Security+ Puzzles

CompTIA Exam SY0-601

This is a temporary cover which will be replaced as soon as the cover art is ready! Please feel free to use this in the meanwhile.

Security+ Puzzles

CompTIA® Exam SY0-601

Acknowledgements

Donna Schwartz, Author
Kimberly Ovejero, Cover Art

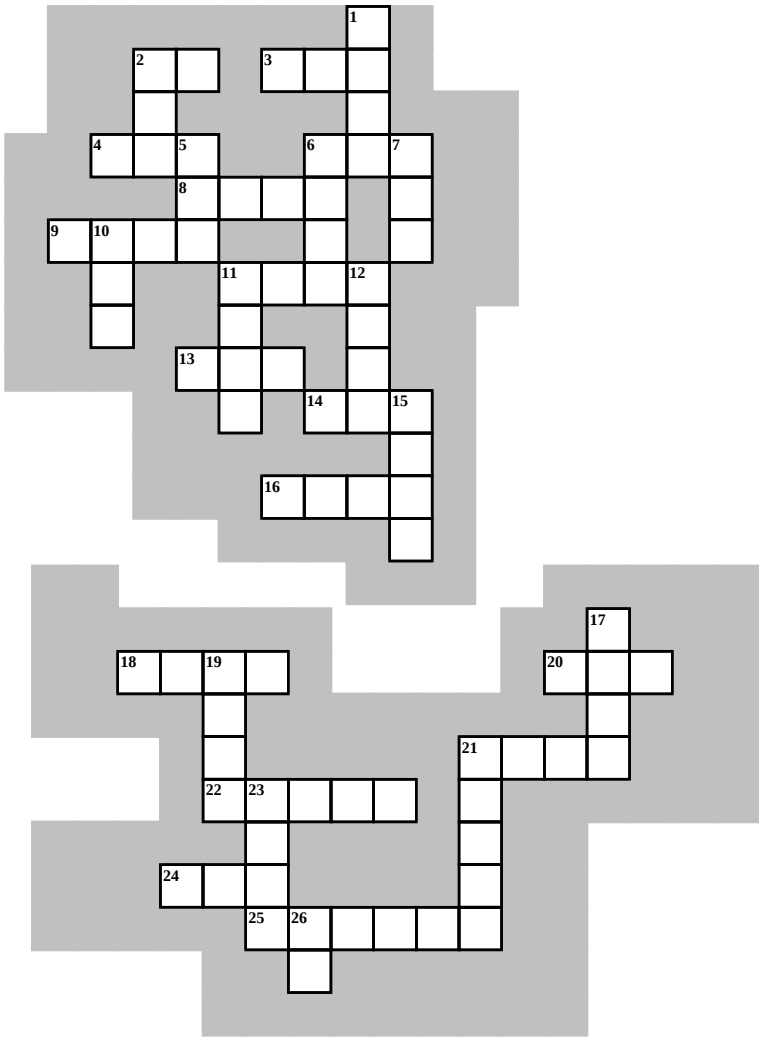
Disclaimer

The author has taken care to ensure the accuracy and quality of the information used to create these puzzles, however, this material is being provided without any warranty whatsoever. Please contact the author at donna.schwartz.1@us.af.mil if you have any comments or concerns regarding the content. Constructive feedback is ALWAYS appreciated!

The author would like to convey special thanks to Mrs. Jennifer M. Bishop for allowing her Security+ class to be used as beta testers for these puzzles.

Table of Contents

ACRONYMS 1



Across

2 In IPSec, this protects integrity, but it does not provide privacy because only the header is secured.

3 If it has the word "Smart" in front of its name, it is part of this. It comprises small devices, such as wearable technologies, that can use an IP address and connect to internet.

4 Permanent and Disolvable, for example.

6 This algorithm is used to create a hash a hash, which is then encrypted using a private key.

8 Identifies a specific 802.11 wireless network. It transmits information about the access point to which the wireless client is connecting.

9 This regulation means that personal data cannot be collected, processed, or retained without the individual's informed consent.

11 A risk management approach to quantifying vulnerability data and then taking into account the degree of risk to different types of systems or information.

13 Passphrase-based mechanism to allow group authentication to a wireless network.

Across

14 Never connect to a public wireless network without one!

16 A measurement of life expectancy.

18 The automatic way of allocating IP addresses. This is a server with a database of IP addresses that can allocate to requesting hosts.

20 This is a binary operand from Boolean algebra. This operand will compare two bits and will produce one bit in return.

21 This tokenized passwprd can be used once, but there is no restriction on time.

22 PFS can be implemented using these algorithms together provide.

24 A removable device that is used to store encryption keys.

25 This standard deals with the handling and storage of data used for card payments. (2 words)

Down

1 A sucure protocol for transfering files using TLS.

2 The framework for identity access security.

5 Base64 ASCII file that a subject sends to a CA to get a certificate.

6 An attack that uses multiple compromised hosts (a botnet) to overwhelm a service with request or response traffic.

7 A representation of the frequency of an event, measured in a standard year.

10 This is a library that contains code and data that can be used by more than one program at the same time.

11 Overall internal responsibility for security might be allocated to a dedicated department, run by this person.

12 A secure version of the standard protocol for a standardized packet format used to carry audio and video traffic over IP networks.

15 This has the ability to carry out deep packet filtering. Also known as layer 7 firewall.

17 This terminology is used for government facilities, but is functionally similar to business continuity planning.

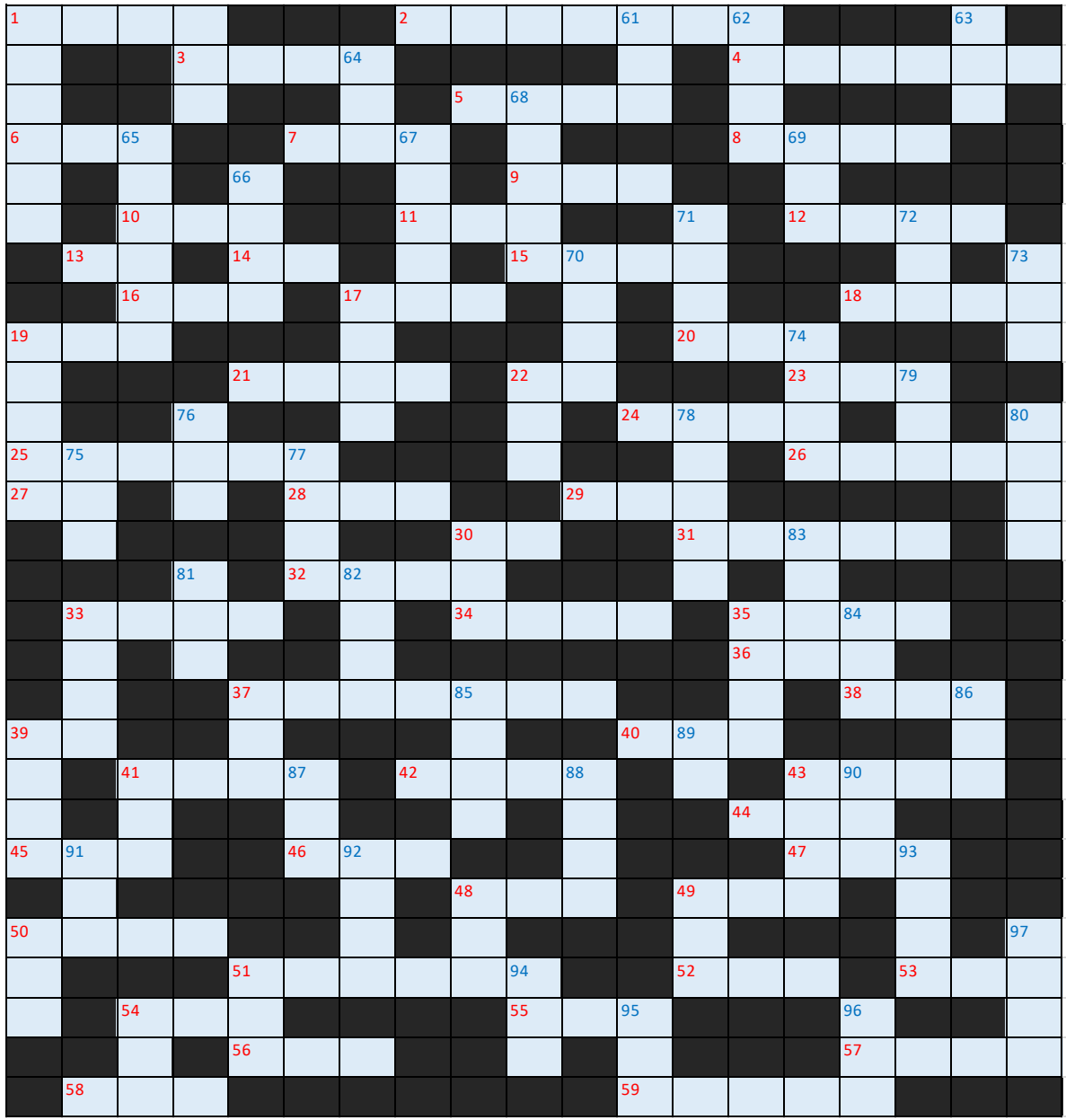
19 Enterprise mobile device provisioning model where the device remains the property of the organization, but certain personal use, such as private email, social networking, and web browsing, is permitt

21 This can be used to secure a web page but is more commonly used when making a purchase on a website, where you will be diverted to a secure server that uses this so that your session is secure.

23 An enhanced data cryptographic encapsulation mechanism based on the Counter Mode with CBC-MAC from AES, designed for use over wireless LANs.

26 When certificates were first introduced, this attribute was used to identify the FQDN by which the server is accessed, such as www.comptia.org.

Acronyms 2



Across	Clue
1	Microsoft Azure, for example.
2	Use of this protocol requires certificates on both the client and the server.
3	A protocol used to request the revocation status of a digital certificate. This is an alternative to certificate revocation lists.
4	framework is a comprehensive matrix of attack elements, including the tactics and techniques used by attackers on a system.
5	A system that automatically responds to computer intrusions by monitoring activity on one or more individual PCs or servers and responding based on a rule set.
6	This type of encoding is used for binary certificates
7	A group of policy settings that defines what a system will look like and how it will behave for a defined group of users. It is primarily a security tool.
8	A vendor neutral, open, industry standard application protocol for accessing and maintaining distributed directory information services over TCP/UDP networks. The protocol provides an interface with directories that follow the X.500 model.
9	This is used with WPA3-Personal and replaces the WPA2-PSK. It uses a very secure Diffie Hellman handshake, called dragonfly, and protects against brute-force attacks. It uses Perfect Forward Secrecy (PFS), which ensures that your session keys cannot be compromised and is immune to offline attacks.
10	A cryptographic method of establishing a shared key over an insecure medium in a secure fashion using a temporary key to enable perfect forward secrecy.
11	The first stage of an IPSec session iused to create a secure tunnel. Uses UDP port 500.
12	The use of generic routing encapsulation over PPP to create a methodology used for virtual private networking.
13	The use of complex models to simulate functions of the brain
14	A network access device that facilitates the connection of devices to a network.
15	A security policy enforcement mechanism between cloud users and providers.
16	A protocol in the TCP/IP protocol suite for the transport layer that does not sequence packets—it is “fire and forget” in nature.

17	An encryption mode of operation where a numerical counter value is used to create a constantly changing IV. Each block I combined with a nonce and is processed individually. This is used to create a stream from a block cipher.
18	The use of a cryptographic hash function and a message authentication code to ensure the integrity and authenticity of a message.
19	The service that translates an Internet domain name
20	A method of adding randomization to blocks, where each block of plaintext is XORed with the previous ciphertext block before being encrypted.
21	The big disadvantage of this mobile device deployment model is that employees will not be eager to limit their use of their personal device based on corporate policies, so corporate control will be limited.
22	This process is the set of actions security personnel perform in response to a wide range of triggering events. These actions are broad and varied, as they have to deal with numerous causes and consequences.
23	The part of IPSec that uses symmetric encryption.
24	This would be used by a small company that does not have security staff and wants to improve its security posture.
25	A European standard for hashing
26	The part of the OASIS CTI framework that provides the MEANS for transmitting CTI data between servers and clients (i.e., the protocol).
27	A trusted organization that validates and issues digital certificates.
28	A component of the Kerberos system for authentication that manages the secure distribution of keys.
29	This can be executed between any two parties where one party wishes that the material being shared is not further shared, enforcing confidentiality via contract.
30	LDAP in a Windows environment
31	All Industrial Control systems should be controlled by this. Always air gapped.
32	A means of fully outsourcing responsibility for information assurance to a third party in the cloud, and only in the cloud.
33	This brings back the replies when you use command-line commands like ping.

34	This works by using a shared secret combined with the card's MAC address to generate a new key, which is mixed with the initialization vector (IV) to make per-packet keys that encrypt a single packet using the same RC4 cipher. Used only for backwards compatability.
35	A broadcast domain inside a switched system; it is created by using the software on the switch where you can bond a number of ports to work together as a separate logical network.
36	Operational Support and Readiness
37	This is the CISCO AAA server that uses TCP for authentication. It CAN authenticate people, but it is used primarily to authenticate services and devices.
38	This type of certificate coding uses ASCII Base64 and is the most commonly used type of certificate encoding.
39	This function is delegated by the CA. These entities complete identity checking and submit CSRs on behalf of end users, but they do not actually sign or issue certificates.
40	This protocol deletes the copy of a message from the server once email is downloaded.
41	An xml-based password that is used once and is only valid during a specific time period.
42	The implementation of access controls as part of a file system. Denoted as a plus sign in Linux DAC.
43	An XML-based API for exchanging information associated with web services.
44	This enables companies to open up their applications' data and functionality to external third-party developers, business partners, and internal departments . Itlists operations that developers can use, along with a description of what they do.
45	A technology employed to detect and prevent transfers of data across an enterprise. Employed at key locations; this technology can scan packets for specific data patterns.
46	Although not dangerous, this should be removed from a computer just like malware.
47	Its primary responsbility is to detect new hosts on a network
48	This protocol, used to send files between systems, will use random ports if the primary ports are blocked by the firewall.
49	An application designed to bring enterprise-level functionality onto a mobile device, including security functionality and data segregation.
50	This protocol gathers metrics and manages network devices.

51	The extension of DNS using cryptographically signed requests and answers.
52	Used in quantitative risk assessments; represents the total amount of money an organization expects to lose for a particular asset in one year.
53	An attack that, always using javascript, adds malicious code to a site's script and runs whenever users visit the site. It can be appended to a URL or injected via public input (e.g., users reviews, message boards).
54	One purpose of this document is to outline how the loss of any of your critical functions will impact the organization.
55	The workspace presented when accessing an instance in a virtual desktop infrastructure solution (VDI).
56	A digitally signed object that lists all of the current but revoked certificates issued by a given certification authority.
57	A measure of reliability
58	This operates at the application layer and is specifically designed to protect web applications by examining requests at the application stack level.
59	The secure version of the standard Internet protocol used to transfer e-mail between hosts.

Down	
1	This stores passwords with a random salt and with the password hash using HMAC. It then iterates, which forces the regeneration of every password and prevents any rainbow table attack.
17	This avoids problems of ownership because the company has a variety of tablets, phones, and laptops. When employees leave the company and offboard, the devices are taken from them as they belong to the company.
19	An e-mail authentication, policy, and reporting protocol. prevents spammers and attackers from spoofing your email domain in sending spam and phishing to others
22	This might stipulate what forms of encryption to companies will use to communicate, for example.
30	Refers to the ongoing ability of an adversary to compromise network security- to obtain and maintain access- using a variety of tools and techniques.

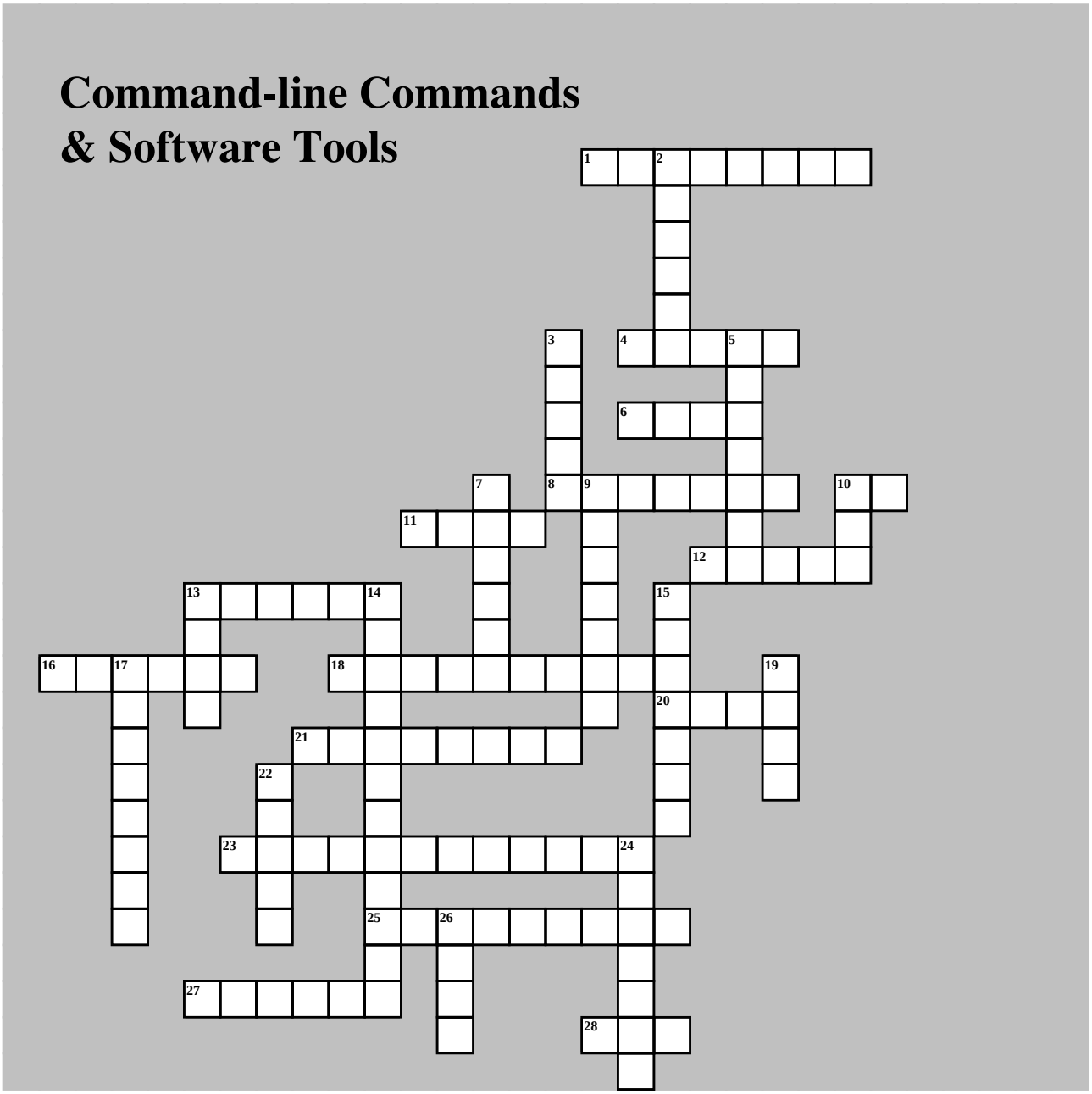
33	A symmetric encryption algorithm used in a variety of systems for bulk encryption services. It takes 64 bit as an input, 28-bit key and performs 8 identical rounds for encryption in which 6 different subkeys are used, and four keys are used for output transformation.
35	A method and group of technologies for the delivery of voice communications and multimedia sessions over Internet Protocol networks, such as the Internet.
37	When a user logs in to an Active Directory domain using Kerberos authentication they receives this to get service.
39	A method of ensuring fault tolerance. Uses techniques such as striping, mirroring, and parity.
41	This is information on adversaries and the attack methods, tools, and techniques that they use. A good source of information for this is the MITRE ATT&CK framework, where you have a spreadsheet of adversaries and can drill down into relevant details.
43	This is sending spam messages via instant messaging or SMS.
48	The application of encryption to an entire disk, protecting all of the contents in one container.
49	Something you have, something you know, and something you do, for example.
50	A language used in relational database queries.
51	An access control mechanism in which the owner of an object (such as a file) can decide which other subjects (such as other users) may have access to the object as well as what access (read, write, execute) these subjects can have.
54	This is used between two companies who want to participate in a business venture to make a profit. It sets out how much each person should contribute, their rights and responsibilities, the rules for the day-to-day running of the business, who makes the decisions, and how the profits are shared.
60	A low-power integrated chip that integrates all of the components of a computer or electronic system. An example would be the controller for a defibrillator.
61	Used to protect data in transit and is an upgraded version of SSL that is used to encrypt communications on the internet, such as email or internet faxing, and transfer data securely. It can be used in a web browser.
62	Based on XML, this allows services to be separated from identity providers and not have to authenticate directly. The service provider receives an authentication attestation from the identity provider.

63	The big benefit of this cryptographic system is that it requires less computing power for a given bit strength. This makes it ideal for use in low-power mobile devices.
64	A popular encryption program that has the ability to encrypt and digitally sign e-mail and files.
65	AAA server for authentication. Each device has an X509 certificate for identification.
66	A wireless authentication protocol used in large networks.
67	A coomon reconaissance technique where the attacker harvests domains, IP address ranges, employees, and other data that will assist in identifying attack vectors. This intelligence is derived from publically available information.
68	A protocol used to secure IP packets during transmission across a network. offers authentication, integrity, and confidentiality services and uses Authentication Headers (AH) and Encapsulating Security Payload (ESP) to accomplish this functionality.
69	A security feature of an OS that can be driven by software, hardware, or both, designed to prevent the execution of code from blocks of data in memory. Helps prevent buffer overflows.
70	A memory-protection process employed by operating systems where the memory space is block randomized to guard against targeted injections from buffer-overflow attacks.
71	Access is granted based on four elements: who is requesting access, what they are requesting access to, what they want to do with the asset, and the environment (context of the session).
72	A chip stored on the motherboard used to store the encryption keys so that when the system boots up, it can compare the keys and ensure that the system has not been tampered with.
73	This represents the planning and advanced policy decisions to ensure the business continuity objectives are achieved during a time of obvious turmoil.
74	The group responsible for investigating and responding to security breaches, viruses, and other potentially catastrophic incidents.
75	The policies and procedures used to manage access control.
76	A fast, secure symmetric algorithm with key lengths of -128, -192, and -256 bits.
77	An email authentication technique that allows the receiver to check that an email was indeed sent and authorized by the owner of that domain. This is done by giving the email a digital signature. This signature is a header that is added to the message and is secured with encryption.

78	A not-for-profit, online community that publishes several secure application development resources, such as the Top 10 list of the most critical application security risks.
79	A telephone exchange that serves a specific business or entity.
80	Provides a cybersecurity framework consisting of five functions: identify, protect, detect, respond, and recover.
81	A text-based, human-readable data markup language. Based on HTML.
82	There are two main models: Waterfall and Agile.
83	Different devices and appliances use these. They are also used in DAC. They consist of rules to determine actions. An example would be Implicit Deny.
84	A computer might not respond to a ping, but it will ALWAYS respond to this, which resolves IP addresses to MAC addresses.
85	Used to provide authentication across a point-to-point link using PPP. In this protocol, authentication after the link has been established is not mandatory. It is designed to provide authentication periodically through the use of a challenge/response system sometimes described as a three-way handshake,
86	A third party that manages aspects of a system under some form of service agreement.
87	A two-way handshake which does not provide any protection against playback and line sniffing.
88	Replaced by EAP-FAST because it was unsecure (it used WEP).
89	This acts as an interface between the software and different parts of the computer or the computer hardware. It is designed in such a way that it can manage the overall resources and operations of the computer.
90	Each certificate can be identified by this, which is similar to a serial number.
91	A collection of devices connected together in one physical location, such as a building, office, or home.
92	The aggregation of multiple network security products into a single appliance for efficiency purposes. (plural)
93	The part of the OASIS CTI framework that describes standard terminology for IoCs and ways of indicating relationships between them (i.e, syntax)

94	A list of known vulnerabilities in software systems. Each vulnerability in the list has an identification number, description, and reference. This list is the basis for most vulnerability scanner systems, as the scanners determine the software version and look up known or reported vulnerabilities.
95	Users can still use the product but there will be no more security updates or technical support available from the vendor.
96	When an attacker escapes from one, they will be able to attack other guest OSs or the hypervisor from within a nother one of these (plural)
97	exploits the trust a site has in the user's browser.

Command-line Commands & Software Tools



Across

1 If you are having network connection issues, this is one of the firsr Linux tools you should use, to verify the network setup of the operating system and its interfaces.

4 This works in Linux and Windows systems to provide information on current routing parameters and to manipulate these parameters.

6 This Linux command-line tool used to search for a string of characters in a specified file.

8 The main purpose of this tool is to gather as much information as possible aout a domain.

10 This is a Linux command-line utility used to convert and copy files.

11 This tool is used for recovering web session information and exploiting client-side scripting.

12 This is a TCP/IP packet creation tool that allows a user to craft raw TCP, IP, UDP, and ICMP packets from scratch. This tool provides a means of performing a wide range of network operations.

13 The primary purpose of this command is to establish sockets/connections. It has other uses as well.

16 This is the GUI version of nmap.

Across

18 The best-known exploit framework.

20 You will need to run this Linux command to run as the root user.

21 This is a command-line utility to interface with websites that can perform port scans as part of a penetration test. When you use this tool, the source IP address for the scan is the website, not your testing machine.

23 This tool is used for vulnerability scanning and exploit modules targeting embedded systems.

25 This tool specifically replays a PCAP file on a network.

27 This is an automated scanner designed to collect a large amount of information while scanning for vulnerabilities. It runs a series of automated scripts to enumerate servers, open ports, and vulnerabilities.

28 This command allows a system administrator the ability to see and manipulate the ARP cache on a system. This way they can see if entries have been spoofed or if other problems, such as errors, occur.

Down

2 This is a sandbox used for malware analysis.

3 This Linux command is used to change DAC file permissions.

5 This tool allows you to use the command line to capture You can save these packets, which you can load up in a protocol analyzer.

7 This is one of the leading vulnerability scanners in the marketplace.

9 This tool was designed by Cisco to capture information about packet flows (that is, a sequence of related packets) as they traverse a network.

10 This command is used for zone transfers in Linux.

13 This is used to discover what systems are on a network and the open ports and services on those systems. This tool has many other additional functions, such as OS fingerprinting.

14 This is a reconnaissance tool which is useful for exploring public sources. It can provide information on employees, e-mails, and subdomains using different public sources such as search engines and PGP key servers, and Shodan databases.

15 This command is used to monitor network connections to and from a system.

17 Somtimes, this Windows command will return a nonauthoritative answer. This typically means the result is from a cache as opposed to a server that has an authoritative (known to be current) answer.

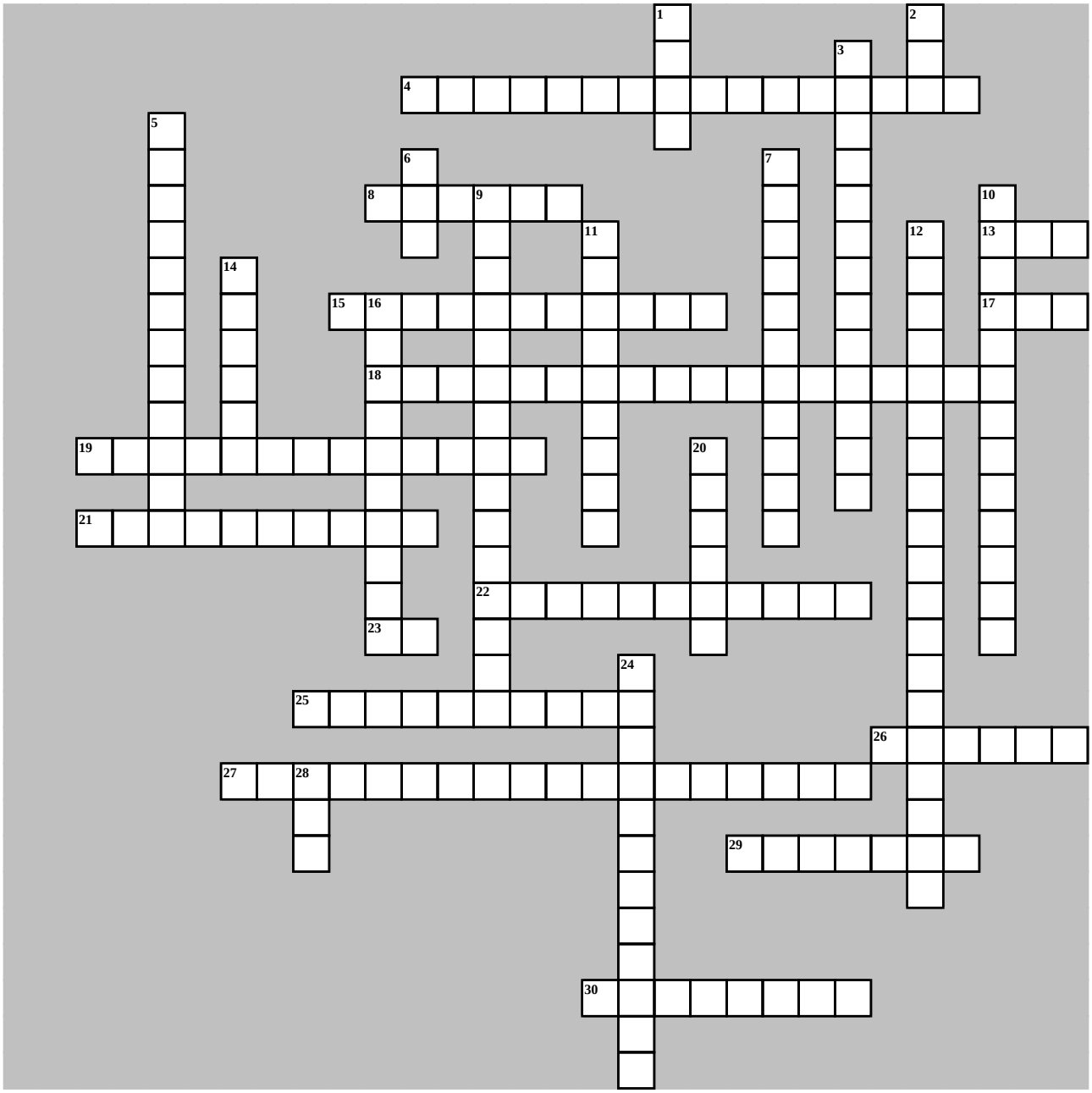
19 This is a tool designed to transfer data to or from a server, without user interaction. It support a long list of protocols and acts like a Swiss army knife for interacting with a server.

22 This Linux command is used to change the ownership of a file.

24 This Windows command provides a list of the hosts, switches, and routers in the order in which a packet passes through them.

26 This command sends echo requests to a designated machine to determine if communication is possible.

CRYPTOGRAPHY AND PKI



Across

4 Provides integrity and non-repudiation. (2 words)

8 This holds the private keys for third parties and stores them in a hardware security module.

13 It takes less processing power, so is commonly used with small, wireless devices.

15 Creates a stream from a block cipher. (2 words)

17 Prone to collisions, this hashing algorithm should not be used without HMAC.

18 This provides a higher level of trust in identifying the entity that is using the certificate. Normally used in the financial arena. (2 words)

19 An X.509 certificate that that proves the ownership of a domain name. (2 words)

21 This type of certificate is only valid in-house, not on a web server. (2 words)

22 This type of certificate is used to digitally sign software to guarantee its authenticity. (2 words)

23 A key agreement algorithm using "clocl arithmetic." It creates the keys used in IKE.

25 Exists to protect symmetric keys.

26 A European hashing algorithm

Across

27 A technique used to ensure that when a client inspects a certificate presented by a server or a code-signed application, it is inspecting the proper certificate. (2 words)

29 Helps prevent brute force and rainbow table attacks.

30 A certificate that is used for multiple servers (sub-domains) within the same main domain.

Down

1 Used when the CRL is going slow. It is much faster than the CRL and can take the load from a CRL in a very busy environment.

2 When a subject wants to obtain a certificate, it must complete this and send it to the CA with the public key.

3 Hides data within data.

5 This trust model starts with the root CA and goes through intermediary CAs. This is the normal PKI model.

6 This can be a piece of hardware attached to the server or a portable device that is attached to store the keys.

7 A binary operand from Boolean Algebra that compares two bits and produces one bit in return. (2 words)

9 This identifies the certificate authority itself. (2 words)

10 refers to operational considerations for the various stages in a key's life cycle. (2 words)

11 Also known as "private key encryption."

12 The chain of trust used to verify the validity of a certificate as it includes details of the CRL. It normally has three layers: the certificate vendor, the vendor's CA, and the computer where the certificate is installed. (2 words)

14 This must be kept secret and may NOT be stored with the hash.

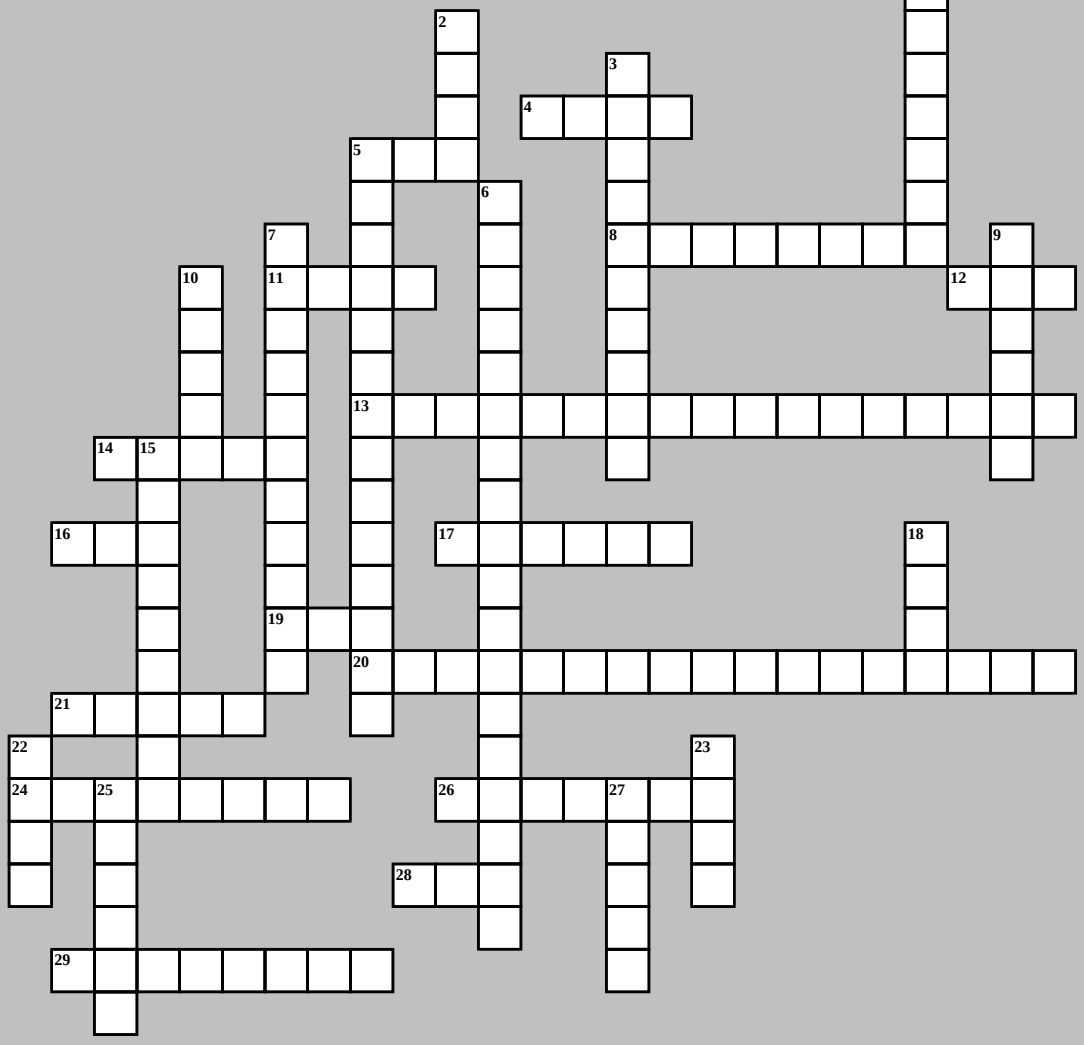
16 The only truly unbreakable code. (3 words)

20 This trust model is peer-to-peer, where two separate PKI environments trust each other.

24 Te web server periodically reaches out to the CA and gets a digitally signed date-time stamp to show certificate validity. (2 words)

28 A symmetric stream cypher used for backwards compatability with TKIP.

IT GOVERNANCE: STANDARDS, FRAMEWORKS, AND LAWS



Across

4 Audit specifications developed by the American Institute of Certified Public Accountants. These audits are designed to assure consumers that service providers meet professional standards.

5 This organization produces benchmarks for compliance with IT frameworks and compliance programs.

8 Security techniques for information security management systems. (2 words)

11 This professional association of engineers and scientists of many disciplines has the mission to adance technological innovations of all sorts.

12 This agency is responsible for information gathering , codebreaking, and codemaking. This agency develops cryptographic standards and secures government information against attack.

13 Concerns information security risk management (2 words)

14 This is an international professional association focused on IT governance.

16 This standards organization develops and maintains standards for the World Wide Web.

Across

17 This act requires publically traded companies to adhere to very stringent reporting requirements and implement strong controls on elecronic financial reporting systems.

19 Produces various resources to to assist cloud service providers in setting up and delivering secure cloud platforms.

20 Code of practice for information security controls based on ISO/IEC 27002 for cloud services. (2 words)

21 Specofoes that all organizations having anything to do with healthcare must protect the health information that they maintain.

24 Code of practice for information security controls. (2 words)

26 This model of intrusion analysis suggests a framework to analyze an intrusion event by exploring the relationship between four core features: adversary, capability, infrastructure, and victim.

28 A list of publicly disclosed computer security flaws.

29 This is about managing risk for company organizations and management in general. (2 words)

Down

1 This report assesses system design. (3 words)

2 A scoring system to show the level of severity of vulnerabilities.

3 This act enables law enforcement agencies to detect and suppress terrorism by giving law enforcement the authority to request information from organizations. (2 words)

5 The series of stages in a cyberattack. By understanding this model, organizations can better identify, prevent, and mitigate ransomware, security breaches, and APTs. (3 words)

6 This requirea that all banks and any other financial institutions to alert their customers as to that organization's privacy policies.

7 a database of threat actors, their techniques, and the vulnerabilities that they exploit. This helps security teams protect themselves against such attacks. (2 words)

9 An audit standard to enhance the quality and usefullness of Service Organizational Control reports.

10 This requires that organizations that provide online services designed for children below the age of 13, to obtain parental consent prior to collecting a child's information.

15 This report assesses the ongoing effectiveness of a security architecture over a 6-12-month period. (4 words)

18 This report evaluates the internal controls implemented by a service provider to ensure compliance with Trust Serices Criteria when storing and processing customer data.

