|  |  |  |  |
| --- | --- | --- | --- |
| Network Architecture | Knowing your network architecture is one of the most important principles in security. It is comprised of Conceptual Design, Logical Design and Physical Design. Where my valuable data is located (stored) and communication flow is highly important as well. | 1 | 15 |
| Non-Traditional IT assets | Door locks, refrigerators, televisions | 1 | 15 |
| Assets IT | Servers, desktops, and applications. | 1 | 15 |
| Conceptual Design | A high-level overview of why we need our network. | 1 | 17 |
| up to date network diagram | When you know what things are connected to your network | 1 | 15 |
| Conceptual Design components | As conceptual design is a high-level design overview, it includes the core components of your network's architecture. These components represent internal and external systems, data flow, and overall system behavior. The conceptual design should consider (a) OS platforms, (b) server services, (c) critical processes, (d) critical core functions, and (e) the critical individuals who leverage these functions, processes, and services to help achieve organizational success. | 1 | 17 |
| gitClosed box diagraming | It is describing a system by its functionality and use without requiring any knowledge of how the systems achieves its functionality. | 1 | 18 |
| Logical Design | Represents the logical functions in the system, while putting the conceptional design into paper. | 1 | 19 |
| Physical Design | A physical design has all major components and entities identified within specific physical servers and locations or specific software services, objects, or solutions. This design level represents how the network, and all its components are expected to behave, while still being on paper. The physical design is the last one created before the network design is implemented. | 1 | 20 |
| Physical Design details | Include OS versions, patch levels, hardening configurations, risk categorization. | 1 | 20 |
| Physical Design security | Physical security can always betray logical security controls. | 1 | 21 |
| Knowing your environment - Principals. | Knowing where your data is located and communication flow | 1 | 22 |
| Valuable data - Location | Securing a network requires knowledge of where each piece of valuable data resides as it could end up in the most unusual locations such as desktop of senior leadership, hard drives of systems admin or unintentional like a cloud, Dropbox, OneDrive, etc. | 1 | 22 |
| Critical data | Often lives in critical servers, being accessed by critical applications, an asset. | 1 | 22 |
| Communication flow | Understanding Who and when accesses data and how much data is accessed? | 1 | 24 |
| Lateral movement | What an adversary does to gain leverage in our networks. Stage 1 | 1 | 24 |
| Persistence | Is what adversaries do to keep ahold on our network and survive a restart. Stage 2 | 1 | 24 |
| Data loss Prevention (DLP) | Is a security control that can attempt to discover sensitive data on our networked systems, monitor for the misuse of that data across the networks and potentially prevent exfiltration of the same | 1 | 24 |
| Know thy systems | Is never a one-and-done proposition. Keeping up with change is the only way to move toward being successful in cybersecurity. | 1 | 25 |
| Key network devices | Routers and switches | 1 | 27 |
| Key network devices compromise | Allows for sniffing and could be catastrophic. Compromise of routers and switches can facilitate communication interception and manipulation. | 1 | 27 |
| Critical assets | Like routers and switches are very important and largely neglected, and even running outdated software due to the impact on security due to downtime. | 1 | 27 |
| Switches | Allow all of your devices together to form a network. | 1 | 27 |
| Routers | Are devices that can connect different networks together or facilitate network to networks communication and are the most ignored IT assets. | 1 | 27 |
| Threat enumeration | Part of understanding the TTP: tactics, techniques, procedures. | 1 | 29 |
| Threat intelligence | Strives to understand the adversary’s tactics, techniques, and procedures. | 1 | 29 |
| Threat agents | An individual, organization or group that is capable and motivate to carry out an attack of one sort or another | 1 | 30 |
| Attackers | Threat agents | 1 | 30 |
| Opportunistic attacker | Is looking for an easy target while leverage malicious websites, malicious advertising, emails and so on. | 1 | 30 |
| Organized cybercrime | Ransomware, traditional extortion | 1 | 30 |
| APT (Advanced persistent threat) | Defined as highly capable adversaries, acting under the authority of a specific government or military organization. | 1 | 30 |
| Router attacks | Most common are Denial of service (DoS) Distributed Denial of Service (DDoS) Packet sniffing, Routing table poisoning. | 1 | 32 |
| Denial of Service - Dos | Service of the device is being impacted (denied). At a minimum, it could result in a total impact of device availability. | 1 | 32 |
| Distributed Denial of Service – DDos | It is similar to DoS but in this case, the attack is coming from different locations in order to counter defense. | 1 | 32 |
| CDN (Content Distribution network) | Way to get relief on a DDoS attack by using infrastructure to re-rout the victim’s organization traffic. | 1 | 33 |
| Packet sniffing | Refers to the capture and analysis of a network’s traffic impacting the confidentiality and integrity. | 1 | 33 |
| Packet misrouting | Integrity based attack. A routers configuration is manipulated such that traffic is no longer routed properly, traffic might be routed to a non-existent network location, traffic might be sent back to a previous router, resulting in a routing loop. | 1 | 33 |
| Routing table poisoning | The adversary convinces a router to update its routing table resulting in traffic redirection. This is also a machine in the middle attack. | 1 | 33 |
| Switches attacks | Could be identified as a way of manipulating the network traffic in a specific manner to convince a switch to do something it shouldn’t. | 1 | 34 |
| CDP information disclosure | CDP ( Cisco Discovery protocol). Discovery protocols are used to aid devices in discovering other devices that also exist on a network. | 1 | 34 |
| Discovery protocol traffic | Is being broadcasted across the entire network, and limiting to the management interfaces, we can limit the disclosure of this data to a potential attacker. | 1 | 34 |
| Mac Flooding | Is when an attacker floods our MAC ( Media Access Control) address table of a switch with fake MAC addresses. | 1 | 34 |
| Network interfaces | Wired or wireless internet | 1 | 34 |
| Switches | Leverage the MAC Address to determine which connected computer traffic is destine for. | 1 | 34 |
| MAC Downgrading | This happens when the switch doesn’t have enough memory to record each new MAC address that connects, and it will downgrade itself to a hub rather than shutting down. | 1 | 34 |
| Hubs | The predecessor of switches, and it is not as secure as a switch since it will broadcast all information within the network allowing this for sniffing. | 1 | 34 |
| DHCP Dynamic host configuration protocol | Commonly used by computing devices to obtain their network configuration including their IP addresses. | 1 | 36 |
| DHCP Manipulation | It is when an attacker is waiting for a DHCP interchange and before the right device responds, the attacker provides the requested information gaining control over the network. | 1 | 36 |
| STP ( Spanning tree protocol) | STP,  Layer 2 network protocol used to prevent looping within a network topology. | 1 | 36 |
| STP Manipulation | An attacker with sufficient access to a network, might be able to impersonate an STP communication and manipulate to their advantage to get a switch re-configuration to facilitate an MITM attack. | 1 | 36 |
| VLAN (Virtual Local Area Network) | Is a concept of network segmentation. | 1 | 36 |
| VLAN Hopping: | An attacker will manipulate the characteristics of network packets in such a way that a switch will allow an attacker to hop from one VLAN to another in a way that would otherwise be prohibited | 1 | 36 |
| Topologies | Define the inter-relationship of network-based components, and can be defined as physical or logical | 1 | 38 |
| Topology – Physical | It is defined as how devices are physically connected together, and how communication is sent over the physical connection (electrical) signaling, pulses of light, etc) | 1 | 38 |
| Topology – logical | How communication is logically formed prior to transmission. | 1 | 38 |
| Network Diagram | Shows the topology of our network. | 1 | 38 |
| Topology – star | type of network topology in which every device in the network is individually connected to a central node, known as the switch or hub. When we connect cables from our desktops, phones, and printers to the switch. | 1 | 38 |
| Segmentation | Means separation, assets should not be free to communicated unabated. One of the most important concepts related to network architecture security. The idea of segmentation is that the network is not a single trusted entity and highly sensitive data should be placed in a segmented part of the network restricting access. | 1 | 40 |
| Least Privilege | A user needs to have access to only the necessary data to complete their jobs functions and nothing more. | 1 | 40 |
| SND – Software Defined Networking | Is the concept related to the notion of virtualization. Virtualization is an abstraction. With SDN we are not dependent upon what underlying network hardware is in place since it is becoming a more valuable aspect of cloud computing. | 1 | 41 |
| NotPetya | Type of malware with devastating consequences. Proof that segmentation could’ve prevented that attack. Costed 10 billion in damages around the world. | 1 | 41 |
| VLAN Network Security | Is a Virtual LAN. This logical control allows for the network to be logically separated into virtual segments. Is a very valid form of segmentation. Each VLAN is technically its own network and will have their own IP ranges separating devices allowing it for better management. | 1 | 42 |
| VLAN & ACL | If you add an ACL (Access control list) this will increase security. | 1 | 42 |
| 802.1X | Port-Based Network Access Control. Is a standard that allows for authentication to occurs prior to a user and/or computing device being granted access to a network. The “X” represents the eXtensible nature of authentication methods. It could be used on wired and wireless networks. | 1 | 43 |
| Network Jack | It is used to connect to the network; however, it could be a mean for attackers to connect to our network. | 1 | 43 |
| Attack vector | a pathway or method used by a hacker to illegally access a network or computer in an attempt to exploit system vulnerabilities. | 1 | 44 |
| Web applications – attack vector | Web applications are hacker’s best attack vector because are difficult to build securely and often provide access to sensitive data found in an internet network segment. Web-apps most time are built insecurely. | 1 | 44 |
| Tiered architecture | It is the concept separating network segments based on trust while the segments form tiers of separation | 1 | 44 |
| Defense in depth | It is described by the idea of no single failure of any part of the environment would result in the total catastrophic failure of the entire environment. | 1 | 44 |
| 3 tier architecture | 3 tiers of separation, the tiers represent our network, and the separation is based upon criticality, security, sensitivity. The separation is enforced by firewalls.  Systems in each category serve a similar purpose and have common security requirements. This allows you to group resources within a category by placing them into a common network section. You should locate firewalls: • Between the Internet and the other networks • Between the semi-public and private network • Between sections of varying trust levels | 1 | 44 |
| Segmented tiers | More defined names are: Public tier, Semi-Public tier (DMZ), Middle tier, and private tier. | 1 | 45 |
| Public tier (segmentation) | Resources that reside on the internet are not reliable and cannot be trusted. | 1 | 45 |
| Semi-Public tier-DMZ  (Segmentation) | The DMZ is a tier that includes Web, email, and DNS servers and they are used for organizational systems that intend to be public facing. The DMZ is a great risk of compromise since they are connected to the internet 24/7 and because of that, better efforts to protect it are made. The DMZ is also considered unreliable but not as much as the public tier. | 1 | 45 |
| Middle tier  (Segmentation) | Also known as application tier, because it is the separation between the DMZ and the private (internal) network tier by using a proxy allowing the communications to be inspected both ways (in and out) before reaching out the webserver. | 1 | 46 |
| Private tier  (segmentation) | AKA as the internet network segment and where you find your trusted assets and your internal network and internal systems are located. Also, it represents the last tier in our segmentation example and is of higher trust and lower risks. | 1 | 46 |
| Tiered arch rules | * Any system visible from the internet must reside on the DMZ and may NOT contain sensitive data. * Any system with sensitive data must reside on the private (internal) network and must NOT be accessible from the public network (the internet). * The only way a DMZ system can communicate with a private (internal system is via the middle tier. | 1 | 47 |
| Logical topology | Communication flows from the internet to a machine in the DMZ, through a proxy and then delivered to an internal database server. | 1 | 48 |
| Physical topology | Network traffic from the public tier enters our networks through a router. While a router is not commonly used for security but in this instance is used as an initial filtering, once it determines the communication is secure, it will send it to the DMZ for further inspection at the firewall. | 1 | 48 |
| DMZ (segmentation) | The DMX machine would understand that the traffic received needs to be forward to the internal database server. The DMZ will first send this request through the middle tier (proxy) and the firewall will inspect it. Once its determined safe, it will be forwarded to their destination. | 1 | 48 |
| Benefits of understanding your network arch. | Situational awareness, prioritization of effort, reduced cost of effort, timely detection of attacker prescence, timely detection, timely response, and reduction of damage. | 1 | 49 |
| Network Protocol | It is a set of rules that dictate how computer networks communicate. | 1 | 54 |
| ISO OSI Protocol stack | ISO (International Organization for Standardization) OSI (Open Systems Interconnection) model divides network communication into 7 layers. Each layer has a specific job or function. Each layer is only concerned in their own specific function and disregards the layers above and below functions. | 1 | 56 |
| ISO OSI Layer 7 (Application) | Interacts with an application to determine which network services are required. This is where applications interface. | 1 | 56 |
| ISO OSI Layer 6 (Presentation) | Makes sure that the data sent from one side of the connection is received in a format that is useful to the other side. Presents the data in a unified structure. | 1 | 56 |
| ISO OSI Layer 5 (Session) | The session layer handles the establishment and maintenance of connections between systems. It negotiates the connection, sets it up, maintains it, and makes sure that information exchanged across the connection is in sync on both sides. This is where the encryption occurs. HTTPS transit. | 1 | 56 |
| ISO OSI Layer 4 (Transport) | It sequences packets and provides end-to-end data delivery service and ensures the transport of the data is successful. | 1 | 57 |
| ISO OSI Layer 3 (Network) | IP is the basis for all communication on the Internet. It is so important that it even gets its own layer in the TCP/IP stack. Its primary purpose is to handle the transmission of packets between network endpoints, usually single hosts identified with a unique address. IP includes some features that provide basic measures of fault-tolerance (time to live, checksum), traffic prioritization (type of service), and support for the fragmentation of large packets into multiple smaller packets (ID field, fragment offset) | 1 | 57 |
| ISO OSI Layer 2 (Data Link) | It connects the physical part of the network (cables and electrical signals) with the abstract part (packets and data streams). | 1 | 57 |
| ISO OSI Layer 1 (Physical) | It handles the transmission across the physical media, such as an electrical pulse, modulation of radio waves, connection specifications between interface hardware and network cabling, voltage regulation, etc. | 1 | 57 |
| Stack based communication | Is when data from one layers of the stack in the transmitting computer can be understood by the corresponding receiving layer of the receiving computer. The layers do not communicate with each other directly, rather they use headers to do so. | 1 | 58 |
| Headers | Are blocks of data that describe the work that was done at the corresponding layer. They are also referred as “protocol headers”. | 1 | 59 |
