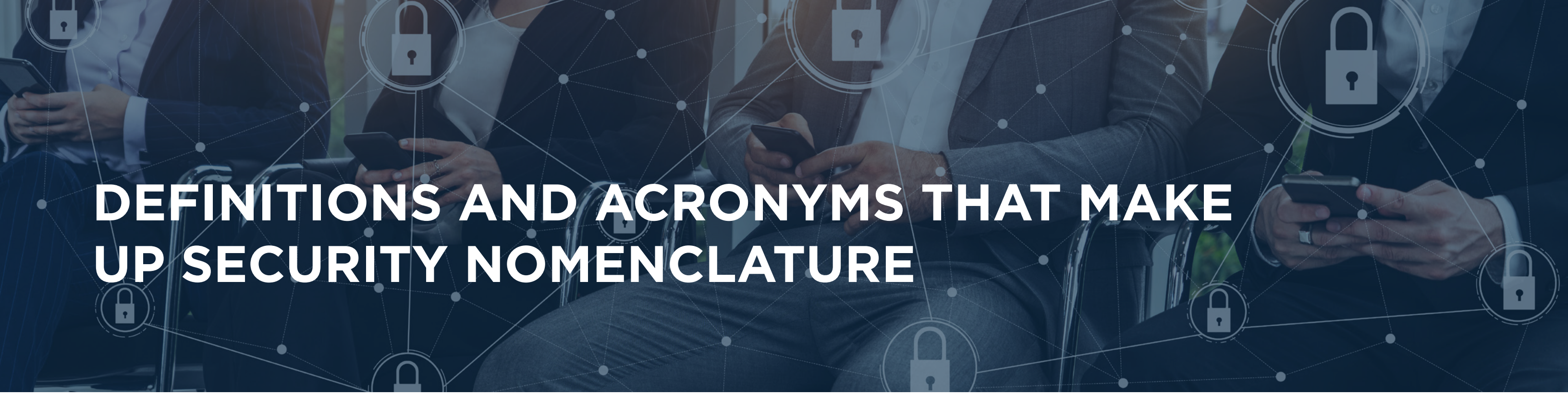

DEFINITIONS AND ACRONYMS THAT MAKE UP SECURITY NOMENCLATURE

Cybercrime is a very real threat to your organization. You need security technology to prevent breaches — know the various risks you face, so you can ensure that you're protected. Below are some examples of these threats:

CYBERSECURITY THREATS

Adware. A software application that automatically downloads or displays advertising banners or pop-ups when an application is running or when a user is online. It can be defined as software that feloniously creeps advertisements into your browsers/applications with the goal of producing monetary payoff for adware producers.

Attribution. The process of establishing who is behind a hack. Often, attribution is the most difficult part of responding to a major breach since experienced hackers may hide behind layers of online services that mask their true location and identity. Many incidents may never produce any satisfactory attribution.

Backdoor. Entering a protected system using a password can be described as going through the front door. Companies may build "backdoors" into their systems, however, so that developers can bypass authentication and dive right into the program. Backdoors are usually secret but may be exploited by hackers if/when they're revealed or discovered.

Baiting. An attack and defense strategy that relies on the curiosity and greed of the victim or a specific target. It is almost like a phishing attack, but this comes with a promise of a product or an item that hackers use to compel users to click on it.

Black Hat Hacker. Someone hacking for personal gain and/or who engages in illicit and unsanctioned activities. They often attempt to sell the weaknesses they discover to other hackers or use them.

Botnet. Your computer could be part of a botnet, and you might not know it. Botnets, or zombie armies, are networks of computers controlled by an attacker. Having control over hundreds/ thousands of computers lets bad actors perform cyberattacks (like DDoS). Hackers deploy malware to infect random computers that are connected to the internet to create the botnet. Infected machines can perform tasks in the background without the user noticing.

Brute Force. A brute force attack is arguably the least sophisticated way of breaking into a password-protected system, short of simply obtaining the password itself. It usually consists of an automated process of trial and error to guess the correct passphrase. Most modern encryption systems use different methods for slowing down brute force attacks, making it hard or impossible to try all combinations in a reasonable amount of time.

