**BASICS**

**To Delete files permanently**

SDelete for windows, Shred for Linux and Secure Empty Trash for Linux to delete files permanently.

1. **CYBER WARFARE**

**Stuxnet**

Stuxnet is a computer worm that was originally aimed at Iran’s nuclear facilities and has since mutated and spread to other industrial and energy-producing facilities. The original Stuxnet malware attack targeted the programmable logic controllers (PLCs) used to automate machine processes. It was the first known virus to be capable of crippling hardware and because it appeared to have been created by the U.S. National Security Agency, the CIA, and Israeli intelligence.

Stuxnet reportedly destroyed numerous centrifuges in Iran’s Natanz uranium enrichment facility by causing them to burn themselves out. Over time, other groups modified the virus to target facilities including water treatment plants, power plants, and gas lines.

Stuxnet was a multi-part worm that travelled on USB sticks and spread through Microsoft Windows computers. It can install its own stolen but legitimate drivers and if it gets deleted, it can download again within 24 hours. It had the ability to update its code along the way and if two of these worms meets at a single system, they compare their versions to update them. The virus searched each infected PC for programmable logic controllers (PLCs), which industrial computers serving as PLCs use for automating and monitoring electro-mechanical equipment. After finding a PLC computer, the malware attack updated its code over the internet and began sending damage-inducing instructions to the electro-mechanical equipment the PC controlled. At the same time, the virus sent false feedback to the main controller. Anyone monitoring the equipment would have had no indication of a problem until the equipment began to self-destruct.

1. **HARDWARE VULNERABILITIES**

Hardware vulnerabilities are most often the result of hardware design flaws. For example, the type of memory called RAM basically consists of lots of capacitors (a component which can hold an electrical charge) installed very close to one another. However, it was soon discovered that, due to their close proximity, changes applied to one of these capacitors could influence neighbour capacitors. Based on this design flaw, an exploit called Rowhammer was created. By repeatedly accessing (hammering) a row of memory, the Rowhammer exploit triggers electrical interferences that eventually corrupt the data stored inside the RAM.

**Meltdown and Spectre**

Google security researchers discovered Meltdown and Spectre, two hardware vulnerabilities that affect almost all central processing units (CPUs) released since 1995 within desktops, laptops, servers, smartphones, smart devices and cloud services.

Attackers exploiting these vulnerabilities can read all memory from a given system (Meltdown), as well as data handled by other applications (Spectre). The Meltdown and Spectre vulnerability exploitations are referred to as side-channel attacks (information is gained from the implementation of a computer system). They have the ability to compromise large amounts of memory data because the attacks can be run multiple times on a system with very little possibility of a crash or other error.

1. **SOFTWARE VULNERABILITIES**

**Buffer overflow**

Buffers are memory areas allocated to an application. A vulnerability occurs when data is written beyond the limits of a buffer. By changing data beyond the boundaries of a buffer, the application can access memory allocated to other processes. This can lead to a system crash or data compromise, or provide escalation of privileges.

**Race condition**

This vulnerability describes a situation where the output of an event depends on ordered or timed outputs. A race condition becomes a source of vulnerability when the required ordered or timed events do not occur in the correct order or at the proper time.

Race condition occurs when multiple threads read and write the same variable i.e., they have access to some shared data and they try to change it at the same time. In such a scenario threads are “racing” each other to access/change the data. This is a major security vulnerability.

**Crypto Jacking**

Cryptojacking is an emerging threat that hides on a user’s computer, mobile phone, tablet, laptop or server, using that machine’s resources to ‘mine’ cryptocurrencies without the user’s consent or knowledge. Cryptojackers are people who want the benefits of cryptocurrency mining without incurring the huge costs. By not paying for expensive mining hardware or large electricity bills, cryptojacking allows hackers to mine for cryptocurrency without the large overheads.

1. **KEY TERMS**

**SSID (Service Set Identifier)**

A preset network identifier, often referred to as an SSID (Service Set Identifier), is the name of a Wi-Fi network. It’s the name that devices used to identify and connect to a specific wireless network, like “MyHomeWiFi” or “CoffeeShopGuest”. Each Wi-Fi network has a unique SSID to distinguish it from others in range

**SERVER SPRAWL**

Dedicated servers offering services like rarely used applications often sat idle for long periods of time, waiting until there was a need to deliver the specific service they provide. These servers wasted energy and took up more space than was warranted by the amount of service provided.

This is solved by virtualization where multiple applications are run on a single server so it’s resources will be utilized even if one of the applications is rarely used.

1. **DATA**

Computers use binary codes to represent and interpret letters, numbers and special characters with bits. A commonly used code is the American Standard Code for Information Interchange (ASCII). With ASCII, each character is represented by eight bits. For example:

* **Capital letter:**A = 01000001
* **Number:** 9 = 00111001
* **Special character:** # = 00100011

Each group of eight bits, such as the representations of letters and numbers, is known as a byte.

**NETWORK BASICS**

**Network Media**

Codes can be used to represent almost any type of information digitally including computer data, graphics, photos, voice, video, and music.

There are three common methods of signal transmission used in networks:

* **Electrical signals –**Transmission is achieved by representing data as electrical pulses on copper wire.
* **Optical signals –**Transmission is achieved by converting the electrical signals into light pulses.
* **Wireless signals –**Transmission is achieved by using infrared, microwave, or radio waves through the air.

**Data types**

* Volunteer Data

Data being collected, used and shared on the network with the user knowledge

* Inferred Data

Data being collected, used and shared on the network without the user knowledge

Eg: Use of credit card in multiple places helps to identify user preferences, locations, etc

* Observed Data

This is captured by actions of individuals. Data being observed from our device like location

**Bandwidth and Throughput**

Bandwidth and throughput are both measures of data transfer over a network, but they represent different aspects. Bandwidth is the theoretical maximum capacity of a network connection, while throughput is the actual speed of data transfer taking into account various network conditions.

**Bandwidth**

* Definition:

Bandwidth is the maximum amount of data that can be transferred over a network connection in a given amount of time (usually measured in bits per second, like Mbps or Gbps)

**Throughput**

Definition:

Throughput is the actual rate of data transfer over a network connection, taking into account factors like network congestion, latency, and interference

Many factors influence throughput including:

* The amount of data being sent and received over the connection
* The types of data being transmitted
* The latency created by the number of network devices encountered between source and destination
  1. **PEER TO PEER NETWORKS**

Client and server software usually run on separate computers, but it is also possible for one computer to run both client and server software at the same time

The simplest P2P network consists of two directly connected computers using either a wired or wireless connection. Both computers are then able to use this simple network to exchange data and services with each other, acting as either a client or a server as necessary.

Multiple PCs can also be connected to create a larger P2P network, but this requires a network device, such as a switch, to interconnect the computers.

**Peer to Peer Applications**

In this model, every client is a server and every server is a client. P2P applications require that each end device provide a user interface and run a background service.

Hybrid peer-to-peer (P2P) systems combine the characteristics of both pure P2P and client-server architectures. They leverage a central server for specific functions like indexing or resource discovery while maintaining the core P2P principle of direct node-to-node interaction for data sharing and other tasks.

* 1. **HOME NETWORK ROUTERS**

**Ethernet Ports**

These ports connect to the internal switch portion of the router. These ports are usually labelled “Ethernet” or “LAN”, as shown in the figure. All devices connected to the switch ports are on the same local network.

Internet Ports

This port is used to connect the device to another network. The internet port connects the router to a different network than the Ethernet ports. This port is often used to connect to the cable or DSL modem in order to access the internet.

**LAN Wireless Frequencies**

**The IEEE 802.11 standard governs the WLAN environment.**

The wireless technologies most frequently used in home networks are in the unlicensed 2.4 GHz and 5 GHz frequency ranges.

Bluetooth is a technology that makes use of the 2.4 GHz band

Other technologies that use the 2.4 GHz and 5 GHz bands are the modern wireless LAN technologies that conform to the various IEEE 802.11 standards

**Lan cables**

* The Twisted pair cable is made up of 4 pairs of wires that are twisted to reduce electrical interference. Category 5e is the most common type of twisted pair used in a LAN.
* Coaxial cable has an inner wire surrounded by a tubular insulating layer, that is then surrounded by a tubular conducting shield. Most coax cables also have an external insulating sheath or jacket.
* Fiber-optic cables can be either glass or plastic with a diameter about the same as a human hair and it can carry digital information at very high speeds over long distances

**Network Modes**

* 802.11b: Offers the slowest speeds (up to 11 Mbps) and is rarely used in modern networks
* 802.11g: Offers faster speeds than 802.11b (up to 54 Mbps)
* 802.11n: Offers the fastest speeds (up to 600 Mbps theoretical, but often less in practice) and utilizes MIMO technology for better range and performance
* Mixed Mode (b/g/n):
* Best compatibility: Supports all three standards (802.11b, 802.11g, and 802.11n).
* Potential speed limitations**:** When older devices connect, the network may need to slow down to accommodate them, potentially impacting the performance of 802.11n devices.
  1. **TRANSMISSION**
* **Unicast**

Sent and received from a single host

* **Multicast**

Hosts that receive particular multicast packets are called multicast clients. The multicast clients use services requested by a client program to subscribe to the multicast group.

Each multicast group is represented by a single IPv4 multicast destination address. When an IPv4 host subscribes to a multicast group, the host processes packets addressed to this multicast address, and packets addressed to its uniquely allocated unicast address.

Destination MAC address of 01-00-5E when the encapsulated data is an IPv4 multicast packet and a destination MAC address of 33-33 when the encapsulated data is an IPv6 multicast packet.

The range of IPv4 multicast addresses is 224.0.0.0 to 239.255.255.255. The range of IPv6 multicast addresses begins with ff00::/8.

Eg: pc1, pc2 and pc3 will have Multicast address of 224.168.1.10 and each of them have their own Ip addresses. If the message is sent to 224.168.1.10, the message will go to pc1, pc2 and pc3. If the Ip address of specific address is used, then the message will only reach that device.

* **Broadcast**

Packet is sent from the source to every other host in that network. Switches are responsible for Broadcasting Packets in the Network. Routers don’t broadcast to avoid the packets being sent to other networks so if a router receives a broadcast packet, it will drop the packet.

If there are no switches in the network, Routers LAN Ports will act as mini switch and all devices physically (wired) connected can receive broadcast packets within that network. In wireless routers, WIFI is located in same interface of LAN Ports so it can act as mini switch to broadcast within that network.

The destination MAC address for an Ethernet broadcast is FFFF.FFFF.FFFF.

The destination IP address for a Broadcast is 255.255.255.255

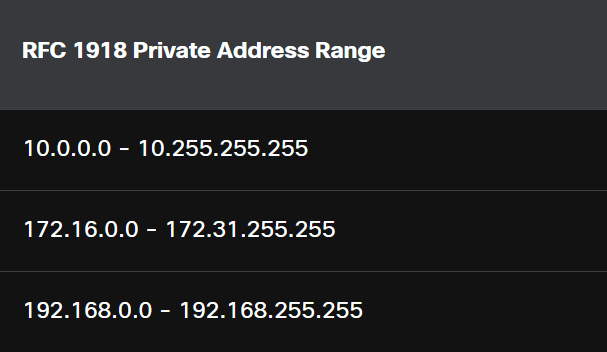
* 1. **IP ADDRESSES**

Significant fields in the IPv4 header include the following:

* **Version -**Contains a 4-bit binary value set to 0100 that identifies this as an IPv4 packet.
* **Differentiated Services or DiffServ (DS) -**Formerly called the type of service (ToS) field, the DS field is an 8-bit field used to determine the priority of each packet. The six most significant bits of the DiffServ field are the differentiated services code point (DSCP) bits and the last two bits are the explicit congestion notification (ECN) bits.
* **Time to Live (TTL) –**TTL contains an 8-bit binary value that is used to limit the lifetime of a packet. The source device of the IPv4 packet sets the initial TTL value. It is decreased by one each time the packet is processed by a router. If the TTL field decrements to zero, the router discards the packet and sends an Internet Control Message Protocol (ICMP) Time Exceeded message to the source IP address. Because the router decrements the TTL of each packet, the router must also recalculate the Header Checksum.
* **Protocol –**This field is used to identify the next level protocol. This 8-bit binary value indicates the data payload type that the packet is carrying, which enables the network layer to pass the data to the appropriate upper-layer protocol. Common values include ICMP (1), TCP (6), and UDP (17).
* **Header Checksum –** This is used to detect corruption in the IPv4 header.
* **Source IPv4 Address –**This contains a 32-bit binary value that represents the source IPv4 address of the packet. The source IPv4 address is always a unicast address.
* **Destination IPv4 Address –**This contains a 32-bit binary value that represents the destination IPv4 address of the packet. The destination IPv4 address is a unicast, multicast, or broadcast address.

**Private IP Address**

Private addresses are used in a local network like home, companies, etc. Private IP addresses make a local LAN Network. It doesn’t need to unique in the world and same IP addresses are allowed to be used for different devices in the different local networks because Private IP addresses are only used in local networks not to connect to Internet.



**Multicasting And Experimental Address**

224.0.0.0 – 239.255.255.255 = Multicasting

240.0.0.0 – 255.255.255.255 = Experimental

**Link-Local addresses**

Link-local addresses (169.254.0.0 /16 or 169.254.0.1 to 169.254.255.254) are more commonly known as the Automatic Private IP Addressing (APIPA) addresses or self-assigned addresses. They are used by a Windows client to self-configure in the event that the client cannot obtain an IP addressing through other methods. Link-local addresses can be used in a peer-to-peer connection but are not commonly used for this purpose.

**IPV6**

* The fields in the IPv6 packet header include the following:
* **Version -**This field contains a 4-bit binary value set to 0110 that identifies this as an IP version 6 packet.
* **Traffic Class -**This 8-bit field is equivalent to the IPv4 Differentiated Services (DS) field.
* **Flow Label -**This 20-bit field suggests that all packets with the same flow label receive the same type of handling by routers.
* **Payload Length -**This 16-bit field indicates the length of the data portion or payload of the IPv6 packet. This does not include the length of the IPv6 header, which is a fixed 40-byte header.
* **Next Header -**This 8-bit field is equivalent to the IPv4 Protocol field. It indicates the data payload type that the packet is carrying, enabling the network layer to pass the data to the appropriate upper-layer protocol.
* **Hop Limit** - This 8-bit field replaces the IPv4 TTL field. This value is decremented by a value of 1 by each router that forwards the packet. When the counter reaches 0, the packet is discarded, and an ICMPv6 Time Exceeded message is forwarded to the sending host. This indicates that the packet did not reach its destination because the hop limit was exceeded. Unlike IPv4, IPv6 does not include an IPv6 Header Checksum, because this function is performed at both the lower and upper layers. This means the checksum does not need to be recalculated by each router when it decrements the Hop Limit field, which also improves network performance.
* **Source IPv6 Address -**This 128-bit field identifies the IPv6 address of the sending host.
* **Destination IPv6 Address -**This 128-bit field identifies the IPv6 address of the receiving host.
* **Rule 1 – Omit Leading Zeros**

The first rule to help reduce the notation of IPv6 addresses is to omit any leading 0s (zeros) in any hextet. Here are four examples of ways to omit leading zeros:

* 01ab can be represented as 1ab
* 09f0 can be represented as 9f0
* 0a00 can be represented as a00
* 00ab can be represented as ab
* 0000 can be represented as 0

This rule only applies to leading 0s, NOT to trailing 0s, otherwise the address would be ambiguous. For example, the hextet “abc” could be either “0abc” or “abc0”, but these do not represent the same value.

* **Rule 2- Double Colon**

Continuous string of hextet having 0 can be indicated as :: But if in multiple places, most continuous sting will be used as ::

* Eg: 2001:0db8:0000:1111:0000:0000:0000:0001
* First rule removes the leading zeros
* 2001:db8:0:1111:0:0:0:1
* Second rule joins continuous zero string as ::
* 2001;db8:0:1111::1
  1. **FRAGMENTATION**

Maximum transmission unit (MTU) is maximum amount of PDU (Protocol Data Unit) at different type of network medium like wireless, copper, fibre, etc

PDUs are structured differently at each layer of the OSI model. They contain both user data and protocol-specific control information (e.g., addresses, sequence numbers and the data content). As data moves down the layers, each layer adds its own PDU information, encapsulating the data from the layer above. It de-encapsulates when moving up

PDUs at different OSI layers:

* **Layer 1 (Physical):** Raw bits
* **Layer 2 (Data Link):** Frame
* **Layer 3 (Network):** Packet
* **Layer 4 (Transport):** Segment or datagram
* **Layer 5 (Session) and above:** Data

Routers are responsible for fragmenting packets that are capable of travelling on the network medium using MTU. IPV6 Packets can’t ne fragmented.

* 1. **SUBNET MASK and ANDing**

**Subnet Mask**

Subnet Mask is used to say which is the network portion and host portion with its associated IP Address. subnet mask does not actually contain the network or host portion of an IPv4 address, it just tells the computer where to look for the part of the IPv4 address that is the network portion and which part is the host portion.

**The Prefix length** or Slash Notation can also be used to denote a Subnet Mask

For example:

* 255.0.0.0 (subnet) can be denoted as /8
* IP Address 192.168.100.1 has subnet mask of 255.255.255.0 which can be denoted as 192.168.100.1/24

**ANDing**

The actual process used to identify the network portion and host portion is called ANDing.

When using a Boolean AND operation, both input values must be True for the result to be True (1). Even if one of them is false (0), the whole result is false.

* 1 AND 1 = 1
* 0 AND 1 = 0
* 1 AND 0 = 0
* 0 AND 0 = 0

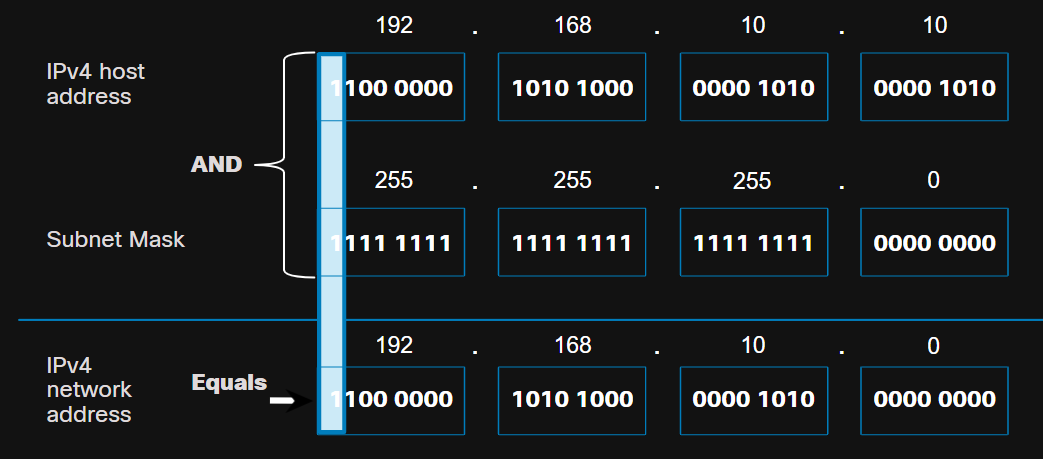
The Both IP Address and Subnet Mask is taken in its Binary format and decimal. Each Digit is compared with them in AND Boolean expression

Eg: 192.168.100.1 has subnet mask of 255.255.255.0

192 binary value 1100 0000

255 binary value 1111 1111

Network IP 1100 0000 (Result using Boolean Operation) is 192 in decimal

Continuing this for other portions of IP and subnet mask will give the network address. In this example as 192.168.100.0

* 1. **MAC ADDRESS**

Also referred to as content addressable memory (CAM) table.

**Address Resolution Protocol (ARP)**

Address Resolution Protocol (ARP) is used to determine the device MAC address of a known destination device IPv4 address. ARP sends broadcast to all devices in the network to find MAC Address. The destination MAC address for an Ethernet broadcast is FFFF.FFFF.FFFF.

* Show ip arc command can be used to see arp table in cisco devices
* Arp -a in windows
* ARP REQUEST
* ARP Reply

**Neighbor Discovery (ND)**

Neighbor Discovery (ND) is used to determine the MAC address of a known destination device IPv6 address.

* 1. **PORT**

**Ports**

* Well Known Ports: Destination ports ranging from 0 to 1023
* Registered Ports: Source or destination ports for registered applications (Ports are registered for applications by request to IANA) ranging from 1024 to 49151
* Private ports: source ports for applications. These are not pre-registered so any applications can use these ports for temporary communication. They range from 49152 to 65535

**Socket**

The source and destination ports are placed within the segment. The segments are then encapsulated within an IP packet. The IP packet contains the IP address of the source and destination. The combination of the source IP address and source port number, or the destination IP address and destination port number is known as a socket.

* Eg 192.168.10.1:80
* : is used to separate IP from Ports
  1. **HIERARCHICAL NETWORK DESIGN MODEL**

**Access Layer**

The access layer provides a connection point for end user devices to the network and allows multiple hosts to connect to other hosts through a network device, usually a switch

**Distribution Layer**

The distribution layer provides a connection point for separate networks and controls the flow of information between the networks.

**Core Layer**

The core layer is a high-speed backbone layer with redundant (backup) connections. It is responsible for transporting large amounts of data between multiple end networks.

* 1. **RELIABLE NETWORK**

**Fault Tolerance**

Reduce the number of affected devices during a failure

**Quality of Service**

Managing network traffic to avoid congestion and prioritize network traffic based on data types.

**Scalability**

Ability of the network to grow without affecting performance

**Hypervisor**

**Type 1 – Bare Metal hypervisor**

Hypervisor is installed on top of the hardware and all the operating systems are created as virtual machines using the hypervisor

**Type 2 – Hosted Hypervisor**

Hypervisor is installed on top on already installed host operating systems so the virtual machines created using hypervisor has to share the hardware resources with the virtual machines and the host OS.

* 1. **DNS**

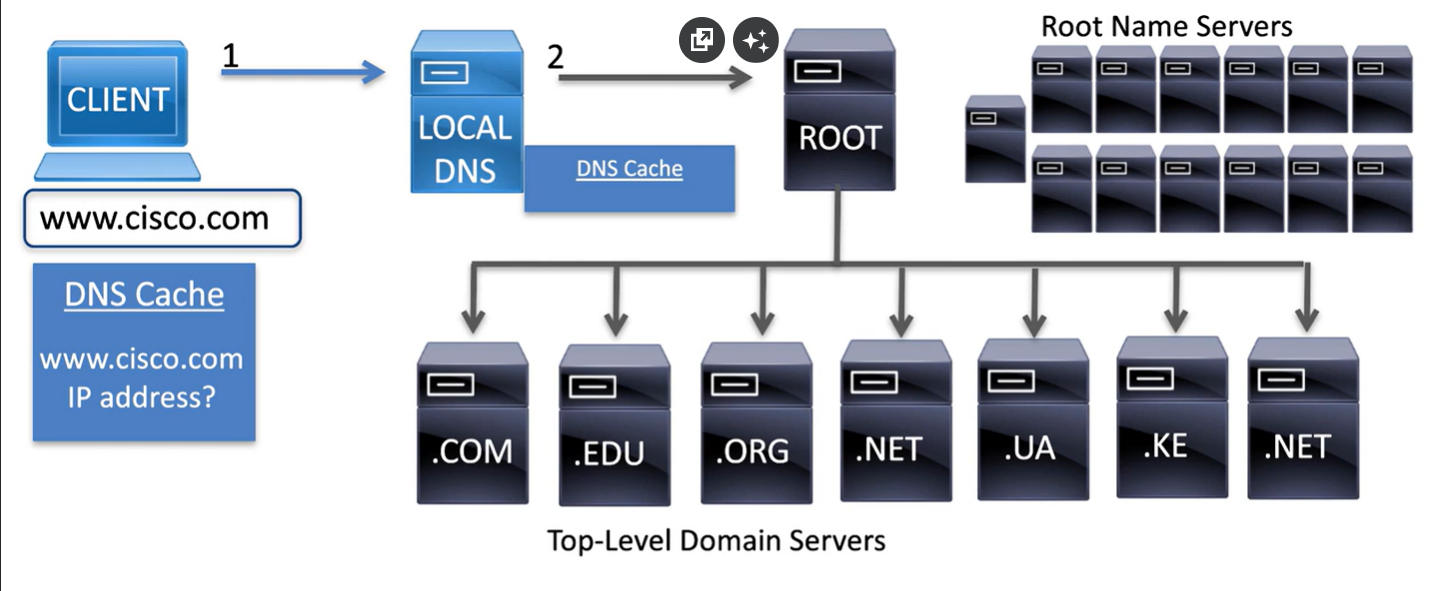
fully-qualified domain names (FQDNs), such as http://www.cisco.com

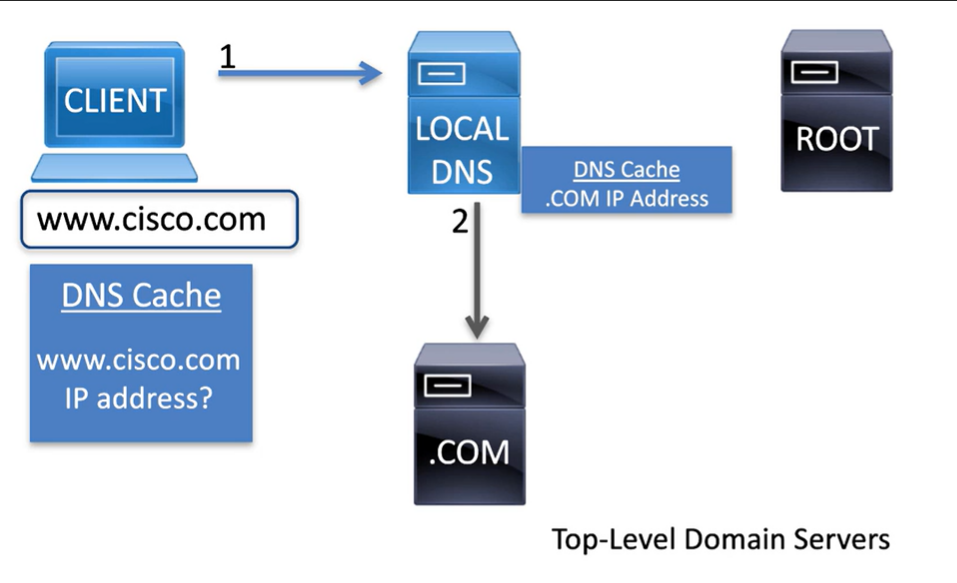
Ipconfig /displaydns is used to see DNS cache table

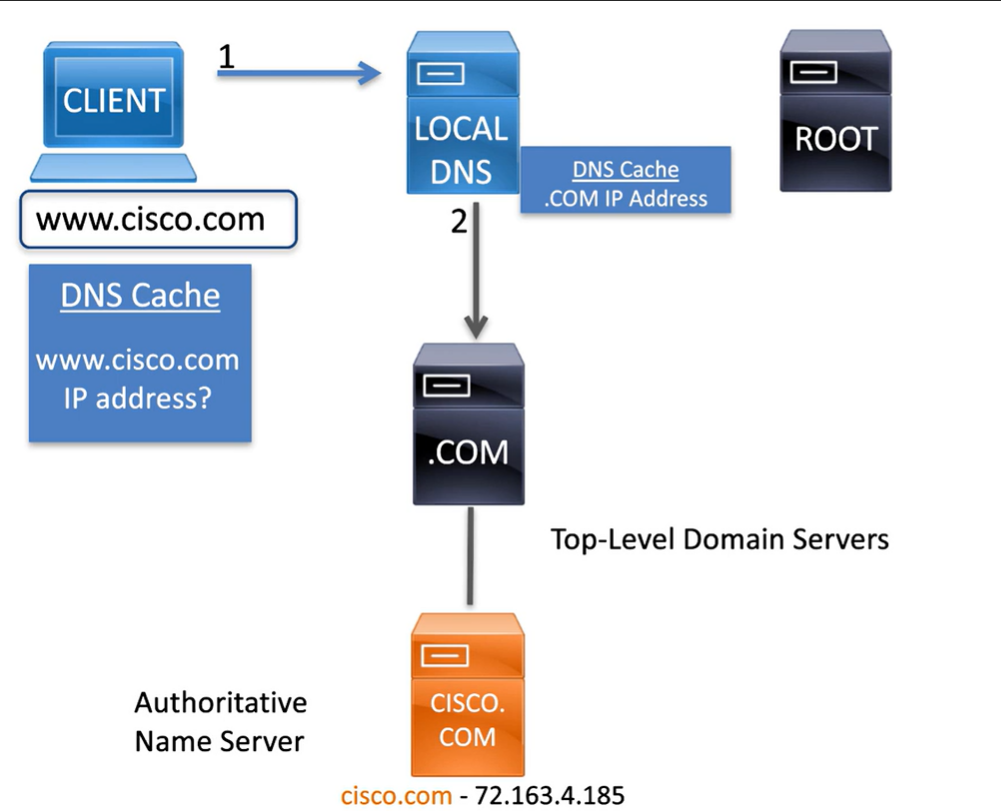
To resolve a domain name to its IP address, Device uses DNS Server. Every Device has a local DNS Server also known as **Recursive Resolver**.