| Encapsulation | The process of moving down a stack, with each later doing work, leveraging the addition of a heard to describe said work. | 1 | 59 |
| Decapsulation | Is the process of moving up a stack with each layer doing work, combined with the reading and removing of headers. | 1 | 59 |
| TCP/IP Model | Has 4 layers and still have to perform the same functions as the OSI model, meaning that each layer needs to perform more work. The network layer comprises both the physical and data link layers of the OSI model, and the application layers encompasses the Application, Presentation, and Session layers. | 1 | 60 |
| TCP/IP packets | Each layer on the sender needs to communicate with the same layer on the receiving computer. However, they cannot directly talk because you must go down the stack, across the network, and back up the stack on the receiving system. This is accomplished by having each layer add a header as you go down the stack on the sender and each layer remove a header on the receiving system as it goes up the stack. | 1 | 62 |
| IP  Internet protocol | Works at the internet layer of the TCP/IP stack (network layer of the OSI model). Foundational protocol of the TCP/IP Suite. Assists with path determination for transmission of packets between endpoints on different networks. Defines the formation of IP address, based upon network characteristics. | 1 | 64 |
| IPv4 | Accommodates 4.2 billion unique 32-bit addresses. Has serious limitations such of the number of unique addresses supported. To address the shortage, NAT(Network address translation) and CIDR (Classless interdomain routing). However, wasn’t enough | 1 | 65 |
| IPv6 | 128 bits of address space – 340 undecillion address. Larger address space allows for better flexibility in allocating addresses. Created to address the IPv4 address shortage. Utilizing IPv6 ISPs (internet service providers) will be able to provide a geographical IPv6s prefixes to different parts of the world. | 1 | 65 |
| IPv4 Header Key field | All fields of the ip header have importance. The most important are Version, 4 bits; Protocol 8 bits, time-to-live (TTL) 8 bits, Fragmentation 16 bits, and source address and destination address 32 bits. | 1 | 69 |
| IPv4 Header Key field – version 4 bits | This field contain a short integer value, corresponding to the internet protocol version used to create the header. A value of 4 decimal indicates IPv4 and value of 6 indicates IPv6. | 1 | 69 |
| IPv4 Header Key field – protocol 8 bits | This field will contain and integer value denoting the exact type of IP message encapsulated in the packet. Although the meaning of the possible values are standardized, the values themselves are arbitrary. | 1 | 70 |
| IPv4 Header Key field – Time to live (TTL) 8 bits | A packets TTL specifies how many router “hopes” a packet can transit before the packet will expire. If a destination router can be reached in less hops than allowed by the TTL, it will not expire prior to delivery | 1 | 70 |
| IPv4 Header Key field – fragmentation 16 bits | It is also known but hos 16 bits (3 bits for flags and 13 bits for fragment offset. Sometimes a router encounters a packet that is too large for it to transmit at once. Instead of singling the sender it is too bit, the router fragments. It only happens when the network’s size requires it due to a maximum | 1 | 70 |
| IPv4 Header Key field – source address and destination address | Routers and networks need to know who they are speaking to. The source address contains the IP address of the packet’s sender. The destination address list the IP address of the recipient. | 1 | 70 |
| IPv4 Header Key field – Options | Options are optional and they happen to be set the length of the IPv4 hear will extend beyond the size of 20 bites, | 1 | 70 |
| IPv6 header Key field - | It looks a different than IPv4 but has the same purpose as IPv4. It is known for version 4 bits, Traffic class, flow label, payload length, next header, hop limit, source address and destination address. | 1 | 72 |
| IPv6 header Key field – Version 4 bits | Just as the IPv4, this field indicates the IP version in use. | 1 | 71 |
| IPv6 header Key field – Traffic class and flow label | They are 2 fields, and their case can be related. Traffic class is used to provide QoS (quality of service) for network communication Traffic class also indicates the packets priority. Flow label indicates that this packet belongs to a specific sequence of packets between a source and a destination, requiring special handling of the IPv6 routers | 1 | 71 |
| IPv6 header Key field – Psyload length | Specifies the length of a load | 1 | 72 |
| IPv6 header Key field – Next header | Contains an integer value denoting the type of IP message encapsulated in the packet. | 1 | 72 |
| IPv6 header Key field – hop limit | Is the same concept as time to live field and works in the same manner | 1 | 72 |
| IPv6 header Key field – source address and destination address | These fields represent the source and destination addresses of the computer involved in a communication | 1 | 72 |
| IPv6 Features | Extended address space, auto configuration support, support for IPv6 over IPv4 (tunneling) support of the IPv4 over Ipv6 (translation), Authentication of endpoints and cryptographic protection of communication (utilizing concepts of IPsec), flexible embedded protocol support. | 1 | 73 |
| ICMP (internet Control Message Protocol) | ICMP has 2 purposes, Report errors or troubleshooting such as destination host unreachable and TTL exceeded in transit, to provide network information like pings. | 1 | 76 |
| ICMP versions | It has 2 versions, ICMP for IPv4 based networks and ICMPv6 for IPv6 based networks | 1 | 76 |
| ICMP Headers | It is the easiest to understand as it only contains 3 fields such as version, code and the last one is a checksum. | 1 | 77 |
| ICMP Header – Type | It is like a category of conditions that are often related. | 1 | 77 |
| ICMP Header – Code | The code provides a clarification of the header “type” | 1 | 77 |
| ICMP Types and codes | Types and codes are related to each other. See book for more examples | 1 | 79 |
| TCP  Transmission control protocol | Works by establishing a session prior to data exchange, session leads to connection- oriented communication, provides a “guarantee of delivery” by providing “receipts of successful delivery” and other protocols leverage from TCP’s benefits (HTTP, HTTPS, SSH, etc). It operates on the transport layer (layer 4 of the OSI model) | 1 | 82 |
| TCP Uses | Flow control to better support changing network and host communication capabilities in real-time. Confidence in TCP’s ability to perform data receipt validation allows for greater confidence in larger data transmission (per packet) than other transport layer protocols. Application developers can take advantage of transport later functionality without having to build the capabilities themselves. | 1 | 83 |
| TCP ports | FTP (file transfer protocol) data (20), FTP(21), SSH(22), telnet (23), SMTP(25), DNS(53), HTTP(80), HTTPs(443). | 1 | 83 |
| Virtual connection | Session between hosts that desire to communicate | 1 | 82 |
| TCP Benefits | Flow control, verification of data received, and retransmission of any missed communication are all examples of TCP benefits this is also why is the most utilized of the transport layer protocols. | 1 | 82 |
| TCP connection (establishing) | Is stablished by a 3-way handshake in which ISN(initial sequence numbers) are exchanged. | 1 | 85 |
| TCP handshake | It is also known as a 3-way handshake. The client initiates a 3-way handshake by sending a “SYN” requesting a TCP connection to the server. If the server accepts the connection in response of the “SYN” will send a “SYN/ACK” and in turn, the client will send an “ACK” response completing the handshake. In other words, the computer systems are synchronizing their sequence numbers that assist in tracking the data communicated in each direction. By the end of the handshake both computers will have each other’s sequence numbers and after that each sequence number will increase by 1 for each byte of data that is transmitted by each party. | 1 | 85 |
| TCP Response packet | The response consists of both an acknowledgment of the client's initial connection request (the ACK flag is set) and a connection request of its own (the SYN flag is set), together in a single packet (a SYN-ACK). | 1 | 85 |
| TCP ISN (initial sequence number) | Sent together with “SYN” while the 3-way handshake gets stablished. It is a way for a computer to count how much data is sent from computer to computer. | 1 | 86 |
| TCP Headers | Source port and destination port, sequence number, acknowledgement number, data offset, TCP flags, window size, options. | 1 | 87 88 |
| TCP Headers – Source port and destination port | It is a port number that indicates on a host system where an application is sending and receiving its network communications. It is 16 bits each. | 1 | 87 |
| TCP Headers – sequence number | Represents either the ISN or the accumulated sequence number which is a totality of data related to the current packet. It is 32 bits. | 1 | 87 |
| TCP Headers – Acknowledgement number | It indicates the value of the next expected sequence number from a party of the communication. 32 bits. | 1 | 87 |
| TCP Headers – Data offset | It refers to the length of the header and indicates the number of 32-bit words (4 bytes) that are contained in the TCP header. | 1 | 87 |
| TCP Headers – TCP flags | Represents a characteristic of the session’s status or of the importance of a specific packet such as NS, CWR, ECE, URG, ACK, PSH, SYN, FIN. | 1 | 88 |
| TCP Headers – Windows size | It represents the value described by the window size that indicates the number of data octets that the sending of this segments is willing to accept (see flow control). | 1 | 88 |
| TCP Headers – options | It is represented by the minimum of 32 bits and multiples also of 32 bits. If TCP options are used this field is occupied by a minimum of 4 bites and consumes multiples of 4 bytes. Unneeded space is padded with zeros. | 1 | 88 |
| TCP closing session | There are 2 methods of closure, Graceful and abrupt | 1 | 89 |
| TCP Abrupt closure | Either host can abrupt terminate a session by sending an RST packet and an ACK packet will not be sent due to the fact that whoever sent the RST packet has become unavailable. | 1 | 89 |
| TCP Graceful closure | Hosts can initiate a graceful closure. Host A sends a “FIN” packet, upon receipt host B sends an “ACK” acknowledging the request and sends a “FIN” terminating then Host A will reply by with “ACK” packet finalizing the session. | 1 | 89 |
| UDP (User Datagram Protocol) | is a good multicast solution for optimized real-time communications delivered over a wireless network. Connectionless (Non-Session-based) communication, doesn’t provide any guarantee of delivery, requires less overhead than TCP, resulting in performance gains, can work well even when a small amount of packets loss is acceptable. It is used in a reliable network with high level of confidence and because of this, other transport layer protocol functions can be sacrificed. UDP is the complete opposite as TCP since there is no handshake. | 1 | 91 |
| UDP transmission | The sender isn’t required to check if the receiving host is available prior to transmission. After the sender transmits the UDP packet the sender forgets the packet was even sent and the receiver doesn’t even acknowledge receipt and there is also no guarantee that the packets arrive in the same order they were sent. | 1 | 91 |
| UPD traditional uses | Applications where small amounts of occasional packet loss may be acceptable or where retransmission doesn’t make sense such as DNS request and responses. Applications where the overhead of TCP could impact performance like VoIP or other multimedia exchange. | 1 | 93 |
| UPD ports | DNS (53), BOOT/DHCP (67, 68), TFTP (69), NTP (123), SNMP (161, 162) NFS (2049). | 1 | 93 |
| UDP based protocols - Network Time Protocol (NTP) | Time synchronization | 1 | 94 |
| UDP based protocols – BOOT/DHCP | Autoconfiguration of network interfaces and the ability to atomically start an OS from the networks during startup. | 1 | 94 |
| UDP based protocols – Network File System (NFS) | File sharing support for UNIX-based networks. | 1 | 94 |
| UDP based protocols – Simple network management protocol (SNMP) | Monitoring and troubleshooting for server-based devices. | 1 | 94 |
| UDP based protocols – Trivial File transfer protocol (TFTP) | Inter-device file transfer without the requirement for authentication | 1 | 94 |
| UDP header | It is 8 bytes; we save 12 bytes of data in every single packet. There are only 4 fields, Source port, destination port, length, and checksum. | 1 | 95 |
| Sniffing | A sniffer provides the capability to observe, record and analyze traffic as it transits a network. They can also observe network communication on a wired and wireless network, used legitimately by administrations and security professionals, and can asl o be used maliciously to obtain credentials, sensitive data, and audio from VoIP calls. | 1 | 98 |
| Sniffers | Are tools that come in different forms based on required functionality, work- flow ability, or application best practice. Here is a list. Tcpdump: initial triage, Wireshark: Detailed and protocol analysis, Snort: intrusion detection system, Kismet: Wireless network sniffer, BetterCAP: Sniffing on switches, via the use of MiTM attacks. | 1 | 99 |
| TCPdump | Is primarily run on Linux - UNIX OS and it is considered to be “lean and mean” it doesn’t provide a detail interpretation of the data it sees and leaves it to the analyst to interpret. It is a sniffer that displays traffic from your ethernet adapter | 1  1  LB | 99  103  3 |
| Wireshark | Is not a sniffer per say but a network protocol analyzer. It can understand hundreds of different protocols and media types. Its primary purpose is to analyze what’s being communicated. can be used to perform detailed analysis and automatic packet decoding of network packet data in a GUI environment. | 1 | 99 |
| Snort | Is an instance of IDS (Intrusion detection system) it performs a detailed inspection of network traffic to assist in the earlier detection of malicious activity. | 1 | 99 |
| Kismet | Is a sniffer designed for traditional wireless (WLAN) networks. It processes the radio signals produced by WLANs to provide information on what security controls are in place. The data can be combines with geographic mapping tools. | 1 | 100 |
| BetterCAP | It obtains sniffing capabilities by utilizing stacks, including MiTM. Once MiTM is in place, BetterCAP will sniff the traffic it can observe. | 1 | 100 |
| Virtualization Introduction | Is an abstraction. Abstraction is a way to separate function from form and allows us to focus on the “what” and not the “how” a computing function is achieved. Abstractions are not a new concept, they have served our evolving technological world well and allow for the creating of “virtual hardware: from physical hardware, leading to the virtual machines. | 1 | 108 |
| Virtualization  Virtual machines | Using virtual hardware, we can create virtual computers (virtual machines). The physical computer requires an OS. This OS is referred to as the “Host OS”. A virtual machine requires its own OS. This OS is referred as “Guest OS”. The software makes this all possible is known as the hypervisor. | 1 | 110 |
| Virtualization  Isolation | Is another word for segmentation. A separation from physical to virtual allows for “hardware independence” This separation can help to reduce the scope of damage from the compromise of a VM since the damage can be isolated away from the physical hardware of both. This separation further enables other key functionality such as a malware analysis and Improved disaster recovery. A compromise of the virtualization doesn’t mean a compromise of the host. The more we abstract and isolate, the more difficult it would be for an adversary to attack us. | 1 | 111  114 |
| Virtualization  Hypervisor | It is like a broke, it is aware of all the hardware you have and allocates that hardware virtually to virtual machines. It also presents simulated hardware to the virtual machine OS. | 1 | 110 |
| Virtualization  Security. | It provides incredible security powers; however, it also provides security issues. Benefits are Isolation, disaster Recovery and VDI, Malware and forensic analyses and the risks are the hypervisor, isolation violation, | 1 | 110 |
| Virtualization security benefit: Disaster recovery and VDI. | A virtual machine is nothing more than a collection of files on a storage medium and a hypervisor take those files and creates a VM concept. Recovery of a VM might be as single as copying the VM’s files again. VDI (virtual desktop infrastructure) is facilitates through this easy of creating and destroying of VMs. These abstractions further allow for the migration of virtual workload in the presence of a perceived technical outage thus providing a faster recovery. | 1 | 115 |
| Virtualization security benefit: Malware and forensic analyses | Adversaries rely on malware for success and malware analysis can provide information on the goals of an adversary, how a system was broken into, and the weakness exploited. The isolation feature of a VM provides a benefit in this regard. Forensic methodology is a key part of incident response. The available system evidence (and how it can be collected), can be sometimes aided by the use of virtualization. | 1 | 117 |