Bug/Bug Bounty. A bug is a flaw or error in a software program. Some are harmless or merely annoying, but some are exploitable. Many companies have started using "Bug Bounty Programs" to pay anyone who spots a bug before the bad guys do.

Cracking. A general term that describes breaking into a security system. The New Hacker's Dictionary (MIT Press) states "hacking" and "hacker" have replaced "cracking" and "cracker," but that's misleading. Hackers are tinkerers, not necessarily bad guys. Crackers are malicious. You may also see cracking used to refer to breaking, say, digital copyright protections — which many people feel is a just and worthy cause — and in other contexts, such as penetration testing, without the negative connotation.

Crypto. Short for cryptography, the science of secret communication or the procedures and processes for hiding data and messages with encryption.

Chip-off. An attack that requires the hacker to physically remove memory storage chips in a device so that information can be scraped from them using specialized software. This attack has been used by law enforcement to break into PGP-protected phones.

Dark Web. Sites that are not indexed by Google and are only accessible through specialty networks such as Tor. Often the dark web is used by website operators who want to remain anonymous. Everything on the dark web is on the deep web, but not everything on the deep web is on the dark web.

Data Breach. The most common cybersecurity term, it is an unauthorized entry into an organization's database, providing hackers access to all customer data (e.g., SSNs, bank account numbers, passwords, credit card numbers). A data breach exposes the organization's most valuable and sensitive information.

DDoS. DDoS stands for Distributed Denial of Service Attack. This type of cyberattack has become popular in recent years because it's relatively easy to execute and its effects are obvious immediately. The attacker uses a number of computers to flood the target with data or data requests, causing the target, usually a website, to slow down or become unavailable. Attackers may also use the simpler Denial of Service (DoS) attack, which is launched from one computer.

Deep Web. This term and "dark web" or "dark net" are sometimes used interchangeably, though they shouldn't be. The deep web is the part of the internet that is not indexed by search engines. That includes password-protected pages, paywalled sites, encrypted networks, and databases.

DEF CON. One of the most famous hacking conferences in the US or the world, is held every summer in Las Vegas.

Evil Maid Attack. An evil maid attack is a hack that requires physical access to a computer — the kind of access an evil maid might have while tidying his or her employer's office. By having physical access, a hacker can install software to track your use and gain a doorway even to encrypted information.

Exploit. A way or process to take advantage of a bug or vulnerability in a computer or application. Not all bugs lead to exploits.

Hacker. This term has become incorrectly associated with criminal behavior. Originally, hackers were simply tinkerers or people who enjoyed "exploring the details of programmable systems and how to stretch their capabilities." Hackers refer to good guys (white hats) and cybercriminals (black hats).

Keylogger. A software program, hardware device, or virus which reports keyboard strokes. Criminals use keyloggers to monitor and track input on a numerical pad or keyboard with the intent of capturing the most sensitive information like credit/debit card numbers, PINs, and passwords in real-time.

Lulz. An internet-speak variation on "lol" (short for "laughing out loud") employed regularly among the black hat hacker set, typically to justify a hack or leak performed at the expense of another person or entity. Sample use: "y did I leak all contracts and employee info linked to Sketchy Company X? for the lulz."

Malware. Stands for "malicious software." It's software that accesses, controls, and damages systems using harmful code. It's also an umbrella term used for various types of malicious software that have been designed to cause damage to a system, including ransomware, viruses, worms, spyware, adware, and trojans (trojan horses). They're often delivered through spam emails.

Man-in-the-middle (MitM). A common attack where someone puts themselves between two parties, impersonating them. This allows the attacker to intercept and potentially alter their communications. The attacker can passively listen in, relay messages and data between the two parties, or even alter and manipulate the data flow.

Phishing. The most common technique used by hackers to steal personal information (e.g., emails, phone numbers, PINs, passwords, bank account numbers, credit card numbers). It's more of a form of social engineering than hacking or cracking. In a phishing scheme, the attacker may reach out to the victim to extract specific information that can be used in a later attack, often through an email from a legitimate organization (e.g., Google, Facebook, bank, cell company, credit card company, charitable trust) asking the victim to reply with personal information, download a file, or click a link that infects their system with malware. Attackers blast out phishing attempts by the thousands, but sometimes employ more targeted attacks known as spearphishing.