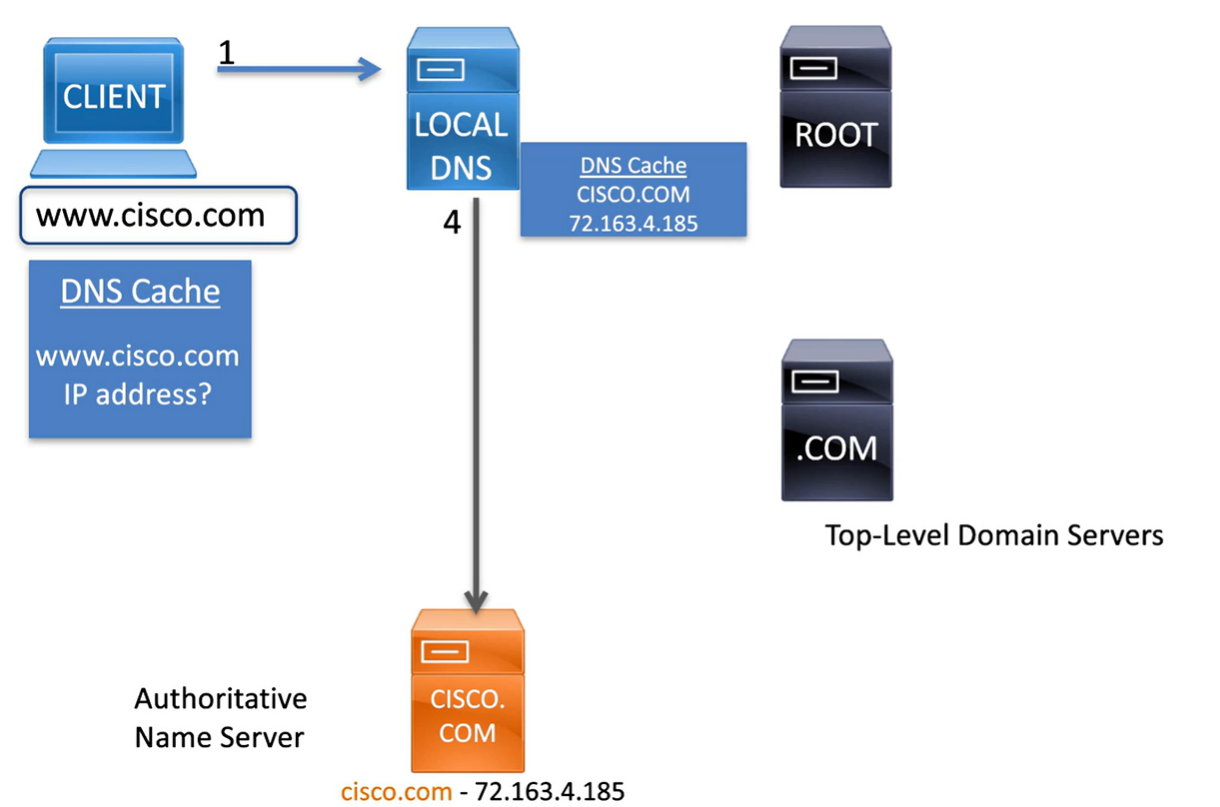
Device will check with the Local DNS Server for the IP address of a domain. If it doesn’t have it, the local DNS server will contact the Root DNS Server maintained by 12 Organizations around the world.

Root DNS Server transfers the request to top level domain server (.com server, .in server, .edu server, etc). If the request made by the device is for .com. The .com Top level Domain Server will reply with its own IP Address to the local DNS Server.



After storing the .com Server IP in its cache, the local DNS can directly contact the .com server whenever it needs a request for IP for a page with .com instead of going to the .com server via the root server.

Top level Domain Server will reach the Authoritative Name Server which will have Domain Name and IP Address of a Specific Domain so The top level domain will send the IP of the Authoritative Name Server to The local DNS Server

After storing the IP of Authoritative Name Server in the local DNS Server cache or if it already has the IP of Authoritative Name Server, the local DNS Server can Directly contact it without going through root and top-level domain server

Authoritative Name Server will have domain and IP address of various query in a single domain so it will reply to the local DNS Server for the IP address of requested query

* 1. **DHCP**

For IPV4

* DHCP DISCOVER
* DHCP OFFER
* DHCP REQUEST
* DHCP ACK

FOR IPV6

The DHCPv6 messages are SOLICIT, ADVERTISE, INFORMATION REQUEST, and REPLY.

* 1. **TCP**
* The six control bits flags in the tcp header
* **URG** (Urgent pointer field) - The data starting from here is urgent — process it immediately
* **ACK** - Acknowledgment flag used in connection establishment and session termination
* **PSH** (Push function) - “Deliver the data to the application immediately, don’t wait to fill the buffer.” Normally, TCP may hold data in a buffer to optimize transmission. PSH overrides this and forces an immediate push up to the application layer.
* **RST** - Reset the connection when an error or timeout occurs
* **SYN** - Synchronize sequence numbers used in connection establishment
* **FIN** - No more data from sender and used in session termination

**Window size** – Amount of data that can be sent before getting an acknowledgment

* Eg: 16mb is sent to server from host, then the server will send an acknowledgment saying that data was received and request host to send the next 16 mb of data.
* If there is no acknowledgement from server after sending data from host to server, the host will resend the data
  1. ICMP

ICMP (Internet Control Message Protocol) is a network layer protocol (part of the IP suite). It’s mainly used for error reporting and diagnostics, not for sending user data.

Type of ICMP considered essential:

* Ping echo packets
* Reply packets
* Unreachable message
* source quench - tells the source to reduce the pace of traffic

**CISCO OS AND DEVICES**

Cisco IOS Software uses Command Line Interface (CLI) to monitor and configure Cisco Devices. There are two modes in Cisco IOS. This IOS is same for both switches and Routers.

* User EXEC Mode: Monitor commands and limited basic commands. It can’t change the configuration of the devices and is considered as a view only mode. Denoted as >
* Privileged EXEC Mode: Access all monitor, managing and configuration commands. Denoted as #
* Global Configuration Mode: Make Major Configuration to the device. There are sub configuration modes for different device features and components. Denoted as (config)#
* enable – move from user exec to privileged exec mode
* disable – move from privileged exec mode to user exec mode
* configure terminal – move from privileged exec mode to global configuration
* exit – leave global configuration mode to privileged exec mode
* end & ctrl+z – directly go back to privileged exec mode from any of the sub configuration mode
* ? is used to see the available commands in each mode. It can also be used to find the arguments available for a single command
* Eg; interface ? will give result as Ethernet, range, vlan and others that can be used as an argument for interface command
* ? can also be used to find a specific command. If i ? is used, it will give result as interface, ip cause these commands start with i
* Show running-config = current configurations
* Show interfaces = configurations of interfaces only
* Show ip interface = layer 3 info of the interface
* Show arp = arp table
* Show ip route = routing table by listing the connected devices
* Show version = hardware and os info
* Show protocols = protocols being used

**END POINT SECURITY**

The United States Computer Emergency Readiness Team (US-CERT) and the U.S. Department of Homeland Security sponsor a dictionary of **common vulnerabilities and exposures (CVE).**

**Automated Indicator Sharing (AIS)**, a Cybersecurity and Infrastructure Security Agency (CISA) capability, enables the real-time exchange of cybersecurity threat indicators using a standardized and structured language called Structured Threat Information Expression (STIX) and Trusted Automated Exchange of Intelligence Information (TAXII).

* 1. **SOCIAL ENGINEERING ATTACKS**

**Pretexting**

when an individual lies to gain access to privileged data. For example, an attacker pretends to need personal or financial data in order to confirm a person’s identity.

**Quid pro quo attacks**

Quid pro quo attacks involve a request for personal information in exchange for something, like a gift. For example, a malicious email could ask you to give your sensitive personal details in exchange for a free vacation.

**Consensus**

Often called ‘social proof,’ consensus attacks work because people tend to act in the same way as other people around them, thinking that something must be right if others are doing it.

For example, cybercriminals may publish a social media post about a ‘business opportunity’ and get dozens of legitimate or illegitimate accounts to comment on its validity underneath, which encourages unsuspecting victims to make a purchase.

**Shoulder surfing**

It is a simple attack that involves observing or literally looking over a target’s shoulder to gain valuable information such as PINs, access codes or credit card details. Criminals do not always have to be near their victim to shoulder surf — they can use binoculars or security cameras to obtain this information.

**Dumpster diving**

The process of going through a target's trash to see what information has been thrown out.

This is why documents containing sensitive information should be shredded or stored in burn bags until they are destroyed by fire after a certain period of time.

**Piggybacking** or **tailgating**

occurs when a criminal follows an authorized person to gain physical entry into a secure location or a restricted area.

A watering hole attack describes an exploit in which an attacker observes or guesses what websites an organization uses most often, and infects one or more of them with malware.

**Typo squatting**

This type of attack relies on common mistakes such as typos made by individuals when inputting a website address into their browser. The incorrect URL will bring the individuals to a legitimate-looking website owned by the attacker, whose goal is to gather their personal or financial information.

**Short message service phishing** or **SMiShing**

Itis another tactic used by attackers to trick you. Fake text messages prompt you to visit a malicious website or call a fraudulent phone number, which may result in malware being downloaded onto your device or personal information being shared.

**Anti-Phishing Working Group (APWG**) is an international association of companies focused on eliminating identity theft and fraud resulting from phishing and email spoofing.

**Grayware**

It is any unwanted application that behaves in an annoying or undesirable manner. for example, tracking your location or delivering unwanted advertising.

* 1. **APPLICATION ATTACKS**

**Dynamic link library (DLL)**

A dynamic link library (DLL) file is a library that contains a set of code and data for carrying out a particular activity in Windows. Applications use this type of file to add functionality that is not built-in, when they need to carry out this activity.

DLL injection allows a cybercriminal to trick an application into calling a malicious DLL file, which executes as part of the target process.

**Lightweight Directory Access Protocol (LDAP)**

It is an open protocol for authenticating user access to directory services. An LDAP injection attack exploits input validation vulnerabilities by injecting and executing queries to LDAP servers, giving cybercriminals an opportunity to extract sensitive information from an organization’s LDAP directory.

**Replay Attack**

This describes a situation where a valid data transmission is maliciously or fraudulently repeated or delayed by an attacker, who intercepts, amends and resubmits the data to get the receiver to do whatever they want.

**Directory traversal Attack**

occurs when an attacker is able to read files on the webserver outside of the directory of the website. A Directory Traversal Attack (also called Path Traversal) is when a hacker tricks a website or system into showing files or folders that they should not normally have access to.

Normally, websites keep their important system files hidden (like passwords, configuration files, etc.). But if the website does not check user input properly, attackers can sneak into those files by climbing up the folder structure.

Example

Suppose a website lets you download reports like this:

https://example.com/download?file=report1.pdf

A normal user can only see report1.pdf.

But a hacker might change the input to:

https://example.com/download?file=../../etc/passwd

**Pharming**

A cyberattack that redirects a user from a legitimate website to a fake one, even if the user types the correct URL.

1. Attackers corrupt DNS servers or the victim’s local DNS cache.
2. When you enter a genuine web address (e.g., www.bank.com), it secretly redirects you to a fake site.

**Watering Hole Attack**

An attack where hackers compromise a website that a specific group of users is known to Attackers study the target group (e.g., employees of a company or industry).

* 1. They identify and infect websites that the group frequently visits.
  2. When users visit the site, malware is automatically delivered to their devices.

**Smurf Attack – A Type of DOS Attack**

Amplification - The threat actor forwards ICMP echo request messages to many hosts. These messages contain the source IP address of the victim.

Reflection - These hosts all reply to the spoofed IP address of the victim to overwhelm it.

**Spoofing**

Non-blind spoofing **-**The threat actor can see the traffic that is being sent between the host and the target. The threat actor uses non-blind spoofing to inspect the reply packet from the target victim. Non-blind spoofing determines the state of a firewall and sequence-number prediction. It can also hijack an authorized session.

Blind spoofing **-**The threat actor cannot see the traffic that is being sent between the host and the target. Blind spoofing is used in DoS attacks.

**TCP SYN Flood Attack**

a threat actor continually sending TCP SYN session request packets with a randomly spoofed source IP address to a target. The target device replies with a TCP SYN-ACK packet to the spoofed IP address and waits for a TCP ACK packet. Those responses never arrive. Eventually the target host is overwhelmed with half-open TCP connections, and TCP services are denied to legitimate users.

**TCP session Hijacking**

a threat actor takes over an already-authenticated host as it communicates with the target. The threat actor must spoof the IP address of one host, predict the next sequence number, and send an ACK to the other host. If successful, the threat actor could send, but not receive, data from the target device.

**UDP Flood Attacks**

send a flood of UDP packets, often from a spoofed host, to a server on the subnet. The program will sweep through all the known ports trying to find closed ports. This will cause the server to reply with an ICMP port unreachable message. Because there are many closed ports on the server, this creates a lot of traffic on the segment, which uses up most of the bandwidth. The result is very similar to a DoS attack.

**ARP POISONING**

Any client can send an unsolicited ARP Reply called a “**gratuitous ARP.**” This is often done when a device first boots up to inform all other devices on the local network of the new device’s MAC address. When a host sends a gratuitous ARP, other hosts on the subnet store the MAC address and IP address contained in the gratuitous ARP in their ARP tables.

Threat actors can use this technique to conduct ARP Poisoning

* 1. **DNS ATTACKS**

**DNS Stealth Attacks**  
Techniques that evade detection by spreading malicious queries across time, IPs, or domains. Example: attackers querying slowly to avoid IDS alerts.

* **Fast Flux**  
  Uses rapidly changing DNS records (IPs linked to a domain) to hide phishing or malware servers behind a botnet. Example: a phishing site’s IP changes every few minutes.
* **Double IP Flux**  
  An advanced fast flux where both the domain’s **A records** and the **name server records (NS)** rotate quickly, making takedown harder.
* **Domain Generative Algorithms (DGA)**  
  Malware generates thousands of pseudo-random domain names daily to contact its command-and-control server, avoiding simple blocking. Example: Conficker worm.

**DNS Open Resolver Attacks**  
Many organizations use the services of publicly open DNS servers such as GoogleDNS (8.8.8.8) to provide responses to queries. This type of DNS server is called an open resolver. A DNS open resolver answers queries from clients outside of its administrative domain Attackers abuse misconfigured public DNS resolvers to hide their source or amplify traffic in DDoS attacks.

* **DNS Cache Poisoning**  
  Injecting false DNS records into a resolver’s cache to redirect users to malicious sites. Example: redirecting bank.com to an attacker’s IP.
* **DNS Amplification & Reflection Attacks**  
  Attackers send spoofed queries with victim IP as source to open resolvers, which reply with large responses to the victim’s IP, overwhelming it. Example: small query → 100x larger response.
* **DNS Resource Utilization Attack**  
  Flooding DNS servers with valid or malformed queries to exhaust CPU, memory, or bandwidth, causing denial of service

**DNS Domain Shadowing Attack**  
the threat actor gathering domain account credentials in order to silently create multiple sub-domains to be used during the attacks. These subdomains typically point to malicious servers without alerting the actual owner of the parent domain.

**DNS Tunnelling**  
Encodes data inside DNS queries and responses to bypass firewalls and exfiltrate information stolen from command-and-control (CnC) servers. Example: malware sending stolen data disguised as DNS traffic.

Various types of encoding, such as Base64, 8-bit binary, and Hex can be used to camouflage the data and evade basic data loss prevention (DLP) measures.

* 1. **HTTP ATTACKS**

An **inline frame (iframe)** is an HTML element that allows you to add another webpage inside the current webpage. they are often used to insert advertisements from other sources into the page

**Malicious iframe**

Threat actors often make use of malicious inline frames. the iFrame is run in the page, it can be used to deliver a malicious exploit, such as spam advertising, an exploit kit, and other malware. Iframe can be even invisible by uploading malicious web pages that only have very few pixels so it can’t be seen

**HTTP 302 Cushoning**

Sometimes a page might be moved from one web server to another. In such cases, the url and location of new server is added to the place of old url in the 1st server. This is HTTP 302 Found code.

Threat actors use the 302 Found HTTP response status code to direct the user’s web browser to a new location

* 1. **EMAIL ATTACKS**

**Open Mail Relay server**

This type of server can be accessed by anyone on internet to spend large volume of mails so if a company mail server is mistakenly configured as open relay mail server, attackers can send large amounts of spam and phishing mails,

**Homoglyphs**

Homoglyphs are characters from different writing that **look visually similar** but are technically different.

* Eg: I and 1 might look the same
* 0 and O might look the same
* URL in mails with homoglyphs can take the user to malicious site
  1. **COUNTERMEASURES AGAINST WORMS, VIRUSES**

**Containment**

limiting the spread of a worm infection to areas of the network that are already affected.

**Inoculation**

all uninfected systems are patched with the appropriate vendor patch

**Quarantine**

tracking down and identifying infected machines within the contained areas and disconnecting, blocking, or removing them

**Treatment**

actively disinfecting infected systems. This can involve terminating the worm process, removing modified files or system settings that the worm introduced, and patching the vulnerability the worm used to exploit the system.

* 1. **WIRELESS LAN**

**Infrastructure Mode**

Wireless Router can be used to connect devices using both wired and wireless devices

Eg: wired communication between PC and Router with ethernet, Wireless communication between router and smartphone

**AD Hoc Mode**

Wireless communication between two devices without a router

* Eg: Bluetooth, peer to peer
* Tethering: Variation of ad hoc where smart phone connects internet to other devices like pc or laptop by acting as an access point

**BSS – Basic Service Set**

Small wireless network with a single access point – a wireless router, area of the LAN is called BSA = Basic Service Area

Devices use Routers MAC Address to connect which is also referred to as BSSISD

**ESS – Extended Service Set**

Multiple BSS are connected together using a wired connection

**Frames in Wireless LAN**

* Frame Control **-**This identifies the type of wireless frame and contains subfields for protocol version, frame type, address type, power management, and security settings.
* Duration **-**This is typically used to indicate the remaining duration needed to receive the next frame transmission.
* Address1 **-**This usually contains the MAC address of the receiving wireless device or AP.
* Address2 **-**This usually contains the MAC address of the transmitting wireless device or AP.
* Address3 **-**This sometimes contains the MAC address of the destination, such as the router interface (default gateway) to which the AP is attached.
* Sequence Control -This contains information to control sequencing and fragmented frames.
* Address4 **-**This usually missing because it is used only in ad hoc mode.
* When communication between one access point, Addr1 = Receiver Address (RA) → e.g., AP
* Addr2 = Transmitter Address (TA) → e.g., STA
* Addr3 = Destination/Source depending on To Distribution System/From Distribution System
* When communication between one access point, Address 1**:** Final receiver at the wireless hop (e.g., AP2’s MAC)
* Address 2**:** Immediate transmitter (e.g., AP1’s MAC)
* Address 3**:** Destination (client device)
* Address 4: Original Source (client device)
* Payload **-**This contains the data for transmission.
* FCS **-**This is used for Layer 2 error control.

**CSMA/CA**

WLANs are half-duplex, shared media configurations. Half-duplex means that only one client can transmit or receive at any given moment. Shared media means that wireless clients can all transmit and receive on the same radio channel. This creates a problem because a wireless client cannot hear while it is sending, which makes it impossible to detect a collision.

1. Listens to the channel to see if it is idle, which means that is senses no other traffic is currently on the channel. The channel is also called the carrier.
2. Sends a ready to send (RTS) message to the AP to request dedicated access to the network.
3. Receives a clear to send (CTS) message from the AP granting access to send.
4. If the wireless client does not receive a CTS message, it waits a random amount of time before restarting the process.
5. After it receives the CTS, it transmits the data.
6. All transmissions are acknowledged. If a wireless client does not receive an acknowledgment, it assumes a collision occurred and restarts the process.

**Discover Network**

**Passive mode**

The AP openly advertises its service by periodically sending broadcast beacon frames containing the SSID, supported standards, and security settings, it is normal Wi-Fi searching in devices

**Active Mode**

Wireless devices manually send a request with SSID, security setting and standards to connect to the wireless network

**Security Methods**

**SSID Cloaking –** Active mode doesn’t not transmit SSID so to connect to the access point, they have to be manually entered

**MAC Filtering -** Access Points can be configured to deny access to specific MAC address

**Authentication**

* **Open Authentication –** No passwords
* **Shared Key Authentication**
* Wired Equivalent privacy (WEP) – Rivest Cipher 4 with static key
* Wifi Protected Access (WPA) – Temporal Key Integrity Protocol Algorithm for encryption
* WPA2 – AES encryption. Currently Strongest
* WPA3- Latest security methods and use PMF (Protected Management Frames). It disallows Legacy methods. Not in use yet
* In Enterprise Mode, access point can be only authenticated using a RADIUS server for better security

**Advanced Encryption Standard (AES)** - AES is the encryption method used by WPA2. It is the preferred method because it is a far stronger method of encryption. It uses the Counter Cipher Mode with Block Chaining Message Authentication Code Protocol (CCMP) that allows destination hosts to recognize if the encrypted and non-encrypted bits have been altered

**Temporal Key Integrity Protocol (TKIP)** - TKIP is the encryption method used by WPA. It provides support for legacy WLAN equipment by addressing the original flaws associated with the 802.11 WEP encryption method. It makes use of WEP, but encrypts the Layer 2 payload using TKIP, and carries out a Message Integrity Check (MIC) in the encrypted packet to ensure the message has not been altered

* 1. **FIREWALL**

**Designs**

**Private and Public**

* Traffic originating from the private network is permitted and inspected as it travels toward the public network. Inspected traffic returning from the public network and associated with traffic that originated from the private network is permitted.
* Traffic originating from the public network and traveling to the private network is generally blocked.

**Demilitarized zone (DMZ)**

A demilitarized zone (DMZ) is a firewall design where there is typically one inside interface connected to the private network, one outside interface connected to the public network, and one DMZ interface

* Traffic originating from the private network is inspected as it travels toward the public or DMZ network. This traffic is permitted with little or no restriction. Inspected traffic returning from the DMZ or public network to the private network is permitted.
* Traffic originating from the DMZ network and traveling to the private network is usually blocked.
* Traffic originating from the DMZ network and traveling to the public network is selectively permitted based on service requirements.
* Traffic originating from the public network and traveling toward the DMZ is selectively permitted and inspected. This type of traffic is typically email, DNS, HTTP, or HTTPS traffic. Return traffic from the DMZ to the public network is dynamically permitted.
* Traffic originating from the public network and traveling to the private network is blocked.

**Zone-based policy firewalls (ZPFs)**

Zone-based policy firewalls (ZPFs) use the concept of zones to provide additional flexibility. A zone is a group of one or more interfaces that have similar functions or features. Zones help you specify where firewall rule or policy should be applied.

**Types**

**Packet Filtering (Stateless) Firewall**

Packet filtering firewalls are usually part of a router firewall, which permits or denies traffic based on Layer 3 and Layer 4 information. Uses a simple policy table look-up that filters traffic based on specific criteria. It does not track the state of a connection, making it fast but less secure since it cannot differentiate between legitimate and malicious traffic within a session.

**Stateful Firewall**

Stateful firewalls are the most versatile and the most common firewall technologies in use. Stateful firewalls provide stateful packet filtering by using connection information maintained in a state table. It improves on this by monitoring active connections and keeping track of session states. It only allows packets that are part of valid, established connections. Stateful filtering is a firewall architecture that is classified at the network layer. It also analyses traffic at OSI Layer 4 and Layer 5.

**Application Gateway Firewall**

An **Application Gateway Firewall**, also known as a proxy firewall, works at the application layer. It acts as an intermediary between clients and servers, inspecting the actual application-level traffic (such as HTTP or FTP). This provides deeper inspection and control but can slow down performance because all traffic must pass through the proxy.

**Next-generation firewalls (NGFW)**

* Integrated intrusion prevention
* Application awareness and control to see and block risky apps
* Upgrade paths to include future information feeds
* Techniques to address evolving security threats

**Host based (server and personal) firewall -** A PC or server with firewall software running on it.

**Transparent firewall -**Filters IP traffic between a pair of bridged interfaces

**Hybrid firewall -** A combination of the various firewall types. For example, an application inspection firewall combines a stateful firewall with an application gateway firewall

**Layered Defence** is a security design uses different types of firewalls and security measures that are combined at different areas of the network to add depth to the security of an organization

* 1. **IDS AND IPS**

IDS and IPS technologies use signatures to detect patterns in network traffic. A signature is a set of rules that an IDS or IPS uses to detect malicious activity. Signatures can be used to detect severe breaches of security, to detect common network attacks, and to gather information. IDS and IPS technologies can detect atomic signature patterns (single-packet) or composite signature patterns (multi-packet).

**IDS Advantages**

* The IDS do not impact network performance. Specifically, it does not introduce latency, jitter, or other traffic flow issues.
* The IDS do not affect network functionality if the sensor fails. It only affects the ability of the IDS to analyse the data.

**IDS Disadvantages**

* An IDS sensor cannot stop the packets that have triggered an alert and are less helpful in detecting email viruses and automated attacks, such as worms.
* Tuning IDS sensors to achieve expected levels of intrusion detection can be very time-consuming. Users deploying IDS sensor response actions must have a well-designed security policy and a good operational understanding of their IDS deployments.
* An IDS implementation is more vulnerable to network security evasion techniques because it is not inline.

**IPS Advantages**

* An IPS sensor can be configured to drop the trigger packets, the packets associated with a connection, or packets from a source IP address.
* Because IPS sensors are inline, they can use stream normalization. Stream normalization is a technique used to reconstruct the data stream when the attack occurs over multiple data segments.

**IPS Disadvantages**

* Because it is deployed inline, errors, failure, and overwhelming the IPS sensor with too much traffic can have a negative effect on network performance.
* An IPS sensor can affect network performance by introducing latency and jitter.
* An IPS sensor must be appropriately sized and implemented so that time-sensitive applications, such as VoIP, are not adversely affected.

**Host-based IPS**

Host-based IPS (HIPS) is software installed on a host to monitor and analyse suspicious activity. it can monitor and protect operating system and critical system processes that are specific to that host. HIPS can monitor abnormal activity and prevent the host from executing commands that do not match typical behaviour.

This suspicious or malicious behaviour might include unauthorized registry updates, changes to the system directory, executing installation programs, and activities that cause buffer overflows. Network traffic can also be monitored to prevent the host from participating in a denial-of-service (DoS) attack or being part of an illicit FTP session.

**Network-based IPS**

A network-based IPS can be implemented using a dedicated or non-dedicated IPS device. Network-based IPS implementations are a critical component of intrusion prevention. There are host-based IDS/IPS solutions, but these must be integrated with a network-based IPS implementation to ensure a robust security architecture.

Sensors detect malicious and unauthorized activity in real time and can take action when required. As shown in the figure, sensors are deployed at designated network points. This enables security managers to monitor network activity while it is occurring, regardless of the location of the attack target.