| Virtualization security Risk: the hypervisor | The hypervisor is a software and like any software it could have vulnerabilities that can range from DoS to remote code execution. DoS on the hypervisor is a DoS on the virtual workload. Remote code execution will occur under the privilege of the hypervisor. Hypervisor compromise might allow for configuration modification, direct access to all VMs, abuse of underlying host OS, processes and hardware. | 1 | 118 |
| Virtualization security benefit: Isolation Violation | Virtual hardware ties back to physical hardware if vulnerabilities are present in that relationship, a VM escape might be possible. A VM escape allows a malicious actor to leverage a compromised VM to execute code on the host computer. VM escapes are discovered more frequently than many would expect. | 1 | 119 |
| Virtualization  Virtual Environment Defense | Guest OS minimal footprint, disabling of unnecessary services, patching and baselines. Hypervisor minimal footprint, patches installed as quickly as possible. Maintaining appropriate visibility of VM-to-VM communication. | 1 | 120 |
| Cloud | Virtualization is the foundation of cloud. It is used when referring to technological abstraction. | 1 | 122 |
| Cloud  Types of deployment | Public: Operated by a third party provided. Private: Built of operated by a single company or organization. Hybrid: combination of public and private tools. | 1 | 123 |
| Cloud  Trade off | Include control and visibility | 1 | 123 |
| Cloud  Public cloud (why?) | Building and maintain IT infrastructure is expensive, it is computing that can be rented, and providers build the computing infrastructure and spread the cost among its customers (subscribers(. Allowing entities to do more at a lower price point than on their own, and services are often defined (or offered) in terms of “subscription models” or “subscription services” | 1 | 124 |
| Cloud  Computing benefits | Cost: trade fixed expense for variable expense. Speed: resources are a click away, Scale: Global elasticity when it is needed, Productivity: on-demand resources, Security: Major cloud providers have a huge business incentive to invest in security. | 1 | 125 |
| Cloud  Type services | IaaS, PaaS, SaaS. | 1 | 127 |
| Cloud  IaaS | “Infrastructure as a service” Servers and storage network data center. The resources are provisioned as needed from a shared pool and billed based on consumption. Ex: AWS EC2, Windows Azure Virtual Machines, Google Compute Engine. | 1 | 127 |
| Cloud  PaaS | “Platform as a service” Dev platforms and tools middleware operating systems. Allows customers to access a “platform” that enables the customer to run custom order or applications. Ex: AWS Elastic Beanstalk, Google App Engine, Heroku, Force.com and CloudFoundry. | 1 | 127 |
| Cloud  SaaS | “Software as a service” Hosted applications, subscription based. Basically, the user can make his own account, but any administrative settings that apply globally are made by the customer’s organization. Ex: Google apps like Gmail, Salesforce, office 365. | 1 | 127 |
| Cloud - Serverless Computing  FaaS | Refers to new, non-traditional architecture as it does not use dedicated containers, event-triggered computing requests, ephemeral environment, servers fully managed by a third party (AWS) and are referred to as Function as a Service (FaaS) | 1 | 128 |
| Cloud - Infrastructure-as-code | IaC allow us to create infrastructure from templates. DevOps teams rely heavily on IaC. Security teams can introduce controls/checks prior to infrastructure being created. Many different tools available, from CSP’s native offering to third-party tools such as terraform, AWS Cloud Formation, Ansible, Chef, etc. | 1 | 130 |
| Could providers:  Amazon, Microsoft, Google | The cloud market space is rapidly growing and the three largest CSPs, Amazon’s AWS has strong offerings in the IaaS and PaaS space, but is now expanding more into serverless computing, artificial intelligence, and IoT. Microsoft offerings are split between Azure (IaaS, PaaS, serverless) and SaaS (Microsoft 365, Microsoft Dynamics). GCP (Google Cloud Platform) is less mature, IaaS and PaaS are still developing, Google workspace is the largest SaaS offering. | 1 | 133 |
| Cloud Security:  Shared responsibility | The term “shared responsibility” makes clear that neither a cloud provider, not a cloud subscriber is solely responsible for security and the responsibility can’t be offloaded from a subscriber to a provider. | 1 | 137 |
| Cloud security:  Point of demarcation | Is where the cloud provider responsibility ends, and the users begins. Remember, we chose to put our data in the cloud therefore we are responsible.9 | 1 | 137 |
| Cloud Security Alliance (CSA) | Organization dedicated to raising security awareness and best practices for secure cloud computer. Publishes the cloud security governance, Risk Management, and compliance (GRC) stack for the community such as Cloud Audit, Cloud Controls Matrix (CCM) and Consensus Assessments Initiative Questionary (CAIQ). | 1 | 142 |
| Cloud - CSA Cloud Security Guidance Project | The CSA Cloud Controls Matrix (CCM) provides fundamental security principles covered by the CSA Security Guidance. The CSA Security Guidance defines critical areas of focus for organizations managing and mitigating cloud risks. | 1 | 142 |
| Cloud – CSA Guidance Domain Matrix | There are 14 CSA guidance domains. See book | 1 | 144 |
| Cloud infrastructure leaders | There are 3, Amazon, Microsoft and google. They all have similar features but for the sake of training, we are just going to focus on AWS | 1 | 145 |
| Cloud AWA Regions and Availability Zones | A region is a physical location in the world that is composed of multiple availability zones and each availability zone consisted of one or more data center with redundant power, networking and connectivity. | 1 | 146 |
| Cloud – Virtual Private Cloud (VPC) | Provides a dedicated network inside an AWS account and logically isolate networks resources from other VPCs. Control networks flow using cloud-based networking (route tables, internet gateways, NAT, and network interfaces. IP address blocks are defined by Classless Inter-Domain Routing (CIDR) . VPCs m ay contain resources in both public and private subnets. Scoped to a single AWS Region. | 1 | 147 |
| Cloud – internet gateway (IGW) | Internet gateways connect resources or instances within a VPC to the internet and it is responsible for handling traffic from router tables. | 1 | 148 |
| Cloud – Subnets | Subnets divide cloud VPCs into smaller virtual network segments. | 1 | 149 |
| Cloud – Network Address Translation (NAT) Gateway | NATs enable the instances in private subnets to access the internet. | 1 | 150 |
| Cloud – Subnet Network Access Control Lists (NACLs) | VPC and subnet security starts with controlling traffic flow using a network access control list (NACL). The default NACL allows all inbound and outbound traffic and a custom can be associate with a lot of subnets. NACLs are stateless. | 1 | 151 |
| Cloud - Elastic Compute Cloud (EC2) | It provides a virtual computing in the cloud, configurable instance types with different CPU, Memory, storage, etc. Deploy into different regions and availability zones and Access Control using AWS key pairs. It also uses preconfigured templates using Amazon Machine Images and Control Traffic flow using security groups. | 1 | 152 |
| Cloud – Amazon Machine Images (AMIs) | Amazon Marketplace provides AMIs for new EC2 instances and supports several AMIs for customers to consume such as Amazon Linux, ECS Optimized, Windows Server, etc. Customers can create private AMIs stored in their account and can share public AMIs with the community. Vendors publish AMIs on the AWS Marketplace. | 1 | 153 |
| Cloud – EC2 Security Groups | Security groups control the ingress and egress traffic flow to an EC2 instance’s network interfaces. | 1 | 154 |
| Cloud – Management subnets | Secure cloud architecture commends created a separate management VPC as it contains bastion/RPD gateway to admin instances. VPC peering connectors to application servers/resources and can contain CI, CD, CM monitoring resources. | 1 | 155 |
| Cloud – serverless security Benefits | Surface attack is smaller, no servers to patch, no long running servers, fewer compromised servers | 1 | 156 |
| Cloud – Serverless Security concerns | Attack surface is bigger, as anyone can deploy a function, and the cost to deploy a function is zero and it is difficult to track and delete functions. Authentication and access control as we are not sure who is allowed to deploy functions and how to lock down each function. Lastly compliance. | 1 | 157 |
| Cloud – Serverless and application security. | Application security is even more important with serverless. Every function crosses a tryst boundary. Apply application security best practices | 1 | 158 |
| IEEE802.11 | Also known as traditional wireless | 1 | 170 |
| IEEE802.11 – Evolution | 802.11 refers to Part 11 of the 802 standards, created by IEEE (The institute of Electrical and Electronic Engineers). It was the first type of widely used wireless. The 802 standards give us the methods by which we can create LANs (local area networks) and MANs (Metropolitan Area Networks). Part 11 specifically gives us the methods by which we can create WLANs (Wireless Local Area Networks) | 1 | 171 |
| IEE802.11 – 802.11 | Is a standard that was created in 1997 and ratified in 1999. Over a dozen of amendments have been made since then, however is a document that is always being updated. Keep in mind that the amendments came with a potential risk. | 1 | 172 |
| IEE802.11 – 802.11 Amendments | Have focused on making improvements in the areas of performance, range, and reliability. Security has often not been the primary driver of amendments. Each amendment is represented by a letter added like 802.11ac and the letters will represent the amendments. | 1 | 174 |
| IEE802.11 – 802.11b | Supported a max of 11MBPs and operates in a 2.4 GHz. Ratified in 1999 and incorporated to the standard in 2007 | 1 | 175 |
| IEE802.11 – 802.11a | Supported a max of 54MBPs and operates in a 5 GHz. Ratified in 1999 and incorporated to the standard in 2007 | 1 | 175 |
| IEE802.11 – 802.11g | Supported a max of 54MBPs and operates in a 2.4 GHz. Ratified in 2003 and incorporated to the standard in 2007 | 1 | 175 |
| IEE802.11 – 802.11n | Brought substantial performance improvements and overcome limitations of early amendments. Leveraging new techniques such as MIMO (Multiple Input Multiple Output) and signal reflection and higher bandwidth to up to 100 Mbps. | 1 | 177 |
| IEE802.11 – 802.11ac | Shows us what is possible for WLAN with incredible improvements to range and bandwidth. Bandwidth of 1 Gbps up to 6.77. operates in the 5 ghz frequency range and was ratified in 2013 and incorporated in 2016. | 1 | 179 |
| IEE802.11 – 802.11ax | Represents the future of WLAN capability and it is proof WLAN networks must be able to support simultaneous access to large amounts of bandwidth. | 1 | 181 |
| IEE802.11 – (In)Security: WEP | WEP or wired equivalent privacy was design to prevent a signal from being intercepted and was design to protect the confidentiality of data transmitted across the WLAN via the use of encryption by using RC4 symmetric stream cipher. | 1 | 187 |
| IEE802.11 – (In)Security: WEP issues | Limited to 40-bit, RC4 relies on the concept of key material NOT repeating and an IV (Initialization Vector) is combined with pre-shared keys. WEP based network can be discovered in less than a minute and WEP was deprecated in 2004 and should not be used. | 1 | 189 |
| IEE802.11 – (In)Security: WEP replacements Wi-Fi Alliance | The WEP replacements were created in conjunction with work performed by the Wi-Fi Alliance and a membership representing companies, consumers, etc was created. The Wi-fi alliance was created to certified providers. | 1 | 191 |
| IEE802.11 – (In)Security: WPA1 | WPA1 was released in 2003. RC4 used an underlying encryption algorithm same as WEP to facilitate a software upgrade and TKIP (temporary key integrity protocol) to generate better encryption keys and MIC (Message Integrity Check) to prevent forgery attacks. Deprecated on 2009 due to several vulnerabilities. | 1 | 194 |
| IEE802.11 – (In)Security: WPA2 | Represents the strongest protection for WLAN. Ratified in 2004, and the only amendment with security focus. AES (advanced Encryption Standard) uses 128 key lengths for confidentially protection. It’s been available for 15 years. | 1 | 196 |
| IEE802.11 – (In)Security: WPA3 | Full specs were released in 2018, and vendors agreed it will take tame for accessibility. All devices issued a Wi-Fi 6 certification will need to support WPA3. | 1 | 199 |
| IEE802.11 – (In)Security: WPA3 Enhancements | 192-bit key length, 128 bits still supported, 192 bit is an optional choice. Better implementation of pre-shared Keys (PSK), better password guessing protection, and OWE (Opportunistic Wireless Encryption). | 1 | 201 |
| IEE802.11 – (In)Security: WPA3 Attacks | Even though WAP3 is new, it’s been discovered there are some vulnerabilities such as downgrade attacks, password cracking and Denial of Service DoS. | 1 | 204 |
| IEE802.11 – (In)Security: Rogue Access Points | This is a downgrade attack and was Initially referred to an unauthorized access point connected to the internal wired network and created an evil twin and force the user to downgrade the client to a WPA2. | 1 | 208 |
| IEE802.11 – (In)Security: DoS | Wireless communications are simply radio signals being sent through the air all around us and can only be successful if the communication devices can “hear” each other. bSignals that are present that we didn’t create can be referred as noise and noise can be created to “Jam” a signal. Best mitigation is early detection. | 1 | 210 |
| Wireless – PAN | Short for “Personal Area Network”. It is a network that exists around our person and in our personal space. Make not that PAN lacks privacy and anyone can connect to it such as a Bluetooth and Zigbee. | 1 | 213 |
| Wireless – PAN Bluetooth | Design to create a personal network for devices that interact in our personal space and replace cables, first implemented for mice, keyboard and printers, and became popular for “hands-free” communication. Its software and hardware have evolved to send signals from far away making attacks easier. | 1 | 215 |
| Wireless – PAN Bluetooth attack | “BlueBorne” vulnerabilities include remote code execution and information disclosure that can result in exposure of encryption keys. The number of impacted devices were in the billions including Android, Windows, smartphones, refrigerators, Etc. | 1 | 217 |
| Wireless – PAN Bluetooth protections | Try to use the latest version of Bluetooth and that might mean software and hardware upgrades. Disable unnecessary profiles, don’t leave it always one, install all available patches . | 1 | 219 |
| Wireless – PAN: Zigbee | Low-cost alternative to other PAN technologies, can be run on a battery and last years. Best defined as an “automation” technology and doesn’t have one single standard but a collection of related technologies with security being included in the standards. | 1 | 221 |
| Wireless – PAN: NFC | “Near Field Communications” design to operate in close proximity of 1 to 2 inches. Used in contactless debit cards, transit passes. Security is determined by the vendor since this technology is widely used in many different markets. | 1 | 223 |
| Wireless – PAN RFID | “Radio Frequency Identification” linked to tags and can be attached to an object for identification, almost like a serial number. | 1 | 225 |
| Wireless – 5G | Is the next evolution for mobile communications, and has improvements such as low latency, high bandwidth and multiclient support. Smartphones will start using it first but won’t be available everywhere in the world. | 1 | 228 |
| Wireless – IoT | Concept created to represent of non-traditional computing devices on networks such a light bulb, refrigerators, thermostats, toothbrushes. These devices are computers with RAM, storage, software code and OS and requires the same protections given to desktops and servers. IoT can leverage Bluetooth, Zigbee, Wi-Fi, 5G, etc. | 1 | 231 |
| Defense in depth | There is not just one way to protect all your assets and to prevent an attack, we need to deploy multiple levels of protection across a wide range of controls. Prevention is ideal, detection is a must but detection without response, is useless. | 2 | 5 |
| Defense in depth –  Layers | Describe what kind of protections should be in place, such as perimeter security, network security, host security, application security and Data security. | 2 | 5 |
| Defense in depth –  Perimeter security | Focuses on security controls at the borders of a network such as firewalls, proxy servers, and anti DDoS appliances. This is referred at the protections between you and the internet. | 2 | 5 |
| Defense in depth –  Network Security | Aims to protect the internal network. “Network Segmentation” and “Network Access Control” are key security controls. | 2 | 5 |
