Network Security & CyberOps Revision

1. **The Cisco Talos Intelligence Group website**
   - provides comprehensive security and threat intelligence.
   - The Cisco Product Security Incident Response Team (PSIRT), is responsible for investigating and mitigating potential vulnerabilities in Cisco products
2. **Securing Network**
   - **V**PN
   - ASA Firewall
   - IPS
   - Layer 3 Switches
   - Layer 2 Switches
   - ESA/WSA
   - AAA Server
   - Physical Security
3. **Threat, Vulnerability, and Risk**
   - **Threat:**
   - **Vulnerability:**
   - **Risk:**
   - **Attack Surface:**
   - **Exploit:**
4. **Attack Surface**
   - **Network Attack Surface:** Exploits vulnerabilities in networks.
   - **Software Attack Surface:** exploitation of vulnerabilities in web, cloud, or host-based software applications.
   - **Human Attack Surface:** Exploits weaknesses in user behavior.
5. **Threat Actors**
   - **Script Kiddies:**
   - **Vulnerability Brokers:**
   - **Hacktivists:**
   - **Cybercriminals:**
   - **State- Sponsored:**
6. **White, Gray, Black Hackers**
   - **White Hat Hackers:** ethical hackers who use their programming skills for good, ethical, and legal purposes.
   - **Gray Hat Hackers:** commit crimes and unethical things but not to cause damage.
   - **Black Hat Hackers:** unethical criminals who violate computer and network security for personal gain.

7. **(IOC) indicators of compromise**
   - Many network attacks can be prevented by sharing information about indicators of compromise (IOC).
   - Each attack has unique, identifiable attributes. Indicators of compromise are the evidence that an attack has occurred.
   - can be features that identify (malware files - IP addresses – filenames - characteristic changes made to end system software.
8. **(IOA) Indicators of Attack**
   - IOA focus more on the motivation and strategies behind an attack and the attackers to gain access to assets
   - IOAs helps to generate a proactive security approach that can be reused in multiple contexts and multiple attacks
   - Defending against a strategy can therefore prevent future attacks.
9. **Sharing and Building Cybersecurity Awareness**
   - **CISA: (US) – tool (AIS)**
   - **NCSA:**
10. **Security tools**
    - You can identify it in ethical hacker course.
11. **Types of malware**
    - **Virus:**
    - **Worm:**
    - **Trojan horse:**
    - **Ransomware:**
12. **Types of Network Attacks**
    - Reconnaissance Attacks
    - Access Attacks
      - Password Attacks
      - Spoofing Attack
      - Trust Exploitation
      - Port redirection
      - Man-in-the-Middle
      - Buffer Overflow Attack
    - DOS Attacks
      - DOS Attack
      - DDOS Attack
        - Zombies
        - Botnet
        - Handler

        - Bots
        - botmaster

13. Social Engineering Attacks

- Pretexting
- Phishing
- Spear phishing
- Something for Something
- Baiting
- Impersonation
- Tailgating
- Shoulder surfing
- Dumpster diving

14. Evasion Methods

- Encryption and tunneling
- Resource exhaustion
- Traffic fragmentation
- Protocol-level misinterpretation
- Traffic substitution
- Traffic insertion
- Pivoting
- Rootkits
- Proxies

15. Intelligence Communities – Organizations

- SANS
- Mitre
- FIRST
- SecurityNewsWire
- (ISC)^2
- CIS

16. CIA

- **Confidentiality**
- **Integrity**
- **Availability**

17. BYOD Policies Practices

- Password protected access
- Manually control wireless connectivity
- Keep updated
- Back up data
- Enable “Find my Device”
- Provide antivirus software
- Use Mobile Device Management (MDM) software

18. NFP (Network Foundation Protection) Framework

NFP logically divides routers and switches into three functional areas:

- **Control plane:** Responsible for routing data correctly
- **Management plane:** Responsible for managing network elements
- **Data plane:** Responsible for forwarding data.