Pwned. Computer nerd jargon (or "leetspeak") for the verb "own." In the video game world, a player that beats another player can say he pwned him. Among hackers, the term has a similar meaning, signifying the hacker has gained access to another user's computer. Visit HaveIBeenPwned.com to see if your online accounts have been compromised.

Rainbow Table. A complex technique allowing hackers to simplify the process of guessing what passwords hide behind a "hash."

Ransomware/Cryptopviral Extortion. A kind of malware that prevents you from accessing certain computer files by encrypting them, in essence, locking up your computer. You'll see a message telling you how much the ransom is and where to send the (bitcoin) payment in order to get your files back. It's a good racket for hackers, with many considering it an "epidemic" as people typically are willing to pay a few hundred bucks in order to recover their machine. It's not just individuals; organizations have received, and paid, demands for millions of dollars. With ransom payment, the victim can unlock and restore access to their computer. WannaCry and NotPetya are the most aggressive forms of Ransomware.

Remote Access Tool/Remote Access Trojan (RAT). An attacker who successfully installs a RAT on a computer can gain full control of the machine. There is also a legitimate business in RATs for people who want to access their office computer from home. There are many malicious RATs available in the internet's underground for sale (or free), so attackers can be unskilled and still utilize this sophisticated tool.

Rootkit. A particular type of malware that lives deep in a system and is activated each time it boots up, even before the operating system starts. This makes rootkits hard to detect, persistent, and able to capture practically all data on an infected computer.

Script Kiddies. A derisive term for someone who's a little computer savvy, and only able to use off-the-shelf software to do things like knock websites offline or sniff passwords over an unprotected Wi-Fi access point. This is basically a term to discredit someone who claims to be a skilled hacker.

Shodan. It's been called "hacker's Google" and a "terrifying" search engine for connected devices rather than websites. Using Shodan, you can find unprotected webcams, baby monitors, printers, medical devices, gas pumps, and infrastructure like wind turbines. Shodan's true value is in helping researchers find unprotected devices and alert owners so they can secure them.

Side Channel Attack. Your computer's hardware is always emitting a steady stream of barely perceptible electrical signals. This attack identifies patterns in these signals to learn what kind of computations the machine is performing. For example, a hacker can listen to your hard drive "whir" while generating a secret encryption key, and be able to reconstruct that key, effectively stealing it without your knowledge.

Spoofing. One of the most common techniques used by black hat hackers is to hide their identity and fool people over the internet, by pretending to be a trusted source. This involves sending emails while changing the IP address so that it seems to come from a trusted source, to gain unauthorized entry into a secure system.

Sniffing. A way to intercept data sent over a network without being detected, using special sniffer software. Once data is collected, a hacker can sift through it to get useful information, like passwords. It's a particularly dangerous and hard-to-detect hack and can be performed from inside or outside a network.

Social Engineering. Sometimes gaining entry to a secure system is as easy as placing a phone call or sending an email while pretending to be somebody else — namely someone who regularly accesses a system but forgot their password on a given day. Phishing attacks include aspects of social engineering because they involve convincing somebody of an email sender's legitimacy.

Spearphishing. Phishing and spearphishing are often used interchangeably, but the latter is a tailored, targeted form of phishing where hackers try to trick victims into clicking on malicious links or attachments pretending to be from a close acquaintance, rather than a generic sender. When done well, spearphishing can be extremely effective and powerful.

Spoofing. Hackers can trick people into falling for a phishing attack by forging their email address, making it look like the address of someone the target knows for example. Spoofing can also be used in telephone scams, or to create a fake website address.

Spyware. A specific type of malware of malicious software designed to spy, monitor, and potentially steal data from the target.

State Actor. Hackers or groups of hackers who are backed by a government (often the US, Russia, or China). These hackers have virtually unlimited legal and financial resources of a nation-state. State actors can also be a group of hackers who receive tacit (or at least hidden from the public) support from their governments, such as the Syrian Electronic Army.

Tor. Short for The Onion Router. Originally developed by the United States Naval Research Laboratory, it's now used by bad guys (hackers, pedophiles) and good guys (activists, journalists) to anonymize their activities online. Basically, there is a network of computers around the world — some operated by universities, some by individuals, some by governments — that will route your traffic in byzantine ways in order to disguise your true location. The Tor network is this collection of volunteer-run computers. The Tor Project is the nonprofit that maintains the Tor software. The Tor browser is a free piece of software that lets you use Tor. Tor hidden services are websites that can only be accessed through Tor.