| Defense in depth –  Host security | It is all about hardening systems and securing the setup and endpoints of servers by securely configuring the system, implementing an application control solution, scanning the system for vulnerabilities, and installing anti-malware agent. | 2 | 6 |
| Defense in depth –  Application Security | Refers to creating a secure application by the means of implementing authentication mechanisms, writing overflow protections, performing input validation, etc. | 2 | 6 |
| Defense in depth –  Data Security | Techniques such as encryption and data classification in order to handle data properly according to its sensitivity. | 2 | 6 |
| Risk | Is the level of exposure to certain danger and is composed of a vulnerability threat level. Risks, threats, and vulnerabilities are highly interrelated.  **Risk** (due to a threat) = **Threat** x **Vulnerability** (to that threat) | 2 | 6 |
| Risk Key Focus –  CIA | Are confidentiality (vs. Disclosure), Integrity (vs. Alteration) and Availability (vs. Destruction). | 2 | 9 |
| Risk Key Focus –  CIA: examples | **Confidentiality:** customers will expect that the privacy of their credit card numbers, or other information shared during a transaction to be ensured.  **Integrity:** Customer will expect product availability to be accurate, to quantities and quality be what they agreed to, and anything that they download be authentic and complete.  **Availability:** Customers will expect to be able to place orders when is convenient for them and the employer will want the revenue stream to not be disturbed. | 2 | 9  11 |
| Risk – Right Balance | Security vs. Functionality: Application updates bring more functionality over time; however, more functionality typically means a drastic drop in security. | 2 | 12 |
| Filtering | Filtering is the foundation of Defense in Depth. We have Network Filtering technologies such as firewalls, Anti-DDoS, Proxy Servers, Mail Relays and Host-Based Filtering Technologies like Anti-malware software and application control. | 2 | 14 |
| Approaches | There are 4 basic approaches: Uniform protection, protected enclaves, information-centric, and threat vector analysis. | 2 | 16 |
| Uniform protection | This is the most common approach to DiD. In this setup, all parts of the organization receive equal protection and are treated the same. This is a very common approach and the weakest. | 2 | 17 |
| Protected Enclaves | Assets that require additional protection are segmented from the rest of the internal organization, and access to it is restricted. This can be done by using VLANs or Network Firewalls or (N)ACLs. | 2 | 18 |
| information-centric | Any organization uses multiple layers to access confidential information and they need to build successive layers of protection on top of your other layers. It is key that proper data classification standard is in place, security controls for each confidentiality level are defined. | 2 | 19 |
| Vector-Oriented threat analysis | A threat requires a vector to cross the vulnerability. Preventing the threat from using that vector will stop its capability to exploit it. Vectors such as malicious USB Drives, attachments containing malware, spoofed emails. | 2 | 20 |
| System Security Layer | Most of the DiD principles are focused on the network layer which focused on filtering. At a system level we can implement configuration hardening on assets such as network components, operating systems, software and cloud environments to protect this layer. | 2 | 21 |
| Configuration Management | Is the discipline of establishing a known baseline condition such a document compliant with applicable standards and then managing that condition. Revie and change control are critical as they provide a way to detect when a change occurs to that baseline. | 2 | 23 |
| Configuration management –  Fixing it | The main strategy for fixing an infected system is to rebuild that system from scratch because you would never know if there is anything that was left behind if we don’t have a baseline. | 2 | 25 |
| DiD – Not limited to on-premises | Did is not only applicable to your own-premise environment, thing larger cloud environments, you will find several security controls that can be implemented on different layers. | 2 | 26 |
| Defense in depth in the cloud | It is something that can be done on premises and in the cloud just as easy. | 2 | 27 |
| On Premise IAM | Identity And Access Management Authentication includes multiple components. Context based authentication is enforcer via multiple technologies such as multifactor authentication and device compliancy checks. | 2 | 30 |
| Azure AIM | Azure makes use of a “IF-This-THEN-That” mechanism that allows an administration to tell the system what to do in certain conditions.  Conditional access will validate several settings based on the polices that were created. There policies will be defined in your Azure administrative portal. Then, Based on conditions that were met a risk level is applied and certain actions are defined in the “then” part of the policy. | 2 | 31 |
| AWS AIM | Similar to the other platforms, AWS allows for multi-factor authentication and “Identity Federation”, meaning a user can either be logged in with a designated AWS account or with an account on another platform (Google account, Microsoft account, etc) That has been linked to AWS. After the user has been authenticated, they can then access the resources on the system that they have been authorized to. | 2 | 32 |
| GCP AIM | Role based access control means that you gain access depending on your job function and only when you need it. | 2 | 34 |
| On-premises Network Segmentation | Network segmentation is typically done by splitting up networks into different zones (VLANS) and firewalls to control and allow access to specific resources within your network. | 2 | 35 |
| Azure Network Segmentation | For IaaS Azure uses virtual networks band network security groups to do stateful packet inspection. A network security group is reusable object within azure that can be assigned to an azure resource. | 2 | 36 |
| AWS Network Segmentation | Amazon AWS uses VPC, security groups and Networks access control list to enable segmentation. A Security group acts as a virtual firewall that controls the traffic for one or more instances. | 2 | 37 |
| GCP Network Segmentation | Google Cloud Platform uses virtual private cloud and VPC Firewall Rules that filter both ingress and egress traffic on a per-instance basis to allow network segmentation. | 2 | 38 |
| Defense in depth: shortfalls | Internal threats already bypassed a few of the outer security controls. The rise of unmanaged devices within a network such as mobile phones and tables from a new challenge to secure environments. | 2 | 39 |
| Zero-Trust | Every request, regardless if it comes from inside or outside your network perimeter, must be properly authenticated an authorized . It does not replace the Defense-in-Depth principle but complements it. | 2 | 39 |
| Zero-Trust:  Basic principles. | Internal and external threats will always be present. Every user, device or network connection must be proven, log and inspect all network traffic. | 2 | 40 |
| Zero-Trust:  Securing your traffic. | All traffic must be Authenticated to prove the user, device, or network connection is legitimate and Encrypted to protect the confidentiality of the traffic while cryptographically proving its source and destination. | 2 | 41 |
| Zero-Trust:  Variable trust | Variable trust enables you to dynamically change access for good or bad based on conditions. Some conditions that can be used to dynamically change access are Type of user access, Geo Location, Device compliancy and type of application. | 2 | 42 |
| Zero-Trust: Variable trust examples | An employee wants to access an internal application. The access is granted when the variable trust score is 30 or above. | 2 | 43 |
| Zero-Trust:  Log inspection | For zero trust to work, logging and inspection is required. This is often seen as the need to log everything centrally, which is then left there to be forgotten. | 2 | 44 |
| Digital identity | Is the online persona of a subject. A single subject can have multiple digital identities for different services. | 2 | 48 |
| Authorization | Is the process of determining what a subject is allowed to do or access after authentication. | 2 | 48 |
| Authentication | Is a process in which a subject proves they are in the possession of one or more valid authenticators associated with an identity. It relays in 3 factors: Something you know such as your password, something you have such a token, and something you are like your thumbprints or retina (Biometrics) | 2 | 48  55 |
| Accountability | Is the process of identifying who did what on the system, as well as when they did it. | 2 | 48 |
| Identity Access Management IAM | Is the organizational process for identifying, authenticating, and authorizing individuals or groups of people to have access to applications, systems, or networks by associating user rights and restrictions with established identities. | 2 | 50 |
| Process of enrollment | An individual can become a subscriber to a system and going through the process of enrollment. The outcome of enrollment is typically the assignation of a user ID and credentials. This this end, the applicant will undergo identity proofing by the system owner. Examples: Identity proofing, identity assurance levels, and credentials. | 2 | 51 |
| Identity Proofing | The process has 3 distinctive steps. Resolution, Validation and Verification. It is the process in which an applicant proves they are who they claim to be. After successfully undergoing the identity proofing, the applicant is provided with one or more credentials they can use at a later time to authenticate the system. | 2 | 52 |
| Identity Assurance Levels (AIL) | Depending on the contexts of the enrollment, a verifier can require different levels of certainty concerning an applicant identity. NIST outlines three different Identity Assurance levels with varying degrees of proofing requirements. | 2 | 53 |
| Identity Assurance Levels (AIL) 1:  Self-asserted | Any information on the applicant’s attributes is deemed self-asserted and, thus, cannot be confirmed | 2 | 53 |
| Identity Assurance Levels (AIL) 2:  Evidence based | Applies to situations where the system owner is somewhat assured the applicant is associated with the real-world identity they claim to have. Additionally, there is the possibility for the identity of the applicant to be verified by a third party,. The credential service providers who will assert their attributes. | 2 | 53 |
| Identity Assurance Levels (AIL) 3  Evidence based | Applies to situations where the system owner has performed a direct verification of the identity of the individual, the applicant needs to be physically present and has to provide substantial evidence to prove their identity. | 2 | 54 |
| Authenticator Assurance Levels (AAL) | Depending on the sensitivity of the resource being accessed and the context of the access requested, the user can be asked to provide a different level of user authentication. NSIT outlines three different authenticator assurance levers with varying degrees of proofing requirements such as Single factor at least, any two factors and strong crypto, and selected 2 factors and strong crypto | 2 | 56 |
| Authenticator Assurance Levels (AAL1) Single Factor at least | Requires either single-factor or multifactor authentication using a wide range of available authentication technologies. | 2 | 56 |
| Authenticator Assurance Levels (AAL2) Any two factors & strong crypto | Proof of possession and control of two different authentication factors is required through secure authentication protocol and approved cryptographic techniques are required. | 2 | 56 |
| Authenticator Assurance Levels (AAL3) Selected 2 factors & strong Crypto | Based on proof of possession of a key through a cryptographic protocol. It requires a hardware-based authenticator and an authenticator that provides verifier impersonation resistance. | 2 | 56 |
| Single sign-on (SSO) | A single Sign-On system allows the user to authenticate once with a single set of credentials in order to access different resources. It doesn’t mean single authentication; it is a balance approach where users automatically login. | 2 | 57 |
| SSO protocols: SAML 2.0 | “Security Assertion Markup Language” Is an XML based protocol for exchanging identities. It uses tokens containing information about the identities to enable SSO on different environments. | 2 | 59 |
| SSO protocols: OAuth 2.0 | Is an open standard for access delegation, it is used to grant websites or applications access to their information on other websites but without exchanging passwords. In general OAuth 2.0 provides secure delegated access and supports SSO. | 2 | 60 |
| Access control | Is the broader concept of controlling the access to resources, as well as managing this access. Additionally, constant monitoring is needed in the process to ensure access is revoked when it is no longer needed. The 3 most important concepts are controlling access, managing access and monitoring access. | 2 | 61 |
| Controlling access | The most important principles associated with controlling access are Least privilege, Need to know, Separations of Duties and Rotation of Duties. | 2 | 62 |
| Access control techniques | There are many types but the most important are: Discretionary access control (DAC), Mandatory access control (MAC), Role-Based Access control (RBAC) and Lattice-Based Access Control (LBAC) | 2 | 64 |
| Access control techniques:  Discretionary Access Control (DAC) | Is a type of access control that controls access to certain resources via a credential given to the authorized party. This party is able to transfer this credential and, thus, authorization to another party at their own discretion | 2 | 64 |
| Access control techniques:  Mandatory Access Control (MAC) | Is a type of access control that controls access to all resources via System-enforced credentials that are nontransferable by the authorized party. MAC requires all users of the system to be assigned a clearance as well as all data to be assigned a classification level. | 2 | 64 |
| Access control techniques:  Role-Based Access control (RBAC) | Is a type of discretionary or mandatory access control that assigns users to roles or groups based on their organizational function(s). Each group is associated with an authorization to access certain resources. | 2 | 65 |
| Access control techniques:  Lattice-Based Access control (LBAC) | Is a type of mandatory access control that defines access restrictions on the interactions between subjects and object. A subject is only allowed to access an object if the security level of said subject is greater than or equal to that of the object. | 2 | 65 |
| Managing and Monitoring access | It is a process called “Access Management” and consists of 4 tasks. Account administration, maintenance, monitoring and revocation.  Account administration is a setoff processes and controls. Maintenance is the process of reviewing account data and spot-checking for inconsistences or errors. Monitoring is enforcing accountability of accesses to information, authentications and authorizations and Revocation is when account management staff and systems administrators revoke privileges when they are no longer needed, especially if users have been fired. | 2 | 67 |
| Privileged access | Is the access to a computer system with the elevated access rights, such as a root or administrator access, or access to service accounts. | 2 | 68 |
| Password vault: privileged access management tools | Enable an organization to regulate who can get privileged access to their critical systems. It is also transparent to the user, provides policy enforcement, generate strong shared secrets, securely store credentials, rotate credentials, monitor, and log privileged access, and generate reports. | 2 | 69 |
| Azure privileged identity management | To implement the least privilege principle within Azure AD, privileged identity management can be used to assign on-demand, time limited, administrative privileges when approved by a workflow. | 2 | 72 |
| 3-Tiered privileged access management. | It is basically separating the administration of, for example, end-user workstations and domain controllers. For example, tier 0 users have access to active directory, critical and secret servers (crown Jewels) and not tier 1 tools such as exchange servers, intranet servers, and tier 2 tools such as workstation, printers, mobile devices and vice versa. | 2 | 73  75 |
| Authentication Types | They are different factors of authentication. Something you know, something you have, and something you are. | 2 | 78 |
| Something you know | A memorized secret authenticator or a password, or a pin, it is a secret value intended to be used by the user. | 2 | 79 |
| Something you have | Look-up secrets, out-of-band devices, OTP Tokens, Cryptographic devices | 2 | 79 |
| Something you are | Fingerprints, retina scans, voice recognition, facial recognition | 2 | 79 |
| Storing passwords | Storing passwords in clear text on a specific system is not the best practice. Hashing is a one-way transformation of password, and it is practically impossible to turn that string into the original readable password. | 2 | 81 |