* 1. **SECURITY SERVICES**

**Access Control List (ACL)**

An Access Control List (ACL) is a series of commands that control whether a device forwards or drops packets based on information found in the packet header. When configured, ACLs perform the following tasks:

* They limit network traffic to increase network performance. For example, if corporate policy does not allow video traffic on the network, ACLs that block video traffic could be configured and applied. This would greatly reduce the network load and increase network performance.
* They provide traffic flow control. ACLs can restrict the delivery of routing updates to ensure that the updates are from a known source.
* They provide a basic level of security for network access. ACLs can allow one host to access a part of the network and prevent another host from accessing the same area. For example, access to the Human Resources network can be restricted to authorized users.
* They filter traffic based on traffic type. For example, an ACL can permit email traffic, but block all Telnet traffic.
* They screen hosts to permit or deny access to network services. ACLs can permit or deny a user to access file types, such as FTP or HTTP.

**Simple Network Management Protocol (SNMP)**

Simple Network Management Protocol (SNMP) allows administrators to manage end devices such as servers, workstations, routers, switches, and security appliances, on an IP network. It enables network administrators to monitor and manage network performance, find and solve network problems, and plan for network growth.

**NetFlow**

NetFlow is a Cisco IOS technology that provides statistics on packets flowing through a Cisco router or multilayer switch. While SNMP attempts to provide a very wide range of network management features and options, NetFlow is focused on providing statistics on IP packets flowing through network devices. Similar tech is used by other vendors with varying names. NetFlow does not do a full packet capture or capture the actual content in the packet. NetFlow records information about the packet flow including metadata. NetFlow information can be viewed with tools such as the nfdump

an IP Flow is based on a set of 5 to 7 IP packet attributes flowing in a single direction. A flow consists of all packets transmitted until the TCP conversation terminates. IP Packet attributes used by NetFlow are:

* IP source address
* IP destination address
* Source port
* Destination port
* Layer 3 protocol type
* Class of Service
* Router or switch interface

All packets with the same source/destination IP address, source/destination ports, protocol interface and class of service are grouped into a flow, and then packets and bytes are tallied.

**Port mirroring**

A **Switched Port Analyzer (SPAN)**, often called **port mirroring**, is a feature on network switches that allows traffic from one or more switch ports (or VLANs) to be copied and sent to another port. This destination port is usually connected to a monitoring device such as a network analyser, IDS/IPS, or packet sniffer.

**Syslog**

When certain events occur on a network, networking devices have trusted mechanisms to notify the administrator with detailed system messages and logs. These logs can be either non-critical or significant. Network administrators have a variety of options for storing, interpreting, and displaying these logs, and for being alerted to those logs that could have the greatest impact on the network infrastructure. UDP port 514

The next generation (ng) syslog implementation, known as syslog-ng, offers enhancements that can help prevent some of the exploits that target syslog.

**NTP**

This protocol allows routers on the network to synchronize their time settings with an NTP server. A group of NTP clients that obtain time and date information from a single source have more consistent time settings. When NTP is implemented in the network, it can be set up to synchronize to a private primary clock or it can synchronize to a publicly available NTP server on the Internet. UDP port 123

NTP networks use a hierarchical system of time sources. Each level in this hierarchical system is called a stratum. The stratum level is defined as the number of hops counts from the authoritative source. The synchronized time is distributed across the network using NTP

**Stratum 0 -**An NTP network gets the time from authoritative time sources. These authoritative time sources, also referred to as stratum 0 devices, are high-precision timekeeping devices assumed to be accurate and with little or no delay associated with them.

**Stratum 1 -**The stratum 1 devices are directly connected to the authoritative time sources. They act as the primary network time standard.

**Stratum 2 and lower strata -** The stratum 2 servers are connected to stratum 1 devices through network connections. Stratum 2 devices, such as NTP clients, synchronize their time using the NTP packets from stratum 1 servers. They could also act as servers for stratum 3 devices.

* 1. **WINDOWS**

**Disk Operating System (DOS)**

The Disk Operating System (DOS) is an operating system that the computer uses to enable these data storage devices to read and write files. DOS provides a file system which organizes the files in a specific way on the disk. Microsoft bought DOS and developed MS-DOS.

**MACE**

**M – Modified Time (Last Write Time)**

* The last time the file’s **content** was modified.
* Example: If you open a .txt file and change its text, this timestamp updates.

**A – Access Time (Last Access Time)**

* The last time the file was **read or accessed**.
* Example: Opening a file (even without editing) update this.
* Some OS/file systems disable or delay updating this for performance reasons.

**C – Create Time (Creation Time)**

* The time the file was **created** in the filesystem.
* Example: Copying a file into a folder gives it a new create time in that folder.

**E – Entry Modified Time (MFT Entry Modified Time)**

* The last time the **metadata** of the file was changed (not the content).
* Example: Renaming a file, changing permissions, or moving it within the same drive updates this.

**Boot Process**

**Partition Boot Sector -**This is the first 16 sectors of the drive. It contains the location of the Master File Table (MFT). The last 16 sectors contain a copy of the boot sector.

**Master File Table (MFT) -** This table contains the locations of all the files and directories on the partition, including file attributes such as security information and timestamps.

**System Files -** These are hidden files that store information about other volumes and file attributes.

**File area -** The main area of the partition where files and directories are stored.

* In BIOS firmware, the process begins with the BIOS initialization phase. This is when hardware devices are initialized and a power on self-test (POST) is performed to make sure all of these devices are communicating. When the system disk is discovered, the POST ends. The last instruction in the POST is to look for the master boot record (MBR).
* The MBR contains a small program that is responsible for locating and loading the operating system. The BIOS executes this code and the operating system starts to load.
* In contrast to BIOS firmware, UEFI firmware has a lot of visibility into the boot process. UEFI boots by loading EFI program files, stored as .efi files in a special disk partition, known as the EFI System Partition (ESP).
* **Note:**A computer that uses UEFI stores boot code in the firmware. This helps to increase the security of the computer at boot time because the computer goes directly into protected mode.
* Whether the firmware is BIOS or UEFI, after a valid Windows installation is located, the **Bootmgr.exe** file is run. **Bootmgr.exe** switches the system from real mode to protected mode so that all of the system memory can be used.
* **Bootmgr.exe** reads the Boot Configuration Database (BCD). The BCD contains any additional code needed to start the computer, along with an indication of whether the computer is coming out of hibernation, or if this is a cold start. If the computer is coming out of hibernation, the boot process continues with**Winresume.exe.** This allows the computer to read the**Hiberfil.sys**file which contains the state of the computer when it was put into hibernation.
* If the computer is being booted from a cold start, then the **Winload.exe**file is loaded. The **Winload.exe** file creates a record of the hardware configuration in the registry. The registry is a record of all of the settings, options, hardware, and software the computer has. The registry will be explored in depth later in this chapter.**Winload.exe** also uses Kernel Mode Code Signing (KMCS) to make sure that all drivers are digitally signed. This ensures that the drivers are safe to load as the computer starts.
* After the drivers have been examined, **Winload.exe**runs **Ntoskrnl.exe** which starts the Windows kernel and sets up the HAL. Finally, the Session Manager Subsystem (SMSS) reads the registry to create the user environment, start the Winlogon service, and prepare each user’s desktop as they log on

**Processes and Threads**

A Windows application is made up of processes. The application can have one or many processes dedicated to it. A process is any program that is currently executing. Each process that runs is made up of at least one thread. A thread is a part of the process that can be executed. The processor performs calculations on the thread. All of the threads dedicated to a process are contained within the same address space. This means that these threads may not access the address space of any other process. This prevents corruption of other processes. Because Windows multitasks, multiple threads can be executed at the same time. The amount of threads that can be executed at the same time is dependent on the number of the computer’s processors.

**Registry**

The registry is a hierarchical database where the highest level is known as a hive, below that there are keys, followed by subkeys. Values store data and are stored in the keys and subkeys. A registry key can be up to 512 levels deep.

New hives cannot be created. The registry keys and values in the hives can be created, modified, or deleted by an account with administrative privileges

Registry keys can contain either a subkey or a value. The different values that keys can contain are as follows:

* **REG\_BINARY -** Numbers or Boolean values
* **REG\_DWORD -** Numbers greater than 32 bits or raw data
* **REG\_SZ -** String values

**Net command**

Windows has many commands that can be entered at the command line. One important command is the **net** command, which is used in the administration and maintenance of the OS.

* Net accounts - Sets password and logon requirements for users
* Net session - Lists or disconnects sessions between a computer and other computers on the network
* Net share - Creates, removes, or manages shared resources
* Net start - Starts a network service or lists running network services
* Net stop - Stops a network service
* Net use - Connects, disconnects, and displays information about shared network resources
* Net view - Shows a list of computers and network devices on the network

**Network resources**

Originally developed by IBM, Microsoft aided in the development of the Server Message Block (SMB) protocol to share network resources. SMB is mostly used for accessing files on remote hosts. The Universal Naming Convention (UNC) format is used to connect to resources, for example:

∖∖servername∖sharename∖file

**Netstat**

When malware is present in a computer, it will often open communication ports on the host to send and receive data. The **netstat** command can be used to look for inbound or outbound connections that are not authorized. When used on its own, the **netstat** command will display all of the active TCP connections.

To make this process easier, you can link the connections to the running processes that created them in Task Manager. To do this, open a command prompt with administrative privileges and enter the **netstat -abno** command

**Local Security Policy**

A security policy is a set of objectives that ensures the security of a network, the data, and the computer systems in an organization. The security policy is a constantly evolving document based on changes in technology, business, and employee requirements.

Password guidelines are an important component of a security policy. Use the Account Lockout Policy in Account Policies to prevent brute-force login attempts, The Local Security Policy applet contains many other security settings that apply specifically to the local computer. You can configure User Rights, Firewall Rules, and even the ability to restrict the files that users or groups are allowed to run with the AppLocker.

* 1. **LINUX**

Security Union is a Linux distro that is used for network security analysis, mainly used by Security Operations Centre (SOC)

Kali Linux distro has tools that are essential for Penetration Testing

Fabrice Bellard has created JSLinux which allows an emulated version of Linux to run in a browser. Search for it on the internet. Open a Linux console in JSLinux

**Commands**

dd – copy data from input to output

ps – lists current running processes

iwconfig – similar to ifconfig, shows wireless network card information

shutdown – shutdown system

passwd – used to change the password

man – display documentation for a specific command

grep – searches for a specific string or characters within a file or other commands

**Monitoring Service Logs**

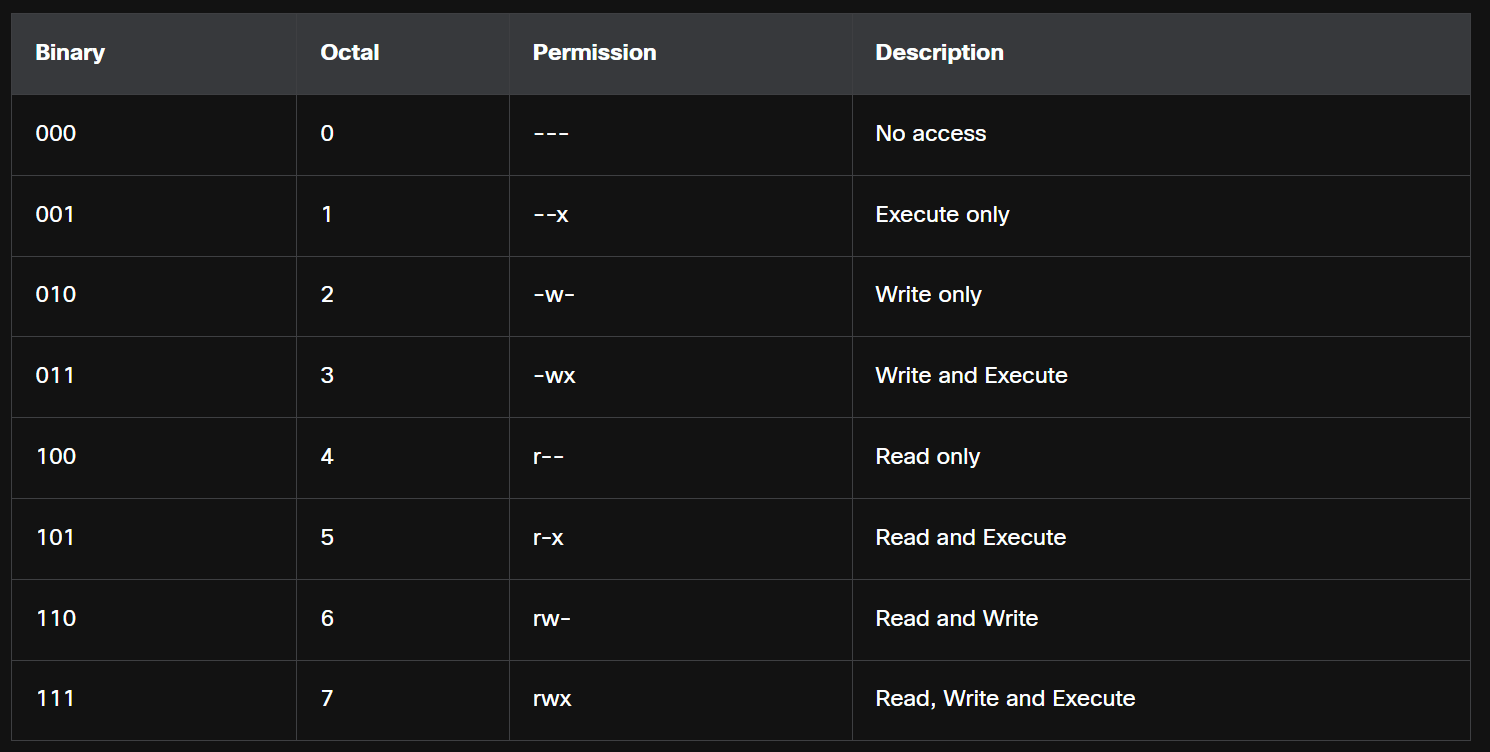
In Linux, log files can be categorized as

* Application logs
* Event logs
* Service logs
* System logs

Some logs contain information about daemons that are running in the Linux system. A daemon is a background process that runs without the need for user interaction. For example, the System Security Services Daemon (SSSD) manages remote access and authentication for single sign-on capabilities.

|  |  |  |
| --- | --- | --- |
| **Linux Log File** | **Description** | |
| /var/log/messages | * This directory contains generic computer activity logs. * It is mainly used to store informational and non-critical system messages. * In Debian-based computers, /var/log/syslog directory serves the same purpose. | |
| /var/log/auth.log | * This file stores all authentication-related events in Debian and Ubuntu computers. * Anything involving the user authorization mechanism can be found in this file. | |
| /var/log/secure | * This directory is used by RedHat and CentOS computers instead of /var/log/auth.log. * It also tracks sudo logins, SSH logins, and other errors logged by SSSD. | |
| /var/log/boot.log | * This file stores boot-related information and messages logged during the computer startup process. | |
| /var/log/dmesg | | * This directory contains kernel ring buffer messages. * Information related to hardware devices and their drivers is recorded here. * It is very important because, due to their low-level nature, logging systems such as syslog are not running when these events take place and therefore are often unavailable to the administrator in real-time. |
| /var/log/kern.log | * This file contains information logged by the kernel. | |
| /var/log/cron | * Cron is a service used to schedule automated tasks in Linux and this directory stores its events. * Whenever a scheduled task (also called a cron job) runs, all its relevant information including execution status and error messages are stored here. | |
| /var/log/mysqld.log or /var/log/mysql.log | * This is the MySQL log file. * All debug, failure and success messages related to the mysqld process and mysqld\_safe daemon are logged here. * RedHat, CentOS and Fedora Linux distributions store MySQL logs under /var/log/mysqld.log, while Debian and Ubuntu maintain the log in /var/log/mysql.log file. | |

**File Permissions**



**Hard link and soft link**

**Hard link**

A hard link is another file that points to the same location as the original file. Use the command **ln** to create a hard link. The first argument is the existing file and the second argument is the new file. It has same inode (metadata) for both files

Eg: ln name.txt myname.txt

Both files point to the same location in the file system. If you change one file, the other is changed, as well but if you delete one file, the other will still exist.

**Soft Link**

A symbolic link, also called a symlink or soft link, is similar to a hard link in that applying changes to the symbolic link will also change the original file but unlike a hard link, deleting the original text.txt file means that**mytext.txt**is now linked to a file that no longer exists.

Ln -s command is used

It has different inode files for each of them

**X WINDOW**

The graphical interface present in most Linux computers is based on the X Window System. Also known as X or X11. X works as a server which allows a remote user to use the network to connect, start a graphical application, and have the graphical window open on the remote terminal. While the application itself runs on the server, the graphical aspect of it is sent by X over the network and displayed on the remote computer.

It provides the basic framework for building a GUI:

* Drawing windows on screen
* Handling mouse & keyboard input
* Communicating between applications and the display server

[ A window in a GUI = a rectangular area on your screen where an application displays its content.

Drawing a window means:

1. Allocating screen space (deciding *where* on the monitor it goes).
2. Rendering the rectangle (the window background).
3. Displaying borders, title bar, and control buttons (close, minimize, maximize).
4. Updating graphics/text inside the window when the app needs to show something]

X does not specify the user interface, leaving it to other programs, such as window managers, to define all the graphical components. This abstraction allows for great flexibility and customization. Because of this separation, the Linux GUI varies greatly from distribution to distribution.

X window is a backend necessary for employing GUI, X window only offers graphics and input which can be used to create a GUI interface over it. That is why, Varying Linux Distro has different GUI

**LINUX GUI**  
It refers to the user interface Environment that runs above the x window or other similar systems

Examples:

* GNOME
* KDE Plasma
* XFCE
* Cinnamon

These desktop environments provide:

* Window managers (decorations, resizing, tiling)
* Panels/menus
* Icons, themes
* File manager, system settings

**Updates**

Install

* Arch pacman -S
* Debian/ubuntu apt install

Remove

* Arch pacman -Rs
* Debian/ubuntu apt remove

Update local Package

* Arch pacman -Syy
* Debian/ubuntu apt-get update

Upgrade all Packages

* Arch pacman -Syu
* Debian/ubuntu apt-get upgrade

**Forking**

Forking is used to make multitasking in Linux systems and is the act of a process creating a copy of itself.

The fork () system call is used by a process (called the parent) to create a new process (called the child).

the child process is an almost identical copy of the parent:

* Same code
* Same data (at the time of fork)
* Same open file descriptors
* child has a different Process ID (PID).

**Manage Process**

ps – print the current state of running processes and its details

top – print the running processes details and updates in every 3 seconds with another output

kill – used to remove, restart or pause a process

**Detect Rootkits**

chkrootkitis a popular Linux-based program designed to check the computer for known rootkits. It is a shell script that uses common Linux tools such as **s**tringsand grep to compare the signatures of core programs. It also looks for discrepancies as it traverses the /proc file system comparing the signatures found there with the output ofps**.**

[/proc is a **virtual filesystem** created by the Linux kernel.

It does not exist on disk → it’s generated dynamically in memory.

Provides a **view into the kernel and processes** (process info, hardware info, system configuration).]

**Tokenization**

In data security, tokenization = replacing sensitive data with a random token (non-sensitive substitute).

The original data is stored securely in a vault, and only the token is exposed.

Common in payment systems:

* Your 16-digit credit card number 1234-5678-9012-3456
* becomes a token like A9FJ-82KD-LQ77-PZ88.

If leaked, the token is useless without the secure vault.

**NETWORK DEFENCE**

* 1. **DEFENCE-IN-DEPTH APPROACH**

Organizations must use a defence-in-depth approach to identify threats and secure vulnerable assets. This approach uses multiple layers of security at the network edge, within the network, and on network endpoints.

Defence in Depth approach examples

* **Security Onion**

a threat actor would have to peel away at a network defences layer by layer in a manner similar to peeling an onion. Only after penetrating each layer would the threat actor reach the target data or system.

* **Security Artichoke**

threat actors no longer have to peel away each layer. They only need to remove certain “artichoke leaves.” The bonus is that each “leaf” of the network may reveal sensitive data that is not well secured which can be used to find a path to the core,

**Business Policies**

Business policies are the guidelines that are developed by an organization to govern its actions. The policies define standards of correct behaviour for the business and its employees. In networking, policies define the activities that are allowed on the network. This sets a baseline of acceptable use. If behaviour that violates business policy is detected on the network, it is possible that a security breach has occurred.

Main Business Policies are as follows

* Company Policy
* Employee Policy
* Security Policy

**Tor**

Tor is a software platform and network of P2P hosts that function as internet routers on the Tor network. The Tor network allows users to browse the internet anonymously. Users access the Tor network by using a special browser. When a browsing session is begun, the browser constructs a layered end-to-end path across the Tor server network that is encrypted, as shown in the figure. Each encrypted layer is “peeled away” like the layers of an onion (hence “onion routing”) as the traffic traverses a Tor relay. The layers contain encrypted next-hop information that can only be read by the router that needs to read the information. In this way, no single device knows the entire path to the destination, and routing information is readable only by the device that requires it. Finally, at the end of the Tor path, the traffic reaches its internet destination. When traffic is returned to the source, an encrypted layered path is again constructed.

* 1. **SECURITY PRACTICES**

**Biometric Security Errors**

The Type I errors or false rejections. A Type I error rejects a person that registers and is an authorized user.

Type II errors allow entry to people who should not have entry, meaning a cybercriminal can potentially gain access.

**Secure Coding Practice**

**Normalization**

In secure coding, normalization means converting input data into a consistent, standard format before processing or validating it. This prevents attackers from exploiting variations in how data can be represented.

**Stored procedure**

A stored procedure is a group of precompiled SQL statements stored in a database that execute a task. If you use a stored procedure to accept input parameters from clients using different input data, you will reduce network traffic and get faster results.

**Obfuscation**

Obfuscation hides original data with random characters or data. Camouflage replaces sensitive data with realistic fictional data.

**validation rule**

validation rule checks that data falls within the parameters defined by the database designer.

* Size – checks the number of characters in a data item
* Format – checks that the data conforms to a specified format
* Consistency – checks for the consistency of codes in related data items
* Range – checks that data lies within a minimum and maximum value
* Check digit – provides for an extra calculation to generate a check digit for error detection

**Secure copy Protocol (SCP)**

Secure copy Protocol (SCP)securely transfers files between two remote systems. SCP uses SSH for data transfer and authentication, ensuring the authenticity and confidentiality of the data in transit.

**VLAN AND TRUNKS**

VLANs provide a way to group devices within a local area network (LAN) and on individual switches. VLANs are not the same as LANs: virtual LANs are based on logical connections, while LANs are based on physical connections. Individual ports on a switch can be assigned to a specific VLAN. Other ports can be used to physically interconnect switches and allow multiple VLAN traffic between switches. These ports are called trunks.

**Spanning Tree Protocol (STP)**

The Spanning Tree Protocol (STP)’s basic function is to prevent loops on a network when switches interconnect via multiple paths (even though multiple paths is present between one device and another, sending packets in multiple paths will cause a loop). STP ensures that redundant physical links are loop-free and only one logical path runs between all destinations on the network. To do this, STP intentionally blocks redundant paths that could cause a loop.

Blocking the redundant paths is critical to preventing loops on the network. The physical paths still exist to provide redundancy, but STP disables these paths to prevent the loops from occurring. If a network cable or switch fails, STP recalculates the paths and unblocks the necessary ports to allow the redundant path to become active.

**First Hop Redundancy**

Having Multiple Default Gateway to make sure that when one fails, another default gateway can take over to do its job

**Location redundancy**

Location redundancy means having critical IT systems, services, or data replicated across multiple physical locations so that if one site fails, the other can continue operations.

* Synchronous Replication

Synchronizes both locations in real time so it requires high bandwidth and locations must be close together to reduce latency

* Asynchronous Replication

Not synchronized in real time but close to it. It requires less bandwidth and Sites can be further apart because latency is less of an issue

* Point in Time Replication

Updates the backup data location periodically, at certain points in time. More bandwidth conservative because it does not require a constant connection

**Application resilience**

Application resilience is an application’s ability to react to component problems while still functioning. Application errors or infrastructure failures can cause downtime, but an administrator will eventually need to shut down applications for patching, version upgrades, or to deploy new features.

* Fault tolerant hardware**:** A system designed by building multiples of all critical components into the same computer.
* Cluster architecture**:** A group of servers acting like a single system.
* Backup and restore**:** Copying files for the purpose of being able to restore them if data loss occurs.

**Power Excess**

* Spike: momentary high voltage.
* Surge: prolonged high voltage.

**Power Loss**

* Fault: momentary loss of power.
* Blackout: complete loss of power.

**Power Degradation**

* Sag/dip: momentary low voltage.
* Brownout: prolonged low voltage.
* Inrush current: initial surge of power.

**Heating, Ventilation and Air Conditioning (HAVC)**

HVAC systems are critical to the safety of people and information systems in an organization's facilities. When designing modern IT facilities, these systems play a very important role in the overall stability and security.

* 1. **NETWORK SYSTEMS**

**Embedded system**

An embedded system is a special-purpose computer system designed to perform dedicated functions within a larger system. Unlike general-purpose computers, they are optimized for specific tasks, often with real-time performance and limited resources.

* Eg: Microwave Oven - Embedded chip controls heating time and power.
* Embedded system is like the tiny computer inside a washing machine or microwave that makes it "smart" enough to do its specific job.

They are susceptible to timing attacks, whereby attackers discover vulnerabilities by studying how long it takes the system to respond to different inputs. A timing attack is considered a side-channel attack.

This type of attack is based on information gained from the implementation of a system, rather than on weaknesses in the software. Timing information, power consumption, electromagnetic leaks or even sound can be that source of information.

**Real-Time Operating System (RTOS)**

A Real-Time Operating System (RTOS) is an operating system that runs tasks and responds to events within a fixed and guaranteed time. An RTOS is like a controller for tasks — it makes sure the most urgent task (like an airbag opening or a robot stopping) happens exactly when needed.

**DNS Sinkhole**

A DNS Sinkhole is a security technique where fake or controlled DNS servers are used to redirect malicious domain requests away from attackers’ servers and instead send them to a safe server (the “sinkhole”).

Eg:

* Malware on a computer tries to connect to badwebsite.com (attacker’s server).
* Instead of reaching the attacker, the DNS sinkhole redirects badwebsite.com to a safe IP (like a security server or 127.0.0.1).
* The malware fails to communicate, and security teams can monitor or block it.
  1. **ACCESS CONTROL**

**Single Sign-On (SSO)**

* Definition: A system that lets a user log in once and access multiple applications/services within the same organization without logging in again.
* Scope: Usually internal (inside one company or organization).
* Example: You log in once to your company portal → then access email, HR system, and intranet without logging in again.

**Federated Identity Management (FIM)**

* Definition: An identity management system that allows a user’s login credentials from one organization to be used to access resources in another organization (trust relationship).
* Scope: Cross-organization / cross-domain.
* Example: You use your Google account to log in to Spotify, Zoom, or third-party apps.

**Knowledge-Based Authentication (KBA)**

Knowledge-Based Authentication (KBA) to provide a password reset should a user forget their password. KBA is based on personal information known by the user or a series of questions.

**Hash-Based Message Authentication Code (HMAC)**

An HMAC is a security mechanism that combines a cryptographic hash function (like SHA-256) with a secret key to create a message authentication code (MAC).

**Steps in HMAC**

1. Choose a hash function (e.g., SHA-256).
2. Share a secret key between sender and receiver.
3. Sender generates HMAC:
   * Combine the message with the secret key in a specific way.
   * Pass it through the hash function.
   * Produce an HMAC value (a fixed-length tag).
4. Send message + HMAC to receiver.
5. Receiver recomputes HMAC using the same message + secret key.
6. Compare values:
   * If both HMACs match → message is authentic and unchanged.
   * If not → message was altered or sender is not trusted.

**DAC – Discretionary Access Control**

* Definition: The data owner decides who gets access.
* Example: A file owner on Windows gives read/write permission to specific users.

**MAC – Mandatory Access Control**

* Definition: Access is decided by the system or security policy, not the user.
* Example: Military system – users with “Top Secret” clearance can access only matching classified documents.

**ABAC – Attribute-Based Access Control**

* Definition: Access is based on attributes of user, resource, and environment.
* Example: A doctor can access patient records only if (role = doctor) AND (location = hospital network) AND (time = working hours).