Virus. A virus is a software program (malicious code) typically embedded and hidden in a program or file which copies itself to other programs with the intent of corrupting, erasing, and destroying information on a computer without the user's knowledge. Unlike a worm, it needs human action to spread (such as a human forwarding a virus-infected attachment or downloading a malicious program). Viruses infect computers to steal data, delete data, encrypt it, or mess with it in just about any other way.

Warez. Refers to pirated software that's typically distributed via technologies like BitTorrent and Usenet. Warez is sometimes laden with malware, taking advantage of people's desire for free software or media files.

White Hat Hacker. Someone who uses their hacking skills to find vulnerabilities, alert companies, and improve services.

Worm. A standalone malware that replicates itself without human interaction, with the sole intent of spreading itself to other systems in a connected network. These are the most common type of malware programs that cause harm to their host networks by overloading the server and consuming bandwidth.

Zero-Day/Zero-Day Virus/"0day". A bug that's unknown to the software vendor, or at least not yet patched. The name comes from the notion that there have been zero days between the discovery of the bug or flaw and the first attack taking advantage of it. Zero-days are the most prized bugs and exploits for hackers because a fix has yet to be deployed for them, so they're almost guaranteed to work.

SOLUTIONS AND CONCEPTS

Active Directory (AD). Microsoft's directory and identity management service for Windows domain networks used for user authentication and authorization.

Attack/Threat Surface. The sum of the different points, or attack vectors, where an unauthorized user can try to access a system, enter data, or extract data from an environment is called the attack or threat surface. Networks are dynamic, constantly growing to incorporate new devices, data, applications, and users, as business needs evolve. Organizations must constantly monitor their attack surface to identify and block potential threats as quickly as possible. Understanding your threat surface is a critical step to improving your network security posture. Keeping the attack surface as small as possible is a basic security measure.

Attack Surface Management (ASM). Refers to processes and technologies that take a hacker's view and approach to an organization's attack surface — discovering and continuously monitoring assets and vulnerabilities hackers see and attempt to exploit when targeting the organization.

Authentication. Is the process of identifying whether someone/something is who or what it declares to be. It is used to provide access control for systems by verifying whether a user's ID matches the ID of authorized users in the database or on the data authentication server.

Blue Team. A group of individuals who perform an analysis of information systems to verify the effectiveness of each security measure and make certain all security measures will continue to be effective after implementation. They act as a defensive team fortifying the structure while a Red Team postures for offensive attacking.

Cloud Access Security Broker (CASB). On-premises or Cloud-based software that sits between a Cloud service consumer and a Cloud service provider. It serves as a tool for enforcing an organization's security policies through risk identification and regulation compliance whenever its Cloud-residing data is accessed.

Cloud Security. The procedures and technologies that secure Cloud computing environments against internal and external Cybersecurity threats.

Cloud Security Gateway. On-premises enforcement points that are implemented between Cloud service consumers and Providers to interject security policies as Cloud-based resources are accessed.

Compliance. The minimum security/process standard/conduct an organization adheres to. This is a legal concern for many verticals and can be resolved through proper technology implementation.

Cybersecurity Risk Assessment. The process of identifying, analyzing, and evaluating risk. It helps to ensure that the Cybersecurity controls chosen are appropriate to the risks the organization faces.

Data Loss Prevention (DLP). Method to make sure that users do not send sensitive or critical information outside the corporate network. The term describes software products that help a network administrator control the data that users can transfer. DLP products use business rules to classify and protect confidential and critical information so that unauthorized users cannot accidentally or maliciously share data, which would put the organization at risk. Organizations are adopting DLP because of insider threats and rigorous data privacy laws, many of which have stringent data protection or data access requirements. In addition to monitoring and controlling endpoint activities, some DLP tools can also be used to filter data streams on the Network and protect data in motion.

DDoS Mitigation. Technology and techniques that prevent and combat a DDoS (Distributed Denial of Service) attack, implemented on networks attached to the internet.

