Appendix
Answers to Review Questions

Chapter 2: Networking Foundations

1. A. A thermostat is an embedded device without a traditional user interface. A light bulb would have no user interface, even if it has network capabilities. A set-top cable box would have a custom interface and not a general-purpose one. The only device here that is a general-purpose computing platform with a traditional user interface—screen and keyboard—is the smartphone, so it isn't part of the IoT.
2. D. TCP uses a three-way handshake, which is fairly heavyweight. HTTP uses TCP and adds more on top of it. ICMP is used for control messages. UDP has very little overhead and is commonly used for real-time data transport.
3. B. From top to bottom, the TCP/IP architecture is Link, Internet, Transport, and Application. B is the only answer that reflects that.
4. B. While Microsoft Azure and Google Compute have storage capabilities, they aren't storage as a service solutions. Drop leaf is a type of table. The only one listed here that is storage as a service solution is iCloud, which is Apple's cloud storage platform.
5. B. The IP headers include addresses. UDP headers use ports. TCP headers use flags, but UDP headers do not. The UDP headers have the source and destination port fields along with checksum and length.
6. C. The three-way handshake is used to establish a connection. The first message has the SYN flag set and includes the sequence number. The response from the server has the ACK flag set for the SYN message that was sent from the client. The acknowledgment number is set. Additionally, in the same message, the server sends its own SYN flag and sequence number. The client then responds with an ACK message. So, the sequence is SYN, SYN/ACK, and ACK.
7. D. While ICMP may be used as part of passing control messages in case of errors in the network, it wouldn't be used between the IoT device and a server. SMTP is an email protocol that also wouldn't be used. Telnet is a cleartext protocol used to gain command-line access to a system. HTTP would commonly be used to pass messages between a controlling server and an IoT device.

8. D. Ring networks were once common but are much less so now. You may find a ring network in a service provider network today. A bus topology is best suited for a smaller network. Full mesh isn't a very common topology, in part because of the expense and complexity it brings. A star-bus hybrid would be common. An enterprise would use multiple switches that were all connected to one another over a bus, while all the endpoints would connect to the switch in a star topology.
9. B. A /23 network would be 255.255.254.0. A /21 would be 255.255.248. A /20 would be 255.255.240.0. Only a /22 would give you a 255.255.252.0 subnet mask.
10. C. The RFC 1918 address blocks are 10.0.0.0/8, 172.16.0.0/12, and 192.168.0.0/16. The only address listed that fits into one of those address blocks is 172.20.128.240. The address block is 172.16.0.0–172.31.255.255.
11. A. Manual pages provide documentation for commands and programs. IEEE is the Institute of Electrical and Electronics Engineers, which does manage some protocols but isn't documentation itself. Standards on the Internet are actually uncommon and happen only after a long period of time. The best place to find definitive documentation about protocols seen on the Internet is in the request for comments (RFC) documents.
12. D. At the Network layer, the PDU is a packet. The Network layer is IP. At the Data Link layer, the PDU is a frame. Commonly, the protocol would be Ethernet there. UDP uses *datagram* as the PDU. TCP uses *segment* for the PDU.
13. B. The source address is used as the address to send back to on the response, making it the destination address. The don't fragment bit is used to tell network devices not to fragment the packet. The acknowledgment field is part of the TCP header and not the IP header. The IP identification field is used to identify fragments of the same packet, as they would all have the same IP identification number.
14. C. The traceroute program uses UDP messages with the time to live field starting at 1. This is incremented for each hop in the network until the destination is reached. Each device would send an ICMP time

exceeded in transit message back to indicate the TTL had expired. The source of that message indicates the address of the network hop. On Windows systems, tracert uses ICMP echo request messages, also incrementing the time to live value. Because of these two factors, traceroute requires ICMP to work.

15. D. Systems over a VPN may use a MAC address, but they may also use IP addresses. The same would be true for a tunnel. Using TCP, we would use ports for addressing. On the local network, the MAC address is used.

Chapter 3: Security Foundations

1. C. Packet filters are used to make block/allow decisions based on header data like source and destination address and port. Stateful firewalls add in the ability to factor in the state of the connection—new, related, established. An application layer gateway knows about application layer protocols. A unified threat management appliance adds additional capabilities on top of firewall functions, including antivirus.
2. D. Confidentiality is about making sure secrets are kept secret. Integrity makes sure that data isn't altered accidentally or by an unauthorized agent. Nonrepudiation makes sure someone can't say a message didn't originate with them if it came from their identity. Availability means making sure data is where it needs to be when it should be there. This includes services as well.
3. A. Risk is the probability of the occurrence of an event multiplied by the dollar value of loss. There is no mitigation factor that is quantified, so it could be put into a risk calculation.
4. D. Switches and optical cable connections can certainly be part of a network design, but in and of themselves they don't add any security features. You may use Linux on the desktop, but without more of a strategy for patch and vulnerability management, Linux is no better than other operating systems. Access control lists on routers can add an additional layer of security, especially when combined with other elements like firewalls and intrusion detection systems.
5. B. Confidentiality is keeping secret information secret, which means unauthorized users can't access it. Encryption is a good way to keep unauthorized users from data because to get to the data, they need to have the key. Watchdog processes are used to ensure that programs remain running. Cryptographic hashes are used to verify the integrity of data. Web servers are used to serve up information.
6. C. Firewalls are used to block traffic into a network, though an intrusion prevention system will also block traffic. A packet filtering firewall uses header information, such as source and destination address and port, to determine whether to allow traffic into the

network. Syslog and the Windows event subsystem can be used to log system messages. Intrusion detection systems can be used to generate alerts on traffic.

7. D. If a user makes a change to a file and saves it, that's an intentional act and the data is what the user expects and wants. If the disk drive has flagged bad blocks on the disk, the drive won't write any data out to those blocks, so there will be no loss of integrity. Credit cards passed in cleartext would be a violation of confidentiality. Memory failures, though, could cause a loss of data integrity, even in the case of writing data to the drive. The corrupted data in memory could be written to disk. Also, memory failures may cause issues with the disk driver, which may also cause data corruption.
8. A. Security information event managers are used to aggregate event data, such as log information. Once the data has been aggregated, it can be searched and correlated. Even though it's called an event manager, it isn't used to manage security projects, nor is it used to escalate security events. Other tools can be used to gather and store open source intelligence.
9. C. Commonly, system logs are stored on the system that generated the log message. Certainly local systems can handle the logs they have generated. Log messages don't typically consume a lot of space at an individual message level, so bandwidth isn't a problem. Transmitting over a network is generally not faster than moving data within local disks. System logs can be used in identifying attacks, but the logs won't defend against attacks. However, if an attacker does compromise a system, the attacker may delete the local logs because they could get access to them.
10. B. In TCP, a three-way handshake is used to synchronize sequence numbers and establish a connection. While the sequence numbers are shared, they wouldn't be called aligned, which might suggest that each end was using the same sequence number. A SYN message is part of the three-way handshake, but it is not sufficient to establish a connection. Option A, “Final acknowledgment message,” is ambiguous. It could refer to the acknowledgment to a FIN message, closing the connection.

11. A. Standards and practices should be derived from a security policy, which is the high-level guidance on the role of security within an organization. Security does not generally increase the bottom line of a company. Policies are not for providing specific directions, which would be the role of procedures.
12. C. The Parkerian hexad takes the confidentiality, integrity, and availability of the CIA triad and adds utility, possession (or control), and authenticity.
13. D. While system shutdown, service startup, and package installation may be events that are logged, they are generally logged by normal system logging. Auditing functions are different between Windows and Linux/Unix, but audit systems for both will generate logs when a user logs into a system.
14. B. While an intrusion prevention system can generate alerts, so can an intrusion detection system. Both systems may also be able to log packets, as needed. A bogus message likely wouldn't result in a completed three-way handshake, and the handshake shouldn't be completed anyway. An intrusion prevention system can, however, block or reject network traffic, while an intrusion detection system can't.
15. A. Runtime application self-protection is a plugin used on an application server to prevent bad messages from impacting the application. A Java applet is an implementation of a Java program. An intrusion prevention system is used to detect and block potential intrusions. A web application firewall, however, makes decisions based on application layer traffic and will either allow or block that traffic. This makes it an application layer gateway.
16. C. A packet filter would use layer 2/3/4 headers to make decisions. An HTTP REQUEST message is at the Application layer (layer 7). Ethernet type isn't used to make decisions in a packet filter. SNMP OID is also an Application layer message. A packet filter would, though, use source or destination ports, potentially, to make decisions about allowing or blocking a packet.

17. C. Elastic Stack is an implementation of a security information event manager. Prewikka can be used along with an intrusion detection system as a dashboard. Snorby is an auxiliary program used with Snort. Snort is an intrusion detection program.

18. D. A buffer overflow attack is used to execute attacker-supplied code by altering the return address in the stack. A man-in-the-middle attack can be used to intercept and potentially alter a conversation between two systems. A heap spraying attack sends a lot of data into the heap to overwrite what's there. A watering hole attack does not compromise integrity since its purpose is to introduce malware to a system. The malware might eventually compromise integrity, but the watering hole attack itself does not.

19. B. A watering hole attack looks to compromise a system that visits a website. A phishing attack looks to gather information from victims, potentially by compromising the victim's system. A buffer overflow attack tries to introduce code provided by the attacker. A denial-of-service attack, however, has the intention of making a service unavailable for users.

20. D. An endpoint detection and response solution can be used to provide host isolation to endpoints as well as remote evidence collection and malware detection. Some companies use EDR solutions to replace anti-malware software since it can do that as well as perform other functions.

21. C. A firewall is a technical control, because it is hardware or software that is used to provide protection to an asset. It is not a policy or guideline, so it is not an administrative control. It may have a physical form, but since its purpose is not to protect against physical access, it is not a physical control. It may be both preventive or detective (logs can be used to identify malicious or suspicious behavior), but it is not corrective.

22. D. The business has not chosen to transfer the risk to someone else, nor have they chosen to not engage in the activity (developing the application) that would avoid the risk. Mitigation would mean they were doing something to reduce the risk. In this case, they are accepting the risk.

23. A. Standards are written down as guidelines that need to be followed to implement security policies based on business requirements. As they are documents, they are administrative controls. They are not corrective controls, though they may include recommendations for corrective controls. They are also not logical controls, which is another word for technical controls. There are no functional controls in the context of information security.

