtml#page_211), [261](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch6.xhtml#page_261)

payload, [15](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_15)

Payment Card Industry Data Security Standard (PCI-DSS), [35](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_35), [335](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch9.xhtml#page_335)

PayPal, [369](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch10.xhtml#page_369)

PCI-DSS (Payment Card Industry Data Security Standard), [35](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_35), [335](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch9.xhtml#page_335)

PDQ Deploy, [211](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch5.xhtml#page_211)

PDU (protocol data unit), [7](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_7), [84](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch3.xhtml#page_84)

peer to peer attacks, [367](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch10.xhtml#page_367)

pen testers, [28](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_28), [29](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_29), [30](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_30), [31](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_31), [32](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_32), [161](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch4.xhtml#page_161). *See also* hackers

pen testing. *See also* hacking

assessment, [32](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_32)

black-box testing, [32](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_32)

conclusion, [32](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_32)

considerations, [30](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_30), [31](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_31)–32

gray-box testing, [33](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_33)

*vs.* hacking, [53](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch2.xhtml#page_53)

“no harm” clause, [29](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_29)

overview, [31](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_31)–33

pen test phases, [32](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_32)

physical security and, [443](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch12.xhtml#page_443)

preparation phase, [32](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_32)

reconnaissance, [28](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_28)

target of evaluation, [32](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_32)

types of, [32](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_32)–33

vulnerabilities, [13](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_13)–14

white-box testing, [33](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_33)

penetration testing. *See* pen testing

permanent attacks, [367](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch10.xhtml#page_367)

permissive policy, [23](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_23)

personal identification numbers (PINs), [447](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch12.xhtml#page_447)

personally identifiable information (PII), [15](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_15), [76](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch2.xhtml#page_76)

Petya, [360](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch10.xhtml#page_360)

PGPcrack, [417](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch11.xhtml#page_417)

pharming, [438](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch12.xhtml#page_438)

Phish Tank Toolbar, [438](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch12.xhtml#page_438)

phishing

e-mail, [202](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch5.xhtml#page_202), [435](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch12.xhtml#page_435)–438, [439](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch12.xhtml#page_439)

mobile devices, [307](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch8.xhtml#page_307)–308

obtaining passwords via, [202](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch5.xhtml#page_202)

phlashing, [367](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch10.xhtml#page_367)

PhoneSnoop, [309](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch8.xhtml#page_309)

phreakers, [24](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_24)

physical controls, [16](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_16)

Physical layer, [6](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_6), [7](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_7)

physical security, [443](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch12.xhtml#page_443)–449

access controls, [445](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch12.xhtml#page_445)–448

basics, [443](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch12.xhtml#page_443)–449

biometric identifiers, [445](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch12.xhtml#page_445)–447

bump key, [449](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch12.xhtml#page_449)

considerations, [16](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_16), [28](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_28), [443](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch12.xhtml#page_443)

described, [443](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch12.xhtml#page_443)

hacks, [449](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch12.xhtml#page_449)

IoT devices, [315](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch8.xhtml#page_315)

locks, [443](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch12.xhtml#page_443), [445](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch12.xhtml#page_445), [447](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch12.xhtml#page_447), [449](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch12.xhtml#page_449)

mantraps, [447](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch12.xhtml#page_447)–448

operational measures, [444](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch12.xhtml#page_444)

pen testing and, [443](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch12.xhtml#page_443)

physical measures, [444](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch12.xhtml#page_444)

technical measures, [444](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch12.xhtml#page_444)

piggybacking, [259](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch6.xhtml#page_259), [429](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch12.xhtml#page_429)

PII (personally identifiable information), [15](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_15), [76](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch2.xhtml#page_76)

ping, [98](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch3.xhtml#page_98), [99](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch3.xhtml#page_99), [367](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch10.xhtml#page_367)

ping of death, [367](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch10.xhtml#page_367)

PING packets, [98](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch3.xhtml#page_98)

ping sweeps, [98](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch3.xhtml#page_98)–99, [100](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch3.xhtml#page_100), [101](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch3.xhtml#page_101)

PINs (personal identification numbers), [447](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch12.xhtml#page_447)

PKI (public key infrastructure), [392](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch11.xhtml#page_392), [399](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch11.xhtml#page_399)–407

PKI system, [399](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch11.xhtml#page_399)–407

plain text, [386](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch11.xhtml#page_386), [387](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch11.xhtml#page_387)

plain-text attacks, [415](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch11.xhtml#page_415)

Planning Tool for Resource Integration, Synchronization, and Management (PRISM), [148](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch4.xhtml#page_148)

Platform as a Service (PaaS), [332](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch9.xhtml#page_332)

PMK (pair master key), [280](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch7.xhtml#page_280)

PNZ (production network zone), [11](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_11)

POC (point of contact), [70](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch2.xhtml#page_70)–73

point of contact (POC), [70](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch2.xhtml#page_70)–73

policies, security, [22](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_22)–23

Polybius, [385](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch11.xhtml#page_385)

polymorphic viruses, [360](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch10.xhtml#page_360)

POODLE (Padding Oracle On Downgraded Legacy Encryption), [411](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch11.xhtml#page_411), [413](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch11.xhtml#page_413)–414

POP3 (Post Office Protocol 3), [142](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch4.xhtml#page_142)

pop-up windows, [437](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch12.xhtml#page_437), [438](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch12.xhtml#page_438)–439

port address translation, [166](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch4.xhtml#page_166)

port numbers, [63](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch2.xhtml#page_63), [88](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch3.xhtml#page_88)–91, [354](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch10.xhtml#page_354)–355

port sweeping, [107](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch3.xhtml#page_107)

Portable Penetrator, [288](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch7.xhtml#page_288)

ports

closed, [104](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch3.xhtml#page_104)

dynamic, [89](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch3.xhtml#page_89)

important port numbers, [89](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch3.xhtml#page_89)

listening for, [90](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch3.xhtml#page_90)

mirroring, [150](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch4.xhtml#page_150)

open, [96](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch3.xhtml#page_96)

registered, [89](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch3.xhtml#page_89)

scanning, [101](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch3.xhtml#page_101)–111

security, [151](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch4.xhtml#page_151), [155](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch4.xhtml#page_155)

span, [150](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch4.xhtml#page_150)

states, [90](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch3.xhtml#page_90)–91

TCP/IP, [356](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch10.xhtml#page_356)

UDP, [356](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch10.xhtml#page_356)

well-known, [89](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch3.xhtml#page_89), [90](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch3.xhtml#page_90)

POST method, [240](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch6.xhtml#page_240)

Post Office Protocol 3 (POP3), [142](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch4.xhtml#page_142)

power issues, [444](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch12.xhtml#page_444)

Presentation layer, [6](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_6), [7](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_7)

Pretty Good Privacy (PGP), [411](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch11.xhtml#page_411)

Pretty Park worm, [361](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch10.xhtml#page_361)

preventive controls, [16](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_16)

PRISM (Planning Tool for Resource Integration, Synchronization, and Management), [148](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch4.xhtml#page_148)

privacy issues

health information, [35](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_35)

IoT, [314](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch8.xhtml#page_314)

laws/standards, [33](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_33)

Samsung smart TV, [212](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch5.xhtml#page_212)–213

U.S. government, [396](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch11.xhtml#page_396)–397

private cloud model, [333](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch9.xhtml#page_333)

private keys

asymmetric encryption, [391](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch11.xhtml#page_391)–392

considerations, [399](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch11.xhtml#page_399), [412](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch11.xhtml#page_412), [413](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch11.xhtml#page_413)

described, [399](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch11.xhtml#page_399)

digital signatures and, [406](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch11.xhtml#page_406)–407