Digital Certificate. A digital passport or stamp of approval that proves the identity of a person, website, or service on the internet. In more technical terms, it proves that someone is in possession of a certain unforgeable cryptographic key. Common digital certificates are for websites, which ensure a connection to them is properly encrypted. Displayed on your browser as a green padlock.

Disaster Recovery (DR). Organization's ability to respond to and recover from an event that negatively affects operations. DR methods goals are to enable the organization to regain use of critical systems and IT infrastructure as soon as possible after a disaster occurs.

Domain Name System Security. DNS converts a domain name into an IP number. The Domain Name System Security secures the DNS service, protocol, and web traffic from cyber-attacks

Encryption. The process of making information unreadable to anybody who is not authorized to access it. The information is encoded using PKI and SSL.TLS protocol, and only authorized users can decode the encrypted data using decryption keys or passwords. The opposite is decryption, the decoding of the message. Both encryption and decryption are functions of cryptography. Encryption is used by individuals as well as corporations and in digital security for consumer products.

End-to-End Encryption. A particular type of encryption where a message or data gets scrambled or encrypted on one end (e.g., computer or phone) and is decrypted on the other (another computer or phone). The data is scrambled in a way that, in theory, only the sender and receiver can read.

Endpoint Detection & Response (EDR)/Endpoint Detection and Threat Response (EDTR). An integrated, layered approach to endpoint protection that combines real-time continuous monitoring and endpoint data analytics with rule-based automated response. Next-Gen antivirus and malware protection.

Endpoint Protection. An approach to the protection of computer networks that are remotely bridged to client devices. Protection platforms examine files as they enter the network for security.

Ethical/White Hat Hacker. A person authorized to test out systems and servers to identify any security vulnerabilities and inform the organization as to where security needs to be strengthened.

Extended Detection & Response (XDR). A consolidation of tools and data that provides extended visibility, analysis, and response across endpoints, workloads, users, and Networks.

Firewall. A defensive security technology developed with the intent of keeping bad guys out. It's software used to maintain security for private networks by keeping the intruders out — a firewall blocks or permits network traffic based on a pre-defined set of security rules. Firewalls can be hardware- or software-based.

Forensics. Investigators look for digital fingerprints instead of physical ones. This process usually involves trying to retrieve messages or other information from a device (e.g., phone, computer, server) used by a suspected criminal.

Government Communications Headquarters (GCHQ). The UK's equivalent of the US National Security Agency, focuses on foreign intelligence, especially around terrorism threats and Cybersecurity. It also investigates the digital child pornography trade.

Governance, Risk, and Compliance (GRC). Structured way to align IT with business goals while managing risks and meeting all industry and government regulations. Includes tools and processes to unify an organization's governance and risk management with its technological innovation and adoption. (e.g. HIPPA, PCI, Cybersecurity insurance).

Hacktivist. Someone who uses their hacking skills for political ends; their actions may be small (defacing the public website of a security agency or other government department) or large (stealing and distributing sensitive government information). Anonymous is an example of a hacktivist group.

Hashing. Say you have a piece of text that should remain secret, like a password. You could store the text in a secret folder on your machine, but if anyone gained access to it, you're in trouble. To keep the password a secret, you could also "hash" it with a program that executes a function resulting in garbled text representing the original information. Companies store passwords/facial recognition data with hashes to improve security.

HTTPS/SSL/TLS. Hypertext Transfer Protocol, with the "S" for "Secure." The Hypertext Transfer Protocol (HTTP) is the basic framework that controls how data is transferred across the web, while HTTPS adds a layer of encryption that protects your connection to the most important sites in your daily browsing (e.g., bank, email provider, social network). HTTPS uses SSL and TLS protocols to protect your connection and prove the identity of the site.

Identity Access Management. A framework of policies and technologies that allows the right individuals to access the right resources at the right times, for the right reasons.

Incident Response. An organized approach to contain, manage, and recover from a security breach or event. The objective is to quickly respond to the situation to reduce recovery time and cost.

Infosec. An abbreviation of "Information Security." It's the inside baseball term for what's more commonly known as Cybersecurity.

Intrusion Detection System. A solution that monitors a network for malicious activity. The system reports the activity to an administrator or collects it using a Security Information and Event Management (SIEM) system.