24. B. Security policies and standards are both administrative controls, not technical controls. A host-based firewall may not be effective against insider threat, since the insider is on a device where the host-based firewall exists already. Host-based firewalls on other devices may not be effective. A good identity and access management (IAM) solution can help to provide strong authentication and access control, which can keep insiders from getting to data they shouldn't have access to.

25. D. While the phishing itself would be categorized as initial access, registering the domain to be used for phishing would not. Credential access may be the goal, but again, registering the domain is not credential access. Registering the domain name is resource development, as the attacker is building infrastructure that can be used to attack.

Chapter 4: Footprinting and Reconnaissance

1. B. France is in Europe, and as such, it falls under the jurisdiction of RIPE. ARIN handles North America. AfriNIC handles Africa, and LACNIC handles Latin America and parts of the Caribbean.
2. D. The keyword site indicates the site (or domain) you want to search in. You need to provide either a domain, which would catch all FQDNs in that domain that were available in the search database, or a specific hostname. The keyword filetype indicates the file extension for the results. This keyword requires that a file extension be provided. There is no files or domain keyword that can be used in Google or other search engines.
3. A. PGP uses public servers and shared verification to store and validate keys and key ownership. Keys are owned by individuals as a general rule. If someone were searching at `pgp.mit.edu`, they would likely be looking for people and, most specifically, email addresses.
4. D. `p0f` can provide the uptime for some systems. Packets don't include any time information, so it's not possible to gather local or remote time. Absolute time would be based in a particular time zone, and time zones aren't communicated at the Network or Data Link layers.
5. C. A local caching server is what most people use to perform DNS lookups from their systems to get better performance. Recursion is the process used to look up DNS addresses from a caching server. Eventually, the caching server would ask an authoritative server for the information.
6. A. DNS requests from a local caching server start with the cache and then move to root servers and then subsequent servers, always getting closer to the final destination. This process of asking a question, getting an answer, and asking again using the new information is called *recursion*. Neither serial nor combinatorics make sense in this context, and bistromathics is a field of study invented by Douglas Adams for the book *Life, the Universe and Everything*.
7. B. It would be unusual to find executive staff identified in a job listing. It may be possible to get phishing targets, but it's not

guaranteed, and a single individual usually isn't identified. No financial records would be available in a job listing. Technologies used at a company, though, would be identified to ensure that the applicant has the right experience.

8. D. `whois` is used to inquire about domains, IP addresses, and other related information. `dig` is used to issue queries to DNS servers. `netstat` is used for network statistics. theHarvester, though, can be used to search across multiple sources, including Bing, Google, PGP servers, and LinkedIn.

9. B. While the others may include details about companies, only LinkedIn is primarily used as a business social networking site. People who have profiles there would list job titles, and job searches would indicate openings, including job titles.

10. A. Shodan is a website you would use to look for IoT devices. The query language is similar to that used by Google, except it has additional keywords that could be used to identify network traffic. This may include port numbers. `p0f` is used for passive network traffic analysis. You might query an RIR for information about an IP address block. The domain name for Shodan is `shodan.io`, but there is no I/O search.

11. D. Wappalyzer is an extension for the Chrome browser that can be used to identify technologies used in a website. It will, in part, use HTTP headers, but it doesn't identify the headers. It's also not used for analyzing web headers because there is more to what Wappalyzer does than that. It may look at some pieces of application code to get frameworks that are used, but it doesn't analyze application code in the traditional sense of application code analysis.

12. C. A DNS query can be used to identify an IP address from a hostname or vice versa. You could potentially use a brute-force technique to identify hostnames, though you may not get everything using that method. A recursive request is common from a caching server to get an authoritative response. The term for getting all the contents of the zone is a *zone transfer*.

13. B. When you run a `whois` query against an IP address, you will get the block the address belongs to, the owner of the block, and the technical contact. You will also get address information and possibly additional information. You will not get an association between a domain and the address block. This may be something you might infer, but it is not something that the results provide for you.

14. C. Google uses the keyword filetype: to identify filename extensions that should be searched. Administrator: is not a keyword, which means Administrator:500: is the search term that Google would use along with the filetype of txt, which would mean text files.

15. D. The command `whois` would be used to query the RIR for information about an IP address block. It could also be used to identify information about a domain. The program `netstat` is used for network statistics. `dig` can be used, but when you provide the `@` parameter, it would be followed by the name server you want to query. The correct way to look for name server records is to use `ns` as the record type. When you are looking for mail servers, you would look for the `mx` record type.

16. B. Mail exchanger records would be identified as mx records. A name server record is identified with the tag ns. While an enterprise may have one or even several caching name servers, the caching name server wouldn't be said to belong to the domain because it doesn't have any domain identification associated with it.

17. A. Twitter and Facebook are social networking sites. While you may be able to locate someone using a username, you may not be able to get detailed information about the user. Intelius is a person search site, and you can get detailed information there, but you can't search by username. PeekYou is a website that will allow you to search for people by either name or username.

18. C. LinkedIn is typically used for business networking, but there wouldn't be much in the way of detailed financial information there. Facebook is a social networking site, commonly used by people for social interaction. EDGAR is the database that is maintained by the SEC and includes filing information from public companies. MORTIMER is a joke. Bonus points if you recognize what the joke is.

19. D. The 10-Q is a quarterly filing. The 11-K form is related to stock options for employees. The 401(k) is a retirement account. The 14A report required by the SEC for public companies would include the annual report to shareholders.

20. C. New Zealand is located in Oceania, considered to be in the Pacific Rim. This means it falls under the Asia Pacific Network Information Center (APNIC). AfriNIC covers Africa. RIPE covers Europe, and LACNIC covers Latin America and parts of the Caribbean.

21. C. The TXT is a text record that can have multiple purposes. An MX record is for mail exchanger records, identifying the mail server for the domain. A PTR record maps an IP address to an FQDN. An NS record is one that identifies a name server for a domain.

22. B. PeekYou is used to perform people searches. Other tools are used for the other tasks.

23. A. The first query results in a canonical name, pointing `www.wiley.com` to `www.wiley.com.cdn.cloudflare.net`. An alias is a CNAME record. To get the IP address from an FQDN uses an A record. A PTR record gets an FQDN from an IP address and an MX record is the mail exchanger record.

24. A. `Pastebin.com` is a commonly used website for storing data. Typically, this is plaintext data. The intext: key says we are looking for some text in the page. This query suggests we are looking for a file of passwords on `pastebin.com`. There is no suggestion there are usernames and binary data is not stored on `pastebin.com`. It wouldn't be pasted passwords because there is a filename referenced.

25. C. Sherlock searches hundreds of social networks for usernames provided. This will give you a better idea of where individuals use specific usernames. It won't give you job information, look for fingerprints, or search domain registrars.

Chapter 5: Scanning Networks

1. C. A TCP scan sends messages to the target, expecting to get a response. With a SYN or full connect scan, the target will respond with a SYN/ACK message from an open port. With a closed port, the target will respond with a RST.
2. D. A SYN scan sends the first SYN message and then responds with a RST message after receiving the SYN/ACK from the target. A full connect scan completes the three-way handshake before sending the RST message. Since the full connect scan follows the correct order of the three-way handshake, it doesn't send an ACK first. There is also no PSH flag sent with the SYN flag, since there is no data to push up the stack yet.
3. A. There is no defined response to a message to a UDP port. It is left entirely up to the application. Since a lack of response can mean the message never reached its recipient, the scanning system has to retransmit to closed ports. UDP is generally quicker than TCP because of a lack of overhead, it requires no messages to set up, and it has the same number of ports as TCP.
4. C. When a system receives an ACK message, meaning a TCP segment with the ACK flag enabled (bit position storing a 1), it assumes there is an open connection and there is data that is being acknowledged. When there is no open connection, there is nothing to respond with. The system, not having anything else to do with the ACK, discards it. The scanner won't receive a response if the port is open. However, the scanner can't be certain that the message hasn't just been discarded by a firewall. As a result, it indicates that the port is either open or filtered. Either would result in no response. The scanner isn't guessing; it is providing two alternatives but can't be certain which it is. ACK is a supported flag in the right circumstances and ACK scans do not cause retransmits, since no response means one of two things.
5. A. Evasion is an important concept. You may spend a lot of time working on evading detection or getting blocked. Since an ACK without an open connection is aberrant, the firewall or IDS may ignore it, avoiding detection. As a result, you may be able to get ACK

messages through. ACK scans are not better supported. In fact, there is really no support from the network stack for an ACK scan. The code is no more robust in `nmap` for an ACK scan than other scans, or at least there is no evidence of that being the case. ACK scans are not needed for scripting support.

6. D. When `nmap` performs an operating system scan, it is looking for fingerprints of the network stack in the operating system kernel. Some of the information that `nmap` will look at is in the IP ID field to see what numbers are used. Similarly, it will look at the initial sequence number in TCP messages to see what numbers are used there. The application version isn't relevant to an operating system scan, and there are no operating system headers that would be associated with network traffic. Operating system headers could be considered to be part of the source code for the operating system, but `nmap` wouldn't be able to see those. Port 0 is considered an invalid port, so the response to a connection from that port is irrelevant.
7. B. A version scan with `nmap` is looking to identify versions of the services/applications running on the target. The kernel is identified with an OS scan. TCP and IP headers don't provide application versions. The IP ID field and TCP sequence number fields don't provide version information either.
8. C. The program `masscan` is a port scanner, like `nmap`. However, `masscan` was developed to scan the entire Internet as quickly as possible. As a result, if speed is a consideration, and especially if you are scanning large address blocks, `masscan` is probably better suited for that task. Both `nmap` and `masscan` have access to the same address space, and `masscan` uses the same command-line parameters, for the most part, as `nmap`, so they are similarly easy to use. `nmap` has also been around for considerably longer, since the 1990s, than `masscan` has.
9. B. `hping` is a program used to send specially designed messages to a target. You use command-line parameters to tell `hping` what to include in the message being sent. The command `hping -S -p 25 10.5.16.2` is used to have `hping` send SYN messages to port 25, the default SMTP port, at 10.5.16.2. It's possible that someone mistyped `ping`, but those parameters aren't used by ping programs, and since they are

coherent for the previous action, it makes more sense that they were trying to use `hping`. SNMP and web traffic both use different ports than port 25.

