Network Security Essentials

User Workstations (Endpoint)
- most common entry point for attackers, via phishing email or malicious downloads

Endpoint logs can reveal malicious processes, but network logs may first show C2 connections

File & Database Servers

Network visibility is essential in security.
- security analysts can't defend what we can not see

Two main categories of log sources.

Host-Centric logs: generated by individual devices (hosts) on the network, such as servers, workstation and laptops. These logs give us a detailed ground level view of what's happening in the machine.

Key Host-Centric Log Sources:

- operating system Logs: Windows Event Logs, Linux (syslog), macOS logs. These record events like user logons, process creation, service startups, and failed login attempts

- Application Logs : Logs from software running on the host, such as webservers, databases and other application

- Security Tool Logs : Logs from antivirus software, Endpoint Detection and Response (EDR) agents, and host-Based intrusion detection system (HIDS)

Network Centric Logs.

- tells us what is happening Between devices. These are generated by network appliances that sit on the network and monitor the traffic flowing through them

Key Network - Centric - Log Sources :

- Firewalls
- Intrusion Detection/Prevention System (IDS/IPS) → signature Behaviour
- Routers and switches
- Web proxies
- Vpn

Network Perimeter

- Boundary that seperates internal network from external network, or internet. It is the point where data enters or leaves the network

The Perimeter

→ is defined by hardware devices at the edge of the network, it also includes (virtual gateway, cloud connections, and remote access points)

Common components:

- Firewalls → filter traffic
- Routers/Gateways → Devices that route traffic and enforce access rules
- Demilitarized zone (DMZ) → network segment where public facing servers are placed.
- Remote Access Gateways/VPN → secure end point

Network Perimeter in a Small Enterpise

- A firewall sits between the Internet and the internal LAN
- Webserver placed in DMZ
- Internal Server live behind firewall and are accessible only to employees
- Outside employees connect through VPN gateway.

The perimeter is the first line of defense

Network Perimeters : Monitoring and Protecting

Question 1 :

Examine the firewall logs. Which IP address is performing the port scan?

203.0.113.10 (Because trying out every connection in short item. Trying establish TCP handshake with everyport)

In the WAF logs, which single source IP is responsible for all the blocked web attacks?

198.51.100.12 (no authorized, tried SQL injection)

In the VPN logs, how many brute-force attempts failed.

90

Which suspicious IP address was found attempting the brute-force attack against the VPN gateway?

45.137.22.13

Perimeter Logs: Investigating the Breach

Questions

1) Examine the firewall logs. What external IP performed the most reconnaissance?

```
cat firewall.log | grep "Block" | head
```

2) In the firewall log, which internal host was targeted by scans?

10.0.0.20

3) Which username was targeted in VPN logs?

svc_backup (brute force)

4) What internal IP was assigned after successful VPN login?

10.8.0.23 (brute force found success)

5) Which port was used for lateral SMB attempt?

```
cat ids_alerts.log | grep "Lateral Movement" | head
```

6) In the IDS logs, which host beaconed to the C2?

```
cat ids_alerts.log | grep "C2" | head
```

During the investigation, which IP was observed to be associated with C&?

198.51.100.77

Which host showed the exfiltration attempts?

cat ids_alerts.log | grep "Exfiltration" | head