GEN NORTON – INTERVIEW SIMULATION (Endpoint Security Focus)

Level 1 – Technical Basics

1. Explain the difference between Antivirus, EDR, and XDR.
2. What is a **malicious process**? How do you identify one in Windows?
3. What is a **false positive**? Give an example related to malware alerts.
4. Explain signature-based vs behaviour-based detection.
5. What is a **hash value**? Why do we use hashing in cybersecurity?
6. What is a **quarantine folder** and how does it work?
7. What is the difference between **virus, worm, trojan, ransomware**?
8. Explain **IoC** with an example (file hash / domain / registry change).
9. What is a **sandbox**? Why is it used?
10. How does a **ransomware attack** typically start and spread?

Level 2 – Endpoint & Malware Scenarios (Most Important)

Scenario 1 – Suspicious CPU Spike

A user reports that their system is unusually slow and Task Manager shows a process using 90% CPU. What steps will you take?

Expected points:

- Identify process → verify path → check signature → cross-check with hash → look for network connections → isolate if required.

Scenario 2 – Malware Detected

Norton blocks a file as “Trojan.Gen”. The user insists it's safe. How will you validate?

Expected points:

- Check file hash → check reputation → scan in sandbox → research threat → check behavior logs → allow only if confirmed safe.

Scenario 3 – Suspicious Email Attachment

A user opened an email PDF and nothing happened, but later system is lagging. What next?

Expected points:

- Check logs → inspect running processes → check startup entries → run full system scan → review event viewer → isolate if needed.

Scenario 4 – Unwanted Browser Redirects

User browsing redirects to unknown sites. What steps to investigate?

Points:

- Check browser extensions → DNS settings → hosts file → suspicious software → run malware scan.

Scenario 5 – Multiple Endpoint Alerts

You see alerts from 10 machines in the same subnet. What does it indicate?

Possible answers:

- Lateral movement
- Worm propagation
- Common malicious email
- Shared drive infection

Level 3 – Tools / Log Analysis

1. Read this Event Log snippet → What does it indicate?
2. How do you use **Process Explorer** to identify malicious behavior?
3. How do you identify persistence mechanisms? (registry → startup → services)
4. How do you isolate a compromised system?