Charpter 4 – Quiz

1. Which tool can identify malicious traffic by comparing packet contents to known attack signatures?

- Nmap
- Netflow
- Zenmap
- IDS

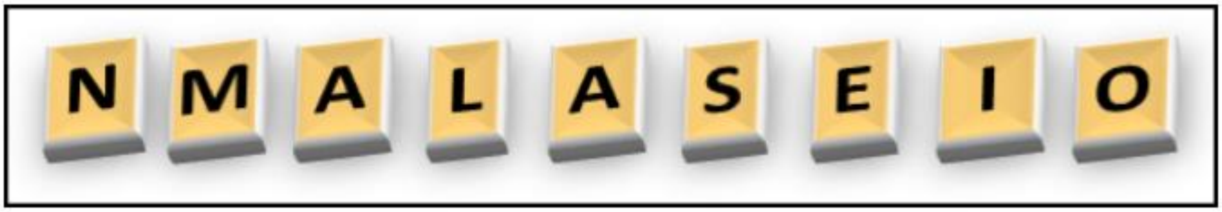
  Explanation:
  An IDS, or intrusion detection system, is a device that can scan packets and compare them to a set of rules or attack signatures. If the packets match attack signatures, then the IDS can create an alert and log the detection.

2. Fill in the blank.

A botnet is a group of compromised or hacked computers (bots) controlled by an individual with malicious intent.

Explanation:
A compromised or hacked computer that is controlled by a malicious individual or group is known as a bot. A group of these hacked computers under the control of a malicious individual or group is known as a botnet.

3. Refer to the exhibit. Rearrange the letters to fill in the blank.



Behavior-based analysis involves using baseline information to detect anomaly that could indicate an attack.

Noted: You should type “anomaly” in our system exam, but you can type one of the folowing answer with nedacad test system:

- anomalies
- anomaly

Explanation:
Behavior-based security uses informational context to detect anomalies in the network.

4. Which tool can perform real-time traffic and port analysis, and can also detect port scans, fingerprinting and buffer overflow attacks?

- Netflow
- Snort
- Nmap
- SIEM

Explanation:
Snort is an open source intrusion protection system (IPS) that is capable of performing real-time traffic and port analysis, packet logging, content searching and matching, as well as detecting probes, attacks, port scans, fingerprinting, and buffer overflow attacks.

5. What is the last stage of the Cyber Kill Chain framework?

- remote control of the target device
- creation of malicious payload
- gathering target information
- malicious action

Explanation:
The Cyber Kill Chain describes the phases of a progressive cyberattack operation. The phases include the following:

*Reconnaissance

*Weaponization

*Delivery

*Exploitation

*Installation

*Command and control

*Actions on objectives

In general, these phases are carried out in sequence. However, during an attack, several phases can be carried out simultaneously, especially if multiple attackers or groups are involved.

6. Fill in the blank.

Any device that controls or filters traffic going in or out of the network is known as a firewall

Explanation:
A firewall is a network device used to filter inbound or outbound traffic or both.

7. What type of attack disrupts services by overwhelming network devices with bogus traffic?

- brute force
- port scans
- zero-day
- DDoS

Explanation:
DDoS, or distributed denial of service, attacks are used to disrupt service by overwhelming network devices with bogus traffic.

8.Which protocol is used by the Cisco Cyberthreat Defense Solution to collect information about the traffic that is traversing the network?

- HTTPS
- Telnet
- NAT
- NetFlow

Explanation:
NetFlow is used both to gather details about the traffic that is flowing through the network, and to report it to a central collector.