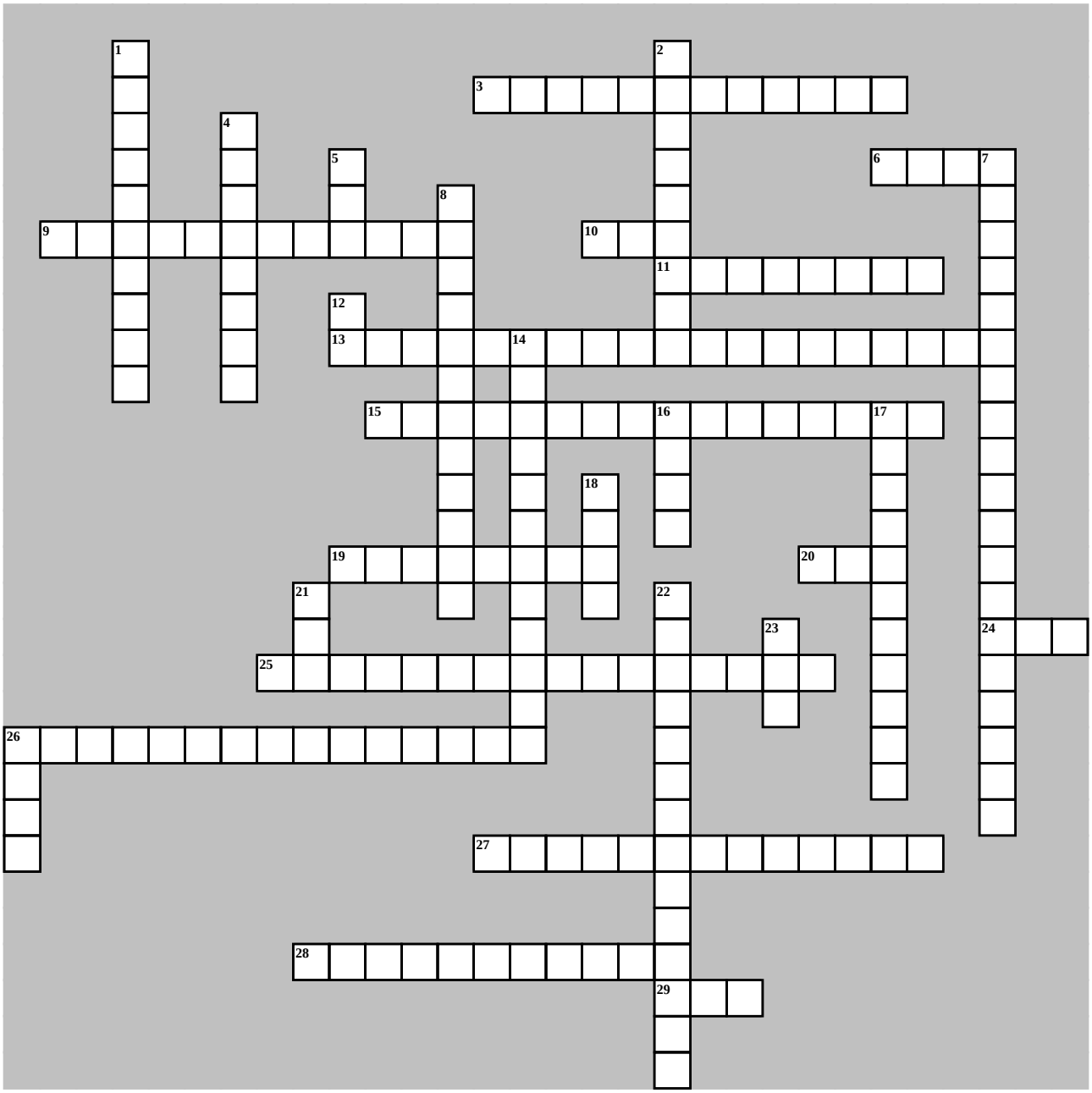
22 A framework which provides guidance to better manage and reduce cybersecurity risk.

23 A European Union regulation that deals with the handling of data while maintaining the privacy and rights of the individual.

25 This deals with the handling and storage of data used for card payments.

27 A non-profit foundation that works to improve the security of software. This organization provides a list of the top ten web application securty risks.

Risk Management Terms & Acronyms



Across

3 A repository of information on risks. (2 words)

6 Used for non-repairable assets, this is a measure of life expectancy.

9 A type of risk assessment based on financial loss.

10 Used to determine the reliability of each asset, such as servers, disk arrays, switches, routers, etc.

11 The cheapest backup site to maintain but the slowest to get up and running. (2 words)

13 These are scanrio-based activities that take place in a simulated environment. (2 words)

15 Also known as "sharing risk." (2 words)

19 Raw risk, prior to any risk mitigation strategies being implemented.

20 The longest period of time that a business function outage may occur for without causing irrevocable business failure. Each business process can have its own MTD.

Across

24 The period following a disaster that an individual IT system may remain offline. This represents the amount of time it takes to identify that there is a problem and then perform recovery,

25 Someone who has been overlooked for promotion or unhappy with their current salary, for example. (2 words)

26 Systems necessary to perform essential functions and activities. (2 words)

27 A weakness or flaw that helps a threat exploit a system or work flow.

28 A type of risk assessment based on probability and impact.

29 The amount of data loss that a system can sustain, measured in time.

Down

1 This is used to get a visual representation of the risks affecting a company (2 words)

2 Risk mitigation is this type of control.

4 Amount of risk remaining after you mitigate the risk.

5 Following systems recovery, there may be additional work to reintegrate different systems, test overall functionality, and brief system users on any changes or different working practices so that the

7 These are action-based practice sessions that reflect real situations. (2 words)

8 The vendor has deemed that the system has reached the end of its life. (2 words)

12 The measurement of the magnitude of the loss. In other words, what percentage of the asset is lost.

14 This type of property might be stolen by a competitor.

16 Reducing dependencies helps to prevent these.

17 This continuiaty of operations site ensures business is always operational with the least amount of man hours needed.

18 A measure of the time taken to correct a fault so that a system is returned to full operation. This metric is important in determining the RTO.

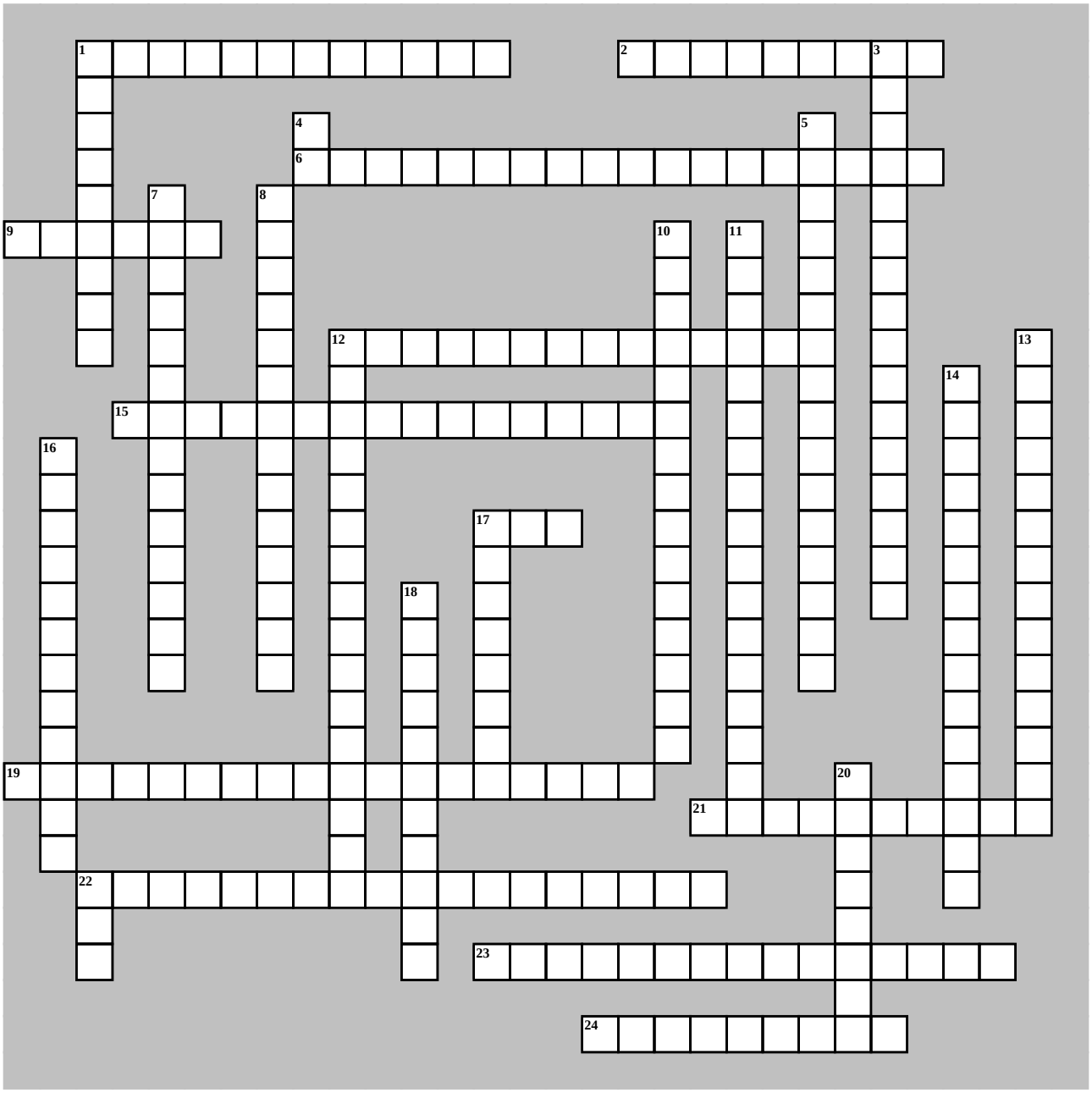
21 This identifies inputs, hardware, staff, outputs, and process flows.

22 The number two priority when evaluating impact. (3 words)

23 One that cannot be deferred; the organization must be able to perform the function as close to continually as possible, and if there is any service disruption, the mission essential functions must be

26 A measure of reliability.

STARTS WITH "D"



Across

1 An attack in which an attacker responds to a client requesting address assignment from a DHCP server. (2 words)

2 A cryptographic attack where the attacker exploits the need for backward compatibility to force a computer system to abandon the use of encrypted messages in favor of plaintext messages.

6 Institutional data governance role with responsibility for compliant collection and processing of personal and sensitive data. (3 words)

9 A security protocol that uses digital signatures to provide authentication of DNS data and upholds DNS data integrity.

12 Spoofing frames to disconnect a wireless station to try to obtain authentication data to crack.

15 In data protection, methods and technologies that remove identifying information from data before it is distributed.

17 A documented and resourced plan showing actions and responsibilities to be used in response to critical incidents.

Across

19 An application attack that allows access to commands, files, and directories that may or may not be connected to the web document root directory. (2 words)

21 The process of rendering a storage drive inoperable and its data unrecoverable by eliminating the drive's magnetic charge.

22 A backup type in which all selected files that have changed since the last full backup are backed up. (2 words)

23 In data protection, the principle that countries and states may impose individual requirements on data collected or stored within their jurisdiction. (2 words)

24 A senior (executive) role with ultimate responsibility for maintaining the confidentiality, integrity, and availability of an information asset. (2 words)

Down

1 Cybersecurity resilience strategy that increases attack costs by provisioning multiple types of controls, technologies, vendors, and crypto implementations.

3 A network service that stores identity information about all the objects in a particular network, including users, groups, servers, client computers, and printers. (2 words)

4 Linux command that makes a bit-by-bit copy of an input file, typically used for disk imaging.

5 A type of password attack that compares encrypted passwords against a predetermined list of possible password values. (2 words)

7 A security strategy that positions the layers of network security as network traffic roadblocks; each layer is intended to slow an attack's progress, rather than eliminating it outright. (3 words)

8 The social engineering technique of discovering things about an organization (or person) based on what it throws away. (2 words)

10 A type of attack where the attacker steals a domain name by altering its registration information and then transferring the domain name to another entity. (2 words)

11 A segment isolated from the rest of a private network by one or more firewalls that accepts connections from the Internet over designated ports. (2 words)

12 In data protection, the principle that only necessary and sufficient personal information can be collected and processed for the stated purpose. (2 words)

13 The process of removing an application from packages or instances.

14 Any type of physical, application, or network attack that affects the availability of a managed resource. (3 words)

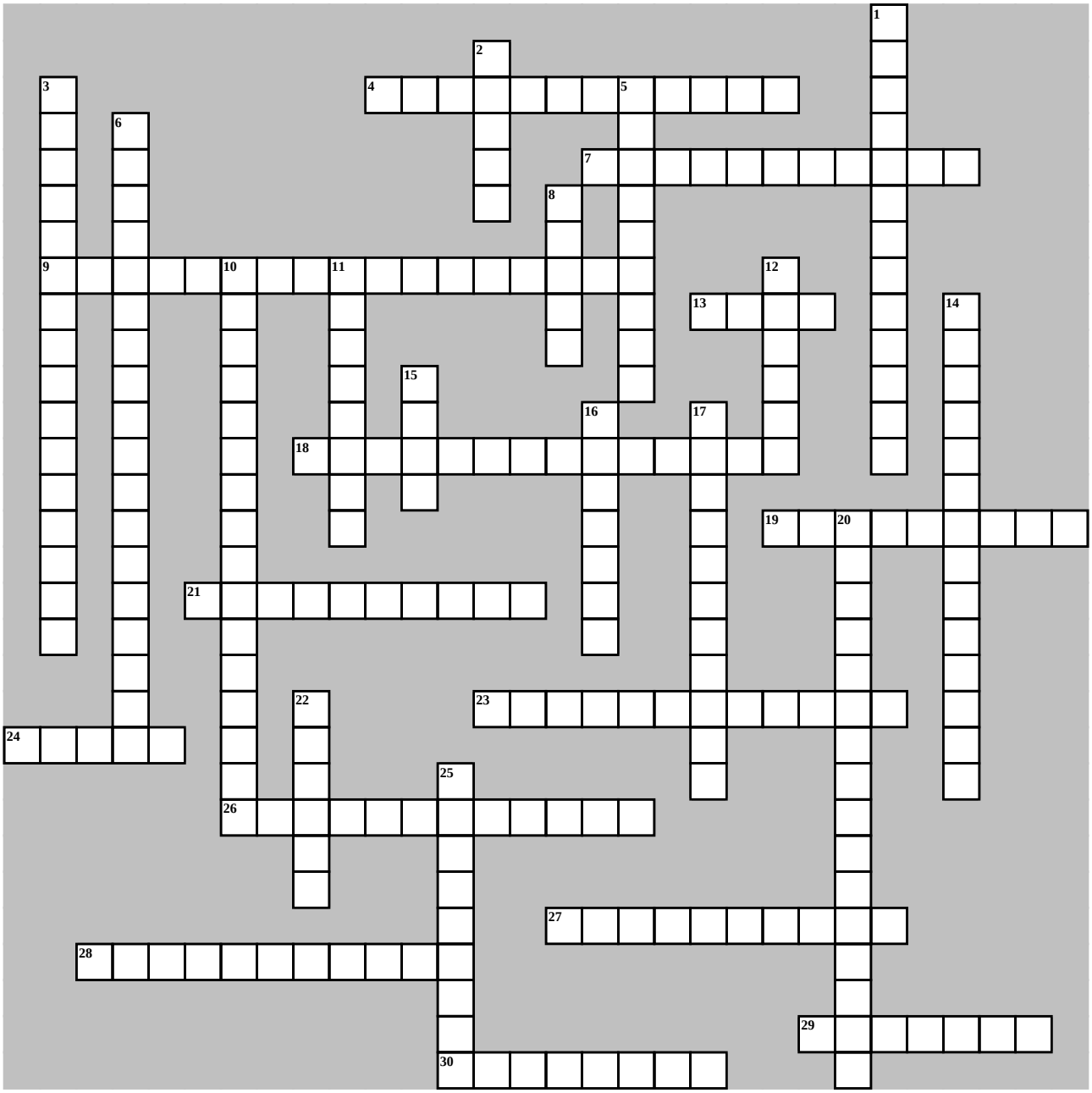
16 A network-based attack where an attacker exploits the traditionally open nature of the DNS system to redirect a domain name to an IP address of the attacker's choosing. (2 words)

17 Code in an application that is redundant because it will never be called within the logic of the program flow. (2 words)

18 A deidentification method where generic or placeholder labels are substituted for real data while preserving the structure or format of the original data. (2 words)

20 File containing data captured from system memory. (2 words)

22 The binary format used to structure the information in a digital certificate.



Across

4 Uses code like, <name>John Doe</name>. (2 words)

7 The attacker is able to send unauthorized text messages from the Bluetooth-enabled device.

9 This virus changes its internal code to one of a set number of predefined mutations whenever it is executed. (2 words)

13 This steals cookies, makes purchases, and harvests passwords. The user MUST be logged in to a secure host. because this attack attempts to take advantage of the user's active session.

18 A wireless attack that involves jamming the wireless access point (WAP) forcing the victim to reauthenticate enabling the attacker to sniff and capture credentials that will enable impersonation.

19 Installed by attackers who have compromised a system to ease their subsequent return to the system. Allows attackers to bypass authentication. They are undocumented and usually illegal.

21 A type of Brute Force attack that tries to determine a decryption key or passphrase by trying thousands or millions of likely possibilities.

Across

23 Tricking the user into clicking something that they hadnâ€™t intended. It uses HTML frames to mask what the user is clicking on.

24 The attacker sends ICMP Echo Request packets where the source IP address has been forged to be that of the target of the attack.

26 Database attack that uses code like, “OR,” “1=1,” “SELECT*FROM,”(2 words)

27 Initiates a SYN Flood attacker by spoofing the IP address of the victim. The victim ends up trying to establish a connection with itself resulting in an endless loop that persists until the timeout v (2 words)

28 The attacker is able to completely take over the mobile device.

29 A number of Internet computers that, although their owners are unaware of it, have been set up to forward transmissions (including spam or viruses) to other computers on the Internet

30 UEFI Secure Boot can identify one because it prevents unsigned code from executing.

Down

1 Directory attack that uses code like BIND, SEARCH, MODIFY, CN, DC, OU (AD uses o, c). Mitigation- Input Validation; WAF, stored procedures. Look for a lot of â€œ (2 words)

2 Requires human interaction in order to spread.

3 A type of horizontal brute force online attack where the attacker chooses one or more common passwords (for example, password or 123456) and tries them in conjunction with multiple usernames. (2 words)

5 When a function produces the same hash value for two different plaintexts; This type of attack can be used for the purpose of forging a digital signature.

6 Takes place at the Application Layer of the OSI model. This attack intercepts browsing data using a trojan (malicious add-in).

8 Programs that reproduce, execute independently (without user intervention) and travel across the network connections

10 This virus can actually rewrite its own code and thus appear different every time it is executed by creating a logical equivalent of its code whenever it is run. (2 words)

11 Poisoning the "hosts" file of a computer in order to redirect the client to a fake website.

12 A network software application designed to remain hidden on an installed computer; accesses personal information stored locally on home or business computers then send these data to a remote party via the Internet.

14 In this attack, the threat actor deliberately submits input that is too large to be stored in a variable assigned by the application. (2 words)

15 A port scan that reveals details of the OS and open ports; uses PSH, URG and FIN flags.

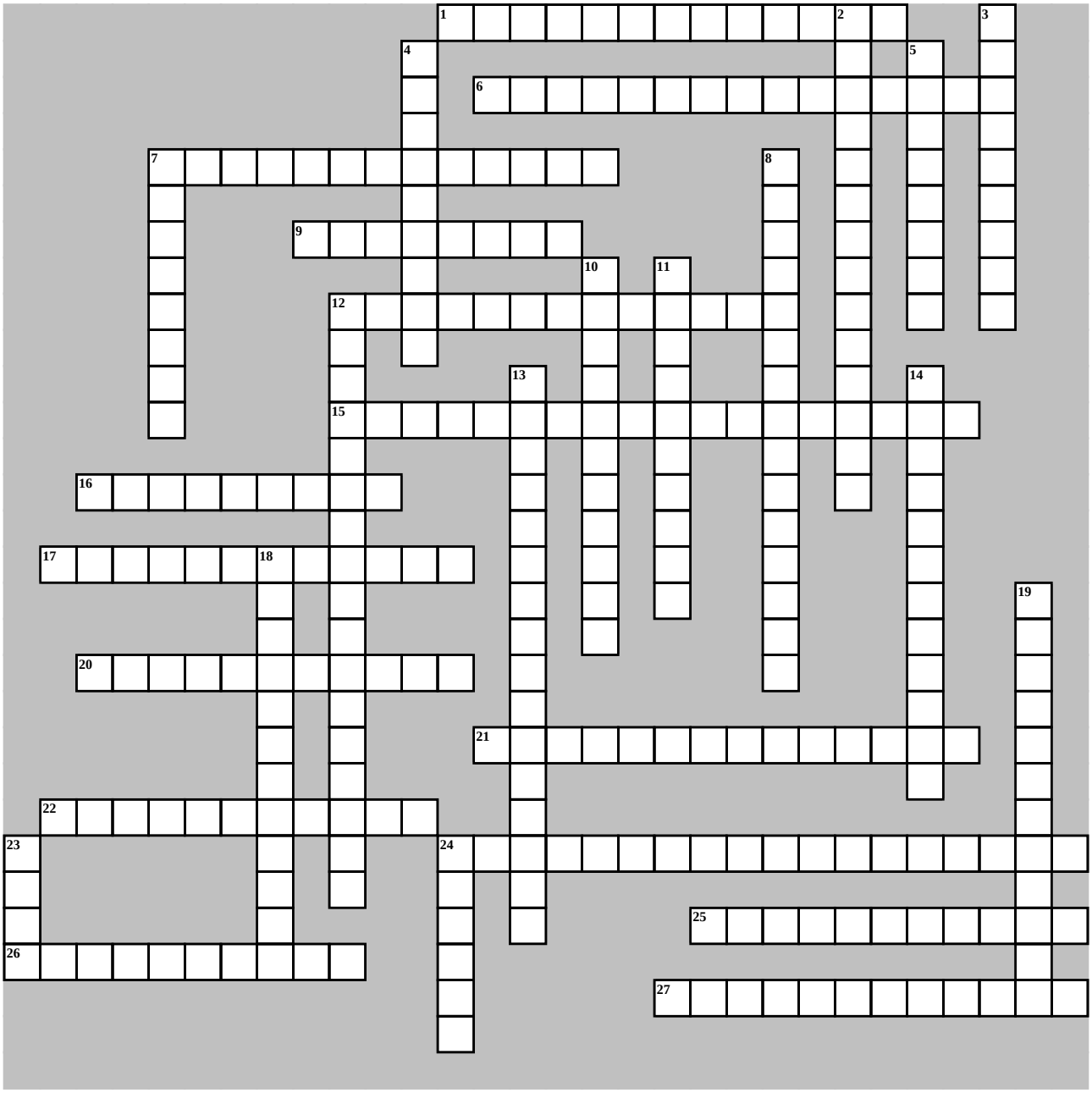
16 A variation of phishing that uses voice communication technology to obtain the information the attacker is seeking.

17 A DoS attack which involves sending a malformed ping to a computer. The attacker breaks down the packets into fragments, which when recombined, are greater than 65,535. (3 words)

20 An attack in which the goal is execution of arbitrary commands on the host operating system via a vulnerable application. (2 words)

22 This attack occurs when occurs when the attacker captures a portion of a communication between two parties and retransmits it at a later time, often with changes.

25 A type of spyware that captures all of a user's keystrokes.



Across

1 A type of ransomware that encrypts any or all files until payment has been made. (2 words)

6 When an attacker changes the domain name registration, typically using social engineering. The site may be held for ransom or used for malicious purposes. (2 words)

7 The threat actor doesn't need to decrypt the hash to obtain a plain text password.

9 A vulnerability that is unknown by the vendor.

12 An error that occurs during the execution of a program. (2 words)

15 This gives cybercriminals complete, unlimited, and remote access to a victimâ€™s computer. Once activated, it can hide within the system for many months and remain undetected. (3 words)

16 When an application receives data from an untrusted source and includes that data within its later HTTP responses in an unsafe way. (2 words)

17 A virus that is difficult to reverse engineer. (2 words)

20 Uses a replay mechanism that targets the 4-way handshake. It is effective regardless of whether the authentication mechanism is personal or enterprise. (2 words)

Across

21 Occurs at the Network layer of the OSI model. It interferes with the public key presented to the client. (4 words)

22 Sending packets to all ports on a switch. Overwhelming the switch causes it to behave like a HUB. (2 words)

24 A software vulnerability that can occur when code attempts to read a memory location specified by a pointer but the memory location is null. (2 words)

25 This type of virus completely changes from its original form whenever it is executed.

26 This occurs when an application fails to properly release memory allocated to it or continuously requests more memory than it needs. (2 words)

27 Unauthorized access to leading to theft of information from a Bluetooth-enabled device.

Down

2 These occur when the outcome from an execution process is directly dependent on the order and timing of other events, and those events fail to execute in the order and timing intended by the develope (2 words)

3 A program, or portion of a program, which lies dormant until a specific piece of program logic is activated (2 words)

4 An attack virus that spreads through air and gets into a device via bluetooth and can then take full control of the device.

5 This attack depends on the higher likelihood of collisions found between random attack attempts and a fixed degree of permutations.

7 is a type of social engineering in which an individual attempts to obtain sensitive information from a user by masquerading as a trusted entity in an e-mail or instant message sent to the user.

8 These viruses infect floppy and hard drives. The virus program will load first, before the operating system. (3 words)

10 Rewriting code to perform the same function in a different way, Used to prevent A-V software from recognizing malware by its signature.

11 This attack is occurring when an attacker submits many passwords or passphrases with the hope of eventually guessing a combination correctly. (2 words)

12 Software testing that looks speciafically for security flaws. It uses a technique called "fuzzing." (2 words)

13 Bypassing a user's or computer's browser privacy settings and then impersonating the user by using their session ID, which is stored in a cookie. (2 words)

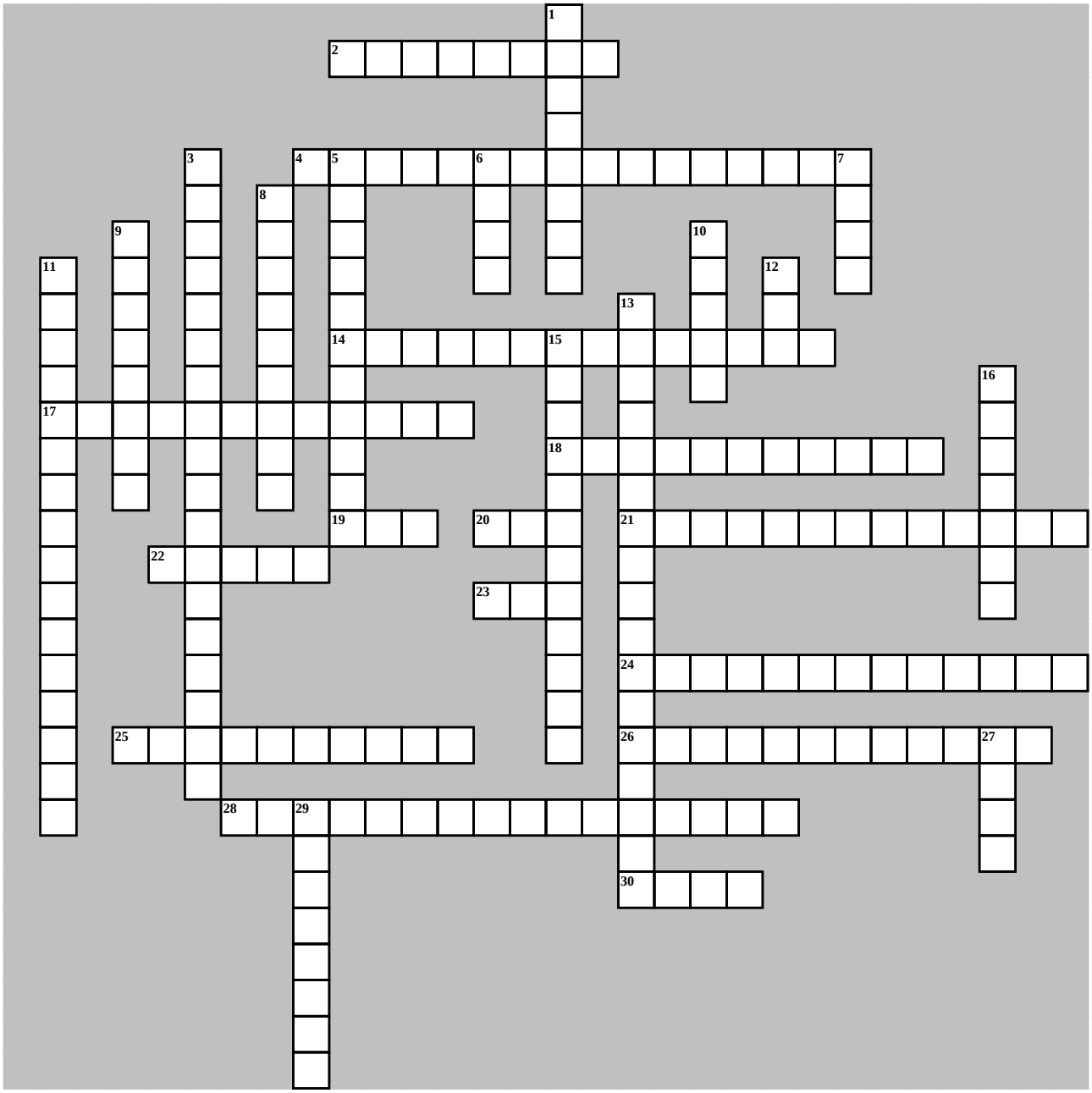
14 An attack that uses a table of plaintext permutations of encrypted passwords specific to a hash algorithm. (2 words)

18 A fault that allows priviledged information (such as a token or password) to be read without being subject to the appropriate access controls. (2 words)

19 A vulnerability in the way the operating system allows one process to attach to another. (2 words)

23 The code library that intercepts and redirects calls to enable legacy mode functionality.

24 A man-in-the-middle attack that takes advantage of Internet and security software clients' fall-back to SSl 3.0. It is a protocol downgrade that allows exploits on an outdated for of encryption.



Across

2 A security exploit for which a vendor patch is not readily available.

4 This technology would be BEST to balance a BYOD culture while also protecting the companyâ€™s data.

14 When collecting evidence, this technique is used to preserve the admissibility of the evidence, (3 words)

17 A RAT that evaded AV detection and was installed on a machine by a user who had local administrator rights. This would BEST prevent this situation from reoccurring.

18 This incident response step involves actions to protect critical systems while maintaining business operations.

19 A data owner should require all personnel to sign one to legally protect intellectual property.

20 A company is adopting a BYOD policy and is looking for a comprehensive solution to protect company information on user devices. This solution would best support this policy.

Across

21 A security analyst is using a recently released security advisory to review historical logs, looking for the specific activity that was outlined in the advisory. The security analyst is ... (2 words)

22 Which disk redundancy solution provides a two-drive failure for better fault tolerance.

23 This document would be used by two organizations that are in early discussions to define the responsibilities of each party, but do not want to establish a contractually binding aggreement.

24 This require guests to sign off on the acceptable use policy before accessing the Internet. (2 words)

25 Tis would would MOST likely support the integrity of a voting machine.

26 Sharing risk, such as by buying insurance.

28 This plan is used in the event of a complete loss of critical systems and data. (2 words)

30 A small company that does not have security staff wants to improve its security posture. This would best assist the company.

Down

1 In this type of exercise, a facilitator presents a scenario with flashcards to replicate what might occur in a dynamic cybersecurity event involving the company.

3 The server can no longer function after suffering a DDoS attack. (2 words)

5 Steganography, for example.

6 This cloud model provides clients with servers, storage, and networks but nothing else.

7 A security administrator suspects there may be unnecessary services running on a server. This tool could be used to confirm his suspicions.

8 An intrusion detection system (IDS) is this type of control.

9 An analyst needs to identify the applications a user was running and the files that were open before the userâ€™s computer was shut off by holding down the power button. The analyst should look here.

10 A cybersecurity analyst needs to implement secure authentication to third-party websites without user's passwords.This would be the BEST way to achieve this objective.

11 This is an attack that uses a limited number of commonly used passwords and applies them to a large number of accounts. (2 words)

12 An organization with a low tolerance for user inconvenience wants to protect laptop hard drives against loss or data theft. This would be the most acceptable solution.

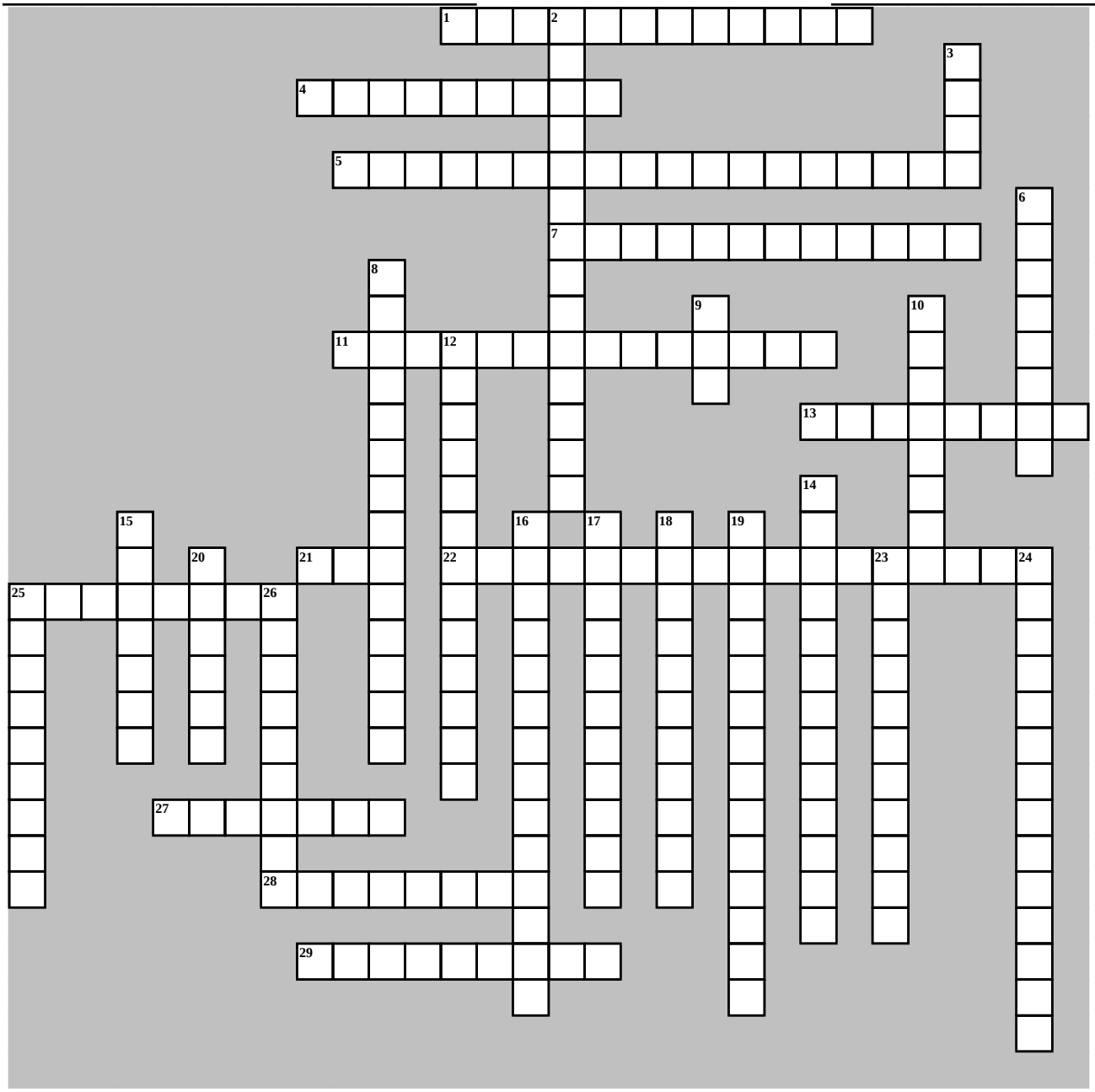
13 A company is implementing MFA for all applications that store sensitive data. The IT manager wants MFA to be non-disruptive and user friendly. What technology should be used to implement MFA? (2 words)

15 This distributes data among nodes, making it more difficult to manipulate data while also minimizing downtime. (2 words)

16 A CEO received an email from an employee who has had her bag stolen and is in need of immediate money.

27 A company uses multiple SaaS and IaaS platforms for its corporate infrastructure and web application. This solution would provide security, manageability, and visibility of the platforms.

29 The IT department at a university is concerned about professors placing servers on the university network in an attempt to bypass security controls. This is called.... (2 words)



Across

1 A software developer needs to perform code-execution testing, black-box testing, and non-functional testing on a new product before its general release. The developer is conducting...

4 A manufacturer creates designs for very high security products that are required to be protected. These designs are not accessible by corporate networks or the Internet. They are.. (2 words)

5 This policy would help an organization identify and mitigate potential single points of failure in the company's IT security operations. (3 words)

7 This method is used for creating a detailed diagram of wireless access points and hotspots.

11 A company recently experienced a data breach and the source was determined to be an executive who was charging a phone in a public area. The executive should have used one of these. (3 words)

Across

13 Joe receives an email stating he won the lottery. The email includes a link that requests a name, mobile phone number, address, and DOB be provided to confirm identity before sending him the prize.

21 You need this to generate a server certificate to be used for 802.1X and secure RDP connections.

22 Under GDPR, this person is MOST responsible for the protection of privacy and website user rights. (3 words)

25 A server certificate that will work for all an organization's existing applications and any future applications that follow the same naming conventions, such as store.company.com.

27 A host was infected with malware. Joe reported that he did not receive any emails with links, but he had been browsing the Internet all day. This would likely show where the malware originated. (2 words)

28 Applications and systems that are used within an organization without consent or approval.

29 A company processes highly sensitive data and senior management wants to protect the sensitive data by utilizing classification labels. The company should use this access control scheme.

Down

2 This is the phase of the incident response process where a security analyst would run a vulnerability scan to check for missing patches during a suspected incident.

3 A security analyst is looking for a solution to help communicate to the leadership team the severity levels of the organization's vulnerabilities. This would best meet that need.

6 A user received an SMS on a mobile phone that asked for bank details.

8 This type of training might be used to enhance the skill levels of a company's developers.(2 words)

9 An organization that is located in a flood zone is MOST likely to document the concerns associated with the restoration of IT operations in a...