PKI and, [399](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch11.xhtml#page_399)–401, [407](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch11.xhtml#page_407)

private zone, [166](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch4.xhtml#page_166)

privileges

administrator, [209](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch5.xhtml#page_209)–210

escalation of, [29](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_29), [33](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_33), [208](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch5.xhtml#page_208)–210

root, [209](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch5.xhtml#page_209)–210

procedures, [23](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_23)

Process Explorer, [356](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch10.xhtml#page_356)

processors, [230](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch6.xhtml#page_230), [374](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch10.xhtml#page_374)

production network zone (PNZ), [11](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_11)

promiscuous mode, [139](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch4.xhtml#page_139)

promiscuous policy, [23](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_23)

protection rings, [217](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch5.xhtml#page_217)

protocol data unit (PDU), [7](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_7), [84](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch3.xhtml#page_84)

proxies, [96](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch3.xhtml#page_96), [113](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch3.xhtml#page_113)

proxy chains, [113](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch3.xhtml#page_113)

prudent policy, [23](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_23)

pseudonymous footprinting, [49](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch2.xhtml#page_49)

pseudorandom number, [86](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch3.xhtml#page_86)

PSH flag, [86](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch3.xhtml#page_86)

Psiphon, [115](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch3.xhtml#page_115)

public cloud model, [333](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch9.xhtml#page_333)

public key infrastructure. *See* PKI

public keys

asymmetric algorithms, [392](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch11.xhtml#page_392)

asymmetric encryption, [391](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch11.xhtml#page_391)–392

considerations, [399](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch11.xhtml#page_399)–400, [402](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch11.xhtml#page_402)

described, [399](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch11.xhtml#page_399)

digital signatures and, [406](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch11.xhtml#page_406)–407

PKI and, [399](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch11.xhtml#page_399)–402, [407](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch11.xhtml#page_407)

public zone, [166](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch4.xhtml#page_166)

PUT method, [240](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch6.xhtml#page_240)

“pwning,” 245

**Q**

QoS (quality of service), [142](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch4.xhtml#page_142)

quality of service (QoS), [142](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch4.xhtml#page_142)

Qualys, [14](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_14)

**R**

RADIUS servers, [276](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch7.xhtml#page_276), [279](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch7.xhtml#page_279)

rainbow tables, [207](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch5.xhtml#page_207), [396](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch11.xhtml#page_396)

ransomware, [358](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch10.xhtml#page_358)–360

RAs (registration authorities), [400](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch11.xhtml#page_400), [402](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch11.xhtml#page_402)

RC (Rivest Cipher), [390](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch11.xhtml#page_390)

RC4, [414](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch11.xhtml#page_414)

RC4 algorithm, [278](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch7.xhtml#page_278)

*Ready Player One,* 59

reconnaissance, [47](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch2.xhtml#page_47)–82

described, [28](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_28)

*vs.* footprinting, [48](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch2.xhtml#page_48)

passive footprinting, [50](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch2.xhtml#page_50)–52

search engines, [53](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch2.xhtml#page_53)–60

regedit.exe, [192](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch5.xhtml#page_192)

regedt32.exe, [192](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch5.xhtml#page_192)

regional Internet registries (RIRs), [68](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch2.xhtml#page_68)

registration authorities (RAs), [400](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch11.xhtml#page_400), [402](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch11.xhtml#page_402)

registry, [189](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch5.xhtml#page_189)–192, [214](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch5.xhtml#page_214)

registry hacking, [190](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch5.xhtml#page_190)–192

registry information, [72](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch2.xhtml#page_72)

regulatory efforts, [335](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch9.xhtml#page_335)

Remote Exec, [211](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch5.xhtml#page_211)

replay attacks, [205](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch5.xhtml#page_205), [416](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch11.xhtml#page_416)

Requests For Comments (RFCs), [228](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch6.xhtml#page_228)

Réseaux IP Européens (RIPE) NCC, [68](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch2.xhtml#page_68)

resource identifiers (RIDs), [118](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch3.xhtml#page_118), [119](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch3.xhtml#page_119)

Responder, [203](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch5.xhtml#page_203)

Retina CS, [14](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_14), [115](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch3.xhtml#page_115)

reverse engineering, [301](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch8.xhtml#page_301)

reverse social engineering, [430](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch12.xhtml#page_430)

RFCs (Requests For Comments), [228](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch6.xhtml#page_228)

RFID features, [447](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch12.xhtml#page_447)

RFID identify theft, [429](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch12.xhtml#page_429)–430

RFID skimming, [429](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch12.xhtml#page_429)–430

RIDs (resource identifiers), [118](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch3.xhtml#page_118), [119](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch3.xhtml#page_119)

RIoT Vulnerability Scanner, [318](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch8.xhtml#page_318)

RIPE (Réseaux IP Européens) NCC, [68](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch2.xhtml#page_68)

RIPEMD-160 hash, [395](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch11.xhtml#page_395)

RIRs (regional Internet registries), [68](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch2.xhtml#page_68)

risk. *See also* vulnerabilities

assessment, [13](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_13)

considerations, [25](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_25), [28](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_28), [31](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_31)

management, [15](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_15)–16

quantifying dangers of, [12](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_12)–13

risk analysis matrix, [15](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_15)–16

Ritz, David, [62](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch2.xhtml#page_62)

Rivest Cipher (RC), [390](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch11.xhtml#page_390)

Rivest, Ronald, [394](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch11.xhtml#page_394)

roaming, [274](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch7.xhtml#page_274)

robots.txt file, [233](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch6.xhtml#page_233), [234](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch6.xhtml#page_234)

rogue access points, [274](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch7.xhtml#page_274), [283](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch7.xhtml#page_283), [284](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch7.xhtml#page_284)–285

Rogue Security, [437](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch12.xhtml#page_437)

rolling code attack, [316](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch8.xhtml#page_316)

root CAs, [402](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch11.xhtml#page_402), [406](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch11.xhtml#page_406)

root privileges, [209](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch5.xhtml#page_209)–210

rooting, [303](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch8.xhtml#page_303), [305](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch8.xhtml#page_305)

rootkits, [216](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch5.xhtml#page_216)–218

Rosenworcel, Jessica, [279](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch7.xhtml#page_279)

routers, [1](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_1)–2, [10](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_10)

rpcclient tool, [119](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch3.xhtml#page_119)

rpcinfo tool, [119](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch3.xhtml#page_119)

RSA algorithm, [392](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch11.xhtml#page_392), [410](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch11.xhtml#page_410)

RST flag, [86](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch3.xhtml#page_86)

R-U-Dead-Yet (RUDY), [368](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch10.xhtml#page_368)

RUDY (R-U-Dead-Yet), [368](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch10.xhtml#page_368)

rule-based attacks, [202](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch5.xhtml#page_202)

**S**

SaaS (Software as a Service), [333](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch9.xhtml#page_333)

Salesforce, [330](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch9.xhtml#page_330)

salt, [186](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch5.xhtml#page_186), [396](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch11.xhtml#page_396)

SAM database, [119](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch3.xhtml#page_119)

SAM (Security Accounts Manager) file, [184](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch5.xhtml#page_184)–187, [188](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch5.xhtml#page_188)

Sarbanes-Oxley (SOX) Act, [35](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_35)

scalar objects, [123](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch3.xhtml#page_123)

scanning, [84](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch3.xhtml#page_84)–117

considerations, [99](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch3.xhtml#page_99)–101

described, [84](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch3.xhtml#page_84)

evasion, [111](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch3.xhtml#page_111)–115

examples of, [28](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_28)