**TAC**

* **Task-Based Access Control**
* Definition: Access is given based on tasks assigned to a user, not just role or identity.
* Example: In a workflow system, a user can access a purchase order only while reviewing/approving it.
* **Time-Based Access Control**
* Time-Based Access Control is a security method where user access to resources is allowed or denied depending on specific time conditions (such as hours, days, or dates).
* An employee can log in to the office VPN only between 9:00 AM – 6:00 PM

**RBAC**

* **Role-Based RBAC**:
  + Access depends on user’s role in the organization.
  + Also known as Non-Discretionary Access Control
  + Example: HR staff can access employee data; Finance role can access payroll.
* **Rule-Based RBAC**:
* Network security staff specify sets of rules regarding or conditions that are associated with access to data or systems.
* These rules may specify permitted or denied IP addresses, or certain protocols and other conditions.
* Example: A system admin role can access servers, but only during office hours.

**NAC**

Network access control (NAC) systems support access management by enforcing organizational policies regarding the people and devices that are attempting to access the network. NAC systems allow cybersecurity professionals to monitor the users and devices that are attached to the network, and manually control access

**ACCESS CONTROL LIST**

Access control Entries or Access control Statements are used to create an Access control Lists. By default, a router does not have any ACLs configured. When ACL is configured in an interface, Routers controls the traffic based on ACL even though it normally doesn’t work that way

The last ACE statement of an ACL is always an implicit deny that blocks all traffic. By default, this statement is automatically implied at the end of an ACL even though it is hidden and not displayed in the configuration.

An ACL must have at least one permit statement otherwise all traffic will be denied due to the implicit deny ACE statement.

Wildcard Mask is used to specify a host, Network or range of networks which should be allowed or denied access

**Numbered ACL**

1 to 99, 1300 to 1999 = Standard

100 to 199, 2000 to 2699 = Extended

Standard: filters source Ip only

Extended: filters by

Source IP

Destination IP

Protocol (IP, TCP, UDP, ICMP, etc.)

Port number)

**Named ACL**

Named ACL uses names instead of numbers. It also offers standard and extended ACL

Assign a name to identify the purpose of the ACL.

Names can contain alphanumeric characters.

Names cannot contain spaces or punctuation.

It is suggested that the name be written in CAPITAL LETTERS.

Entries can be added or deleted within the ACL.

To create

Router(config)# **ip access-list standard** *access-list-name*

To remove

Router(config)# **no** **ip access-list standard** *access-list-name*

**Numbered Standard IPv4 ACL Syntax**

To create

Router(config)# **access-list** *access-list-number* {**deny** | **permit** | **remark** *text*} *source* [*source-wildcard*] [**log**]

To remove

Router(config)# **no access-list** *access-list-number*

|  |  |
| --- | --- |
| **Parameter** | **Description** |
| **access-list-number** | * This is the decimal number of the ACL. * Standard ACL number range is 1 to 99 or 1300 to 1999. |
| **deny** | This denies access if the condition is matched. |
| **permit** | This permits access if the condition is matched. |
| **remark text** | * (Optional) This adds a text entry for documentation purposes. * Remarks are extremely useful, especially in longer or more complex ACLs. * Each remark is limited to 100 characters. |
| **source** | * This identifies the source network or host address to filter. * Use the **any** keyword to specify all networks. * Use the **host***ip-address*keyword or simply enter an*Ip-address*(without the **host** keyword) to identify a specific IP address. |
| **source-wildcard** | (Optional) This is a 32-bit wildcard mask that is applied to the source. If omitted, a default 0.0.0.0 mask is assumed. |
| **log** | * (Optional) This keyword generates an informational message whenever the ACE is matched. * Message includes ACL number, matched condition (i.e., permitted or denied), source address, and number of packets. * This message is generated for the first matched packet. * Unfortunately, ACL logging can be CPU intensive and can negatively affect other functions therefore it should only be implemented for troubleshooting or security reasons. |

**Numbered Extended IPv4 ACL Syntax**

Extended will have all the features included in standard table along with destination IP, Protocols, Port, established section (for tcp)

Established is used to create a tcp connection to send traffic from inside network to outside and vive versa. This allows to receive tcp reply for already made requests and deny new tcp connections m,ade from outer networks to inside.

**Named Extended IPv4 ACL Syntax**

* SURFING - This will permit inside HTTP and HTTPS traffic to exit to the internet.
* BROWSING - This will only permit returning web traffic to the inside hosts while all other traffic exiting the R1 G0/0/0 interface is implicitly denied.

**Sequence numbers**

An ACL ACE can also be deleted or added using the ACL sequence numbers. Sequence numbers are automatically assigned when an ACE is entered. These numbers are listed in the **show access-lists**command.

* 1. **WILDCARD MASK**

**Calculation**

Wildcard Mask is used to specify a host, Network or range of networks which should be allowed or denied access in Access Control List (ACL)

To calculate:

255.255.255.255 – subnet Mask = Wildcard Mask

Eg:

**/24** → mask 255.255.255.0 → wildcard **0.0.0.255**

**/26** → mask 255.255.255.192 → wildcard **0.0.0.63**

**/16** → mask 255.255.0.0 → wildcard **0.0.255.255**

**WILDCARD MASK – Opp to Subnet Mask**

When you have an IP with a Wildcard Mask, it can be used to find the range of network

1. Bitwise Comparison: When a wildcard mask is applied to an IP address, each bit in the mask is compared with the corresponding bit in the IP address.

2. Matching: "0" in the wildcard mask means the IP address bit must be identical to the bit in the rule or policy. "1" in the wildcard mask means the IP address bit can be either a 0 or a 1.

Example:

Consider the IP address 192.168.1.0 with a wildcard mask of 0.0.0.255.

The wildcard mask "0.0.0.255" indicates that the first three octets (192.168.1) must match exactly, while the last octet (0) can be any value.

This means the rule or policy will apply to the entire subnet 192.168.1.0/24 (192.168.1.0 to 192.168.1.255)

**Bitwise Meaning:**

* 0.0.0 → The first three octets (**192.168.1**) must match exactly.
* .255 (binary 11111111) → The last octet can be any value from **0 to 255** so this represents the entire /24 network
* 0.0.0.0 specifies a single host (Eg: 192.168.1.1 with 0.0.0.0 wildcard mask represents only that host
* 255.255.255.255 represents all hosts

**ROUTE SUMMARIZATION / SUPERNETTING**

This is used to combine subnets or range of Ips to single IP with a mask so a wildcard mask can be created

**COMBINE SUBNETS**

Step 1: Write the Networks in Binary

* 192.168.10.0 → 11000000.10101000.00001010.00000000
* 192.168.11.0 → 11000000.10101000.00001011.00000000

Step 2: Compare Bit by Bit

* Up to the 23rd bit, both networks are identical.
* The difference starts at the 24th bit (the last octet’s first bit).

So:

* Common prefix = 23 bits
* That means subnet mask = /23 = 255.255.254.0

Step 3: What Does /23 Cover?

* /23 = 512 addresses (2 subnets of /24)
* Range: 192.168.10.0 – 192.168.11.255
* Which includes:
  + 192.168.10.0/24 to 192.168.11.0/24

**RANGE OF IPs TO SINGLE IP WITH A MASK SO A WILDCARD MASK CAN BE CREATED**

192.168.16.0/24 to 192.168.31.0/24

* Third octet in binary:
  + 16 = 00010000
  + 31 = 00011111
* The first 4 bits of the third octet are identical (0001).
* So, network prefix = 16 bits (192.168) + 4 bits = 20 bits → 192.168.16.0/20.

**Subnet mask and wildcard**

* /20 subnet mask = 255.255.240.0
* Wildcard = 255.255.255.255 - 255.255.240.0 = 0.0.15.255
  1. **ZONE BASED FIREWAL**

**Zone-Based Firewall (ZBFW) configuration**

**Step 1: Create Zones**

A zone is like a security area.

You usually make at least 3 zones:

INSIDE → Your internal network (LAN).

OUTSIDE → The Internet (WAN).

DMZ → Servers that outsiders may access (like a webserver).

Example commands:

zone security INSIDE

zone security OUTSIDE

zone security DMZ

**Step 2: Assign Interfaces to Zones**

Every interface (router port) must belong to a zone.

If an interface is not in any zone, traffic through it is dropped.

Example:

interface g0/0

ip address 192.168.1.1 255.255.255.0

zone-member security INSIDE

interface g0/1

ip address 203.0.113.2 255.255.255.0

zone-member security OUTSIDE

interface g0/2

ip address 10.0.0.1 255.255.255.0

zone-member security DMZ

**Step 3: Create ACLs (Access Control Lists)**

ACLs define what traffic should be matched.

Example 1: Allow inside LAN to go anywhere.

ip access-list extended INSIDE\_TO\_OUT

permit ip 192.168.1.0 0.0.0.255 any

Example 2: Allow Internet users to access only HTTP/HTTPS on DMZ server (10.0.0.10).

ip access-list extended OUT\_TO\_DMZ

permit tcp any host 10.0.0.10 eq 80

permit tcp any host 10.0.0.10 eq 443

**Step 4: Create Class-Maps**

A class-map tells the firewall: “Watch for traffic that matches this ACL.”

Example:

class-map type inspect CM\_INSIDE\_TO\_OUT

match access-group name INSIDE\_TO\_OUT

class-map type inspect CM\_OUT\_TO\_DMZ

match access-group name OUT\_TO\_DMZ

**Step 5: Create Policy-Maps**

A policy-map tells the firewall what action to take for the matched traffic.

Actions are:

inspect → Allow + keep track of connection (stateful).

pass → Allow one-way only, no state.

drop → Block traffic.

Example:

policy-map type inspect PM\_INSIDE\_TO\_OUT

class type inspect CM\_INSIDE\_TO\_OUT

inspect

class class-default

drop

policy-map type inspect PM\_OUT\_TO\_DMZ

class type inspect CM\_OUT\_TO\_DMZ

inspect

class class-default

drop

**Step 6: Create Zone-Pairs**

A zone-pair connects one zone to another in a specific direction.

You must apply the policy-map to the zone-pair.

Example:

zone-pair security ZP\_IN\_TO\_OUT source INSIDE destination OUTSIDE

service-policy type inspect PM\_INSIDE\_TO\_OUT

zone-pair security ZP\_OUT\_TO\_DMZ source OUTSIDE destination DMZ

service-policy type inspect PM\_OUT\_TO\_DMZ

**Step 7: Configure SELF Zone (Optional)**

The router itself also needs access sometimes (ping Internet, allow SSH).

For this, use the SELF zone.

Example:

zone security SELF

ip access-list extended SELF\_TO\_OUT

permit icmp host 203.0.113.2 any

permit tcp any eq 22

class-map type inspect CM\_SELF\_TO\_OUT

match access-group name SELF\_TO\_OUT

policy-map type inspect PM\_SELF\_TO\_OUT

class type inspect CM\_SELF\_TO\_OUT

inspect

class class-default

pass

zone-pair security ZP\_SELF\_TO\_OUT source SELF destination OUTSIDE

service-policy type inspect PM\_SELF\_TO\_OUT

**Step 8: Default Behavior**

By default, traffic between zones is blocked unless you make a zone-pair with a policy.

Example: If you don’t create an OUTSIDE → INSIDE policy, nobody from the Internet can directly reach your LAN.

**Step 9: Verification Commands**

To check your setup, use:

show zone security → Lists zones and members.

show zone-pair security → Shows connections between zones.

show policy-map type inspect → Displays policies and actions.

show policy-map type inspect zone-pair ZP\_IN\_TO\_OUT sessions → Shows active connections being tracked.

* 1. **CLOUD COMPUTING**

**Virtual Machine**

VM includes the entire Operating systems, its default applications, settings and configurations creating a isolated system from host OS

**Containers**

Containers can be used in specific applications that can run and manage containers. Containers only have specific applications and their dependencies offering a isolated environment for those applications but different applications in different containers share the same underlying OS Kernel.

**SECURITY GUIDANCE FOR CRITICAL AREAS OF FOCUS IN CLOUD COMPUTING V4 DOCUMENT**

Developed by the Cloud Security Alliance (CSA). it promotes best practices to provide security assurance within the cloud computing domains. Specifically, the document covers 14 domains of cloud security.

* Cloud Computing Concept and architecture

The domain defines cloud computing terminology and details the overall logical and architectural frameworks used

* Governance and Enterprise Risk Management

The domain describes four areas impacted by cloud computing:

* Governance
* Enterprise Risk Management
* Information Risk Management
* Information Security
* Legal Issues, Contracts and Electronic Discovery

The domain describes legal issues associated with cloud computing including the moving of data to the cloud, contracting with cloud service providers, and handling electronic discovery requests in litigation.

* Compliance and Audit Management

The domain describes challenges of delivering, measuring, and communicating compliances when organizations migrate from traditional data centers to the cloud.

* Information Governance

The domain describes the need to ensure that the use of data and information complies with organizational policies, standards, and strategy including regulatory, contractual, and business objectives.

* Management Plane and Business Continuity

The domain describes the need to secure the cloud computing management plane (i.e., the protocols and resources used to manage the cloud). It also describes business continuity and disaster recovery procedures to be used by the cloud provider and the cloud client.

* Security as a Service

The domain covers the continually evolving security services delivered from the cloud.

* Infrastructure Security

The domain describes cloud-specific aspects of infrastructure security and the foundation for operating securely in the cloud.

* Virtualization and Containers

The domain describes the need to secure the virtualization technology and virtual assets which are the foundation for cloud computing.

* Incident Response

The domain describes the critical aspects of incident response (IR) including the Incident Response Lifecycle and considerations for responders as they work in a cloud environment.

* Application Security

The domain provides guidance on how to securely build and deploy applications in cloud computing environments, specifically for PaaS and IaaS.

* Data Security and Encryption

Data Security should be risk-based since it is not appropriate to secure everything equally. The domain describes those controls related to securing the data itself, of which encryption is one of the most important.

* Identity, Entitlement, and Access Management (IAM)

The domain describes how cloud identity is different than traditional identity management.

* Related Technologies

The domain provides background and recommendations for technologies that rely nearly exclusively on cloud computing to operate and for technologies that do not necessarily rely on cloud but are commonly seen in cloud deployments.

**Microsegmentation**

Microsegmentation is the practice of dividing a network (or data center) into very small, granular segments and applying security policies individually to each segment, workload, or even application. Instead of just securing the perimeter (firewall at the network edge), microsegmentation enforces security inside the network between workloads.

* 1. **CRYPTOGRAPHY**

**CRYPTOGRAPHICALLY SECURE PSEUDO-RANDOM NUMBER GENERATOR (CSPRNG)**

It is used to create salting for hashing. CSPRNGs generate a random number that has a high level of randomness and is completely unpredictable, so it is cryptographically secure.

**Key Stretching**

Key Stretching is a technique used to make a weak key (like a password) stronger and harder to brute-force by attackers.

* It takes a password (which might be short or simple)
* Runs it through a computationally expensive algorithm many times
* Produces a derived cryptographic key

Eg:

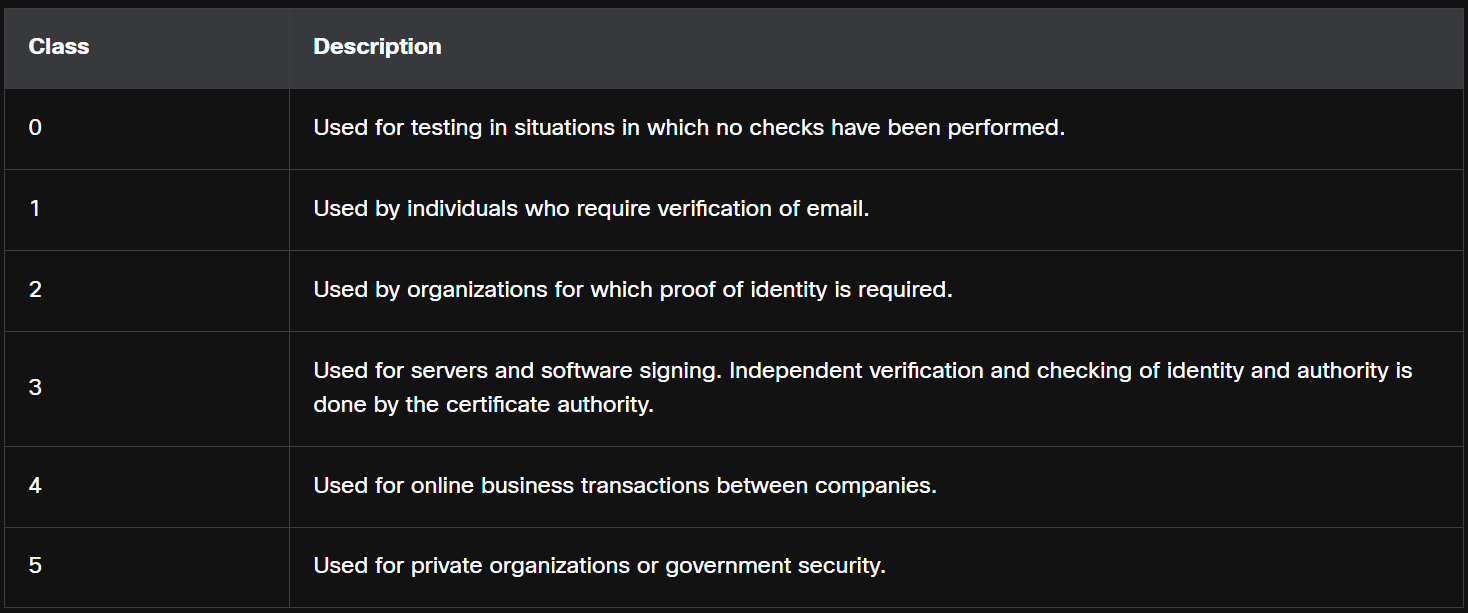
This way, even if the password is weak, it becomes much harder to crack because each guess takes more time.

imagine locking a box with a simple lock (weak password).

Key stretching = adding 100 extra locks on top of it.

Now, even if someone knows the weak lock, they must open all extra locks → takes much longer.

* 1. **DIGITAL CERTIFICATE**

**Classes**

Certifying Authority (CA) Provides digital Certificate to websites, companies and son on. These certificates are offered in different classes based on the amount of verification and checks happened before offering certificates

**single-root PKI topology**

A single CA, called the root CA, issues all the certificates to the end users, which are usually within the same organization. It is difficult to scale to a large environment because it requires a strictly centralized administration, which creates a single point of failure.

**Cross-certified CA topologies**

this is a peer-to-peer model in which individual CAs establish trust relationships with other CAs by cross-certifying CA certificates. Users in either CA domain are also assured that they can trust each other. This provides redundancy and eliminates the single-point of failure.

**Hierarchical CA**

the highest-level CA is called the root CA. It can issue certificates to end users and to a subordinate CA. The sub-CAs could be created to support various business units, domains, or communities of trust. The root CA maintains the established “community of trust” by ensuring that each entity in the hierarchy conforms to a minimum set of practices. The benefits of this topology include increased scalability and manageability. This topology works well in most large organizations.

**Framework**

IETF published the Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework (RFC 2527). The X.509 version 3 (X.509 v3) standard defines the format of a digital certificate.

**CA Authentication**

CA authentication procedure is to securely obtain a copy of the CA’s public key. All systems that leverage the PKI must have the CA’s public key, which is called the self-signed certificate. The CA public key verifies all the certificates issued by the CA and is vital for the proper operation of the PKI.

For many systems such as web browsers, the distribution of CA certificates is handled automatically. The web browser comes pre-installed with a set of public CA root certificates. Organizations and their website domains push their public certificates to website visitors. CAs and certificate domain registrars create and distribute private and public certificates to clients that purchase certificates.

**Certificate Revocation**

Certificates must sometimes be revoked. For example, a digital certificate can be revoked if key is compromised or if it is no longer needed.

Certificate Revocation list

A list of revoked certificate serial numbers that have been invalidated because they expired. PKI entities regularly poll the CRL repository to receive the current CRL.

Online Certificate Status Protocol (OCSP)

An internet protocol used to query an OCSP server for the revocation status of an X.509 digital certificate. Revocation information is immediately pushed to an online database.

**Certificate Enrollment**

Certificate Enrollment is the process of a device, user, or server requesting and obtaining a digital certificate from a CA within a PKI (Public Key Infrastructure).

That certificate proves the identity of the entity and provides a public key that others can trust.

**Steps**

1. Key Pair Generation
   * The device/user/application generates a public-private key pair.
   * The private key stays secret.
   * The public key will go into the certificate.
2. Certificate Signing Request (CSR)
   * Device/user/application creates a CSR containing:
     + Public key
     + Identifying info (CN, org, domain name, etc.)
   * Signed with the private key to prove ownership.
3. Submit CSR to CA
   * CSR is sent to the CA for validation.
4. Identity Verification
   * CA verifies the requester’s identity (this depends on certificate type: DV, OV, EV).
5. Certificate Issuance
   * CA signs the CSR with its private key, creating a digital certificate.
   * This certificate now binds the requester’s identity + public key.
6. Installation
   * The issued certificate is installed on the system (web server, client, router, etc.).
   * Now others can trust it because they trust the CA’s root certificate.
   1. **DATA FOR MONITORING**

**Alert data**

Alert data consists of messages generated by intrusion prevention systems (IPSs) or intrusion detection systems (IDSs) in response to traffic that violates a rule or matches the signature of a known exploit. A network IDS (NIDS), such as Snort, comes configured with rules for known exploits. Alerts are generated by Snort and are made readable and searchable by the Sguil and Squert applications, which are part of the Security Onion suite of NSM(Network Security Management) tools.

A testing site that is used to determine if Snort is operating is the tesmyids site. Search for it on the internet. It consists of a single webpage that displays only the following text uid=0(root) gid=0(root) groups=0(root). If Snort is operating correctly and a host visits this site, a signature will be matched and an alert will be triggered. This is an easy and harmless way to verify that the NIDS is running.

**Session and Transaction Data**

1. ts: session start timestamp
2. uid: unique session ID
3. id.orig\_h: IP address of host that originated the session (source address)
4. id.orig\_p: protocol port for the originating host (source port)
5. id.resp\_h: IP address of host responding to the originating host (destination address)
6. id.resp\_p: protocol of responding host (destination port)
7. proto: transport layer protocol for session
8. service: application layer protocol
9. duration: duration of the session
10. orig\_bytes: bytes from originating host
11. resp\_bytes: bytes from responding host
12. orig\_packets: packets from the originating host
13. resp\_packets: packets from responding host

**Session Data - Partial Contents**

Session data is a record of a conversation between two network endpoints, which are often a client and a server. The server could be inside the enterprise network or at a location accessed over the internet. Session data is data about the session, not the data retrieved and used by the client. Session data will include identifying information such as the five tuples of source and destination IP addresses, source and destination port numbers, and the IP code for the protocol in use. Data about the session typically includes a session ID, the amount of data transferred by source and destination, and information related to the duration of the session.

Zeek, formerly Bro, is a network security monitoring tool used for session data

**Transaction Data**

Transaction data consists of the messages that are exchanged during network sessions. These transactions can be viewed in packet capture transcripts. Device logs kept by servers also contain information about the transactions that occur between clients and servers. For example, a session might include the downloading of content from a webserver. The transactions that represent the requests and replies would be logged in an access log on the server or by a NIDS. The session is all traffic involved in making up the request, the transaction is the request itself.

**Statistical Data**

Statistical characteristics of normal network behavior can be compared to current network traffic in an effort to detect anomalies. Statistics can be used to characterize normal amounts of variation in network traffic patterns in order to identify network conditions that are significantly outside of those ranges. Statistically significant differences should raise alarms and prompt investigation.

Network Behavior Analysis (NBA) and Network Behavior Anomaly Detection (NBAD) are approaches to network security monitoring that use advanced analytical techniques to analyse NetFlow or Internet Protocol Flow Information Export (IPFIX) network telemetry data. Techniques such as predictive analytics and artificial intelligence perform advanced analyses of detailed session data to detect potential security incidents.

IPFIX is the IETF standard version of Cisco NetFlow version 9.

* 1. **LOGS AND SIEM TOOLS**

**Host Logs**

Host-based intrusion detection systems (HIDS) run on individual hosts. HIDS not only detects intrusions, but in the form of host-based firewalls, can also prevent intrusion. This software creates logs and stores them on the host.

HIDS systems can use agents to submit logs to management servers. OSSEC, a popular open-source HIDS, includes a robust log collection and analysis functionality. Tripwire offers a HIDS for Linux

Microsoft Windows host logs are visible locally through Event Viewer

* Application logs – These contain events logged by various applications.
* System logs – These include events regarding the operation of drivers, processes, and hardware.
* Setup logs – These record information about the installation of software, including Windows updates.
* Security logs – These record events related to security, such as logon attempts and operations related to file or object management and access.
* Command-line logs - Attackers who have gained access to a system, and some types of malwares, execute commands from the command-line interface (CLI) rather than a GUI. Logging command line execution will provide visibility into this type of incident.

On Windows computers, security logging is carried out by the Local Security Authority Subsystem Service (LSASS), which is also responsible for enforcing security policies on a Windows host. LSASS runs as lsass.exe. It is frequently faked by malware. It should be running from the Windows System32 directory. If a file with this name, or a camouflaged name, such as 1sass.exe, is running or running from another directory, it could be malware.

|  |  |
| --- | --- |
| Error | indicates a significant problem such as loss of data or loss of functionality |
| Warning | not necessarily significant but may indicate a possible future problem |
| Information | An information event describes the successful operation of an application, driver, or service. For example, when a network driver loads successfully, it may be appropriate to log an information event |
| Success Audit | A success audit is an event that records an audited security access attempt that is successful |
| Failure Audit | A failure audit is an event that records an audited security access attempt that fails. |

**Syslog**

Syslog incudes specifications for message formats, a client-server application structure, and network protocol. Many different types of network devices can be configured to use the syslog standard to log events to centralized syslog servers.

The Syslog sender sends a small (less than 1KB) text message to the Syslog receiver. The Syslog receiver is commonly called "syslogd, "Syslog daemon," or "Syslog server." Syslog messages can be sent via UDP (port 514) and/or TCP (typically, port 5000). While there are some exceptions, such as SSL wrappers, this data is typically sent in plaintext over the network.

The full format of a Syslog message that is seen on the network has three distinct parts

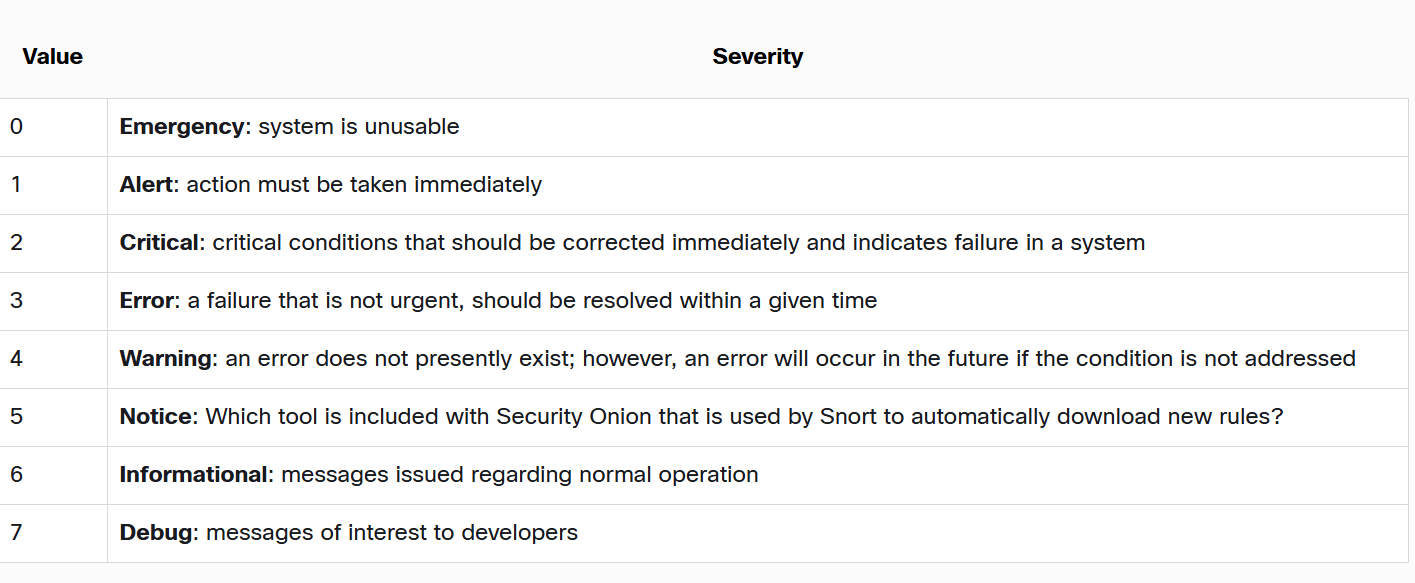
* PRI (priority)
* HEADER
* MSG (message text)

The PRI consists of two elements, the Facility and Severity of the message, which are both integer values. The Facility consists of broad categories of sources that generated the message, such as the system, process, or application. The Facility value can be used by logging servers to direct the message to the appropriate log file. The Severity is a value from 0-7 that defines the severity of the message.