10 A turnstile is this type of control.

12 This access control scheme allows an object's access policy to be determined by its owner.

14 The manager who is responsible for a data set has asked a security engineer to apply encryption to the data on a hard disk. The security engineer is an example of a... (2 words)

15 This team of people is dedicated to testing the effectiveness of organizational security programs by emulating the techniques of potential attackers. (2 words)

16 A security assessment determines DES and 3DES are still being used on recently deployed production servers. The assessment has identified this. (2 words)

17 Your mobile phone does not work in the elevator in your office building. Your elevator is a ... (2 words)

18 This would allow functional test data to be used in new systems for testing and training purposes while protecting the real data. (2 words)

19 After entering a username and password, an administrator must draw a gesture on a touch screen. In MFA, this would be classified as this. (3 words)

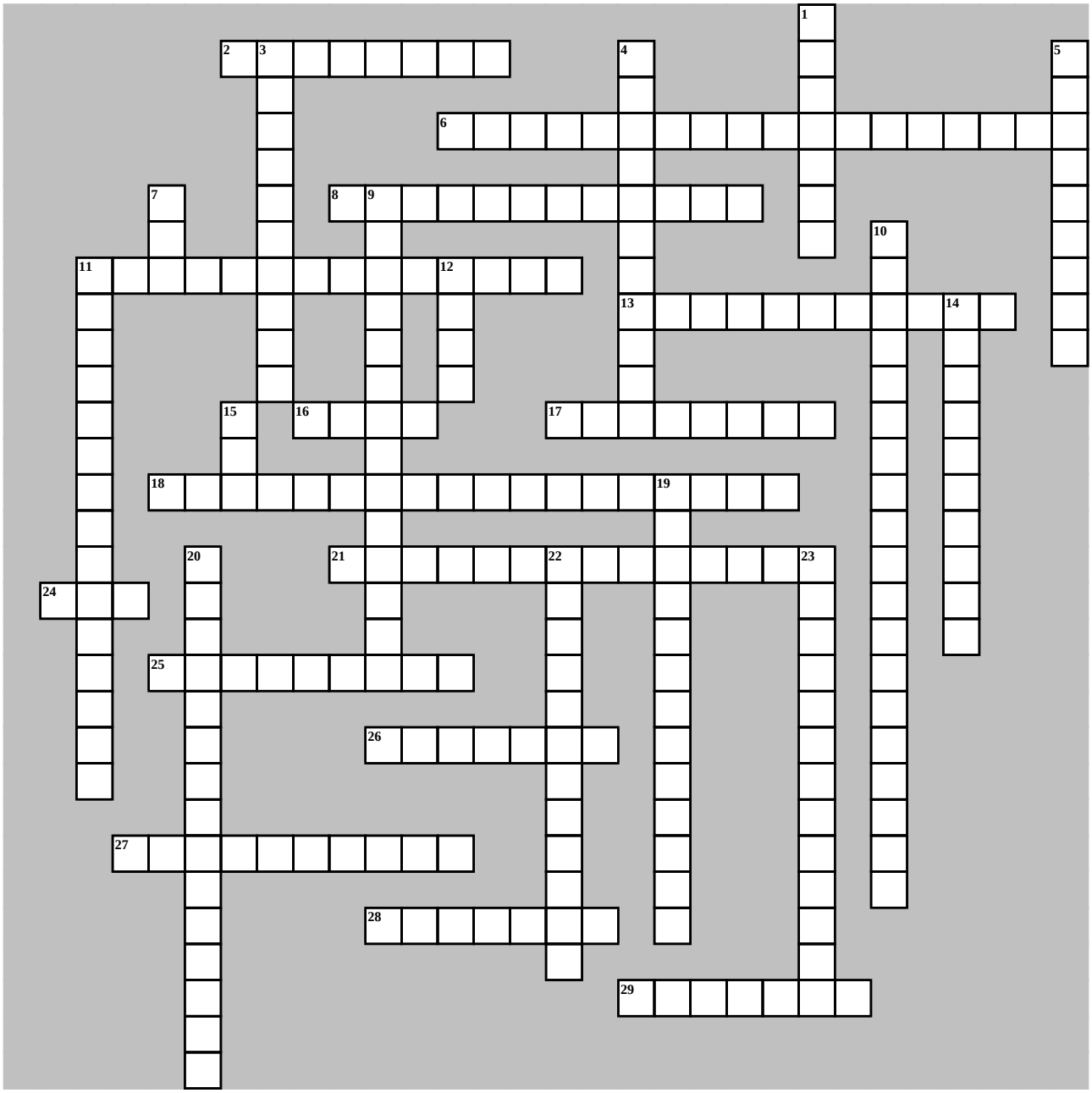
20 This RAID configuration is focused on high read speeds and fault tolerance.

23 Security logs have identified successful logon attempts to access a departed executive's accounts. This would have addressed this issue.

24 A company recently transfered sensitive videos between on-premises, company-owned websites learned the videos were shared on the Internet. This clause would MOST likely allow the company allow the company to find the cause.

25 An analyst captures 1Gb worth of inbound network traffic to the server and transfers the pcapback to the machine for analysis. The analyst would use this tool to further review the pcap.

26 An attacker has penetrated a company's network and moved laterally to the datacenter. The investigator needs these files to find out what was in the memory on the compromised server. (2 words)



Across

2 This pentester is conducting a pentest with prior knowledge of the network and applications being tested. (2 words)

6 This is a brute force attack in which stolen user account names and passwords are tested against multiple websites. (2 words)

8 A security analyst needs to perform periodic vulnerability scans on production systems. This type of scan would produce the best report.

11 In this stage of the incident response process, a security operations analyst may use the company's SIEM solution to correlate alerts.

13 You need to to identify a method for determining the tactics, techniques, and procedures of a threat actor against the organization's network. You will use this to accomplish your objective. (2 words)

16 To reduce overhead, an organization will use this cloud model to move from an on-premises email solution to a cloud-based email solution. At this time no other services will be moving.

Across

17 This may cause machine learning and AI-enabled systems to operate with unintended consequences. (2 words)

18 This would identify and remediate a data-loss event in an enterprise using third-party, web-based services and file-sharing platforms. (3 words)

21 This provides the best protection for sensitive information and data stored in cloud-based services but still allows for full functionality and searchabilityof data within the cloud-based services. (2 words)

24 This technical control is best suited for the detection and prevention of buffer overflows on hosts.

25 This type of control is a CCTV camera that is not being monitored.

26 A database administrator needs to ensure all passwords are stored in a secure manner, so the administrator adds randomly generated data to each password before storing. This is called...

27 A Chief Executive Officer's (CEO) personal information was stolen in a social engineering attack. You might find his personal information here. (3 words)

28 A security researcher is tracking an adversary by noting its attacks and techniques based on its capabilities, infrastructure, and victims. He is using this model of intrusion analysis.

29 A developer has just finished coding a custom web application and would like to test it for bugs by automatically injecting malformed data into it. The developer is using this technique.

Down

1 An analyst is logged into a server and must use native tools to map services running on it to the server's listening ports. This tool can best accomplish this task.

3 Aaron Swartz, The Jester, and Oxblood Ruffin (Cult of the Dead Cow network), for example.

4 In this phase of a cyberattack, a security engineer removes the infected devices from the network and locks down all compromised accounts.

5 An enterprise has hired an outside security firm to facilitate penetration testing on its network and applications. The firm has agreed to pay for each vulnerability that is discovered. This is a... (2 words)

7 A coffee shop runs a WiFi hotspot for its customers that utilizes WPA2-PSK. It would like to implement WPA3 to make its WiFi more secure. In plase of PSK, the coffee shop will most likely use this.

9 The process of passively gathering information prior to launching a cyberattack is called ...

10 In this type of attack, the attacker is trying to gain access by installing malware on a website that is known to be visited by the target victims. (2 words)

11 This helps mitigate injection attacks. (2 words)

12 This environment minimizes end-user disruption and is most likely to be used to assess the impacts of any database migrations or major system changes by using the final version of the code?

14 A university wants to protect the desktops in its classrooms and labs. It should use these. (2 words)

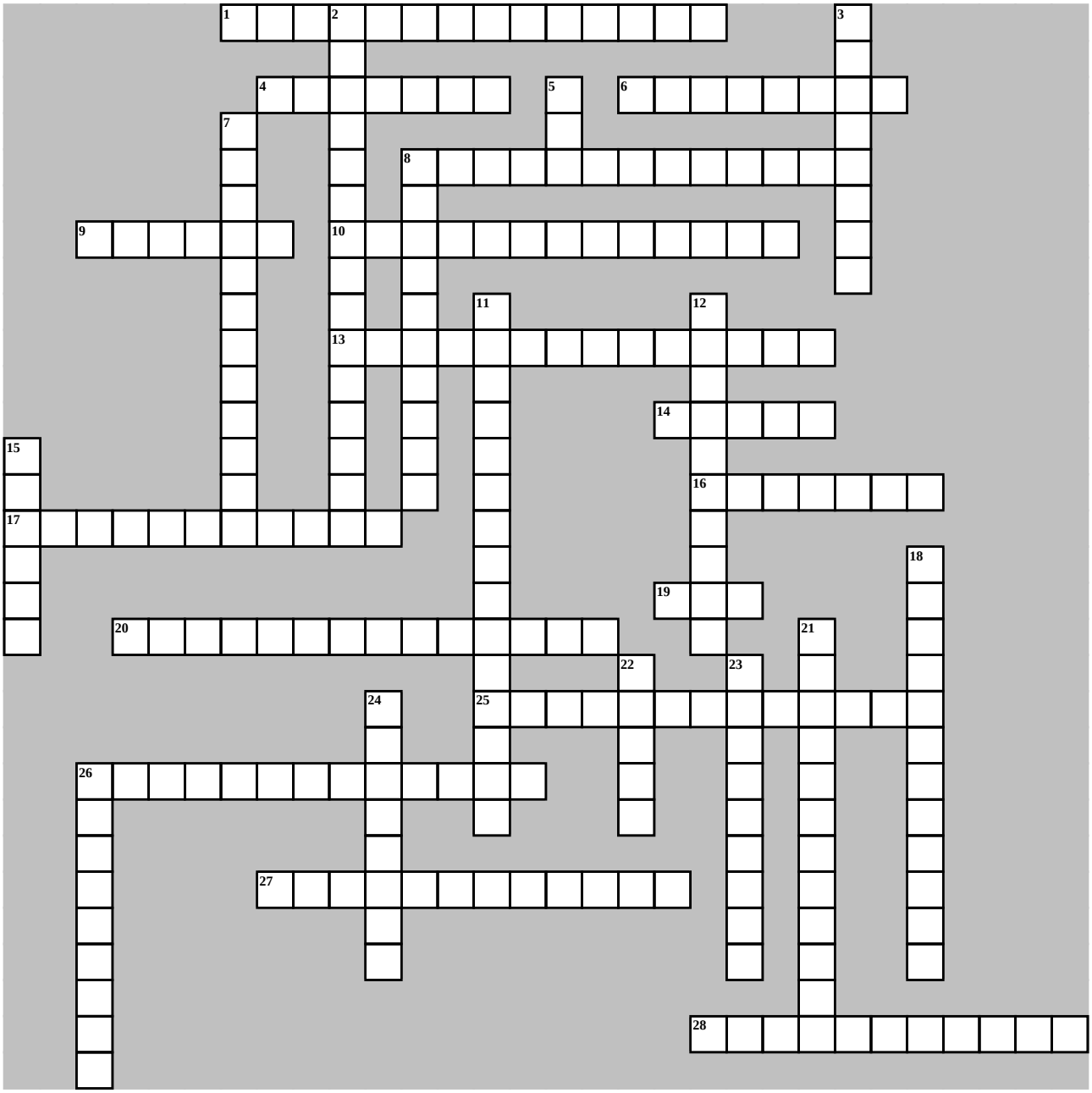
15 An organization just experienced a major cyberattack incident. The attack was well coordinated, sophisticated, and highly skilled. This was an...

19 AN attacker's intent is to imitate the look and feel of a legitimate website to obtain personal information from unsuspecting users. This is an example of...

20 This is the MFA attribute that requires a callback on a predefined landline. (3 words)

22 This kind of control is used when a primary control is unavailable.

23 When used in the design stage, this improves the efficiency, accuracy, and speed of a database.



Across

1 The record of evidence history from collection, to presentation in court, to disposal. (3 words)

4 These are used for purposes such as preventing bots from creating accounts on web forums and social media sites to spam them.

6 The output of a hash function. chmod Linux command for managing file permissions.

8 Information that is being transmitted between two hosts, such as over a private network or the Internet. (3 words)

9 A set of hosts that has been infected by a control program called a bot that enables attackers to exploit the hosts to mount attacks.

10 The points at which a network or application receives external connections or inputs/outputs that are potential vectors to be exploited by a threat actor. (2 words)

13 In privacy regulations, the entity that determines why and how personal data is collected, stored, and used. (2 words)

14 If compromised, this system may may cause great danger to the integrity of water supplies and their chemical levels.

Across

16 The process of extracting data from a computer when that data has no associated file system metadata.

17 The method of using a digital signature to ensure the source and integrity of programming code. (2 words)

19 A systematic activity that identifies organizational risks and determines their effect on ongoing, mission critical operations.

20 A cloud that is deployed for shared use by cooperating tenants. (2 words)

25 The process by which the need for change is recorded and approved. (2 words)

26 A software application or gateway that filters client requests for various types of internet content (web, FTP, IM, and so on). (2 words)

27 This threat actor is motivated primarily by a desire for personal recognition and a sense of accomplishment. (2 words)

28 Sending an unsolicited message or picture message using a Bluetooth connection.

Down

2 Buffer overflow attacks can be prevented using this. (2 words)

3 The defensive team in a penetration test or incident response exercise. (2 words)

5 A library of programming utilities used, for example, to enable software developers to access functions of the TCP/IP network stack under a particular operating system.

7 A wireless attack where an attacker gains access to unauthorized information on a device using a Bluetooth connection.

8 Information that is primarily stored on specific media, rather than moving from one medium to another. (3 words)

11 A set of rules governing user security information, such as password expiration and uniqueness, which can be set globally. (2 words)

12 A concept in which an expanding list of transactional records listed in a public ledger is secured using cryptography.

15 A specific path by which a threat actor gains unauthorized access to a system.

18 The fundamental security goal of ensuring that computer systems operate continuously and that authorized persons can access data that they need.

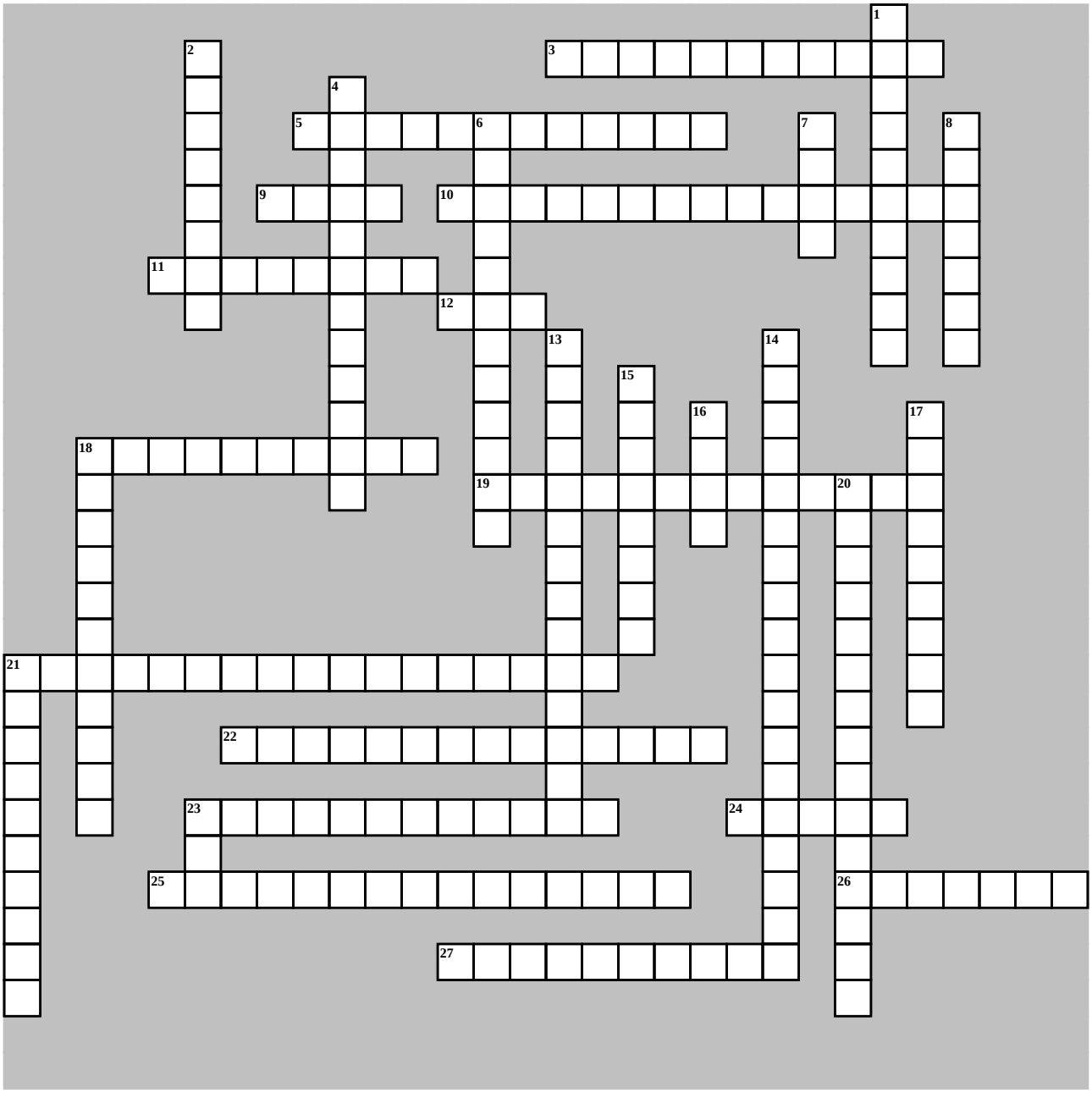
21 A software vulnerability where an attacker is able to circumvent access controls and retrieve confidential or sensitive data from the file system or database. (2 words)

22 A software development model that focuses on iterative and incremental development to account for evolving requirements and expectations.

23 In cryptography, the act of two different plaintext inputs producing the same exact ciphertext output.

24 Duplicating a smart card by reading the confidential data stored on it.

26 Potentially unsecure programming practice of using code originally written for a different context. (2 words)



Across

3 A cloud deployment that uses both private and public elements. (2 words)

5 Applying an access control list to a switch or access point so that only clients with approved MAC addresses can connect to it. (2 words)

9 An algorithm that generates a one-time password using a hashbased authentication code to verify the authenticity of the message.

10 The process by which an attacker is able to move from one part of a computing environment to another. (2 words)

11 A network set up with the purpose of luring attackers away from assets of actual value and/or discovering attack strategies and weaknesses in the security configuration.

12 Framework for negotiating authentication methods that enables systems to use hardware-based identifiers, such as fingerprint scanners or smart card readers, for authentication.

18 The property by which a computing environment can instantly react to both increasing and decreasing demands in workload.

Across

19 Coding methods to anticipate and deal with exceptions thrown during execution of a process. (2 words)

21 On a Windows domain, a way to deploy peruser and per-computer settings such as password policy, account restrictions, firewall status, and so on. (3 words)

22 In risk calculation, the percentage of an asset's value that would be lost during a security incident or disaster scenario. (2 words)

23 The last rule at the bottom of a static firewall access control list (ACL) (2 words)

24 A set of open, non-proprietary standards that are used to secure data through authentication and encryption as the data travels across the network or the Internet.

25 A basic principle of security stating that something should be allocated the minimum necessary rights, privileges, or information to perform its role. (2 words)

26 A dynamic code analysis technique that involves sending a running application random and unusual input so as to evaluate how the app responds.

27 A process that provides a shared login capability across multiple systems and enterprises. It essentially connects the identity management services of multiple systems.

Down

1 A hardened server that provides access to other hosts. (2 words)

2 A single sign-on authentication and authorization service that is based on a time-sensitive ticket-granting system.

4 Biometric mechanism that identifies a subject based on movement pattern. (2 words)

6 A type of switch or router that distributes client requests between different resources. This provides fault tolerance and improves througput. (2 words)

7 Linux command for searching and filtering input. This can be used as a file search tool when combined with ls.

8 A measure of disorder. Cryptographic systems should exhibit high entropy to better resist brute force attacks.

13 A model developed by Lockheed Martin that describes the stages by which a threat actor progresses a network intrusion. (3 words)

14 Encryption of all data on a disk can be accomplished via a supported OS, third party software, or at the controller level by the disk device itself. (3 words)

15 A private network that is only accessible by the organization's own personnel.

16 method used to verify both the integrity and authenticity of a message by combining a cryptographic hash of the message with a secret key.

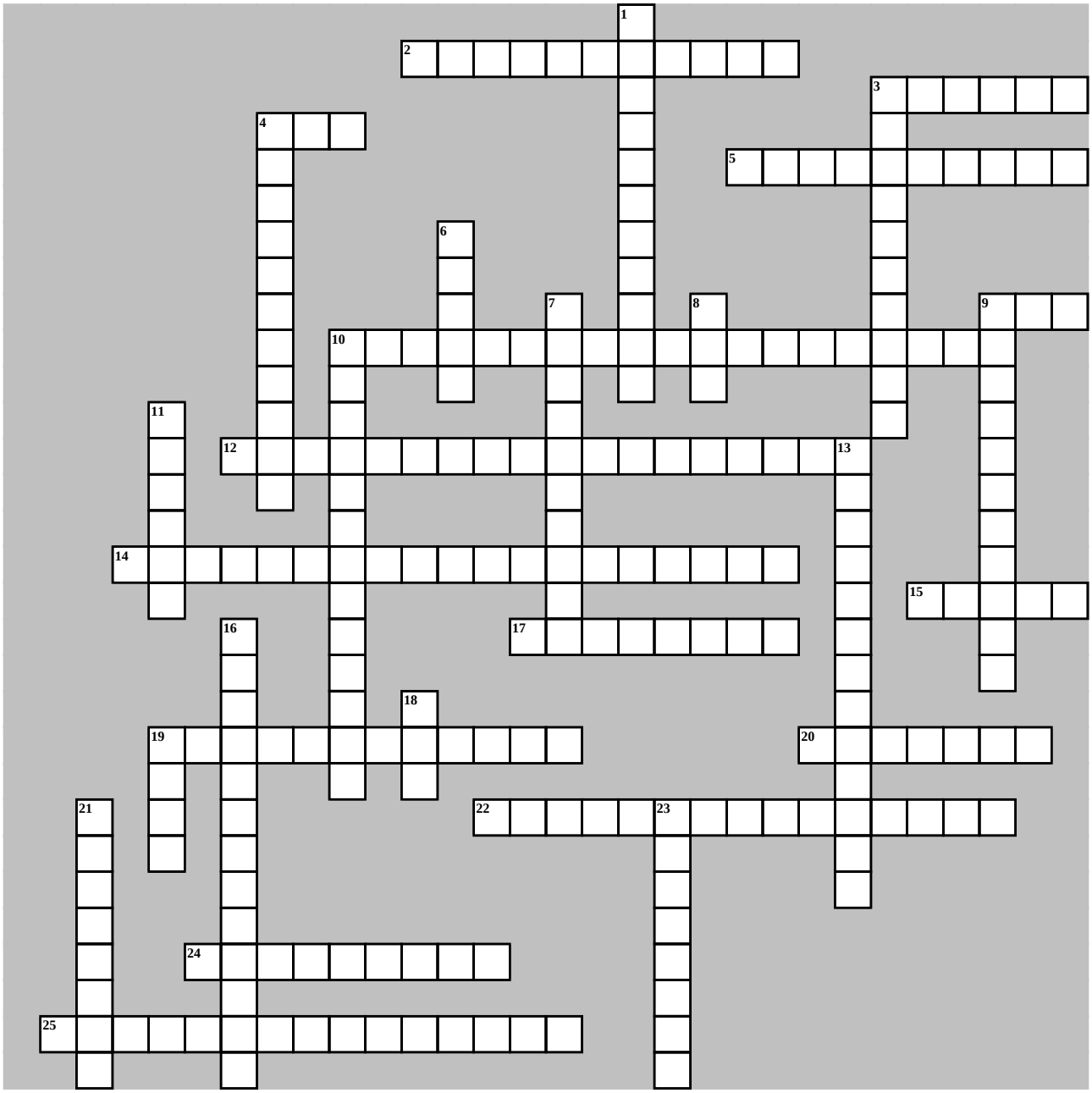
17 A malicious program or script that is set to run under particular circumstances or in response to a defined event. (2 words)

18 Procedures and tools to collect, preserve, and analyze digital evidence.

20 An attack in which a computed result is too large to fit in its assigned storage space. (2 words)

21 The practice of creating a virtual boundary based on real-world geography.

23 Framework for creating a Security Association (SA) used with IPSec.



Across

2 The process of ensuring that all HR and other requirements are covered when an employee leaves an organization. Also known as exit interview.

3 High-level programming language that is widely used for automation.

4 Dial-up protocol working at layer 2 (Data Link) used to connect devices remotely to networks.

5 A software vulnerability that can occur when software does not release allocated memory when it is done using it, potentially leading to system instability. (2 words)

9 Format that allows a private key to be exported along with its digital certificate.

10 A software vulnerability that can occur when code attempts to read a memory location specified by a pointer, but the memory location is null. (2 words)

12 An attack when the web browser is compromised by installing malicious plug-ins or scripts, or intercepting API calls between the browser process and DLLs.

Across

14 risk analysis method that uses opinions and reasoning to measure the likelihood and impact of risk. (2 words)

15 An arbitrary number used only once in a cryptographic communication, often to prevent replay attacks.

17 Information stored or recorded as a property of an object, state of a system, or transaction.

19 Preventing a device attached to a switch port from communicating on the network unless it matches a given MAC address or other protection profile. (2 words)

20 A secure entry system with two gateways, only one of which is open at any one time.

22 Identifying, testing, and deploying OS and application updates. (2 words)

24 A type of RAID that using two hard disks, providing the simplest way of protecting a single disk against failure. Data is written to both disks and can be read from either disk.

25 The security goal of ensuring that the party that sent a transmission or created data remains associated with that data and cannot deny sending or creating that data.

Down

1 A server that mediates the communications between a client and another server. (2 words)

3 A mode of penetration testing where red and blue teams share information and collaborate throughout the engagement. (2 words)

4 An enumeration or vulnerability scan that analyzes only intercepted network traffic rather than sending probes to a target. (2 words)

6 Publicly available information plus the tools used to aggregate and search it.

7 In digital forensics, being able to trace the source of evidence to a crime scene and show that it has not been tampered with.

8 Base64 encoding scheme used to store certificate and key data as ASCII text.

9 In cybersecurity, the ability of a threat actor to maintain covert access to a target host or network.

10 Passphrase-based mechanism to allow group authentication to a wireless network. The passphrase is used to derive an encryption key. (2 words)

11 One of the best-known commercial vulnerability scanners, produced by Tenable Network Security.

13 In PKI, an account or combination of accounts that can copy a cryptographic key from backup or escrow and restore it to a subject host or user. (2 words)

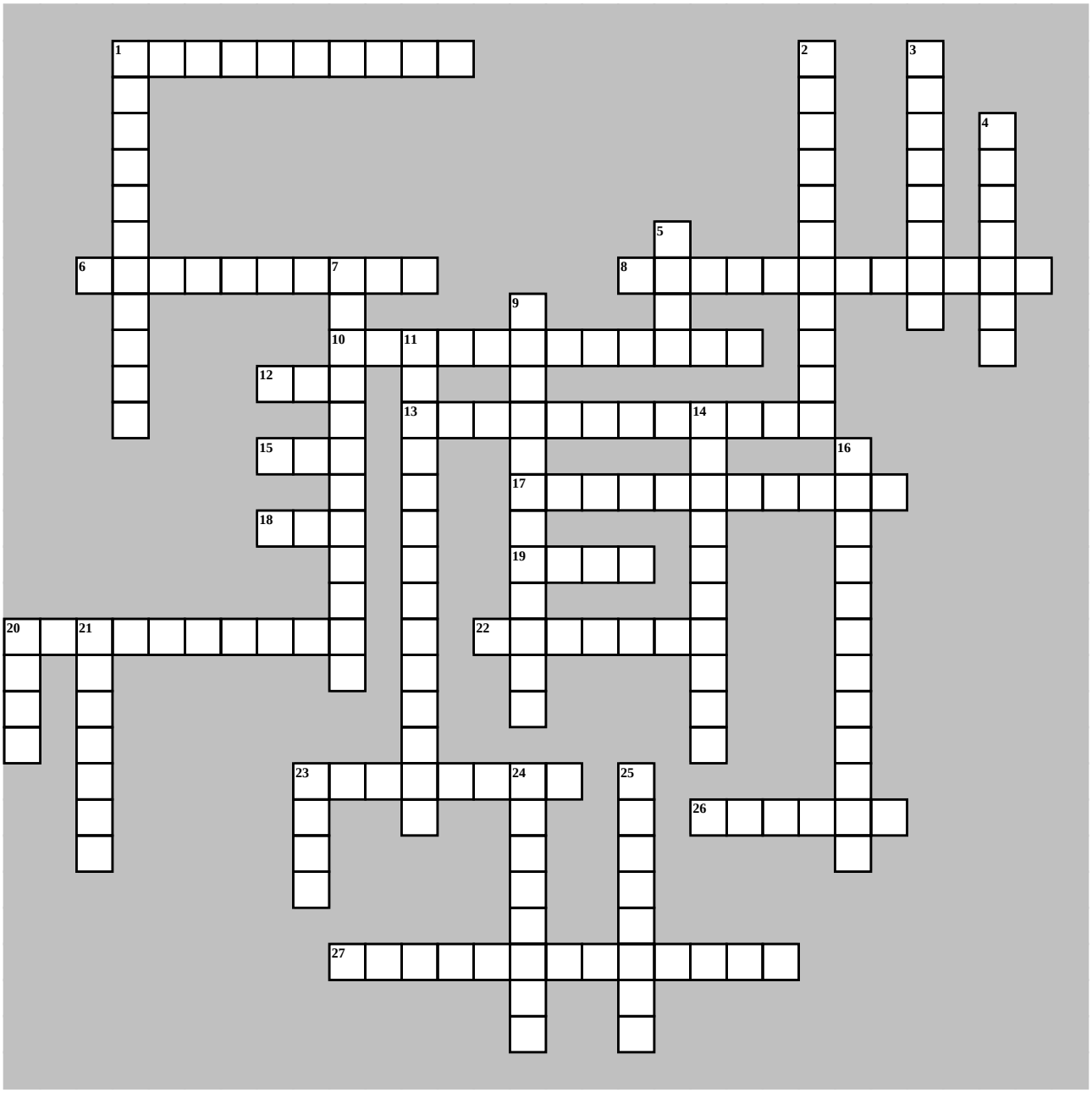
16 A software architecture where components of the solution are conceived as highly decoupled services not dependent on a single platform type or technology.

18 Software that cannot definitively be classed as malicious, but may not have been chosen by or wanted by the user.

19 A switch (or router) that performs some sort of authentication of the attached device before activating the port.

21 A checklist of actions to perform to detect and respond to a specific type of incident

23 In threat hunting, the concept that threat actor and defender may use deception or counterattacking strategies to gain positional advantage.



Across

1 A UEFI feature that prevents unwanted processes from executing during the boot operation. (2 words)

6 A nondiscretionary access control technique that is based on a set of operational rules or restrictions to enforce a least privileges permissions policy.

8 The process of thorough and completely removing data from a storage medium so that file remnants cannot be recovered.

10 A document highlighting the results of risk assessments in an easily comprehensible format. (2 words)

12 Personal authentication mechanism for Wi-Fi networks introduced with WPA3 to address vulnerabilities in the WPA-PSK method.

13 A type of proxy server that protects servers from direct contact with client requests. (2 words)

15 Field in a digital certificate allowing a host to be identified by multiple host names or subdomains.

17 A digital certificate that has been signed by the entity that issued it, rather than by a CA.

Across

18 A disk drive where the controller can automatically encrypt data that is written to it.

19 An XML-based data format used to exchange authentication information between a client and a service.

20 A software architecture that runs functions within virtualized runtime containers in a cloud rather than on dedicated server instances.

22 A portion of a network where all attached hosts can communicate freely with one another.

23 Utility that runs port scans through third-party websites to evade detection.

26 In PKI, a CA that issues certificates to intermediate CAs in a hierarchical structure. (2 words)

27 When the resulting outcome from a process is directly dependent on the order and timing of certain events, and those events fail to execute in the order and timing intended by the developer. (2 words)

Down

1 VPN configuration where only traffic for the private network is routed via the VPN gateway. (2 words)

2 The property by which a computing environment is able to gracefully fulfill its ever-increasing resource needs.

3 A scheduling approach used by load balancers to route traffic to devices that have already established connections with the client in question.

4 An automated version of a playbook that leaves clearly defined interaction points for human analysis.

5 A security countermeasure that mitigates the impact of a rainbow table attack by adding a random value to each plaintext input.

7 A dual-homed proxy/ gateway server used to provide Internet access to other network nodes, while protecting them from external attack. (2 words)

9 A maliciously spawned remote command shell where the victim host opens the connection to the attacking host. (2 words)

11 A host or network account that is designed to run a background service, rather than to log on interactively. (2 words)

14 A graphical table indicating the likelihood and impact of risk factors identified for a workflow, project, or department for reference by stakeholders. (2 words)

16 An attack where the attacker intercepts some authentication data and reuses it to try to re-establish a session. (2 words)

20 A spam attack that is propagated through instant messaging rather than email.

21 A class of malware that modifies system files, often at the kernel level, to conceal its presence.

23 A class of security tools that facilitates incident response, threat hunting, and security configuration by orchestrating automated runbooks and delivering data enrichment.

24 A DoS attack mitigation strategy that directs the traffic that is flooding a target IP address to a different network for analysis.

25 The process of developing and implementing additional code between an application and the operating system to enable functionality that would otherwise be unavailable.

Curvy Words

Network Architecture

Solve the clues and find the words. Can you find all 20? One word has already been found for you!

Curvy Words: Network Architecture: CLUES

1. This is the process of spanning a single VLAN across multiple switches.
2. A deviation from an expected pattern or behavior.
3. This can be hardware, software, or a combination of both whose purpose is to enforce a set of network security policies across network connections.
4. This is where you have configured the network devices to limit traffic access across different parts of a network.
5. This allows multiple systems to be reflected back as a single IP address.
6. This is a passive signal-copying mechanism installed between two points on the network.
7. Provides the system information as to what objects are permitted which actions.
8. The use of specific technologies on a network to guarantee its ability to manage traffic based on a variety of indicators.
9. This is an example of a segment, one that is accessible from the Internet, and from the internal network, but cannot be crossed directly.
10. These are sensors, or concentrators that combine multiple sensor that collect data for processing by other systems.
11. Communication links that are network connections to two or more networks across an intermediary network layer.
12. These management channels are physically separate connections, via separate interfaces that permit the active management of a device even when the data channel is blocked for some reason.
13. This is a hardened system on a network specifically used to access devices in a separate security zone.
14. This can be used to filter out undesirable traffic and prevent employees from accessing potentially hostile websites.
15. This is an extension of a selected portion of a company's intranet to external partners. This allows a business to share information with customers, suppliers, partners, and other trusted groups while using a common set of Internet protocols to facilitate operations.
16. In these management systems, the management channel is the same channel as the data channel.
17. A set of protocols developed by the IETF to securely exchange packets at the network layer (layer 3) of the OSI reference model.
18. In this mode, the security of packet traffic is provided between endpoint node machines in each network and not at the terminal host machines.
19. A device that takes multiple inputs and combines them to a single output.
20. Involves sending each new request to the next server in rotation.

Curvy Words 2
Network Architecture

Solve the clues and find the words. Can you find all 14? Good luck!!

R	C	W	L	Y	X	S	I	H	R	S	E	E	W	T	A	Z
T	R	P	C	P	R	E	W	O	E	A	F	P	D	Y	S	E
U	N	N	W	L	A	V	M	V	F	R	Z	F	R	Z	R	U
T	T	U	E	K	H	I	M	A	E	V	I	C	N	O	O	R
T	R	A	P	O	R	T	M	O	D	E	N	I	T	Y	X	T
I	N	S	K	T	Y	I	M	N	V	K	U	N	K	X	E	Y
L	O	R	T	N	O	C	S	S	E	C	C	A	H	R	C	T
Z	P	S	F	A	S	E	P	O	B	R	K	N	T	W	O	E
N	O	I	T	A	L	S	N	A	R	T	S	S	E	R	R	Y
Z	K	P	O	U	E	I	L	T	E	M	G	P	D	A	T	P
C	F	B	O	H	E	S	F	C	A	R	N	Y	L	D	T	O
T	S	B	M	T	A	W	D	S	E	V	I	I	S	E	S	R
B	Z	P	E	R	F	C	G	R	H	Y	T	A	N	L	O	F
U	I	H	L	M	V	I	C	E	A	M	A	E	U	S	A	G
N	K	E	X	E	G	T	I	E	U	U	G	D	F	R	I	Z
D	V	S	T	T	N	S	H	R	S	F	G	D	O	W	F	O
N	U	I	N	V	R	A	O	E	F	S	L	O	C	P	L	S

Curvy Words 2 Network Architecture: CLUES

1. Designed to keep a host connected to the same server across a session.
2. Often happens when alerts that should be generated aren't.
3. These occur when expected behavior is identified as malicious.
4. These are commonly implemented in firewalls and IDS/IPS solutions to prevent DoS and DDoS attacks.
5. This model uses artificial intelligence (AI) to detect intrusions and malicious traffic.
6. This is a private, internal network that uses common network technologies (HTTP, FTP, and so on) to share information and provide resources to internal organizational users.
7. This is the selective admission of packets based on a list of approved Media Access Control addresses.
8. Managing the endpoints on a case-by-case basis as they connect.
9. Allows many different internal, private addresses to share a single external IP address.
10. When a user requires access to a network and its resources but is not able to make a physical connection
11. Typically installed on the server side of a network connection, often in front of a group of web servers, and intercepts all incoming web requests.
12. This is a form of VPN where not all traffic is routed via the VPN.
13. In this mode, the security of packet traffic is provided by the endpoint computers.
14. This is a security model centered on the belief that you should not trust any request without verifying authentication and authorization.

Network Architecture Word Search

Find each of the following words.

PROXY SERVER
TRANSPORT MODE
FILE INTEGRITY MONITORS
OUT OF BAND
INTRANET
NETWORK TAP
FALSE NEGATIVES
FIREWALL
QUALITY OF SERVICE
UNIFIED THREAT MANAGEMENT
VIRTUALIP
REMOTE ACCESS
EXTRANET
COLLECTORS
MAC FILTERING
FALSE POSITIVES
ACCESS CONTROL LIST
TUNNEL MODE
VIRTUAL PRIVATE NETWORK
AGGREGATOR
SPLIT TUNNEL
AFFINITY
ROUND ROBIN
PORT ADDRESS TRANSLATION
SCREENED SUBNET
IN BAND
SITE TO SITE
TRUNKING
FLOOD GUARDS
ZERO TRUST
REVERSE PROXY
JUMP SERVER
HEURISTIC
NETWORK SEGMENTATION
IPSEC

E T N E M E G A N A M T A E R H T D E I F I N U R E
R T O S S E V I T A G E N E S L A F A T P A R T E W
E D N A B N I Q U A L I T Y O F S E R V I C E E V R
N E T W O R K S E G M E N T A T I O N I L T T N R T
A K V I R T U A L I P T R U N K I N G N A R R A E O
A R T C F D A G G R E G A T O R S F B B U U U R S V
C O R E C E D O M L E N N U T R E R S A T N N T Y L
C W F S E C E A F F I N I T Y I L V T N R K K X X R
E T R P S D N A B F O T U O M N T F R D I I I E O E
S E E I P Z T L A T D N A B F O T U O E V N N S R J
S N S N I E E D O M T R O P S N A R T L S G G S P D
C E E R B R E R F I R E W A L L I C E S I P S P D E
O T V S E U G E O I S H C O L L E C T O R S M I K E
N A E I S V S N S T N I P S E C C E S P I G L U G R
T V P L T E E D I I R R E V R E S Y X O R P E O J O
R I A I I I C R E R T U G F I R E W A L L E N P N N
O R T S P F S C S N E E S N D R C E S P I X N A I C
L P K D S I C O A E E T T T I N T R A N E T U T B U
L L R R E R E H P E P E L O T K A U O L R R T K O V
I A O A C E S A E E T R R I S C N B A R D A T R R E
S U W U E W P S B U S O O C F I E U F L N N I O D N
T T T G S A I C I N R L M X S C T S R O I L L W N O
E R E D P L C E S P I I A E Y A A E P T T P P T U M
R I N O I L D N A B N I S F R N I M L I L U S E O H
N V P O R T A D D R E S S T R A N S L A T I O N R R
U I I L S R O T I N O M Y T I R G E T N I E L I F S
W I F F I O E S B T U E O R R C W E Y N L T L N R F

Solve the clues to uncover the secret, which is something related to cryptography.