Intrusion Detection Systems (IDS). Solution (set of tools/resources) that monitors Network events and analyzes them to detect security incidents and imminent threats. IDS can either be host-based or network-based.

Intrusion Prevention System (IPS). Solution (set of tools/resources) that performs intrusion detection and then goes one step ahead and prevents any detected threats.

Intrusion Response (IR). The steps used to prepare for, detect, contain, and recover from a data breach.

Intrusion Response & Remediation (IRR). Customized, industry-informed mitigation plan that an organization should closely follow during a breach scenario or other form of Cyberattack.

Jailbreak. Circumventing the security of a device, like an iPhone or a PlayStation, to remove a manufacturer's restrictions, generally with the goal to make it run software from non-official sources.

Keys. Modern cryptography uses digital "keys." In the case of PGP encryption, a public key is used to encrypt, or "lock," messages, and a secret key is used to decrypt, or "unlock," them. In other systems, there may only be one secret key that is shared by all parties. In either case, if an attacker gains control of the key that does the unlocking, they may have a good chance of gaining access.

Log Management. An approach consisting of processes and policies that deal with large volumes of computer-generated log messages.

Malware Defense. Protection that blocks malicious code from tampering with system settings or contents, capturing sensitive data, or spreading.

Managed Detection & Response (MDR). Often in an Incident Investigation, using specialized endpoint software from leaders such as SentinelOne, Crowdstrike, or Cybereas, MDR Security service Providers will investigate an alert and determine whether it is a true incident or a false positive. This is accomplished through a combination of data analytics, Machine Learning (ML) from the EDR and SIEM being used to manage and human investigation.

Managed Security Services Provider (MSSP). Outsourced monitoring and management of security devices and systems. MSSPs use high-availability security operation centers to provide 24/7 services to reduce the amount of security staff an organization needs to hire and train. An MSSP can also handle upgrades, system changes, and modification.

Multi-Factor Authentication. An authentication system that requires more than one distinct factor for successful authentication. This uses three authentication factors: something you know, something you have, and something you are.

Next-Generation Firewall. A network security device that provides capabilities beyond a traditional firewall. It includes extra features such as application awareness and control, integrated intrusion prevention, and Cloud-delivered threat intelligence.

Metadata. Simply data about data. If sending an email, for example, the text you type will be the content of the message, but the address you used to send it, the address you sent it to, and the time you sent it would all be metadata. This may sound innocuous, but with enough sources of metadata (e.g., geolocation information from a photo posted to social media), someone's identity or location can easily be pieced together.

MITRE ATT&CK. Stands for MITRE Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK). The MITRE ATT&CK framework is a curated knowledge base and model for cyber adversary behavior, reflecting the various phases of an adversary's attack lifecycle and the platforms they are known to target.

National Institute of Standards and Technology (NIST). An arm of the US Department of Commerce dedicated to science and metrics that support industrial innovation. NIST is responsible for developing information security standards for use by the federal government and is therefore often cited as an authority on which encryption methods are rigorous enough to use given modern threats.

Nonce. A blend of "number" and "once," nonce literally means "a number only used once" — a string of system-generated numbers to identify a user for a one-time-use session or specific task. After that session or set time period, the number isn't used again.

OpSec. OpSec is short for operational security, and it's all about keeping information secret, online and off. Originally a military term, OpSec is a practice and in some ways a philosophy that begins with identifying what information needs to be kept secret, and whom you're trying to keep it a secret from. "Good" OpSec flows from there and may include everything from passing messages on Post-Its instead of emails to using digital encryption.

OTR. What do you do if you want to have an encrypted conversation, but it needs to happen fast? OTR (Off-the-Record) is a protocol for encrypting instant messages end-to-end. Unlike PGP which is generally used for email and so each conversant has one public and one private key in their possession, OTR uses a single temporary key for every conversation, which makes it more secure if an attacker hacks into your computer and gets a hold of the keys. OTR is generally easier to use than PGP.

Password Managers. Using the same password for all logins is a bad idea. Once a hacker gets access to one account, they have access to all. Memorizing a unique string of characters for every platform is daunting. Password Manager software keeps track of your various passwords for you or even auto-generates complicated/long passwords for you. All you need to remember is your master password to log into the manager and access your many different logins.