| Key Derivation functions | Irreversible hashing function, input transformation, salt (and pepper( values, difficulty factor. | 2 | 82 |
| Strength of a password hash | Key Derivation function quality, password & derived Key length, Character set support, difficult factor. | 2 | 84 |
| Key derivation function: PBKDF2 | DK = PBKDF2(PRF, Password, Salt, c, dkLen)  PRF: a pseudorandom function to 2 parameters with output length hLen such as HMAC-SHA3. C: cost factor or number of iterations, and dkLen: derived key length. | 2 | 86 |
| MD5 | Is a cryptographic hash algorithm which produces a hash value in hexadecimal format. This algorithm has serious weaknesses as it is known to have hash collisions. A collision happens when 2 unique plaintext hash to same hash value. | 2 | 87 |
| SHA | Secure Hash Algorithm . There are several iterations: SHA, SHA1, SHA2 and SHA3. Passwords saved in online databases are typically stored as SHA hash. | 2 | 88 |
| LM hash | LM or Lan Manager hash was introduced by Microsoft in 1980 and has multiple weaknesses. The LM hash is typically stored in the system in the SAM/NTDS database. 2 severe weaknesses are a maximum password length, or 14 characters and passwords converted to uppercase. | 2 | 89 |
| NTLM (NTHash) | Is the successor of LM. Is a challenge and response authentication mechanism which uses messages to authenticate a certain client. | 2 | 89 |
| NTLMv2 | When Kerberos is not available, windows will fall back to NTLMv2. Authentication is a 2-party: the client and the server and it takes 3 steps, Negotiate, challenge and response. Within a windows domain, it is vulnerable to relay attacks. | 2 | 91 |
| Password dumps | Password cracking requires the attacker to possess a list of hashed passwords. Often, these passwords are obtained from the internet in so-called password dumps. | 2 | 92 |
| Password Cracking | Is the process of trying to guess or determine plaintext passwords, given only hashed passwords. The process does not actually break the encryption, it mimics the actions that would take place if a user tried passwords until guessing the right one. The cracking operation is usually performed offline against a recovere4d password file. | 2 | 93 |
| Password cracking method | Using a password hashing tools like Mimikatz or hashcat, determine the encryption algorithm used, create a list of possible passwords, encrypt each password in the list, and determine whether there is a match with the collected hashes. | 2 | 94 |
| Password cracking specialized attacks | Brute Force attack, Dictionary attack, hybrid attack, pre-computation attack | 2 | 96 |
| Brute force attack | The most powerful cracking method. Enumerate all possible combinations, slowest attack, 100% success rate given enough time. | 2 | 96 |
| Dictionary attack | Enumerate all entries from a dictionary or wordlist, fastest attack, only effective against weak passwords. | 2 | 96 |
| Hybrid attack | Extends dictionary attack with numerals and symbols, combines effectivity of brute force with speed of dictionary attack | 2 | 96 |
| Pre-computation attack | Trades processing cycles for memory, hashes for attack are pre-computed and stored in “rainbow tables”, significantly increases cracking speed. | 2 | 97 |
| Speeding cracking process: GPU Acceleration | Password cracking is highly suitable for applying data parallelism. This means the process of calculating hashes can be split up over large amounts of processing units (CPU cores). Highly specialized password cracking can be done using tools that make use of the larger number of cores presents on hardware like GPUs, with OpenCL or CUDA APIs. | 2 | 98 |
| Speeding cracking process: Rainbow tables | Enables the attacker to trade CPU or GPU cycles for memory, As password cracking comes with a high computational cost, it can prove beneficial to calculate hashes in advance. The use of pre-computation attack can immensely speed up the cracking process. | 2 | 98 |
| Strong password: DO | Force length to >8 characters, check for recognizable words of numbers of sequences, block after x failed attempts, force change in case of (suspected) breach. | 2 | 99 |
| Strong password: DO NOT | Truncate passwords, allow password hints, force specific composition rules, force periodic password changes, save passwords in clear text | 2 | 99 |
| Fighting pre-computational attacks | Can be fought by preventing hashes from being exact representations of passwords or “salting and Peppering” | 2 | 101 |
| Salting | Additional input for KDF ensures output is different for different salts. Salts are unique per password, but not secret | 2 | 101 |
| Peppering | Additional KDF ensures hashes cannot be reproduced, peppers are unique per application and secret. | 2 | 101 |
| Salting example | Please see book | 2 | 102 |
| Password cracking tools | Hashcat, Mimikatz | 2 | 103 |
| Hashcat | Is a password cracking tool that takes advantage of the potential hardware acceleration provided by parallelizing the workload over multiple cores. | 2 | 104 |
| Mimikatz | Mimikatz is a feature-rich post-exploitation tool that can be used to extract plaintext passwords, PINs, hashes, and Kerberos tickets from system memory on windows machines, as well as exploit several vulnerabilities and apply multiple credential-gathering techniques. It can be used as a standalone tool, has a PowerShell version, and is also integrated in Metasploit and meterpreter modules | 2 | 106 |
| Multi-factor authentication | Is a method of authentication in which access is only granted after being presented with more than one authenticator. Often MFA combines a shared secret (something you know) with an OTP token (something you have) or Biometrics (something you are). | 2 | 108 |
| Adaptive authentication | In an adaptive authentication mechanism, the party that is requesting access will need to provide one or more authenticators, depending on the context of their request and the sensitivity of the resource they are attempting to access. | 2 | 109 |
| Security Frameworks | Provide guidance for organizations such as “CIS Center for Internet Security”, “NIST National institute of Standards and Technology”, and “MITRE ATT&ACK" on prioritizing their most critical risks. | 2 | 114 |
| CIS: Principles | Defenses should be automated where possible and periodically or continuously measured using automated measurement techniques where feasible.  To address current attacks occurring on a frequent basis against numerous organizations, a variety of specific technical activities should be undertaken to produce a more consistent defense.  Root cause problems must be fixed in order to ensure the prevention or timely detection of attacks.  Measures should be established that facilitate common ground for measuring the effectiveness of security measures, providing a common language to communicate about risk. | 2 | 117  118 |
| CIS: Controls summary | There are 5 critical rules: Offense informs defense, prioritization, measurements and metrics, continuous diagnostics and mitigation, and automation. | 2 | 119 |
| CIS: Controls | CIS controls are 20 rules and are split into 3 groups: Basic (Controls 1-6), Foundational (Controls 7-16) and Organizational (Controls 17-20). Please see book | 2 | 120 |
| CIS Control #2 Example | “Inventory and Control of Software Assets”. The goal of this control is that only authorized software should be installed on the organization’s computers systems. | 2 | 122 |
| CIS control #2 Core evaluation test | Install a benign software application on 10 unauthorized devices on various portions of the organization’s network unannounced to see how long it takes for the software to be detected. | 2 | 123 |
| CIS control #2 Measures | 1. How may unauthorizes software applications are presently located on business systems within the organization (By business unit)? 2. How long, on average does it take to remove unauthorized applications from business systems within the organization (by business unit)? 3. What is the percentage of the organization’s business systems that are not running application control software that blocks unauthorized software application software applications (by business unit)? 4. How many software applications have been recent blocked from executing by the organization’s application control software (by business unit)? 5. How long does it take to detect new software installed on systems in the organization (time in minutes, by business unit)? 6. How long does it take to remove unauthorized software from one of the organization’s systems (time in minutes, by business unit)? | 2 | 124 |
| NIST Cyber Security Framework | The NIST framework is a risk-based approach to managing cybersecurity risk and includes 3 parts:   1. The framework core: consists of 5 concurrent and continuous functions. “Identify, Protect, Detect, Respond, Recover” 2. Framework implementation tiers: contextualize risk for a specific organization and how these risks can be managed. “T1 Partial, T2 Risk informed, T3 Repeatable, T4 Adaptive” 3. Framework profiles: the profile is typically used a target and provides guidelines or us being used as a roadmap to further strengthen your security controls. | 2 | 125 |
| NIST Framework Core: Identify | Develop an organizational understanding to manage cybersecurity risk to systems, people, assets, data and capabilities. | 2 | 126 |
| NIST Framework Core: Protect | Develop and implement appropriate safeguards to ensure delivery of critical services, an example is to use perimeter filtering. | 2 | 126 |
| NIST Framework Core: Detect | Develop and implement appropriate monitoring capabilities, this means looking at certain events and alerting policies. | 2 | 126 |
| NIST Framework Core: Respond | Develop and implement appropriate activities to take action regarding a detected security incident. | 2 | 126 |
| NIST Framework Core: Recover | Develop and implement appropriate activities to plan for resilience and restore capabilities | 2 | 126 |
| NIST Implementation tiers | Implementation tiers provide context on your organization and the process in place to manage certain types of risk. Organizations should determine the desired tier. If an organization identifies a certain control as Tier 1, they should be encouraged to move to Tier 2 or greater. | 2 | 128 |
| NIST Implementation tiers: T1 Partial | Certain controls are partially implemented, processes are not formalized and there is limited awareness of cyber security risks. This is the lowest tier within the NIST Cybersecurity Framework. | 2 | 128 |
| NIST Implementation tiers: T2 Risk informed | Risk management practices are formalized and approved by management. It has not been published organization wide and cyber risk awareness is limited to the organization level. | 2 | 128 |
| NIST Implementation tiers: Tier 3 Repeatable | Risk management practices are formally approved and expressed as policy. There is an organization-wide approach to manage cybersecurity risk. | 2 | 128 |
| NIST Implementation tiers: Tier 4 Adaptive | Adapts cybersecurity practices based on previous and current cybersecurity activities, including lessons learned and predictive indicators. this includes continues improvement. | 2 | 128 |
| NIST Frameworks Profiles | Within the framework profile, you align the functions, categories, and subcategories based on your business needs. Your profile is based on risk appetite and risk tolerance and, depending on your security profile, additional security controls can be implemented. | 2 | 130 |
| MITRE ATT$CK | Is a globally-accessible Knowledge base of adversary tactics and techniques based on real-world observations. The ATT$CK knowledge base is used as a foundation for the development of specific threat models and methodologies in the private sector, in government, and in the cybersecurity product and service community. | 2 | 131 |
| MITRE ATT$CK Tactics and Techniques | Tactics are used to describe high-levels attacks steps used by an adversary. MITRE ATT$CK assumes break and thus the “first” tactic is initial intrusion | 2 | 131 |
| MITRE ATT$CK: Matrix | It is pretty extensive and is divided in sub-techniques, tactics, and techniques. Please see book for more info | 2 | 132 |
| MITRE ATT$CK: Technique details | It gives information about the techniques being used by actual adversaries. The technique valid account is categorized as initial access and explains how attackers are using compromised credentials. In addition, ATT$CK also describes the data sources required to detect these types of techniques. | 2 | 133 |
| MITRE ATT$CK: Mapping to known adversaries | Knowing which adversaries are known to abuse the technique (threat intelligence), you can map this technique toward a known campaign and look for specific details within your environment. | 2 | 134 |
| Security frameworks: Other frameworks | All security controls have similarities. EX: CIS controls are complementary to other information security standards, such as ISO27001 or NIST 800-53 standards and security controls. | 2 | 135 |
| DL Data Loss | Data loss occurs when data is being corrupted, deleted or made unreadable in any way | 2 | 141 |
| Data Leakage | In most cases, data leakage is categorized as a security incident that result in data being access in a security incident that results in data being accessed in an unauthorized way. One of the typical examples is exposing data on publicly available sites by using external sharing platforms | 2 | 141 |
| DL: Types | Procedural, (un)intentional, failure, disaster, crime. | 2 | 142 |
| DL: Cost | Value of lost data, cost of continuing without, cost of recreation, reputational damage. | 2 | 142 |
| DL: Prevention | Backups, Data Redundancy. | 2 | 142 |
| DL: Recovery | Data Recovery labs, dependent on storage mediums. | 2 | 142 |
| Ransomware | Is a variety of malware that, upon infecting a system, encrypts all the data on the hard drive it can find. Subsequently, the user of the system is prompted with a screen explaining what has happened and a ransom note requiring them to pay a certain amount of money, often in the form of cryptocurrency in order to get their data back. More often than not, even after payment, the user does not get a way to retrieve their data and the data is lost forever. | 2 | 143 |
| Data Loss Prevention strategies | Redundancy, Backups, Access Control. | 2 | 144 |
| Data Loss Prevention strategies -  Redundancy | In-house, Cloud infrastructure. | 2 | 144 |
| Data Loss Prevention strategies - Backups | On-site, Off-site, Automated. | 2 | 144 |
| Data Loss Prevention strategies - Access Control | Need-to-have, Prevents Accidental deletion | 2 | 144 |
| Redundancy: in House | Error-Correction Code (ECC Memory) adds some extra bits to each data unit, enabling the system to detect if a bit in the data has been c hanged accidentally and to correct the issue. RAID configurations (Redundant Array of Independent Disks) it is a way of combining multiple physical hard drives into one or more logical drives on the system. Data redundant file systems (btrfs, zfs) or journaling filesystems that keep a log of the changes made and intend to make to the system. In the event of a crash during a write or delete operation, the system can simply reconstruct a valid state by repeating the steps as kept in the journal logbook. | 2 | 145 |
| Redundancy: cloud | Solutions often offer replication between so-called “storage nodes”. There are abstractions of physical storage devices in the data center on which the data is stored when one node fails it will retrieve the data from another node. Availability, integrity, Geo-Replication | 2 | 146 |
| Redundancy: Cloud – Data Availability | Administrators can set a system parameter that forces replication on at least N nodes. This ensures there are always N copies of the data. | 2 | 146 |
| Redundancy: Cloud – Data integrity | When retrieving data, replication nodes can come to a consensus on the value of the data to ensure it wasn’t corrupted on a single node | 2 | 146 |
| Redundancy: Cloud – Geo-Replication | Replication between regions ensures data can be recovered even in the event of a regional disaster like an earthquake. | 2 | 146 |
| Backups: Methods | Full system imaging: copying the entire system in a single image and storing it, continuous backups: Stores data automatically after each change is made to its data, incremental backups: Store data changed since a reference point in time, and differential backups: stores the difference between the current data and the data stored in the last backup. | 2 | 148 |
| Backups: Common Pitfalls | Backup storage should not be connected to the network when not actively taking a backup. Often a cloud vendor only has limited retention periods for backup data. In this case, it might be necessary to store the backup data yourself if it needs to be kept for a longer time than the given retention time. If all the systems are running on the same OS, a single compromise might spread across the entire network. Sometimes a backup does not get properly scheduled, or the backup data itself gets corrupted during the backup process | 2 | 149 |
| Data Recovery | Is a procedure in which corrupted or unreadable data in recovered from a faulty storage medium. It is usually 4 steps: Repair storage medium, Image data to another medium, Logical data recovery, Repair damage data. | 2 | 150 |
| Data leakage | It is when we lost control of our data | 2 | 151 |