Facility codes between 15 and 23 (local0-local7) are not assigned a keyword or name. They can be assigned to different meanings depending on the use context. Also, various operating systems have been found to utilize both facilities 9 and 15 for clock messages.

Priority = (Facility \* 8) + Severity

The Priority value is the first value in a packet and occurs between angled brackets **<>**.



The HEADER section of the message contains the timestamp in MMM DD HH:MM:SS format. If the timestamp is preceded by the period (.) or asterisk (\*) symbols, a problem is indicated with NTP. The HEADER section also includes the hostname or IP address of the device that is the source of the message.

The MSG portion contains the meaning of the syslog message. This can vary between device manufacturers and can be customized.

**Server Logs**

Network application servers such as email and web servers keep access and error logs. DNS proxy server logs which document all the DNS queries and responses that occur on the network are especially important. DNS proxy logs are useful for identifying hosts that may have visited dangerous websites and for identifying DNS data exfiltration and connections to malware command-and-control servers.

**SECURITY INFORMATION AND EVENT MANAGEMENT (SIEM)**

Security Information and Event Management (SIEM) technology is used in many organizations to provide real-time reporting and long-term analysis of security events

* Log collection – Event records from sources throughout the organization provide important forensic information and help to address compliance reporting requirements.
* Normalization – This maps log messages from different systems into a common data model, enabling the organization to connect and analyse related events, even if they are initially logged in different source formats.
* Correlation – This links logs and events from disparate systems or applications, speeding detection of and reaction to security threats.
* Aggregation – This reduces the volume of event data by consolidating duplicate event records.
* Reporting – This presents the correlated, aggregated event data in real-time monitoring and long-term summaries, including graphical interactive dashboards.
* Compliance – This is reporting to satisfy the requirements of various compliance regulations.

SIEM provides details on the source of suspicious activity, including:

* User information (name, authentication status, location, authorization group, quarantine status)
* Device information (manufacturer, model, OS version, MAC address, network connection method, location)
* Posture information (device compliance with corporate security policy, antivirus version, OS patches, compliance with mobile device management policy)

**SECURITY ORCHESTRATION, AUTOMATION, AND RESPONSE (SOAR)**

SOAR is a security approach (and set of tools) that helps organizations:

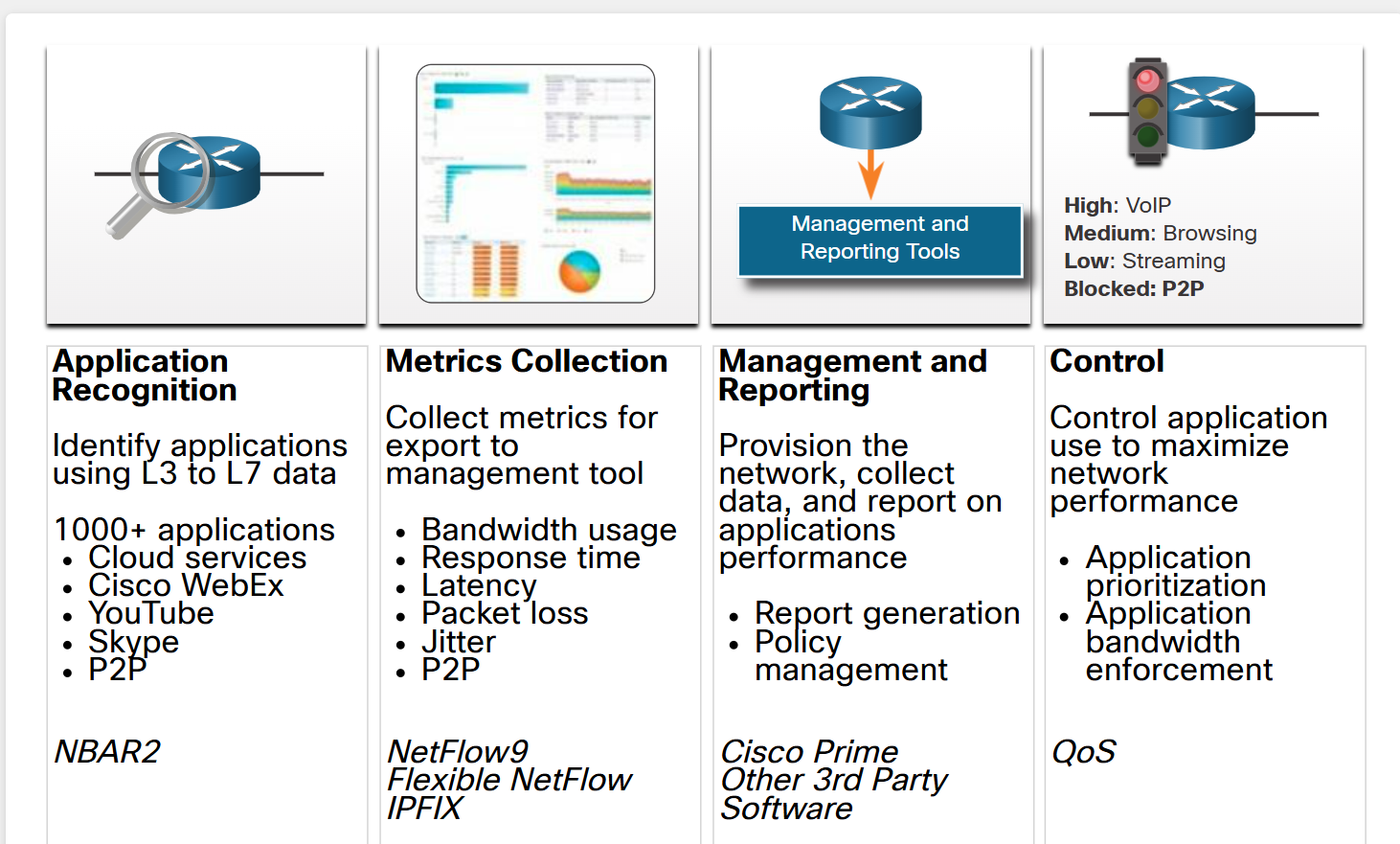
1. Orchestrate – Connect and coordinate different security tools and processes.
2. Automate – Perform repetitive tasks without human effort (like blocking an IP, quarantining a file).
3. Respond – Take faster, consistent, and more effective actions against threats.

SOAR ties together your SIEM, firewalls, threat intel, and other security systems.

**Application Visibility and Control**

The Cisco Application Visibility and Control (AVC) system, combines multiple technologies to recognize, analyse, and control over 1000 applications. These include voice and video, email, file sharing, gaming, peer-to-peer (P2P), and cloud-based applications. AVC uses Cisco next-generation network-based application recognition version 2 (NBAR2), also known as Next-Generation NBAR, to discover and classify the applications in use on the network. The NBAR2 application recognition engine supports over 1000 network applications.

Identification of network applications by port provides very little granularity and visibility into user behaviour. However, application visibility through the identification of application signatures identifies what users are doing, whether it be teleconferencing or downloading movies to their phones.



**Proxy Logs**

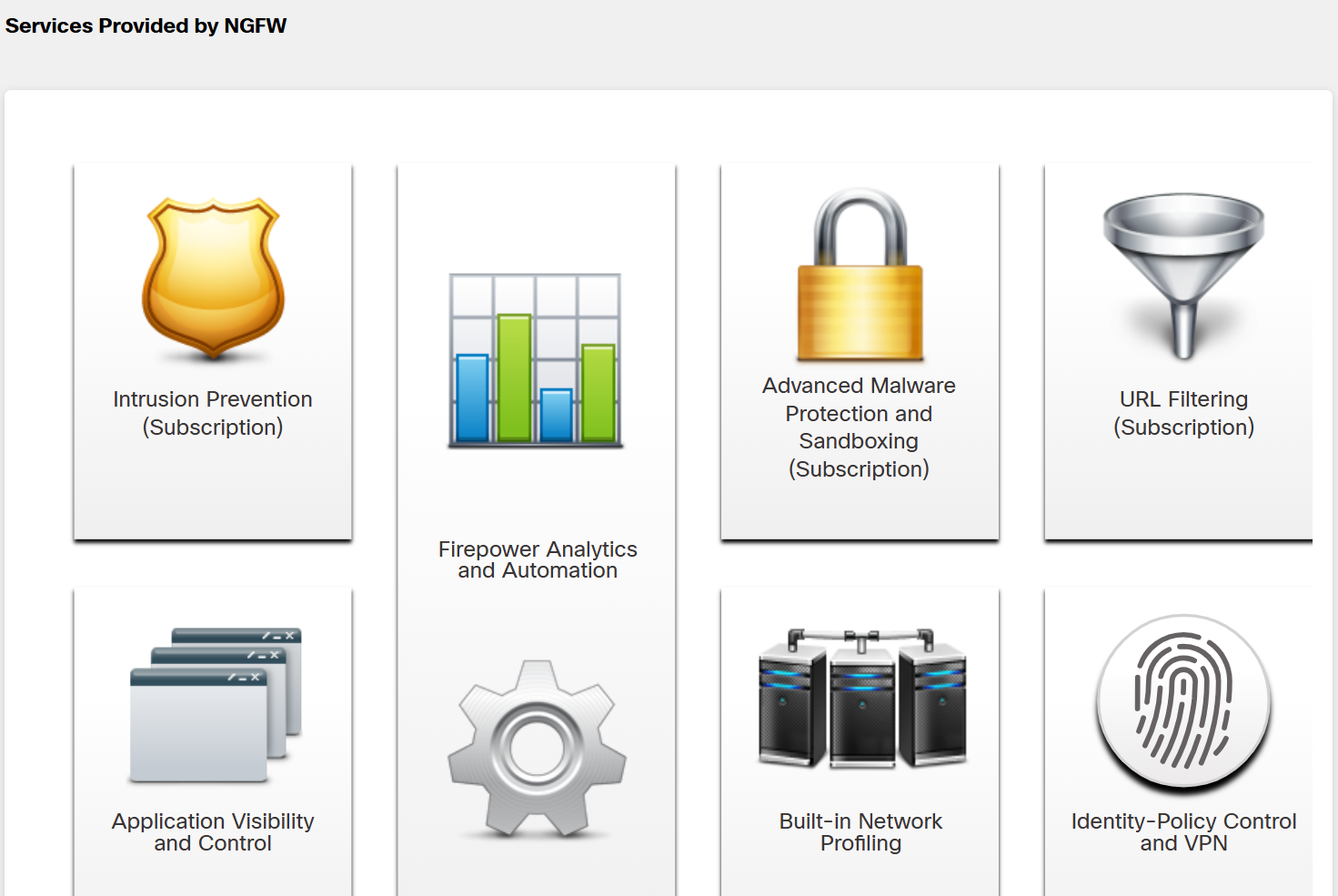
Proxy servers are devices that act as intermediaries for network clients. The proxy server generates logs of all requests and responses. These logs can then be analysed to determine which hosts are making the requests, whether the destinations are safe or potentially malicious, and to also gain insights into the kind of resources that have been downloaded.

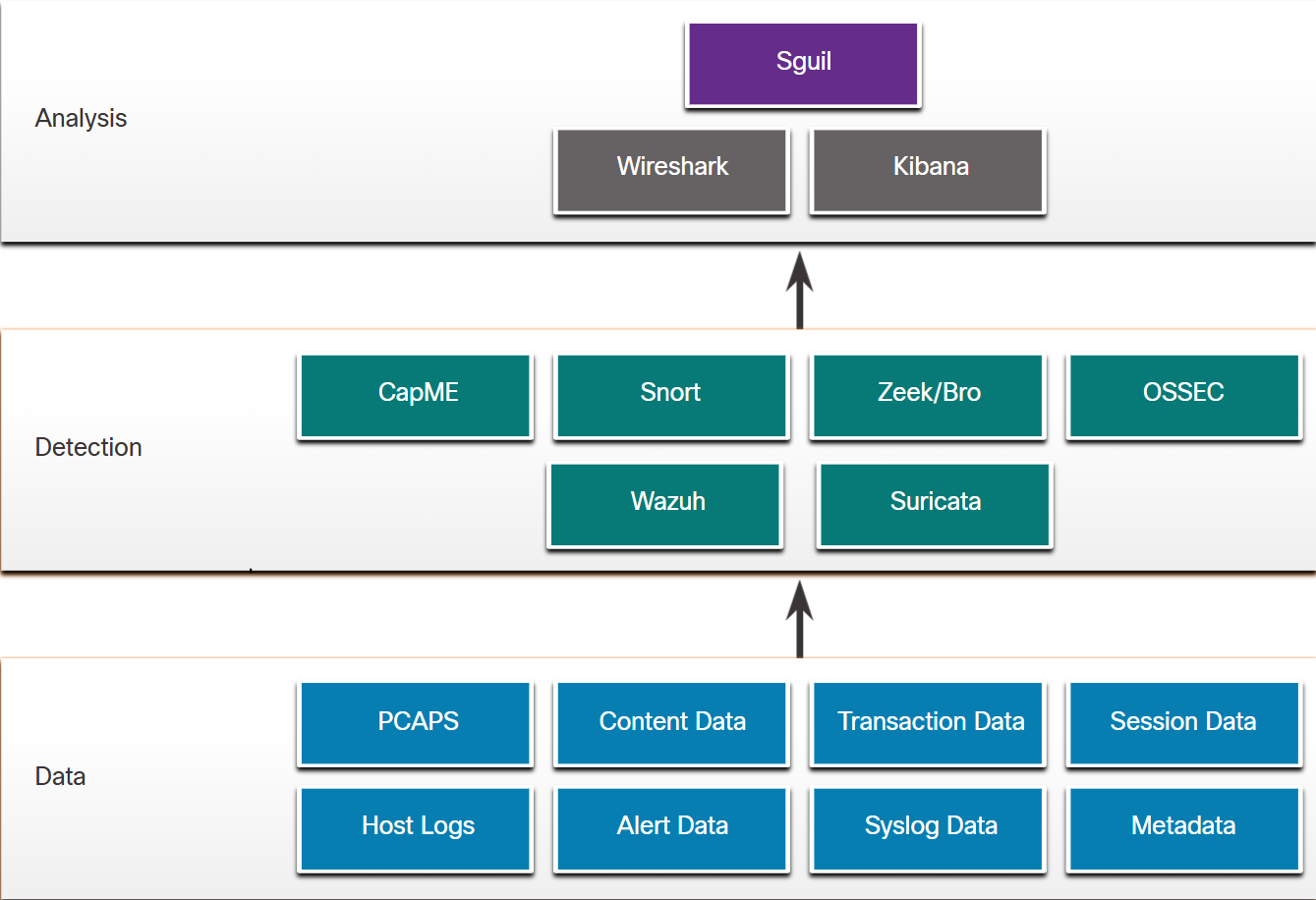
Web proxies provide data that helps determine whether responses from the web were generated in response to legitimate requests or have been manipulated to appear to be responses but are in fact exploits. It is also possible to use web proxies to inspect outgoing traffic as means of data loss prevention (DLP). DLP involves scanning outgoing traffic to detect whether the data that is leaving the web contains sensitive, confidential, or secret information.

**NexGen Firewalls**

NexGen Firewalls are advanced devices that provided much more functionality than previous generations of network security devices.

NGFW events include:

* **Connection Event** - Connection logs contain data about sessions that are detected directly by the NGIPS. Connection events include basic connection properties such as timestamps, source and destination IP addresses, and metadata about why the connection was logged, such as which access control rule logged the event.
* **Intrusion Event** - The system examines the packets that traverse the network for malicious activity that could affect the availability, integrity, and confidentiality of a host and its data. When the system identifies a possible intrusion, it generates an intrusion event, which is a record of the date, time, type of exploit, and contextual information about the source of the attack and its target.
* **Host or Endpoint Event** - When a host appears on the network it can be detected by the system and details of the device hardware, IP addressing, and the last known presence on the network can be logged.
* **Network Discovery Event** - Network discovery events represent changes that have been detected in the monitored network. These changes are logged in response to network discovery policies that specify the kinds of data to be collected, the network segments to be monitored, and the hardware interfaces of the device that should be used for event collection.
* **NetFlow Event** -Network discovery can use a number of mechanisms, one of which is to use exported NetFlow flow records to generate new events for hosts and servers.
  1. **SECURITY ONION**

Security Onion contains many components. It is an integrated environment which is designed to simplify the deployment of a comprehensive NSM solution. Security Onion tools provide three core functions for the cybersecurity analyst: full packet capture and data types, network-based and host-based intrusion detection systems, and alert analyst tools.

**Analysis Tools**

Security Onion integrates these various types of data and Intrusion Detection System (IDS) logs into a single platform through the following tools

* **Sguil -**This provides a high-level console for investigating security alerts from a wide variety of sources. Sguil serves as a starting point in the investigation of security alerts. A wide variety of data sources are available to the cybersecurity analyst by pivoting directly from Sguil to other tools.
* **Kibana -**Kibana is an interactive dashboard interface to Elasticsearch data. It allows querying of NSM data and provides flexible visualizations of that data. It provides data exploration and machine learning data analysis features. It is possible to pivot from Sguil directly into Kibana to see contextualized displays based on the source and destination IP addresses that are associated with an alert. Search the internet and visit the elastic.co website to learn more about the many features of Kibana.
* **Wireshark -**This is a packet capture application that is integrated into the Security Onion suite. It can be opened directly from other tools and will display full packet captures relevant to an analysis.
* **Zeek -**This is a network traffic analyser that serves as a security monitor. Zeek inspects all traffic on a network segment and enables in-depth analysis of that data.

**Detection Tools**

**CapME**

This is a web application that allows viewing of pcap transcripts(a human-readable representation of the captured packets) rendered with the tcpflow or Zeek tools. CapME can be accessed from the Enterprise Log Search and Archive (ELSA) tool. CapME provides the cybersecurity analyst with an easy-to-read means of viewing an entire Layer 4 session. CapME acts as a plugin to ELSA and provides access to relevant pcap files that can be opened in Wireshark.

**Snort**

This is a Network Intrusion Detection System (NIDS). It is an important source of alert data that is indexed in the Sguil analysis tool. Snort uses rules and signatures to generate alerts. Snort can automatically download new rules using the PulledPork component of Security Onion. Snort and PulledPork are open-source tools that are sponsored by Cisco.

**Zeek**

Formerly known as Bro. This is a NIDS that uses more of a behaviour-based approach to intrusion detection. Rather than using signatures or rules, Zeek uses policies, in the form of scripts that determine what data to log and when to issue alert notifications. Zeek can also submit file attachments for malware analysis, block access to malicious locations, and shut down a computer that appears to be violating security policies.

**OSSEC**

This is a host-based intrusion detection system (HIDS) that is integrated into Security Onion. It actively monitors host system operations, including conducting file integrity monitoring, local log monitoring, system process monitoring, and rootkit detection. OSSEC alerts and log data are available to Sguil and Kibana. OSSEC requires an agent to be running on the Windows computers in the enterprise.

**Wazuh**

Wazuh is a HIDS that will replace OSSEC in Security Onion. It is a full-featured solution that provides a broad spectrum of endpoint protection mechanisms including host logfile analysis, file integrity monitoring, vulnerability detection, configuration assessment, and incident response. Like OSSEC, it requires agents to be running on network hosts.

**Suricata**

This is a NIDS that uses a signature-based approach. It can also be used for inline intrusion prevention. It is similar to Zeek; however, Suricata uses native multithreading, which allows the distribution of packet stream processing across multiple processor cores. It also includes some additional features such as reputation-based blocking and support for Graphics Processing Unit (GPU) multithreading for performance improvement.

**Alert Generation**

Alerts will generally include five-tuples information when available, as well as timestamps and information identifying which device or system generated the alert

* **SrcIP -**the source IP address for the event.
* **SPort -**the source (local) Layer 4 port for the event.
* **DstIP -**the destination IP for the event.
* **DPort -**the destination Layer 4 port for the event.
* **Pr -**the IP protocol number for the event.

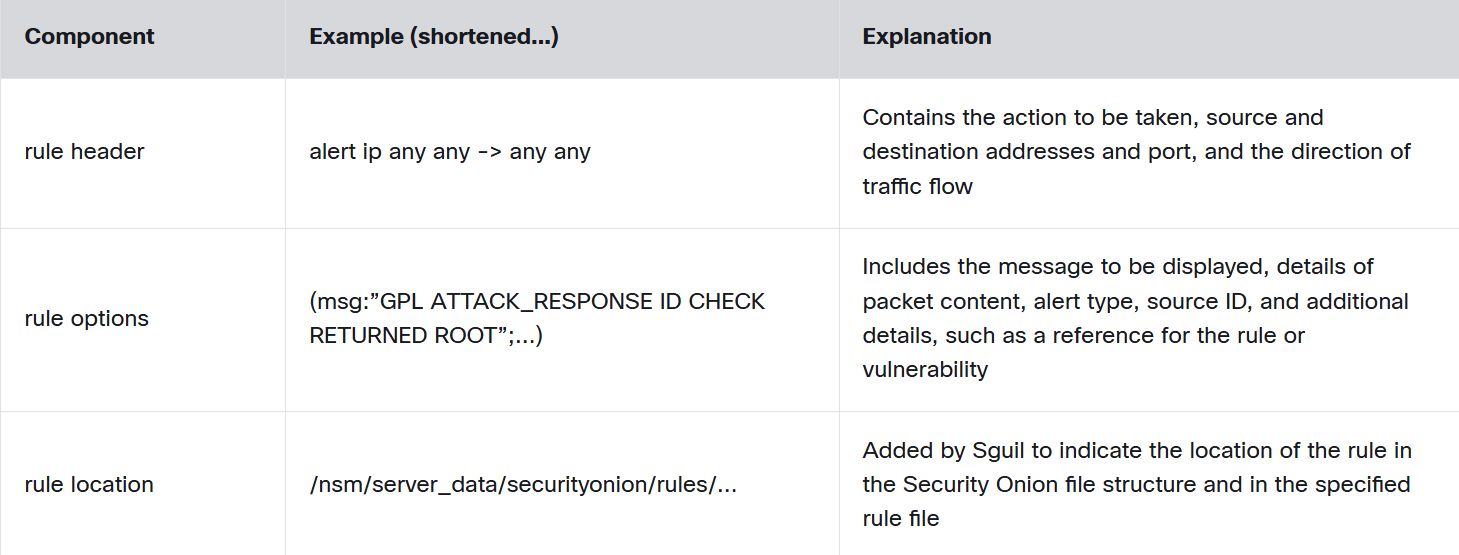
Additional information could be whether a permit or deny decision was applied to the traffic, some captured data from the packet payload, or a hash value for a downloaded file, or any of a variety of data.

**Alerts generated by Snort**

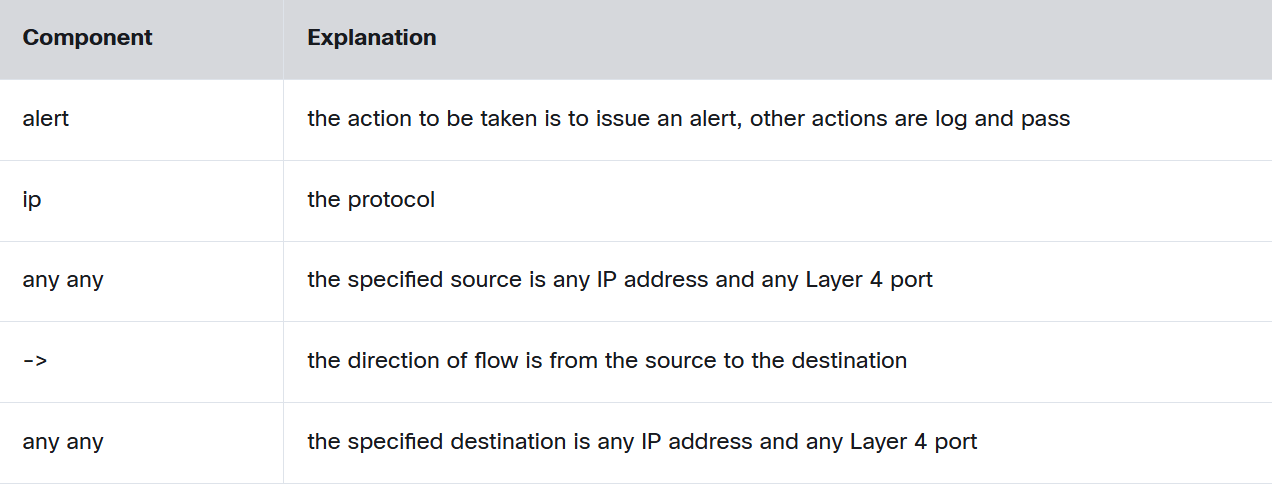
* **ST -**This is the status of the event. RT means real time. The event is color-coded by priority. The priorities are based on the category of the alert. There are four priority levels: very low, low, medium, and high. The colours range from light yellow to red as the priority increases.
* **CNT -**This is the count for the number of times this event has been detected for the same source and destination IP address. The system has determined that this set of events is correlated. Rather than reporting each in a potentially long series of correlated events in this window, the event is listed once with the number of times it has been detected in this column
* **Sensor -**This is the agent reporting the event. The available sensors and their identifying numbers can be found in the Agent Status tab of the pane. These numbers are also used in the Alert ID column.
* **Alert ID -**This two-part number represents the sensor that has reported the problem and the event number for that sensor.