19. Securing the Control Plane

- Routing protocol authentication
- Control Plane Policing (CoPP)
  (feature that lets users control the flow of traffic that is handled by the route processor of a network device)
- AutoSecure

20. Securing the Management Plane

- Login and password policy
- Present legal notification
- Ensure the confidentiality of data
- Role-based access control (RBAC)
- Authorize actions
- Enable management access reporting

21.Securing the Data Plane

- ACLs
- Anti-spoofing mechanisms
- Layer 2 security
  - Port security
  - DHCP snooping
  - Dynamic ARP Inspection (DAI)
  - IP Source Guard

22. Assigning Administrative Roles

- **Configure Privilege Levels**

  To configure a privilege level with specific commands

- **Configure Role-Based CLI**

  Role-based CLI provides three types of views

  - Root View
  - CLI View
  - Superview

23. Limitations of privilege Levels.

- no access control to specific interfaces, ports, logical interfaces, and slots on a router.

- Commands available at lower privilege levels are always executable at higher levels

- ex: allowing access to **show ip route** allows the user access to all **show** and **show ip** commands

24. Cisco IOS resilient configuration feature

- Secure boot image
- Secure configuration files

25. Configuring Secure Copy

- The Secure Copy Protocol (SCP) feature is used to remotely copy IOS and configuration files

- SCP provides a secure and authenticated method for copying router configuration or router image files to a remote location

- SRC relies on SCP relies on SSH to secure communication and AAA to provide authentication and authorization.

26. Cisco AutoSecure

- lock down the management plane functions and the forwarding plane services
- **auto secure** command is initiated, a CLI **wizard** steps the administrator through the configuration of the device
- It is not recommended on **production** routers

27.Types of Management Access

In-band	Out-of-Band (OOB)
Information flows across an enterprise production network	Information flows on a dedicated management network
the Internet, or both, using regular data channels	on which no production traffic resides.
recommended in smaller networks	recommended large enterprise networks
Access via Telnet / SSH	Access via console using console server
Depends on IP and telnet / SSH port number	Depends on IP address and port number
Works when network Links is up	It is alternate path when Network goes down
It is synchronous	It is Asynchronous
Connection speed is high	Connection speed is slow
Connection is established via putty or secure CRT	Connection is established via terminal Access

28. AAA Components

- **Authentication**
- **Authorization**
- **Accounting**

29. Authentication Modes

- **Local AAA Authentication**
- **Server-Based AAA Authentication**
  - **Service:** (RADIUS)
  - **Service:**Terminal Access Controller Access Control System (TACACS+)

30.Comparison between RADIUS and TACAS+

	RADIUS	TACAS+
Transport Protocol	**UDP**	**TCP**
Confidentiality	**Password encrypted**	**Entire packet encrypted**
Functionality	**Combines authentication and authorization but separates accounting**	**Separates AAA**
Accounting	**Extensive**	**Limited**
CHAP	**Unidirectional challenge**	**Bidirectional challenge**
Standard	**Open/RFC standard**	**Mostly Cisco supported**

31. ACLs Tasks

- **Limit network traffic to increase network performance**
- **Provide traffic flow control**
- **Provide a basic level of security for network access**
- **Filter traffic based on traffic type**
- **Screen hosts to permit or deny access to network services**
- **Provide priority to certain classes of network traffic**

32. ACLs Types

- Standard ACLs :
- Extended ACLs:

Standard ACLs	**Extended ACLs**
Layer3	Layer 3,4
Preferred location at Destination	Preferred location at source
Filter Source IP	Filter Source IP, Destination (IP and Protocol)

33. Types of Firewalls

- **Packet Filtering (Stateless) firewalls**
  - permits or denies traffic based on **Layer 3** and **Layer 4** information
  - use a simple policy table look-up that filters traffic based on specific criteria
- **Stateful firewalls**
  - This filter information at Layers 3, 4, 5
  - Stateful firewalls provide stateful packet filtering by using connection information maintained in a state table.
  - Stateful filtering is a firewall architecture at the network layer
- **Application Gateway (Proxy) firewalls**
  - This filter information at Layers 3, 4, 5, and 7
  - control and filtering is done in software
  - When a client needs to access a remote server, it connects to a proxy server.
- **Next Generation firewalls**
  - providing integrated intrusion prevention, application awareness and control
  - upgrade paths to include future information feeds, and techniques to address evolving security threats.