*vs.* footprinting, [84](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch3.xhtml#page_84)

fundamentals, [96](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch3.xhtml#page_96)–117

identifying targets, [97](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch3.xhtml#page_97)–101

naming conventions, [102](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch3.xhtml#page_102)

other tools, [109](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch3.xhtml#page_109)–111

port, [101](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch3.xhtml#page_101)–111

stealth attacks, [211](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch5.xhtml#page_211)–212, [216](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch5.xhtml#page_216)

tools for, [101](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch3.xhtml#page_101)–111, [309](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch8.xhtml#page_309)

ZenMap, [98](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch3.xhtml#page_98)

scanning methodology, [96](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch3.xhtml#page_96)–117

SCAP (Security Content Automation Protocol), [13](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_13)

Scientology website attacks, [367](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch10.xhtml#page_367)

ScoopLM, [205](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch5.xhtml#page_205), [206](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch5.xhtml#page_206)

screened subnet, [166](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch4.xhtml#page_166)

script kiddies, [24](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_24), [26](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_26)

search engines, [53](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch2.xhtml#page_53)–60

footprinting and, [53](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch2.xhtml#page_53)–60

Google hacking, [55](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch2.xhtml#page_55)–60

listed, [53](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch2.xhtml#page_53)

mapping/location tools, [53](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch2.xhtml#page_53)

overview, [53](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch2.xhtml#page_53)

Shodan, [77](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch2.xhtml#page_77), [317](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch8.xhtml#page_317)–318

SEC Info, [51](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch2.xhtml#page_51)

Secure Shell (SSH), [410](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch11.xhtml#page_410)

Secure Sockets Layer. *See* SSL

Secure/Multipurpose Internet Mail Extensions (S/MIME), [411](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch11.xhtml#page_411)

security

applications, [229](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch6.xhtml#page_229)–231

auditing, [23](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_23)

basics, [14](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_14)–23

cloud, [335](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch9.xhtml#page_335)–339

considerations, [415](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch11.xhtml#page_415)

fundamentals, [2](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_2)–23

laws/standards, [33](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_33)–38

Linux systems, [193](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch5.xhtml#page_193)–197

mobile. *See* mobile computing

patches, [13](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_13), [211](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch5.xhtml#page_211), [261](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch6.xhtml#page_261)

physical. *See* physical security

port, [151](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch4.xhtml#page_151), [155](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch4.xhtml#page_155)

Windows systems, [184](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch5.xhtml#page_184)–193

wireless networks, [276](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch7.xhtml#page_276)–280

Security Accounts Manager. *See* SAM

security analysts, [25](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_25)

Security Center, [115](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch3.xhtml#page_115)–116

Security Content Automation Protocol (SCAP), [13](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_13)

security context, [118](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch3.xhtml#page_118)

security controls, [13](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_13), [16](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_16), [31](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_31)–32

Security Focus, [12](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_12)

Security, Functionality, and Usability triangle, [14](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_14), [26](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_26)

security identifiers (SIDs), [118](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch3.xhtml#page_118), [119](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch3.xhtml#page_119)

security incident and event management (SIEM), [29](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_29)

security logs, [215](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch5.xhtml#page_215)

Security Magazine, [12](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_12)

Security Operation Center (SOC), [29](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_29)

security policies, [22](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_22)–23

security zones, [10](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_10)–12

SEF (Social Engineering Framework), [76](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch2.xhtml#page_76)

segments, [6](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_6), [84](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch3.xhtml#page_84)

semagrams, [214](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch5.xhtml#page_214)

sequence attacks, [370](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch10.xhtml#page_370)–371

sequence numbers (SNs), [370](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch10.xhtml#page_370)–371

serial number, zone file, [66](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch2.xhtml#page_66)

servers

Apache, [235](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch6.xhtml#page_235), [236](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch6.xhtml#page_236)–237

application, [235](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch6.xhtml#page_235)

authoritative, [64](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch2.xhtml#page_64)

DNS, [62](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch2.xhtml#page_62)–72, [284](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch7.xhtml#page_284)

e-mail, [71](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch2.xhtml#page_71)

Google, [414](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch11.xhtml#page_414)

HTTPS, [415](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch11.xhtml#page_415)

IIS, [235](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch6.xhtml#page_235)–236, [237](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch6.xhtml#page_237), [238](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch6.xhtml#page_238)

Linux, [193](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch5.xhtml#page_193)

name, [63](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch2.xhtml#page_63)–66, [68](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch2.xhtml#page_68), [72](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch2.xhtml#page_72)

name resolvers, [64](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch2.xhtml#page_64)

NgineX, [236](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch6.xhtml#page_236)

NTP, [124](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch3.xhtml#page_124)

RADIUS, [276](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch7.xhtml#page_276), [279](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch7.xhtml#page_279)

sinkhole, [359](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch10.xhtml#page_359)

SOA, [71](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch2.xhtml#page_71)

unpatched, [13](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_13)

web. *See* web servers

Service Oriented Architecture. *See* SOA

service set identifier (SSID), [276](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch7.xhtml#page_276)

session fixation attack, [253](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch6.xhtml#page_253)

session hijacking, [369](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch10.xhtml#page_369)–374

session IDs, [253](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch6.xhtml#page_253)

Session layer, [6](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_6), [7](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_7)

session management, [229](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch6.xhtml#page_229)

session riding, [342](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch9.xhtml#page_342)

session splicing, [168](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch4.xhtml#page_168)

SHA-1 algorithm, [394](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch11.xhtml#page_394), [395](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch11.xhtml#page_395)

SHA-2 algorithm, [394](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch11.xhtml#page_394), [395](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch11.xhtml#page_395)

SHA-3 algorithm, [395](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch11.xhtml#page_395)

shadow files, [194](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch5.xhtml#page_194), [195](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch5.xhtml#page_195)–196

shadow IT, [339](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch9.xhtml#page_339)

Shadowsocks, [114](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch3.xhtml#page_114)

Shared Key Authentication, [276](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch7.xhtml#page_276)

sheepdip system, [364](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch10.xhtml#page_364)

shell injection, [249](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch6.xhtml#page_249)

shell viruses, [360](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch10.xhtml#page_360)

ShellShock, [247](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch6.xhtml#page_247)

Shodan, [77](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch2.xhtml#page_77), [317](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch8.xhtml#page_317)–318

shoulder surfing, [201](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch5.xhtml#page_201), [429](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch12.xhtml#page_429)

shredders, [428](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch12.xhtml#page_428)

shrink-wrap code attacks, [26](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_26)

side-channel attacks, [342](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch9.xhtml#page_342), [416](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch11.xhtml#page_416)

SIDs (security identifiers), [118](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch3.xhtml#page_118), [119](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch3.xhtml#page_119)

SIEM (security incident and event management), [29](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_29)

signature files, [363](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch10.xhtml#page_363)–364

signature list, [159](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch4.xhtml#page_159)

sign-in seal, [438](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch12.xhtml#page_438)

SIGVERIF log file, [357](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch10.xhtml#page_357)

SIGVERIF tool, [356](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch10.xhtml#page_356), [357](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch10.xhtml#page_357)

Simple Mail Transfer Protocol (SMTP), [124](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch3.xhtml#page_124), [125](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch3.xhtml#page_125), [141](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch4.xhtml#page_141)

Simple Network Management Protocol. *See* SNMP

Simple Object Access Protocol (SOAP), [250](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch6.xhtml#page_250)

single authority system, [402](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch11.xhtml#page_402)

single loss expectancy (SLE), [17](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_17)

sinkhole server, [359](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch10.xhtml#page_359)

Sirefef rootkit, [217](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch5.xhtml#page_217)

Sisyphean activities, [245](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch6.xhtml#page_245)–246

Sisyphus, King, [245](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch6.xhtml#page_245)–246

SiteDigger tool, [57](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch2.xhtml#page_57)

Skyhook tool, [284](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch7.xhtml#page_284)

Slammer worm, [361](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch10.xhtml#page_361)