**Eg of two part no:** 1.23.

* **Date/Time -**This is the timestamp for the event. In the case of correlated events, it is the timestamp for the first event.
* **Event Message -**This is the identifying text for the event. This is configured in the rule that triggered the alert. The associated rule can be viewed in the right-hand pane, just above the packet data. To display the rule, the **Show Rule**checkbox must be selected.
  1. **SNORT RULE STRUCTURE**

Snort rules consist of two sections: the rule header and the rule options

**Rule Header**

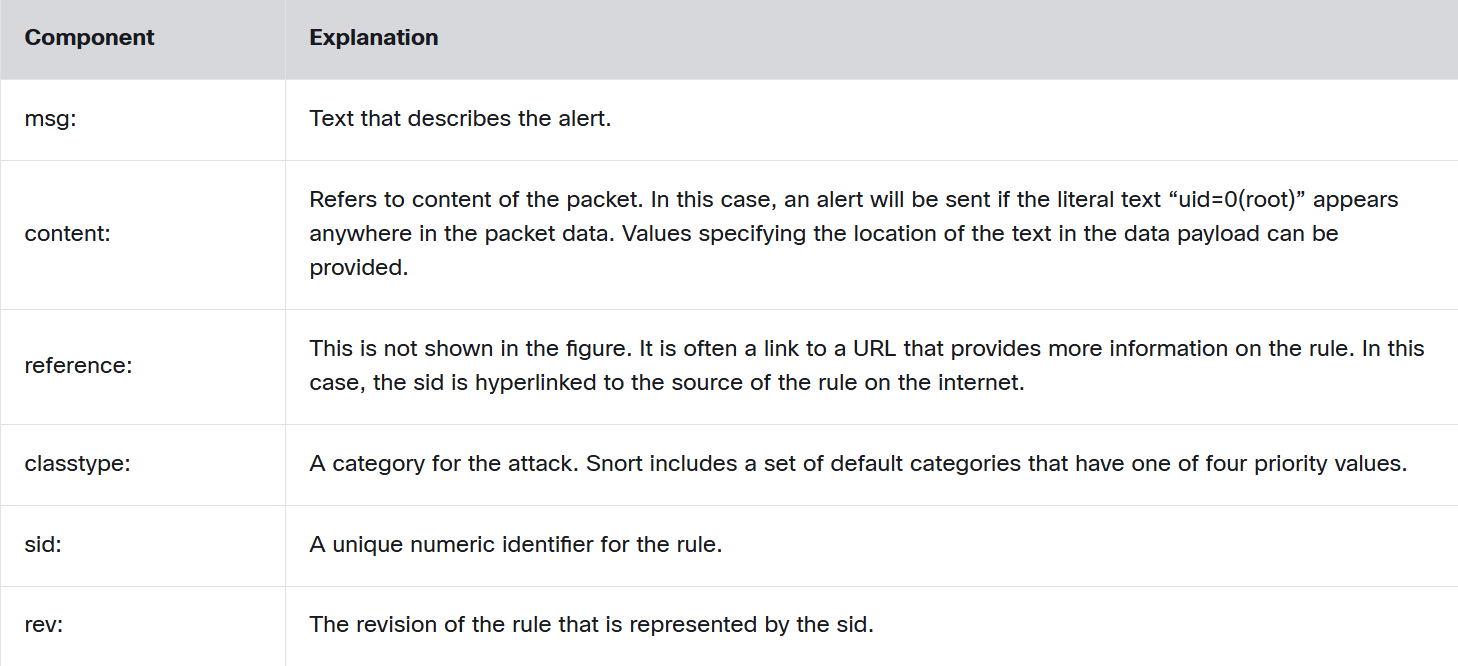
Snort can be configured to use variables to represent internal and external IP addresses. These variables,**$HOME\_NET** and**$EXTERNAL\_NET,** appear in the Snort rules. They simplify the creation of rules by eliminating the need to specify specific addresses and masks for every rule. The values for these variables are configured in the **snort.conf** file. Snort also allows individual IP addresses, blocks of addresses, or lists of either to be specified in rules. Ranges of ports can be specified by separating the upper and lower values of the range with a colon.

**Rule Options**

The structure of the options section of the rule is variable. It is the portion of the rule that is enclosed in parenthesis. It contains the text message that identifies the alert. It also contains metadata about the alert, such as a URL that provides reference information for the alert. Other information can be included, such as the type of rule and a unique numeric identifier for the rule and the rule revision. In addition, features of the packet payload may be specified in the options.

Snort rule messages may include the source of the rule. Three common sources for Snort rules are:

* **GPL -**Older Snort rules that were created by Sourcefire and distributed under a GPLv2. The GPL ruleset is not Cisco Talos certified. It includes Snort SIDs 3464 and below. The GPL ruleset is can be downloaded from the Snort website, and it is included in Security Onion.
* **ET -**Snort rules from Emerging Threats. Emerging Threats is a collection point for Snort rules from multiple sources. ET rules are open source under a BSD license. The ET ruleset contains rules from multiple categories. A set of ET rules is included with Security Onion. Emerging Threats is a division of Proofpoint, Inc.
* **VRT -**These rules are immediately available to subscribers and are released to registered users 30 days after they were created, with some limitations. They are now created and maintained by Cisco Talos.

Rules can be downloaded automatically from Snort.org using the PulledPork rule management utility that is included with Security Onion.

**Alerts Classification**

* True Positive: The alert has been verified to be an actual security incident.
* False Positive: The alert does not indicate an actual security incident. Benign activity that results in a false positive is sometimes referred to as a benign trigger.
* True Negative: No security incident has occurred. The activity is benign.
* False Negative: An undetected incident has occurred.

**Deterministic analysis**

Deterministic analysis evaluates risk based on what is known about a vulnerability. It assumes that for an exploit to be successful all prior steps in the exploit process must also be successful. This type of risk analysis can only describe the worst case. However, many threat actors, although aware of the process to carry out an exploit, may lack the knowledge or expertise to successfully complete each step on the path to a successful exploit. This can give the cybersecurity analyst an opportunity to detect the exploit and stop it before it proceeds any further.

**Probabilistic analysis**

Probabilistic analysis estimates the potential success of an exploit by estimating the likelihood that if one step in an exploit has successfully been completed that the next step will also be successful. Probabilistic analysis is especially useful in real-time network security analysis in which numerous variables are at play and a given threat actor can make unknown decisions as an exploit is pursued.

Probabilistic analysis relies on statistical techniques that are designed to estimate the probability that an event will occur based on the likelihood that prior events will occur. Using this type of analysis, the most likely paths that an exploit will take can be estimated and the attention of security personnel can be focused on preventing or detecting the most likely exploit.

**CYBER THREAT MANAGEMENT**

1. **GOVERNANCE**

IT security governance determines who is authorized to make decisions about cybersecurity risks within an organization. It demonstrates accountability and provides oversight to ensure that any risks are adequately mitigated and that security strategies are aligned with the organization’s business objectives and are compliant with regulations.

IT security governance should not be confused with IT security management, which defines and implements the controls that an organization needs to have in place to mitigate risks. Similarly, **data governance** in particular determines who is authorized to make decisions about data within an organization.

Cybercrime falls into three categories:

1. **Computer-targeted crime** is where a computer is the target of criminal activity. Examples include malware attacks, hacking or denial of service attacks.
2. **Computer-assisted crime**occurs when a computer is used to commit a crime, such as theft or fraud.
3. C**omputer-incidental crime**is where a computer provides information that is incidental to an actual crime. For example, a computer is used to store illegally downloaded videos, not the actual tool used to commit the crime.
4. **TWELVE DOMAINS OF CYBERSECURITY**

ISO/IEC 27000 is a series of information security standards or best practices to help organizations improve their information security. Published by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (ICO), the ISO 27000 standards set out comprehensive information security management system (ISMS) requirements. An ISMS consists of all of the administrative, technical and operational controls that address information security within an organization.

The ISO 27000 standard is represented by twelve independent domains.

**Risk assessment**

This is the first step in the risk management process, which determines the quantitative and qualitative value of risk related to a specific situation or threat.

**Security policy**

This document addresses the constraints and behaviours of individuals within an organization and often specifies how data can be accessed, and what data is accessible by whom.

**Organization of information security**

This is the governance model set out by an organization for information security.

**Asset management**

This is an inventory of and classification scheme for information assets within an organization.

**Human resources security**

This refers to the security procedures in place that relate to employees joining, moving within and leaving an organization.

**Physical and environmental security**

This refers to the physical protection of an organization’s facilities and information.

**Communications and operations management**

This refers to the management of technical security controls of an organization’s systems and networks.

**Information systems acquisition, development and maintenance**

This refers to security as an integral part of an organization’s information systems.

**Access control**

This describes how an organization restricts access rights to networks, systems, applications functions and data in order to prevent unauthorized user access.

**Information security incident management**

This describes an organization’s approach to the anticipation of and response to information security breaches.

**Business continuity management**

This describes the ability of an organization to protect, maintain and recover business-critical activities following a disruption to information systems.

**Compliance**

This describes the process of ensuring conformance with information security policies, standards and regulations.

These twelve domains are made up of **control objectives** (ISO 27001) and **controls** (ISO 27002).

**Control Objectives**

Control objectives define the high-level requirements for implementing a comprehensive information security management system within an organization, and usually provide a checklist to use during an ISMS audit.

Passing this audit indicates that an organization is ISO 27001 compliant and provides partners with confidence in the security of the organization’s data and operations.

**Controls**

Controls set out how to accomplish an organization’s control objectives. They establish guidelines for implementing, maintaining and improving the management of information security in an organization

1. **THE NATIONAL CYBERSECURITY WORKFORCE FRAMEWORK**

The National Institute of Standards and Technologies (NIST) created the National Cybersecurity Workforce Framework to support organizations seeking cybersecurity professionals. The framework organizes cybersecurity work into seven categories, outlining the main job roles, responsibilities and skills needed for each one.

**Operate and maintain**

Provides the support, administration and maintenance required to ensure effective and efficient IT system performance and security.

**Protect and defend**

Identifies, analyses and mitigates threats to internal systems and networks.

**Investigate**

Investigates cybersecurity events and/or cyber-attacks involving IT resources.

**Collect and operate**

Provides specialized denial and deception operations and collection of cybersecurity information.

**Analyse**

Performs highly specialized review and evaluation of incoming cybersecurity information to determine its usefulness for intelligence.

**Oversee and govern**

Provides leadership, management, direction or development and advocacy so an organization may effectively conduct cybersecurity work.

**Securely provision**

Conceptualizes, designs, procures or builds secure IT systems.

1. **THE CIS CRITICAL SECURITY CONTROLS**

The Centre for Internet Security (CIS) developed a set of critical security controls to help organizations with different levels of resources and expertise at their disposal to improve their cyber defences.

**Basic controls**

Organizations with limited resources and cybersecurity expertise available should implement:

* Inventory and control of hardware assets
* Inventory and control of software assets
* Continuous vulnerability management
* Controlled use of administrative privileges
* Secure configurations for hardware and software
* Maintenance, monitoring and analysis of audit logs

**Foundational controls**

Organizations with moderate resources and cybersecurity expertise available should implement the basic controls as well as:

* Email and web browser protections
* Malware defence
* Limitation and control of network ports, protocols and services
* Data recovery capabilities
* Secure configurations for network devices
* Boundary defence
* Data protections
* Controlled access based on the ‘need to know’ principle
* Wireless access control
* Account monitoring and control

**Organizational controls**

Organizations with significant resources and cybersecurity expertise available should implement the basic and foundational controls, as well as:

* A security awareness and training program
* Application software security
* Incident response and management
* Penetration tests and red team exercises (simulated attack exercises to gauge an organization’s security capabilities)

**The Cloud Security Alliance (CSA)**

The Cloud Security Alliance (CSA) provides security guidance to any organization that uses cloud computing or wants to assess the overall security risk of a cloud provider.

Their Cloud Controls Matrix (CCM) is a cybersecurity control framework that maps cloud-specific security controls to leading standards, best practices and regulations. It is composed of 197 control objectives that are structured in 17 domains covering all aspects of cloud technology, including governance and risk management, human resources and mobile security.

**vulnerability scanners**

vulnerability scanners on the market include Nessus, Retina, Core Impact and GFI LanGuard.

Vulnerability scanners fall into one of several categories:

* Network scanners probe hosts for open ports, enumerate information about users and groups and look for known vulnerabilities on the network.
* Application scanners access application source code to test an application from the inside (they do not run the application).
* Web application scanners identify vulnerabilities in web applications.

Intrusive scans try to exploit vulnerabilities and may even crash the target, while a non-intrusive scan will try not to cause harm to the target.

In a credentialed scan, usernames and passwords provide authorized access to a system, allowing the scanner to harvest more information. Non-credentialed scans are less invasive and give an outsider’s point of view.

**Operations security**

Operations security is concerned with the day-to-day practices necessary to first deploy and later maintain a secure system. Operations security starts with the planning and implementation process of a network. During these phases, the operations team analyses designs, identifies risks and vulnerabilities, and makes the necessary adaptations. The actual operational tasks begin after the network is set up and include the continual maintenance of the environment. These activities enable the environment, systems, and applications to continue to run correctly and securely.

An ST&E is an examination of the protective measures that are placed on an operational network.

Objectives of ST&E include the following:

* Uncover design, implementation, and operational flaws that could lead to the violation of the security policy.
* Determine the adequacy of security mechanisms, assurances, and device properties to enforce the security policy.
* Assess the degree of consistency between the system documentation and its implementation.

**Network testing Software tools**

* Nmap/Zenmap - This is used to discover computers and their services on a network, therefore creating a map of the network.
* SuperScan - This port scanning software is designed to detect open TCP and UDP ports, determine what services are running on those ports, and to run queries, such as whois, ping, traceroute, and hostname lookups.
* SIEM (Security Information Event Management) - This is a technology used in enterprise organizations to provide real time reporting and long-term analysis of security events.
* GFI LANguard - This is a network and security scanner which detects vulnerabilities.
* Tripwire - This tool assesses and validates IT configurations against internal policies, compliance standards, and security best practices.
* Nessus - This is a vulnerability scanning software, focusing on remote access, misconfigurations, and DoS against the TCP/IP stack.
* L0phtCrack - This is a password auditing and recovery application.
* Metasploit **-** This tool provides information about vulnerabilities and aids in penetration testing and IDS signature development.

**Nmap**

One of Nmap’s advanced features is the ability to **use decoy hosts** when performing a scan.

* Normally, when you run a scan, the target system sees your IP address in its logs. This makes it easy to trace the scan back to you.
* With decoys, Nmap can generate fake scan traffic that looks like it’s coming from other IP addresses (hosts).
* This way, the target sees multiple IPs scanning it at once, and it’s harder to tell which one is the real source.

**SuperScan**

SuperScan is a Microsoft Windows port scanning tool. It runs on most versions of Windows and requires administrator privileges.

SuperScan version 4 has a number of useful features:

* Adjustable scanning speed
* Support for unlimited IP ranges
* Improved host detection using multiple ICMP methods
* TCP SYN scanning
* UDP scanning (two methods)
* Simple HTML report generation
* Source port scanning
* Fast hostname resolution
* Extensive banner grabbing capabilities
* Massive built-in port list description database
* IP and port scan order randomization
* A selection of useful tools, such as ping, traceroute, and whois
* Extensive Windows host enumeration capability

1. **NETWORK INTELLIGENCE COMMUNITIES**

|  |  |
| --- | --- |
| **Organization** | **Description** |
| SANS | SysAdmin, Audit, Network, Security (SANS) Institute resources are largely free upon request and include:   * The Internet Storm Center - the popular internet early warning system * NewsBites, the weekly digest of news articles about computer security. * @RISK, the weekly digest of newly discovered attack vectors, vulnerabilities with active exploits, and explanations of how recent attacks worked * Flash security alerts * Reading Room - more than 1,200 award-winning, original research papers. * SANS also develops security courses. |
| Mitre | The Mitre Corporation maintains a list of common vulnerabilities and exposures (CVE) used by prominent security organizations. |
| FIRST | Forum of Incident Response and Security Teams (FIRST) is a security organization that brings together a variety of computer security incident response teams from government, commercial, and educational organizations to foster cooperation and coordination in information sharing, incident prevention and rapid reaction. |
| SecurityNewsWire | A security news portal that aggregates the latest breaking news pertaining to alerts, exploits, and vulnerabilities. |
| (ISC)2 | International Information Systems Security Certification Consortium (ISC2) provides vendor neutral education products and career services to more than 75,000+ industry professionals in more than 135 countries. |
| CIS | The Center for Internet Security (CIS) is a focal point for cyber threat prevention, protection, response, and recovery for state, local, tribal, and territorial (SLTT) governments through the Multi-State Information Sharing and Analysis Center (MS-ISAC). The MS-ISAC offers 24x7 cyber threat warnings and advisories, vulnerability identification, and mitigation and incident response. |

1. **THREAT INTELLIGENCE SERVICES**

**Cisco Talos Threat Intelligence Group**

Talos is one of the largest commercial threat intelligence teams in the world, and is comprised of world-class researchers, analysts and engineers. The goal of Talos is to help protect enterprise users, data, and infrastructure from active adversaries. The Talos team collects information about active, existing, and emerging threats. Talos then provides comprehensive protection against these attacks and malware to its subscribers.

**FireEye**

FireEye uses a three-pronged approach combining security intelligence, security expertise, and technology.

FireEye offers SIEM and SOAR with the Helix Security Platform, which uses behavioural analysis and advanced threat detection and is supported by the FireEye Mandiant worldwide threat intelligence network. Helix is cloud-hosted security operations platform that combines diverse security tools and threat intelligence into a single platform.

The FireEye Security System blocks attacks across web and email threat vectors, and latent malware that resides on file shares. It can block advanced malware that easily bypasses traditional signature-based defences and compromises the majority of enterprise networks. It addresses all stages of an attack lifecycle with a signature-less engine utilizing stateful attack analysis to detect zero-day threats.

**Automated Indicator Sharing**

The U.S. Department of Homeland Security (DHS) offers a free service called Automated Indicator Sharing (AIS). AIS enables the real-time exchange of cyber threat indicators (e.g., malicious IP addresses, the sender address of a phishing email, etc.) between the U.S. Federal Government and the private sector.

**Common Vulnerabilities and Exposures (CVE) Database**

The United States government sponsored the MITRE Corporation to create and maintain a catalogue of known security threats called Common Vulnerabilities and Exposures (CVE). The CVE serves as a dictionary of common names (i.e., CVE Identifiers) for publicly known cybersecurity vulnerabilities.

The MITRE Corporation defines unique CVE Identifiers for publicly known information-security vulnerabilities to make it easier to share data.

**Threat Intelligence Communication Standards**

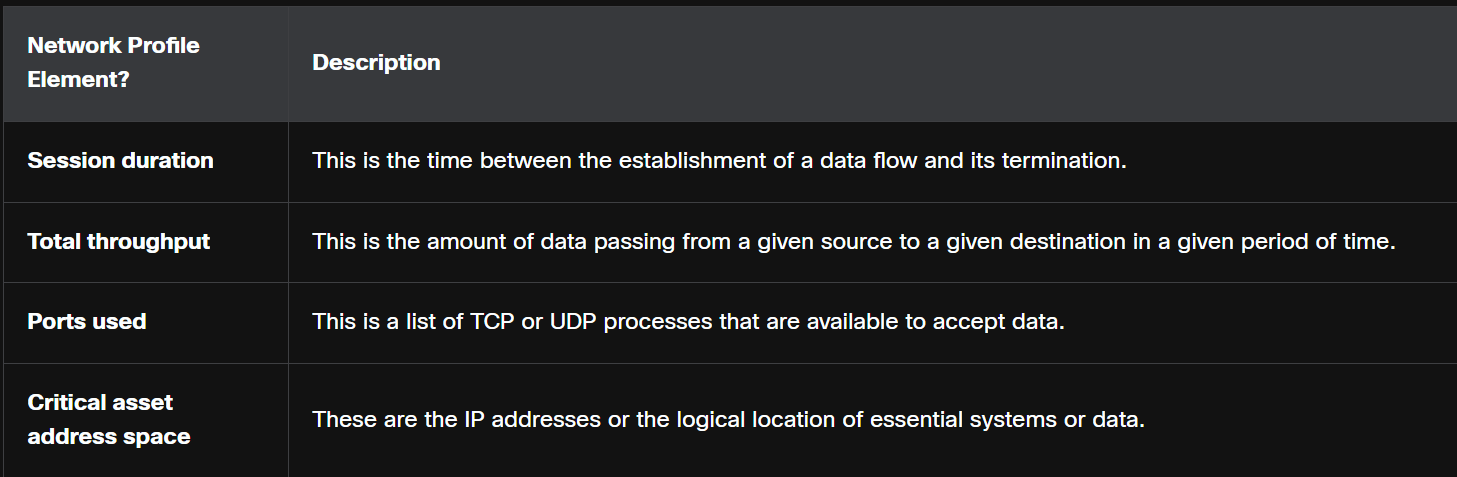
Network organizations and professionals must share information to increase knowledge about threat actors and the assets they want to access. Several intelligence sharing open standards have evolved to enable communication across multiple networking platforms. These standards enable the exchange of cyber threat intelligence (CTI) in an automated, consistent, and machine-readable format.

Three common threat intelligence sharing standards include the following:

* **Structured Threat Information Expression (STIX) -** This is a set of specifications for exchanging cyber threat information between organizations. The Cyber Observable Expression (CybOX) standard has been incorporated into STIX.
* **Trusted Automated Exchange of Indicator Information (TAXII) –** This is the specification for an application layer protocol that allows the communication of CTI over HTTPS. TAXII is designed to support STIX.
* **CybOX -** This is a set of standardized schema for specifying, capturing, characterizing, and communicating events and properties of network operations that supports many cybersecurity functions.

**The Malware Information Sharing Platform (MISP)** is an open-source platform for sharing indicators of compromise for newly discovered threats. MISP is supported by the European Union and is used by over 6,000 organizations globally. MISP enables automated sharing of IOCs between people and machines by using STIX and other export formats.

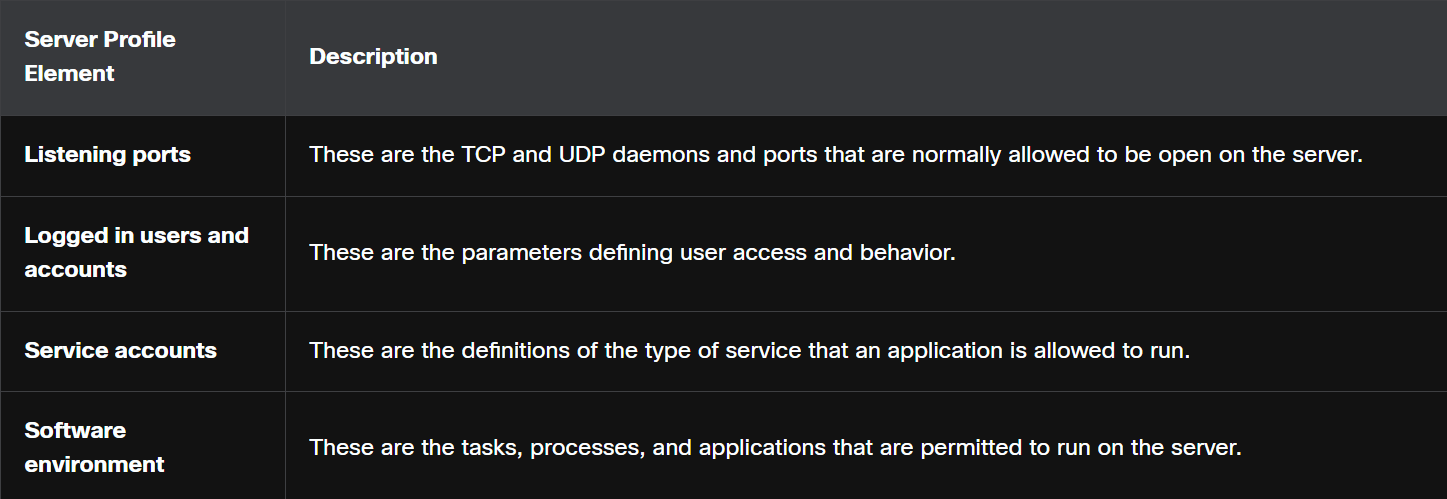
**Network Profiling**

Creating a baseline of network traffic for a prolonged period of time to ensure proper creation of a baseline which can be used to detect deviations of traffic in network

Profile of the types of traffic that typically enter and leave the network is an important tool in understanding network behaviour. Malware can use unusual ports that may not be typically seen during normal network operation. Host-to-host traffic is another important metric. Most network clients communicate directly with servers, so an increase of traffic between clients can indicate that malware is spreading laterally through the network.

changes in user behaviour, as revealed by AAA, server logs, or a user profiling system. Knowing how individual users typically use the network leads to detection of potential compromise of user accounts. A user who suddenly begins logging in to the network at strange times from a remote location should raise alarms if this behaviour is a deviation from a known norm.

**Server Profiling**

Baseline for accepted amount of network traffic, users and applications are used for Server Profiling

**Network Anomaly Detection**

Network behaviour is described by a large amount of diverse data such as the features of packet flow, features of the packets themselves, and telemetry from multiple sources. One approach to detection of network attacks is the analysis of this diverse, unstructured data using Big Data analytics techniques. This is known as network behaviour analysis (NBA).

This entails the use of sophisticated statistical and machine learning techniques to compare normal performance baselines with network performance at a given time. Significant deviations can be indicators of compromise. In addition, network behaviour can be analysed for known network behaviours that indicate compromise.

Anomaly detection can recognize network traffic caused by worm activity that exhibits scanning behaviour. Anomaly detection also can identify infected hosts on the network that are scanning for other vulnerable hosts.

For example, the cybersecurity analyst could provide the following values:

* X = 5
* Y = 100
* Z = 30
* N = 500

Now, the algorithm can be interpreted as: Every 5th minute, get a sampling of 1/100th of the flows during second 30. If the number of flows is greater than 500, generate an alarm. If the number of flows is less than 500, do nothing. This is a simple example of using a traffic profile to identify the potential for data loss.

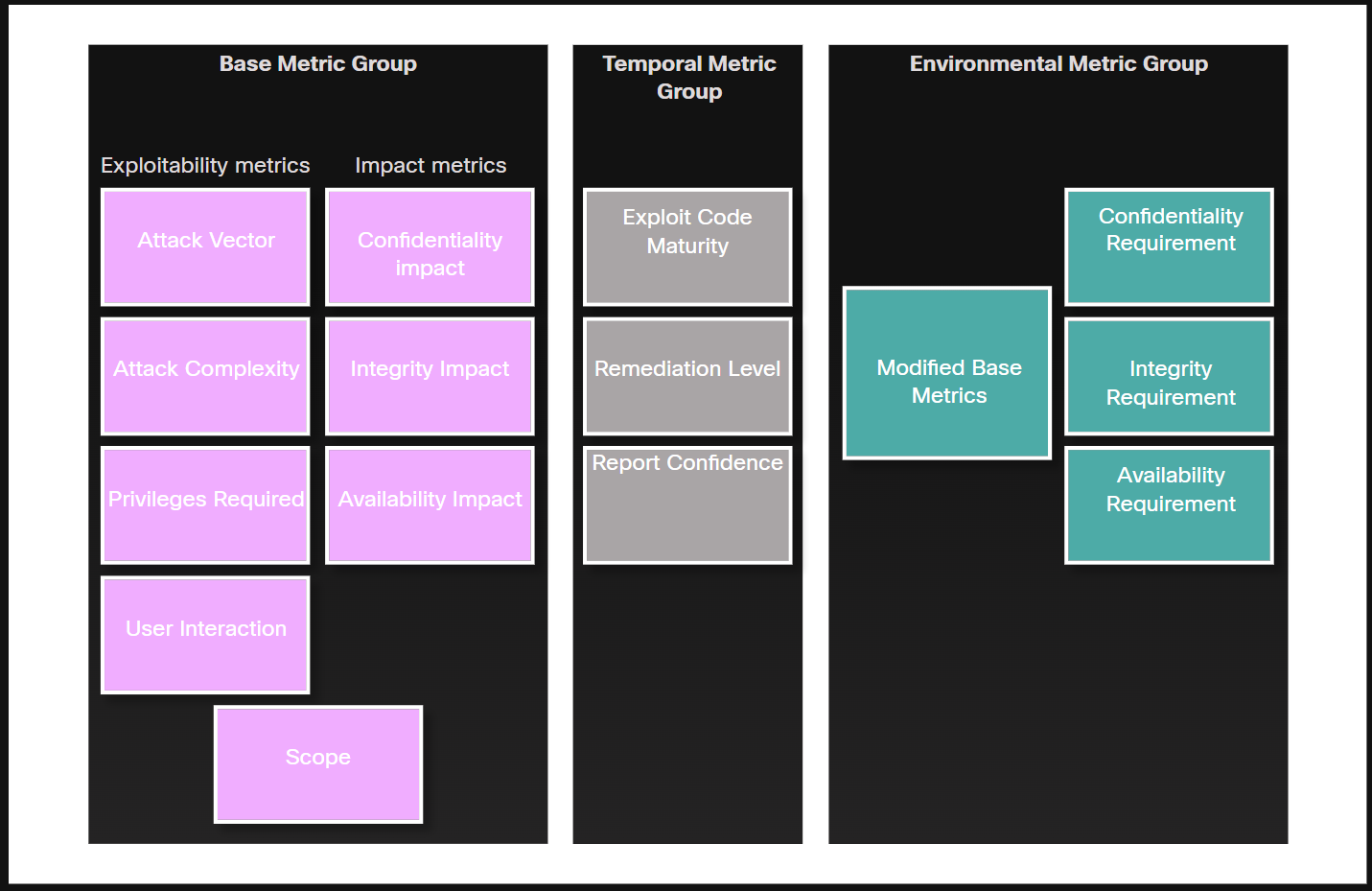
1. **THE COMMON VULNERABILITY SCORING SYSTEM (CVSS)**

The Common Vulnerability Scoring System (CVSS) is a risk assessment tool that is designed to convey the common attributes and severity of vulnerabilities in computer hardware and software systems. The third revision, CVSS 3.0, is a vendor-neutral, industry standard, open framework for weighting the risks of a vulnerability using a variety of metrics. These weights combine to provide a score of the risk inherent in a vulnerability. The numeric score can be used to determine the urgency of the vulnerability, and the priority of addressing it.