10. D. Vulnerability scanners don't exploit vulnerabilities to gain access to a system. They would only exploit a vulnerability to the extent necessary to determine whether a vulnerability exists. If they didn't know how to use Nessus or OpenVAS, they likely wouldn't be using them. It's possible they are looking to compare results from the two, but it's also likely they are trying to compare the results with the intention of reducing false positives.
11. A. A false positive is when a finding is identified when it doesn't actually exist. A false negative is when there is no finding identified but, in fact, there is a vulnerability. A true positive is when a finding is identified that is a vulnerability. A true negative is when a finding isn't identified and there is no known vulnerability.
12. D. There may be several reasons for performing a ping sweep. You likely want to identify responsive hosts on the network segment you are targeting. You may not, though, want to use a full port scan. ICMP is a lightweight protocol, and there is a chance it will be allowed through the firewall, since it's used for troubleshooting and diagnostics.
13. C. You would be expected to scan production servers, since that would be where you would be most interested to find vulnerabilities. Letting operations staff know ahead of time is polite since vulnerability scans may inadvertently knock over systems that would need to be stood back up. Being paged in the middle of the night unexpectedly isn't fun. If you know it's coming, it makes it easier. You may have reasons to use limited details in your scan reports, including trying to reduce the disk space used or the paper used in printing the reports. Taking no action on the results of a vulnerability scan is about the worst thing you can do when it comes to vulnerability scans. It's worse than not running them, since you could be considered liable, because you know about the vulnerabilities, but you aren't doing anything about them.
14. B. Scanning nonstandard ports isn't evasive. It's just as noisy as, and potentially more detectable than, scanning standard ports. You could

use a proxy for some tasks, but all it would do would be to hide your own IP address, which isn't evasive. You could still be blocked or detected. `nmap` does not have a blind mode. When you encode data, though, you make it harder for the firewall or IDS to identify something bad that may be happening, since these devices can't read the messages coming through.

15. A. Tunneling attacks can be used to hide one protocol inside another. They may be used to send operating system commands using a tunnel system. A DNS amplification attack is where a small DNS request results in much larger responses sent to the target. DNS recursion is used to look up information from DNS servers. An XML entity injection attack is a web-based attack and wouldn't be found inside a DNS request.
16. C. The Xmas scan is a TCP scan that uses unusual flag settings in the TCP headers to attempt to evade firewalls or IDSs. The Xmas scan uses the FIN, PSH, and URG flags and is called an Xmas scan because it looks like the packet is lit up like a Christmas tree. None of the other answers matches what an Xmas scan is.
17. B. MegaPing can be used to perform a lot of different functions, but crafting packets, sending manual web requests, and running exploits are not functions it supports. It can, though, run a port scan.
18. D. Plugins are matched to vulnerabilities. A different plugin would identify a different vulnerability and there is no way to change that. Scanner settings can be changed when you set up a scan. Using TCP rather than UDP is vague. If you want to change a severity rating from the one supplied by OpenVAS, you would override that rating. You may have mitigations in place, or you may have investigated and found the finding to be a false positive.
19. C. Credentials wouldn't give better reliability in network findings, and vulnerability scanners don't typically provide a way to directly authenticate through a VPN. The VPN client would be expected to be running ahead of time if the network is behind the VPN. An Active Directory scan is a vague answer, and it may not be something you can do with a vulnerability scanner. If you provide credentials, though, the

scanner can authenticate against systems on the network and check for local vulnerabilities.

20. C. The program `fragroute` uses configuration statements to determine what should be done to packets destined for a specific host. This may include fragmenting application traffic as well as duplicating and delaying traffic. While there is a possibility of fragmenting layer 3 headers, if layer 2 headers were fragmented, there would be no way to get the message to the destination.

21. A. `-f` is for fragment, and `--mtu` sets the maximum transmission unit for the frames. `-g` is used to set the source port, and `--spoof-mac` is used to randomize the source MAC address.

22. C. An idle scan is used to hide behind an unused system's IP address. MAC spoofing is used to take advantage of a trust relationship with a specific host. Fragmentation is used to evade IDS and firewalls. Since FTP and DNS are designed to come from specific source ports, sometimes firewall rules may be in place to trust the source port without looking at other aspects of the packet.

23. D. If your target were on the local network, you could use MAC spoofing. If you were remote, your target would never see the spoofed MAC address since it would be removed at the first layer 3 device, with a new layer 2 header and MAC address put on for sending on the other side. DNS is irrelevant to MAC spoofing and fragmentation is not necessary.

24. D. While every multiple of 8 is also a multiple of 2 and 4, only multiples of 8 will work for an MTU with `nmap`.

25. B. To perform a decoy scan, you would use the command-line parameter `-D` and then specify the decoy addresses you want to use, which can include specifying that `nmap` use random addresses. The other answers are incorrect.

Chapter 6: Enumeration

1. A. Remote procedure calls are a way for processes on one system to communicate with processes on another system. This does not preclude two processes on the same system communicating, of course. Semaphores are another concept in computer science that can enable interprocess communication. Remote method invocation is a way for Java programs to implement interprocess communications. Process demand paging isn't a thing.
2. C. `enum4linux` is a tool that makes use of other, underlying tools to scan systems that have implemented SMB. This means `enum4linux` can be used to enumerate shares or users, as well as other information. None of the other options is valid.
3. D. SNMPv3 implemented username and password authentication. With version 1, you used a cleartext community string. SNMP doesn't use hashes, and while the word *public* is often used to describe a community string, a public string is not a way to authenticate with SNMPv1.
4. C. The SMTP command used to expand a mailing list alias to get the underlying email addresses that belong to that mailing list or group is `EXPN`. The command `VRFY` is verify, and the other two are not valid SMTP commands.
5. B. The utility `dirb` uses a word list to attempt to enumerate directories available through a web server that may not be available by looking at all the pages and links in the site.
6. D. SNMP can be used to retrieve information from remote systems. This information has to be described, including the different datatypes. All of the information available is described in a management information base (MIB). The eXtensible Markup Language (XML) is a way of packaging data in a structured way, but it is not used in SNMP.
7. A. Interprocess communications across systems using a network is called remote method invocation. The process with which programs have to communicate to get a dynamic port allocation is the RMI

registry. This is the program you query to identify services that are available on a system that has implemented RMI.

8. C. The extended SMTP (ESMTP) protocol has a command that is abbreviated `VRFY` that is used to verify email addresses. A mail server may or may not have exposed this command, even if the server software supports ESMTP. Expanding mailing lists is EXPN. You wouldn't use `VRFY` for a mailing list in that same sense. The other two don't have specific commands that are specified in the SMTP protocol definition.
9. B. The Server Message Block (SMB) protocol is used for multiple functions on Windows networks. One of them is to transfer files (data) from one system to another. Email attachments would be transmitted using SMTP. NFS manages its own data transfer when files are being copied from one system to another. There are no data transfers specifically for Windows Registry updates.
10. D. The program `nmblookup` can be used on Linux systems. `smbclient` is a program that comes with a Samba installation that can be used to interact with a system using SMB. Metasploit has a lot of functions, but it's not built into Windows. The program `nbtstat`, though, can be used to gather information using SMB, and it is a program that is installed with Windows.
11. A. The status code you would get if your `VRFY` command failed against an SMTP server is 550. 200 is the status code for success with a web server. The other codes are not valid in this context.
12. B. The programs `smbclient` and `enum4linux` may be used to enumerate information using SMB. The program `snmpwalk` can be used to enumerate information over SNMP. `nmap`, though, can be used to enumerate services running on all the systems on a network.
13. D. Version 1 of SNMP used community strings. Version 2c also used community strings. Version 2 improved version 1, but it was version 3 that implemented user-based authentication as well as encryption.
14. A. The program `wpscan` can be used to enumerate themes, users, and plugins. It can't be used to enumerate administrators, specifically. It

also can't be used to enumerate posts, and since there would be only a single version, you wouldn't enumerate versions.

15. B. Metasploit can be extended with user-created programs. However, you wouldn't call a Metasploit module based on ports being open. Netcat doesn't do any enumeration, and `nbtstat` is a Windows program that can't be extended. `nmap` can be extended with user-written scripts. An `nmap` script includes a port registration so `nmap` knows to call that script when specific ports are found to be open.
16. C. SMB relies on remote procedure calls (RPCs) to function. The common Internet File System (CIFS) is an implementation of file sharing and system management using SMB. The Network File System (NFS) is a protocol that makes use of remote procedure calls. Remote method invocation (RMI) is a way to call procedures remotely over Java.
17. D. The `IPC$` share is a named pipe that enables interprocess communications over a network. While you may be able to do some remote management using the `IPC$` share, it is not used for remote process management.
18. B. The JRE is the Java runtime environment and is necessary to run Java programs. The JDK is the Java development kit and is necessary to develop Java programs. The program `rmic` is used to create RMI programs. It creates the stubs necessary for RMI to function. `rmir` isn't anything.
19. C. RMI is a way to implement interprocess communications using Java. Since Java is an object-oriented programming language, it would transmit objects. SMB is the Server Message Block protocol. SunRPC does remote procedure calls, but the data transmitted isn't object oriented. `nmap` is a program used to scan ports.
20. A. While `nmap` is an excellent program in its own right and can be used to enumerate data across multiple services, it doesn't store data for retrieval later without some additional help. Metasploit can also be used to enumerate data across multiple services and also uses a database on the backend to store data to be retrieved later. RMI is remote method invocation, a way to implement interprocess

communications across a network. PostgreSQL is the database server commonly used underneath Metasploit. Postgres is a much older version of what is now PostgreSQL.

21. D. The `VRFY` command in SMTP is used to verify addresses. The other commands here are essential to send email. The `VRFY` command is not essential and could be used to enumerate users.
22. C. V3 is the current version of SNMP. It allows authentication and encryption, unlike older versions of SNMP.
23. A. The latest NetBIOS patches won't protect an SMB service from having information collected from it. All the other answers are valid ways to protect against enumeration.
24. D. Workstation systems with shares configured by end users may have weaker permissions, which makes looking for shares there a good idea. As a result smb_enumshares is a good module to use. None of the others are going to be useful at enumeration on an endpoint.
25. B. An intrusion detection system may identify enumeration activities, but won't protect against it. Neither EDR nor anti-malware software will protect against service enumeration. A host-based firewall can restrict who can send network requests, which can reduce the possibility of enumeration.