SLE (single loss expectancy), [17](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_17)

Slowloris tool, [368](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch10.xhtml#page_368)

SMAC tool, [287](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch7.xhtml#page_287)

smart watches, [310](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch8.xhtml#page_310), [312](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch8.xhtml#page_312)

smartcards, [447](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch12.xhtml#page_447)

smartphones. *See also* mobile devices

Android. *See* Android phones

attack methodologies, [299](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch8.xhtml#page_299)

Blackberry phones, [303](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch8.xhtml#page_303), [309](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch8.xhtml#page_309)

considerations, [298](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch8.xhtml#page_298)

iPhone. *See* iPhones

vulnerabilities/risks, [299](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch8.xhtml#page_299), [307](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch8.xhtml#page_307)

wireless hacking and, [272](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch7.xhtml#page_272), [281](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch7.xhtml#page_281)

“smashing the stack,” 251–253

SMB exploit, [358](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch10.xhtml#page_358)–359, [360](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch10.xhtml#page_360)

SMB vulnerability, [359](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch10.xhtml#page_359)

S/MIME (Secure/Multipurpose Internet Mail Extensions), [411](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch11.xhtml#page_411)

Smith, Zachary, [331](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch9.xhtml#page_331)

SMS messages, [442](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch12.xhtml#page_442)

SMS phishing, [307](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch8.xhtml#page_307)–308

SMTP (Simple Mail Transfer Protocol), [124](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch3.xhtml#page_124), [125](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch3.xhtml#page_125), [141](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch4.xhtml#page_141)

SMTP commands, [125](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch3.xhtml#page_125)

Smurf attacks, [367](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch10.xhtml#page_367)

sniffers

Cain and Abel tool, [153](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch4.xhtml#page_153), [205](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch5.xhtml#page_205), [288](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch7.xhtml#page_288)

Ettercap, [159](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch4.xhtml#page_159), [205](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch5.xhtml#page_205)–206, [372](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch10.xhtml#page_372)

IoT traffic, [320](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch8.xhtml#page_320)

promiscuous mode, [139](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch4.xhtml#page_139)

tcpdump tool, [158](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch4.xhtml#page_158)–159

Wireshark, [156](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch4.xhtml#page_156)–159

sniffing, [138](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch4.xhtml#page_138)–159

active, [150](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch4.xhtml#page_150)–153

ARP poisoning, [152](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch4.xhtml#page_152)–153

basics, [138](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch4.xhtml#page_138)–151

collision domains, [139](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch4.xhtml#page_139)–141, [150](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch4.xhtml#page_150)

described, [138](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch4.xhtml#page_138)

firewalls, [165](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch4.xhtml#page_165)–167

IPv6 and, [143](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch4.xhtml#page_143)–145

MAC flooding, [151](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch4.xhtml#page_151)–152

network devices and, [138](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch4.xhtml#page_138)–141

network interface cards and, [138](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch4.xhtml#page_138)–139

passive, [150](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch4.xhtml#page_150), [151](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch4.xhtml#page_151), [159](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch4.xhtml#page_159)

passwords, [141](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch4.xhtml#page_141)–142, [201](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch5.xhtml#page_201)–208

protocols, [141](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch4.xhtml#page_141)–147

techniques, [151](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch4.xhtml#page_151)–155

tools, [156](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch4.xhtml#page_156)–159

viewing ARP entries, [144](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch4.xhtml#page_144)–145

wireless, [289](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch7.xhtml#page_289)–290

wiretapping, [148](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch4.xhtml#page_148)–149

SNMP (Simple Network Management Protocol), [123](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch3.xhtml#page_123)–124, [141](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch4.xhtml#page_141)–142

SNMP enumeration, [123](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch3.xhtml#page_123)–124

SNMPScanner, [124](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch3.xhtml#page_124)

Snort IDS, [161](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch4.xhtml#page_161)–165

Snowden, Edward, [397](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch11.xhtml#page_397)

SNs (sequence numbers), [370](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch10.xhtml#page_370)–371

SNScan, [124](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch3.xhtml#page_124)

SOA (Service Oriented Architecture), [341](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch9.xhtml#page_341)

SOA records, [66](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch2.xhtml#page_66)

SOA server, [71](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch2.xhtml#page_71)

SOAP (Simple Object Access Protocol), [250](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch6.xhtml#page_250)

SOAP injection, [250](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch6.xhtml#page_250)

SOC (Security Operation Center), [29](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_29)

social engineering, [426](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch12.xhtml#page_426)–443

authority support, [429](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch12.xhtml#page_429)

computer-based attacks, [434](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch12.xhtml#page_434)–441

defined, [426](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch12.xhtml#page_426)

described, [52](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch2.xhtml#page_52)

disgruntled employees, [55](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch2.xhtml#page_55), [432](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch12.xhtml#page_432)–434

dumpster diving, [201](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch5.xhtml#page_201), [428](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch12.xhtml#page_428)

as footprinting tool, [51](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch2.xhtml#page_51), [52](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch2.xhtml#page_52)

“halo effect,” 430

human-based attacks, [427](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch12.xhtml#page_427)–434

identity theft, [429](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch12.xhtml#page_429)–430, [440](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch12.xhtml#page_440)–441

impersonation, [428](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch12.xhtml#page_428)–429

insider threats, [432](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch12.xhtml#page_432)–434

mobile devices, [307](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch8.xhtml#page_307)–308

mobile-based attacks, [441](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch12.xhtml#page_441)–443

obtaining passwords, [201](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch5.xhtml#page_201), [426](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch12.xhtml#page_426)–427

overview, [426](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch12.xhtml#page_426)–427

phases of, [427](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch12.xhtml#page_427)

phishing e-mail/attacks, [435](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch12.xhtml#page_435)–438, [439](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch12.xhtml#page_439)

piggybacking, [429](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch12.xhtml#page_429)

preventing, [439](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch12.xhtml#page_439)–441

real world, [431](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch12.xhtml#page_431)–432

reverse, [430](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch12.xhtml#page_430)

shoulder surfing, [201](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch5.xhtml#page_201), [429](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch12.xhtml#page_429)

social networking and, [434](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch12.xhtml#page_434)

tailgating, [429](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch12.xhtml#page_429)

technical support, [428](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch12.xhtml#page_428)–429, [430](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch12.xhtml#page_430)

training users on, [439](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch12.xhtml#page_439)

whaling, [438](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch12.xhtml#page_438)

why it works, [427](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch12.xhtml#page_427)

Social Engineering Framework (SEF), [76](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch2.xhtml#page_76)

social networking, [434](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch12.xhtml#page_434)

social networking sites, [52](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch2.xhtml#page_52), [55](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch2.xhtml#page_55)

social skills, [58](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch2.xhtml#page_58)–59

SOCKS5 protocol, [114](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch3.xhtml#page_114)

Softerra, [124](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch3.xhtml#page_124)

Software as a Service (SaaS), [333](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch9.xhtml#page_333)

Sony PlayStation network attacks, [368](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch10.xhtml#page_368)

source host, [66](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch2.xhtml#page_66)

source routing, [112](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch3.xhtml#page_112)

SOX (Sarbanes-Oxley) Act, [35](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_35)

span ports, [150](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch4.xhtml#page_150)

sparse infector viruses, [361](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch10.xhtml#page_361)

spear phishing, [438](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch12.xhtml#page_438)

Spectre attacks, [373](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch10.xhtml#page_373)–374

spectrum analyzer, [274](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch7.xhtml#page_274)

spiders, [54](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch2.xhtml#page_54), [76](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch2.xhtml#page_76)

spimming, [438](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch12.xhtml#page_438)

spoof attacks, [366](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch10.xhtml#page_366)