34.Host-Based Firewalls

- **Windows Defender Firewall**
- **Iptables**
- **Nftables**
- **TCP Wrappers**

35.Common Security Architectures (Firewall Design)

- **Private and Public**
- **Demilitarized Zone (DMZ)**
- **Zone-Based Policy**

36. configuration models for Cisco IOS Firewall

- **Classic Firewall**
- **Zone-based Policy Firewall (ZPF)**

37. ZPF Actions

- Inspect
- Drop
- Pass

38.Zero-Day Attacks

- A zero-day attack is a cyberattack that tries to exploit software vulnerabilities that are unknown or undisclosed by the software vendor.

- The term zero-day describes the moment when a previously unknown threat is identified

39.Comparison between IDS And IPS

IPS	IDS
In line	**Off line**
Some impact on network (latency, jitter)	**No Impact on network (latency, jitter)**
Stops trigger packets	**Response action cannot stop trigger packets**
Sensor issues might affect network traffic	**No Network impact if there is a sensor failure**
Sensor overloading impacts the network	**No network impact if there is sensor overload**
Can use stream normalization techniques	**More vulnerable to network security evasion techniques**

40.Network-based IPS Sensors can be implemented in several ways: (Note)

- **On a Cisco Firepower appliance**
- **On an ASA firewall device**
- **On an ISR router**
- **As an NGIPSv for VMware**

41.HIDS Operation

- **Anomaly based:** Host system behavior is compared to a learned baseline model of normal behavior
- **Policy based:** Normal system behavior is described by rules, or the violation of rules, that are predefined.

42. Snort IPS

- Snort is an **open source network IPS** that performs **real-time traffic analysis** and generates alerts when threats are detected on IP networks
- The Snort engine runs in a **virtual service container** on Cisco 4000 Series ISRs

43.security K9 license (SEC)

- **Community Rule Set**
  (There is 30-day delayed access to updated signatures in the Community Rule Set**)**
- **Subscriber Rule Set**
  (Real Time Update)

44. Snort IPS Rule Actions

(Snort can be enabled in **IDS** mode or in **IPS** mode).

- **<u>Snort IDS mode</u>**
  - **Alert** : Generate an alert
  - **Log :** Log the packet.
  - **Pass :** Ignore the packet.
- **<u>Snort IPS mode</u>**
  - **Drop** : Block and log the packet
  - **Reject :** Block the packet, log it, and then send a TCP reset if the protocol is TCP or an ICMP port unreachable message if the protocol is UDP.
  - **Sdrop** : Block the packet but do not log it.

45.Snort IPS interfaces

(Snort IPS requires two VPG interfaces)

VPG: virtual port group

- **Management interface (VPG0)**
  - This is the interface that is used to source **logs** to the **log collector** and for **retrieving signature updates** from Cisco.com.
  - For this reason, this interface requires a **routable IP address**.
- **Data interface (VPG1)**
  - This is the interface that is used to send user traffic between the Snort **virtual container** service and the **router forwarding plane**.

46.Network Monitoring Methods

- **SPAN (Switch Port Analyzer)**
  - **Port mirroring** enables the switch to copy frames that are received on one or more ports to a Switch Port Analyzer (SPAN) port that is connected to an analysis device.
- **TAPs (test access points)**
  - network tap is typically a passive splitting device implemented inline between a device of interest and the network.
  - A tap forwards all traffic, including physical layer errors.
  - **fail-safe:** if a tap fails or loses power, traffic between the firewall and internal router is not affected.

47. Types of Signatures

- **Atomic Signature**
  - This is the simplest type of signature because a **single packet**, **activity**, or event identifies an attack.
  - IPS does not need to maintain **state information and traffic analysis** can usually be performed **very quickly and efficiently**
- **Composite Signature**
  - Also called a stateful signature because the IPS requires several pieces of data to match an attack signature
  - The IPS must also maintain state information (i.e., IP addresses, port numbers, and more).

48.IPS Signature Alarms (Detection Type)

- **Pattern-Based Detection**
- **Anomaly-Based Detection**
- **Policy-Based Detection**
- **Honey Pot-Based Detection**

49.Evaluating Alerts

- **True Positive:** Attack, Alarm, ideal setting.
- **True Negative:** no attack, no Alarm, ideal Setting.
- **False Positive:** no attack, Alarm, needs to tune Alarm, **Undesirable**.
- **False Negative:** Attack, no Alarm, needs to tune Alarm, **Dangerous**.

50.Traditional Endpoint Security

- Antivirus/Antimalware Software
- Host-based IPS
- Host-based firewall

51.Network-Based Malware Protection devices.