| Data leakage: Types | Breaches, insider leaks. | 2 | 151 |
| Data leakage: Cost | Business losses, reputational damage, fines. | 2 | 151 |
| Data leakage: Prevention | Secure data storage, intrusion detection & prevention, Data exfiltration | 2 | 151 |
| Data leakage: insider threats | Insider threat program, user access monitoring, third-party risk management | 2 | 151 |
| Data leakage: Business losses | Leaked trade secrets or sensitive data can lead to large business losses | 2 | 152 |
| Data leakage: Reputational Damage | Data breaches involving sensitive (user) data can lead to reputational damage | 2 | 152 |
| Data leakage: Fines | Strict regulations apply to data security. Data breaches may lead to high fines | 2 | 152 |
| GDPR | Regulation (EU) 2016/619, also known as the “General Data Protection Regulation”, is a European law enacted in 2016 that outlines data protection measures that need to be taken when an organization collects and processes personal data. | 2 | 153 |
| CCPA | “The California Consumer Privacy Act” is a recently enacted law from 2018 that grants rights concerning privacy to Californian consumers and outlines requirements for organizations on how to process consumer data. | 2 | 153 |
| DLP Storing Sensitive Data | Digital: Encrypt sensitive data should always be stored with strong encryption, delete sensitive data when it is no longer needed.  Physical: having a clean desk policy, shredding data. | 2 | 157 |
| DLP Policies | Aim to provide a better way to protect digitally stored data both in transit and at-rest. A policy defines locations where the tool must monitor for sensitive data, under which conditions it should intervene, and which actions needed to be taken automatically, by the tool when these conditions are fulfilled. | 2 | 158 |
| DLP Policies: Data Classification Labels | To properly function, DLP tools allow the definition of Data Classification Labels. Each piece of data must be assigned such label to designate how sensitive it is an what the appropriate security requirements for the data are.  The owner of the data should assign the label to the data. If needed a DLP tool can often make suggestions to the data owner on which label to use depending on the contents of the data and whether any sensitive information has been found. | 2 | 159 |
| DLP Policies: Data In-Transit | Detect transmission with sensitive data in real-time and take appropriate action such as escalate to a manager for approval, block transmission, alert security staff, remove sensitive data before transmission. | 2 | 161 |
| DLP Tools | DigitalGuardian, Forcepoint, Office 365 DLP | 2 | 162 |
| Digital intrusion | A way for advanced adversaries to steal your online data. Data that is kept offline is not accessible to a digital intruder. Most data have to be online, but archived data, can be stored on storage media that is not directly online thus limiting the impact of a ransomware attack. | 2 | 163 |
| Intrusion Detection and Prevention | We have 2 types of Intrusion Detection Systems (IDSs): Network IDS – Online: is done by real-time traffic analysis, and applies basic detection rules, and Offline: stored traffic analysis, allows for more thorough analysis. Network IDS-Hosts: Logs, and Malware Detection | 2 | 164 |
| Data Exfiltration | When and adversary has successfully intruded the system, they still need to find and extract interesting data. Often this can set off some alarm bells and it is usually 3 steps such as: Search for interesting files, Collect and prep interesting files, exfiltrate interesting files. | 2 | 165 |
| Data Exfiltration: Prevention | Ensure the organization knows what data it possesses and that it is correctly classified. Limit user access only to data they should be allowed to access (“need to know”). Next to limiting user access to data, also consider what type of data you store where.. this includes network segmentation, but also even considering storing some data offline. | 2 | 167 |
| Data exfiltration: Detection | A system-wide search generates a lot of activity on the system being searched. Monitoring for searches through filesystems in not trivial, through there will be several false positives such as antivirus scanners, search indexers, backup programs, etc. Access to network shares can however be monitored (Event ID 5140) – “A network share object was accessed”). Look for repeated audit failures from one source. | 2 | 167 |
| Insider threats | Insiders in the organizations are in a position to easily access sensitive assets and can form a significant threat to your organization’s data. | 2 | 169 |
| Insider Threats: Humans | In order to mitigate insider threats, your organizations needs an “Insider Threat Program” and it begins with raising awareness about its existence within the organization. This serves as a deterrent for insiders to leak information. Research have shown that positive incentives can be used to encourage employess to act in the interest of the organization. Individuals who pose an elevated risk, should be placed under increased monitoring. | 2 | 170 |
| User Activity Monitoring | Tools enable the organization to keep track of internal end-user activity when using the organization’s infrastructure. Many regulations (HIPPA, SOX, GDPR, etc) require organizations to implement some degree of UAM for auditing purposes. | 2 | 171 |
| Digital watermarking | Can be used to embed markers in data to track the data source and ownership. | 2 | 172 |
| Android Security | Previously viewed as more focused on functionality than security. Since Android Oreo significantly focused on security. More built-in security and trying to be similar to iOS. Still open operating system but more embedded security features. Now focused on multiple layers of security, right out of the box. | 2 | 180 |
| Android Security features: Application Security | Applications are rigorously tested for security before there are available for download | 2 | 181 |
| Android Security features: Active Scanning | When applications run, they are monitored to look for suspicious activity. | 2 | 181 |
| Android Security features: Android Pay | Secure payment options do not expose credit card data. | 2 | 181 |
| Android Security features: Virtual Sandbox | Critical Data is sandboxed or isolated from applications to minimized exposure. | 2 | 181 |
| Android Security features: Device manager | Allows for locating and securely wiping remote devices. | 2 | 181 |
| Android Security features: Built-in Encryption | Cryptographic functionality is built in to protect data at rest and in transit. | 2 | 181 |
| Android fragmentation | Multiple competing hardware manufacturers whole sole profit is hardware sales. Manufacturers are free to customize Android source: incompatibilities. Multi-chain update cycles is complex: Issuing updates. These qualities reduce the platform’s effective value; Common complaint from Android users | 2 | 182 |
| Android important characteristics | Open Handset Alliance, led by Google. Manufacturers manipulate the OS add or remove content and control software features. Rapid hardware development. Wide disparity of hardware and software features. | 2 | 182 |
| Android security process | First a flaw is disclosed to the OHA, publicly or privately. When a fix is made available, notice is returned to the OHA. Second, each vendor must test and incorporate the software update into the Android OS. After the update is prepared, it is shared with the MOs. After the MO completes testing and integrations of the fix, it can be made available to Android users as an OTA update or as a download on a website. | 2 | 184 |
| Apple iOS Security | iOS is designed with security at its core. Closed model unless someone jailbreaks the phone. Security is integrated into the entire architecture. Most security is transparent to the user. Key security (that is, encryption) cannot be disabled of turned off. | 2 | 185 |
| Apple iOS security features: System Security | Both hardware and software contain security features that support the architecture and applications that run on the system. | 2 | 186 |
| Apple iOS security features: Encryption and Data protection | Protect critical data id the device is stolen, or unauthorized access is attempted protecting data at rest. | 2 | 186 |
| Apple iOS security features: Network Security | Complements data protections and provides security for data in transit. | 2 | 186 |
| Apple iOS security features: Application Security | Creates a platform to enable third party applications to run in a secure environment. | 2 | 186 |
| Apple iOS security features: Apple Pay | Enables you to make secure payments | 2 | 187 |
| Apple iOS security features: internet services | Provides cloud-based services for backup and capability for communications. | 2 | 187 |
| Apple iOS security features: Device control | Enables management of device to include secure wipe. | 2 | 187 |
| Apple iOS security features: Privacy controls | Enables device information to be shared with external services, such as with location services. | 2 | 187 |
| Apple important characteristics | Massively popular platform, common for enterprise-owned and user-owned deployment. Most restrictive of the 2 major platforms. Apple end-to-end ownership model of hardware and software. Apple forbids mobile operators (MO) software. Minor software differentiation between iPhone, iPod, and iPad. Constant hardware evolution and improved performance. Hardware capabilities frequently dictate software feature capabilities. | 2 | 188 |
| Mobile problems and opportunities | Mobile devices introduce new problems and opportunities for organizations. End users see mobile devices as sophisticated, cutting edge, desirable technology. From a security perspective, mobile devices lack the security functions we expect in modern devices such as lacking functionality needed for security use and immature or hampered enterprises controls. Organizations have sound motivators to leverage mobile devices for many industries. | 2 | 189 |
| Mobile devices threats: TH 1 | Loss of controls and visibility with BYOD (Bring your own device) | 2 | 190 |
| Mobile devices threats: TH 2 | Always-on devices through multiple interfaces such as Bluetooth leaving the door opened for potential attacks. | 2 | 190 |
| Mobile devices threats: TH 3 | Device patching and extended vulnerability periods. | 2 | 190 |
| Mobile devices threats: TH 4 | Device theft and loss. | 2 | 190 |
| Mobile device stolen threat: Loss impact. | An attacker can do many things to a stolen device such as access device resources, extract data, synchronize device, jailbreak/unlock/root, access stored authentications credentials, backdoor device. | 2 | 191 |
| Mobile device stolen threat: Mobile device management | Protect company data, enforce policies, locate devices remotely, updates and installs., diagnosis and troubleshooting, secure communications. | 2 | 192 |
| Mobile device stolen threat: :Loss device reporting | Time sensitive actions, greater risk if not timely reported, encourage quick reporting. | 2 | 192 |
| Unlocking, Rooting and Jailbreaking. | Overcoming restrictions and bypassing intended controls as the process of creating unrestricted devices. | 2 | 193 |
| Mobile malware | Mobile devices malware is a growing threat for devices to exploit users and also for the attacker to get financial gain. It is a small fraction of the overall malware threat; however, it is growing at an alarming rate. Platform exposure varies significantly. | 2 | 194 |
| Mobile user credential theft. | Mobile phones are increasingly relied upon for two-factor authentication via SMS primarily for banking applications and related financial activities. If your credentials are stolen, by an attacker, your whole online persona could be compromised as well. | 2 | 195 |
| ZeuS Trojan | Malware that targets blackberry, android, windows mobile and Symbian phone users. It enables an attacker to gain control of SMS from infected mobile devices to intercept authentication pin numbers. | 2 | 195 |
| Mobile malware delivery methods | Official app store repositories, typically short lived. Third party app stores repositories, primarily Android device or jailbroken iPhone. Malicious websites for direct download installation. Direct victim targeting through email, SMS, and MMS. | 2 | 196 |
| Android Malware | Highly targeted among four major mobile device vendors. Platform accommodates silent SMS delivery, untrusted applications, third-party, applications stores. Premium rate/short code SMS for quick financial gains. Easy for attackers to repackage legitimate applications with malware. Significant market share. Platform fragmentation creates extended lifetime for exploit applicability. | 2 | 197 |
| iOS malware | Platform security prevents unauthorized executables from running. Small number of early malware samples targeted jailbroken devices. No options to automatically send SMS. Handful of questionable applications retrieving sensitive data that were not rejected. OpenFeint, Path, Twitter , and Facebook retrieval and storage of contacts. Storm8, mogoRoad phone number retrieval. Phishing due to the consistency of the iOS UI, users are often nagged for the Apple ID password and exploited by websites pretending to be a native dialog. | 2 | 198 |
| Vulnerability assessment at scale | Modern enterprises have enormous numbers of systems, it can be a challenge to know where they are. New vulnerabilities are discovered every single day. Vulnerabilities have resulted in many recent large-scale breaches. To defend themselves at scale, enterprise organizations must have a consistent, automate vulnerability management program. | 3 | 6 |
| Vulnerability:  Definition | Flaw or weakness in a system that can be exploited | 3 | 8 |
| Vulnerability Assessment: Definition | Description and analysis of vulnerabilities in a system | 3 | 8 |
| Security Audit: Definition | Asses the adequacy of controls and evaluate compliance. | 3 | 8 |
| Vulnerability Management: Definition | Ongoing, repeatable processes for identifying, remediating, or accepting risk. | 3 | 8 |
| Vulnerability Assessors | It is not penetration testing. Many consider vulnerability assessment to be a lesser from of penetration testing. Many think the vulnerability assessors are the people who run the scanners, but they are not. | 3 | 9 |
| Penetration testing | Actualizes risk to demonstrate the business implications. | 3 | 10 |
| Vulnerability Assessments | Increased precision to produce the same. Qualitative and quantitative assessment metrics. Scoring systems and triage at scale. To achieve this, VA MUST be more than running a scan, without breaking in. | 3 | 10 |
| Vulnerability Assessment Framework | Each phase has distinct input and output, data analysis must be performed before moving on to the next phase of the methodology. | 3 | 11 |
| Vulnerability Assessments: Modules | The work flow we follow through the methodology process reflects the modularity. Most tools do not follow the methodology flow precisely or may not allow for data extraction between modules. Run each tool multiple times with different configurations, or different tools for each module. | 3 | 12 |
| Vulnerability assessments steps  VAF | Step 1 Engagement planning, Step 2 Intelligence and Threat Modeling, Step 3 Resource management, Step 4 Scanning, Step 5 Validation, Step 6 Remediation and Step 7 Reporting. See slides on the book. | 3 | 14 |
| Engagement planning: VA Step 1 | This is a crucial step, often skipped or not done correctly. It consists of planning such as rules of engagement scoping, process, procedures and checklists, access and visibility, logistics, and resource management. | 3 | 14 |
| Intelligence and Threat Modeling:  VA Step 2 | Gathering intelligence, identify prioritize most likely threats to the organization. Most likely targets/critical assets/functions. How likely are the mitigation controls able to detect/respond. Level of sophistication and resourcing required. | 3 | 15 |
| Discovery: VA Step 3 | This phase validates documentation, network diagrams, and open-source information.  Input: Domain names, list of host names, subnets, CIDR ranges.  Goal: which subnets are routable, which hosts are accessible, visibility available.  How: Network is mapped using various active and passive methods.  Result: identify individual live hosts. | 3 | 16 |
| Scanning: VA Step 4 | Major considerations are scanner placement and impediments to testing, such as firewalls and load balancers. Various strategies and techniques are used to scan endpoints and network elements across the enterprise. | 3 | 17 |
| Validation: VA Step 5 | Assign a confidence value and validate potential vulnerabilities. Some may require exploitations, pillaging, or pivoting to ascertain impact. Meet compliance and audit requirements. Major issues we face when performing enterprise assessments include collaboration tools and data management. | 3 | 18 |
| Remediation: VA Step 6 | Changes must be prioritized based on risk assessment and cost-benefit analysis that has leadership approval. Remediation loops back into enterprise functions such as change management, configuration management, architectural changes, ticketing system, framework to tie into other systems. | 3 | 19 |