1. A switching protocol that prevents network loops by dynamically disabling links as needed. ◯ _ _ _ _ _ _ _   _ _ _ _   _ _ _ _ _ _ _ _
2. Mechanism used to mitigate performance and privacy issues when requesting certificate status from an OCSP responder. _ ◯ _ _ _ _ _ _
3. Applying consistent names and labels to asset s and digital resources/identities within a configuration management system. _ _ _ _ _ _ _ _   _ _ _ _ _ _   _ _ _ _ ◯ _ _ _ _ _
4. Provisioning processing resource between the network edge of IoT devices and the data center to reduce latency. _ _ ◯   _ _ _ _ _ _ _ _ _
5. The record of evidence history from collection, to presentation in court, to disposal. _ _ ◯ _ _   _ _   _ _ _ _ _ _ _
6. The binary format used to structure the information in a digital certificate. _ _ _ _ _ _ _ _ _ _ _ _ _   _ ◯ _ _ _ _ _ _   _ _ _ _ _
7. A cloud that is deployed for shared use by cooperating tenants. _ ◯ _ _ _ _ _ _ _   _ _ _ _ _
8. In data protection, the principle that countries and states may impose individual requirements on data collected or stored within their jurisdiction. _ _ _ _   _ _ _ _ _ _ _ ◯ _ _ _
9. Utility for command-line manipulation of URL-based protocol requests. _ _ ◯ _
10. Information that is primarily stored on specific media, rather than moving from one medium to another. _ ◯ _ _   _ _   _ _ _ _
11. A measure of disorder. _ _ _ _ _ ◯ _
12. In a Wi-Fi site survey, a diagram showing signal strength at different locations. ◯ _ _ _   _ _ _
13. A method that uses feature comparisons and likenesses rather than specific signature matching to identify whether the target of observation is malicious. _ _ _ _ _ _ _ _ _   _ _ _ _ ◯ _ _ _

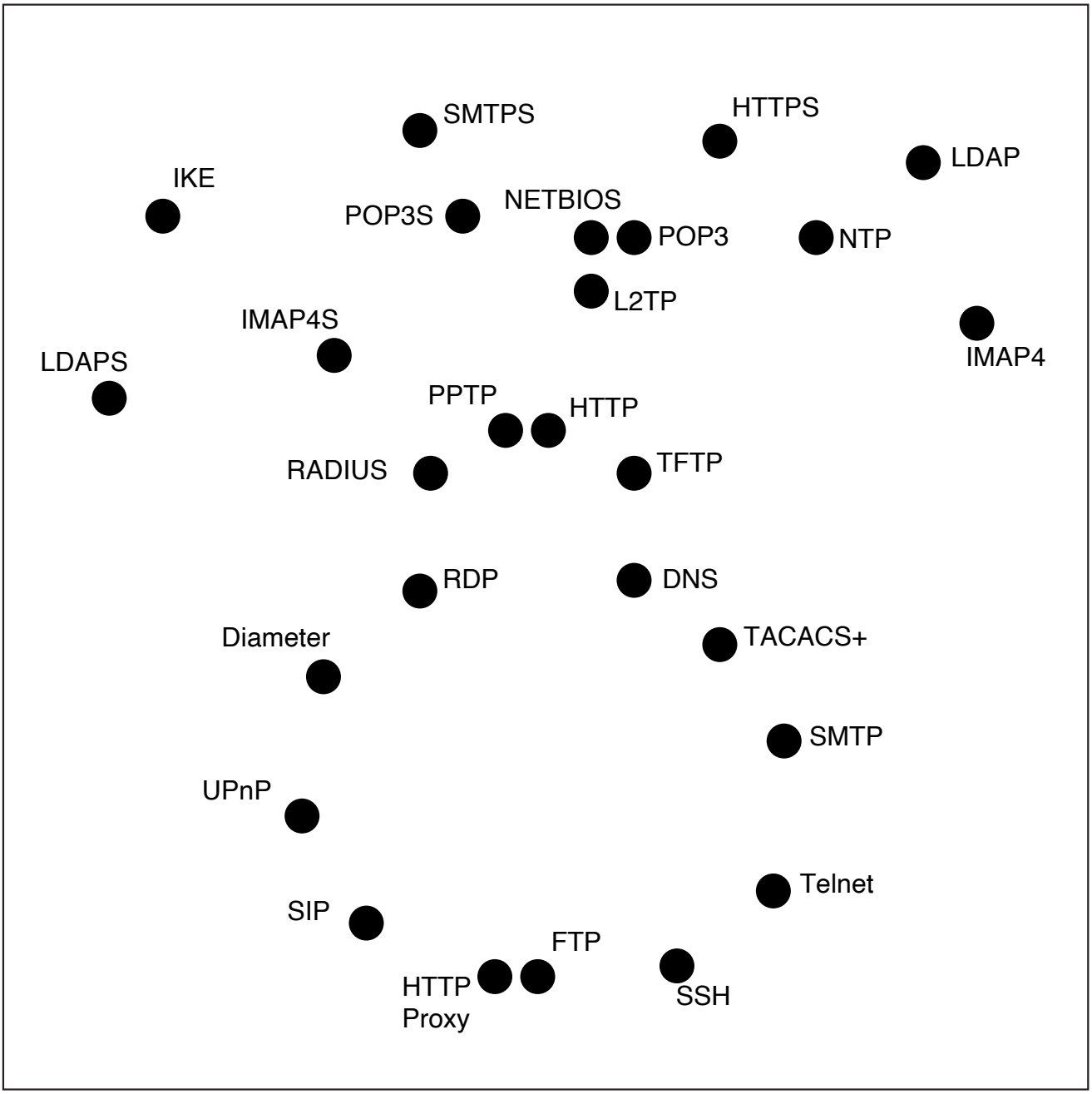
Secret: _ _ _ _ _ _ _ _ _ _ _ _ _

Solve the clues and unscramble the letters in the circles to discover the secret, which is something that blocks external electromagnetic fields.

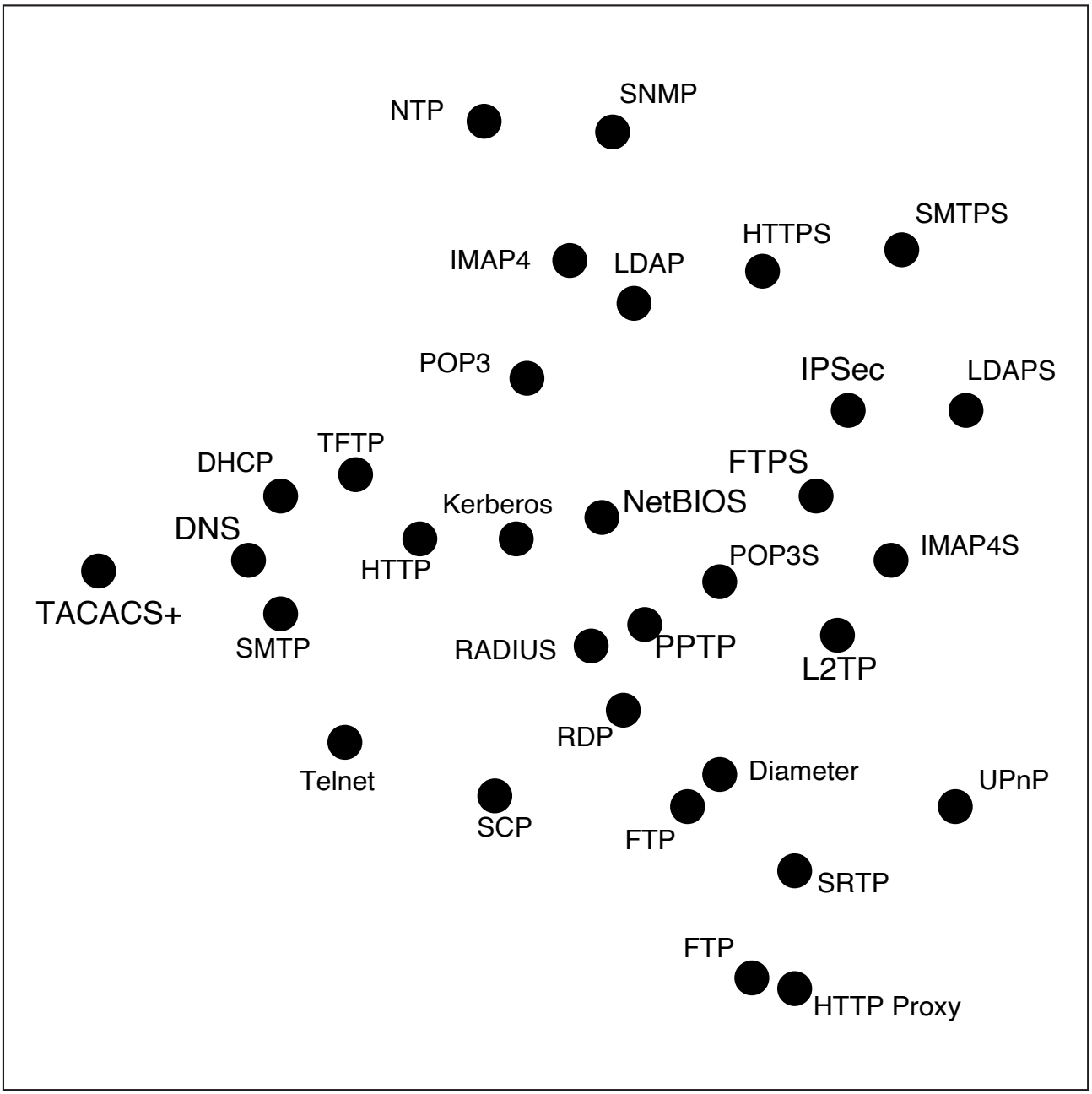
1. Preventing a device attached to a switch port from communicating on the network unless it matches a given MAC address or other protection profile.
   _ _ _ _ _ _ _ _ _ _ _ _
2. The practice of creating a virtual boundary based on real-world geography.
   _ _ _ _ _ _ _ _ _ _
3. The process by which an attacker can move from one part of a computing environment to another. _ _ _ _ _ _ _ _ _ _ _ _ _ _ _
4. Information stored or recorded as a property of an object, state of a system, or transaction. _ _ _ _ _ _ _
5. Risk that an event will pose if no controls are put in place to mitigate it.
   _ _ _ _ _ _ _ _ _ _ _
6. An impersonation attack in which a request for a website, typically an e-commerce site, is redirected to a similar looking, but fake, website. _ _ _ _ _ _ _ _
7. In threat hunting, the concept that threat actor and defender may use deception or counterattacking strategies to gain positional advantage. _ _ _ _ _ _ _
8. The process of making a host or app configuration secure by reducing its attack surface through running only necessary services, installing monitoring software to protect against malware and intrusions, and establishing a maintenance schedule to ensure the system is patched to be secure against software exploits. _ _ _ _ _ _ _ _ _
9. Implementation of a sandbox for malware analysis. _ _ _ _ _ _
10. A deidentification method where generic or placeholder labels are substituted for real data while preserving the structure or format of the original data.
    _ _ _ _ _ _ _ _ _ _ _
11. Code in an application that is redundant because it will never be called within the logic of the program flow. _ _ _ _ _ _ _ _

Secret: _ _ _ _ _ _ _ _ _ _ _

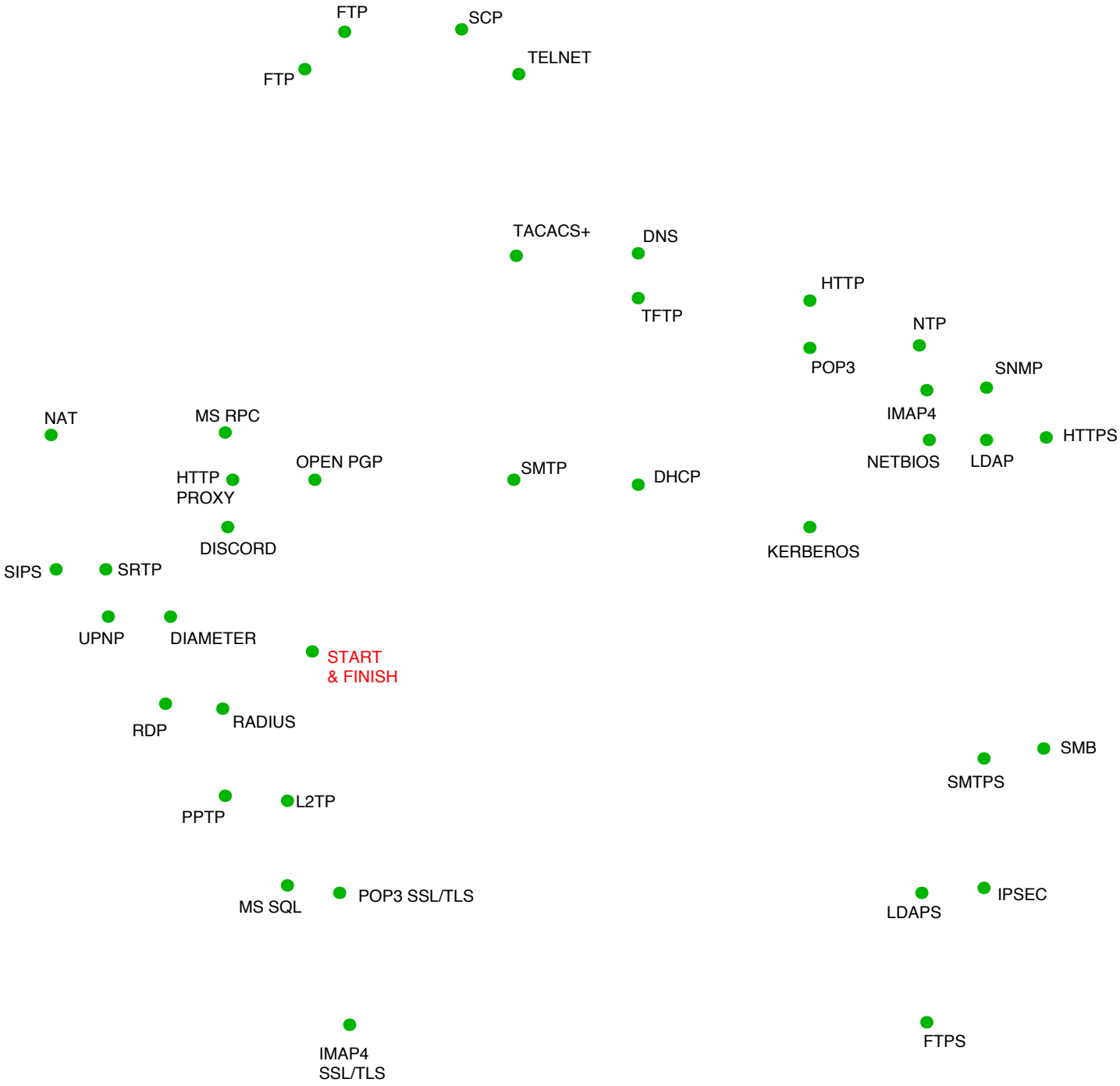
1 Start with the lowest number port and connect the protocols until you complete the image, always working from the lower port number to the next higher port number. Can you label the port numbers with the protocols?



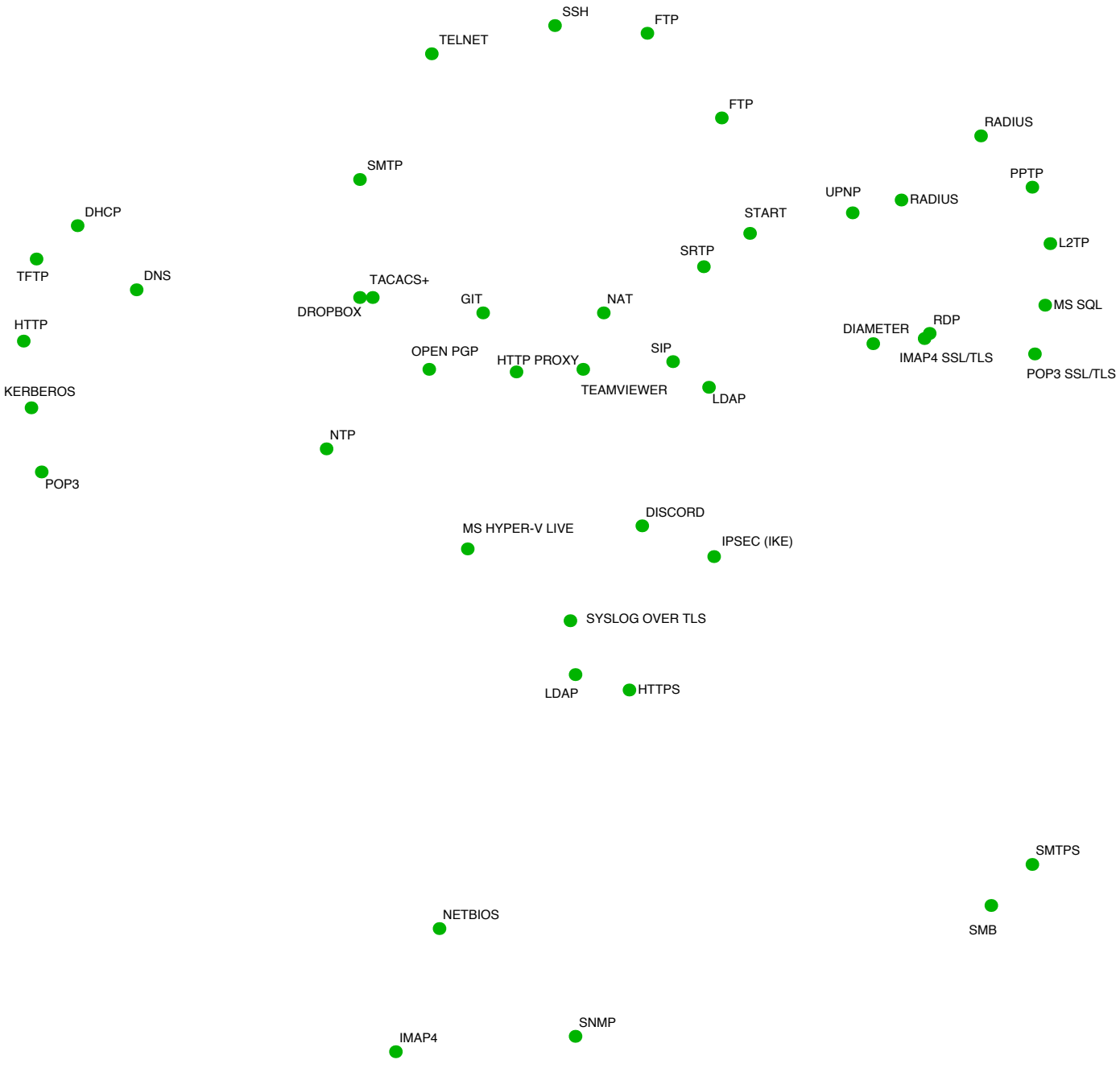
2 Start with the lowest number port and connect the protocols until you complete the image, always working from the lower port number to the next higher port number. Can you label the port numbers with the protocols?



Mystery Puzzle 1



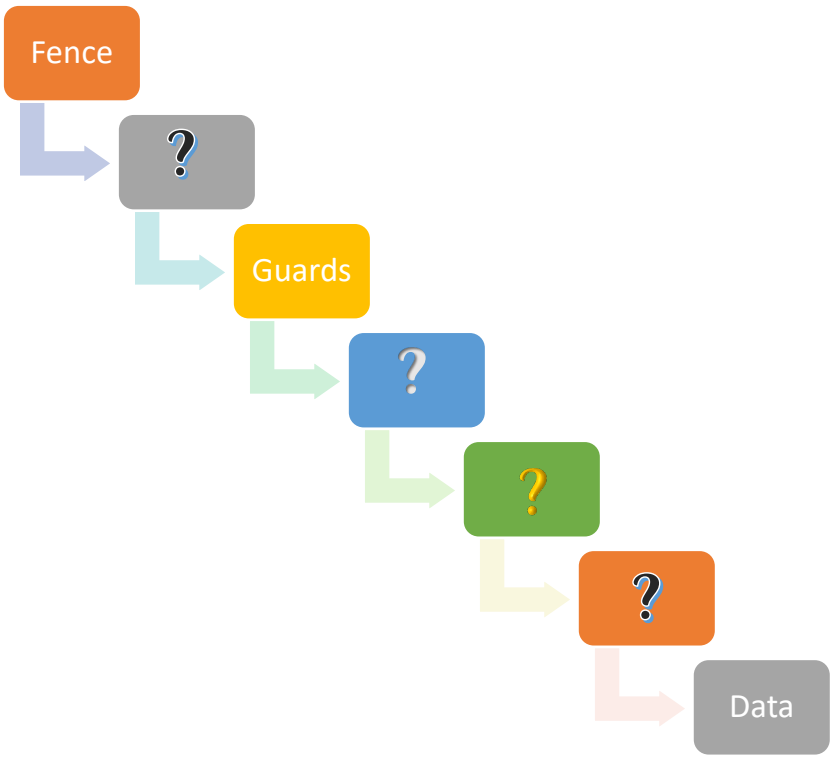
Mystery Puzzle 2



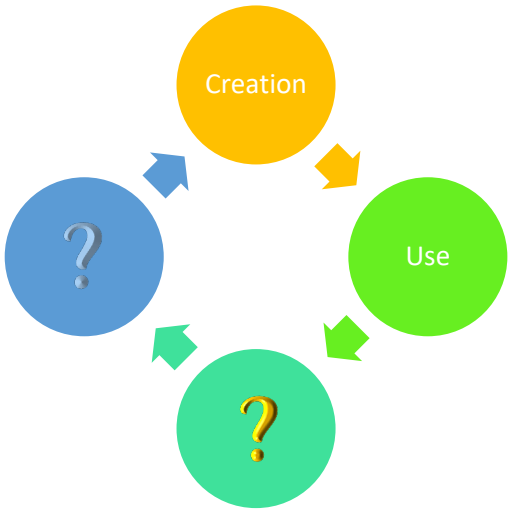
Processes and Cycles

What comes before and after? Fill in the blank spaces!

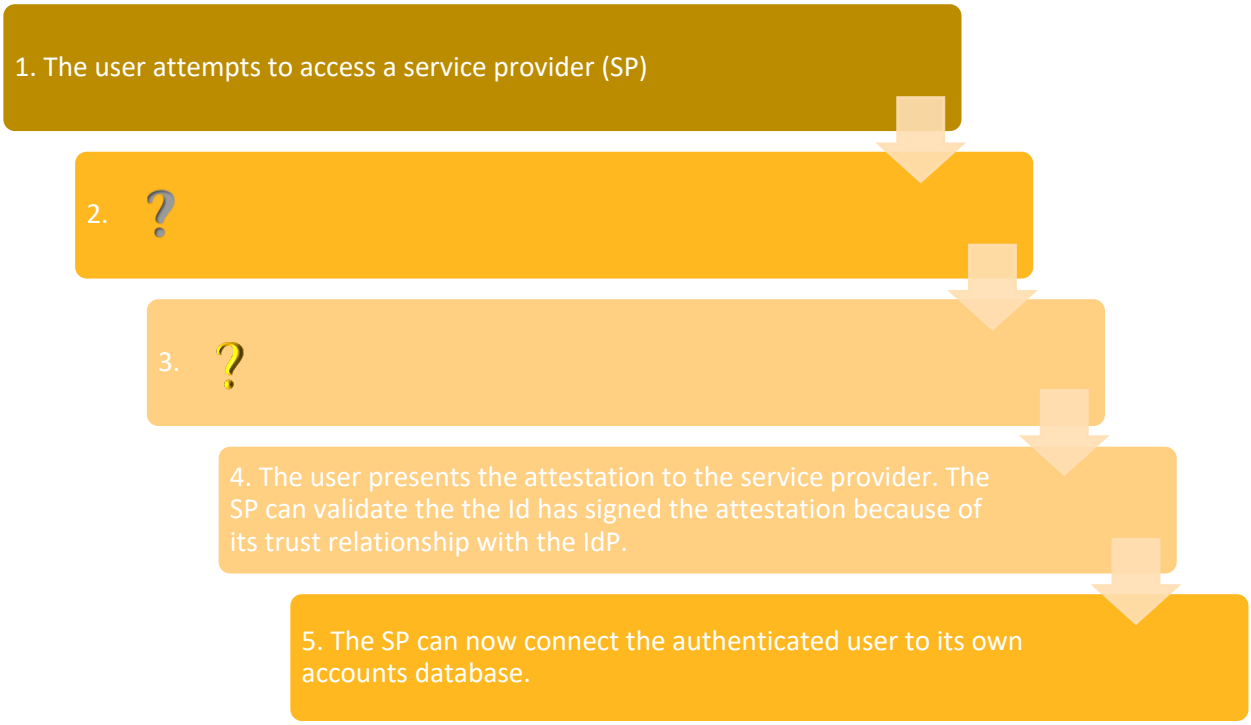
1. Defense in Depth



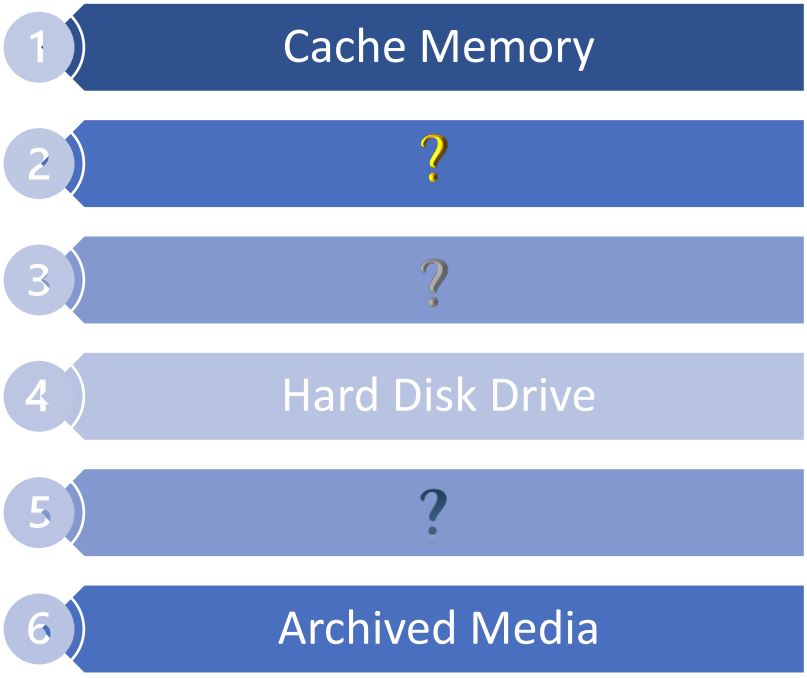
2. Information Life Cycle



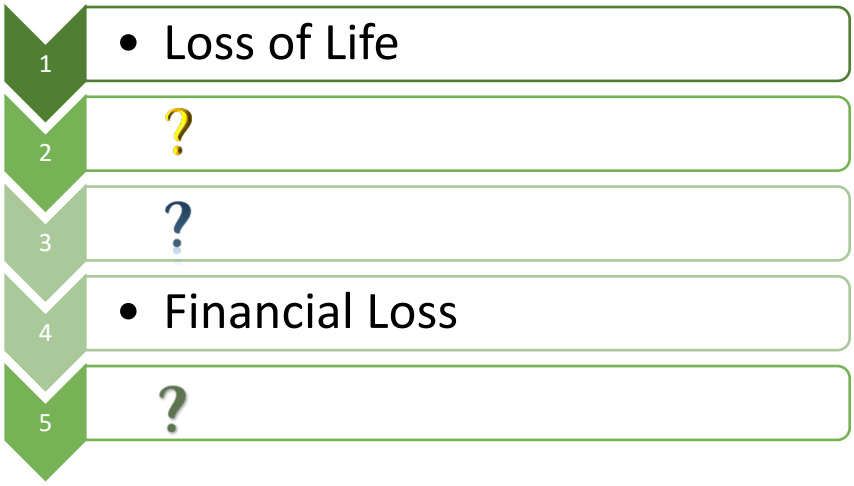
3. Identity Providers and Attestation



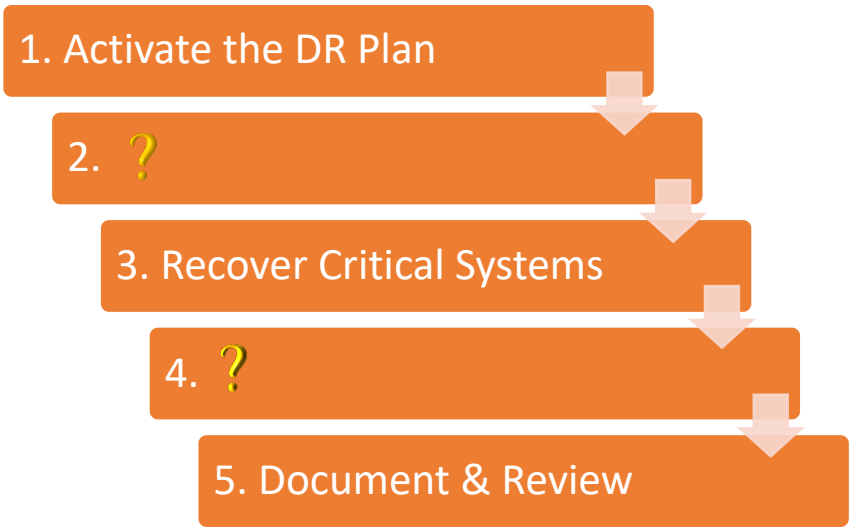
4. The Order of Volatility



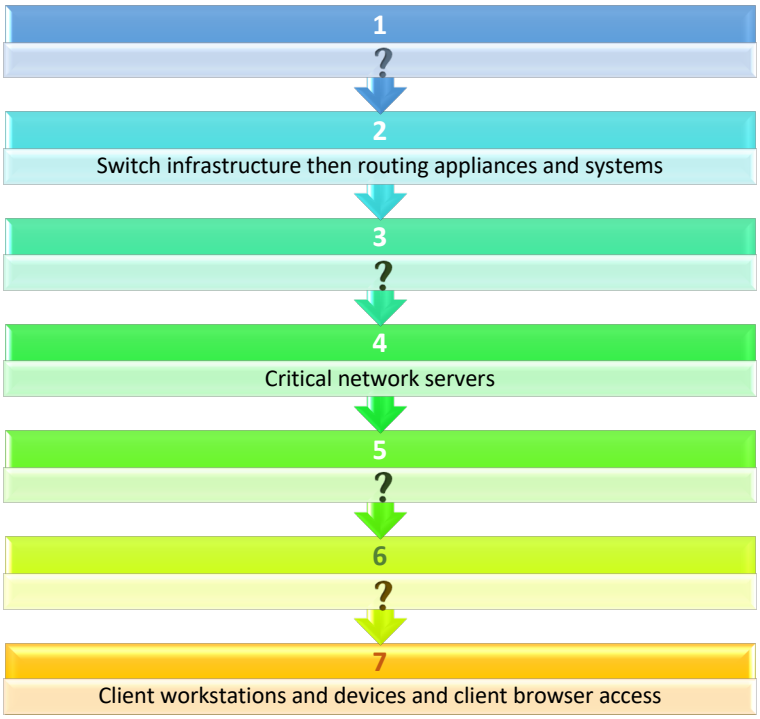
5. Evaluating Impact



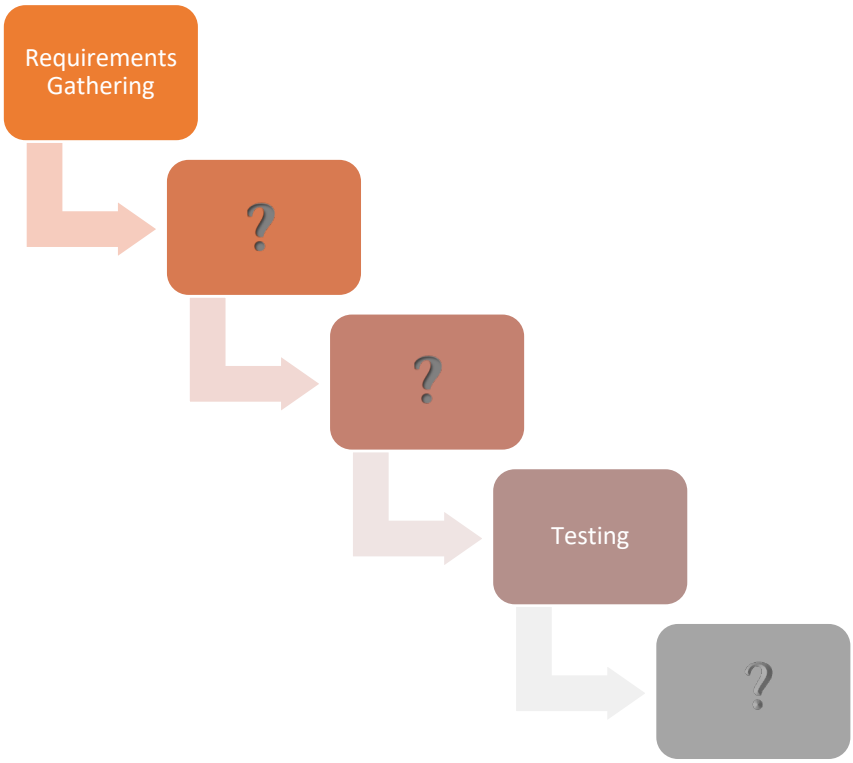
6. Disaster Recovery Plan Phases



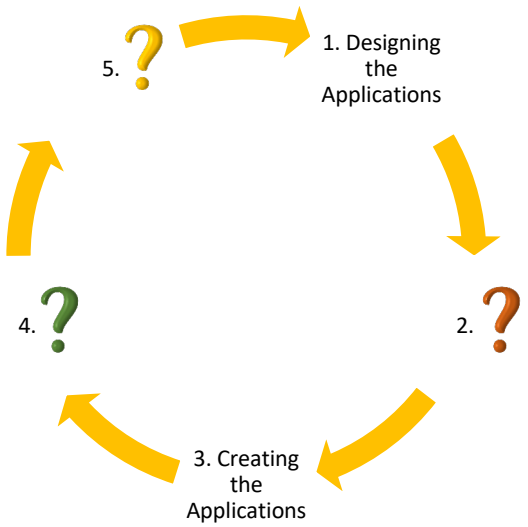
7. Order of Restoration



8. Waterfall Development Model

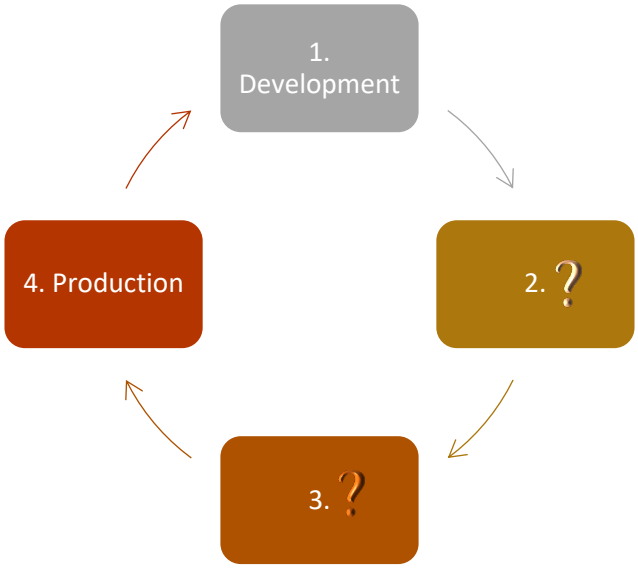


9. Application Provisioning

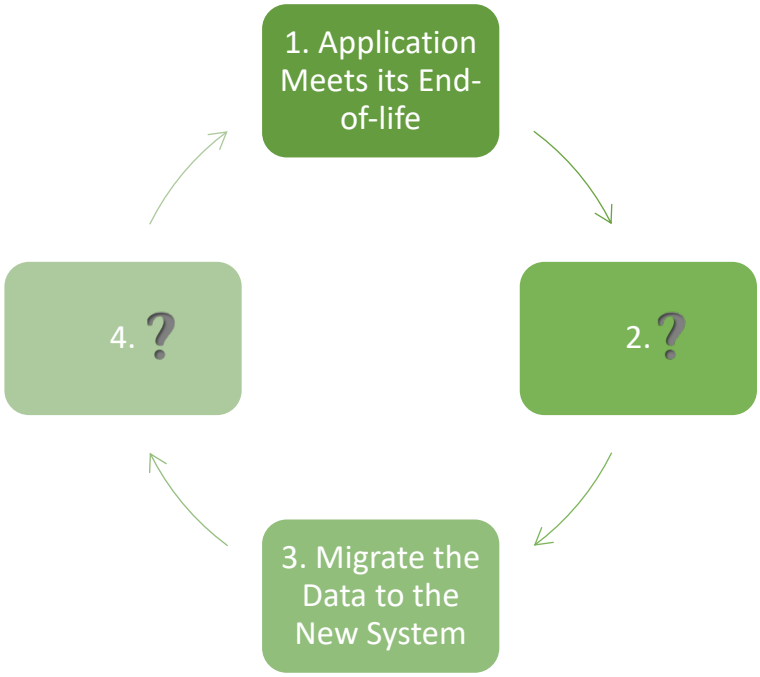


10. Incident Response

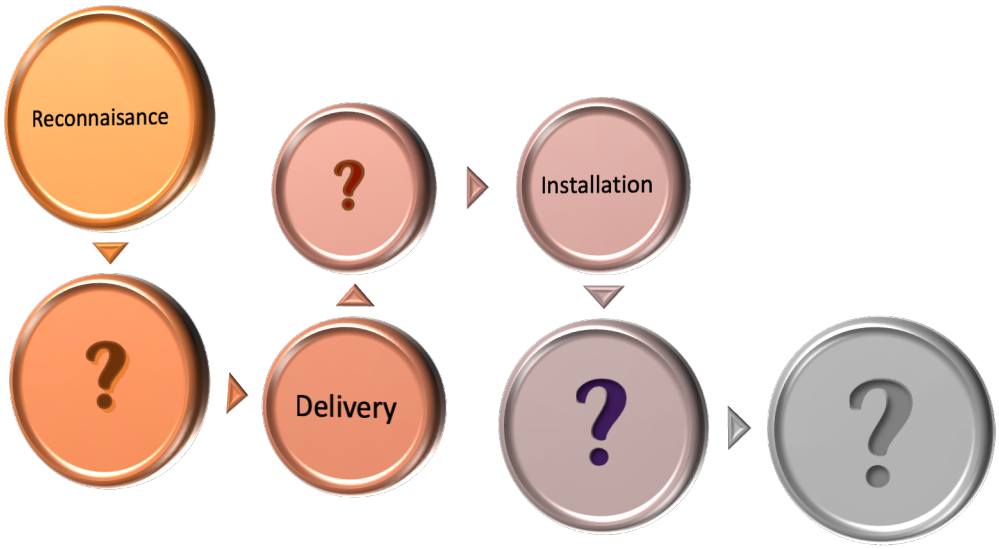
11. Secure Deployment (Secure Staging) Development Life Cycle



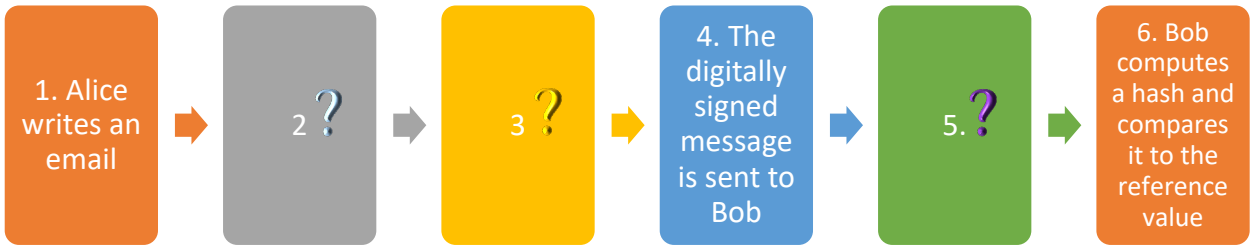
12. Application Deprovisioning



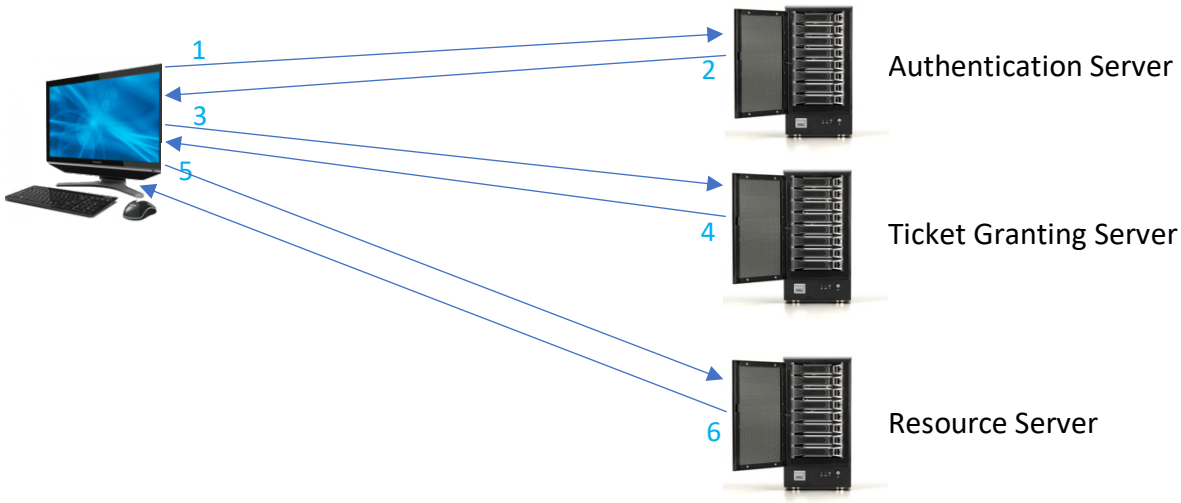
13. The Cyber Kill Chain. See if you can also identify what happens at each phase. Can you name a method of mitigation for each stage?



