IDS/IPS Analysis Questions

By: Ryan Stewart

Log Details

- **date:** Date information
- **time:** Time information
- **devname:** System name
- **devid:** System ID information
- **tz:** Timezone
- **logid:** Log ID information
- **type:** Log type
- **subtype:** Log subtype
- **level:** Log level
- **severity:** Incident severity level
- **srcip:** Source IP address
- **dstip:** Destination IP address
- **srccountry:** Source country
- **dstcountry:** Destination country
- **action:** Action information
- **service:** Service information
- **attack:** Attack details
- **srcport:** Source port information
- **dstport:** Destination port information
- **direction:** Direction of packet
- **attackid:** Attack ID information
- **msg:** Additional message information

Investigation Points

- Check the direction of the attack (inbound or outbound).
- Verify the event severity level.
- Examine different signature triggers between the same source and target.
- Confirm if the port/service specified in the attack detail is running on the target.
- Determine whether the action is just detection or blocked.

IDS/IPS logs contain critical information about source-target IPs, ports, action, attack type, category, and level.

Suspicious Activities Detected by IDS/IPS

- Port scanning activities
- Vulnerability scans
- Code Injection attacks
- Brute-Force attacks
- Dos/Ddos attacks
- Trojan activities
- Botnet activities

Quiz Results

IDS and IPS Functions

Quiz Results: IDS is a system that ……. the attacks. IPS is a system that ……. the attacks.

Fill in the blanks.

- A) prevent - detect
- B) detect - prevent
- C) detect - detect
- D) prevent - prevent

{"timestamp":"2022-06-13T08:25:36", "in_iface":"ens1f1", "event_type":"alert","vlan":1,"src_ip":"192.168.1.11",
"src_port":53,"dest_ip":"172.16.2.25", "dest_port":1029,"proto":"UDP", "alert":{"action":"allowed", "gid":1, "signature_id":2811577,
"rev":3, "signature":"ETPRO TROJAN Possible Virut DGA NXDOMAIN Responses", "category":"A Network Trojan was detected",
"severity":1, "metadata":{"updated_at":["2021_09_22"],"created_at":["2015_06_18"]}}, "app_proto":"failed"},
"payload":"dnV5ZWltLmNvbQo=", "payload_printable":"vuyeim.com", "stream":0}

IDS/IPS Log Analysis

Questions:

1. What is the IP address related to the malicious domain? -172.16.2.25

2. Which of the following is a true statement?

- A) The request is blocked by the firewall.
- B) The related IDS has caught the DNS request in the return traffic.
- C) The category of the IDS rule is in the "DNS attack" category.

IDS/IPS Alarm Outputs

Which of the following information is normally **not included** in the IDS/IPS alarm outputs?

- A) Payload information
- B) IP and Port information
- C) Parent process information
- D) Action information
- E) Signature information

IDS Log Analysis

Answer the following questions according to the above-referenced IDS log:

1. Which of the following is **not** correct?

A) The system making malicious domain requests may be infected.
B) The relevant domain has not been accessed.
C) The DNS server has responded to the domain request.
D) The domain categorized as DGA is vuyeim.com.

Note: Always analyze IDS/IPS logs thoroughly to ensure accurate interpretation and effective response to potential security threats.