Chapter 7: System Hacking

1. D. There are three date and time stamps commonly used in file metadata. When the file is created, that moment is stored. When a file is accessed by a user, that moment is stored. When a file is modified, that moment is stored. Accessed is not the same as modified since accessing a file could be read-only. You could open a file expecting to modify it, but not end up doing the modification. The access time still changes. While moves, adds, and changes may sometimes be referred to as MAC, like modified, accessed, and created, those are not tasks associated with file times.
2. A. Account migration, privilege migration, and account escalation are vague and don't have clearly defined definitions, even if they may exist. Privilege escalation, on the other hand, is used to gain elevated privileges when you only have the permissions of a normal user.
3. B. Incremental mode in John will run an attack in which it will try every possible password within specified parameters, meaning John will generate the passwords. The default mode in John is single crack mode, which uses information including the username and the home directory to generate a password using mangling rules. Incremental mode does not use wordlists, though John does support the use of wordlists.
4. D. Rainbow tables use precomputed hashes that are mapped to plaintext passwords in order to speed up the process of obtaining the passwords from stored hashes. Rainbow tables, though, are very expensive when it comes to disk space. Hashes and passwords are stored in the rainbow tables. Accuracy is neither sacrificed nor prioritized using rainbow tables. You will give up disk space to get faster cracking times using rainbow tables.
5. C. Local vulnerabilities are used against applications that are not listening on the network. This means they require you to be “local” to the machine and not remote. In other words, you have to be logged in somehow. A local vulnerability would not be used to collect passwords; you don't need a vulnerability to do that. Similarly, you don't need to make use of a vulnerability to manipulate logs or to

pivot. Most of those would require you to have elevated permissions, though. A local vulnerability may be exploited to get you those elevated permissions.

6. B. Manipulating time stamps on files is called timestomping. It is used to set file times, which may be used to throw off investigations or identify intrusions. None of the other answers is a real thing.
7. A. Alternate data streams are a function of the New Technology File System (NTFS), created to support the resource forks of Apple's file system in Windows NT. Since many of the utilities and programs in Windows don't natively understand alternate data streams, they can't make use of them and won't show them. The file can be accessed if the user knows how to display and manipulate the alternate data streams.
8. A. You may use a PowerShell script to perform functions that could support persistence on a system, but the PowerShell script alone won't be used to maintain access. Alternate data streams won't be of any use for maintaining access, and a `.vimrc` file is a startup file for the Vi editor. The run key in the Windows Registry, though, could be used to put an entry in that would run a program automatically that could make sure an attacker could get access even after a reboot.
9. D. While the Tor network may be used to obtain an exploit against a vulnerability, there is some question as to how reliable that exploit may be. The Tor network may contain malicious content, even in the case of source code. Meterpreter and `msfvenom` are elements of Metasploit that don't have anything to do with locating vulnerabilities. Exploit-DB is a website and repository of exploits that could be searched to locate an exploit targeting specific and known vulnerabilities.
10. C. The `clearev` command is a Meterpreter command used to clear the Windows Event Viewer logs. While you may be able to manipulate time stamps and log files in Meterpreter, you wouldn't use the `clearev` command for that. The `clearev` command does not allow an attacker to log in remotely.
11. B. When the Apache web server runs on a Linux system, it will commonly run as the user www-data. This is a privilege-restricted

account that would prevent an attacker from doing much on the system. To do anything, like wiping log files or pivoting to another network, you would need to elevate privileges to administrative/root level. Exploiting the web browser wouldn't be done in this context. A web server more than likely wouldn't even have a web browser installed.

12. C. Attackers often install extra files and run extra processes on systems. These could easily be detected by manual investigation or, certainly, by automated detection tools. The way around that is to install a rootkit, which may include kernel-mode drivers or replacement system utilities that would hide the existence of these files and processes. Alternate data streams may be used to hide files but not processes. Registry keys could also hide files but not processes.
13. B. Pivoting is the process of using a compromised system to move onto other systems and networks within the target environment. Pivoting does not get you higher-level permissions or persistent access. You may ultimately get to a database server by pivoting, but that's not what pivoting does or is specifically used for. It would be a nice side effect of pivoting.
14. B. The program `rtgen` is a program that is part of the `rcrack` suite. `rcrack` is used to crack passwords with rainbow tables. It is used to generate the rainbow tables that `rcrack` will use to crack passwords. Rainbow tables are not wordlists but mappings of plaintext passwords to hashes, which makes it much easier to get passwords from hashes.
15. C. Malformed packets could potentially cause a failure or trigger a vulnerability on the server side. Large ICMP packets aren't likely to do anything and certainly wouldn't exploit a client-side vulnerability. A brute-force password attack isn't exploiting a vulnerability, even if it is an attack technique. Sending a crafted URL could potentially exploit a client-side vulnerability in a web browser.
16. A. Steganography is the process of hiding data inside other data, such as media files like MP3s, WAVs, or video files. An alternate data stream is a secondary data stream attached to a filename in the NT file system. A rootkit can be used to hide processes. It may use process injection but wouldn't be the outcome from process injection. When

you inject into a process, you are putting executable operations you have created into the space of another executable. The end result could be an execution thread running your code without any new process name indicating it was running.

17. D. John the Ripper is used for cracking passwords, while `nmap` is used for port scanning. They could be part of the overall process of system compromise, but neither could be used to compromise a system, in spite of what it suggests in *The Matrix*. `searchsploit` is a program used to search a local Exploit-DB repository. Metasploit is an exploit framework that could be used to compromise a system. Once the system is compromised, Metasploit could then be used for post-exploitation actions using modules that come with it.
18. B. Of all of the options presented, only the web browser exists on the client side. By definition, the web server is on the server. A web application firewall is placed with the server to protect the server from Application layer attacks. Web pages are hosted on a web server. They are not a target for client-side exploits, though they would be used to carry out those attacks.
19. C. A rootkit is a piece of malicious software that is used to accomplish several tasks. This may include hiding processes and files through the use of kernel-mode drivers or replaced system utilities. A rootkit may also provide a backdoor for attackers to maintain long-term access to the system after the initial compromise. None of the other answers is a thing that a rootkit does.
20. B. John the Ripper and rainbow tables are tools for cracking passwords, not gathering or obtaining password hashes. Process dumping could possibly yield passwords associated with a certain process/application. However, you may not get password hashes, depending on how the passwords are maintained in memory. Process dumping is taking the memory space of a process and writing it out to disk for analysis. Mimikatz is a utility and Metasploit module that could be used to extract passwords from a compromised system.
21. B. You would use obfuscation on a PowerShell script. There may be some encoding that could happen as part of the obfuscation, but you may also use encoding for other, legitimate purposes. Rainbow tables

are used to crack passwords and Kerberoasting is a way of gathering password information over the network on Windows systems.

22. A. You would use Kerberoasting on a Windows network because the protocol used to exchange authentication information between user systems and servers is Kerberos. Fuzzing is a way of sending anomalous data to applications in the hopes of crashing the application. Rootkits are used to maintain access for an attacker and also obscure the existence of the attacker on the system. PowerShell scripting is used for a lot of reasons, but it wouldn't be the best way to collect passwords from a remote system.

23. D. Ruby isn't common enough to be used, and while Python is common on Unix-like systems like macOS and Linux, PowerShell is more common because it is installed by default on all current Windows systems and there are just more Windows systems around than the other platforms. Cmdlets are part of PowerShell but are not the language.

24. D. Rubeus is used to attack the Kerberos protocol on a Windows network. Ophcrack is a rainbow tables tool used for password cracking. John the Ripper is also used for password cracking. Peach is a tool that is used to perform fuzzing, which is the practice of sending anomalous data to an application, hoping to cause it to crash, which would suggest a new vulnerability.

25. B. Rubeus is a tool used against Kerberos-based networks. Empire is a set of PowerShell scripts used to attack Windows-based systems. Ophcrack is used to crack passwords. Meterpreter is the operating system–agnostic interface in Metasploit that is used after you have compromised a system.

Chapter 8: Malware

1. A. C2 servers are command and control servers. These are servers that can be used to provide management and control of bots in a botnet. The communication may be IRC or HTTP, but not necessarily. The servers aren't called that in a botnet anyway. ISC2 servers don't exist.
2. C. Both worms and viruses could be written to use polymorphic code, which means they could modify what they look like as they propagate. A worm, though, could self-propagate. It's the one distinction between worms and viruses. Viruses require some intervention on the part of the user to propagate and execute.
3. C. Static analysis is looking at the properties of the executable file and evaluating the assembly language code without running the program. This will limit your exposure to infection, because if you do it right, you aren't running the program, which would infect you. Dynamic analysis is trustworthy, and malware can't deploy if you don't run it. Dynamic analysis is commonly done in virtual machines.
4. D. VirusTotal takes dozens of antivirus engines and runs samples through them to identify what malware they might be. VirusTotal is a website, which means it can't check your system for viruses and also can't do any endpoint protection. While VirusTotal can identify the name given to a malware sample by different antivirus solutions, to find the research associated with that malware, you would need to check with the antivirus vendor.
5. D. PE files have multiple sections that you may find in an executable. Two that are very common, though, are `.text` and `.data`. The `.text` section includes all the executable code. The `.data` section includes all the predefined and initialized variables. The other sections listed in other answers aren't sections of a PE file.
6. B. Metasploit can be used to generate your own malware from one of the payload modules. Empire is another exploitation framework built around PowerShell. IDA Pro is a debugger, and Rcconsole doesn't exist.

7. A. All programs that have been compiled are in binary. Even scripting languages are in binary by the time they hit the processor. Packers will make a program smaller, which was initially of some value when bandwidth wasn't as ubiquitous, but a packer doesn't do any compilation. A packer does not remove null characters. A packer can, however, obscure the actual program code because the only executable function is one designed to extract and decompress the real malware.
8. C. Polymorphic means many bodies, which means it has multiple looks. When a program has multiple looks, it can cause antivirus programs to misidentify it. Polymorphic code rewrites the program when it is copied or moved from one system or location to another. It isn't more efficient and doesn't help with propagation, though it could be part of the propagation process. It also doesn't speed compilation.
9. B. Python interpreters may be considered slower to execute than a compiled program, but the difference is negligible, and speed of execution generally isn't much of a concern when it comes to malware. Python is not a hard language to learn, and there are a lot of community-developed libraries. One challenge, though, is that you may need a Python interpreter unless you go through the step of getting a Python compiler and compiling your script. Windows systems wouldn't commonly have a Python interpreter installed.
10. C. Cuckoo Sandbox is a set of programs and infrastructure used to run malware and identify changes to the system that result. This means it is used for dynamic analysis of malware, not for static analysis. Because it's automated, it's not manual. Also, it's used for analysis, not development.
11. B. You need a tool that can perform disassembly if you are doing static analysis. Dynamic analysis can make use of disassembled executables, but the tool would need to also be able to execute the code. IDA is the only tool there that does both disassembly and execution. Cutter only does disassembly. PE Explorer does neither, and MalAlyzer doesn't exist.
12. A. An executable contains a set of binary values that the CPU will interpret as operation codes (opcodes) when the program is run. These binary values won't generally mean much to people when they are

bare. As a result, disassemblers are used to convert opcodes to mnemonics, which are short/abbreviated words that can let someone know what the opcode does.