14. Digital Signature



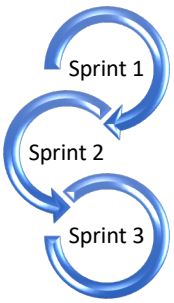
15. Kerberos: What steps are missing?

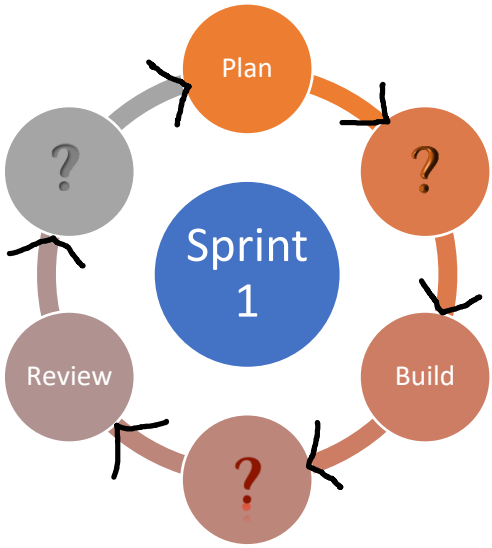


1	The user logs into a client workstation with a username and password and immediately requests a TGT from the AS.
2	?
3	Having the session key, the client sends three messages to the TGS to request access to a specific server: (1) the TGT, (2) an authenticator encrypted with the session key. (3) a plaintext message containing the name of a resource server and requested ticket lifetime.
4	?
5	The client decrypts the second message and uses the session key to create a new authenticator. It sends the authenticator and service ticket to the resource server.
6	?

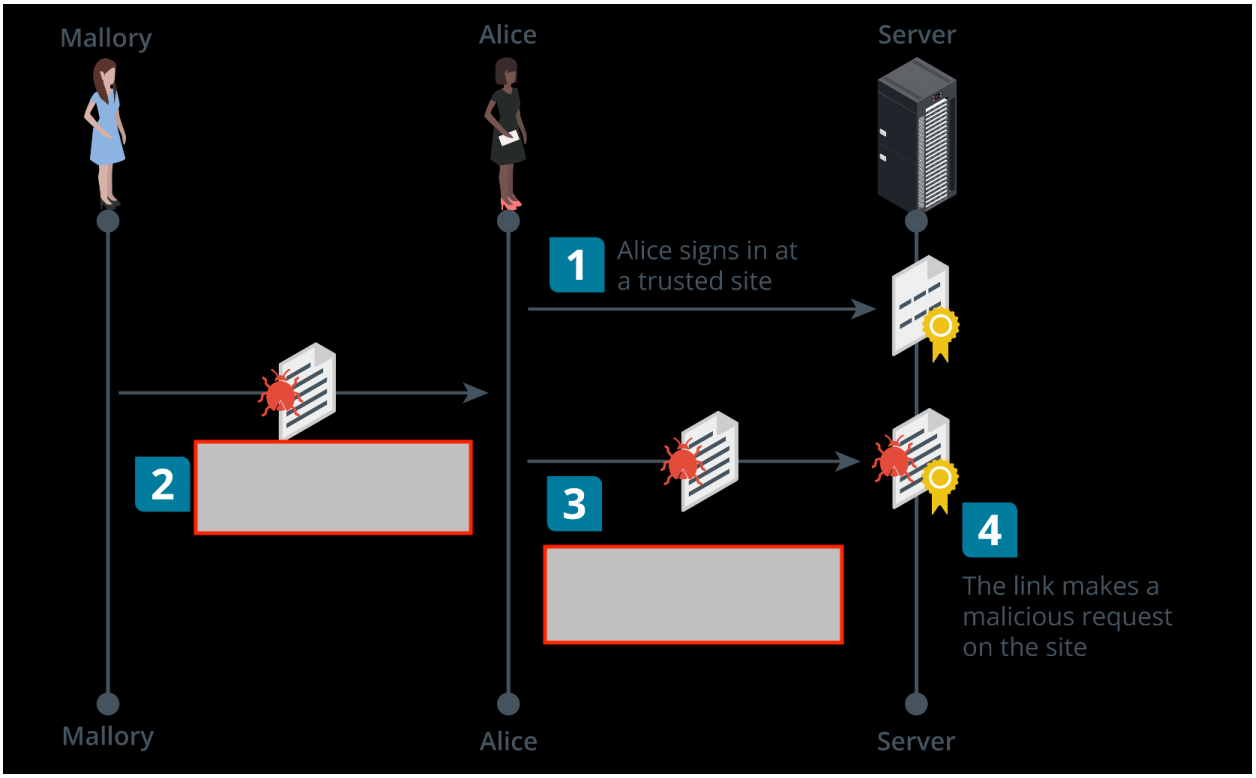
16. The Agile Software Development Life Cycle

Can you remember the life cycle of a Sprint? What happens in each stage?

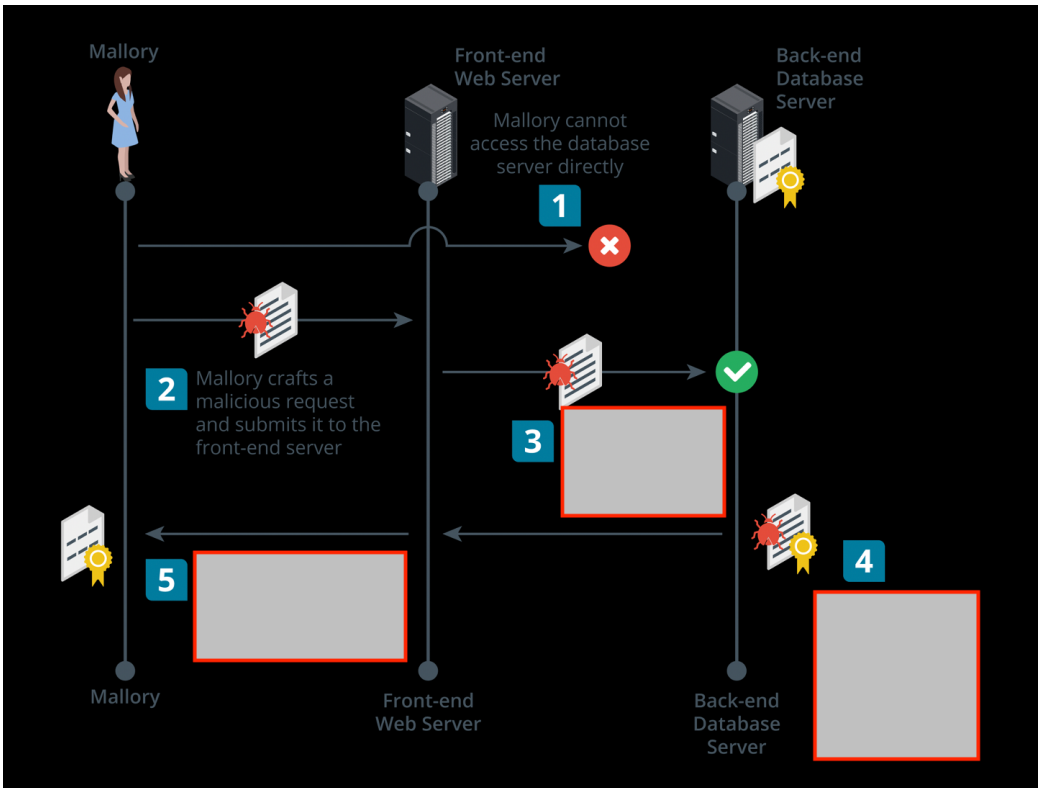




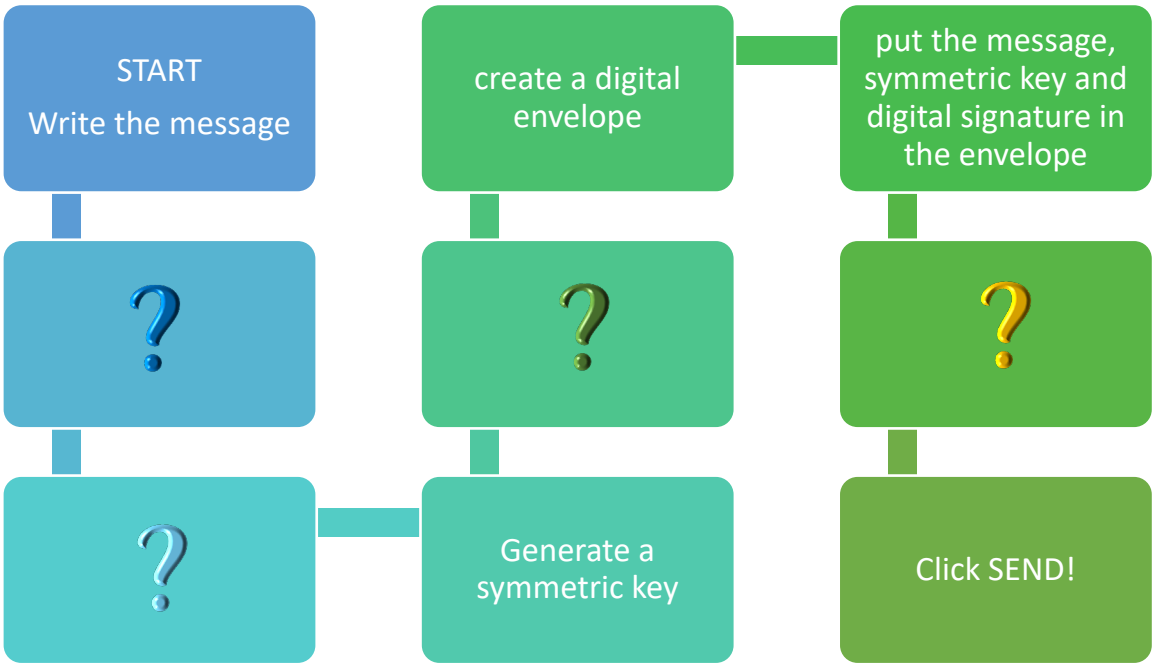
17. Cross-site Request Forgery: What two steps are missing?



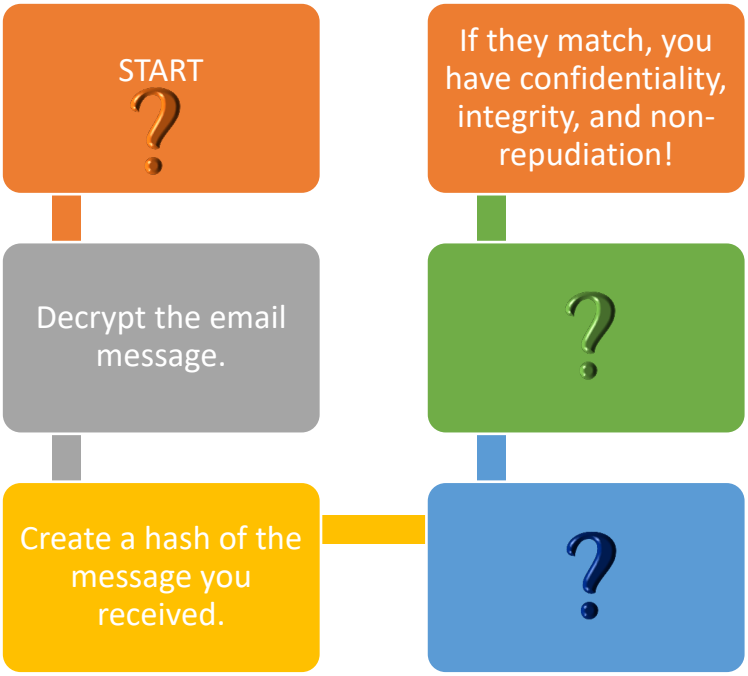
18. Server-side Request Forgery: What three steps are missing?



19. Want to send an encrypted digitally signed email?



20. What happens when you receive an encrypted digitally signed email? What happens first? And then?



21. What if I don't have a digital certificate!

1 Generate a public-private key pair

2 ?

3 ?

4 The CA will verify your ID and create and sign a digital certificate for you

5 ?

6 Now you can send encrypted, digitally signed email!

Can you decrypt these famous quotes?

1. “NAL ZNA JBEGU UVF FNYG JVYY FGVPX HC SBE JUNG UR ORYVRIRF EVTUG, OHG VG GNXRF Z FYVTUGYL ORGGRE ZNA GB NPXABJYRQTR VAFGNAGYL NAQ JVGUBHG ERFREINGVBA GUNG UR VF VA REEBE.”

   -NAQERJ WNPXFBA

2. GURER VF ABGUVAT ZBER PBEEHCGVAT, ABGUVAT ZBER QRFGEHPGVIR BS GUR ABOYRFG NAQ SVARFG SRRYVATF BS BHE ANGHER, GUNA GUR RKREPVFR BS HAYVZVGRQ CBJRE.”

   -JVYYVNZ URAEL UNEEVFBA

3. “VG VF UNEQ GB SNVY, OHG VG VF JBEFR ARIRE GB UNIR GEVRQ GB FHPPRRQ. VA GUVF YVSR, JR TRG ABGUVAT FNIR OL RSSBEG.”

   -GURBQBER EBBFRIRYG

4. “GUR BAYL GUVAT JR UNIR GB SRNE VF…SRNE VGFRYS.”

   -SENAXYVA Q. EBBFRIRYG

5. “N ZNA VF ABG SVAVFURQ JURA UR VF QRSRNGRQ. UR VF SVAVFURQ JURA UR DHVGF.”

   -EVPUNEQ AVKBA

6. “V QBA’G UNIR GB GRYY LBH UBJ SENTVYR GUVF CTRPVBHF GUVF TVSG BS SERRQBZ VF. RIREL GVZR JR URNE, JNGPU, BE ERNQ GUR ARJF, JR NER ERZVAQRQ GUNG YVOREGL VF N ENER PBZZBQVGL VA GUVF JBEYQ.”

   -EBANYQ ERNTNA

7. “JR BJR GUVF SERRQBZ BS PUBVPR NAQ NPGVBA GB GUBFR ZRA NAQ JBZRA VA HAVSBEZ JUB UNIR FREIRQ GUVF ANGVBA NAQ VGF VAGRERFGF VA GVZR BS ARRQ. VA CNEGVPHYNE, JR NER SBERIRE VAQROGRQ GB GUBFR JUB UNIR TVIRA GURVE YVIRF GUNG JR ZVTUG OR SERR,”

   - EBANYQ ERNTNA

8. N YRNQRE JUB QBRFA’G URFVGNGR ORSBER UR FRAQF UVF ANGVBA VAGB ONGGYR VE ABG SVG GB OR N YRNQRE.”

   -TBYQN ZRVE

9. “GEHFG LBHEFRYS. PERNGR GUR XVAQ BS FRYS GUNG LBH JVYY OR UNCCL GB YVIR JVGU NYY LBHE YVSR. ZNXR GUR ZBFG BS LBHEFRYS OL SNAAVAT GUR GVAL, VAARE FANEXF BS CBFFVOVYVGL VAGB SYNZRF BS NPUVRIRZRAG.”

-TBYQN ZRVE

These are a bit harder!

10. “QCTGT ZU VE SDQR NT DVSTGGWQT UE JDFC WU QCT SDQR EM XTZVL CWAAR.”

-GEXTGQ OEDZU UQTKTVUEV

11. “UHWC OCHOVC UYGQ VHRTCD AR GR KHPD YKGR HYKCDU FGR AR G MCCJ.”

-MAVVAGW SCGR KHMCVVU

12. “PVOTA QPT EQKT SMP CTMCOT UZM QPTX’N UJOOJXD NM EQWT VC NZTJP MUX.”

-LZVLW GTQDTP

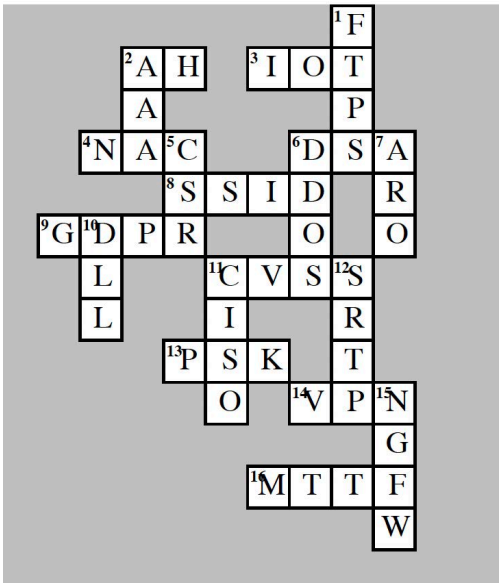
13. “CYRNFR QB ABG GNXR FRPHEVGL CYHF NTNVA.”*