Penetration Testing/Pentesting. An authorized simulated attack (by Pentesters, people employed to identify weak points) that evaluates the security of a computer system. This is done to evaluate the security of a system before an attacker does. A penetration test helps determine how to best mitigate and protect an organization. Pentesting is related to Red Teaming, although it may be done in a more structured, less aggressive way.

PGP. "Pretty Good Privacy" is a method of encrypting data, generally emails, so that anyone intercepting them will only see garbled text. PGP uses asymmetric cryptography, which means that the person sending a message uses a "public" encryption key to scramble it, and the recipient uses a secret "private" key to decode it. Despite being more than two decades old, PGP is still a formidable method of encryption, although it can be difficult to use in practice, even for experienced users.

Plaintext/Cleartext. Refers to text that is kept plain, out in the open, in the clear, or more specifically, ungarbled with encryption. Companies with poor security may store user passwords in plaintext, even if the folder they're in is encrypted, just waiting for a hacker to steal.

RADIUS (Remote Authentication Dial-In User Service). A client-server protocol and software that enables remote access servers to communicate with a central server to authenticate dial-in users and authorize their access to the requested system or service.

Red Team. To ensure the security of their computer systems and to expose unknown vulnerabilities, companies hire hackers who organize into a "Red Team" to run oppositional attacks against the system and attempt to completely take it over. In these cases, being hacked is a good thing, because organizations can fix vulnerabilities before they're exploited. Red teaming is employed across many sectors, including military strategy. They're the "offensive attacking team" to the Blue Team's "defense."

Root. In most computers, "root" is the common name given to the most fundamental (and thus most powerful) level of system access or is the name for the account that has those privileges. That means the "root" can install applications and delete and create files. If a hacker "gains root," they can do whatever they want on the computer or system they compromised.

Salting. When protecting passwords or text, "hashing" is a fundamental process that turns plaintext into garbled text. To make hashing even more effective, companies or individuals can add an extra series of random bytes, known as a "salt," to the password before the hashing process. This adds an extra layer of protection.

Sandbox. In computer security, a sandbox is a security mechanism for separating running programs, usually to mitigate system failures or software vulnerabilities from spreading. It's often used to execute untested or untrusted programs or code, possibly from unverified or untrusted third parties, suppliers, users, or websites, without risking harm to the host machine or operating system. Often sandboxes are seen as a specific example of virtualization, since VM instances of sandboxes are frequently used to test unverified programs that may contain a virus or other malicious code, without allowing the software to harm the host device.

Secure Access Service Edge (SASE)/Secure Services Edge. A framework that applies SD-WAN with security to enable Cloud adoption and the ability for organizations to apply security no matter the location of users.

Security Incident Event Management (SIEM). A system that collects, stores, investigates, supports, mitigates, and reports on security data for incident response, forensics, and regulatory compliance.

Security Information and Event Management (SIEM). Solution that helps organizations detect, analyze, and respond to security threats before they harm operations.

Security Operations Center (SOC). Team of IT security professionals that protects the organization by monitoring, detecting, analyzing, and investigating cyber threats. Networks, servers, computers, endpoint devices, operating systems, applications, and databases are continuously examined for signs of a Cybersecurity incident. The SOC team analyzes feeds, establishes rules, identifies exceptions, enhances responses, and looks for new vulnerabilities.

Signature. Another function of PGP, besides encrypting messages, is the ability to "sign" messages with your secret encryption key. Since this key is only known to one person and is stored on their own computer and nowhere else, cryptographic signatures are supposed to verify that the person who you think you're talking to actually is that person. This is a good way to prove that you really are who you claim to be on the internet.

Single Sign-On (SSO). Authentication method that lets users access multiple applications and services using a single set of login credentials. SSO can help businesses improve user satisfaction and productivity, strengthen access security, and reduce IT operations expense and complexity.

Structured Data. Information that conforms to a data model with a well-defined structure and consistent order and can be easily accessed and used by a person or a computer program. This is often information stored in a relational database (RDBMS), with mapped designated fields ranging from an individual data point, such as a number (e.g., revenues), date (e.g., the date of a transaction), or text (e.g., a name), to data that includes multiple individual data points (e.g., an entire section of disclosure). Examples of structured data include SQL (Structured Query language), SQL Databases, Spreadsheets, OLTP Systems, Online forms, Sensors (GPS or RFID tags), Network and Web server logs, and Medical devices. Structured data accounts for only about 20% of data, but its high degree of organization and performance makes it a foundation of Big data.