- Advanced Malware Protection (AMP)
- Email Security Appliance (ESA)
- Web Security Appliance (WSA)
- Network Admission Control (NAC)

52.Network Access Control

- **Profiling and visibility**: recognizes and users and their devices.
- **Guest network access:** guest registration and authentication.
- **Security posture checking**: evaluates security-policy for user and OS
- **Incident response:** Mitigating network threats without administrator attention.

53. IEEE 802.1X

- standard defines **authentication protocol** that restricts unauthorized workstations from connecting to a LAN through switch ports.

54.Switch Attack Categories

- **MAC Table Attacks:** Attacker use **MACOFF tool** for Mac Address Flooding.
- **VLAN Attacks:** VLAN hopping and VLAN double-tagging attacks.
- **DHCP Attacks:** DHCP starvation and DHCP spoofing attacks.
- **ARP Attacks: ARP spoofing and poisoning attacks**
- **Address Spoofing Attacks:** MAC Address and IP address spoofing attacks
- **STP Attacks:** Spanning Tree Protocol manipulation attacks

55.Switch Attack mitigation

- Port Security: Port security prevents many types of attacks including MAC table overflow attacks and DHCP starvation attacks.

- DHCP Snooping: DHCP Snooping prevents DHCP starvation and DHCP spoofing attacks by rogue DHCP servers

- Dynamic ARP Inspection (DAI): DAI prevents ARP spoofing and ARP poisoning attacks.

- IP Source Guard (IPSG): IP Source Guard prevents MAC and IP address spoofing attacks.

56.PVLAN

divide the broadcast domain into multiple broadcast sub-domains

- Promiscuous:

- Isolated:

- Community:

57.securing communications:

- **Authentication:** validating a source in network communications.
- **data nonrepudiation:** sender of a message to be uniquely identified (Digital Certificate)
- **Confidentiality:** Data confidentiality ensures privacy so that only the receiver can read the message. (encryption)
- **Integrity:** messages are not altered in transit (Hashing)

58. Cryptographic Services

- **Cryptography:** security professionals for encryption - development and use of codes
- **Cryptanalysis:** Hackers for decryption and crack - breaking of those codes
- **Cryptology:** Science for Cryptography and Cryptanalysis.

59. securing communications Algorithms

- **Data Integrity** : Integrity is ensured by implementing either of the Secure Hash Algorithms (SHA-2 or SHA-3). The MD5
- **Origin Authentication**: networks ensure authentication with algorithms such as hash-based message authentication code (HMAC).
- **Data Confidentiality:** Data confidentiality is implemented using symmetric and asymmetric encryption algorithms.
  - **Symmetric algorithms:** DES, 3DES, AES, SEAL, RC.
  - **Asymmetric algorithms:** RSA, DSS, DSA, DH, ElGamal, ECT.
- **Data Non-Repudiation :** Nonrepudiation relies on the fact that only the sender has the unique characteristics or signature for how that message is treated.

60.Public and Private Keys

- **Confidentiality:** Encrypt Public Key + Decrypt Private Key (Destination)
- **Authentication:** Encrypt Private Key + Decrypt Public Key (Source)

61.Diffie-Hellman

Diffie-Hellman (DH) is an asymmetric mathematical algorithm that allows two computers to generate an identical shared secret without having communicated before.

62.VPN

- VPNs create end-to-end private network connections
- it carries information within a private network, but that information is transported over a public network.

63.VPNs encryption features

- Internet Protocol Security (IPsec)
- Secure Sockets Layer (SSL)

64.VPN Benefits vs Leased Lines

- Cost Savings (no need for ISPs service Fees)
- Security (carries information within a private network over public network)
- Scalability (Remote Access VPN)
- Compatibility of WAN link options (supports all popular broadband technologies)

65.VPN Topologies

- Site-to-Site VPNs
- Remote-Access VPNs

66.compares IPsec and SSL remote access

Feature	IPsec	SSL
Applications supported	Supports All Apps	web-based applications
Authentication strength	Strong	Moderate
Encryption strength	Strong	Moderate – Strong
Connection complexity	Moderate	Low
Connection option	Only specific devices with specific configurations	Any device with a web browser