Spoofcard, [70](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch2.xhtml#page_70)

spoofing

considerations, [70](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch2.xhtml#page_70)

IP addresses, [112](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch3.xhtml#page_112)

IRDP, [155](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch4.xhtml#page_155)

MAC addresses, [152](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch4.xhtml#page_152), [154](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch4.xhtml#page_154)–155, [287](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch7.xhtml#page_287)

overview, [154](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch4.xhtml#page_154)

spyware, [202](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch5.xhtml#page_202)

SQL (Structured Query Language), [255](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch6.xhtml#page_255)–256

SQL injection, [254](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch6.xhtml#page_254)–259

SQL Slammer worm, [361](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch10.xhtml#page_361)

SQLBrute, [259](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch6.xhtml#page_259)

sqlmap scanner, [259](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch6.xhtml#page_259)

sqlninja scanner, [259](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch6.xhtml#page_259)

“squirreling,” 331–332

SSH (Secure Shell), [410](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch11.xhtml#page_410)

SSID (service set identifier), [276](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch7.xhtml#page_276)

SSID cloaking, [276](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch7.xhtml#page_276)

SSL (Secure Sockets Layer), [205](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch5.xhtml#page_205)–206, [410](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch11.xhtml#page_410), [411](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch11.xhtml#page_411), [414](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch11.xhtml#page_414), [415](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch11.xhtml#page_415)

SSL sites, [205](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch5.xhtml#page_205)–206

sslsniff tool, [206](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch5.xhtml#page_206)

SSLv2, [414](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch11.xhtml#page_414)–415

stack, [251](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch6.xhtml#page_251)

StackGuard, [251](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch6.xhtml#page_251)

Stagefright bugs, [308](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch8.xhtml#page_308)

standards, [21](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_21), [23](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_23), [33](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_33)–36

Start of Authority record. *See* SOA

state-sponsored hackers, [26](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_26)

Static Application Security Testing (SAST), [230](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch6.xhtml#page_230)

static electricity, [444](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch12.xhtml#page_444)

stealth attacks, [211](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch5.xhtml#page_211)–212, [216](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch5.xhtml#page_216)

stealth scan, [102](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch3.xhtml#page_102), [105](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch3.xhtml#page_105)

stealth viruses, [361](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch10.xhtml#page_361)

steganography, [214](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch5.xhtml#page_214), [386](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch11.xhtml#page_386), [398](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch11.xhtml#page_398)–399

Steinberg, Joseph, [412](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch11.xhtml#page_412)

stream ciphers, [386](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch11.xhtml#page_386), [388](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch11.xhtml#page_388)

Structured Query Language. *See* SQL

Stuxnet code, [362](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch10.xhtml#page_362)–363

subnet mask, [92](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch3.xhtml#page_92)

subnetting, [92](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch3.xhtml#page_92)–96

substitution, [387](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch11.xhtml#page_387)

suicide hackers, [25](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_25)

Super Bluetooth Hack, [309](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch8.xhtml#page_309)

SuperScan, [109](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch3.xhtml#page_109), [111](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch3.xhtml#page_111), [123](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch3.xhtml#page_123)

switch port stealing, [152](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch4.xhtml#page_152)

switched networks, [84](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch3.xhtml#page_84)

switches, [141](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch4.xhtml#page_141), [150](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch4.xhtml#page_150), [151](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch4.xhtml#page_151), [152](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch4.xhtml#page_152), [155](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch4.xhtml#page_155)

Sybil attack, [316](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch8.xhtml#page_316)

Symantec Drive Encryption, [408](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch11.xhtml#page_408)

symmetric encryption, [389](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch11.xhtml#page_389)–390

SYN (Synchronize segment), [9](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_9)

SYN attacks, [367](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch10.xhtml#page_367)

SYN flag, [86](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch3.xhtml#page_86), [87](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch3.xhtml#page_87), [102](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch3.xhtml#page_102)

SYN floods, [367](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch10.xhtml#page_367)

SYN packets, [367](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch10.xhtml#page_367)

SYN scan, [102](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch3.xhtml#page_102)

SYN segments, [168](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch4.xhtml#page_168)

SYN/ SYN/ACK, ACK handshake, [10](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_10)

SYN/ACK packets, [367](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch10.xhtml#page_367)

SYN/ACK segment, [9](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_9), [10](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_10)

Synchronize segment. *See* SYN

Syrian Electronic Army, [370](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch10.xhtml#page_370)

system administrators. *See* administrators

system attacks, [183](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch5.xhtml#page_183)–225. *See also* attacks

checking for live systems, [96](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch3.xhtml#page_96)

considerations, [198](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch5.xhtml#page_198)

covering/clearing tracks, [29](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_29), [198](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch5.xhtml#page_198), [199](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch5.xhtml#page_199), [215](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch5.xhtml#page_215)–216

enumeration. *See* enumeration

executing applications, [210](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch5.xhtml#page_210)–211

gaining access, [28](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_28), [197](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch5.xhtml#page_197)–198

getting started, [184](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch5.xhtml#page_184)–199

maintaining access, [29](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_29), [197](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch5.xhtml#page_197), [198](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch5.xhtml#page_198), [199](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch5.xhtml#page_199)

methodology, [197](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch5.xhtml#page_197)–199

password cracking, [201](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch5.xhtml#page_201)–208

phases, [27](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_27)–30, [197](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch5.xhtml#page_197)–199

privilege escalation, [29](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_29), [33](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_33), [208](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch5.xhtml#page_208)–210

reconnaissance. *See* reconnaissance

scanning. *See* scanning

stealth attacks, [211](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch5.xhtml#page_211)–212, [216](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch5.xhtml#page_216)

system logs, [215](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch5.xhtml#page_215)

system viruses, [360](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch10.xhtml#page_360)

systems

“bricking,” 367

causing permanent damage to, [367](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch10.xhtml#page_367)

“live,” 96

**T**

tabular objects, [123](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch3.xhtml#page_123)

tailgating, [429](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch12.xhtml#page_429)

Tails OS, [115](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch3.xhtml#page_115)

target of evaluation (TOE), [32](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_32)

Task Manager, [356](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch10.xhtml#page_356)

TCG (Trusted Computing Group), [337](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch9.xhtml#page_337)

TCP (Transmission Control Protocol), [10](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_10), [85](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch3.xhtml#page_85), [142](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch4.xhtml#page_142)

TCP communication, [370](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch10.xhtml#page_370)–372

TCP connect scan, [101](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch3.xhtml#page_101), [105](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch3.xhtml#page_105)

TCP flags, [86](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch3.xhtml#page_86)–88, [102](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch3.xhtml#page_102)

TCP packets, [371](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch10.xhtml#page_371)

TCP segment structure, [86](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch3.xhtml#page_86)

TCP session hacking, [370](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch10.xhtml#page_370)–371

TCP state-exhaustion attacks, [367](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch10.xhtml#page_367)

TCP streams, [156](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch4.xhtml#page_156)

tcpdump tool, [158](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch4.xhtml#page_158)–159

TCP/IP networks, [5](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_5), [7](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_7)–12, [84](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch3.xhtml#page_84)–88

TCP/IP ports, [356](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch10.xhtml#page_356)

TCP/IP stack, [7](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_7), [8](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_8)

tcptrace tool, [159](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch4.xhtml#page_159)

TCSEC (Trusted Computer System Evaluation Criteria), [21](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_21)–22

teardrop attacks, [367](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch10.xhtml#page_367)

technical controls, [16](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_16)

technical support social engineering, [428](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch12.xhtml#page_428)–429, [430](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch12.xhtml#page_430)

technorati, [364](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch10.xhtml#page_364)