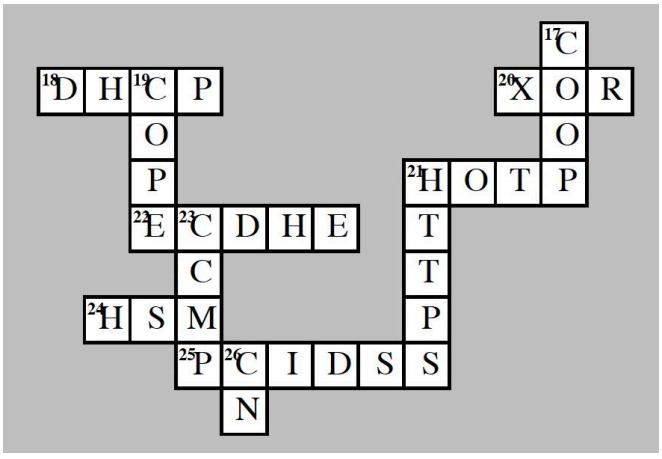
-ZF. FPUJNEGM

**The first letter of each word will help you remember the seven layers of the OSI model!*

Answer Keys

ACRONYMS 1
KEY



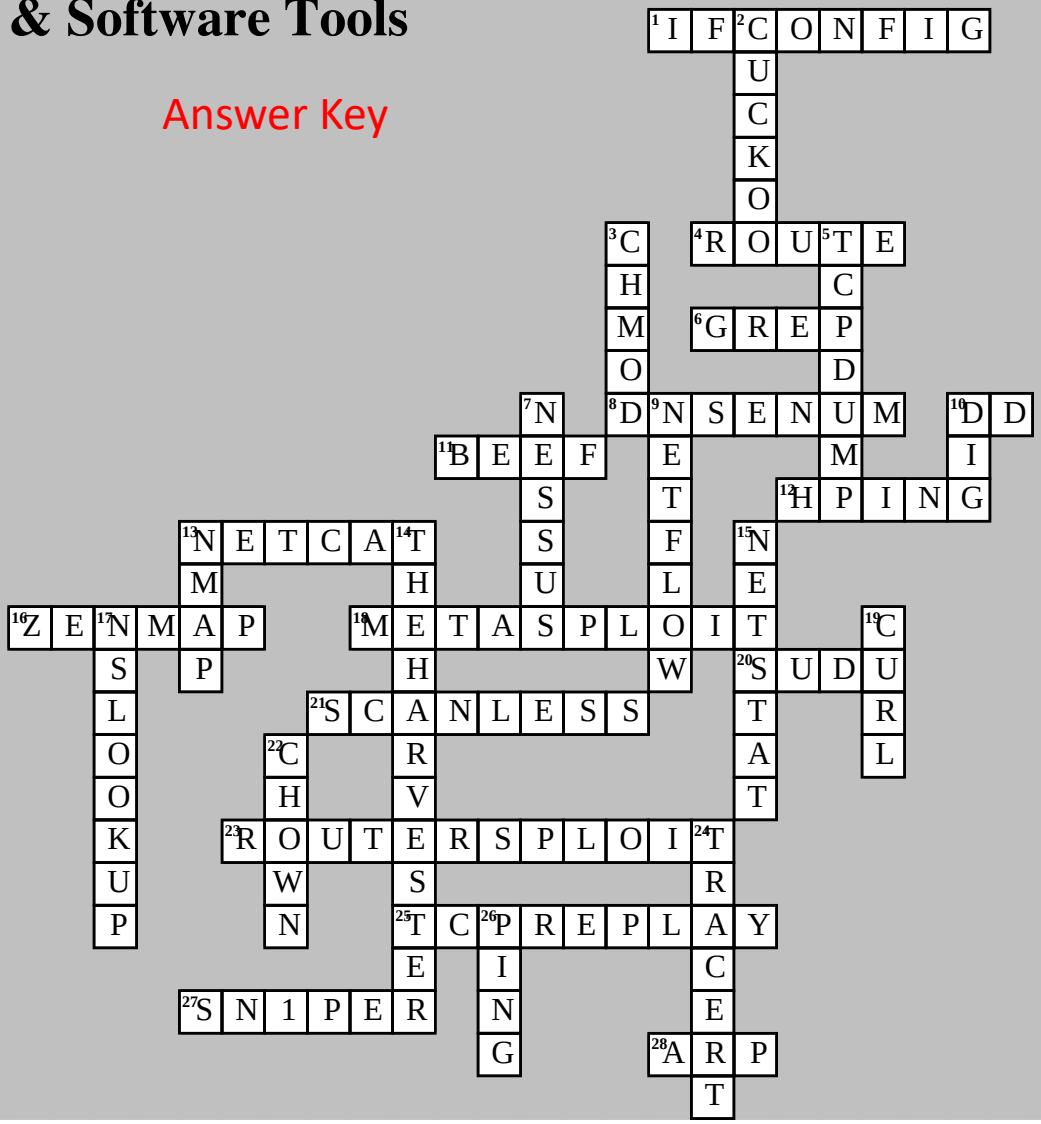


Answer Key

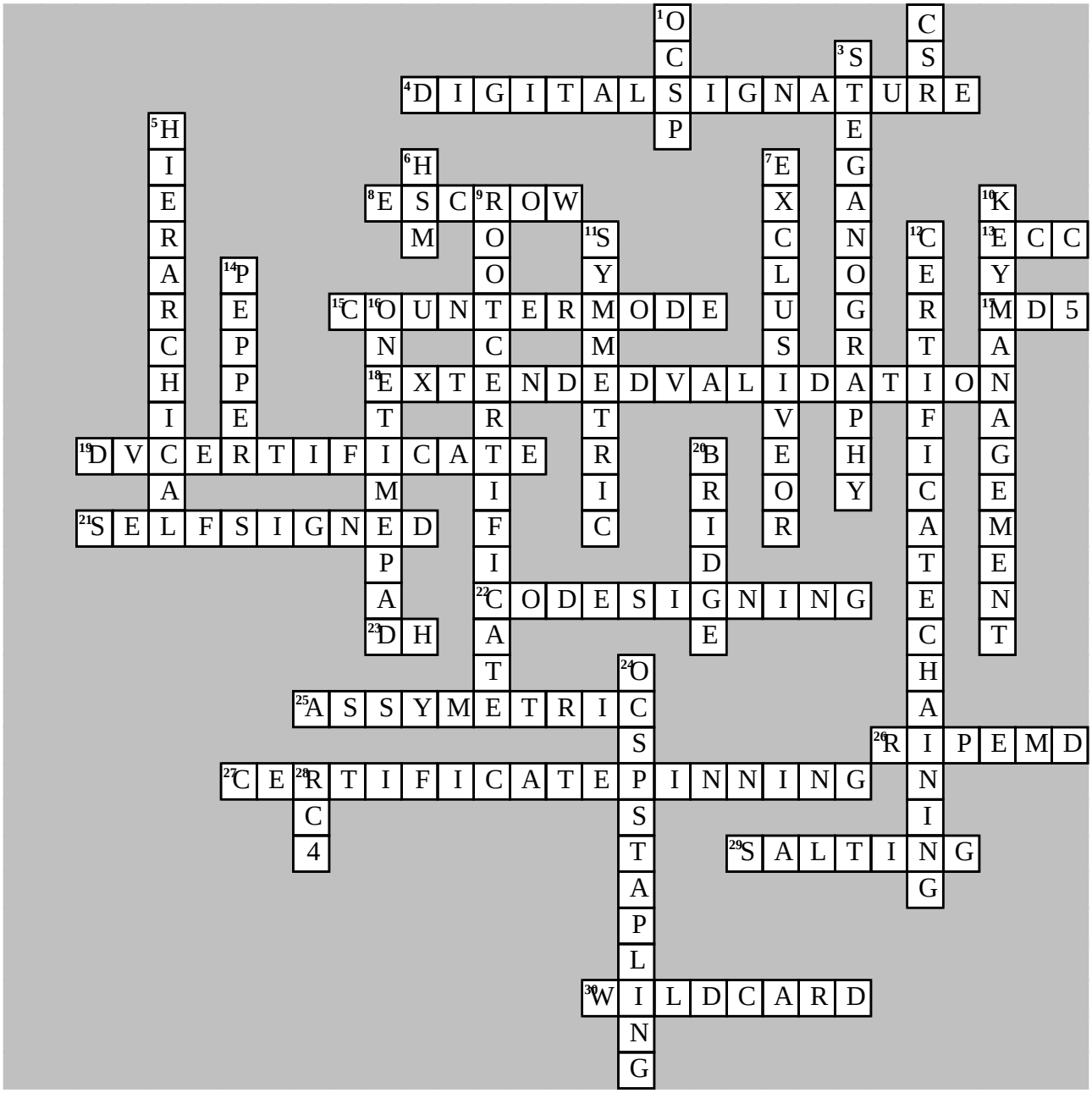
Acronyms 2

Command-line Commands & Software Tools

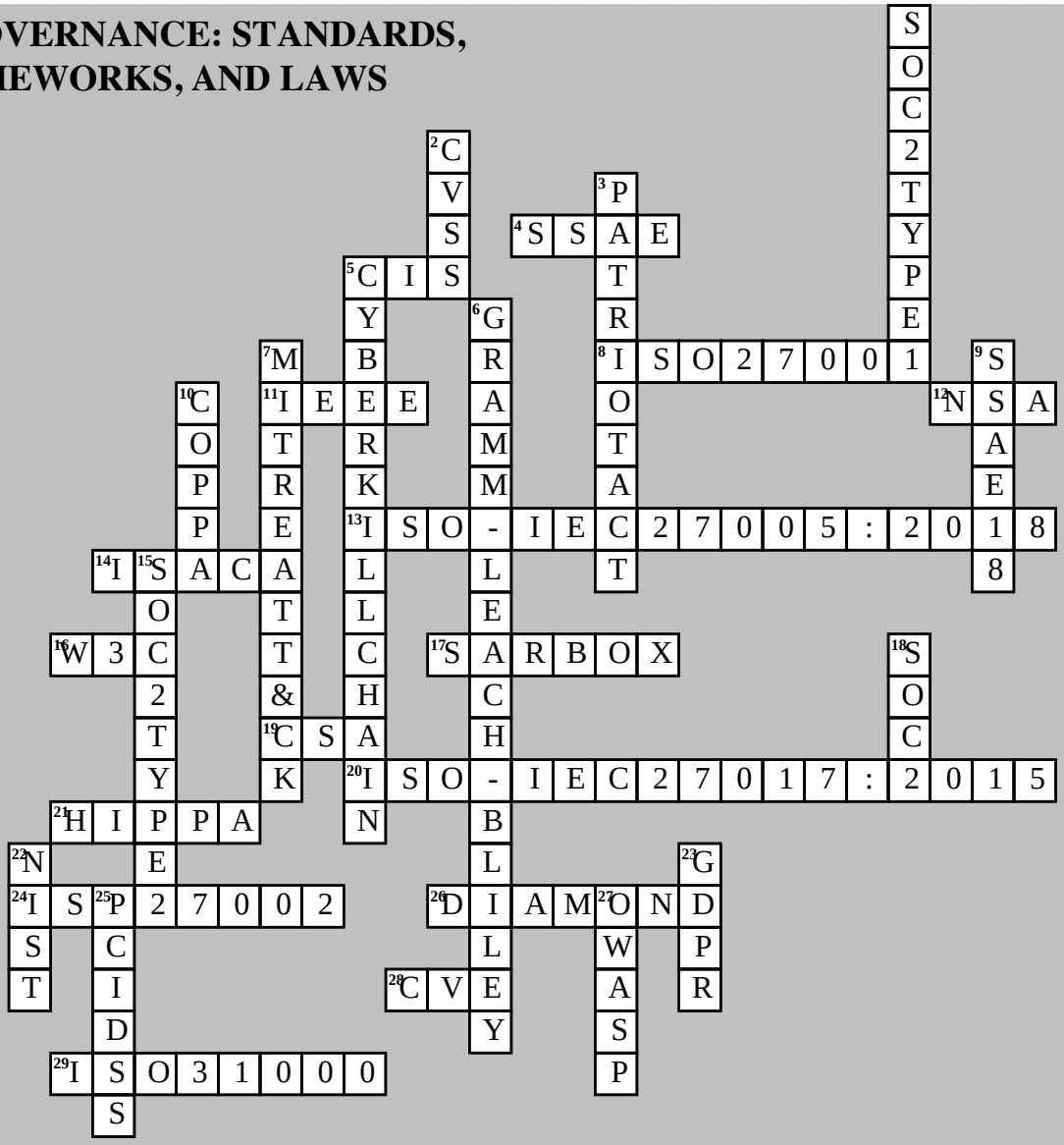
Answer Key

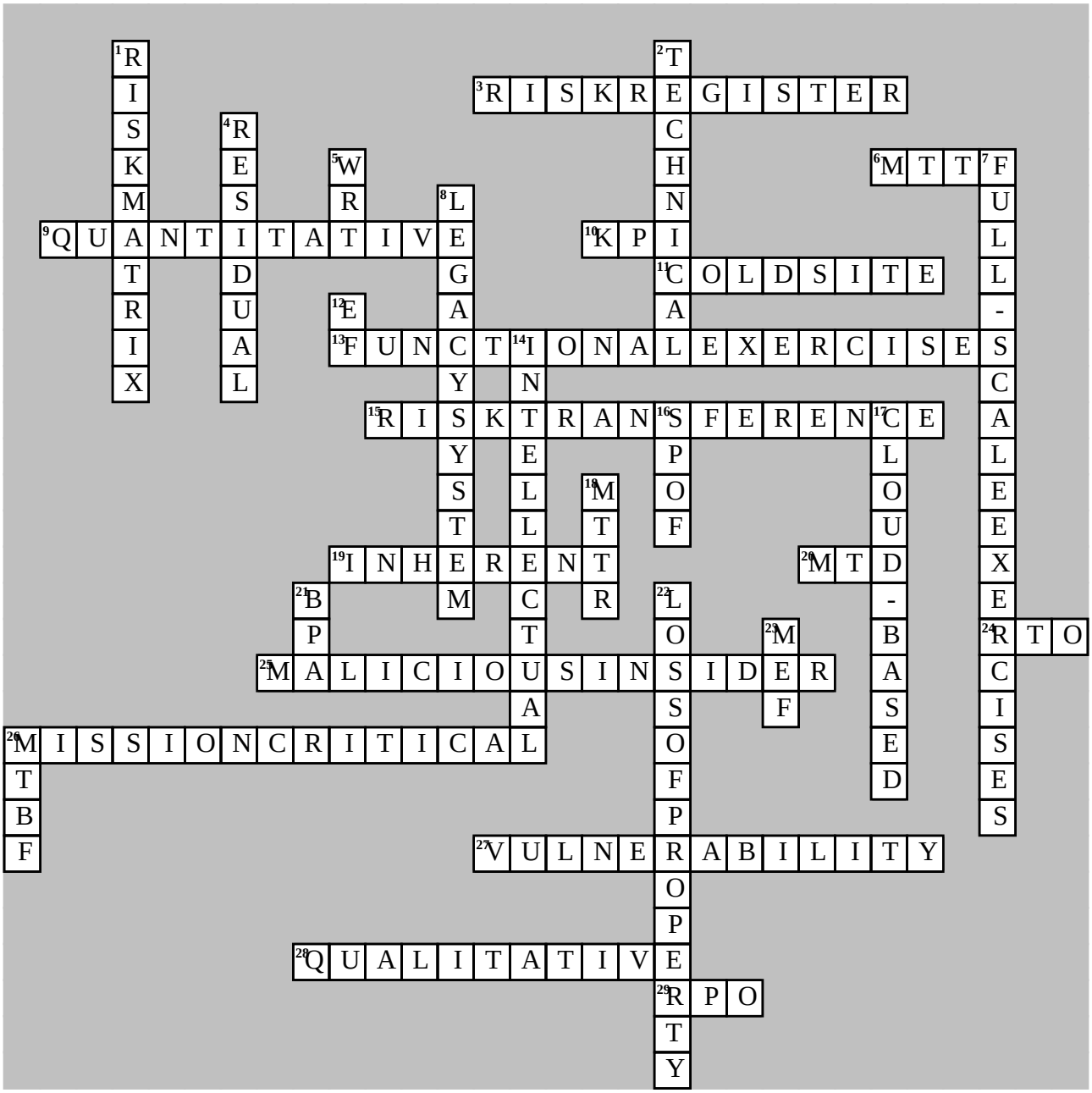


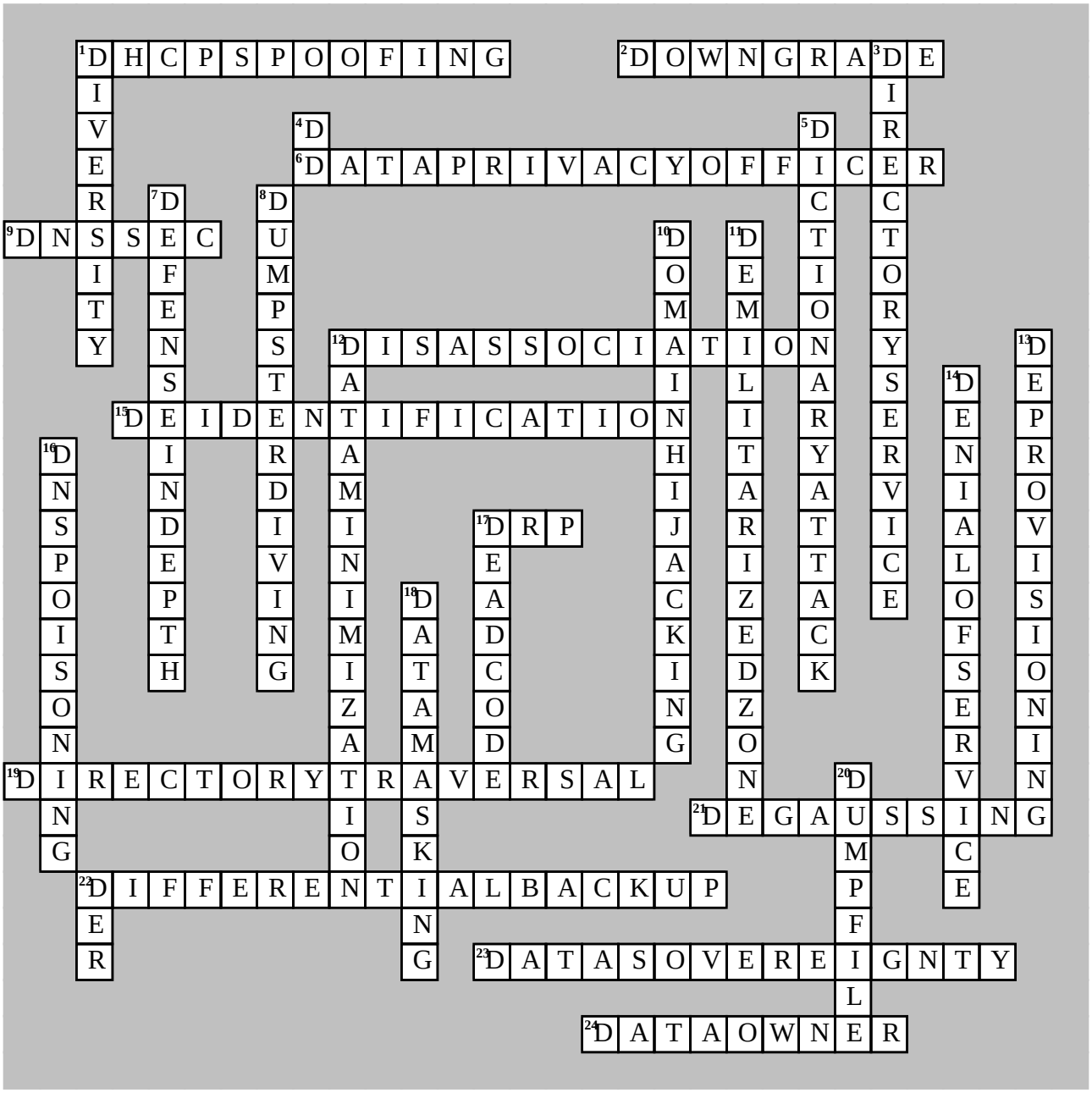
CRYPTOGRAPHY AND PKI KEY

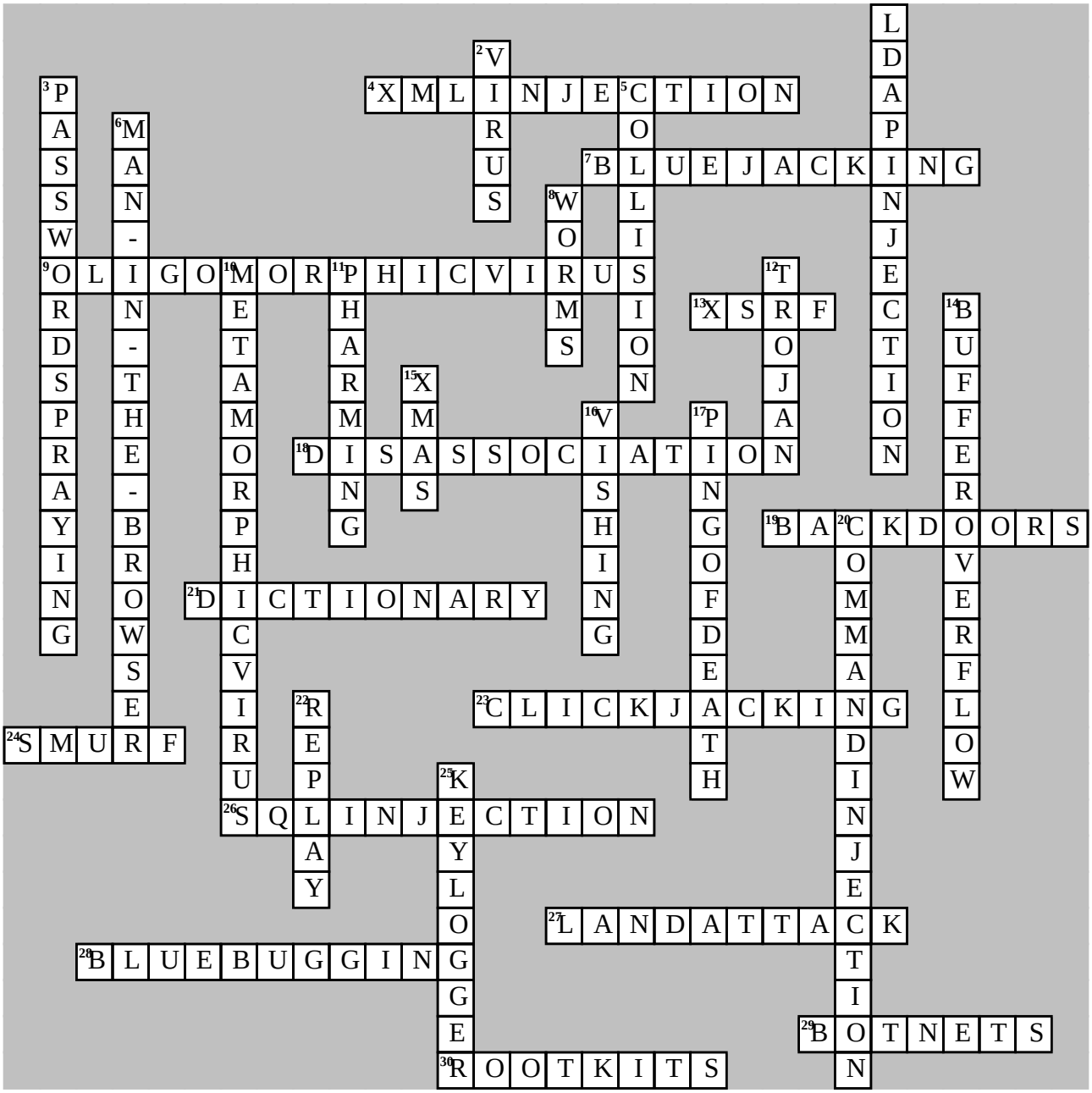


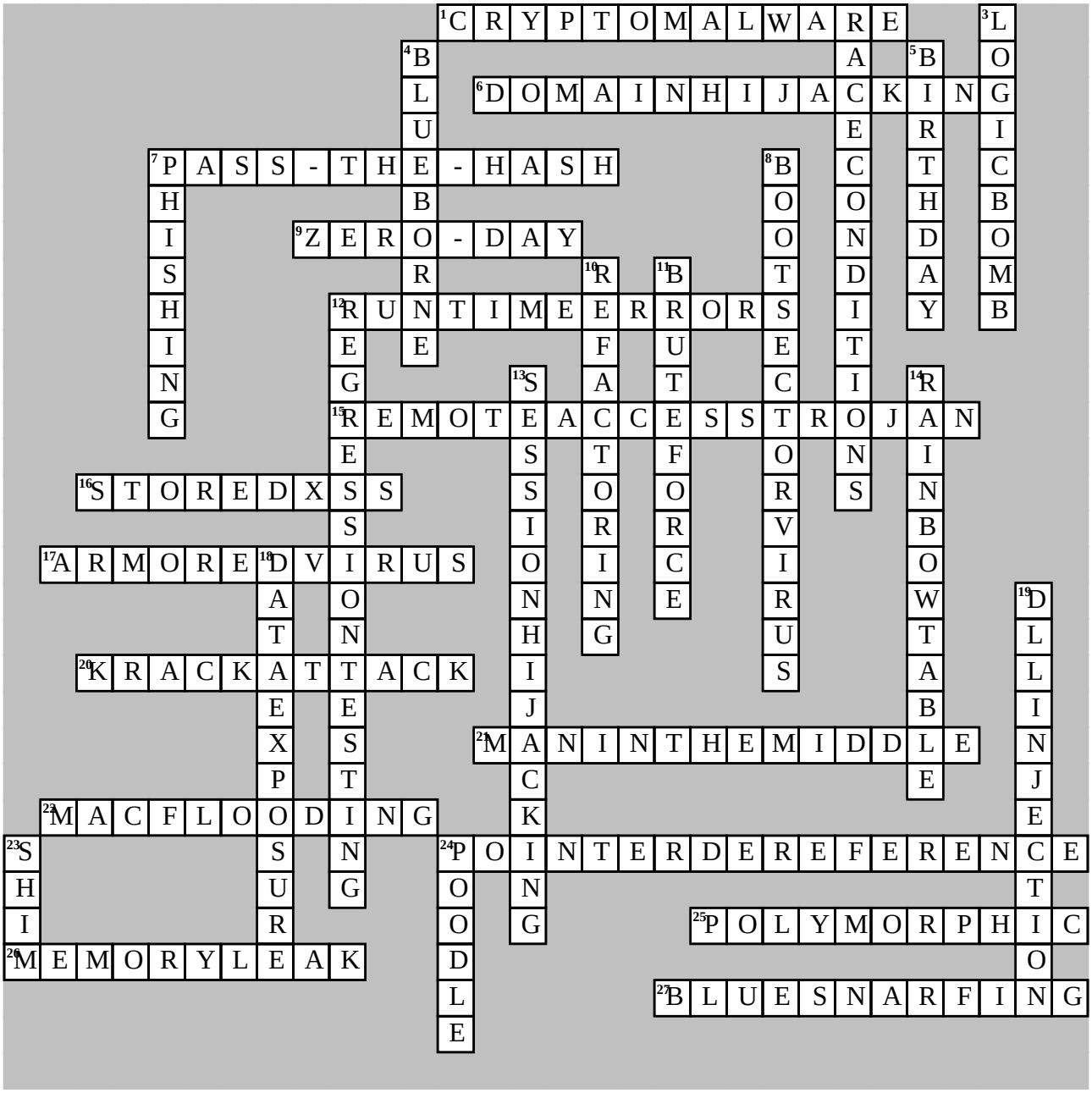
IT GOVERNANCE: STANDARDS, FRAMEWORKS, AND LAWS

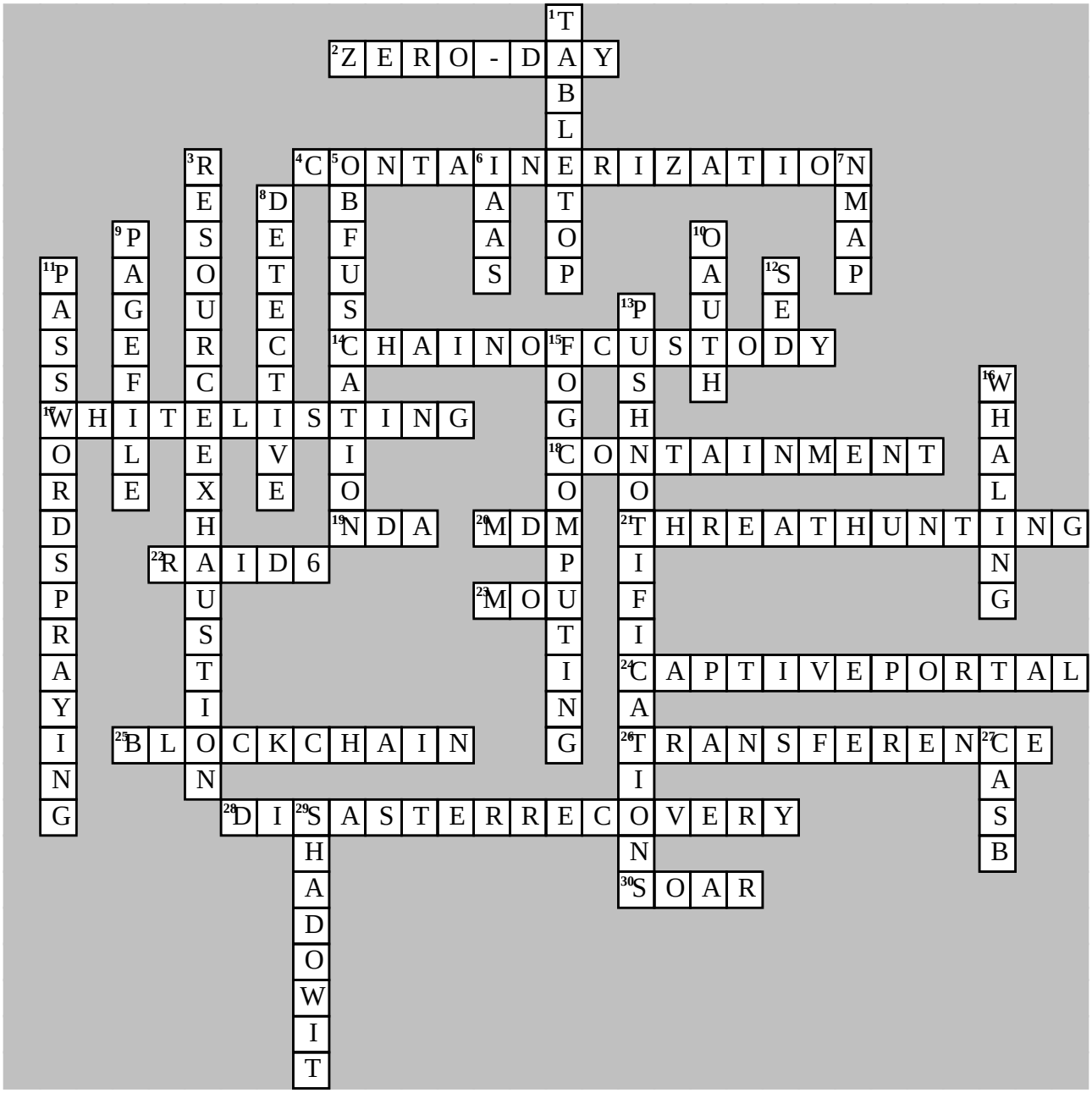


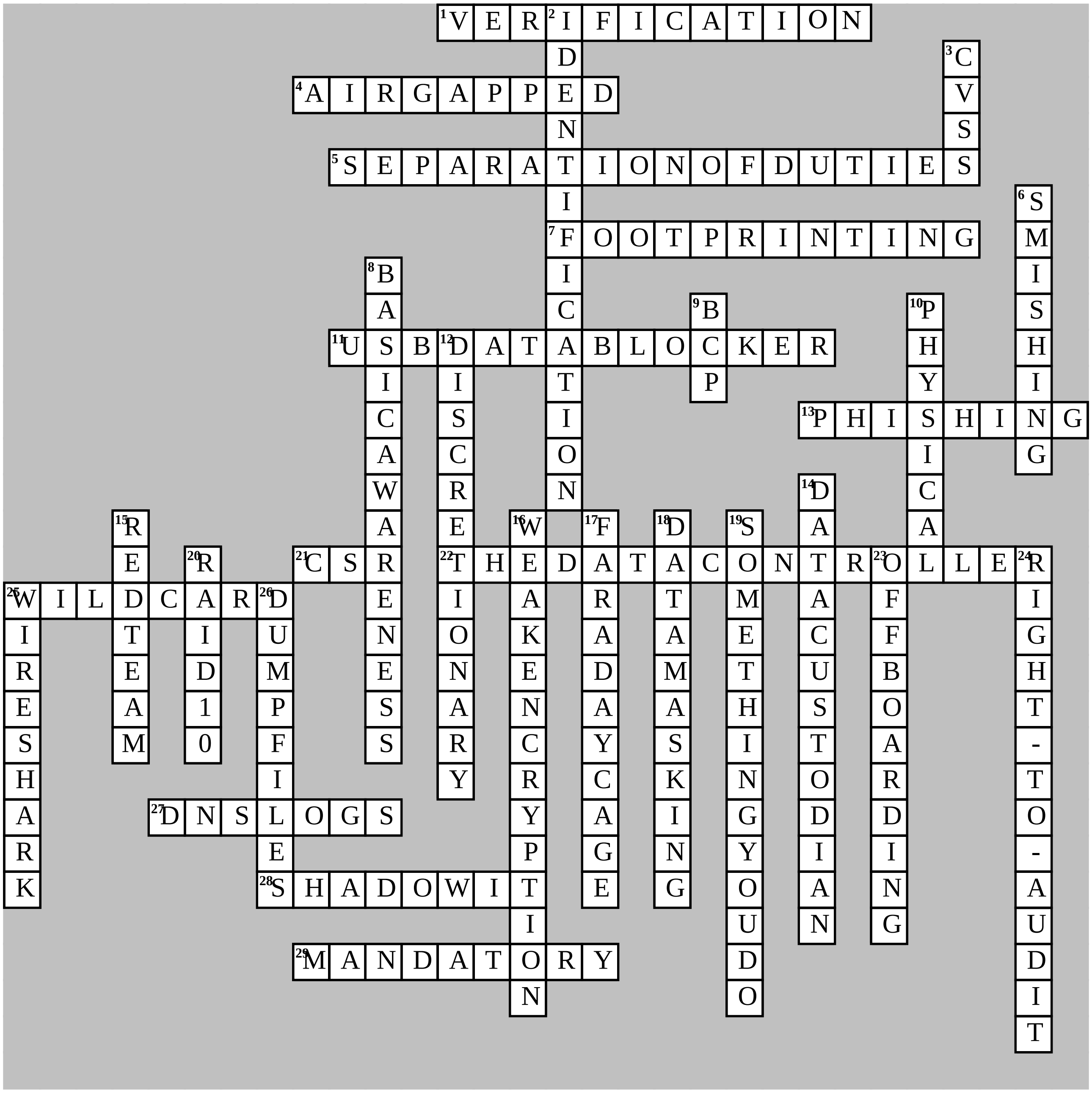

1 R I S K M
9 Q U A N T I T A T I V E
T R I X
4 R E S D U A L
5 W R
12 E
8 L A G Y
13 F U N C T 14 I O N A L E X E R C I S E S
15 R I S K T R A N S F E R E N C E
Y E S L T
19 I N H E R E N T
B M C R
P T
25 M A L I C I O U S I N S I D E R
A
26 M I S S I O N C R I T I C A L
T
B
F
2 T
3 R I S K R E G I S T E R
C
H
N
10 K P I
11 C O L D S I T E
A
16 S
P
O
F
22 L
O
S
O
F
P
27 V U L N E R A B I L I T Y
O
P
28 Q U A L I T A T I V E
29 R P O
T
Y
6 M T T 7 F
U
L
L
-
S
C
A
L
O
U
-
B
D
18 M
T
20 M T D
23 M
F
17 C E
L
O
U
X
E
24 R T O
A
S
E
D
E
S
S
I
S

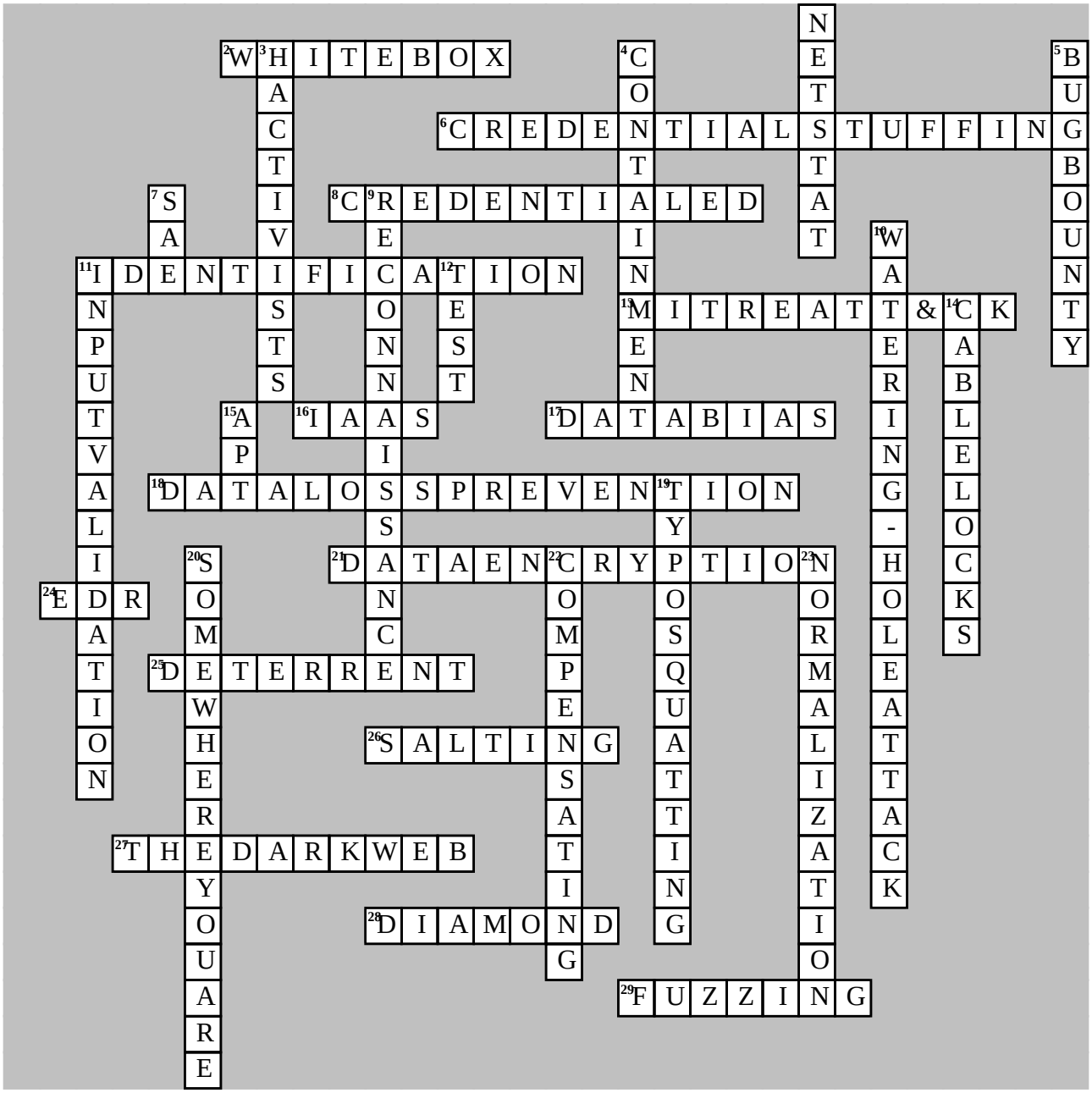

1 DHCPSPOOFING
2 DOWNGRADE
4 D
5 D
6 DATAPRIVACYOFFICER
7 D
8 D
9 DNSSEC
10 D
11 D
12 DISASSOCIATION
13 D
14 D
15 DEIDENTIFICATION
16 D
17 DRP
18 D
19 DIRECTORYTRAVERSAL
20 D
21 DEGAUSSING
22 DIFFERENTIALBACKUP
23 DATASOVEREIGNTY
24 DATAOWNER

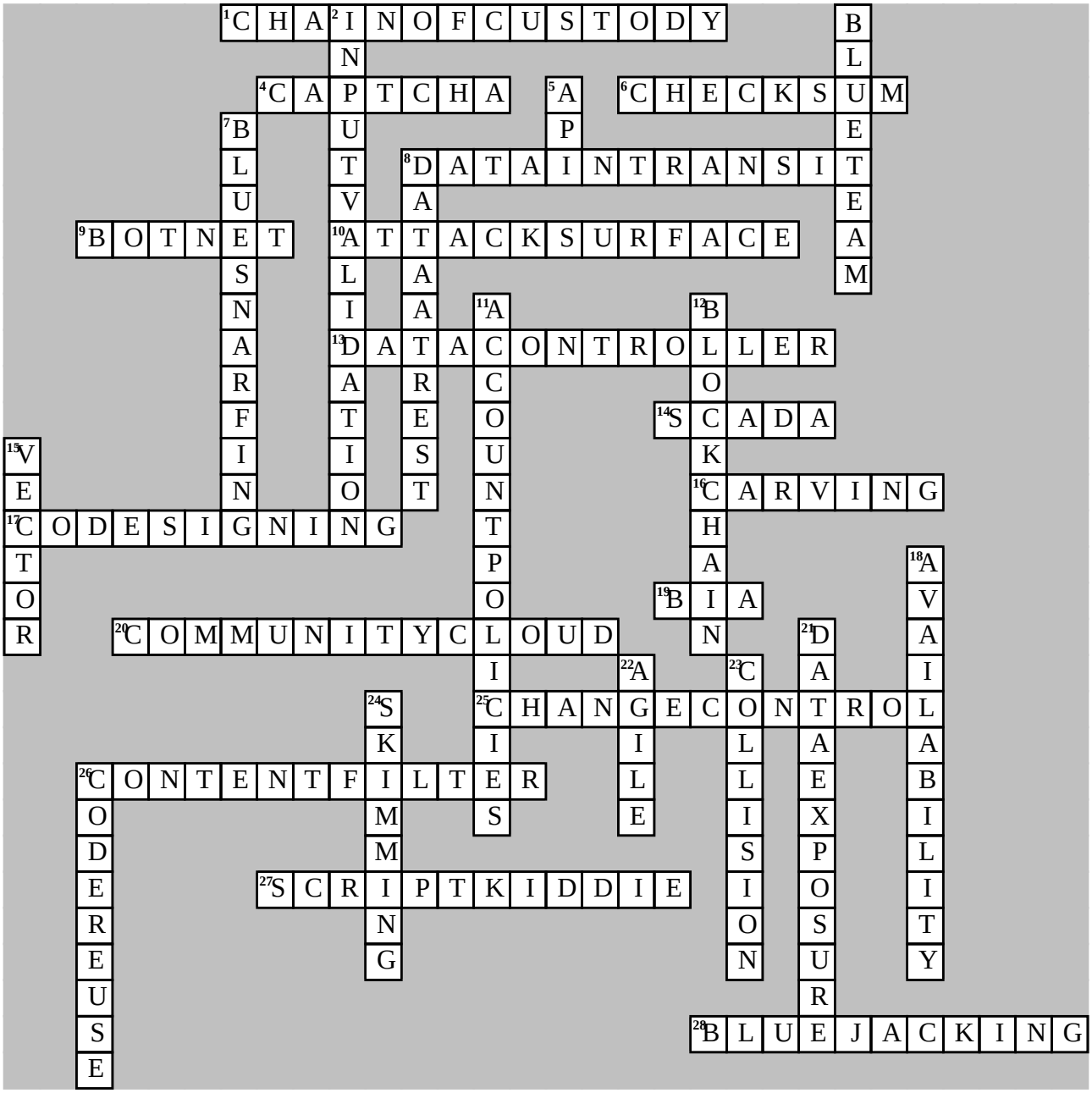

L
D
A
P
[2] V
[3] P
[4] X M L I N J E [5] C T I O N
A
R
O
[6] M
P
S
A
U
[7] B L U E J A C K I N G
S
N
S
[8] W
L
N
W
-
O
I
J
[9] O L I G O [10] M O R [11] P H I C V I R U S
[12] T
E
R
N
E
H
M
I
[13] X S R F
C
[14] B
D
-
T
A
S
O
O
T
U
S
T
A
R
[15] X
N
J
I
F
P
H
M
M
M
[16] V
[17] P
A
O
F
R
E
O
[18] D I S A S S O C I A T I O N
N
E
A
-
R
N
S
S
N
R
Y
B
P
G
H
G
[19] B A [20] C K D O O R S
I
R
H
I
O
O
V
N
O
[21] D I C T I O N A R Y
N
F
M
E
G
W
C
G
D
M
R
S
V
E
A
F
E
I
[22] R
[23] C L I C K J A C K I N G
L
[24] S M U R F
R
E
T
D
O
U
P
[25] K
H
I
W
[26] S Q L I N J E C T I O N
N
A
Y
J
Y
L
E
O
[27] L A N D A T T A C K
[28] B L U E B U G G I N G
T
G
I
E
[29] B O T N E T S
R O O T K I T S
N

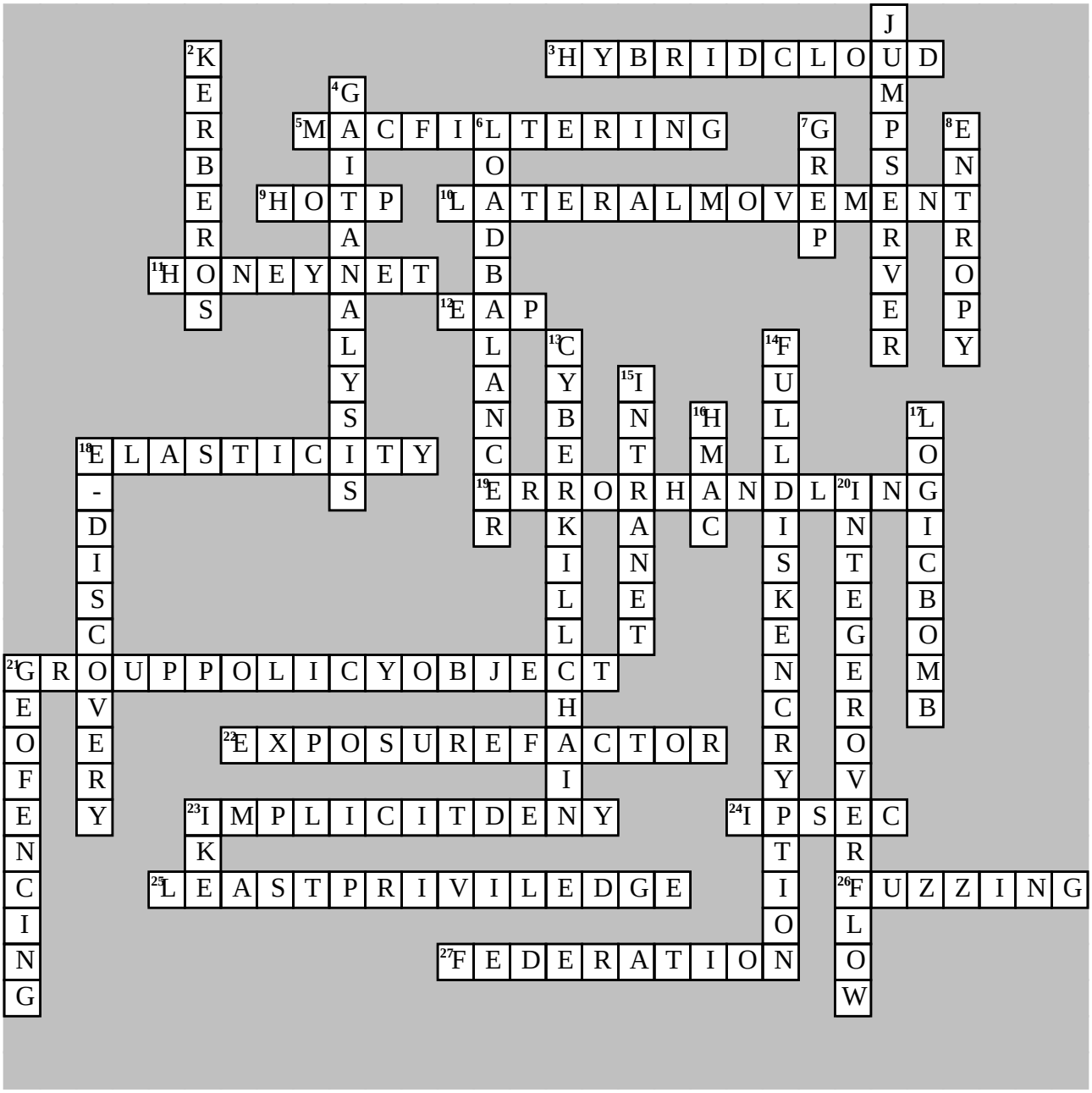

1 CRYPTOMALWARE
3 L
4 B
A
5 B
O
L
6 DOMAINHIJACKING
U
E
R
I
7 PASS-THE-HASH
8 B
C
T
C
H
B
O
O
H
B
I
9 ZERO-DAY
O
N
D
O
S
R
10 R
11 B
T
D
A
M
H
12 RUNTIMEERROR
S
I
Y
B
I
E
E
F
U
E
T
N
G
13 S
A
T
C
I
14 R
G
15 REMOTEACCESSTROJAN
E
S
T
F
O
N
I
16 STOREDXSS
S
O
O
R
S
N
S
I
R
R
V
B
17 ARMOREDVIRUS
18 D
O
I
C
I
O
A
O
N
N
E
R
W
19 D
T
N
H
G
U
T
L
20 KRACKATTACK
I
S
A
L
E
E
J
B
I
X
S
21 MANINTHEMIDDLE
N
P
T
C
E
J
22 MACFLOODING
K
E
23 S
S
N
24 POINTERDEREFERENCE
H
U
G
O
N
T
I
R
O
G
25 POLYMORPHIC
26 MEMORYLEAK
D
O
L
27 BLUESNARFING
E

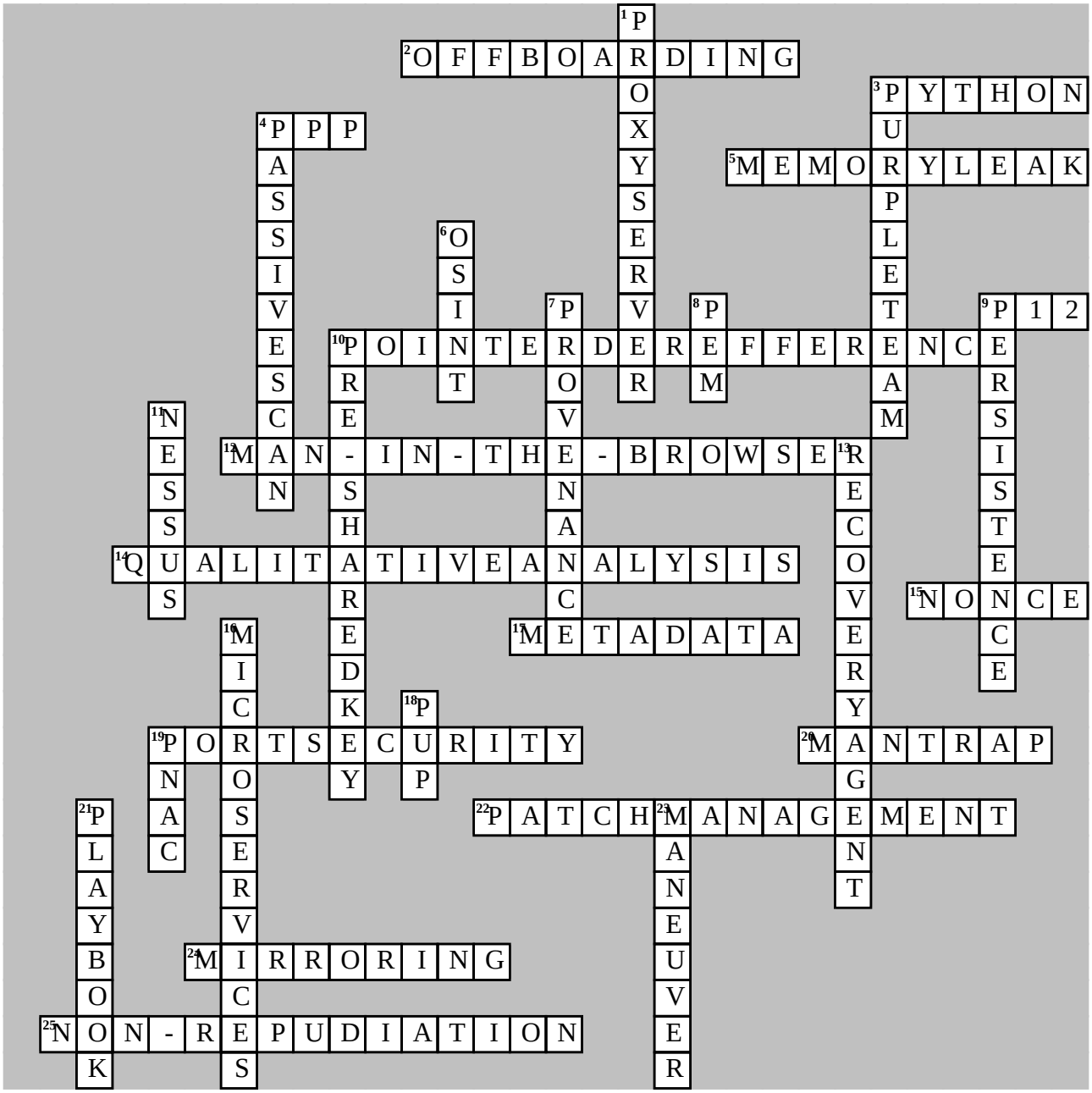

1 T
2 ZERO-DAY
B
L
3 R
4 C 5 O N T A 6 I N E R I Z A T I O 7 N
E
8 D B A T M
9 P S E F A O 10 O A
11 P A O T U S P A 12 S P
A G U E S 13 P U E
S E R C 14 C H A I N O 15 F C U S T O D Y
S F C T A O S H 16 W
17 W H I T E L I S T I N G G H H
O L E V I 18 C O N T A I N M E N T A
R E X E O O O L
D H 19 N D A 20 M D M 21 T H R E A T H U N T I N G
S 22 R A I D 6 P I N
P U 23 M O U F G
R S T I
A T I 24 C A P T I V E P O R T A L
Y I N A
I 25 B L O C K C H A I N G 26 T R A N S F E R E N 27 C E
N N I A
G 28 D I 29 S A S T E R R E C O V E R Y S
H N B
A 30 S O A R
D
O
W
I
T

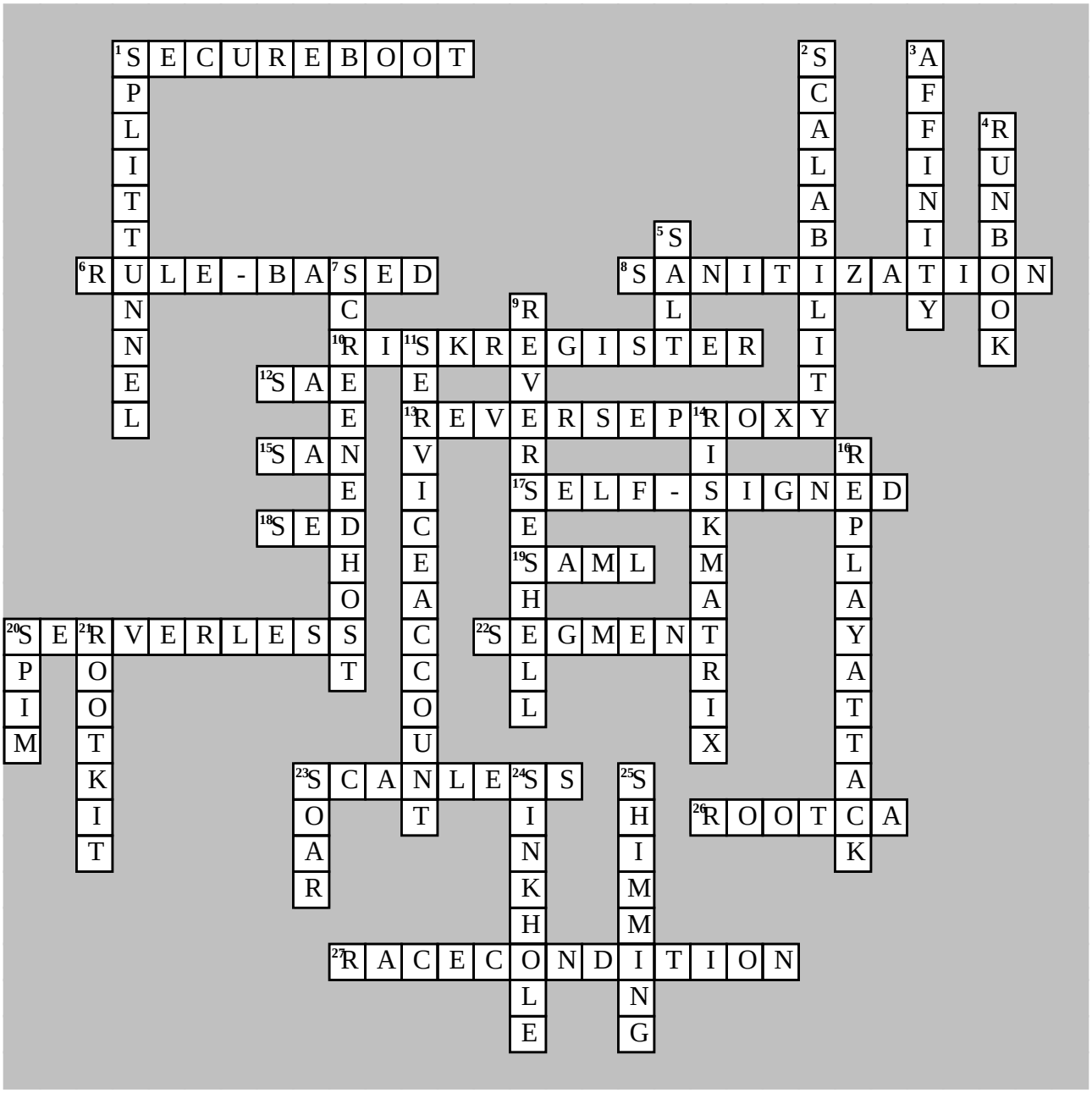

1 VERIFICATION
2 IDENTIFICATION
3 CVSS
4 AIRGAPPED
5 SEPARATIONOFDUTIES
6 SMISHING
7 FOOTPRINTING
8 BASICAWARENESS
9 BCP
10 PHYSICAL
11 USBDATABLOCKER
12 DISCRETIONARY
13 PHISHING
14 DATACUSTODIAN
15 REDTEAM
16 WEAKENCRYPTION
17 FARADAYCAGE
18 DATAMASKING
19 SOMETHINGYOUDO
20 RAID10
21 CSR
22 THEDATACONTROLLER
23 OFFBOARDING
24 RIGHT-TO-AUDIT
25 WIRESHARK
26 DUMPFILE
27 DNSLOGS
28 SHADOWIT
29 MANDATORY


WHITEBOX
CREDENTIALSTUFFING
CREDENTIALED
IDENTIFICATION
MITREATT&CK
WATERBOARDING
DATABIAS
DATALOSSPREVENTION
DATAENCRYPTION
SOMETHINGERRENT
SALTING
THEDARKWEB
DIAMOND
FUZZING