67.IPsec Framework

- **IPsec Protocol:**AH – ESP – AH+ESP
- **Confidentiality:** DES-3DES-AES - SEAL
- **Integrity:** MD5 – SHA1 – SHA2
- **Origin authentication:** PSK – RSA
- **Diffie-Hellman:** DH1 – DH2 - …. – DH24

68.IPsec Protocol Encapsulation

- **AH :**
  - appropriate only when confidentiality is not required.
  - AH uses IP protocol 51
- **ESP :**
  - provides both confidentiality and authentication.
  - ESP uses IP protocol 50
- **AH + ESP**

69.IPsec Protocols Modes

- **Transport Mode:** protects the payload of the packet but leaves the original IP address in plaintext.
- **Tunnel Mode:** The original IP packet is encrypted and then it is encapsulated in another IP packet

70.The IKE Protocol

enhances IPsec by adding features and simplifies configuration for the IPsec.

- phase 1 : uses ISAKMP
- phase 2 : key negotiation

71. ISAKMP

- negotiates a security association (a key) between two IKE peers

72. Advanced ASA Firewall Features

- A single ASA can be partitioned into multiple virtual devices (called a security context)
- <u>Failover configuration</u> to provide device redundancy (devices must be identical.
- The ASA provides access control based on an association of IP addresses to Windows Active Directory login information.
- ASA uses the Advanced Inspection and Prevention (AIP) modules
  - integrating the Content Security and Control (CSC) module.
  - Advanced Inspection and Prevention Security Services Module (AIP-SSM)
  - Advanced Inspection and Prevention Security Services Card (AIP-SSC)

73. Cisco Firepower Series

- Next-generation IPS (NGIPS)
- Advanced Malware Protection (AMP)
- Application control and URL filtering

74.ASA Firewall Modes of Operation

- **Routed Mode:**
  - two or more interfaces separate **Layer 3** networks
  - Routed mode supports multiple interfaces
  - Each interface is on a different subnet and **requires an IP address** on that subnet.
  - ASA applies policies to flows as they transit the firewall
- **Transparent Mode:**
  - ASA functions like a **Layer 2** device and is not considered a router hop.
  - ASA is only assigned an IP address on the local network for management purposes
  - This mode is useful to **simplify a network configuration**, or when the **existing IP addressing cannot be altered**
  - **no support for dynamic routing protocols**, VPNs, QoS, or DHCP Relay.

75.Network Security Monitoring Tools

- **Network protocol analyzers**
- **NetFlow**
- **Security Information and Event Management Systems (SIEM)**

76.SIEM

provide real time reporting and long-term analysis of security events

- **Forensic analysis**
- **Correlation**
- **Aggregation**
- **Reporting**

77.SIEM and SOAR

SIEM	**SOAR**
provides details on the source of suspicious activity.	enhances SIEM, enhanced data gathering and a number of functionalities that aid in security **incident response**
User information such as username, authentication status, location	Use artificial intelligence to detect incidents

78.IP Vulnerabilities

- ICMP attacks
- DoS attacks
- DDoS attacks
- Address spoofing attacks
- Address spoofing attacks
- Session hijacking

79. TCP Vulnerabilities

- TCP SYN Flood Attack
- TCP Reset Attack
- TCP Session Hijacking

80.UDP Attacks

- UDP Flood Attacks

81.ARP Cache Poisoning

-

82.DNS Attacks

- DNS cache poisoning attacks
- DNS amplification and reflection attacks
- DNS resource utilization attacks

83.DHCP

- DHCP Spoofing Attack
- DHCP Starvation Tool

84.Common HTTP Exploits

- Malicious iFrames
- HTTP 302 Cushioning
- Domain Shadowing

85.Email

- Attachment-based attacks
- Email spoofing
- Spam email
- Open mail relay server

86.Web-Exposed Databases

- Code Injection
- SQL Injection
- Cross-Site Scripting

87. Network Intelligence Communities

- **SANS:**
  - the popular internet **early** warning system.
  - **weekly** digest of news **articles** about computer security.
  - **weekly** digest of newly **discovered** attack vectors, vulnerabilities, active exploits.
  - explanations of how recent attacks worked.
  - Reading Room (More than 1,200 award-winning, original research papers)
  - SANS also **develops security courses.**
- **Mitre:**
  - maintains a list of **Common Vulnerabilities and Exposures** (CVE) used by prominent security organizations
- **FIRST**
  - information sharing, incident prevention and rapid reaction
  - computer security incident response **teams** from government, commercial, and educational organizations.
- **CIS**
  - cyber threat prevention, protection, response, and recovery for state, local governments.