Telnet, [120](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch3.xhtml#page_120)–121, [156](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch4.xhtml#page_156)–157, [320](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch8.xhtml#page_320)

temperature, [444](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch12.xhtml#page_444)

Temporal Key Integrity Protocol (TKIP), [278](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch7.xhtml#page_278), [279](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch7.xhtml#page_279)

terminology, [15](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_15), [24](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_24)–30

TGS (ticket granting service), [187](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch5.xhtml#page_187), [188](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch5.xhtml#page_188)

TGT (ticket granting ticket), [187](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch5.xhtml#page_187), [188](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch5.xhtml#page_188)

THC Hydra, [208](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch5.xhtml#page_208), [245](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch6.xhtml#page_245)

The Onion Routing (TOR), [113](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch3.xhtml#page_113)

thermostats, [311](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch8.xhtml#page_311)

Thingful tool, [318](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch8.xhtml#page_318)

Threat Analyzer, [363](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch10.xhtml#page_363)

threat modeling, [15](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_15)

threats, [16](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_16)

three-factor authentication, [200](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch5.xhtml#page_200)

three-way handshake, [10](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_10), [86](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch3.xhtml#page_86), [87](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch3.xhtml#page_87), [372](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch10.xhtml#page_372)

ticket granting service (TGS), [187](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch5.xhtml#page_187), [188](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch5.xhtml#page_188)

ticket granting ticket (TGT), [187](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch5.xhtml#page_187), [188](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch5.xhtml#page_188)

tiger team, [31](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_31)

time to live (TTL), [66](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch2.xhtml#page_66)

TKIP (Temporal Key Integrity Protocol), [278](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch7.xhtml#page_278), [279](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch7.xhtml#page_279)

TLS (Transport Layer Security), [410](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch11.xhtml#page_410), [413](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch11.xhtml#page_413), [415](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch11.xhtml#page_415)

TMAC tool, [287](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch7.xhtml#page_287)

TOE (target of evaluation), [32](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_32)

tokens, [446](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch12.xhtml#page_446), [447](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch12.xhtml#page_447)

Toolset, [124](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch3.xhtml#page_124)

TOR (The Onion Routing), [113](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch3.xhtml#page_113)

TRACE method, [240](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch6.xhtml#page_240)

traceroute tools, [72](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch2.xhtml#page_72)–75, [168](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch4.xhtml#page_168)

tracert tool, [72](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch2.xhtml#page_72)–75

Transmission Control Protocol. *See* TCP

Transport layer, [6](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_6), [7](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_7), [142](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch4.xhtml#page_142)

Transport Layer Security (TLS), [410](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch11.xhtml#page_410), [413](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch11.xhtml#page_413), [415](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch11.xhtml#page_415)

transport mode, [373](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch10.xhtml#page_373)–374

transposition, [387](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch11.xhtml#page_387)

trash intelligence, [428](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch12.xhtml#page_428)

Trend Micro, [12](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_12)

Tribe Flood Network, [368](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch10.xhtml#page_368)

Trinity tool, [368](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch10.xhtml#page_368)

Tripwire, [356](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch10.xhtml#page_356)–357

Trojans, [352](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch10.xhtml#page_352)–357

*vs.* backdoors, [352](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch10.xhtml#page_352)

command shell, [353](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch10.xhtml#page_353)

considerations, [202](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch5.xhtml#page_202), [353](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch10.xhtml#page_353)–354, [363](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch10.xhtml#page_363)

countermeasures, [356](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch10.xhtml#page_356)–357

described, [352](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch10.xhtml#page_352)

EliteWrap, [351](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch10.xhtml#page_351)

mobile devices, [308](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch8.xhtml#page_308)

monitoring services/processes, [356](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch10.xhtml#page_356)

port numbers, [354](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch10.xhtml#page_354)–355

tools for, [355](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch10.xhtml#page_355)–357

types of, [353](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch10.xhtml#page_353)–355

Windows systems, [356](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch10.xhtml#page_356)–357

trust model, [402](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch11.xhtml#page_402)

trust systems, [402](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch11.xhtml#page_402)

Trusted Computer System Evaluation Criteria (TCSEC), [21](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_21)–22

trusted computing, [337](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch9.xhtml#page_337)

Trusted Computing Group (TCG), [337](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch9.xhtml#page_337)

Truth in Caller ID Act, [70](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch2.xhtml#page_70)

T-sight tool, [372](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch10.xhtml#page_372)

TTL (time to live), [66](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch2.xhtml#page_66)

tunnel mode, [373](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch10.xhtml#page_373)

tunneling viruses, [361](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch10.xhtml#page_361)

Twitter, [55](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch2.xhtml#page_55), [306](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch8.xhtml#page_306), [434](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch12.xhtml#page_434)

two-factor authentication, [200](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch5.xhtml#page_200)

Twofish encryption, [390](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch11.xhtml#page_390)

**U**

UBA (User Behavior Analytics), [17](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_17)

Ubiquiti cards, [282](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch7.xhtml#page_282)

Ubuntu, [100](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch3.xhtml#page_100)

UDP (User Datagram Protocol), [10](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_10), [85](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch3.xhtml#page_85), [142](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch4.xhtml#page_142)

UDP ports, [104](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch3.xhtml#page_104), [356](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch10.xhtml#page_356)

UDP scan, [104](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch3.xhtml#page_104)

Ufasoft, [153](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch4.xhtml#page_153)

UIDs (user IDs), [119](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch3.xhtml#page_119)

unicast, [146](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch4.xhtml#page_146), [147](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch4.xhtml#page_147), [151](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch4.xhtml#page_151)

Unicode, [168](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch4.xhtml#page_168), [243](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch6.xhtml#page_243)

unidirectional antenna, [275](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch7.xhtml#page_275)

Uniform Resource Identifier (URI), [238](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch6.xhtml#page_238)

Uniform Resource Locator. *See* URL

UPX tool, [363](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch10.xhtml#page_363)

URG flag, [86](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch3.xhtml#page_86)

URI (Uniform Resource Identifier), [238](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch6.xhtml#page_238)

URL (Uniform Resource Locator), [238](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch6.xhtml#page_238), [248](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch6.xhtml#page_248), [252](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch6.xhtml#page_252)

URL tampering, [242](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch6.xhtml#page_242)

U.S. Government, [362](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch10.xhtml#page_362), [394](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch11.xhtml#page_394), [396](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch11.xhtml#page_396)–397, [417](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch11.xhtml#page_417)

usability, [14](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_14), [415](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch11.xhtml#page_415)

USB, bootable, [408](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch11.xhtml#page_408)

USB wireless adapter, [282](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch7.xhtml#page_282)

User Behavior Analytics (UBA), [17](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_17)

User Datagram Protocol. *See* UDP

user IDs (UIDs), [119](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch3.xhtml#page_119)

Userland exploit, [304](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch8.xhtml#page_304)

**V**

V2V (vehicle-to-vehicle) data exchange, [312](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch8.xhtml#page_312)

VA (validation authority), [400](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch11.xhtml#page_400), [406](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch11.xhtml#page_406)

validation authority (VA), [400](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch11.xhtml#page_400), [406](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch11.xhtml#page_406)

VANET (Vehicle Ad Hoc Network), [312](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch8.xhtml#page_312)

Vehicle Ad Hoc Network (VANET), [312](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch8.xhtml#page_312)

vehicles, [312](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch8.xhtml#page_312), [316](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch8.xhtml#page_316), [331](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch9.xhtml#page_331)

vehicle-to-vehicle (V2V) data exchange, [312](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch8.xhtml#page_312)

virtual machines (VMs), [330](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch9.xhtml#page_330), [332](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch9.xhtml#page_332)