| Reporting: VA Step 7 | Assign risk and priority ratings to confirmed vulnerabilities. Determine the most appropriate options for remediation/mitigation of the issues identified as being a priority by performing analysis, write finding reports, executive summary. | 3 | 20 |
| Vulnerability Criticality | Ratings applied to identified vulnerabilities are likely subjective and have different meanings to different organizations. Without providing any context around those rating they have little meaning. It is often the case where asset value and impact are multiplies by the likelihood of compromise. Rating examples: Low, medium, high, severe, grave. | 2 | 22 |
| Heartbleed: Cerebration over computation | With a common vulnerability scoring system (CVSS) score of 5.0/10, it is often overlooked during triage and placed in the “some-da” stack of info-sec to do list. However, it could have calamitous impacts or organizations, but still a 5.0. Vulnerability rating systems may or may not even approximate rea-world risk. | 2 | 23 |
| Common Vulnerability Scoring System (CVSS) | Universal language to convey vulnerability severity and help determine urgency and priority of response. It serves as the standard by which other systems are judged. | 3 | 24 |
| Common Vulnerability Scoring System (CVSSv2) | Lacked considerations for targets of opportunity, active and successful exploitation in the wild, consideration on easy of exploitation. | 3 | 24 |
| Common Vulnerability Scoring System (CVSSv3) | Environmental considerations are modified to include base modifiers, impact metrics, and impact subscore modifiers. | 3 | 24 |
| CVSS Version 3 NVD Calculator | The national vulnerability database contains a tailored calculator for CVSSv2 and CVSSv3. CVSSv3 calculations are broken into three categories: Base score metrics, temporal score metrics, and environmental score metrics. The National vulnerability database (NVD) calculator provides a five-rank vulnerability categorization. | 3 | 25 |
| CVSS Scores calculating | The calculation for CVSS scoring is broken into 3 segments: Base score metrics (Exploitability metrics, impact metrics), Temporal score metrics (exploitability, report confidence, remediation level) Environmental score metrics (Base modifiers, impact metrics, impact subscore modifiers). These components are further broken down to perform the actual calculation. | 3 | 26 |
| Auto-Generated Risk Ratings: Dangers | Risk ratings, such as Microsoft’s DREAD model, use automated data sources and calculation I order to generate a quantitative risk rating. automated risk ratings fail to account for data singularity. Accurate risk calculation requires customized usage per application, in spite of sophisticated sounding verbiage, computers continue to lag behind in this discipline. | 3 | 27 |
| Customized Risk Calculation | Customized risk analysis is vital component to any holistic assessment strategy. When developing personalized ratings, 2 disciplines should be considered: Quantitative Risk Assessment – factors in the financial impact and other metrics, and Qualitative Risk assessment – Factors in the likelihood, difficulty in exploitations, and other factors. | 3 | 28 |
| Case Study: Meltdown and Spectre | Intel CPU vulnerabilities, it is hardware vulnerability considered a game over scenario vulnerability. Meltdown can allow a lower-privileged process to read data from a higher-privileged process. Spectre can allow one process to read data from other process at the same level of privilege and it can be exploited using java script in a browser. | 3 | 30 |
| Case Study:  MS17-010 | Major vulnerability. It is a vulnerability that affects all versions of a product including unsupported old versions that do not receive patches. Believed to have been a zero-day vulnerability (catastrophic) | 3 | 29 |
| CVSS scores: Not all vulnerabilities have scores | Most “vulnerabilities” triggered by attackers do not have CVSS scores. Attackers use systems the way that they were designed, but with nefarious intentions. | 3 | 31 |
| Penetration testing | Involvers modeling the techniques used by real-world computer attackers to find vulnerabilities; to exploit those flaws under controlled circumstances; in a professional, safe manner according to a carefully designed scope and rules of engagement; to determine business risk and potential impact, all with the goal of helping the organization improve security practices. | 3 | 36 |
| Pen testing: goal | Report all exploitable vulnerabilities under controlled circumstances. | 3 | 36 |
| Pen testing: Effort | ~10% tools based and ~90%. Manual testing | 3 | 36 |
| Pen testing: Frequency | ~once per year. | 3 | 36 |
| Pen testing: customer | System owners, operations, engineering, and application stakeholders. | 3 | 36 |
| Red Team | Emulates tactics, techniques, and procedures (TTPs) of real adversaries to improve the people, processes, and technology in their target environment. “The practice of looking at a problem or situation from the perspective adversary” | 3 | 37 |
| Red Team: Goal | Trans and measure blue teams’ detection and response policies, procedures, and technologies are effective. | 3 | 37 |
| Red Team: effort | Manual; some Red Team Automation tools. | 3 | 37 |
| Red Team: Frequency | Intelligence-led (New exploit, tool, or TTP) | 3 | 37 |
| Red Team: Customer | Blue teams | 3 | 37 |
| Adversary emulation | A type of Red Team exercise where the red team emulates how an adversary operates, following the same tactics, techniques, and procedures (TTPs), with a specific objective similar to those of realistic threats or adversaries. | 3 | 38 |
| Adversary Emulation: Goal | Emulate an end-to-end attack against a target organization. Obtain a holistic view of the organization’s preparedness for a real, sophisticated attack. | 3 | 38 |
| Adversary Emulation: Effort | Manual; more setup than a limited scope penetration test. | 3 | 38 |
| Adversary Emulation: Frequency | Twice a year o yearly. | 3 | 38 |
| Adversary Emulation: Customer | Entire organization | 3 | 38 |
| Purple team: | A function,. Or virtual team, where red and blue work together to improve the overall security of the organization. Red Team does not focus on stealth as they normally would. | 3 | 39 |
| Purple team: Goal | Red team emulates adversary TTOs while blue teams watch and improve detection and response policies, procedures, and technologies in real time. | 3 | 39 |
| Purple team: Effort | Manual | 3 | 39 |
| Purple team: Frequency | Intelligence led (new exploit, tool, or TTP) | 3 | 39 |
| Purple team: Customer | Red Team and Blue Team. | 3 | 39 |
| Pen Testing: Why performing it. | Penetration testing allows for the validation of vulnerability findings. Vulnerability scanners do not typically perform validation. A penetrations test attempts to exploit a given vulnerability to demonstrate the true impact. It shows the effectiveness of security controls. Identify gaps in network and system architecture. Build confidence in potential customers. | 3 | 40 |
| Rules of Engagement | The rules of engagement covers how the test is to be conducted. Start dates and end dates of testing. Time of day testing is permitted. Contact information for testes, system owners, and business owners. What data is and is not allowed to be viewing -thin PII data and regulatory requirements. How to respond if an exploit attempt has been blocked or new rules were added to block the tester’s IP addresses. How results should be submitted and in what format. | 3 | 41 |
| Scoping | The defined scope instructs the penetration testing team as to what systems and services they can and cannot target. Too narrow of a scope reduces the value to the customer. The pen test team can help explain as to why additional targets should be in score. Sometimes the customer intentionally limits the scope. | 3 | 42 |
| Scoping document | It should include items before performing a pen testing such as:  What systems, networks, domains, and applications are in play?  What if new unidentified systems are discovered?  Which ones should explicitly be avoided?  What if the system resides at a vendor location or in the cloud? | 3 | 42 |
| External penetration testing | An external penetration test focuses on the perspective of an attacker from outside the organization. Targets externally-facing systems such as DNS, Mail, and Web servers. May include phishing attacks as another means to gain access. Relies heavily on Open-Source intelligence (OSINT) and scanning. It is often seen as a “real-world” campaign since the testers are not given internal access to start. | 3 | 44 |
| Internal Penetration testing | An internal penetration test focuses on what an attacker could do if starting from within the organization’s network. This can be a malicious insider with privileged access, such as an employee, contractor, or vendor. It could also be an attacker who has successfully gaining a foothold inside the organization – We can assume a breached state. | 3 | 45 |
| Web application penetration testing | Another common penetration test focuses specifically on web applications and data bases. These systems are the ones most often exposed to the internet and provide access to sensitive data. If poorly coded they can be exploited to gain unauthorized access. The open web application security project (OWASP) is a fantastic resource that offers tools and guidance on web app security. | 3 | 46 |
| Social Engineering penetration testing | Use of influence and persuasion to deceive people for the purpose of obtaining sensitive target information or for the victim to perform an action. Enables access to the target usually by a sense of trust or authority of the attacker. Preys on human behavior and works to befriend the victim to obtain the information. Attempts to trick or manipulate data or access from a person. By passes network security by exploiting human vulnerabilities. | 3 | 47 |
| Social Engineering types: Computer based | Pop-up windows. Mail attachments | 3 | 48 |
| Social Engineering types: Human-based | Urgency. Third-person authorization | 3 | 48 |
| Mobile Device penetration testing | The attack surface of mobile devices certainly includes similar attacks as those related to web clients and apps. Mobile devices are used for much more than just the web and require a unique focus. | 3 | 49 |
| Product security penetration testing | This type of testing could include internet of things (IoT) devices, network appliances, such as VOIP, phones, printers, switches, and routers, often involves reverse engineering, fuzzing, and debugging. | 3 | 49 |
| Physical penetration testing | This type of testing factors in devices such as a badge reader, elevators, security gates, biometric devices, safes, and many others. | 3 | 49 |
| Penetrations testing phases | 1. OSINT 2. Scanning and enumeration 3. Vulnerability identification 4. Exploitation 5. Post exploitation | 3 | 52 |
| OSINT | Open-source intelligence (OSINT) Gathering it is the practice of collecting data via open-source location such as the public internet, presentation, printed media and more. Reconnaissance is a passive effort allowing the analyst to go mostly undetected. | 3 | 53 |
| Scanning and enumeration | Tools such as Nmap are commonly used to identify systems, services, OS versions, and more quickly and effectively. We can enumerate discovered systems to learn information such as what services are tied to listening ports. It is not uncommon for administrators to bind services to non-standard ports, such as running an HTTPS services over TCP port 4433. | 3 | 54 |
| Vulnerability identification | This phase is very similar to the tools and techniques covered in the Vulnerability assessment module. Vulnerability identification phase helps us to detect the best targets and services to use in the exploitation phase. If we identify that a service is running, we can check to see if we have a corresponding exploit available. With vulnerability assessments, any validation would be performed manually. | 3 | 55 |
| Exploitation | Is where we take all the knowledge gained thus far and attempt to gain access. Access gained could include a system, network, or other resource. We want to choose the technique and exploit most likely to be successful and go undetected. Exploitation may require that we account for evading protections such as a antivirus, antimalware, and other controls. | 3 | 56 |
| Post exploitation | Includes activities performed once an initial foothold is gained on a system or network. Initial access is great, but a pen tester must demonstrate the true impact. This includes many actions such as pivoting and lateral movement, privilege escalation, data exfiltration, maintaining access. Tools include Metasploit framework, Empire, Covenant, etc. | 3 | 57 |
| Reporting | The pen test report is what you leave behind to your customer and it should include. Executive summary, introduction, methodology, findings, and Risk assessment, Recommendations, Conclusions, Appendix. | 3 | 58 |
| Penetration testing tools | NMAP, Metasploit, Meterpreter, C2 Frameworks (Empire, Cobalt Strike, Covenant, C2 Matrix) | 3 | 60 |
| Nmap | Nmap is a free, aware winning network scanner. Supports a large number of scanning techniques. Numerous other features supported. Remote operating System detection. Application detection.  Common back door is to open a port. Port scan scans for open ports on remote host. Scan0-65535 twice, once for TCP, once for UDP, Various tools available. Scanport and NMAP. | 3 | 61 |
| Nmap: Port scanning | An example of how a port scanning is on the book. Look at the notes there. | 3 | 62 |
| Operating system identification | Looks for subtle differences in target responses. Develops a fingerprint. Compares the fingerprint against a pre-built database of operating system finger fingerprints. | 3 | 65 |
| Metasploit | Exploitation framework. If a module for vulnerability exists, it will attempt to exploit the target and provide access. Useful for organizing and managing exploits. Complementary to vulnerability scanning to reduce false positives. | 3 | 66 |
| Meterpreter | It is in memory in encrypted form. A customer shell offering a large number of post exploitation functionality, such as stopping/starting a process, spawning a shell, sniffing network traffic, screenshots, and even interactive with the microphone and camera. | 3 | 67 |
| C2 Frameworks and Implants | Empire: is a pure PowerShell post-exploitation agent build on cryptological-secure communications and a flexible architecture. Original project no longer supported, but a fork was created.  Cobalt Strike: a commercial adversary emulation product from SpectreOps focusing on covert communication and post-exploitation.  Covenant: a C2 Framework that leverages the attack surface of .NET2. an alternative option to Empire as PowerShell is heavily monitored.  Sliver: A DNS-based implant framework from BishopFox. | 3 | 68 |
| 7T | Matrix of a command-and-control Frameworks. Google doc of most C2 frameworks. Documents various capabilities of each framework. There is no right or wrong, better, or worse framework. Find the ideal C2 for your current objective. Wizard-like UI to select the appropriate one. | 3 | 69 |
| Password compromise | A Password compromise remains one of the most sought-after and effective access methods used by penetration testers, this includes password cracking, spraying, reuse and others. | 3 | 70 |
| Multifactor authentication | Microsoft study: 99.9% less likely to be compromised if you used MFA.  As October 2019 only 8.2% of Azure AD accounts were using MFA. Solutions such as FIDO2 and YubiKeys can greatly increase MFA security. | 3 | 70 |
| Password Reuse and Stuffing | Many of us use the same username and password combinations for multiple resources. This attach is popular thanks to the large dumping of credentials associated with data breaches. Attackers take the dumped credentials and try them over a large number of websites. | 3 | 71 |
| Password Spraying | Is a simple concept where commonly used passwords are tried against many user accounts. Helps prevent against account lockout. By the time a second password is tried, many sites will have reset the account lockout security threshold. Typically targets web and cloud sites. | 3 | 72 |
| Responder | Is a tool that targets Link-Local Multicast Name Resolution (LLMNR), Multicast DNS (mDNS), NetBIOS Name Service (NBT-NS) | 3 | 73 |
| Marriott Data Breach | Confidentiality attack. Breached 4 years before noticing. Details highly guarded. Between 380 and 500 million stolen records. | 3 | 80 |
| Marriot Data Breach: Summary | Marriott discovered breached September 8,2018. Reported the breach November 30, 2018. 9.1 million payment cards | 24 million passports. Breach was active from 2014. | 3 | 81 |
| Marriott Data Breach: Impact | Reservation database, credit card numbers, passport numbers, mailing addresses, name, phone, and emails. | 3 | 83 |
| Marriott Data Breach: Failure | Step taken postmortem: Free web watcher enrollment, website set up for information, huge sum spent on additional security technology, thousands of man-hours still going into finding the root. | 3 | 84 |
| Marriott Data Breach: Fallout | Marriott implemented a website for customers who thought they might have been impacted through a 3rd party, and it is most likely that it had been the company in charge of the post compromise, and it wasn’t on corporate domain. Customers thought it was phishing. | 3 | 85 |