- **Cisco**
  - Cisco Annual Cybersecurity Report and the Mid-Year Cybersecurity Report
  - Cisco provides blogs on security-related topics from a number of industry experts and from the **Cisco Talos Group**
  - Cisco Talos offers a series of over 80 **podcasts** that can be played from the internet or downloaded to your device of choice.

88.Cisco Talos

- Talos is one of the largest commercial threat intelligence teams in the world
- The team collects information about active, existing, and emerging threats, and then provides comprehensive protection against these attacks and malware to its subscribers.
- Cisco Security products can use Talos threat intelligence in real time
- Cisco Talos also provides free software, services, resources, data and maintains the security incident detection rule sets for the Snort.org, ClamAV, and SpamCop network security tools

89.FireEye

- FireEye is another security company that offers services to help enterprises secure their networks.
- It uses a **three-pronged approach** combining
  - security intelligence,
  - security expertise,
  - and technology**.**

90. Helix Security Platform

- <u>**behavioral**</u> **analysis and advanced threat detection** and is supported by the FireEye Mandiant **worldwide threat intelligence network**.

91.FireEye Security System:

- **Security System** blocks attacks across web and email threat vectors, and latent malware that resides on **file shares**
- **traditional signature-based:** It can block advanced malware that easily bypasses traditional signature-based defenses
- **signature-less engine:** It addresses all stages of an attack lifecycle and utilizing stateful attack analysis to detect **zero-day threats**

92.Automated Indicator Sharing (AIS)

- free service offered by the U.S Department
- AIS enables the real-time exchange of cyber threat indicators between the U.S. Federal Government and the private sector
- creates an ecosystem, it is immediately shared with the community to help them protect their networks from that particular threat.

93.Common Vulnerabilities and Exposures (CVE)

- The CVE serves as a **dictionary** of CVE Identifiers for publicly **known** cybersecurity vulnerabilities.
- MITRE Corporation defines unique CVE Identifiers for publicly known information-security vulnerabilities to make it easier to share data.

94.Three common threat intelligence sharing standards

- **STIX :** set of specifications for exchanging cyber **threat information** between organizations.
- **TAXII :** This is the specification for an **application layer protocol** that allows the communication of CTI over HTTPS.
- **CybOX:** set of standardized **schema** for specifying, capturing, characterizing, and communicating **events and properties of network operation**s that supports many cybersecurity functions.

95.The Malware Information Sharing Platform (MISP)

- open source platform for sharing IOCs for newly discovered threats.
- supported by **the European Union** and is used by over 6,000 organizations globally.
- enables automated sharing of IOCs between people and machines by using STIX and other export formats.

96.Threat Intelligence Platform (TIP)

- centralizes the collection of threat data from numerous data sources and formats.

97.Types of threat Intelligence data:

- Indicators of Compromise (IOC)
- Tools Techniques and Procedures (TTP)
- Reputation information about internet destinations or domains

98.Honeypots

- simulated networks or servers that are designed to attract attackers.
- The attack-related information gathered from honeypots can be shared with threat intelligence platform subscribers

99. System-Based Sandboxing

Sandboxing is a technique that allows suspicious files to be executed and analyzed in a **safe environment**

- **Cuckoo Sandbox:** popular free malware analysis system sandbox. It can be run locally and have malware samples submitted to it for analysis
- **ANY.RUN:** online tool that offers the ability to upload a malware sample for analysis like any online sandbox**.**

100. Network and Profiling

- statistical <u>baseline information</u> that can serve as a reference point for normal network and device performance.

101. Elements of network profile:

- Session duration
- Total throughput
- Critical asset address space
- Typical traffic type

102. Elements of Server Profiling

- Listening ports
- Logged in users and accounts
- Service accounts
- Software environment

103. CVSS

- Common Vulnerability Scoring System (CVSS) is a risk assessment tool.
- designed to convey the common attributes and severity of vulnerabilities in computer hardware and software systems.
- CVSS helps prioritize risk.
- **FIRST** has been designated as the custodian of the **CVSS** to promote its adoption globally

104. CVE

- identifier provides a standard way to research a reference to vulnerabilities
- CVE Details **website** provides a linkage between CVSS scores and CVE information.