13. C. A dropper downloads (drops) additional files, which may be malware. It doesn't do any of the things mentioned in the other options.
14. B. An encoder is used to alter the look of an executable file. This alteration is done to prevent the antivirus program from recognizing the executable as malware. It doesn't compile the malware and doesn't evade user detection. A packer would be used to compress malware.
15. B. The program `msfvenom` is used to convert a payload module from Metasploit into an executable program. The malware could potentially be used as part of a poison pill, which is a type of defensive tactic, but it's hard to determine that just from the command line. While the malware is encoded as part of this process, it is not an existing piece of malware. This is not a way to start Metasploit, though `msfvenom` does make use of the Metasploit framework.
16. A. This is a bit of a trick question. Ransomware may be a virus, which means it is a subset of the category virus. Ransomware may ask to be paid in Bitcoin, but it doesn't include Bitcoin. Ransomware has been generated all over the world, and viruses run on all operating systems.
17. C. A Trojan, also called a Trojan horse, appears to be one thing but is, in fact, another. It can fool users into running the malware because they are expecting something else. A Trojan can't evade antivirus if there is a signature that matches the executable. It doesn't act as malware infrastructure, and while it may be polymorphic, that wouldn't be why someone used a Trojan.
18. B. When you are trying to dynamically analyze malware, a debugger is useful because it allows you to run the malware and also control its execution. OllyDbg is the only debugger in that list. Cutter does disassembly but does not allow you to run the malware and control its execution.
19. C. Traditional command and control (C2) infrastructure is made up of a client and a server. The client is the software on the infected system. The client communicates with the server, which sends command and

control messages to the client. Neither satellite nor master station are elements of C2 infrastructure.

20. D. The firewall may block inbound communications, which is why it's better for the communication to originate from the inside. Either direction could be caught by intrusion detection. Virtual machines don't factor in here, and antivirus could catch the malware regardless of which direction the traffic is going, since antivirus uses the executable file rather than the communication stream for detection.

21. B. Obfuscation is the process of making it difficult to read or analyze a program. Disassembly lets us convert opcodes to assembly language. Packing is compressing an executable, which can make it difficult to understand.

22. C. The strings utility could be used to perform a superficial analysis of an executable to get information like library names out. Hashing could be used to identify malicious files if that malicious file is known and the hash is in a database. Metasploit is used to attack systems. Ghidra is a tool developed by the NSA that does some of the work of a disassembler while adding additional tools for malware analysis.

23. D. Data loss is not the only potential impact from ransomware, but if you are concerned about data loss, having a good backup practice will help protect against that data loss. Anti-malware, endpoint detection and response, and indicators of compromise won't protect you against data loss.

24. A. Since some ransomware uses file encryption to deny typical access to data, a decryptor could be used to recover from this type of ransomware attack. The encryptor would already have been used, and it's not helpful here. Neither endpoint detection and response nor anti-malware is of any use after the ransomware has encrypted files.

25. C. Anti-malware software can identify anything in a running system. Pre-boot malware, though, can hide and protect itself by intercepting system calls that may allow the anti-malware to work correctly. Only by loading before the operating system can malware evade detection. All the other answers can be picked up by anti-malware with updated signatures and behavior analysis techniques.

Chapter 9: Sniffing

1. C. Different vendors use different terms to refer to port mirroring. Cisco uses the term Switch Port Analyzer (SPAN), which leads to the process sometimes being called port spanning.
2. B. The expression host 192.168.10.5 is BPF, indicating that `tcpdump` should only capture packets to and from 192.168.10.5. If you wanted to only get it to or from, you would need to modify `host` with `src` or `dest`.
3. D. `tcpdump` uses the format *hostname/IP.port* when it prints an address. The addresses go source > destination, so yazpistachio.lan is the hostname, and 62882 is the port on the source address.
4. A. By default, `tcpdump` does name resolution. Not only does `tcpdump` look up port numbers and print their service names, it also triggers a DNS lookup. This DNS lookup is network traffic, which means that for most packets there is probably a DNS lookup request showing in the packet capture.
5. C. BPF operates at the Data Link layer. This allows filtering down to the MAC address. If BPF operated at other layers, you wouldn't get the entire set of packet headers.
6. C. When an ARP response is sent without a corresponding ARP request, it's an unexpected or unnecessary message. This makes it a gratuitous ARP.
7. C. While conversations and endpoints are statistics you can get from Wireshark, the protocol hierarchy view shows a layered look at all the protocols in the capture, showing percentages for all of the protocols.
8. D. While `tcpdump` and `tshark` can both be used to capture packets, `tshark` gives you the ability to specify which fields you want to output. The other two options don't exist.
9. C. By default, Wireshark shows a relative time since the start of the packet capture. You can change the field to show absolute time, such as the time of day or the time since 1970 (epoch time). However, that's not what is shown.

10. D. After the frame number, time, source IP, and destination IP is the protocol. This frame shows that TCP is the protocol in use.
11. C. `arpspoof` and Ettercap can both be used to perform ARP spoofing. Ettercap also supports other types of spoofing attacks and plugins. `sslstrip` is a plugin supported in Ettercap. `fragroute` is a program that does something completely different.
12. C. A DNS spoofing attack requires that the program can see the DNS request to respond to it. This means there needs to be an ARP spoof in place so Ettercap (or another tool) can get the traffic on the network to get the DNS request to respond to.
13. A. The `-i` flag indicates which interface you are going to listen on. The `-n` flag tells Wireshark to not do name resolution, leaving you with numeric values for the IP address and port number.
14. B. The number of MAC addresses can be smaller than the number of layer 3 addresses because multiple IP addresses could be associated with a single MAC address if the IP addresses are off network; the MAC address for those would be the gateway's MAC address. If a system opens multiple connections to the same system, as may happen when rendering a web page, there would be multiple port combinations for the same IP source and destination.
15. A. `sslstrip` is used to get plaintext traffic. It does not remove SSL requests, though it may be used to convert an HTTPS request to an HTTP request. It does not convert SSL to TLS or TLS to SSL, and there would be no particular advantage to either of those tasks.
16. B. `sslstrip` was released in 2009 and took advantage of problems in SSL. These problems not only existed in SSL but also continued through early versions of TLS. Newer versions of TLS don't have the same issues, which means `sslstrip` won't work with them.
17. A. Wireshark presents a relative sequence number, which means the initial sequence number as far as Wireshark is concerned in presenting it to you is 1. The relative sequence number increments just as the real sequence number does. The real sequence number, which is a very large value, is hidden to make analysis easier.

18. B. Anything you see in Wireshark that is in square brackets, [], is something Wireshark has calculated or inferred. It is not something that has been extracted directly from the packet capture. Wireshark is helping with the packet analysis.

19. C. Switches filter traffic by only sending traffic destined for the MAC address associated with the port to which the system that owns the MAC address is attached. Switches are reliable. They don't support layer 3 as switches, though there are such things as multilayer switches that include routing functionality. Either way, that's not something that port spanning overcomes. Switches may aggregate ports, but port spanning doesn't have anything to do with that.

20. B. The `ipchains/iptables` command to turn on redirection for Ettercap is done in a different file. In the `etter.dns` file is the mapping of hostnames to IP addresses as well as other DNS resource records.

21. C. In the flags, you can see PROMISC, which is an indicator the interface is in promiscuous mode. This is necessary for a system to be sniffing network traffic. Without promiscuous mode, the system only gets packets that are specifically addressed to it. While the other attacks could also be happening, the only thing we can say for sure based on this output is that the interface is in promiscuous mode, suggesting there is network sniffing happening.

22. A. A DHCP starvation attack could result in a denial-of-service condition, or it could result in an attacker being able to send configurations to endpoints with rogue default gateways or rogue DNS servers. The attack itself would not result in an attacker getting a new IP address.

23. C. A large number of DHCPDISCOVER messages is a resource exhaustion attack, trying to deplete all the IP addresses available on a DHCP server. This is a DHCP starvation attack. ARP spoofing would use ARP messages. DNS poisoning would be manipulating the DNS server and network sniffing would be putting a local network interface into promiscuous mode.

24. C. Switches ensure only traffic specifically addressed to a host is sent on to the port that host is connected through. Hubs will send all traffic

to all ports. DHCP is responsible for dynamic host configuration and has no impact on sniffing. You don't need an IP address on your interface to sniff. The mail server would have no impact on sniffing.

25. D. `sslstrip` takes advantage of a vulnerability in the SSL/TLS encryption. This was resolved in later versions of TLS. Versions of SSL would be vulnerable, as would earlier versions of TLS. TLS v1.3 would not be susceptible to an `sslstrip` attack.

Chapter 10: Social Engineering

1. A. Biometrics is the use of a physical attribute to provide authentication. Smishing is using short message service (SMS/texting) to gather information from people. Rogue access isn't really anything. Pretexting is coming up with a believable story that you can use when trying to perform a social engineering attack on someone.
2. C. Baiting is leaving a lure out in order to gather targets. You could use USB sticks or CDs around as bait if they had software on them that would run and "infect" the target system in a way that would give you control over them. While all of the other options are related to social engineering, none of them is called baiting.
3. B. Social proof is in use when it appears to be okay to engage in a behavior because you see others engaging in it. When people see a line of others waiting to grab USB sticks, in spite of knowing they shouldn't trust USB sticks, they may be inclined to lower their defenses. There is no reciprocity or authority here. There may eventually be scarcity, but that's not what would drive people to stand in line to acquire a potentially dangerous item.
4. D. Biometrics and badge access are forms of physical access control. Phone verification could possibly be used as a way of verifying identity, but it won't protect against tailgating. A man trap, however, will protect against tailgating because a man trap allows only one person in at a time.
5. B. Especially in enterprises, there is generally some authentication that happens. This could be in the form of a pre-shared key or a username/password combination. Either way, when you are using social engineering of wireless networks, you are probably attempting to gather credentials to gain access to sites. It's unlikely you'd use this vector for sending phishing messages or getting email addresses, and it wouldn't be used to make phone calls.
6. D. While you might be imitating someone, imitation is not a social engineering principle. Neither social proof nor scarcity are at play in this situation. However, if you are calling from the help desk, you may be considered to be in a position of authority.