VirtualBox, [100](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch3.xhtml#page_100)

virtualization, [330](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch9.xhtml#page_330)

virus hoax, [358](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch10.xhtml#page_358)

virus making software, [361](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch10.xhtml#page_361)

viruses, [357](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch10.xhtml#page_357)–361, [363](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch10.xhtml#page_363). *See also* AV

VirusTotal, [363](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch10.xhtml#page_363)

Visual Trace tool, [74](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch2.xhtml#page_74)

VMs (virtual machines), [330](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch9.xhtml#page_330), [332](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch9.xhtml#page_332)

voice recognition, [212](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch5.xhtml#page_212)

volumetric attacks, [366](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch10.xhtml#page_366)

vulnerabilities

categories of, [13](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_13)

considerations, [13](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_13)

insider threats, [432](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch12.xhtml#page_432)–434

IoT, [298](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch8.xhtml#page_298), [313](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch8.xhtml#page_313)–316

mobile devices, [299](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch8.xhtml#page_299)–305

overview, [12](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_12)–14

quantifying danger/risk of, [12](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_12)–13

resources/tools, [12](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_12)–14

scanning for, [96](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch3.xhtml#page_96)

web applications, [229](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch6.xhtml#page_229)–232

web servers, [229](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch6.xhtml#page_229)–232, [238](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch6.xhtml#page_238)–241

vulnerability scanning, [115](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch3.xhtml#page_115)–117

IoT, [318](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch8.xhtml#page_318)–320

overview, [115](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch3.xhtml#page_115)

tools for, [115](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch3.xhtml#page_115)–116, [128](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch3.xhtml#page_128)

web servers, [233](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch6.xhtml#page_233)–235

**W**

W3C (World Wide Web Consortium), [228](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch6.xhtml#page_228)–229

W3Techs, [235](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch6.xhtml#page_235)

Walker, Angie, [340](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch9.xhtml#page_340)

Walker, Hope, [340](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch9.xhtml#page_340), [431](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch12.xhtml#page_431)–432

Wall Street Monitor, [51](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch2.xhtml#page_51)

WAN Killer, [86](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch3.xhtml#page_86)

WannaCry attack, [358](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch10.xhtml#page_358)–359, [360](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch10.xhtml#page_360)

war chalking, [276](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch7.xhtml#page_276)

war driving, [281](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch7.xhtml#page_281)

war walking, [281](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch7.xhtml#page_281)

watches, smart, [310](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch8.xhtml#page_310), [312](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch8.xhtml#page_312)

waveforms, [273](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch7.xhtml#page_273)

Wayback Machine, [61](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch2.xhtml#page_61)

“wearables,” 310

Web 2.0, [248](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch6.xhtml#page_248), [330](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch9.xhtml#page_330)

web applications

architecture, [248](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch6.xhtml#page_248)

attack surface, [248](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch6.xhtml#page_248)

attacks on, [247](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch6.xhtml#page_247)–261

considerations, [248](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch6.xhtml#page_248)

entry points, [248](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch6.xhtml#page_248)

injection attacks, [229](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch6.xhtml#page_229), [249](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch6.xhtml#page_249)–250

risks/vulnerabilities, [229](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch6.xhtml#page_229)–232

server-side issues, [248](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch6.xhtml#page_248), [254](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch6.xhtml#page_254)

SQL injection, [254](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch6.xhtml#page_254)–259

testing, [259](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch6.xhtml#page_259)

types of attacks, [249](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch6.xhtml#page_249)–259

web cache poisoning, [244](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch6.xhtml#page_244)

web defacement attacks, [245](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch6.xhtml#page_245)

web front end servers, [235](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch6.xhtml#page_235)

web mirroring, [60](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch2.xhtml#page_60)

web of trust, [402](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch11.xhtml#page_402)

web organizations, [228](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch6.xhtml#page_228)–233

web servers, [228](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch6.xhtml#page_228)–247. *See also* servers

Apache, [235](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch6.xhtml#page_235), [236](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch6.xhtml#page_236)–237

architecture, [235](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch6.xhtml#page_235)–241

attack methodology, [233](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch6.xhtml#page_233)–235

attacks on, [233](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch6.xhtml#page_233)–235, [241](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch6.xhtml#page_241)–247

directory traversal, [241](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch6.xhtml#page_241)–243

footprinting, [233](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch6.xhtml#page_233)–234

parameter tampering, [242](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch6.xhtml#page_242)

password cracking, [245](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch6.xhtml#page_245)

protecting, [261](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch6.xhtml#page_261)

risks/vulnerabilities, [229](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch6.xhtml#page_229)–232, [238](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch6.xhtml#page_238)–241

types of attacks, [241](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch6.xhtml#page_241)–247

types of servers, [235](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch6.xhtml#page_235)

web spiders, [54](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch2.xhtml#page_54), [76](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch2.xhtml#page_76), [233](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch6.xhtml#page_233)

web-based hacking, [227](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch6.xhtml#page_227)–269

web applications, [247](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch6.xhtml#page_247)–261

web servers, [233](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch6.xhtml#page_233)–235, [241](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch6.xhtml#page_241)–247

webcrawlers, [54](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch2.xhtml#page_54)

WebGoat project, [231](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch6.xhtml#page_231)–232

website footprinting, [60](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch2.xhtml#page_60)–61

Website Watcher, [61](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch2.xhtml#page_61)

websites

company, [51](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch2.xhtml#page_51)–52

competitive intelligence on, [51](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch2.xhtml#page_51)–52, [76](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch2.xhtml#page_76)–77

cookies, [60](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch2.xhtml#page_60), [205](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch5.xhtml#page_205), [253](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch6.xhtml#page_253)–254

defacement attacks, [245](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch6.xhtml#page_245)

dynamic web pages, [248](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch6.xhtml#page_248)

fake, [284](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch7.xhtml#page_284)

increase in attacks, [260](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch6.xhtml#page_260)

mirroring, [60](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch2.xhtml#page_60), [234](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch6.xhtml#page_234), [248](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch6.xhtml#page_248)

scanning targets, [50](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch2.xhtml#page_50)

traffic statistics, [51](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch2.xhtml#page_51)

Wayback Machine, [61](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch2.xhtml#page_61)

WeFi tool, [284](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch7.xhtml#page_284)

WEP (Wired Equivalent Privacy), [277](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch7.xhtml#page_277)–278, [280](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch7.xhtml#page_280)

WEP attacks, [287](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch7.xhtml#page_287)–289

WEP cracking, [287](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch7.xhtml#page_287)–289

WEP keys, [277](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch7.xhtml#page_277), [278](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch7.xhtml#page_278)

WEPAttack, [288](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch7.xhtml#page_288)

WEPCrack, [288](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch7.xhtml#page_288)

WFETCH tool, [244](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch6.xhtml#page_244)

whaling, [438](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch12.xhtml#page_438)

white hats, [25](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_25)

white-box testing, [33](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_33)

whois tools, [68](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch2.xhtml#page_68)–70

Wi-Fi connections, [307](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch8.xhtml#page_307), [308](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch8.xhtml#page_308)

WiFi Explorer, [281](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch7.xhtml#page_281)

Wi-Fi hotspots, [285](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch7.xhtml#page_285), [307](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch8.xhtml#page_307)

WiFi Pilot, [289](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch7.xhtml#page_289)

Wi-Fi Protected Access. *See* WPA

WiFiFoFum, [281](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch7.xhtml#page_281)

WiFinder, [281](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch7.xhtml#page_281)

WIGLE service, [281](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch7.xhtml#page_281), [283](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch7.xhtml#page_283)

WikiLeaks, [370](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch10.xhtml#page_370)

WiMAX standard (802.16), [272](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch7.xhtml#page_272)

WINARPAttacker, [153](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch4.xhtml#page_153)