105. NVD

- utilizes CVE identifiers and supplies additional information on vulnerabilities such as CVSS threat scores, technical details, affected entities, and resources for further investigation.
- database was created and is maintained by the **U.S (NIST)**

106. Risk Management

- **Risk avoidance**: Stop performing the activities that create risk
- **Risk reduction**: Take measures to reduce vulnerability
- **Risk sharing:** Shift some risk to other parties.
- **Risk retention:** Accept the risk and its consequences.

107. Vulnerability Management

- **Discover:** Develop a network baseline. Identify security vulnerabilities on a regular automated schedule.
- **Prioritize Assets:** Categorize assets into groups or business units, and assign a business value based on their criticality to business operations
- **Assess:** Determine a baseline risk profile to eliminate risks based on asset criticality, vulnerability, threats, and asset classification.
- **Report: -** Measure the level of business risk associated with your assets according to your security policies. Document a security plan, monitor suspicious activity, and describe known vulnerabilities
- **Remediate:** Prioritize according to business risk and address vulnerabilities in order of risk.
- **Verify :** Verify that threats have been eliminated through follow-up audits.

108. Patch Management Techniques (Self Study)

- **Agent-based:**
- **Agentless Scanning:**
- **Passive Network Monitoring:**

109. Types of Security Data (NOTES)

- **Alert Data**
- **Session and Transaction Data**
- **Full Packet Captures**
- **Statistical Data**

110. Syslog Message Format

- “PRI (priority), HEADER, MSG (message text)”.
- The PRI consists of two elements, **the Facility** and **Severity**

- **Facility**: consists of sources that generated the message, such as the system, process, or application
- **Severity:** value from 0-7 that defines the severity of the message. **(Emergency- Alert- Critical- Error- Warning- Notice- Informational- Debug).**

“Priority = (Facility * 8) + Severity”

111. SIEM Functions

- Log collection
- Normalization
- Correlation
- Aggregation
- Reporting
- Compliance

112. Splunk

- A popular SIEM, which is made by a Cisco partner.

113. Tcpdump

- The tcpdump **command line tool** is a very popular **packet analyzer**
- It can display packet captures **in real time**.
- It captures detailed packet protocol and content data.
- **Wireshark** is a GUI built on tcpdump functionality.

114. NetFlow

- protocol that was developed by Cisco as a tool for network troubleshooting
  It records information about the packet flow including metadata
- NetFlow information can be viewed with tools such as the **nfdump.**

115. Application Visibility and Control (AVC)

- The Cisco Application system combines multiple technologies to recognize, analyze, and control over 1000 applications

116. Cisco Umbrella

- The Cisco Umbrella suite of security products apply **real-time threat intelligence** to managing **DNS access** and the security of **DNS records.**

117. Next-Generation Firewalls

- NexGen Firewalls are advanced devices that provided much more functionality than previous generations of network security devices.
- Common NGFW events include:

- Connection Event
- Intrusion Event
- Host or Endpoint Event
- Network Discovery Event
- Netflow Event

118. **Security Onion**

- open-source suite of Network Security Monitoring (NSM) tools that run on an Ubuntu Linux distribution
- provides three core functions for the cybersecurity analyst such as full packet capture and data types, network-based and host-based intrusion detection systems, and alert analyst tools.
- can be installed as a **standalone installation** or as **a sensor and server platform.**

119. **Detection Tools for Collecting Alert Data**

- **CapME:** This is a web application that allows viewing of pcap transcripts rendered with the tcpflow or Zeek tools
- **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.
- **Zeek:** Formerly known as Bro. This is a NIDS that uses more of a behavior-based approach to intrusion detection**.**
- **OSSEC**: This is a host-based intrusion detection system (HIDS) that is integrated into Security Onion**.**
- **Wazuh:** 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.
- **Suricata:** This is a NIDS that uses a signature-based approach. It can also be used for inline intrusion prevention.
-

120. **Analysis 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. Many data sources are available by pivoting directly from Sguil to other tools**.**
- **Kibana:** It is an interactive dashboard interface to Elasticsearch data. It allows querying of NSM data and provides flexible visualizations of that data. It is possible to pivot from Sguil directly into Kibana to see contextualized displays.
- **Wireshark:** It is a packet capture application that is integrated into the Security Onion suit. It can be opened directly from other tools and display full packet captures relevant to an analysis.