Many of the metrics address the role of what the CVSS calls an authority. An authority is a computer entity, such as a database, operating system, or virtual sandbox, that grants and manages access and privileges to users.

**CVSS Metric Groups**

Many of the metrics address the role of what the CVSS calls an authority. An authority is a computer entity, such as a database, operating system, or virtual sandbox, that grants and manages access and privileges to users.



**Base Metric Group – set by vendor, doesn’t change**

This represents the characteristics of a vulnerability that are constant over time and across contexts. It has two classes of metrics:

* Exploitability - These are features of the exploit such as the vector, complexity, and user interaction required by the exploit.
* Impact metrics - The impacts of the exploit are rooted in the CIA triad of confidentiality, integrity, and availability.
* Attack Vector – How close is the attacker to vulnerable component. If the attacker is in more distance with the help of remote attacking methods, it will be hard to detect
* Attack Complexity – System components like hardware and software which needs to be taken in control in order to perform an attack
* Privileges required – Privilege level required to perform an attack
* User Interaction – Presence or Absence of user interaction to trigger the exploit
* Scope – Ability or Inability of an exploit to spread to other systems

**Temporal Metric Group – set by vendor, changes over time**

This measures the characteristics of a vulnerability that may change over time, but not across user environments. Over time, the severity of a vulnerability will change as it is detected and measures to counter it are developed. The severity of a new vulnerability may be high, but will decrease as patches, signatures, and other countermeasures are developed.

**Environmental Metric Group – set by users**

This measures the aspects of a vulnerability that are rooted in a specific organization’s environment. These metrics help to rate consequences within an organization and allow adjustment of metrics that are less relevant to what an organization does.

**Process**

severity of a vulnerability is based on the characteristics of a successful exploit of the vulnerability. The other metric groups modify the base severity score by accounting for how the base severity rating is affected by time and environmental factors.

CVSS Provides a Vulnerability Score and Vector String, which is a line of information that abbreviates the base metric groups and their results in a summarized form to be easily seen

**CVSS SCORE**

* None 0
* Low 0.1 to 3.9
* Medium 4 to 6.9
* High 7 to 8.9
* Critical 9 to 10

**Vector String**

It also has Confidentially (C), Integrity (I), Availability (A) with possible values from None, low and high

**Other Values Include:**

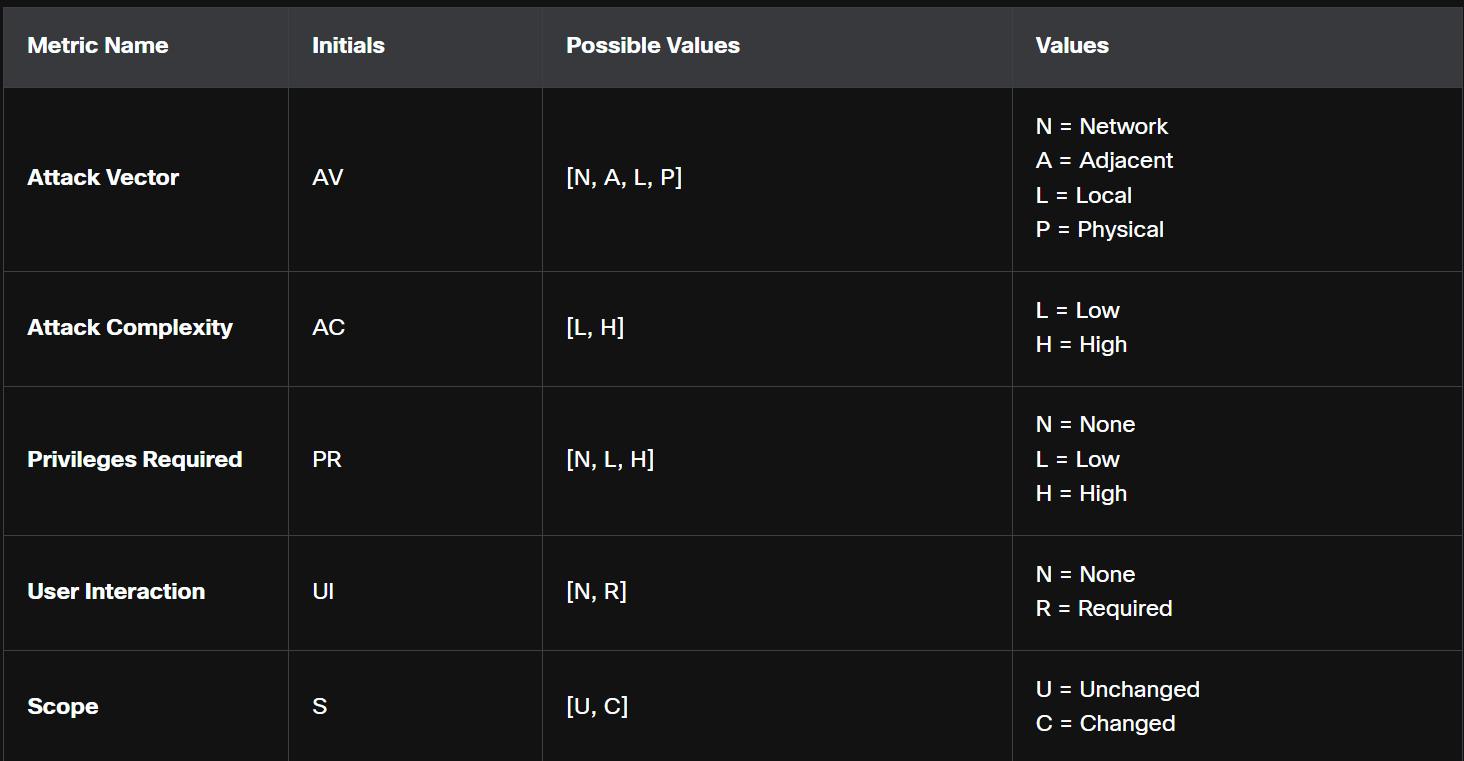
For Attack Vector

N = Network → Can attack over the internet (most dangerous).

A = Adjacent → Must be on the same local network (like Wi-Fi, Bluetooth).

L = Local → Needs access to the local machine (e.g., logged-in user).

P = Physical → Needs physical access to the device (least dangerous)



Privilege

NONE – no account needed

Low – basic account needed

High – Admin account needed

Scope

Unchanged – only exploits the current system

Changed – moves to other systems

**OTHER VULNERABILITY INFORMATION SOURCES**

There are other important vulnerability information sources. These work together with the CVSS to provide a comprehensive assessment of vulnerability severity. There are two systems that operate in the United States:

**CVE (Common Vulnerabilities and Exposures)**

The CVE Details website provides a linkage between CVSS scores and CVE information. It allows browsing of CVE vulnerability records by CVSS severity rating.

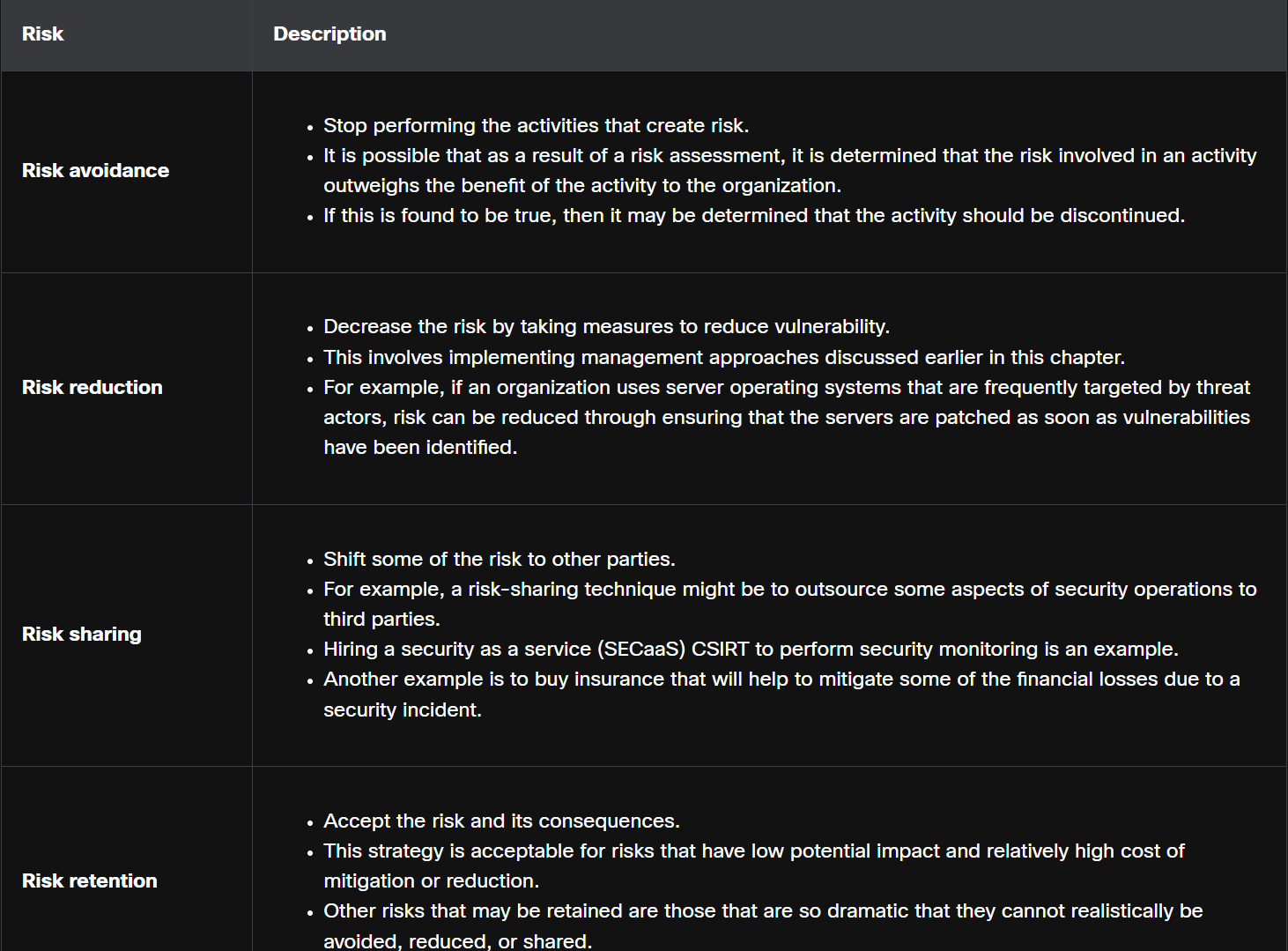
* A list of publicly known security flaws.
* Each vulnerability gets a unique ID like CVE-2025-12345.

**National Vulnerability Database (NVD)**

This utilizes CVE identifiers and supplies additional information on vulnerabilities such as CVSS threat scores, technical details, affected entities, and resources for further investigation. The database was created and is maintained by the U.S. government National Institute of Standards and Technology (NIST) agency.

1. **MANAGEMENT STEPS**

**Risk Management**

A Critical activity in risk assessment is finding vulnerabilities and matching it to possible threats that exploit the vulnerabilities which is known as threat-vulnerability(T-V) Pairing. It is used to create a baseline that can be used during security control implementations.

**Asset management**

Asset management involves the implementation of systems that track the location and configuration of networked devices and software across an enterprise. organizations must know what equipment accesses the network, where that equipment is within the enterprise and logically on the network, and what software and data those systems store or can access. Asset management not only tracks corporate assets and other authorized devices, but also can be used to identify devices that are not authorized on the network.

NIST specifies in publication NISTIR 8011 Volume 2, the detailed records that should be kept for each relevant device. NIST describes potential techniques and tools for operationalizing an asset management process:

* Automated discovery and inventory of the actual state of devices

Use tools to automatically **find and list all devices** connected to your network (computers, servers, printers, etc.), and record their details.

* Articulation of the desired state for those devices using policies, plans, and procedures in the organization’s information security plan

Clearly define how those devices should be set up (security settings, software versions, access rules) based on company policies.

* Identification of non-compliant authorized assets

Check if any devices don’t match the rules you set (e.g., outdated software, missing patches, weak passwords).

* Remediation or acceptance of device state, possible iteration of desired state definition

If something is wrong, **fix it** (patch, update, reconfigure) or, if it’s not risky/important, you might **accept it** and note it down. Sometimes you may even **update your rules** if they weren’t practical.

* Repeat the process at regular intervals, or ongoing

**Mobile Device Management**

Mobile device management (MDM), especially in the age of BYOD, presents special challenges to asset management. Mobile devices cannot be physically controlled on the premises of an organization. They can be lost, stolen, or tampered with, putting data and network access at risk. Part of an MDM plan is acting when devices leave the custody of the responsible party. Measures that can be taken include disabling the lost device, encrypting the data on the device, and enhancing device access with more robust authentication measures.

**Configuration Management**

Configuration management addresses the inventory and control of hardware and software configurations of systems. Secure device configurations reduce security risk. the organization may create baseline software images and hardware configurations for each type of machine. These images may include a basic package of required software, endpoint security software, and customized security policies that control user access to aspects of the system configuration that could be made vulnerable. Hardware configurations may specify the permitted types of network interfaces and the permitted types of external storage.

NIST Special Publication 800-128 on configuration management for network security is available

**PATCH MANAGEMENT**

Patch management involves all aspects of software patching, including identifying required patches, acquiring, distributing, installing, and verifying that the patch is installed on all required systems. Installing patches is frequently the most effective way to mitigate software vulnerabilities.

Patch management is required by some compliance regulations, such as Sarbanes Oxley (SOX) and the Health Insurance Portability and Accountability Act (HIPAA). Failure to implement patches in a systematic and timely manner could result in audit failure and penalties for non-compliance. Patch management software is available from companies such as SolarWinds and LANDesk. Microsoft System Center Configuration Manager (SCCM) is an enterprise-level tool for automated distribution of patches to a large number of Microsoft Windows workstations and servers.

**Agent Based**

a software agent to be running on each host to be patched. The agent reports whether vulnerable software is installed on the host. The agent communicates with the patch management server, determines if patches exist that require installation, and installs the patches. The agent runs with sufficient privileges to allow it to install the patches. Agent-based approaches are the preferred means of patching mobile devices.

**Agentless Scanning**

Patch management servers scan the network for devices that require patching. The server determines which patches are required and installs those patches on the clients. Only devices that are on scanned network segments can be patched in this way.

**Passive Network Monitoring**

Devices requiring patching are identified through the monitoring of traffic on the network. This approach is only effective for software that includes version information in its network traffic.

**Threat source type**

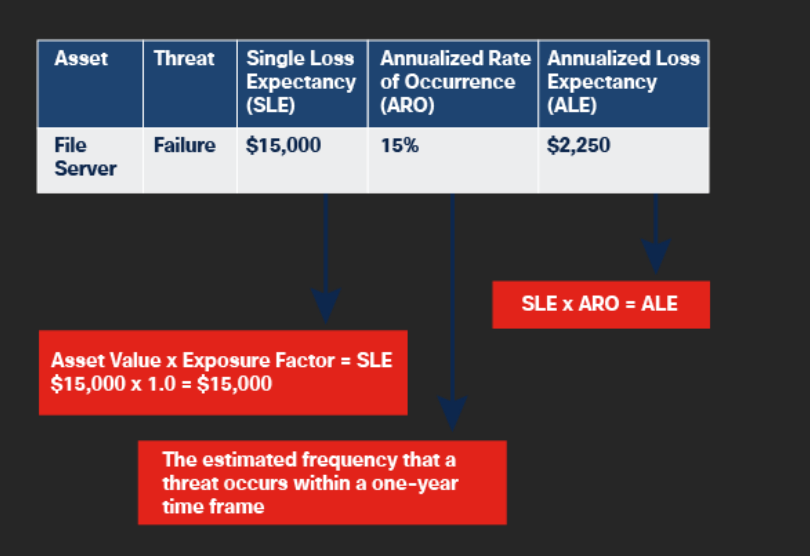
* Adversarial: Threats from individuals, groups, organizations or nations.
* Accidental: Actions that occur without a malicious intent.
* Structural: Equipment and software failures.
* Environmental: External disasters that can be either natural or human-caused, such as fires and floods.

**Quantitative risk analysis**

A quantitative risk analysis assigns numbers to the risk analysis process. In this example, the asset value is the replacement cost of the file server (the asset). The value of an asset can also be measured by the income gained through the use of the asset.

The exposure factor (EF) is a subjective value expressed as a percentage of the file server lost due to a particular threat. If total loss occurs, the EF equals 1.0 (100%).

The annualized rate of occurrence (ARO) is the probability that a loss will occur during the year. An ARO can be greater than 100% if a loss can occur more than once a year.



**Qualitative risk analysis**

Qualitative risk analysis uses opinions and scenarios plotting the likelihood of a threat against its impact. For example, a server failure may be likely, but its impact may only be marginal.

A risk matrix is a tool that helps prioritize risks to determine which ones the organization needs to develop a response for. The results can be ranked and used as a guide to determine whether the organization takes any action.

1. **FUNCTIONAL SECURITY CONTROLS**

The functional use of a specific safeguard or counter measure will help determine the reason for choosing and implementing it.

**Preventive controls**

Preventive security controls stop unwanted and unauthorized activity from happening and/or apply restrictions for authorized users.

For example, assigning user specific privileges on a system is a preventive control, as it puts limits in place to prevent certain users from accessing and performing unauthorized actions. A firewall that blocks access to a port or service that cybercriminals can exploit is also a preventive control.

**Deterrent controls**

A deterrent aims to discourage something from happening. Cybersecurity professionals and organizations use deterrents to limit or mitigate an action or behaviour — but deterrents cannot stop them completely.

Deterrent controls discourage cybercriminals from gaining unauthorized access to information systems and sensitive data. They can be effective at discouraging many different types of attacks on systems, as well as data theft and spreading malicious code.

**Detective controls**

Access control detection identifies different types of unauthorized activity. Detective controls are not a preventive measure and instead focus on the discovery of a security breach after it has occurred.

All detective systems have several things in common. They look for unusual or prohibited activity and can be very simple, such as a motion detector or security guard, or complex, such as an intrusion detection system. Detective controls may also provide methods to record or alert system operators of potential unauthorized access incidents.

**Corrective controls**

Corrective controls counteract something undesirable by restoring the system back to a state of confidentiality, integrity and availability. They can also restore systems to normal after unauthorized activity occurs.

Organizations will implement corrective access controls after a system experiences a threat. Examples include security policies, alarms, antivirus software, intrusion detection systems, mantraps and business continuity planning.

**Recovery controls**

Recovery security controls restore resources, functions and capabilities back to a normal state after a violation of a security policy. Recovery controls can repair damage, in addition to stopping any further damage. These controls have more advanced capabilities over corrective access controls.

Examples of recovery controls include backup/restore operations, fault tolerance drive systems, server clustering, and database shadowing.

**Compensative controls**

Compensative controls provide options to other controls to bolster enforcement in support of a security policy.

A compensative control can also be a substitution used in place of a control that is not possible under the circumstances. Perhaps an organization is not able to have a guard dog so, instead, it deploys a motion detector with a spotlight and a barking sound.

Examples of compensative security controls include security policies, personnel supervision, monitoring and work task procedures that are used in the absence of the ideal control an organization would have put in place.

**TYPES OF EVIDENCE**

In legal proceedings, evidence is broadly classified as either direct or indirect. Direct evidence is evidence that was indisputably in the possession of the accused, or is eyewitness evidence from someone who directly observed criminal behaviour.

Evidence is further classified as:

**Best evidence**

This is evidence that is in its original state. This evidence could be storage devices used by an accused, or archives of files that can be proven to be unaltered.

**Corroborating evidence**

This is evidence that supports an assertion that is developed from best evidence.

**Indirect evidence**

This is evidence that, in combination with other facts, establishes a hypothesis. This is also known as circumstantial evidence. For example, evidence that an individual has committed similar crimes can support the assertion that the person committed the crime of which they are accused.

**RFC 3227**

* Title: "Guidelines for Evidence Collection and Archiving"
* Published: February 2002 by the Internet Engineering Task Force (IETF).
* Purpose: It gives best practices for collecting, handling, and preserving digital evidence (useful in computer forensics and incident response).

It describes an order for the collection of digital evidence based on the volatility of the data. Data stored in RAM is the most volatile, and it will be lost when the device is turned off. In addition, important data in volatile memory could be overwritten by routine machine processes. Therefore, the collection of digital evidence should begin with the most volatile evidence and proceed to the least volatile

most volatile to least volatile evidence collection order is as follows:

* Memory registers, caches
* Routing table, ARP cache, process table, kernel statistics, RAM
* Temporary file systems
* Non-volatile media, fixed and removable
* Remote logging and monitoring data
* Physical interconnections and topologies
* Archival media, tape or other backups

**Threat attribution**

Threat attribution refers to the act of determining the individual, organization, or nation responsible for a successful intrusion or attack incident.

In an evidence-based investigation, the incident response team correlates Tactics, Techniques, and Procedures (TTP) that were used in the incident with other known exploits. Threat intelligence sources can help to map the TTP identified by an investigation to known sources of similar attacks. However, this highlights a problem with threat attribution. Evidence of cybercrime is seldom direct evidence. Identifying commonalities between TTPs for known and unknown threat actors is circumstantial evidence.

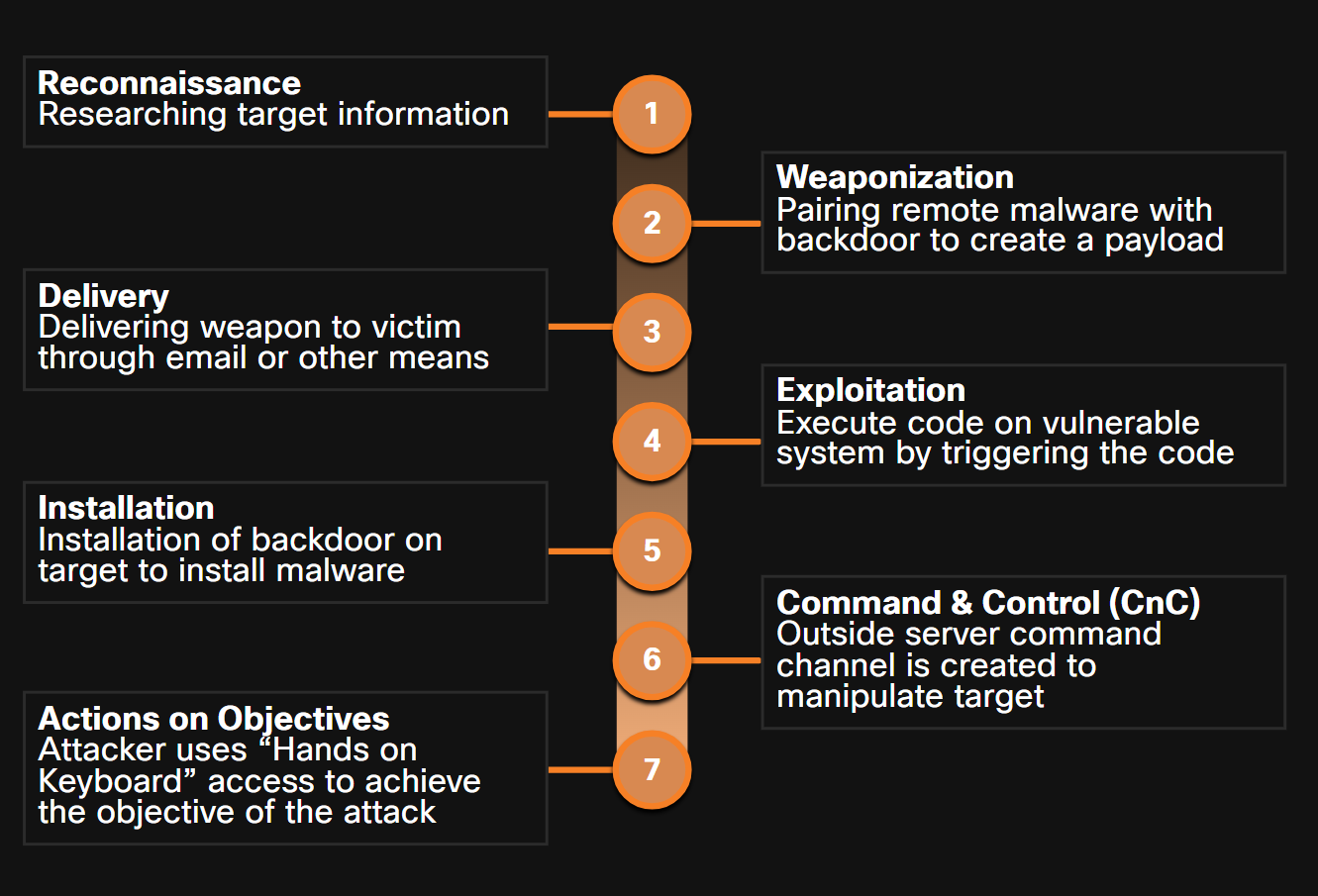
**The MITRE ATT&CK Framework**

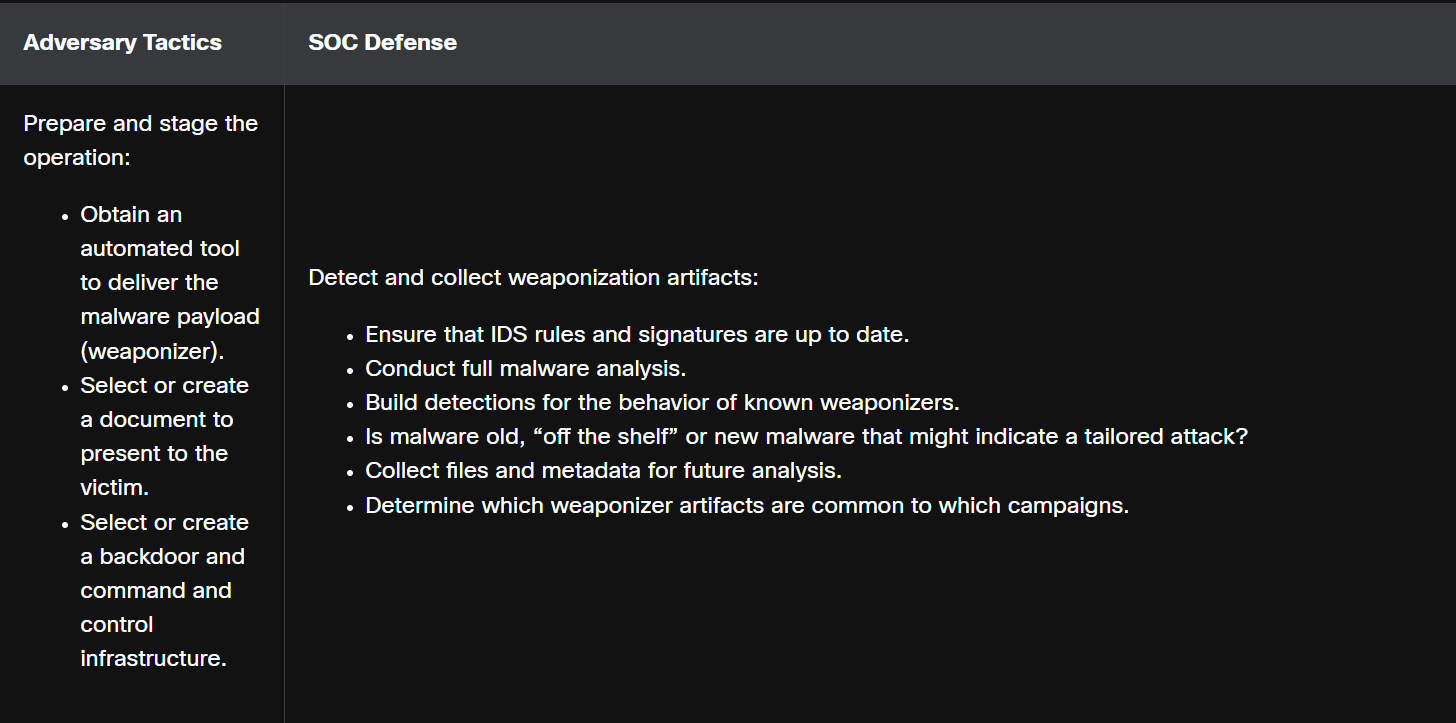
One way to attribute an attack is to model threat actor behaviour. The MITRE Adversarial Tactics, Techniques & Common Knowledge (ATT&CK) Framework enables the ability to detect attacker tactics, techniques, and procedures (TTP) as part of threat defence and attack attribution. This is done by mapping the steps in an attack to a matrix of generalized tactics and describing the techniques that are used in each tactic. Tactics consist of the technical goals that an attacker must accomplish in order to execute an attack and techniques are the means by which the tactics are accomplished. Finally, procedures are the specific actions taken by threat actors in the techniques that have been identified. Procedures are the documented real-world use of techniques by threat actors.