Windows 8, [118](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch3.xhtml#page_118), [119](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch3.xhtml#page_119)

Windows 10, [118](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch3.xhtml#page_118)

Windows root, [193](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch5.xhtml#page_193)

Windows Server, [117](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch3.xhtml#page_117)

Windows Service Manager, [356](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch10.xhtml#page_356)

Windows systems

alternate data stream, [212](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch5.xhtml#page_212)–214

enumeration, [117](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch3.xhtml#page_117)–119

hashing passwords, [185](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch5.xhtml#page_185)–189

*vs.* Linux systems, [191](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch5.xhtml#page_191)–192

MMC, [192](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch5.xhtml#page_192)–193

NTFS file streaming, [212](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch5.xhtml#page_212)–213

password cracking, [184](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch5.xhtml#page_184)–189, [207](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch5.xhtml#page_207)

password recovery tools, [204](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch5.xhtml#page_204)

registry, [189](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch5.xhtml#page_189)–192, [214](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch5.xhtml#page_214)

route tables, [193](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch5.xhtml#page_193)

security, [184](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch5.xhtml#page_184)–193

Trojans, [356](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch10.xhtml#page_356)–357

verifying integrity of, [357](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch10.xhtml#page_357)–358

Windows XP, [117](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch3.xhtml#page_117)

WinDump sniffer, [158](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch4.xhtml#page_158)

Winfingerprint, [123](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch3.xhtml#page_123)

WinPcap, [139](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch4.xhtml#page_139)

Wired Equivalent Privacy. *See* WEP

wireless access points, [274](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch7.xhtml#page_274), [278](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch7.xhtml#page_278), [281](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch7.xhtml#page_281), [284](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch7.xhtml#page_284)–285

wireless adapters, [282](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch7.xhtml#page_282)

wireless antennas, [274](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch7.xhtml#page_274)–276

wireless cards, [282](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch7.xhtml#page_282)

wireless hacking, [280](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch7.xhtml#page_280)–290

discovery, [281](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch7.xhtml#page_281)–284

encryption attacks, [287](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch7.xhtml#page_287)–289

IoT, [313](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch8.xhtml#page_313)

MAC spoofing, [287](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch7.xhtml#page_287)

overview, [271](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch7.xhtml#page_271)–272

smartphones, [272](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch7.xhtml#page_272), [281](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch7.xhtml#page_281)

sniffing, [289](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch7.xhtml#page_289)–290

WEP attacks, [287](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch7.xhtml#page_287)–289

wireless jammers, [285](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch7.xhtml#page_285)–287

wireless networks, [271](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch7.xhtml#page_271)–295

802.11 standards, [272](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch7.xhtml#page_272)–273

access points, [274](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch7.xhtml#page_274), [278](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch7.xhtml#page_278), [281](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch7.xhtml#page_281), [284](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch7.xhtml#page_284)–285

ad hoc, [273](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch7.xhtml#page_273), [274](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch7.xhtml#page_274), [285](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch7.xhtml#page_285)

antennas, [274](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch7.xhtml#page_274)–276

architecture, [272](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch7.xhtml#page_272)–277

authentication, [276](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch7.xhtml#page_276)–277

basic setup, [273](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch7.xhtml#page_273)–274

basics, [272](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch7.xhtml#page_272)–277

Bluetooth, [272](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch7.xhtml#page_272)

considerations, [272](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch7.xhtml#page_272)

encryption, [277](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch7.xhtml#page_277)–280, [287](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch7.xhtml#page_287)–289

finding/discovery, [281](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch7.xhtml#page_281)–284

Gigabit Wi-Fi, [279](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch7.xhtml#page_279)

hacking. *See* wireless hacking

identifying, [276](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch7.xhtml#page_276), [281](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch7.xhtml#page_281)–284

infrastructure mode, [274](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch7.xhtml#page_274)

modes, [273](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch7.xhtml#page_273)–274

security, [276](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch7.xhtml#page_276)–280

service set identifiers, [276](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch7.xhtml#page_276)

standards, [272](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch7.xhtml#page_272)–273

WEP. *See* WEP

WPA, [278](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch7.xhtml#page_278)–280, [288](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch7.xhtml#page_288)–289

WPA2, [278](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch7.xhtml#page_278)–280, [288](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch7.xhtml#page_288)–289

wireless NICs, [274](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch7.xhtml#page_274)

Wireless Security Auditor tool, [288](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch7.xhtml#page_288)

wireless sniffing, [289](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch7.xhtml#page_289)–290

wireless standards, [272](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch7.xhtml#page_272)–273

Wireshark sniffer, [100](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch3.xhtml#page_100), [124](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch3.xhtml#page_124), [156](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch4.xhtml#page_156)–159, [289](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch7.xhtml#page_289)

wiretapping, [138](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch4.xhtml#page_138), [148](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch4.xhtml#page_148)–149

World Wide Web Consortium (W3C), [228](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch6.xhtml#page_228)–229

worms, [357](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch10.xhtml#page_357), [361](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch10.xhtml#page_361)–363

WPA (Wi-Fi Protected Access), [278](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch7.xhtml#page_278)–280, [288](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch7.xhtml#page_288)–289

WPA2 Enterprise, [278](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch7.xhtml#page_278)–279, [280](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch7.xhtml#page_280)

WPA2 Personal, [279](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch7.xhtml#page_279)

WPA2 standard, [278](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch7.xhtml#page_278)–280, [288](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch7.xhtml#page_288)–289

wrappers, [351](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch10.xhtml#page_351)

wrapping attacks, [342](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch9.xhtml#page_342)

**X**

X.509 standard, [402](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch11.xhtml#page_402)

XMAS scan, [102](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch3.xhtml#page_102), [105](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch3.xhtml#page_105), [106](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch3.xhtml#page_106)

XML (Extensible Markup Language), [108](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch3.xhtml#page_108), [239](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch6.xhtml#page_239)

XML External Entities (XXE), [230](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch6.xhtml#page_230)

XML processors, [230](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch6.xhtml#page_230)

XOR ciphers, [389](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch11.xhtml#page_389)

XOR comparison, [93](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch3.xhtml#page_93)

XOR (exclusive-or) operation, [278](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch7.xhtml#page_278), [388](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch11.xhtml#page_388)–389

XSS (cross-site scripting), [230](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch6.xhtml#page_230), [251](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch6.xhtml#page_251)–253

XXE (XML External Entities), [230](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch6.xhtml#page_230)

**Y**

Yagi antenna, [275](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch7.xhtml#page_275)

Yahoo!, [370](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch10.xhtml#page_370)

YouTube, [53](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch2.xhtml#page_53), [246](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch6.xhtml#page_246)

Yubikey token, [446](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch12.xhtml#page_446)

**Z**

Zenmap, [98](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch3.xhtml#page_98), [100](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch3.xhtml#page_100), [105](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch3.xhtml#page_105), [108](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch3.xhtml#page_108)

zero-day attack vector, [15](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_15)

ZeuS-in-the-Mobile (ZitMo), [442](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch12.xhtml#page_442)

Zigbee Framework, [320](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch8.xhtml#page_320)

Zigbee standard (802.16), [272](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch7.xhtml#page_272)

ZitMo (ZeuS-in-the-Mobile), [442](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch12.xhtml#page_442)

zombies, [29](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_29), [439](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch12.xhtml#page_439)

zone file, [66](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch2.xhtml#page_66)

zone transfers, [63](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch2.xhtml#page_63), [66](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch2.xhtml#page_66), [71](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch2.xhtml#page_71)

zones, security, [10](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch1.xhtml#page_10)–12

Z-Wave, [320](https://learning.oreilly.com/library/view/ceh-certified-ethical/9781260454567/ch8.xhtml#page_320)