Tails. Stands for The Amnesic Incognito Live System. If you're serious about digital security, this is the operating system endorsed by Edward Snowden. Tails is an amnesic system, which means your computer remembers nothing; it's like a fresh machine every time you boot up. The software is free and open source. While well-regarded, security flaws have been found.

Threat Detection and Response. Software and technology usage to enable security operators to detect, identify, and respond to attacks and neutralize them before they disrupt an organization.

Threat hunting. Threat hunting goal is to monitor everyday activities and traffic across the Network and investigate possible anomalies to find any yet-to-be-discovered malicious activities that could lead to a full-blown breach. Often performed by a Managed Security Professional.

Threat Intelligence/Cyber Threat Intelligence (CTI). Information gathered from a range of sources about current or potential attacks against an organization. Information is analyzed, refined, and organized and then used to minimize and mitigate Cybersecurity risks.

Threat Model. A description of the capabilities of the enemy (threat) you want to guard against, and your own vulnerabilities. Are you an activist attempting to guard against a state-sponsored hacking team? Your threat model needs to be robust. Just shoring up your home network, you can be less robust.

Token. A small physical device that allows its owner to log in or authenticate into a service. Tokens can serve as an extra layer of security on top of a password. The idea is that even if the password or key gets stolen, the hacker would need the actual physical token to abuse it.

Two-Factor Authentication. An extra step added to the login process. Typically, it takes the form of a code sent to a device or a face or fingerprint scan to help verify your identity. It ultimately requires the user to prove their identity before accessing information.

Unstructured Data. Information that is not arranged by a preset data model or scheme, and therefore cannot be stored in a traditional relational database (RDBMS). It can be generated by humans or machines. Examples include emails, media (photos, audio, video), text files, social media/websites, mobile/communication data, satellite images, digital surveillance, and scientific data. Approximately 80% of the world's data is unstructured. New AI and Machine Learning tools are emerging that can search through this vast quantity of data and uncover (and protect) beneficial and actionable business intelligence.

Verification (dump). The process by which reporters and security researchers go through hacked data and make sure it's legitimate. This process is important to make sure data is authentic and the claims of anonymous hackers are true, and not just an attempt to gain notoriety or make money scamming people on the dark web.

Virtual Private Network (VPN). A secure channel for connecting a series of systems and devices in a private secure encrypted network. VPNs allow users to maintain anonymity when using the network (making it difficult for hackers to attack), employees to connect to their employer's network remotely, and others to protect their connection. They also allow users to bounce off servers in other parts of the world, making them look like they're connecting from that distant location. There are endless VPNs, making it almost impossible to decide which one's the best.

Vuln. Abbreviation for "vulnerability." Another way to refer to bugs or software flaws that can be exploited by hackers.

Vulnerability Management. Continuous, proactive, and often automated process that keeps computer systems, networks, and enterprise applications safe from cyberattacks and data breaches. As such, it is an important part of an overall security program.

Web Application Firewall (WAF). Protects web applications from a variety of application layer attacks such as cross-site scripting (XSS), SQL injection, and cookie poisoning, among others. Attacks on apps are the leading cause of breaches and a gateway to valuable data.

Zero Trust. A strategy to realign security practices and tooling into a modern security architecture that ensures least-privileged access to data and resources. Access decisions are based on strong identity validation, context-aware policies (e.g., location, time, device type/status, user behavior), and authorization that is as granular as possible. A guiding principle of Zero Trust is to assume that the network has already been compromised, thus reinforcing the need to move away from implicit trust based on user location and an overreliance on perimeter-based protections.

OTHER GENERAL TERMINOLOGY YOU NEED TO KNOW

Domain. The networking of devices, such as routers, switches, printers, scanners, and computers that are interconnected and supervised as a whole.

Guessing Entropy. A measure of difficulty a hacker or an attacker has to guess the average password used in a computer system. Guessing Entropy is usually measured in bits.