7. B. It's debatable whether you get better control over outcomes executing your attacks manually. You would not be implementing social proof or demonstrating authority using an automated attack any more than if you did it manually. You would be reducing complexity, though, since doing it manually means you would be setting up and controlling multiple moving pieces. This gets to be complex, and the attack would fail if you didn't get it just right.
8. A. Vishing and smishing are nonkinetic approaches to social engineering. Scarcity is not a social engineering vector. Impersonation is a social engineering vector and the one used to gain unauthorized access to a facility.
9. C. If you sent an email posing as a former coworker, you could be implementing a couple of different social engineering principles. Because you have a story and a means to collect information fraudulently, you are using pretexting. The other attacks are also social engineering, but they are not pretexting.
10. C. `wget` is the only one of these options that is a legitimate program, and it can be used to clone a website.
11. B. While some people do epoxy USB ports to prevent USB sticks from being inserted, it's not a good approach and wouldn't necessarily keep a baiting attack from working if the bait is a CD-ROM. Browsing the Internet is common, and no longer doing that won't protect you against baiting. Registry cloning isn't really a thing in this context. Disabling autorun would keep any malicious software from running automatically from external devices.
12. D. A false acceptance rate measures how often a biometric system allows unauthorized users access to a facility or area. A false failure (or reject) rate is inconvenient, and some organizations may consider that to be an issue, especially if it's very high. However, a high false accept rate is probably more concerning because you are allowing people who are really unauthorized to have access. The other two are not statistics that are measured; though they correlate to the others, they are not called false positive rate or false negative rate.

13. A. Voiceprint identification is the least reliable of these options. As a result, it would be the most likely to give you a high false reject rate, which would lower the true accept rate.
14. D. A proximity card could enable tailgating, but it's not the only thing —a key could enable tailgating as well. Technically, it's not the card that allows tailgating anyway. It's the way the doors are configured and implemented. Phishing is unrelated, and technically, credential theft is as well. Proximity cards, particularly if they use RFID tags, are susceptible to cloning.
15. C. While the retina and the uvea are also parts of the eye, neither of them encloses the pupil. Fingerprints are not part of the eye.
16. A. A false acceptance rate would be allowing unauthorized people in. If you are an authorized person but your biometric scanner isn't working reliably and rejects you, you may need to call security or someone else to let you into the building. Neither of the other two would be a result of a high false failure rate. They may be solutions to other problems, but not a high false failure rate.
17. B. Smishing is short message phishing, which means someone is sending a text message, attempting to fraudulently gather information. Vishing is a phone call (voice). Phishing can be an overall term but commonly refers to email. Impersonation is more of a physical approach.
18. A. Pretexting can work over email just as well as via a phone call. It may be more common for people to have email than a phone, especially a company-owned landline. Phishing attacks are successful, which is why they are so commonly used. With a phone call, though, you could go into more detail and address questions or concerns as they arise. You could include additional layers that you couldn't with an email since you could never be sure if your email was read, deleted, or caught in a filter.
19. B. The captive portal is the page that is opened when you connect to a public access point. None of the other answers is a real thing.
20. C. You may end up with a Meterpreter interface to a remote system, but it wouldn't be used to generate the attacks. `wifiphisher` is used

only for Wi-Fi–based attacks, and Social Automator doesn't exist. The Social-Engineer Toolkit (SE Toolkit) could be used to automate email attacks as well as wireless attacks.

21. D. Pretexting is the story you are using to explain why you are getting in touch with someone. Identity theft is when someone steals personal information to commit fraud. Contact spamming is when you have compromised a user's email account and send a lot of email to their contacts. Baiting is when you leave something like a USB stick with malicious software, hoping someone will plug it into their system in order to compromise it.
22. C. Quid pro quo is something for something. There isn't something for something in this case. You have not been cloned, nor has your email account since there can only be one instance of an email account at a time. Man traps are used for physical security. This is contact spamming and your account is likely compromised.
23. B. The first book you ever read, assuming you can remember, is unlikely to be useful to an attacker. The Social Security number identifies you and could be very useful in stealing an identity. The other information is often used to verify an identity, so would also be useful.
24. B. It seems unlikely the attacker would pretend to be your mother since you'd know if it were your mother calling. Your car dealer wouldn't be able to get much out of you, especially if you aren't currently looking to get a car. Hopefully your dog isn't asking questions of you. Help-desk staff may offer “tech support” while also asking for credentials so they can help you out.
25. C. All of the others are good ways to protect your personal information. Encrypting your file system may do nothing at all to protect your personal information if there is no personal information stored there. Additionally, if your account was compromised, data on the file system would be accessible as your user account, meaning the attacker would get access to it.

Chapter 11: Wireless Security

1. D. An infrastructure wireless network is one that uses an access point. An ad hoc wireless network is one organized by the participants. These are the two types of wireless networks. Star, ring, bus, and hybrid are all wired topologies.
2. B. There are four stages used in a WPA handshake. This four-stage process is used to derive the key and agree on capabilities.
3. B. Promiscuous mode is used on network interfaces to collect frames that are not destined for the network interface. This is insufficient on a wireless network because the radio headers are not captured. To capture radio headers, monitor mode needs to be enabled in addition to the promiscuous mode that will always be set to get all frames and all information from the frame. Only monitor mode gives the radio headers.
4. C. Sniffing can be used to collect information that may be needed to launch wireless attacks. A deauthentication attack can be used to force a station to generate traffic. An evil twin attack uses a rogue access point to pretend to be a legitimate network. In order to decrypt network traffic, you would need the key. One way to get the key is to reuse information from network traffic that generated a known key. This is a key reinstallation attack.
5. C. Bluetooth doesn't use ports. While profiles are important, you get the profile capabilities during the pairing process. Just performing a scan won't get you a list of supported profiles. While you should be able to identify vendors as part of the process of running a Bluetooth scan, it's not the purpose of the scan. The purpose is to identify endpoints and their associated addresses so you can run other attacks on them.
6. B. The purpose of a deauthentication attack is to force stations to reauthenticate. This allows the attacker to collect information from the authentication and handshake. This information could be used later to potentially derive the key, as in WEP transmissions. A deauthentication attack doesn't disable stations. There is no way to

reduce the number of steps in a handshake, and downgrading encryption is considerably harder, if it's possible at all.

7. A. Bring your own device (BYOD) is a policy that allows employees to use their own devices on an enterprise network. This opens the door to the potential for attacks from unknown and unexpected devices. None of the other answers is a real thing.
8. C. The initialization vector is a random value that seeds the key used for encryption and decryption. In WEP, the algorithm specified for the initialization vector yielded nonrandom, predictable values. While the initialization vector is part of keying, it's not the keying itself that was weak. Seeding vector is not a real thing, and Diffie–Hellman is a process used to derive and exchange keys securely. It's not part of WEP.
9. B. The four-stage handshake is used to authenticate stations against wireless networks. As part of the handshake, encryption keys are generated. Keys are derived on both sides of the transaction rather than being exchanged directly. This is handled during the four-stage handshake. Keys are not passed. Messages can't be encrypted until the four-stage handshake is complete and the keys are generated. There is no such thing as initialization seeding.
10. C. The service set identifier (SSID) is used to identify a network. It is the name of the network you would select when you were trying to connect to a network. The SSID is not the MAC address, and it has nothing to do with keys or encryption.
11. D. Ad hoc and infrastructure are types of wireless networks. Only infrastructure uses access points, but infrastructure is not a type of access point. WPA is an encryption protocol. A rogue access point, meaning one that isn't legitimate, is used in an evil twin attack by pretending to be a legitimate access point.
12. B. An evil twin attack uses an access point masquerading as the point of connection for stations trying to connect to a legitimate wireless network. Stations reach out to make connections to this access point masquerading as another access point. While you may phish for credentials as part of an evil twin attack, credential phishing is not how

evil twin attacks work. SSIDs don't get changed as part of an evil twin attack, meaning no SSID that exists will become another SSID. Injecting four-stage handshakes won't do much, since four-stage assumes both ends are communicating, so the injection of a full communication stream will get ignored.

13. C. The Apple App Store and the Google Play Store are controlled by Apple and Google. It's not impossible to get malware onto mobile devices through them, but it's difficult because apps get run through a vetting process. While some Android devices will support external storage, it's not an effective way to get malware onto a smartphone or other mobile device. Jailbreaking can lead to malware being installed, but it's not the means to get malware onto a mobile device. Third-party app stores can be a good means to get malware onto mobile devices because some third-party app stores don't vet apps that are submitted.

14. B. A bluebugging attack is used to gain access to a smartphone to initiate a call out to the attacker's phone. This allows the attacker to listen to anything happening around the phone owner. Scanning is used to identify Bluetooth devices nearby. There is no particular attack used to enable a phone's camera. Gathering data from a target device or system is bluesnarfing.

15. A. While there are Bluetooth devices that will transmit much farther, a common range is about 300 feet (100 meters) for Bluetooth 4.0.

16. D. `tcpdump` can be used to capture frames/packets. Ettercap is used for captures and spoofing attacks. Neither can capture all headers, including radio headers in a wireless network. The package `aircrack-ng` includes the program `airmon-ng`, which can turn on monitor mode on a network interface. The program `aircrack-ng` itself cannot do that.

17. B. Bluesnarfing is an attack that connects to a Bluetooth device to grab data from that device. Bluesnarfing sends data to the attacker. Bluejacking can be used to send information to a Bluetooth device, such as a text message. Neither of these attacks installs a keylogger.

18. C. Wireshark is used to capture packets/frames from a network. Ettercap is used for spoofing attacks. The program `aircrack-ng` can

be used to crack wireless keys. `wifiphisher`, though, can be used to set up an evil twin attack.