| Equifax Data Breach | The Equifax breach was another massive hit to confidentiality of consumer information. Please see book. | 3 | 86 |
| WannaCry Ransomware | Confidentiality, integrity, and availability attack. Spread across over 150 countries. Cripples over 200,000 devices. Much like other high-profile breaches, a few basic security practices could have reduced or prevent these attacks. This is not a zero-day, it was a patchable vulnerability. | 3 | 87 |
| WannaCry Ransomware: The attack | Crippled hospitals, banks, and other industries around the world. Encrypts data and demands ransom. Utilized tools initially believed to have been developed by a nation state. | 3 | 88 |
| WannaCry Ransomware: Breach impact | One of the first public examples of ransomware. The impact of these attacks was widespread. Roughly 230,000 systems breached. Over 150 countries. Gave way to several follow-on attacks. | 3 | 89 |
| WannaCry Ransomware: Root cause | Began May 12th, 2017, in Asia. Ransomware as a worm, not a virus. Largely target Microsoft systems. Patch released 2 months before initial attacks. | 3 | 90 |
| WannaCry Ransomware: Tools | There were multiple layers to the attack that relied on each other. Utilized code to scan for vulnerable systems. Eternal blue: SMBv1 exploit. DoublePulsar: Backdoor Trojan. | 3 | 91 |
| WannaCry Ransomware: Gaining access. | It used 3 primary commands:  Ping: Diagnostic tool used to test system reachability.  Kill: system command used to terminate running processes.  Exec: Which can be used to load and execute malware on the victim system | 3 | 92 |
| WannaCry Ransomware: Attack summary | The system was visible from the internet. Uncheck scanning and enumeration. An unpatched vulnerability was exploited. The system has weak authentication. | 3 | 93 |
| WannaCry Ransomware: Current attacks | WannaCry is mostly patched, but other ransomware has followed in its footsteps. Ransomware remains one of the biggest threats. Methods are changing. Exploiting mostly know vulnerabilities. Spreading due to lack of segregation. | 3 | 94 |
| Ransomware as a Service (RaaS) | Cyber criminals can create a customized version of various types of ransomwares for profit. Satan ransomware has the ability to make your own customized version, in the example, 30% of the profits go to the developer or the service. | 3 | 95 |
| Ransomware as a service: examples | Bitcoin stealer and bitcoin blackmailer. Jigsaw ransomware can be customized at this site, and it allows you to create your own customized version of bitcoin blackmailer for profit, providing instructions on how to compile the code, create new Bitcoin payment addressed and more. | 3 | 96 |
| Input attacks | OS command injections, buffer overflows, SQL injections. | 3 | 98 |
| OS command injection | Attacker sends OS commands as form or other input. Relies on developer using input to build calls back to the OS. See book for slide | 3 | 99 |
| OS command injection: Defenses | Avoid making system calls from within your application, especially to the system () function. Input processed based on user input at biggest risk. Where possible, use built-in application functions instead. Strip OS commands and characters from input. Even better, define valid characters from input used in this way; delete all others from input. | 3 | 100 |
| Buffer overflow | Programs allocate a certain amount of buffer (memory) space to perform operations. In poorly coded applications, no validation is performed to ensure the data being copied is not larger than the allocated memory. When the buffer is overrun, important variables such as the return pointer can be hijacked. | 3 | 101 |
| Buffer overflow: Normal stack memory allocation | This is when the attacker tries to determine how many characters are allowed in memory or hold text. | 3 | 102 103 |
| Buffer overflow: Basic stack overflow I. | This is when we have overwritten the memory because the developer didn’t put a limit on the characters in the input and goes to the return pointer, and we will get a segmentation fault. | 3 | 104 |
| Buffer overflow: Basic stack overflow II | Using a debugger, the attacker gets the static memory address of the buffer. They place their shellcode(executable code) into the buffer and overwrite the return pointer with the address of the buffer and when the process goes to return control to main(), control is instead passed to the attacker’s shellcode. | 3 | 105 |
| Buffer overflow: Defenses | Run the latest versions of all your installed software. Update and patch your software. Update and patch your languages/runtime / environment/server add-ons. Run a vulnerability scanner against your applications. Utilize endpoint protection suites offering exploit mitigations. Validate and Sanitize user input. | 3 | 106 |
| SQL Injection: | SQL Injection is yet another vulnerability taking advantage of insufficient input validation. The technique, if successful, can be used to execute arbitrary SQL commands to which the web server application database account is authorized. | 3 | 107 |
| SQL Injection: Defenses | Validate user input, have length limits on input. More tiers: add an application layer between the webserver and the database. Utilize stored procedures instead of SQL queries. Database access: Web account should not have rights to add/drop/modify tables or stored procedures. Do not display SQL errors to web users. Monitor SQL error messages. | 3 | 108 |
| Input attack defenses summary | Only allow specific valid characters from user input to avoid characters that have special meaning in scripting languages. Be suspicious of all input, including HTTP headers, and cookie data. Validate on the server, not the client. Use an up-to-data well-validates third party library of input and check for encoded characters, v checking routings to use throughout the application. | 3 | 110 |
| Virus | A virus is a type of malware, historically destructive in nature that typically requires user interaction to infect a system. They require a host file, such as an executable or Microsoft Office macro. Once executed, they often copy themselves onto file shares or removable media, email copies of themselves, etc,. in an effort to spread. Their goal is often destructive such as deleting files, however, they can perform whatever actions they were programmed to do by their author. | 3 | 112 |
| Worm | A worm is historically a self-replication piece of code that typically carries one or more exploits and payloads. They often scan systems for vulnerable serves, launch an attack, and execute their payloads. Their goal is often to infect as many systems as possible and set up C2 (Command and control). | 3 | 112 |
| Virus vs. Worms | Virus typically requires user interaction to infect whereas worms do not. They also require a host file, such an executable or document whereas worms’ scans for listening ports associate with vulnerable services. With viruses the goal is data destruction whereas with worms if exploitations is successful, it executes a payload and copies itself onto the infected system. Viruses spread via file shares, removable media, email clients whereas worms’ goals are to set up command and control network and viruses may intentionally or inadvertently impact systems and network performances whereas worms inadvertently impact systems and networks | 3 | 113 |
| Trojans | A trojan horse a program that often performs the desired action of the victim, as well as a malicious action. If we wanted to create a trojan horse on a netcat and if we had the source code, we could add our malicious code to the beginning (hide it) or any other point within it, compile the code, and publish it. When the victim executes the program, they will get their desired result of using the tool, however, our code will also execute. | 3 | 114 |
| Rootkits | Put a system into an unknown state, and restoration typically requires rebuilding from read-only media, or if possible, a known-good backup. The primary goal of a rootkit is to subvert userland and kernel security controls to avoid detection, provide ongoing access from the attacker to the infected system. Utilize default system resources such as .NTS’s “System.Management.Automation” used by PowerShell for all automation-based activities on windows to blend in. | 3 | 115 |
| Malware Analysis Stages | Traditionally, malware analysis has consisted of 2 phases: Behavioral Analysis and code analysis. | 3 | 116 |
| Malware Analysis Additional Stages | Fully automated analysis, Static Properties Analysis, Interactive Behavior Analysis, Manual Code Reversing. | 3 | 116 |
| Fully Automated Malware Analysis | Automation of malware analysis is a good way to perform quick analysis at a relatively low cost when compared to a human analyst. However, they can provide false positives, it is normal for programs to contain strings that also reside in malware, critical function calls by legitime programs will result in alerts, VirtuaProtect, VirtualAlloc, WritePRocessMemory, HeapAlloc, etc. | 3 | 117 |
| Static Properties Analysis | Static properties analysis is a “safer” way to examine the properties of potential malware without actual execution. Behavioral analysis requires execution of the specimen. Much can potentially be learned about the intentions of the malware. Analysis can be hindered by packing, encryption, and other obfuscation techniques. There are many tools available on both Linux and Windows to help. | 3 | 118 |
| Interactive Behavior Analysis | In order to further learn about the characteristic and intentions of a malware specimen, it may be required to manually perform behavioral analysis. The fully automated malware analysis may not have been able to answer all of your questions. Static properties analysis may not be comprehensive due to patching and other protections. By allowing the malware to run in a controlled environment, we can monitor its behavior as well as manually interact. Registry and filesystem access, process behavior and interactions and network activity. | 3 | 119 |
| Manual code reversing | Often very time consuming. Manual code reversing and analysis is considered to be the most advanced form of malware analysis. Requires the use of special tools such as dissemblers to convert machine code back to assembly language and decompilers to convert assembly language or intermediate language back to pseudocode. This stage allows malware analyst to truly see what is happening at the code level. | 3 | 120 |
| Marriot & WannaCry: Lessons learned | Attackers follow a strategy of reconnaissance, enumeration, and penetration. It is important to follow security core concepts such as a patching and limiting network visibility. There are many different methods of attack, including buffer overflows, and SQL injection, etc. Malware remains a real threat. | 3 | 121 |
| Web communications Basics | Stateless communications. Retrieving information: GET, HEAD. Sending information: POST, PUT. The web can be considered a transport mechanism for the information it contains. It boils down to the protocol browsers and servers use to communicate: the Hypertext Transfer Protocol (HTTP). The HTTP is transaction-oriented. Clients make requests, and servers send responses. It is stateless since once a request is responded to; it will forget all about it. | 3 | 128 |
| Port 80 | TCP connects to this port on server/HTTP. End to end unprotected. | 3 | 128 |
| Port 443 | HTTPS connects to this port and all secure transfers are done here. | 3 | 128 |
| Cookies | Stores data from a browser session on the client and are sent to the server. Are often to keep state. Can be: Persistent (Text, file/database) and non-persistent: Session/ in-memory. Cookies can be blocked in you wanted. A Cookie is a named piece of data created by a web server and stored at the web browser. Both the name and the contents are chosen by the application and can be almost anything the programmer wants. | 3 | 130 |
| Cookies: Persistent | Stored on a hard drive, survive a reboot, typically stored for a long period of time, used to track user activity, create privacy concerns. | 3 | 132 |
| Cookies: Non-Persistent. | Session cookies, stored in memory, do not survive a reboot, stored for a short period of time, could require additional authentication, since user ingo is not remembered. | 3 | 132 |
| SSL/TLS: What is it | Protocol for encrypting network traffic. Operates on port 443, provides encryption, server identity verification, and data integrity. | 3 | 133 |
| SSL/TLS: How it works | Client connects to server, servicer indicates SSL configuration, client and server exchange crypto keys, secure session begins, it is not a guarantee of security. | 3 | 133 |
| OWASP top 10 critical issues | 1. Broken access control 2. Cryptographic failures 3. Injection 4. Insecure design 5. Security misconfiguration 6. Vulnerable and outdated components 7. Identification and authentication failures 8. Software and data integrity failures 9. Security logging and monitoring failures 10. Server-side request forgery (SSRF) | 3 | 136 |
| Broken access control | Access control enforces policies such that users cannot act outside their intended permissions | 3 | 136 |
| Cryptographic failures | Leads to sensitive data exposure or system compromise. | 3 | 136 |
| Injection | Happens when a user-suppled data is not validated, filtered or sanitized by the application. | 3 | 136 |
| Insecure design | Represents different weaknesses, expressed as missing or ineffective control design. | 3 | 136 |
| Security misconfiguration | This is commonly a result of insecure default configurations, incomplete or ad hoc configurations, open clod storage, misconfigured HTTP headers, and verbose error messages containing sensitive information. | 3 | 136 |
| Vulnerable and outdated components | Components such as libraries, frameworks and other software modules run with the same privileges as the application, and this can facilitate serious data loss or server takeover. | 3 | 136 |
| Identification and authentication failures | Attackers are able to compromise password, keys or session tokens, or to exploit other implementation flaws to assume other users’ identities temporarily or permanently. | 3 | 137 |
| Software and data integrity failures | Software and data integrity failures related to code and infrastructure that does not protect against integrity violations. | 3 | 137 |
| Security logging and monitoring failures | Allows attackers to further attack systems, maintain persistence, pivot to more systems, and tamper, extract, or destroy data. | 3 | 137 |
| Server-side request forgery (SSRF) | It allows an attacker to coerce the application to send a crafted request to an unexpected destination, even when protected by a firewall, VPN, or another type of network access control list (ACL). | 3 | 137 |
| Developing secure web applications | Security must be built into the software development life cycle. Developer training on vulnerabilities and secure coding. Peer reviews to identify errors or bad practices. Form and through testing using expected and unexpected input. Configuration management and version control. Separate development, testing, and production environments; separation of duties between developers and production administrators. | 3 | 138 |
| Basics of secure coding | Initialize all variables before use, validate all user input before use, don’t make you application require admin permissions on the server or database. Handle errors and don’t display errors to end users, employ least privilege/limit access, don’t store secrets in your code, use tested, reliable libraries or modules for common functions )authentication, encryption, session tracking) watch for vulnerability notifications in any utilized open-source libraries. | 3 | 140 |
| Web application vulnerabilities | In order for an adversary to compromise a web application, they only have to find one vulnerability. Most common are Authentication, access control, session tracking. | 3 | 142 |
| Web Application authentication | HTTP authentication: Credentials sent in HTTP header, basic mode: credentials sent in cleartext (base64 encoded) and Digest mode: Sends MD5 hash of password. Form based authentication: credentials entered and sent as HTML form data. Authentication attacks: password guessing, brute forcing, or bypassing authentication mechanism. Multifactor authentication: Relies upon more than just the user’s password. | 3 | 143 |
| Access Control | Typical users follow the path you anticipated through the site. Keep users out of parts of the server you don’t intend them to be in. default pages, sample sites, code library pages and configurations files, disable directory browsing, URL directory traversal. | 3 | 146 |
| Session Tracking/Maintaining State | HTTP is stateless, so applications must track user interaccions (sessions). The most popular technique is session ID because it can identify users from one request to the next, and stores users’ session data from one request to the next. Session ID works by at session initiation, applications generate a session ID and pass it to the browser. Session ID is often stored in hidden form elements, cookies, or the URL query string. The browser sends this information back to the server with each subsequent request. | 3 | 147 |
| Hacking session information | 7 |  |  |