1 CHA 2 INOFCUSTODY
BL
N
4 CAPTCHA 5 A 6 CHECKSUM
7 BUP E
LT 8 DATAINTRANSIT
UV A E
9 BOTNET 10 ATTACKSURFACE A
SL A M
NI A 11 A 12 B
A 13 DATACONTROLLER
RA RC O
FT EO 14 SCADA
15 V II SU K
E NO TN 16 CARVING
17 CODESIGNING T H
T P A 18 A
O O 19 BIA V
R 20 COMMUNITYCLOUD N 21 D A
I 22 A 23 C A I
24 S 25 CHANGECONTROL
K I I L A A
26 CONTENTFILTER L L E B
O M S E I X I
D M S P L
E 27 SCRIPTKIDDIE I O I
R N O S T
E G N U Y
U R
S 28 BLUEJACKING
E


2 KEBERBERS
3 HYBRIDCLOUD
4 GAIA
5 MACFI
6 LTERING
7 GROW
8 ENTER
9 HOTP
10 LATERALMOVEMENT
11 HONEYNET
12 EAP
13 CLANDESTINE
14 FULL
15 INHERENT
16 HACK
17 LOCKBOX
18 ELASTICITY
19 ERRORHANDLING
20 INSIDE
21 GROUPPOLICYOBJECT
22 EXPOSUREFACTOR
23 IMPLICITDENY
24 IPSEC
25 LEASTPRIVILEDGE
26 FUZZING
27 FEDERATION


1 P
2 OFFBOARDING
OXYSSERVER
3 PYTHON
UPLET
4 PPP
ASSIVE
5 MEMORYLEAK
6 OSI
7 P
8 P
9 P12
10 POINTERDEREFFERENCE
TORMAR
11 NESSS
CEVMS
12 MAN-IN-THE-BROWSER
NSNESI
HACT
14 QUALITATIVEANALYSIS
OE
SRC
15 NONCE
16 MEMETADATA
IDEC
CKP
RY
19 PORTSECURITY
20 MANTRAP
NOYPG
21 PACS
22 PATCH
23 MANAGEMENT
LCEAN
AERNT
YVEU
BMIRRORING
OCV
25 NON-REPUDIATION
KSR


1 SECUREBOOT
2 SCALABLE
3 AFFINITY
4 RUNNIBOK
5 SLIP
6 RULE-BASED
7 SCRIPTKIDDIE
8 SANITIZATION
9 REVERSEPROXY
10 RISKREGISTER
11 SECVECTOR
12 SAFE
13 REVERSEPROXY
14 IMAP
15 SANE
16 RAPPLICATION
17 SELF-SIGNED
18 SEDHEAD
19 SAML
20 SERVERLESS
21 ROOTKIT
22 SEGMENT
23 SCANLOAR
24 SSHKEY
25 SHIM
26 ROOTCAK
27 RACECONDITION

Curvy Words

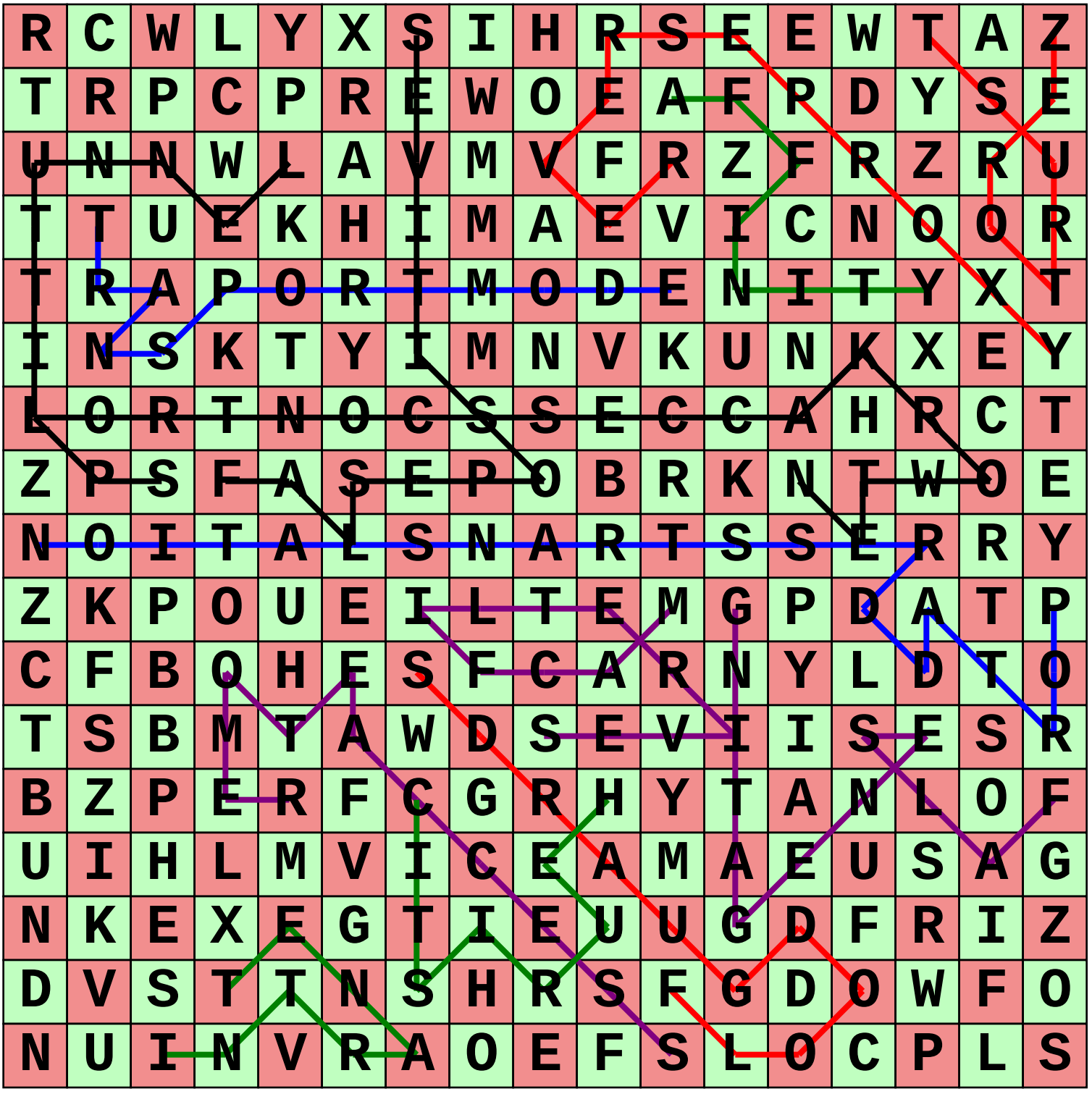
Network Architecture

KEY

Curvy Words: Network Architecture: CLUES: KEY

1. This is the process of spanning a single VLAN across multiple switches. (TRUNKING)
2. A deviation from an expected pattern or behavior. (ANOMALY)
3. This can be hardware, software, or a combination of both whose purpose is to enforce a set of network security policies across network connections. (FIREWALL)
4. This is where you have configured the network devices to limit traffic access across different parts of a network. (NETWORK SEGMENTATION)
5. This allows multiple systems to be reflected back as a single IP address. (VIRTUAL IP)
6. This is a passive signal-copying mechanism installed between two points on the network. (NETWORK TAP)
7. Provides the system information as to what objects are permitted which actions. (ACCESS CONTROL LIST)
8. The use of specific technologies on a network to guarantee its ability to manage traffic based on a variety of indicators. (QUALITY OF SERVICE)
9. This is an example of a segment, one that is accessible from the Internet, and from the internal network, but cannot be crossed directly. (SCREENED SUBNET)
10. These are sensors, or concentrators that combine multiple sensor that collect data for processing by other systems. (COLLECTORS)
11. Communication links that are network connections to two or more networks across an intermediary network layer. (SITE-TO-SITE)
12. These management channels are physically separate connections, via separate interfaces that permit the active management of a device even when the data channel is blocked for some reason. (OUT-OF-BAND)
13. This is a hardened system on a network specifically used to access devices in a separate security zone. (JUMP SERVER)
14. This can be used to filter out undesirable traffic and prevent employees from accessing potentially hostile websites. (PROXY SERVER)
15. This is an extension of a selected portion of a company's intranet to external partners. This allows a business to share information with customers, suppliers, partners, and other trusted groups while using a common set of Internet protocols to facilitate operations. (EXTRANET)
16. In these management systems, the management channel is the same channel as the data channel. (IN BAND)
17. A set of protocols developed by the IETF to securely exchange packets at the network layer (layer 3) of the OSI reference model. (IPSEC)
18. In this mode, the security of packet traffic is provided between endpoint node machines in each network and not at the terminal host machines. TUNNEL MODE
19. A device that takes multiple inputs and combines them to a single output. (AGGREGATOR)
20. Involves sending each new request to the next server in rotation. (ROUND ROBIN)

Curvy Words 2 KEY



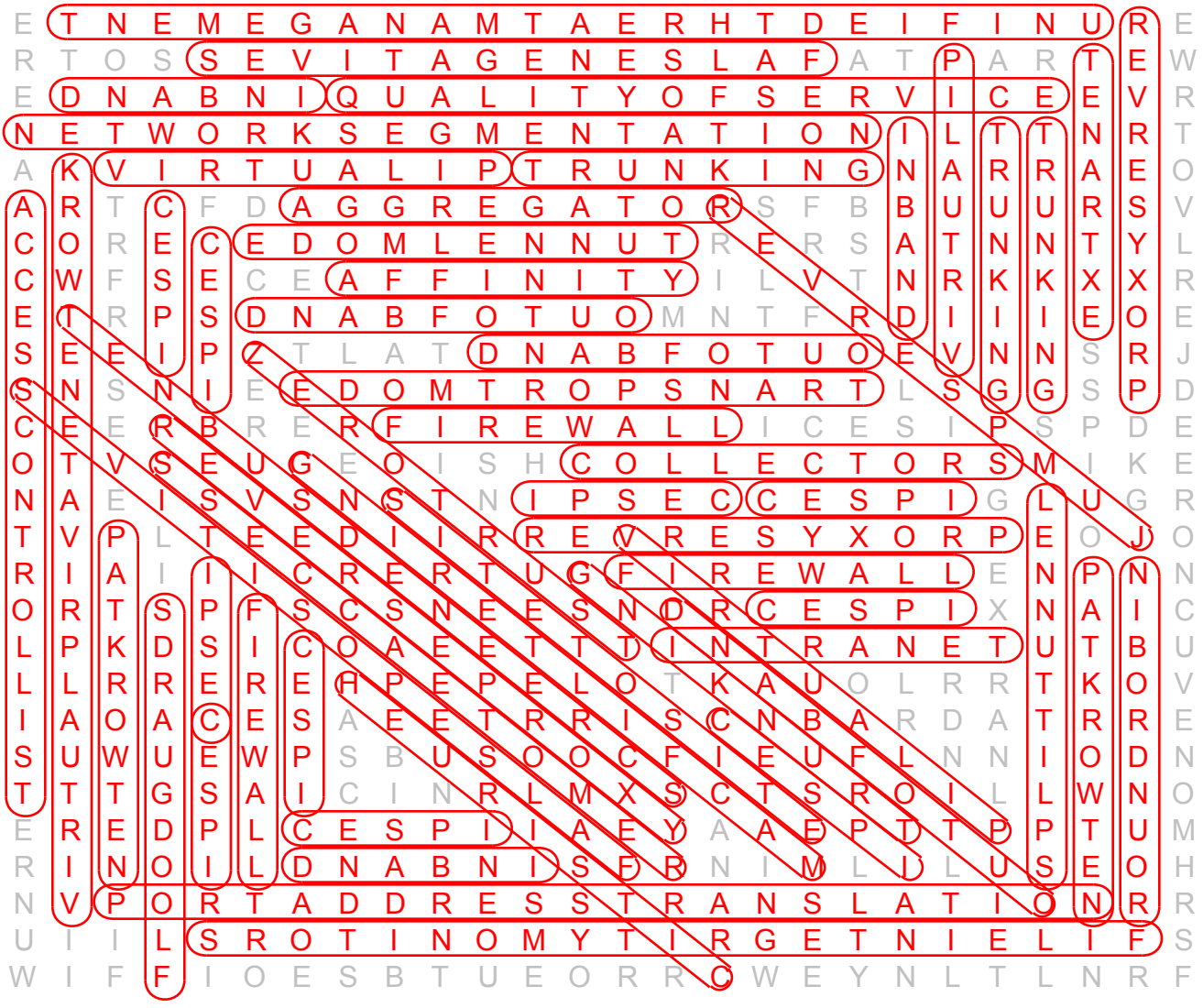
Curvy Words 2 Network Architecture: KEY

1. Designed to keep a host connected to the same server across a session. (AFFINITY)
2. Often happens when alerts that should be generated aren't. (FALSE NEGATIVES)
3. These occur when expected behavior is identified as malicious. (FALSE POSITIVES)
4. These are commonly implemented in firewalls and IDS/IPS solutions to prevent DoS and DDoS attacks. (FLOOD GUARDS)
5. This model uses artificial intelligence (AI) to detect intrusions and malicious traffic. (HEURISTIC)
6. This is a private, internal network that uses common network technologies (HTTP, FTP, and so on) to share information and provide resources to internal organizational users. (INTRANET)
7. This is the selective admission of packets based on a list of approved Media Access Control addresses. (MAC FILTERING)
8. Managing the endpoints on a case-by-case basis as they connect. (NETWORK ACCESS CONTROL)
9. Allows many different internal, private addresses to share a single external IP address. (PORT ADDRESS TRANSLATION)
10. When a user requires access to a network and its resources but is not able to make a physical connection. (REMOTE ACCESS)
11. Typically installed on the server side of a network connection, often in front of a group of web servers, and intercepts all incoming web requests. (REVERSE PROXY)
12. This is a form of VPN where not all traffic is routed via the VPN. (SPLIT TUNNEL)
13. In this mode, the security of packet traffic is provided by the endpoint computers. (TRANSPORT MODE)
14. This is a security model centered on the belief that you should not trust any request without verifying authentication and authorization. (ZERO TRUST)

Word Search KEY

Find each of the following words.

PROXY SERVER
TRANSPORT MODE
FILE INTEGRITY MONITORS
OUT OF BAND
INTRANET (1)
NETWORK TAP
FALSE NEGATIVES
FIREWALL (3)
QUALITY OF SERVICE
UNIFIED THREAT MANAGEMENT
VIRTUALIP (3)
REMOTE ACCESS
EXTRANET (1)
COLLECTORS (1)
MAC FILTERING
FALSE POSITIVES
ACCESS CONTROL LIST
TUNNEL MODE
VIRTUAL PRIVATE NETWORK
AGGREGATOR (1)
SPLIT TUNNEL
AFFINITY (1)
ROUND ROBIN
PORT ADDRESS TRANSLATION
SCREENED SUBNET
IN BAND
SITE TO SITE
TRUNKING (4)
FLOOD GUARDS
ZERO TRUST
REVERSE PROXY
JUMP SERVER
HEURISTIC (1)
NETWORK SEGMENTATION
IPSEC (10)



Solve the clues to uncover the secret, which is something related to cryptography.

1. A switching protocol that prevents network loops by dynamically disabling links as needed. Spanning Tree Protocol
2. Mechanism used to mitigate performance and privacy issues when requesting certificate status from an OCSP responder. Stapling
3. Applying consistent names and labels to assets and digital resources/identities within a configuration management system. Standard Naming Conventions
4. Provisioning processing resource between the network edge of IoT devices and the data center to reduce latency. Fog Computing
5. The record of evidence history from collection, to presentation in court, to disposal. Chain of Custody
6. The binary format used to structure the information in a digital certificate. Distinguished Encoding Rules.
7. A cloud that is deployed for shared use by cooperating tenants. Community Cloud
8. In data protection, the principle that countries and states may impose individual requirements on data collected or stored within their jurisdiction. Data Sovereignty
9. Utility for command-line manipulation of URL-based protocol requests. Curl
10. Information that is primarily stored on specific media, rather than moving from one medium to another. Data at Rest
11. A measure of disorder. Entropy
12. In a Wi-Fi site survey, a diagram showing signal strength at different locations. Heat Map
13. A method that uses feature comparisons and likenesses rather than specific signature matching to identify whether the target of observation is malicious. Heuristic Analysis

Answer: Steganography

Solve the clues and unscramble the letters in the circles to discover the secret, which is something that blocks external electromagnetic fields.

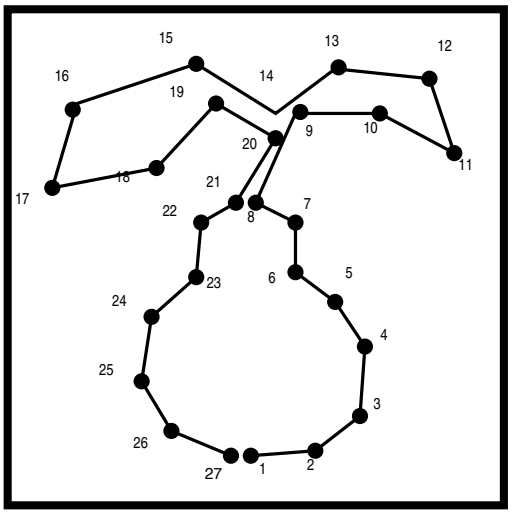
1. Preventing a device attached to a switch port from communicating on the network unless it matches a given MAC address or other protection profile. Port Security
2. The practice of creating a virtual boundary based on real-world geography. Geofencing.
3. The process by which an attacker is able to move from one part of a computing environment to another. Lateral Movement
4. Information stored or recorded as a property of an object, state of a system, or transaction. Metadata
5. Risk that an event will pose if no controls are put in place to mitigate it. Inherent Risk
6. An impersonation attack in which a request for a website, typically an e-commerce site, is redirected to a similar-looking, but fake, website. Pharming
7. In threat hunting, the concept that threat actor and defender may use deception or counterattacking strategies to gain positional advantage. Maneuver
8. The process of making a host or app configuration secure by reducing its attack surface through running only necessary services, installing monitoring software to protect against malware and intrusions, and establishing a maintenance schedule to ensure the system is patched to be secure against software exploits. Hardening
9. Implementation of a sandbox for malware analysis. Cuckoo
10. A deidentification method where generic or placeholder labels are substituted for real data while preserving the structure or format of the original data. Data Masking
11. Code in an application that is redundant because it will never be called within the logic of the program flow. Dead Code

Secret: Faraday cage

Solutions

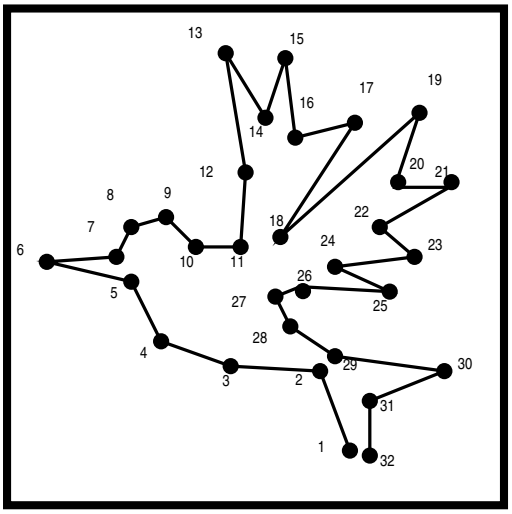
1

Pear

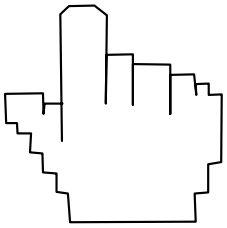


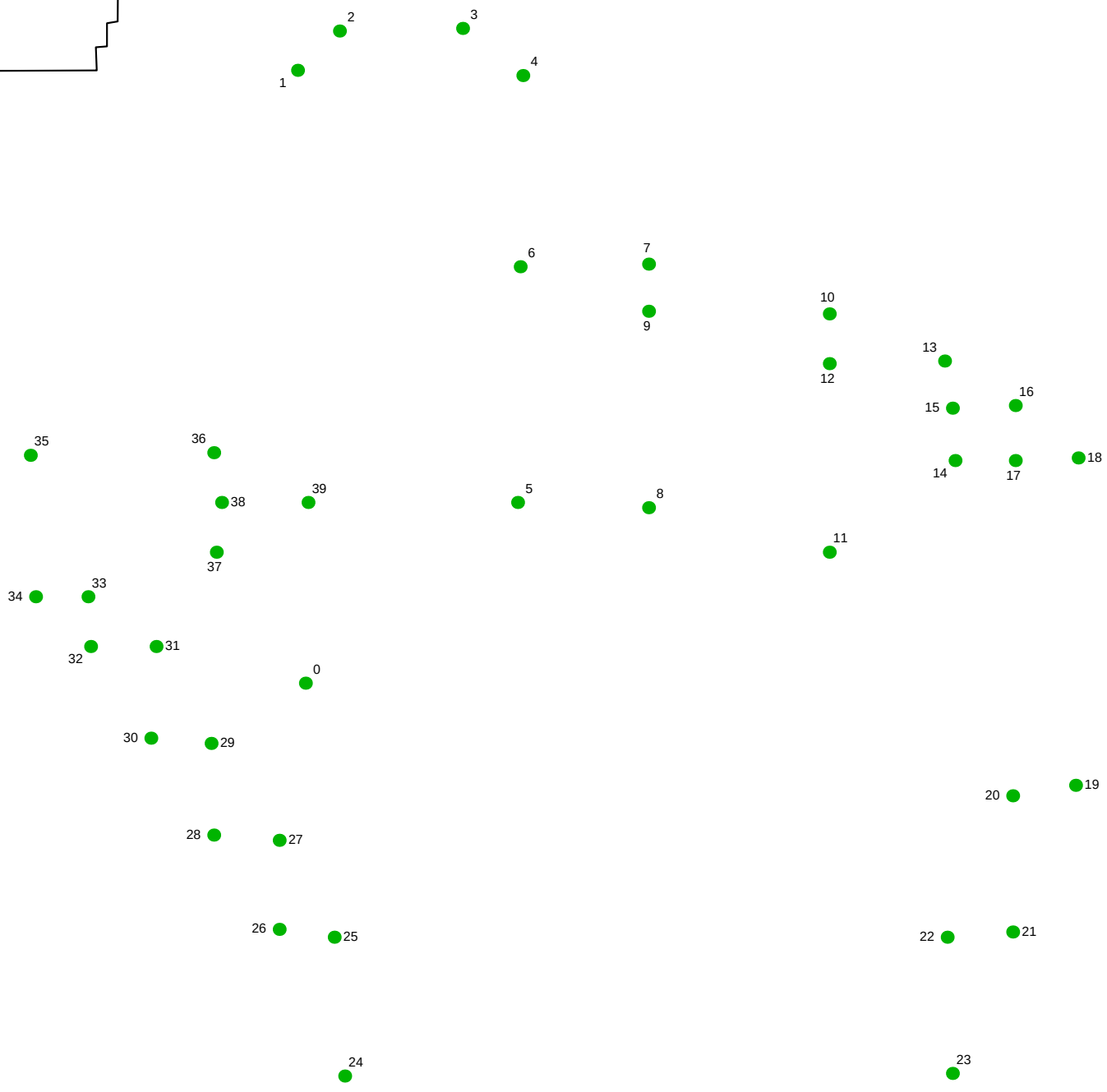
2

Bird



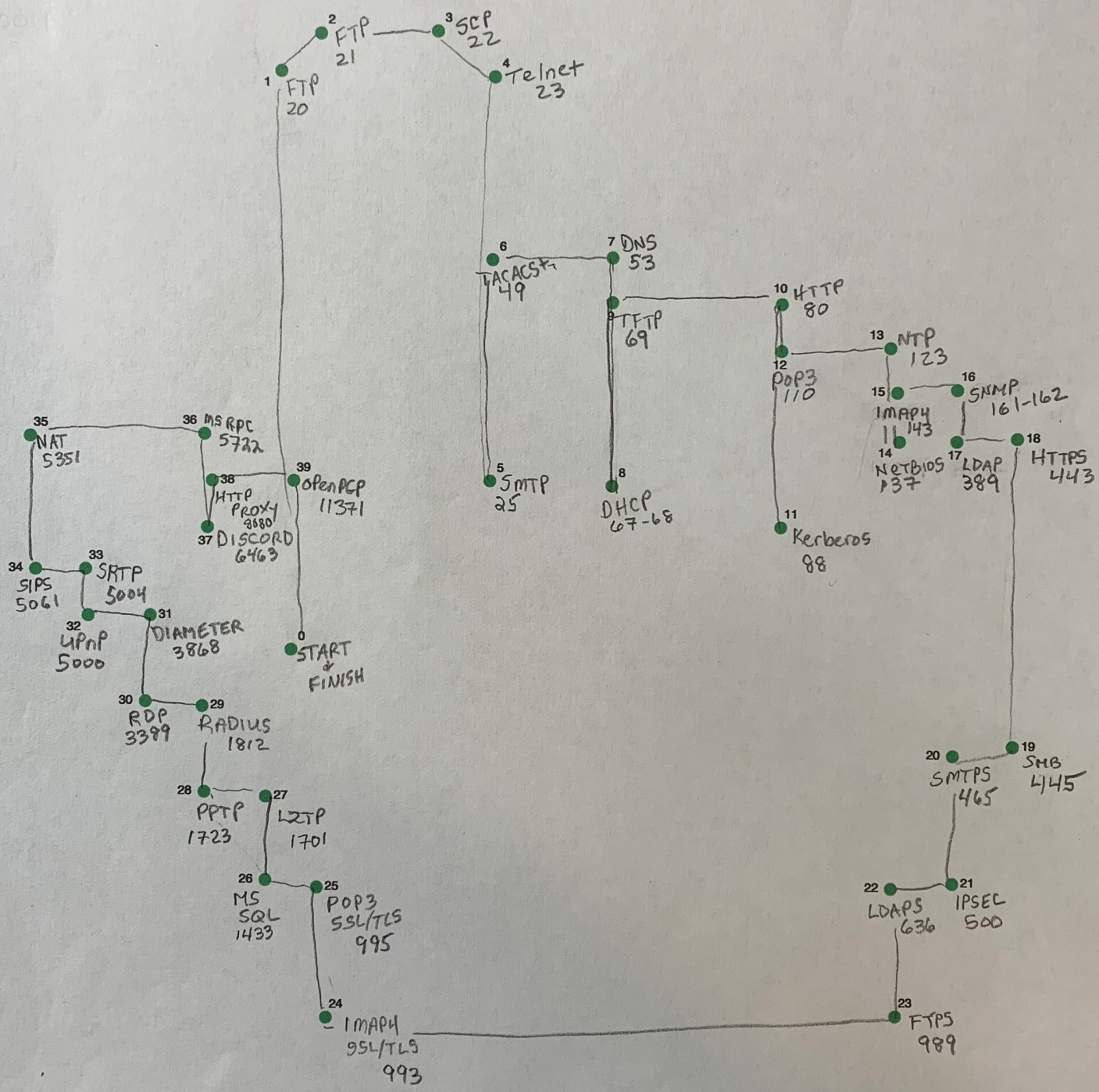
Mystery Puzzle 1 KEY



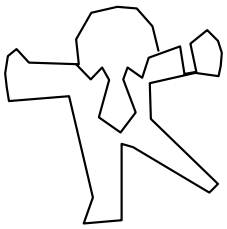


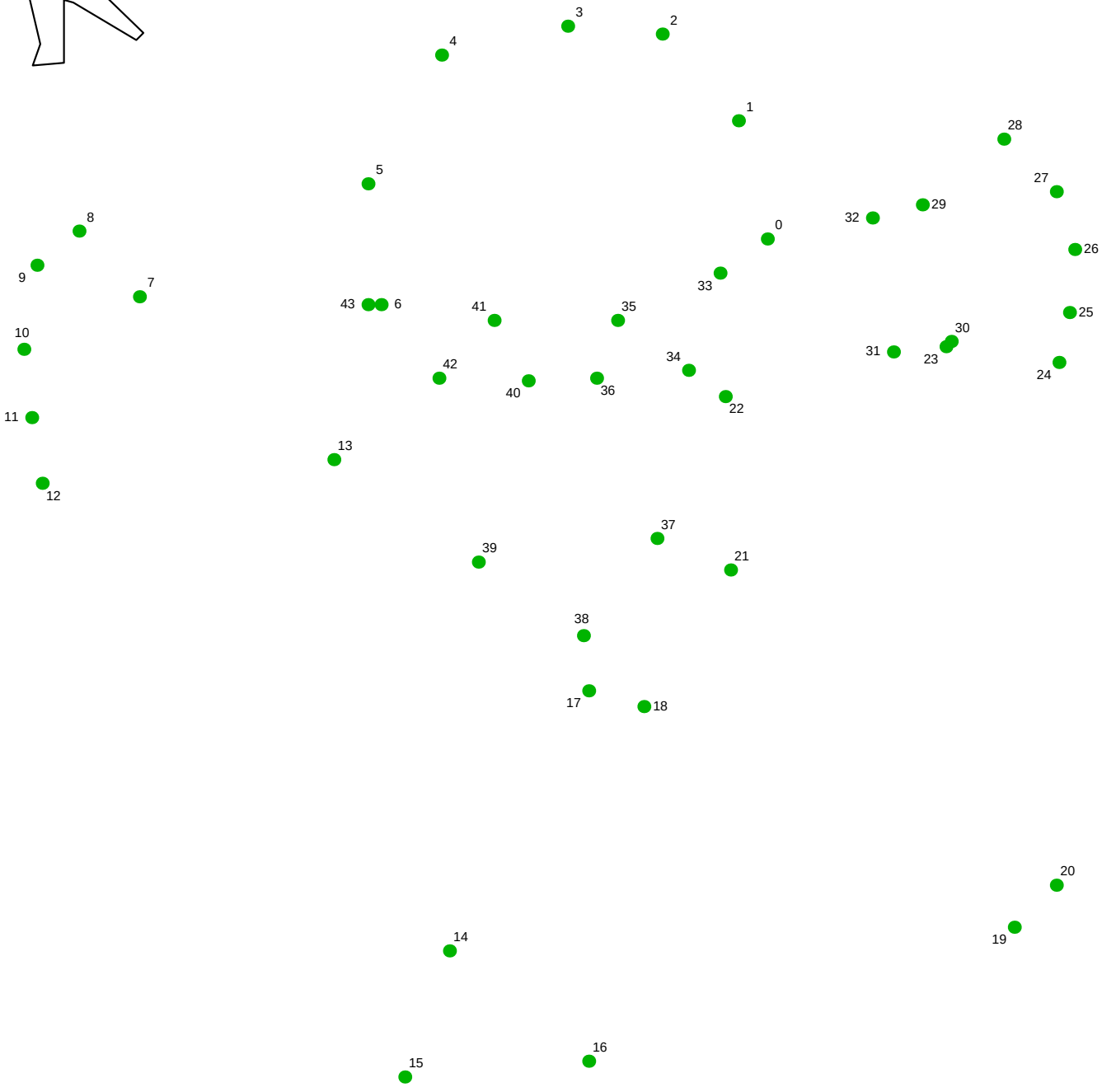
Dot to Dot Mystery Puzzles

Picture 1

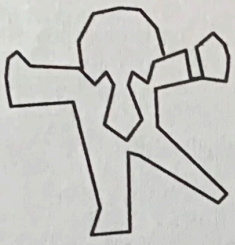


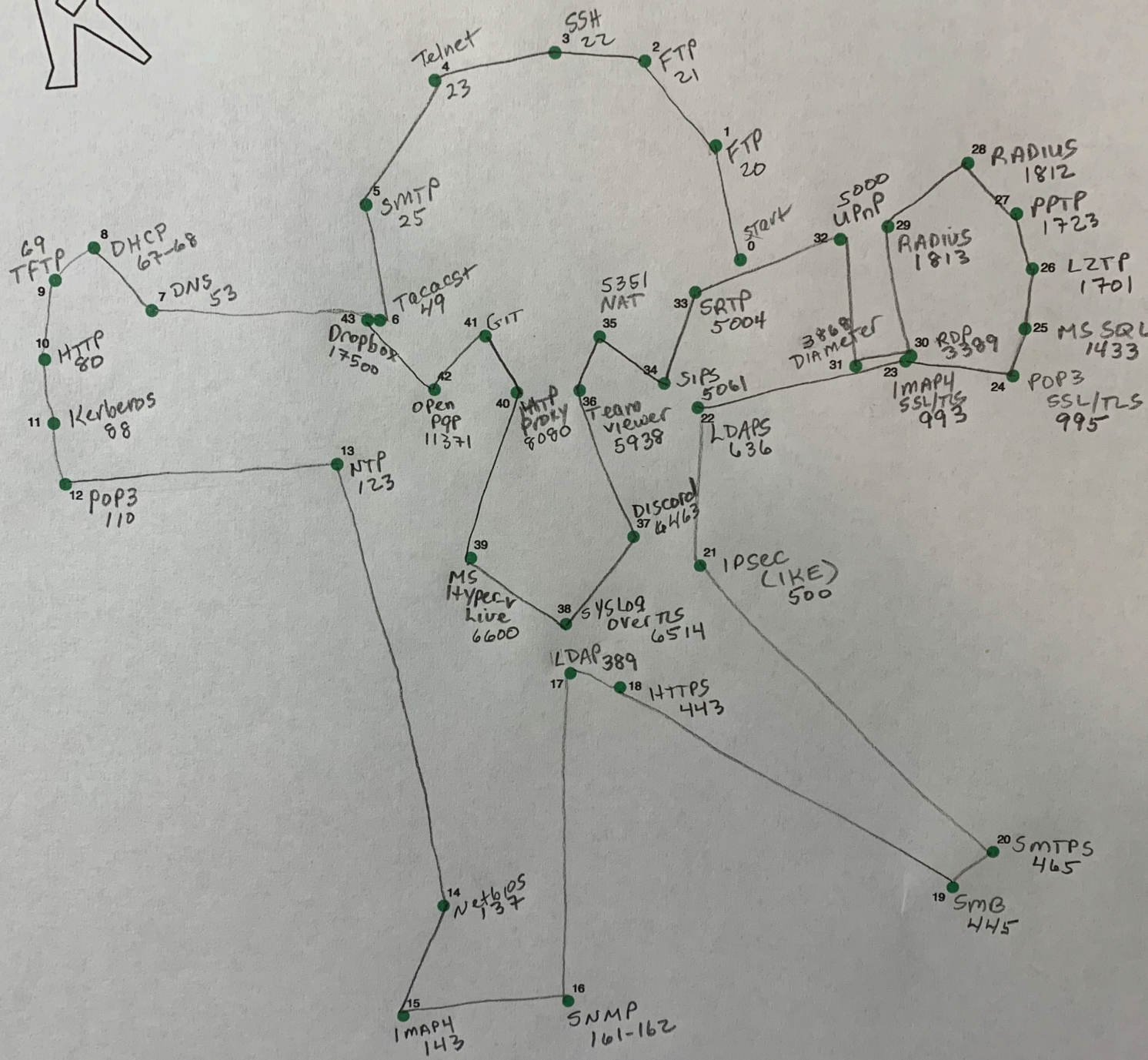
Mystery Puzzle 2 Key





Mystery Puzzle 2 Key

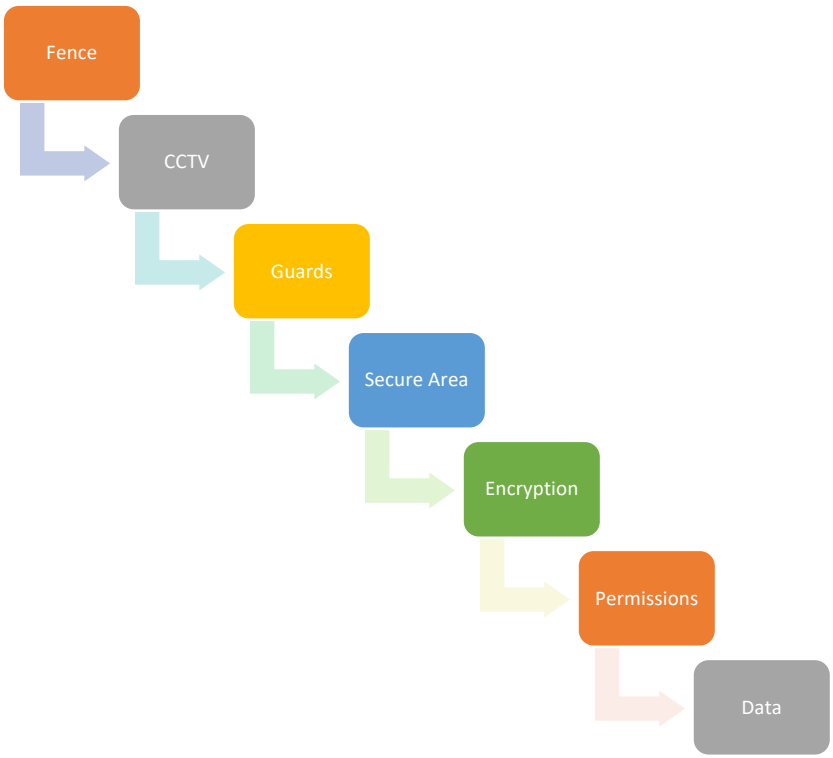




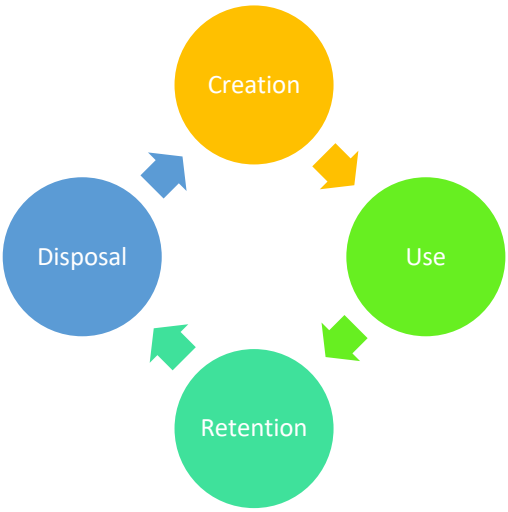
Processes and Cycles

What comes before and after? Fill in the blank spaces!