The MITRE ATT&CK Framework is a global knowledge base of threat actor behaviour. It is based on observation and analysis of real-world exploits with the purpose of describing the behaviour of the attacker, not the attack itself. It is designed to enable automated information sharing by defining data structures for the exchange of information between its community of users and MITRE.

1. **THE CYBER KILL CHAIN**

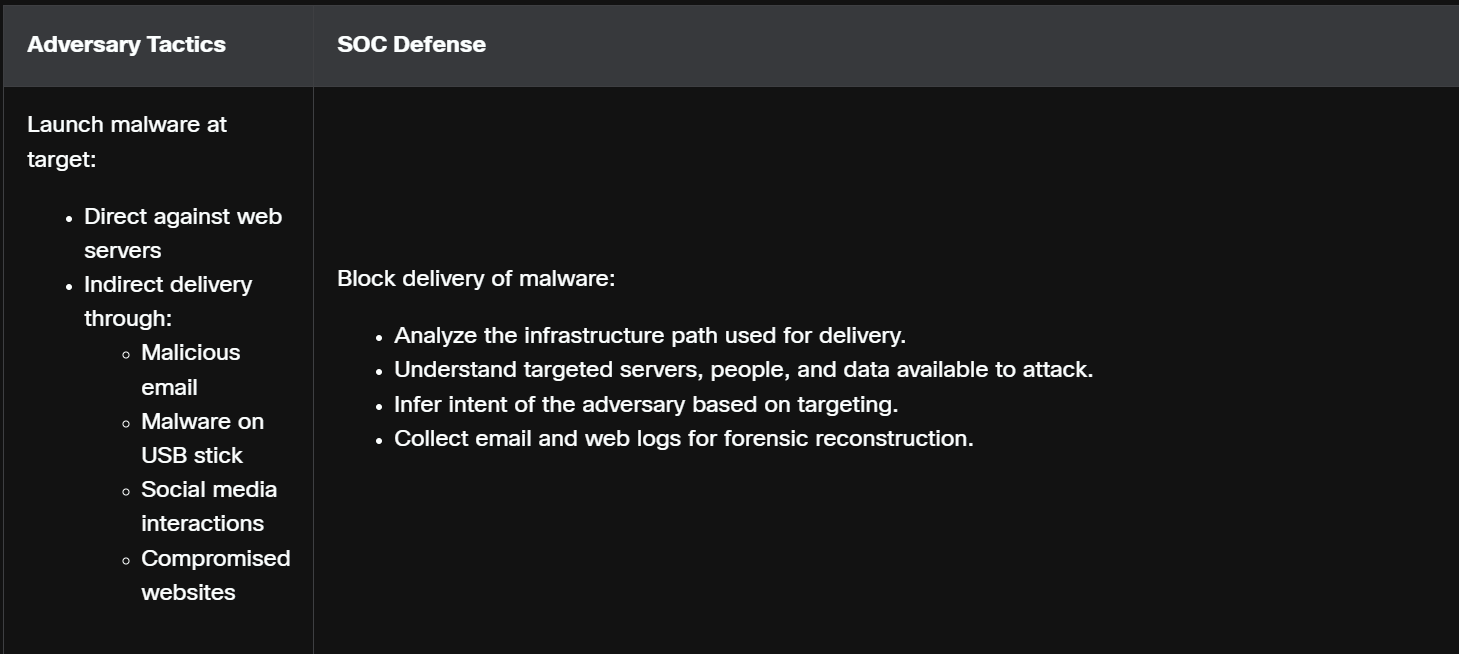
The Cyber Kill Chain was developed by Lockheed Martin to identify and prevent cyber intrusions. There are seven steps to the Cyber Kill Chain. Focusing on these steps helps analysts understand the techniques, tools, and procedures of threat actors. When responding to a security incident, the objective is to detect and stop the attack as early as possible in the kill chain progression. The earlier the attack is stopped; the less damage is done and the less the attacker learns about the target network.

The Cyber Kill Chain specifies what an attacker must complete to accomplish their goal.

**Reconnaissance**

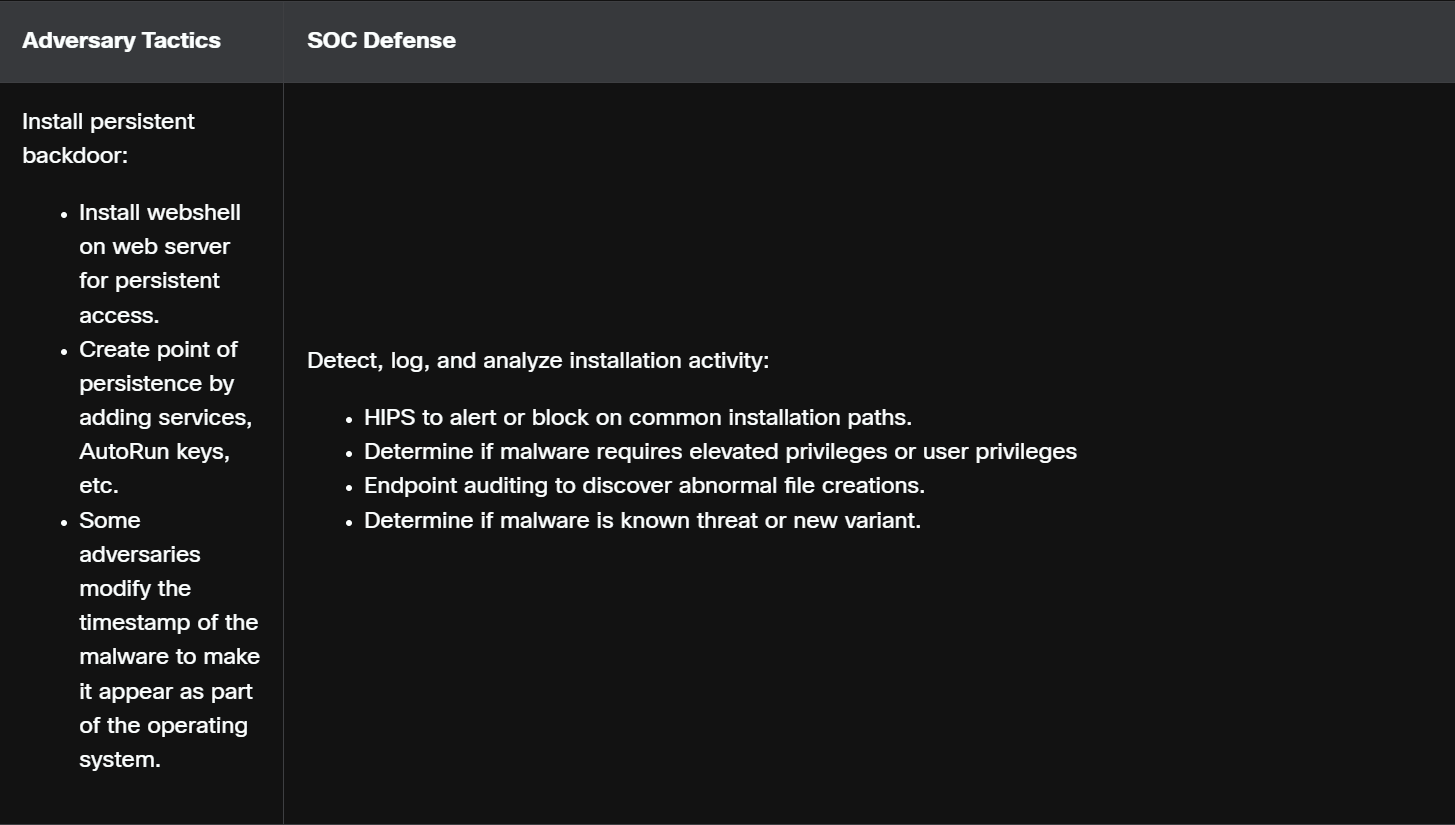
**Weaponization**

Creating malware based on the vulnerabilities found

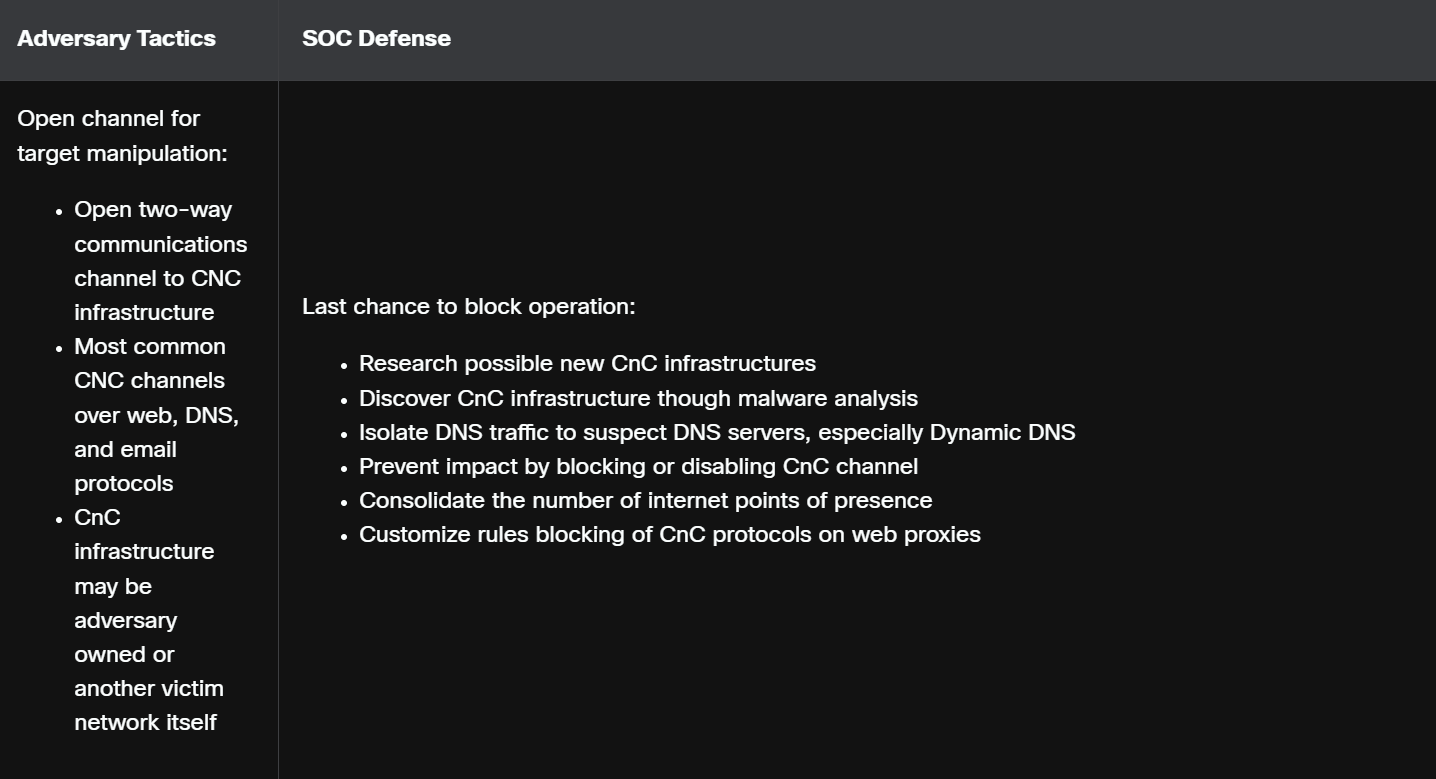
**Delivery**

**Exploitation**

**Installation**

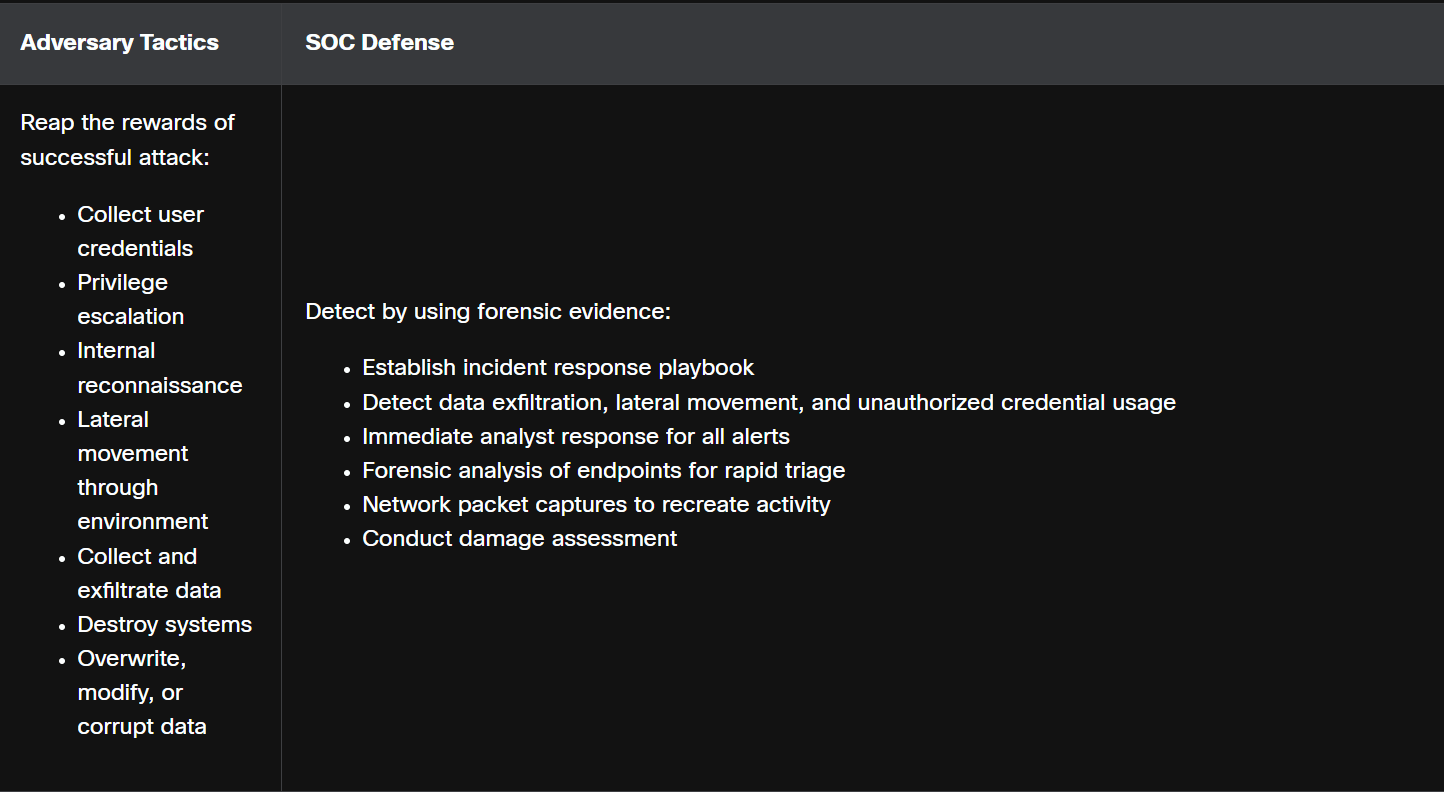
installing back doors

**Command and Control**

The goal is to establish command and control (CnC or C2) with the target system. Compromised hosts usually beacon out of the network to a controller on the internet. This is because most malware requires manual interaction in order to exfiltrate data from the network. CnC channels are used by the threat actor to issue commands to the software that they installed on the target.

The cybersecurity analyst must be able to detect CnC communications in order to discover the compromised host. This may be in the form of unauthorized Internet Relay Chat (IRC) traffic or excessive traffic to suspect domains.

**Actions on Objectives**

The final step of the Cyber Kill Chain describes the threat actor achieving their original objective. This may be data theft, performing a DDoS attack, or using the compromised network to create and send spam or mine Bitcoin. At this point the threat actor is deeply rooted in the systems of the organization, hiding their moves and covering their tracks. It is extremely difficult to remove the threat actor from the network.

1. **DIAMOND MODEL**

The Diamond Model of Intrusion Analysis is made up of four parts, as shown in the figure. The model represents a security incident or event. In the Diamond Model, an event is a time-bound activity that is restricted to a specific step in which an adversary uses a capability over infrastructure to attack a victim to achieve a specific result.

**The four core features of an intrusion event**:

**Adversary**

These are the parties responsible for the intrusion.

**Capability**

This is a tool or technique that the adversary uses to attack the victim.

**Infrastructure**

This is the network path or paths that the adversaries use to establish and maintain command and control over their capabilities.

**Victim**

This is the target of the attack. However, a victim might be the target initially and then used as part of the infrastructure to launch other attacks.

**META FEATURES**

**Timestamp**

This indicates the start and stop time of an event and is an integral part of grouping malicious activity.

**Phase**

This malicious activity includes two or more steps executed in succession to achieve the desired result.

**Result**

This refers to what the adversary gained from the event. Results can be documented as one or more of the following: confidentiality compromised, integrity compromised, and availability compromised.

**Direction**

This indicates the direction of the event across the Diamond Model. These include Adversary-to-Infrastructure, Infrastructure-to-Victim, Victim-to-Infrastructure, and Infrastructure-to-Adversary.

**Methodology**

This is used to classify the general type of event, such as port scan, phishing, content delivery attack, syn flood, etc.

**Resources**

These are one or more external resources used by the adversary for the intrusion event, such as software, adversary’s knowledge, information (e.g., username/passwords), and assets to carry out the attack (hardware, funds, facilities, network access).

1. **INCIDENT RESPONSE**

Computer Security Incident Response Team (CSIRT) is responsible to handle the incident quickly and correctly. The U.S. National Institute of Standards and Technology (NIST) recommendations for incident response are detailed in their Special Publication 800-61, revision 2 entitled “Computer Security Incident Handling Guide

**Policy Elements (the rules & framework)**

This is the high-level guidance that says how the organization will deal with incidents.  
It should be updated regularly to stay relevant.

* Management commitment → Leaders officially support the policy.
* Purpose & objectives → Why the policy exists and what it wants to achieve.
* Scope → What systems, people, and incidents it covers.
* Definitions → Clear meaning of “incident” and related terms.
* Roles & responsibilities → Who does what, and who has authority.
* Severity levels → How to rank incidents from low to critical.
* Performance measures → How success will be tracked (e.g., response time).
* Reporting forms → Standard forms/templates for reporting an incident.

**Plan Elements (the strategy & structure)**

This is the roadmap for how the organization will respond when an incident happens.

* Mission → What the incident response program is trying to achieve.
* Strategies & goals → The big-picture approach (e.g., minimize downtime, protect customer data).
* Senior management approval → Leaders sign off and support the plan.
* Organizational approach → The structure of the response team (who reports to who).
* Communication methods → How the team talks internally and externally (e.g., IT, law enforcement, customers).
* Metrics → How to measure effectiveness (e.g., incidents handled per month, average response time).
* Fit with organization → How incident response ties into the overall business.

**Procedure Elements (the step-by-step actions)**

This is the detailed instruction manual that responders follow during an incident.

* Technical processes → Exact steps to take (e.g., disconnect a system, preserve logs).
* Techniques → Methods/tools used (e.g., forensic tools, malware scanners).
* Forms → Documents that must be filled during response.
* Checklists → Step-by-step tasks to ensure nothing is missed.

**INCIDENT RESPONSE STAKEHOLDERS**

Other groups and individuals within the organization may also be involved with incident handling

**Management**

Managers create the policies that everyone must follow. They also design the budget and are in charge of staffing all of the departments. Management must coordinate the incident response with other stakeholders and minimize the damage of an incident.

**Information Assurance**

This group may need to be called in to change things such as firewall rules during some stages of incident management such as containment or recovery.

**IT Support**

This is the group that works with the technology in the organization and understands it the most. Because IT support has a deeper understanding, it is more likely that they will perform the correct action to minimize the effectiveness of the attack or preserve evidence properly.

**Legal Department**

It is a best practice to have the legal department review the incident policies, plans, and procedures to make sure that they do not violate any local or federal guidelines. Also, if any incident has legal implications, a legal expert will need to become involved. This might include prosecution, evidence collection, or lawsuits.

**Public Affairs and Media Relations**

There are times when the media and the public might need to be informed of an incident, such as when their personal information has been compromised during an incident.

**Human Resources**

The human resources department might need to perform disciplinary measures if an incident caused by an employee occurs.

**Business Continuity Planners**

Security incidents may alter an organization’s business continuity. It is important that those in charge of business continuity planning are aware of security incidents and the impact they have had on the organization as a whole. This will allow them to make any changes in plans and risk assessments.

**Physical Security and Facilities Management**

When a security incident happens because of a physical attack, such as tailgating or shoulder surfing, these teams might need to be informed and involved. It is also their responsibility to secure facilities that contain evidence from an investigation.

**The Cybersecurity Maturity Model Certification**

The Cybersecurity Maturity Model Certification (CMMC) framework was created to assess the ability of organizations that perform functions for the U.S. Department of Defense (DoD) to protect the military supply chain from disruptions or losses due to cybersecurity incidents.

**NIST INCIDENT RESPONSE LIFE CYCLE**

NIST defines four steps in the incident response process life cycle

**Preparation**

The members of the CSIRT are trained in how to respond to an incident. CSIRT members should continually develop knowledge of emerging threats.

* Organizational processes are created to address communication between people on the response team. This includes such things as contact information for stakeholders, other CSIRTs, and law enforcement, an issue tracking system, smartphones, encryption software, etc.
* Facilities to host the response team and the SOC are created.
* Necessary hardware and software for incident analysis and mitigation is acquired. This may include forensic software, spare computers, servers and network devices, backup devices, packet sniffers, and protocol analyzers.
* Risk assessments are used to implement controls that will limit the number of incidents.
* Validation of security hardware and software deployment is performed on end-user devices, servers, and network devices.
* User security awareness training materials are developed.

**Detection and Analysis**

Through continuous monitoring, the CSIRT quickly identifies, analyzes, and validates an incident.

Attack vectors

An organization should be prepared to handle any incident but should focus on the most common types of incidents so that they can be dealt with swiftly. These are some of the more common types of attack vectors:

* Web - Any attack that is initiated from a website or application hosted by a website.
* Email - Any attack that is initiated from an email or email attachment.
* Loss or Theft - Any equipment that is used by the organization such as a laptop, desktop, or smartphone can provide the required information for someone to initiate an attack.
* Impersonation - When something or someone is replaced for the purpose of malicious intent.
* Attrition - Any attack that uses brute force to attack devices, networks, or services.
* Media - Any attack that is initiated from external storage or removable media.

Detection

* Precursor - This is a sign that an incident might occur in the future. When precursors are detected, an attack might be avoided by altering security measures to specifically address the type of attack detected. Examples of precursors are log entries that show a response to a port scan, or a newly-discovered vulnerability to an organization’s web server.
* Indicator - This is a sign that an incident might already have occurred or is currently occurring. Some examples of indicators are a host that has been infected with malware, multiple failed logins from an unknown source, or an IDS alert.

Analysis

When the CSIRT believes that an incident has occurred, it should immediately perform an initial analysis to determine the incident’s scope, such as which networks, systems, or applications are affected, who or what originated the incident, and how the incident is occurring.

**Containment, Eradication, and Recovery**

The CSIRT implements procedures to contain the threat, eradicate the impact on organizational assets, and use backups to restore data and software. This phase may cycle back to detection and analysis to gather more information, or to expand the scope of the investigation.

**Post-Incident Activities**

The CSIRT then documents how the incident was handled, recommends changes for future response, and specifies how to avoid a reoccurrence.

**INCIDENT DATA COLLECTION AND RETENTION**

* Reviewing logs, forms, reports, and other incident documentation for adherence to established incident response policies and procedures.
* Identifying which precursors and indicators of the incident were recorded to determine how effectively the incident was logged and identified.
* Determining if the incident caused damage before it was detected.
* Determining if the actual cause of the incident was identified, and identifying the vector of attack, the vulnerabilities exploited, and the characteristics of the targeted or victimized systems, networks, and applications.
* Determining if the incident is a recurrence of a previous incident.
* Calculating the estimated monetary damage from the incident (e.g., information and critical business processes negatively affected by the incident).
* Measuring the difference between the initial impact assessment and the final impact assessment.
* Identifying which measures, if any, could have prevented the incident.

Evidence is often retained for many months or many years after an incident has taken place. In some cases, compliance regulations may mandate the retention period. These are some of the determining factors for evidence retention:

**Prosecution**

When an attacker will be prosecuted because of a security incident, the evidence should be retained until after all legal actions have been completed. This may be several months or many years. In legal actions, no evidence should be overlooked or considered insignificant. An organization’s policy may state that any evidence surrounding an incident that has been involved with legal actions must never be deleted or destroyed.

**Data Type**

An organization may state that particular types of data should be kept for a specific period of time. Items such as email or text may only need to be kept for 90 days. More important data such as that used in an incident response (that has not had legal action), may need to be kept for three years or more.

**Cost**

If there is a lot of hardware and storage media that needs to be stored for a long time, it can become costly. Remember also that as technology changes, functional devices that can use outdated hardware and storage media must be stored as well.

1. **DISASTER RECOVERY PLANS**

Creating a business continuity plan starts with carrying out a business impact analysis (BIA) to identify critical business processes, resources and relationships between systems.

**Recovery time objectives (RTOs)**

The maximum tolerable length of time that a system, network or application can be unavailable after a failure or disaster.

**Recovery point objectives (RPOs)**

The average lifespan of a given asset before it fails.

**Mean time to repair (MTTR)**

The average time required to repair a failed component.

**Mean time between failures (MTBF)**

The average time that elapses between one failure and the next.

**Business Continuity Considerations**

Organizations need employees to properly configure and operate systems. Data can be useless until it provides information.

An organization should look at the following:

* Getting the right people to the right places.
* Documenting configurations.
* Establishing alternate communication channels for both voice and data.
* Providing power.
* Identifying all dependencies for applications and processes so that they are properly understood.
* Understanding how to carry out automated tasks manually.

The National Institute of Standards and Technology (NIST) developed best practices in relation to business continuity.

1. Develop the policy statement: Write a policy that provides guidance to develop the business continuity plan and assigns roles to carry out the tasks.
2. Conduct the business impact assessment: Identify critical systems and processes and prioritize them based on necessity.
3. Calculate risk: Identify vulnerabilities, threats and calculate risks.
4. Identify preventative controls: Identify and implement controls and countermeasures to reduce risk.
5. Develop recovery strategies: Devise methods to bring back critical systems quickly.
6. Develop the contingency plan: Write procedures to keep the organization functioning in a chaotic state.
7. Test the plan: Verify how effective the plan is in real-time scenarios.
8. Maintain the plan: Update the plan regularly.

**Exercises**

**Tabletop exercises**

The simplest is a tabletop exercise in which participants sit around a table with a facilitator who supplies information related to a scenario incident and processes that are being examined. No actual processes or procedures are invoked; they are just discussed. This may result in the realization that a certain type of incident is not currently covered in existing plans.

**Functional tests**

Another type of exercise is a functional test where certain aspects of a plan are tested to see how well they work (and how well-prepared personnel is).

**Operational exercises**

At the most extreme are full operational exercises, or simulations. These are designed to interrupt services to verify that all aspects of a plan are in place and sufficient to respond to the type of incident that is being simulated.