19. B. WPA supports both Personal and Enterprise authentication. Personal authentication makes use of a pre-shared key, while Enterprise authentication uses usernames and passwords to authenticate specific users, providing accounting and access control, meaning we know exactly who has connected to the network.
20. D. Radio headers in a wireless network will provide you with the capabilities of the devices, since that's negotiated during the association process. You will also see probe requests asking what networks are in the area, including specific networks that a station knows about. These requests will include the SSID. The responses will also include the SSID. You will not get the network type in the headers.
21. C. WPA3 uses the simultaneous authentication of equals (SAE). Previous versions have used the four-stage handshake alone. The other two answers are not real.
22. D. The Bluesmack attack is a denial-of-service attack that is caused by manipulating packet sizes sent to a victim system. The other attacks are Bluetooth but do not result in a denial-of-service attack.
23. B. A Pringles can may be used to increase the wireless signal, so it is helpful for wireless footprinting or wardriving. Evil twin is used to mimic an existing wireless network. Key reinstallation is another type of wireless attack. Bluesnarfing is a Bluetooth attack and wouldn't require a Pringles can.
24. A. The BDADDR is needed to perform a Bluedump attack. An IP address would not be used in a Bluetooth attack. The other answers aren't real things.
25. D. Plywood and sheetrock effectively offer no resistance to a wireless signal. Glass offers minimal resistance. If you wanted to keep your wireless signal inside your building, you should use concrete as a building material. Masonry blocks and bricks would also work well.

Chapter 12: Attack and Defense

1. B. While DNS is also used for amplification attacks, Smurf attacks are a result of someone sending ICMP echo requests to the broadcast address of a network. The echo responses would be sent to the address in the source of the request, which would be spoofed. If enough systems respond, the volume of responses can overwhelm the target system.
2. C. An SQL injection attack makes use of SQL queries, which can include logic that may alter the flow of the application. In the example provided, the intent is to force the result of the SQL query to always return a true. It is quoted the way it is to escape the existing query already in place in the application. None of the other attacks uses a syntax that looks like the example.
3. C. Because TCP uses a three-way handshake, spoofing like that needed in amplification is difficult. SMTP also uses TCP. XML is used for data structure and presentation. DNS is often used for modern amplification attacks.
4. A. A SYN flood takes advantage of the three-way handshake. A SYN message alone will consume a connection buffer at the operating system. Until the operating system has passed the three-way handshake, the request won't make it to the web server at the Application layer. SYN is not a header flag used with UDP.
5. B. A slowloris attack is used to hold open connection buffers at the web server. Enough of these requests will consume all of the possible connections for the web server. The Application layer doesn't factor in here because there are no connection buffers at the Application layer. Web servers don't use UDP for HTTP requests, and slowloris is an attack against a web server.
6. C. Heap spraying uses dynamically allocated space to store attack code. A slowloris attack is used to hold open web server connection buffers. An SQL injection will be used to inject SQL queries to the database server. A buffer overflow sends more data than space has been allocated for into the application.

7. D. A cross-site scripting attack uses a scripting language to run in the browser. Since the browser is with the user, ultimately the attack targets the user, even if the injection code is stored in a database server.
8. D. Cross-site scripting attacks usually use JavaScript or perhaps VBScript. SQL injection uses SQL. Command injection uses operating system commands. The fragment shows XML using an external entity. This is, then, an XML external entity injection.
9. B. SQL injection attacks take data injected from the user/attacker. Any data sent in from a user should always be validated before being acted on. Nothing coming in from a user should be trusted. None of the other answers could be used to prevent an SQL injection attack.
10. A. A defense-in-depth network design makes use of multiple prevention layers to make breaching the inside of the network quite a bit harder. A SIEM is used to collect and correlate intelligence and log data. A web application firewall protects against Application layer attacks. A log management system is just what it says. A firewall, though, is commonly used in a defense-in-depth network design.
11. A. Defense in breadth starts with defense in depth and takes a broader range of attack strategies into consideration. Defense in breadth doesn't necessarily protect against SQL injection and probably doesn't protect against buffer overflows or heap spraying attacks. Those protections may possibly be achieved, but ultimately defense in breadth would achieve them by taking a broader range of attacks into consideration.
12. C. A buffer overflow attack is an attack against data in the stack, which is known about at compile time and, as a result, is not dynamic. Cross-site scripting attacks and slowloris attacks don't inject code into memory. A heap spraying attack, though, injects code into the heap, which is where dynamically allocated memory is taken from.
13. C. A buffer overflow takes an excess amount of data and tries to store it into a memory location that can't accommodate it. An SQL injection attack uses SQL. Command injection attacks use operating system commands. A cross-site scripting attack uses a scripting language such as JavaScript or VBScript. The script is injected using a `<script>`

HTML tag, and the `%3C` is a way of encoding < while `%3E` is a way of encoding >. This means `%3Cscript%3E` would be decoded to `<script>`.

14. B. Base64 encoding takes nonprintable characters and encodes them in a way that they can be rendered in text. Encryption would generally render text unreadable to people. A cryptographic hash is a way of generating a fixed-length value. URL encoding takes text and uses hexadecimal values to represent the characters. This is text that has been converted into hexadecimal so the characters can be used in a URL.
15. D. A slowloris attack uses small HTTP requests to hold open a web server's available connections. There are attacks that use body requests in a slow fashion. However, a slow read attack tries to download a file in small increments to keep a web server from serving legitimate requests.
16. D. While a firewall and an IDS will generate logs, they don't collect them. A log manager will collect logs and perhaps aggregate them, but it probably doesn't correlate log messages. A SIEM, though, will consume logs, aggregate them, and correlate them.
17. A. A command injection sends operating system commands into a web application so they can be run by the operating system. The web server (meaning the web server application) is not the target of the command injection, nor is the database server or the user.
18. C. The Low Orbit Ion Cannon is a .NET-based application used to launch denial-of-service attacks. It is not used for log management or SQL injection attacks, nor is it used for buffer overflows.
19. B. SIEM output is useful and may have some value in understanding current attacks. The same is true with logs and intrusion detection systems. However, the attack lifecycle is a structured way to understand how attacks happen in order to better inform a defensive strategy so controls can be implemented for each of the phases of the attack.
20. C. The stack pointer indicates where the stack is in memory. The frame pointer indicates which part of the stack is being used for the current frame. There is no buffer pointer from the perspective of the

operating system, though applications do use pointers and they do point to buffers. An instruction pointer tells the processor where the next instruction to be executed is. Controlling this piece of information can allow the attacker to control the execution flow of the program.

21. B. A web application firewall could be used to protect against web application attacks, including SQL injections. While it can be used for detection, a WAF could be used to block these attacks. Return to `libc` is a way to get around protections against buffer overflow attacks. Address space layout randomization and stack canaries are ways of protecting against buffer overflow attacks.

22. D. A file traversal attack attempts to break out of the jail that a web server uses to contain interaction to a specific set of directories and files. Cross-site scripting attacks user systems through the browser. SQL injection attacks are targeted at database servers, while command injection attacks target the operating system by trying to inject shell commands into the application to be executed by the underlying system.

23. D. Defense in depth commonly focuses on protection, while defensible network architectures focus on being able to contain attackers as well as monitor attacker activity. A DMZ is a way of protecting the broader network from an attacker. Firewalls are used to protect, and honeypots are deceptive mechanisms. Malware protection is all about protection.

24. C. A honeypot is used to lure an attacker in, providing enough content of interest to keep them busy on that system while you can monitor them. Different firewalls can be used to block bad traffic but would not be used to trap an attacker. A DMZ is a way of isolating Internet-facing systems from other parts of the enterprise network.

25. A. A stack canary could be used to detect a buffer overflow attack. A buffer overflow is an attack technique. Return to `libc` is a way of making use of a fixed, known address to jump to during a buffer overflow attack. There is no such thing as a return to JavaScript.

Chapter 13: Cryptography

1. C. This is a rotation cipher with a key of 4. When you rotate the alphabet by 4, you end up with e = a, r = n, w = s, and so on. In addition to not being the right decryption, none of the others has the correct number of letters. In a substitution cipher like a rotation cipher, you will always have the same number of letters in the output as you do in the input.
2. B. In cryptography, any data or message that is in an unencrypted state is called plaintext. The output from a cryptographic process is ciphertext. While you may have text as input to an encryption process, the word text would be ambiguous in this context. The other two are unrelated to cryptography.
3. C. Where certificate authorities use a centralized mechanism for verification of users or certificate subjects, PGP uses a decentralized model. PGP calls this a web of trust, where individual users sign keys that belong to other people to validate that they are who they say they are. All of the other answers are made-up terms.
4. A. Integrity is part of the CIA triad but isn't the principle that ties a signed message back to the subject of the signing certificate. Nonverifiability is nonsense, and authority isn't relevant here. Instead, nonrepudiation means someone can't say they didn't send a message if it was signed with their key. This assumes the key was in their possession and password protected, meaning no one else could use it.
5. C. Certificates can be revoked, but that's not what Diffie–Hellman is used for. Key management is a much broader topic than key exchange, which is what Diffie–Hellman is used for. It is a process that allows two parties to an encrypted conversation to mutually derive the same key starting with the same base value.
6. D. 3DES, or Triple DES, uses three keys. The first key is used to encrypt the plaintext. The second key is used to decrypt the ciphertext resulting from the first round of encryption. Finally, the third key is used to encrypt the ciphertext that resulted from the decryption with the second key. The key wasn't made longer because the 168 bits used

in 3DES aren't used in a single key. The underlying DES algorithm is still used.

7. A. Algorithms used for elliptic curve cryptography are not more complex necessarily. While they don't use factoring, that fact alone doesn't necessarily make the algorithms better. Instead, elliptic curve cryptography relies on the assumption that a discrete logarithm of a point on an elliptic curve can't be computed in a consistent way. The keys that result from elliptic key cryptography are actually smaller than those that result from factoring with large prime numbers.
8. B. When two different data sets yield the same cryptographic hash, it is called a collision. It relates to a mathematical problem called the birthday paradox, but two values being the same is not a paradox. It's also not unrealistic, nor is it a crash.
9. C. Asymmetric key cryptography uses two related keys. One key is used for encryption, and one is used for decryption. These keys are referred to as the public and private keys. Because it's the public key that is used to encrypt messages to the owner of the paired private key, this type of encryption is commonly referred to as public key cryptography. It is neither single-factor nor multifactor since it's not authentication.
10. C. Public key cryptography works because the public key can be provided to anyone. The only thing you can do with the public key is encrypt a message that could be decrypted by the matched private key. This process uses asymmetric encryption, so it's not a symmetric key. The private key has to be with the owner of the key and protected. If that key gets out, any messages encrypted to the owner by the public key could be decrypted. PGP uses public/private keys and does not have its own type of key.
11. D. What this says is that if A trusts B and B trusts C, then A can trust C. This is an application of the transitive property. The commutative and associative properties are both also mathematical principles. There is no such thing as a communicative property.
12. A. Symmetric key encryption is generally used instead of asymmetric key encryption because symmetric key encryption uses shorter keys

and fewer resources, resulting in shorter times for encryption and decryption. This does not make it more secure, even if that word were to be defined in this context. Symmetric key is not easier to implement, and asymmetric key is not encumbered with patents, which is why C and D are wrong.