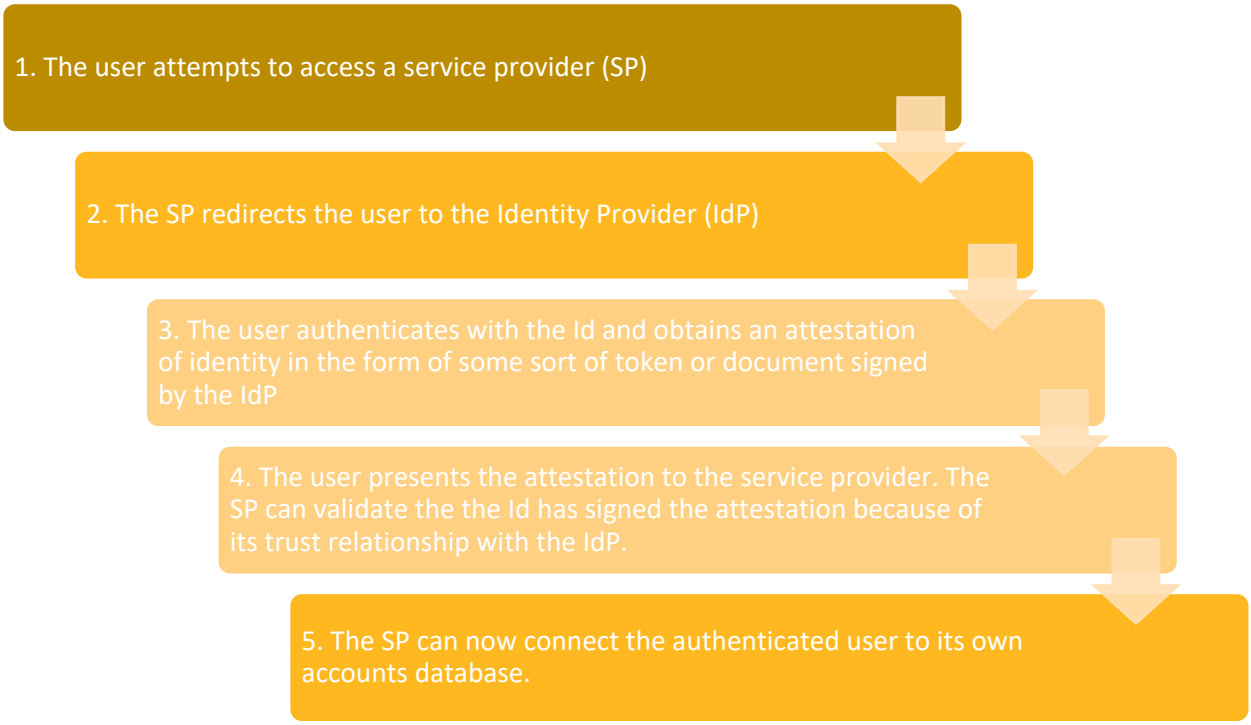
1. Defense in Depth



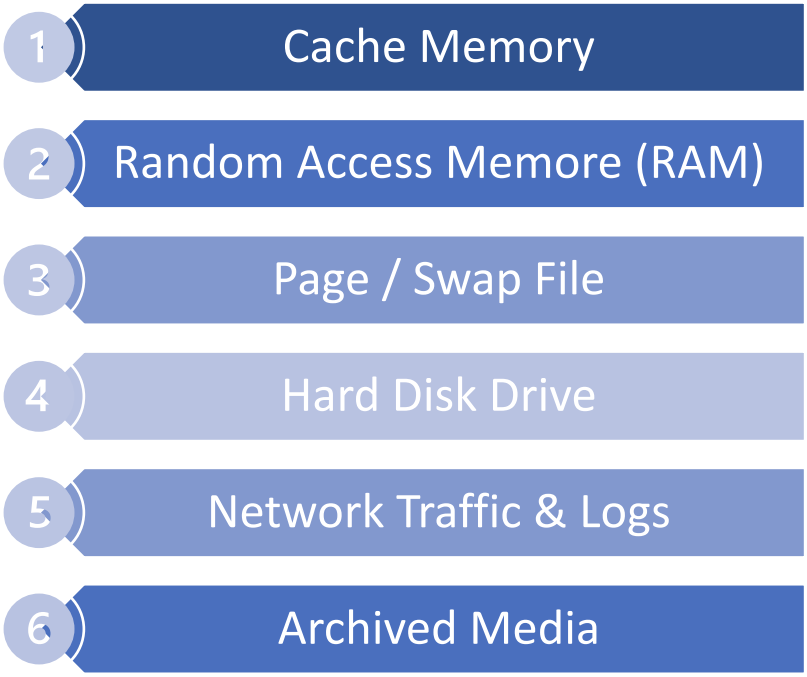
2. Information Life Cycle



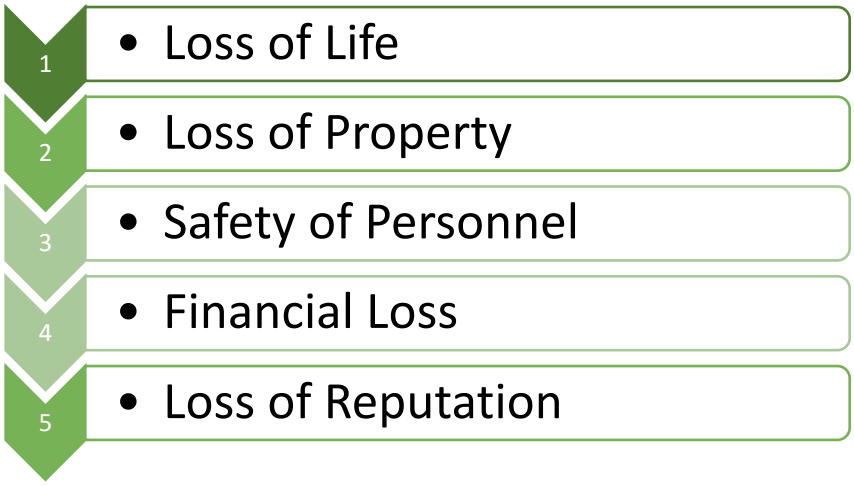
3. Identity Providers and Attestation



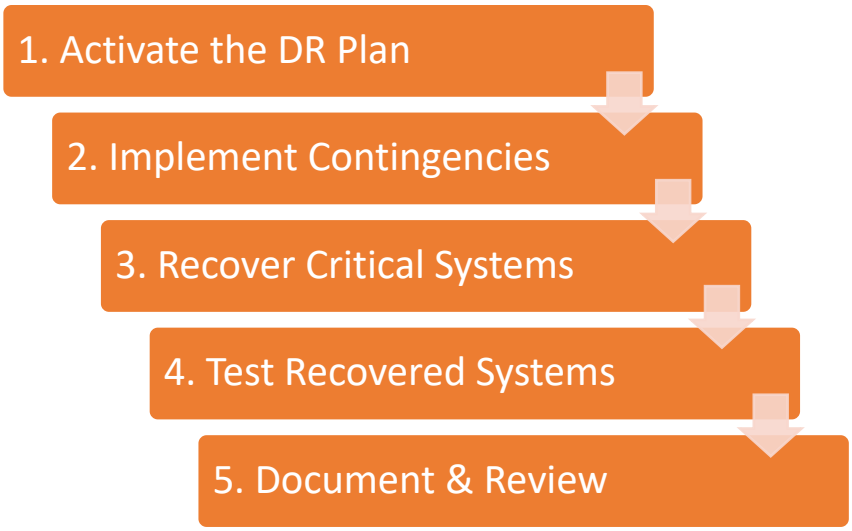
4. The Order of Volatility



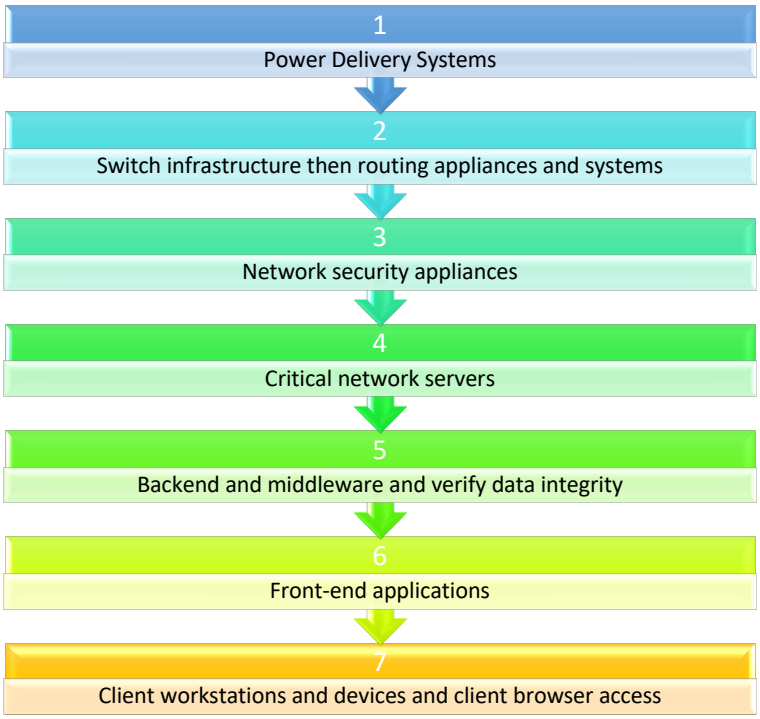
5. Evaluating Impact



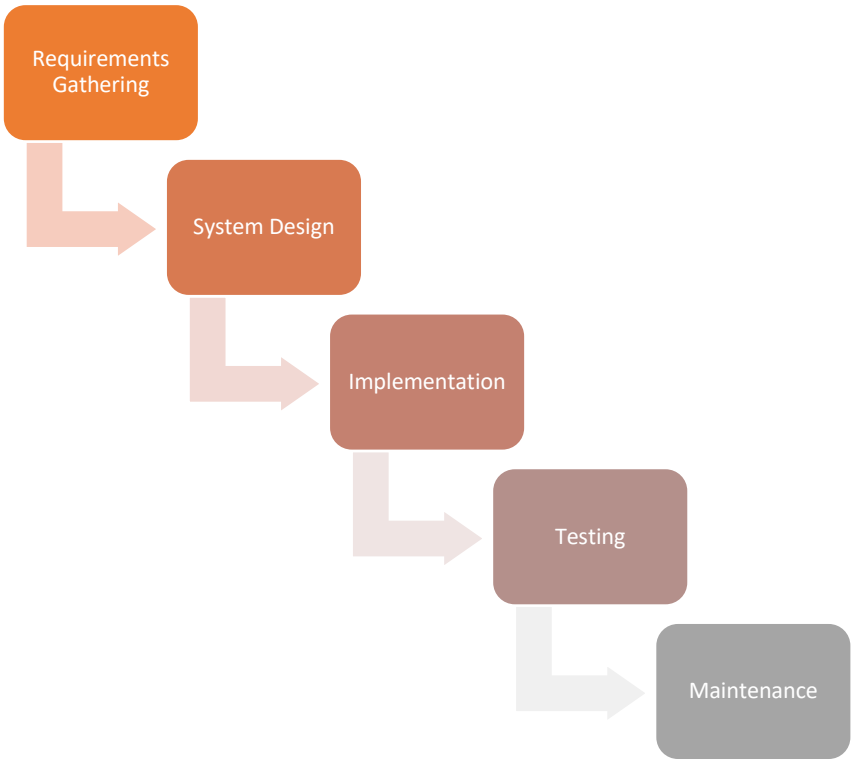
6. Disaster Recovery Plan Phases



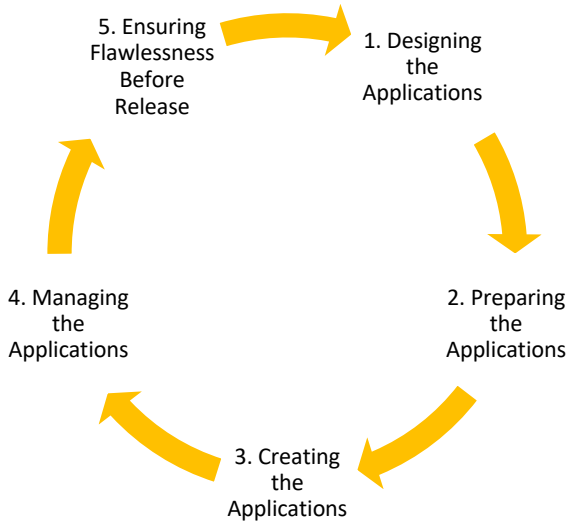
7. Order of Restoration



8. Waterfall Development Model

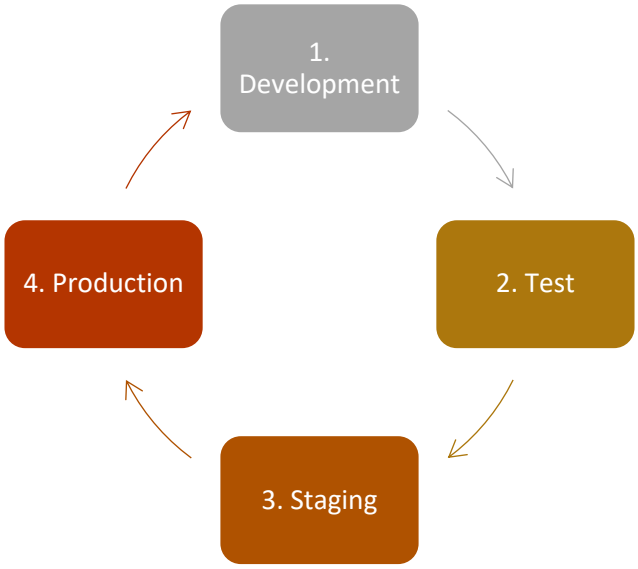


9. Application Provisioning

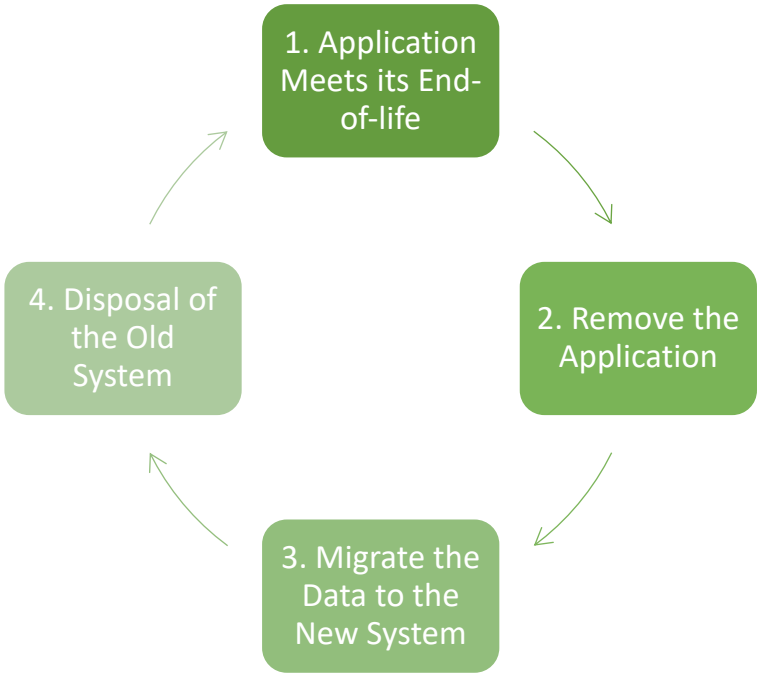


10. Incident Response

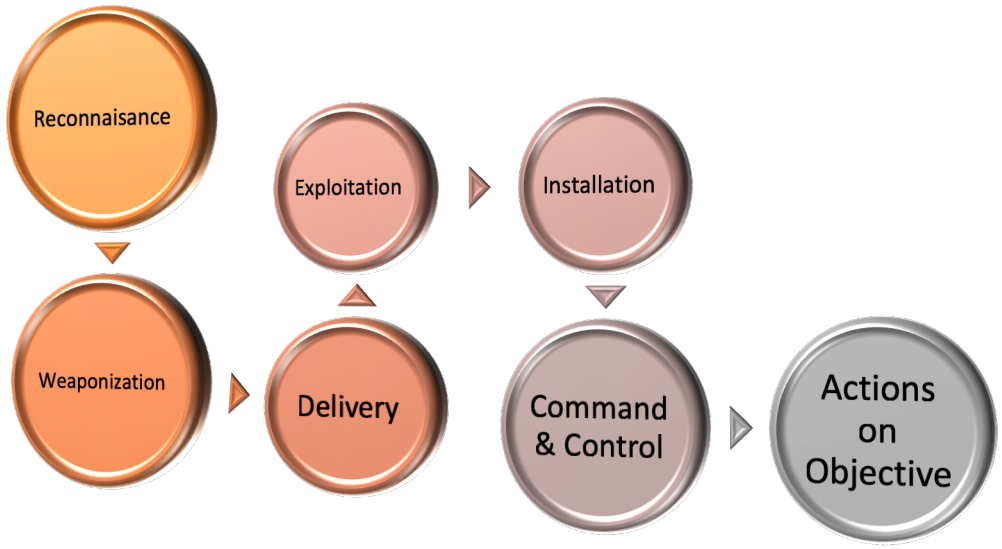
11. Secure Deployment (Secure Staging) Development Life Cycle



12. Application Deprovisioning



13. The Cyber Kill Chain. See if you can also identify what happens at each phase. Can you name a method of mitigation for each stage?

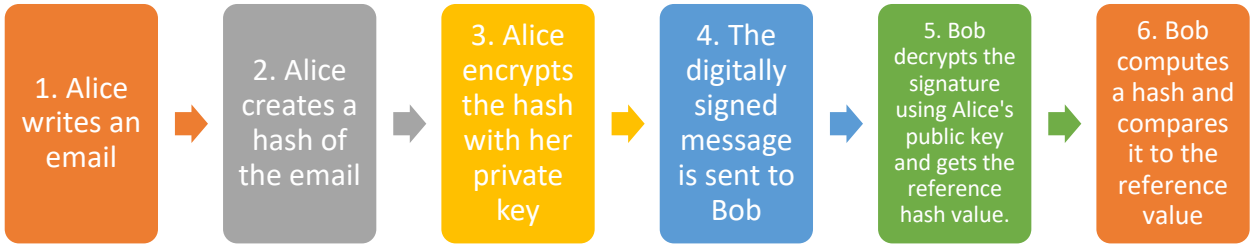


Stages of the Cyber Kill Chain	
Reconnaissance	Calling employees, sending emails, social engineering, dumpster diving
Weaponization	Create malware payload
Delivery	Delivery medium such as USB, email, web page
Exploitation	Executing code via a vulnerability
Installation	Installing malware on the asset
Command and Control	Infected system sends back information to the attacker
Action on Objectives	'Hands-on keyboard' – attack complete

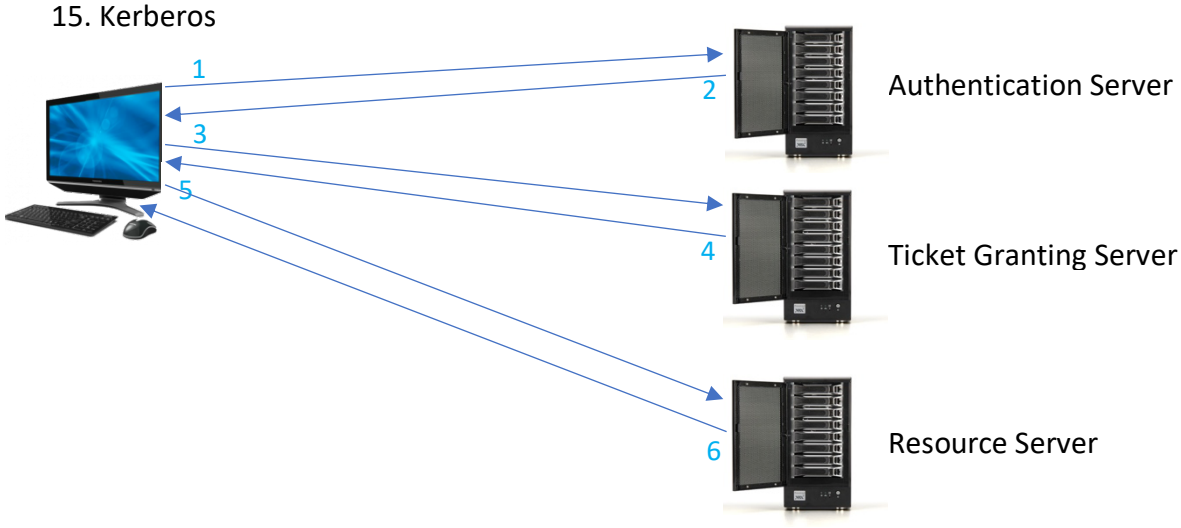
Mitigations	
Reconnaissance	Limit public info (Job postings, LinkedIn, etc.; social media acceptable use; modify server error messages; disable unused ports and services; honeypots; firewall and IPS; TOR and 3rd party VPN inbound blocking
Weaponization	Patch management; disable Office macros, JavaScripts, and browser Plug-ins; antivirus; IPS; email security; MFA; audit logging

Delivery	User awareness training, IPS/IDS, DKIM and SPF (email security), web filtering, disable USB, no “admin” rights, DNS filtering, SSL inspection
Exploitation	DEP, Anti-exploit
Installation	Linux Chroot jail / Windows disable PowerShell; UBA/EDR solution, follow incident response SOPs
Command and Control	Limit what the attacker can control, segmentation/micro segmentation, NGFW, DNS redirect, layer 7 application control, SSL deep packet inspection, IOCs
Action on Objectives	DLP, UBA, network segmentation, zero-trust security model!

14. Digital Signature

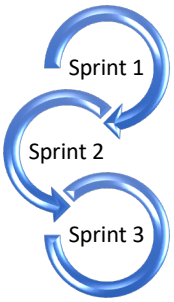


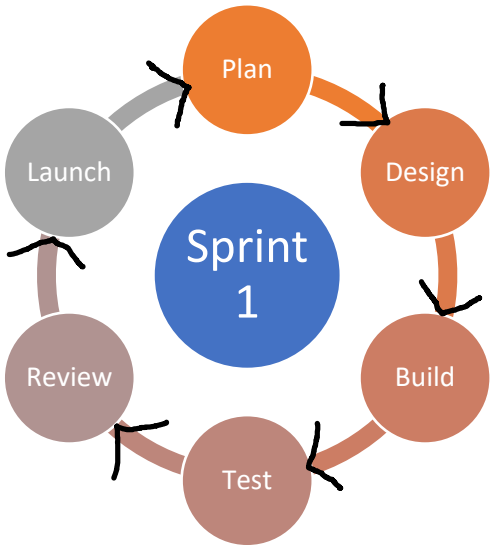
15. Kerberos



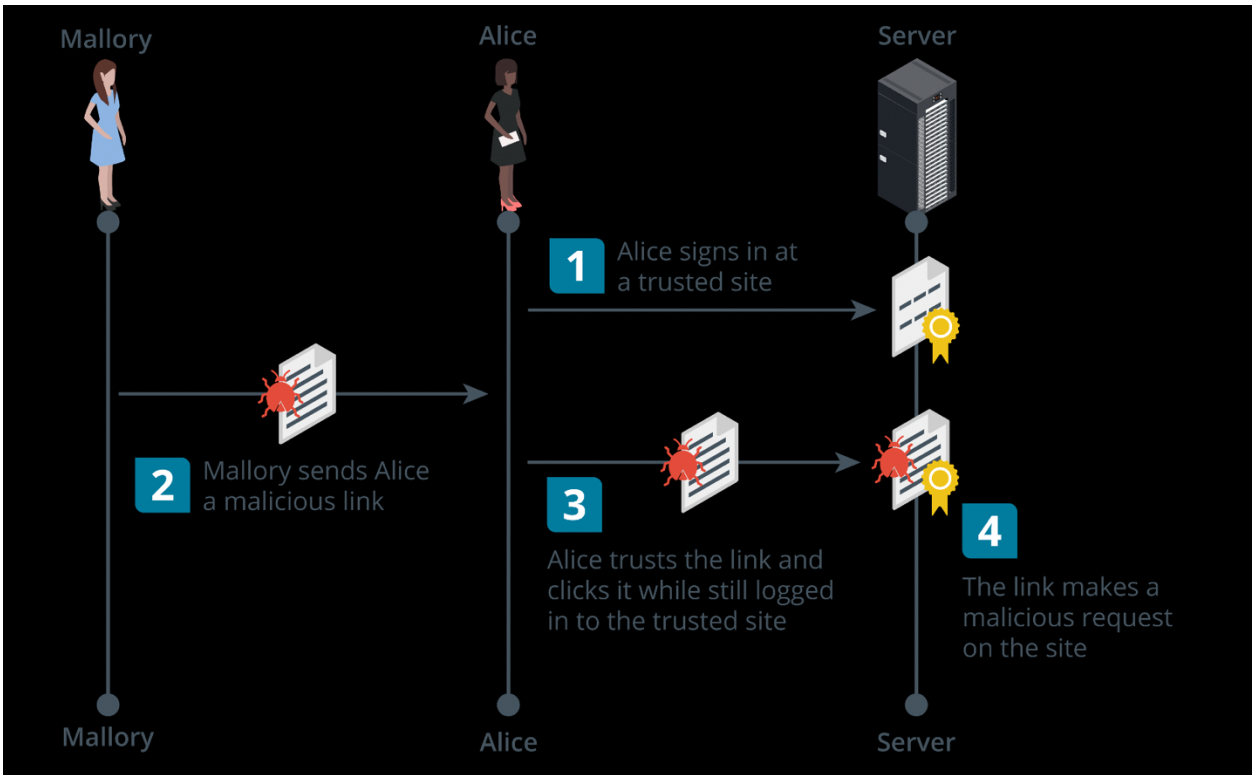
1	The user logs into a client workstation with a username and password and immediately requests a TGT from the AS.
2	If the AS finds the user in its database, it sends back: (1) A TGT, encrypted with the TGS secret key. (2) A matching message encrypted with the user's secret key.
3	Having the session key, the client sends three messages to the TGS to request access to a specific server: (1) the TGT, (2) an authenticator encrypted with the session key. (3) a plaintext message containing the name of a resource server and requested ticket lifetime.
4	The TGS decrypts the TGT with its secret key to learn the session key, then decrypts the authenticator. If the service, timestamp, and user are valid, it sends a credential ticket for the service, encrypted with the resource server's secret key. It has the user's information, a timestamp, lifetime, and a service session key created by the TGS. A matching message encrypted by the TGS session key and containing the service session key.
5	The client decrypts the second message and uses the session key to create a new authenticator. It sends the authenticator and service ticket to the resource server.
6	The resource server (RS) decrypts the service ticket to learn the session key and uses it to decrypt the authenticator. If everything checks out, the client is authenticated on the RS and they can communicate securely; this step can also use mutual authentication.
Note:	Whenever the client wants to log into a new service, or when a service ticket expires, it can present its TGT to the TGS again for a new request.

16. The Agile Software Development Life Cycle
    Can you remember the life cycle of a Sprint? What happens in each stage?

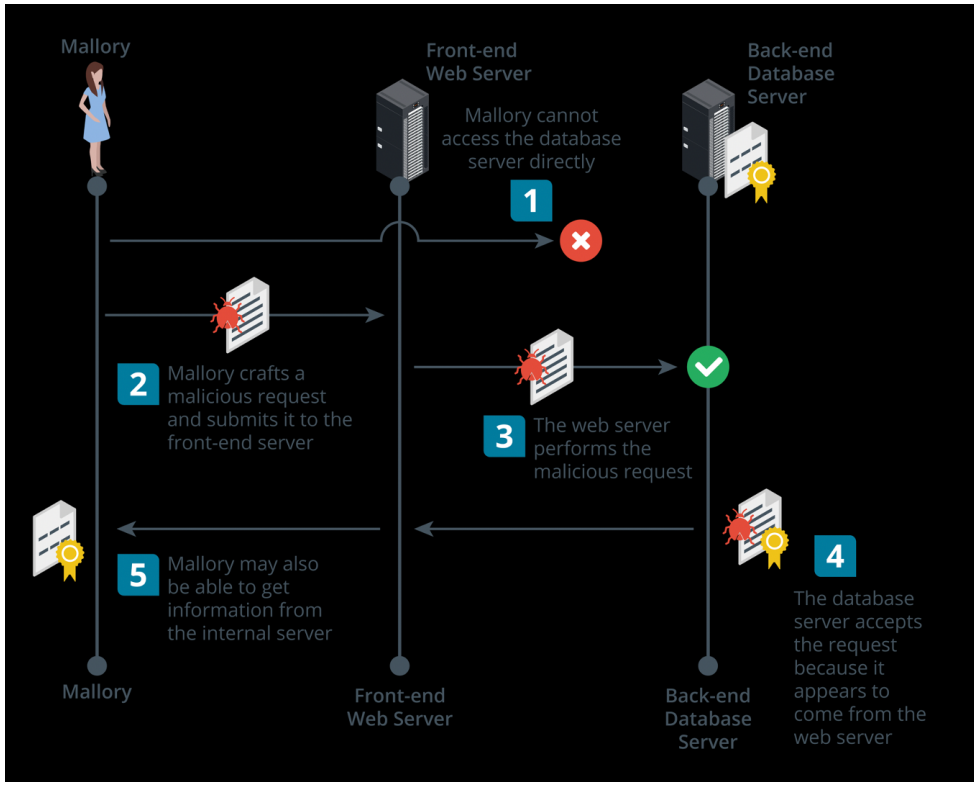




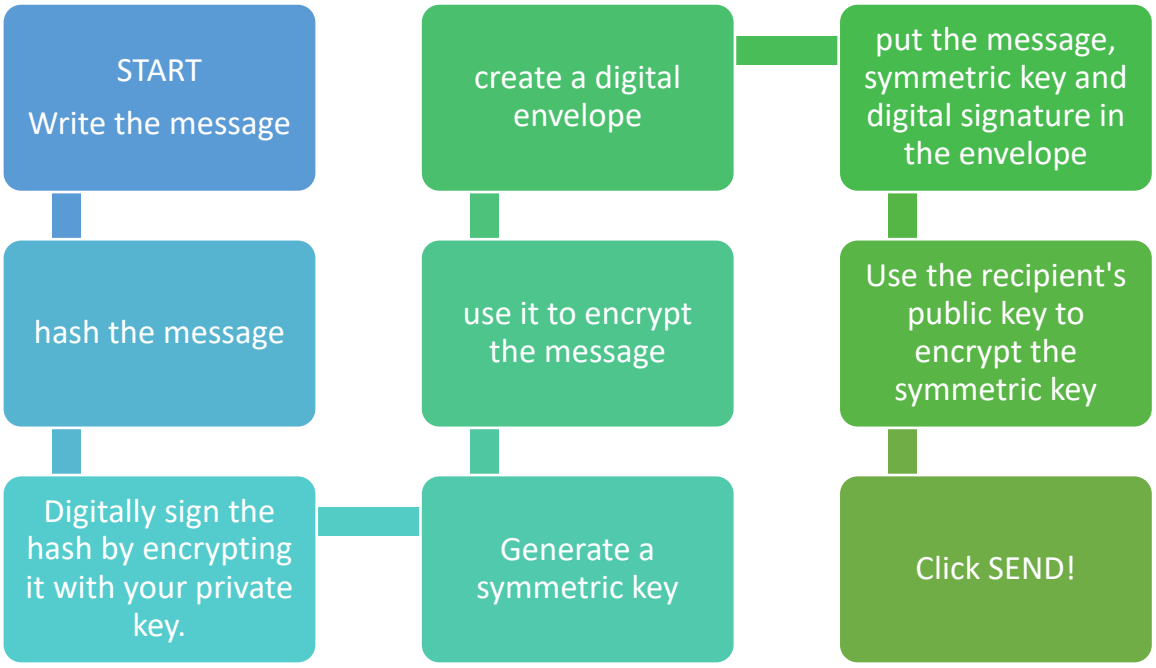
17. Cross-site Request Forgery: What two steps are missing?



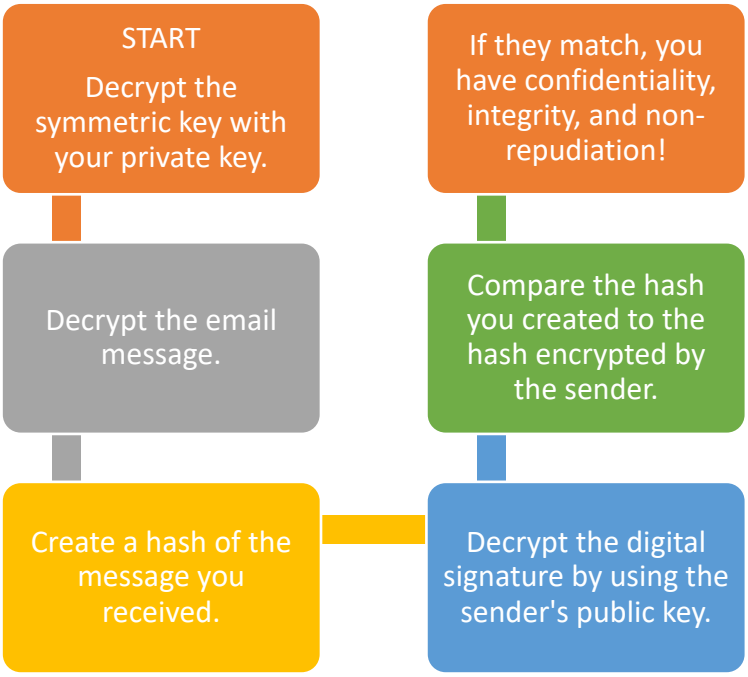
18. Server-side Request Forgery: What three steps are missing?



19. Want to send an encrypted digitally signed email?



20. What happens when you receive an encrypted digitally signed email? What happens first? And then?



21. What if I don't have a digital certificate!

1 Generate a public-private key pair

2 Complete a certificate signing request

3 Send the CSR and your public key to the certificate authority

4 The CA will verify your ID and create and sign a digital certificate for you

5 The CA will store the certificate and your public key in the certificate repository (CR).

6 Now you can send encrypted, digitally signed email!

Can you decrypt these famous quotes?

1. “NAL ZNA JBEGU UVF FNYG JVYY FGVPX HC SBE JUNG UR ORYVRIRF EVTUG, OHG VG GNXRF Z FYVTUGYL ORGGRE ZNA GB NPXABJYRQTR VAFGNAGYL NAQ JVGUBHG ERFREINGVBA GUNG UR VF VA REEBE.”

   -NAQERJ WNPXFBA

   "Any man worth his salt will stick up for what he believes right, but it takes a slightly better man to acknowledge instantly and without reservation that he is in error."

   -Andrew Jackson

2. GURER VF ABGUVAT ZBER PBEEHCGVAT, ABGUVAT ZBER QRFGEHPGVIR BS GUR ABOYRFG NAQ SVARFG SRRYVATF BS BHE ANGHER, GUNA GUR RKREPVFR BS HAYVZVGRQ CBJRE.”

   -JVYYVNZ URAEL UNEEVFBA

   "There is nothing more corrupting, nothing more destructive of the noblest and finest feelings of our nature, than the exercise of unlimited power."

   -William Henry Harrison

3. “VG VF UNEQ GB SNVY, OHG VG VF JBEFR ARIRE GB UNIR GEVRQ GB FHPPRRQ. VA GUVF YVSR, JR TRG ABGUVAT FNIR OL RSSBEG.”

   -GURBQBER EBBFRIRYG

   "It is hard to fail, but it is worse never to have tried to succeed. In this life, we get nothing save by effort."

   -Theodore Roosevelt

4. “GUR BAYL GUVAT JR UNIR GB SRNE VF…SRNE VGFRYS.”

   -SENAXYVA Q. EBBFRIRYG

   "The only thing we have to fear is...fear itself."

   -Franklin D. Roosevelt

5. “N ZNA VF ABG SVAVFURQ JURA UR VF QRSRNGRQ. UR VF SVAVFURQ JURA UR DHVGF.”

-EVPUNEQ AVKBA

"A man is not finished when he is defeated. He is finished when he quits."

-Richard Nixon

6. “V QBA’G UNIR GB GRYY LBH UBJ SENTVYR GUVF CTRPVBHF GUVF TVSG BS SERRQBZ VF. RIREL GVZR JR URNE, JNGPU, BE ERNQ GUR ARJF, JR NER ERZVAQRQ GUNG YVOREGL VF N ENER PBZZBQVGL VA GUVF JBEYQ.”

-EBANYQ ERNTNA

"I don't have to tell you how fragile this precious gift of freedom is. Every time we hear, watch, or read the news, we are reminded that liberty is a rare commodity in this world."

-Ronald Reagan

7. “JR BJR GUVF SERRQBZ BS PUBVPR NAQ NPGVBA GB GUBFR ZRA NAQ JBZRA VA HAVSBEZ JUB UNIR FREIRQ GUVF ANGVBA NAQ VGF VAGRERFGF VA GVZR BS ARRQ. VA CNEGVPHYNE, JR NER SBERIRE VAQROGRQ GB GUBFR JUB UNIR TVIRA GURVE YVIRF GUNG JR ZVTUG OR SERR,”

- EBANYQ ERNTNA

"We owe this freedom of choice and action to those men and women in uniform who have served this nation and its interests in time of need. In particular, we are forever indebted to those who have given their lives that we might be free."

-Ronald Reagan

8. N YRNQRE JUB QBRFA’G URFVGNGR ORSBER UR FRAQF UVF ANGVBA VAGB ONGGYR VE ABG SVG GB OR N YRNQRE.”

-TBYQN ZRVE

“A leader who doesn't hesitate before he sends his nation into battle is not fit to be a leader.”

-Golda Meir

9. “GEHFG LBHEFRYS. PERNGR GUR XVAQ BS FRYS GUNG LBH JVYY OR UNCCL GB YVIR JVGU NYY LBHE YVSR. ZNXR GUR ZBFG BS LBHEFRYS OL SNAAVAT GUR GVAL, VAARE FANEXF BS CBFFVOVYVGL VAGB SYNZRF BS NPUVRIRZRAG.”

-TBYQN ZRVE

“Trust yourself. Create the kind of self that you will be happy to live with all your life. Make the most of yourself by fanning the tiny, inner sparks of possibility into flames of achievement.”

-Golda Meir

These are a bit harder!

10. “QCTGT ZU VE SDQR NT DVSTGGWQT UE JDFC WU QCT SDQR EM XTZVL CWAAR.”

-GEXTGQ OEDZU UQTKTVUEV

“There is no duty we underrate so much as the duty of being happy.”

-Robert Louis Stevenson

11. “UHWC OCHOVC UYGQ VHRTCD AR GR KHPD YKGR HYKCDU FGR AR G MCCJ.”

-MAVVAGW SCGR KHMCVVU

“Some people stay longer in an hour than others can in a week.”

-William Dean Howells

12. “PVOTA QPT EQKT SMP CTMCOT UZM QPTX’N UJOOJXD NM EQWT VC NZTJP MUX.”

-LZVLW GTQDTP

“Rules are made for people who aren’t willing to make up their own.”

-Chuck Yeager

13. “CYRNFR QB ABG GNXR FRPHEVGL CYHF NTNVA.”

-ZF. FPUJNEGM

“**P**lease **D**o Not **T**ake **S**ecurity **P**lus **A**gain!”

-Ms. Schwartz*

**The first letter of each word will help you remember the seven layers of the OSI model!*

References

Conklin, W., & White, G. (2021). *CompTIA Security+ Exam Guide* (6th ed.). New York, NY, USA: McGraw Hill.

Khurana, S. (2019, October 3). *Famous Presidential Quotes From America's Leaders*. Retrieved February 17, 2022, from ThoughtCo.: https://www.thoughtco.com/famous-presidential-quotes-2833521

Khurana, S. (2021, September 8). *Memorial Day Quotes by Ronald Reagan*. Retrieved February 17, 2022, from ThoughtCo,: https://www.thoughtco.com/memorial-day-reagan-quotes-2831788

Lewis, J. J. (2021, October 2). *Golda Meir Quotes*. Retrieved February 17, 2022, from ThoughtCo.: https://www.thoughtco.com/golda-meir-quotes-3530090

Make Puzzles. (2020-2021). Retrieved February 2021, from edHelper.com: https://www.edhelper.com/crossword.htm

Neil, I. (2020). *CompTIA Security+ SY0-601 Certification Guide* (2nd ed.). Birmingham, UK: Packt.

Pengelly, J. (2020). *The Official CompTIA Security+ Instructor Guide (Exam SY0-601).* Downers Grove, IL, USA: CompTIA.

Thaxton, K. (2021, December 16). Security+ Test Review. Biloxi, MS, USA.

The CISO Perspective. (2019, February 5). *Breaking The Kill Chain: A Defensive Approach* . (The CISO Perspective) Retrieved February 22, 2022, from YouTube: https://www.youtube.com/watch?v=II91fiUax2g&list=PLA7bpMWMDc1Fbw1xH9hs8PgI_brfplHjs&index=25

The Saturday Evening Post. (2021, September 1). Break the Code. *The Saturday Evening Post*(September/October 2021), 30. Retrieved February 17, 2022, from the Saturday Evening Post: https://www.saturdayeveningpost.com/issues/2021-09-01/

The Saturday Evening Post. (2021, March 1). Break the Code. *The Saturday Evening Post*(March/April 2021), 30.

The Saturday Evenng Post. (2021, May 1). Break the Code. *The Saturday Evenng Post*(May/June 2021), 24.