121. **five-tuples**
   - **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

122. **Alerts**
   - **NIDS:** Snort, Zeek, and Suricata
   - **HIDS :**OSSEC, Wazuh
   - **Asset management and monitoring**
   - **HTTP, DNS, and TCP transactions:** Recorded by Zeek and pcaps
   - **Syslog messages**

123. **Snort rule messages**
   - **GPL:** Older Snort rules can be downloaded from the Snort website, and it is included in Security Onion, it is not Cisco Talos certified.
   - **ET:** ruleset contains rules from multiple categories A set of ET rules is included with Security Onion.
   - **VRT:** rules are immediately available to subscribers, They are now created and maintained by Cisco Talos**.**

124. **Deterministic Analysis and Probabilistic Analysis**
   - **Deterministic Analysis -** For an exploit to be successful, all prior steps in the exploit must also be successful. The cybersecurity analyst knows the steps for a successful exploit.
   - **Probabilistic Analysis -** Statistical techniques are used to determine the probability that a successful exploit will occur based on the likelihood that each step in the exploit will succeed

125. **Core Components of ELK:**
   - **Beats:** Series of software plugins that send different types of data to the Elasticsearch data stores.
   - **Logstash:** Enables collection and normalization of network data into data indexes that can be efficiently searched by Elasticsearch**.**
   - **Elasticsearch:** An open-core platform for searching and analyzing an organization’s data in near real time**.**
   - **Kibana:** Provides a graphical interface to data that is compiled by Elasticsearch

126. **Data Normalization**
   - process of combining data from a number of sources into a common format.

127. Workflow Management

- Workflows are the sequence of processes and procedures through which work tasks are completed.

128. Managing the SOC workflows:

- Enhances the efficiency of the cyberoperations team
- Increases the accountability of the staff
- Ensures that all potential alerts are treated properly

129. Digital Forensics

recovery and investigation of information found on digital devices as it relates to criminal activity.

130. The Digital Forensics Process

NIST describes the four phases of the digital evidence forensic process

- **Collection**
- **Examination**
- **Analysis**
- **Reporting**

131. Types of Evidence

- **Direct Evidence:** eyewitness evidence from someone who directly observed criminal behavior
- **Indirect evidence:** This evidence establishes a **hypothesis** in combination with other facts (**circumstantial** evidence)
- **Best evidence:** This evidence could be storage devices used by an accused, or archives of files that can be proven to be unaltered**.**
- **Corroborating evidence:** This evidence supports an assertion that is developed from best evidence.

132. Chain of Custody

Chain of custody involves the collection, handling, and secure storage of evidence

133. **MITRE ATT&CK Framework**

- global knowledge base of threat actor behaviour
- The framework is designed to enable automated information sharing by defining data structures for exchanging information between its community of users and MITRE
- enables the ability to detect attacker's **Tactics**, **Techniques**, and **Procedures** (TTP) as a part of threat defense and attack attribution
- **Tactics:** the technical goals that an attacker must accomplish to execute an attack.
- **Techniques:** means by which the tactics are accomplished .
- **Procedures:** specific actions taken by threat actors in the techniques that have been identified

134. **Cyber Kill Chain**

- The Cyber Kill Chain was developed by Lockheed Martin to identify and prevent cyber intrusions

135. **Steps of Cyber Kill Chain**

- **Reconnaissance**
- **Weaponization**
- **Delivery**
- **Exploitation**
- **Installation**
- **Command and Control**
- **Actions on Objectives**

136. **NIST Incident Response Life Cycle**

- **Preparation:** members of the CSIRT are trained in how to respond to an incident
- **Detection and Analysis:** CSIRT quickly identifies, analyzes, and validates an incident
- **Containment, Eradication, and Recovery:** CSIRT implements procedures to contain the threat, eradicate the impact on organizational assets, and use backups to restore data and software**.**
- **Post-Incident Activities:** CSIRT documents how the incident was handled, recommends changes for future response, and specifies how to avoid a reoccurrence

Best Wishes/

Eng. Ahmed Youssef

Hope you great success in your entire life, and to be at the highest level of paradise at hereafter.