13. B. When both symmetric and asymmetric keys are used, typically where the asymmetric key is used to protect the symmetric key, it is called a hybrid cryptosystem. The other options don't exist.
14. D. Media access control (MAC) is an address attached to physical network interfaces. The correct answer is message authentication code because SHA-1 and MD5 are used as message authentication codes to ensure that a message has not been tampered with. This means it is being authenticated.
15. B. PGP uses public and private keys. The public key is stored in a public place like a key repository. Since there are two keys, PGP uses asymmetric key encryption, sometimes known as public key encryption.
16. B. Hydra is used to brute-force passwords against network services. The tools tlsscan and cipherscan don't exist. While the SSL protocol has been deprecated for many years, it is still commonly used, so the tool is sslscan.
17. C. Protecting against related keys is done in the implementation rather than the specification. The implementation of AES should not allow related keys to be issued. None of the other answers are true.
18. A. A certificate authority is a trusted third party that can validate users and their identity, relieving everyone from having to verify every user's identity themselves. A certificate authority is not faster, and they don't offer stronger keys. The certificate authority is not responsible for ciphersuites being supported, just the certificate.
19. D. A certificate revocation list is used to indicate when a certificate is no longer valid. Hashing the list won't help and re-validating identities may only be necessary when a certificate has fully expired. When a certificate expires it may be put on the certificate revocation list. A

periodic CA update is ambiguous, but may be updating software, which won't keep a certificate list up-to-date.

20. D. The property of nonrepudiation says that a key belonging to an individual, where the private key is protected by a password and not accessible to everyone, will not be used by anyone but that individual, so any message signed by their key must have come from them. While encrypted messages are related to confidentiality, signing a message is not encrypting it. The other properties are not related to this scenario.

Chapter 14: Security Architecture and Design

1. B. The Biba security model covers data integrity. While other models cover confidentiality, none of them covers availability.
2. D. An n-tier application, sometimes called a multitier application, can have as many tiers as necessary. While you may think there are three, there could be more tiers than that, depending on how the application is designed.
3. C. JavaScript Object Notation (JSON) uses keys and values to store data. While you could theoretically represent a relational database in JSON, it wouldn't be the most efficient. SQL is a language used to query relational databases, and document-based databases may be more likely to use other document types to store data.
4. C. The NIST cybersecurity framework specifies five functions: identify, protect, detect, response, recover.
5. C. The ISO 27001 specification takes a different approach than NIST's cybersecurity framework. ISO 27001 specifies Plan, Do, Act, Check, which is four steps.
6. A. The highest level of classification used by the U.S. government is top secret. Confidential and restricted are lower levels, and eyes only is not a classification used by the U.S. government.
7. D. Micro Channel architecture is a specification for peripherals to interact with hardware systems that was proposed and implemented by IBM in the 1990s. Service-oriented architecture is an older concept that has been revived, to a degree, by microservices. The other answers are not things that exist.
8. C. Infrastructure as a service is a cloud-based offering where companies may just acquire servers they can use for their infrastructure. Service-oriented is a way of potentially designing applications. Everything in AWS is virtualized. This leaves serverless. Lambda functions don't require the provisioning of servers to support

them. All processing of the function and its data are handled by AWS infrastructure.

9. C. The Clark–Wilson integrity model specifies constrained data items (CDIs) and unconstrained data items (UDIs) that are used when identifying and implementing rules. The other answers either don't exist or refer to things that are not related to information security.
10. D. Emulation is where applications may be run on a processor they were not compiled for so the operation codes are emulated. AWS is Amazon Web Services, which can offer application virtualization services but is not a type of application virtualization. Paravirtualization is partial virtualization. Containers are a way of isolating applications without using full virtual machines on a hypervisor.
11. A. The five functions designated by NIST are identify, protect, detect, respond, and recover. You can't do any of the other functions until you have been through identify, which defines business needs and essential assets for the business.
12. D. Commonly, you will see the following in an n-tier application design as core features: browser, application server, database server. There may also be security functions and load balancers as well as a web server in front of the application server. When you focus just on the core, though, the application server is in the middle of the architecture.
13. B. MongoDB is a NoSQL server that is not relational. SQL Server is ambiguous but could refer to Microsoft SQL Server, which is not open source. Oracle is a company that owns relational database servers, including MySQL, but only MySQL is open source.
14. C. The Bell–LaPadula Simple Security Property says a subject cannot read an object at a higher level than the subject. None of the other answers is correct.
15. D. Some of the answers here mingle the five functions from NIST with the phases of the ISO 27001 cycle. The only option that has only ISO 27001 phases is D, and those are Plan, Do, Check, and Act.

16. B. While cloud-based applications are often used by businesses that implement zero trust, multifactor authentication is essential since all access to resources has to be authenticated. VPNs and VDI have often been used to allow remote access to clients.
17. C. Serverless computing uses an event-based model. The other answers are different types of programming but are not relevant to serverless computing.
18. D. SMS can be prone to hijacking, while push-based approvals can be used to bypass MFA. Username/password is not MFA. A one-time password, provided by either a token or an application, is the best approach out of the ones provided here.
19. C. The Cyber Kill Chain is a process developed by Lockheed Martin describing an attack process. The Cyber Kill Chain is not useful for any of the other answers.
20. B. Syslog is a logging system for Unix-based systems and may not be used on Windows devices, which may be commonly used for user workstations. SAP is enterprise software that may not be used by most users. SCCM is essential for managing Windows systems for some businesses but may not be specifically used to protect those workstations. EDR is endpoint detection and response, which can help keep workstations protected.

Chapter 15: Cloud Computing and the Internet of Things

1. A. A Chromebook is a laptop with a traditional user interface, including a screen and a keyboard. The other devices don't have a traditional user interface but are still connected to networks, allowing anyone who has access to those networks to interface with them.
2. B. HTTP is a stateless protocol, which requires the application to perform some sort of state transfer. REST is Representational State Transfer, which allows the client and server to communicate information about the state of the client and the application between them. HTML is not a protocol but a language, so state doesn't make sense.
3. D. Infrastructure as a service puts everything down to the operating system under the control of the customer. The other services put much more control into the hands of the service provider.
4. C. Cloud-native design takes advantage of lots of technologies that make for responsive applications. This will commonly include containers, which is application virtualization. A virtual machine is a lot slower to start up than a container is. Automation and microservice architecture are important components of cloud-native design.
5. B. Automation leads to consistency, because automation is performed by scripts that will always execute the same way every time. This also leads to repeatability. Because they are scripts, you can test them. What you don't necessarily get is fault tolerance.
6. C. Computing devices generally follow the Von Neumann architecture: there is memory, storage, and a processor. A general-purpose computing device will have some sort of input/output to interface with a user. An IoT device will have a special-purpose input/output device that may not easily allow a user to interact with it in general ways. A smart thermostat, for example, has a simple display that would do things like show the temperature and allow you to adjust the desired temperature.

7. C. Storage as a service is used to store documents. From there, you can share those documents. While you could also share documents from the other cloud-based services, storage as a service would be the most common.
8. B. Cloudscan is used to assess cloud services. Samba is a network sharing application based around the server message block protocol. Postman is an application used to test web application programming interfaces. `nmap` is a port scanner that could be used to identify any devices on a network as well as the ports open on that device.
9. D. While a NoSQL database, data bus, and microservice architecture could be used to develop a web application with a mobile application for a front end that interacts with the user, the most likely would be a RESTful API. This way, it doesn't matter what is behind the API. The API is the interface between the web application and the mobile device.
10. C. Implementing security controls is essential, regardless of where the services are located. Businesses commonly know how to implement these controls in on-premise systems. They may not know the appropriate way of implementing these controls in a cloud environment. All of the other answers could be a problem in an on-premise environment and wouldn't be specific to cloud.
11. B. Fog computing is a way of providing compute and storage resources closer to the "ground," where IoT devices are likely to be. Cloud-native design may be used to support IoT devices that use cloud services but cloud services are not fog computing. Access management is an important element of any good security design, but fog computing does not specifically support access management. Finally, grid computing is a distributed processing model.
12. A. SETI@home is an example of grid computing because it uses distributed processing across a large number of systems. Shodan.io and Thingful are both related to IoT, and the OWASP Top 10 is a list of vulnerabilities to web applications.
13. C. A botnet may use a distributed computing model to perform tasks, which is grid computing. Cloud-native design and RESTful processing

are related to web applications. Fog computing is related to control, and storage associated with IoT devices.

14. D. Insecure third-party components, misconfiguration, and access control issues are all possibilities in serverless web applications that may be built primarily using serverless functions. As there is no server associated, and no guarantee of the type of operating system the function is running on, serverless functions are less likely to be vulnerable to command injection attacks.
15. D. The shared responsibility model of cloud computing means there is a sliding scale where the customer or the provider will be responsible for different aspects of the service. However, no matter which service is used, the customer is always responsible for data, since the data always belongs to the customer.
16. A. Sensors and actuators are the physical devices that allow for manufacturing to be automated. As they have the least “intelligence,” they are at the lowest level of the Purdue model. The other answers are higher up in the model.
17. B. Segmentation is the most important aspect of the Purdue model, since it has the ability to offer better protections for fragile or sensitive devices. None of the other answers here make sense in this context.
18. C. Requiring MFA is the best approach to protecting against credential compromise. Long passwords won't help if the password is stolen. Neither of the other two will have an impact on credential compromise.
19. A. Unfortunately, a common problem with cloud services, as well as on-premise services, is misconfiguration. This may include inadvertently setting an S3 bucket to be public when sensitive data may be stored there. The provider won't make a difference and software as a service won't impact data exposure directly. Insider threat isn't a problem with cloud-based services specifically.
20. D. Templates, Ansible, and PowerShell are all used to automate deployment of systems into a cloud environment. While containers may be deployed, they are not used to automate the deployment.