National Forensic Sciences University

Knowledge | Wisdom | Fulfilment

An Institution of National Importance
(Ministry of Home Affairs, Government of India)

Operation Technology (OT) Security

Top 50 Questions and Answers

Placement Cell, NFSU Goa

January 31, 2025

Operation Technology - Top 50 Questions

1. **What is OT Security?**
   OT Security focuses on protecting industrial control systems (ICS) and operational technology from cyber threats, ensuring the safety and continuity of critical infrastructure.

2. **What are ICS systems?**
   ICS (Industrial Control Systems) are used to monitor and control industrial processes such as manufacturing, power generation, and water treatment.

3. **What is the main difference between IT and OT security?**
   IT security focuses on information systems, while OT security focuses on securing the physical systems that control industrial operations.

4. **What are the key challenges in OT security?**
   Challenges include legacy systems, network integration with IT, a lack of skilled professionals, and ensuring minimal disruption to operations during security updates.

5. **Why are OT systems vulnerable?**
   OT systems are often outdated, lack proper cybersecurity measures, and were not originally designed with modern cyber threats in mind.

6. **What is a SCADA system?**
   SCADA (Supervisory Control and Data Acquisition) systems are used to monitor and control processes in industries like electricity, water, and manufacturing.

7. **What is network segmentation in OT security?**
   Network segmentation separates OT networks from IT networks, reducing the risk of a breach affecting both environments.

8. **What is an air-gap network?**
   An air-gap network is a physical isolation between OT and IT networks to protect OT systems from remote cyber-attacks.

9. **How can legacy OT systems be secured?**
   Legacy OT systems can be secured through network segmentation, firewalls, patch management, and adding cybersecurity layers like IDS/IPS.

10. **What is a threat landscape in OT security?**
    The threat landscape includes various cyber threats such as malware, insider attacks, physical breaches, and denial-of-service attacks targeting OT systems.

11. **What role does encryption play in OT security?**
    Encryption ensures that data transmitted across networks is secure and cannot be easily intercepted or tampered with by malicious actors.

12. **What is a zero trust security model?**
    Zero trust assumes that every access request is a potential threat and enforces strict authentication and authorization checks for every user and device.

13. **Why is physical security important in OT?**
    Physical security protects critical hardware from tampering, theft, and sabotage, which can have direct impacts on OT operations.

14. **What are common OT vulnerabilities?**
Common vulnerabilities include outdated software, weak access controls, insecure communication protocols, and lack of segmentation between IT and OT.

15. **What is penetration testing in OT security?**
Penetration testing involves simulating cyberattacks on OT systems to identify vulnerabilities before malicious actors exploit them.

16. **What is a ransomware attack in OT?**
Ransomware attacks encrypt critical data in OT systems, rendering them inoperable until a ransom is paid.

17. **How do you monitor OT networks for security threats?**
OT networks can be monitored using intrusion detection systems (IDS), security information and event management (SIEM) tools, and continuous traffic analysis.

18. **What is remote access in OT, and why is it risky?**
Remote access allows authorized personnel to control OT systems from a distance but can be exploited by attackers if not secured properly.

19. **What is the role of firewalls in OT security?**
Firewalls are used to filter incoming and outgoing network traffic, helping to protect OT systems from unauthorized access and cyber threats.

20. **What is multi-factor authentication (MFA) in OT?**
MFA requires users to provide two or more verification factors (e.g., password and biometrics) to access OT systems, strengthening security.

21. **What is the significance of patch management in OT?**
Regular patching helps address known vulnerabilities in OT systems, reducing the risk of exploitation by attackers.

22. **What is a cyber-physical attack?**
A cyber-physical attack targets both digital and physical components of OT systems, potentially disrupting operations and causing physical damage.

23. **What are advanced persistent threats (APTs) in OT?**
APTs are prolonged and targeted cyberattacks where attackers gain unauthorized access to OT networks and remain undetected for an extended period.

24. **How can supply chain vulnerabilities affect OT security?**
Supply chain vulnerabilities, such as compromised software or hardware, can introduce malware or insecure components into OT systems.

25. **What is a distributed denial-of-service (DDoS) attack in OT?**
A DDoS attack floods OT systems with traffic, overwhelming them and causing service disruptions, potentially affecting critical operations.

26. **What is an IDS in OT security?**
An Intrusion Detection System (IDS) monitors OT networks for signs of malicious activity and alerts administrators when suspicious activity is detected.

27. **What is the difference between OT and IT security protocols?**
OT security protocols focus on protecting critical infrastructure systems, while IT security protocols primarily protect data and IT systems from digital threats.

28. **How do you mitigate insider threats in OT?**
Mitigating insider threats involves monitoring user activities, applying access controls, training employees, and using behavioral analytics tools.

29. **What is security patching in OT systems?**
Security patching involves applying updates to OT software and hardware to fix vulnerabilities and improve system protection against cyber threats.

30. **How does IoT affect OT security?**
IoT devices introduce new vulnerabilities into OT systems by increasing the number of potential entry points for cybercriminals.

31. **What is the role of vulnerability management in OT security?**
Vulnerability management involves identifying, assessing, and remediating vulnerabilities within OT systems to prevent exploitation by attackers.

32. **What are security policies in OT?**
Security policies in OT define the rules and guidelines for securing OT networks and systems, including access control, incident response, and patching protocols.

33. **What is the impact of a cyberattack on OT systems?**
A cyberattack on OT systems can lead to operational disruptions, financial loss, reputational damage, and even physical harm or environmental hazards.

34. **What is segmentation in OT networks?**
Segmentation involves dividing OT networks into smaller sections to limit the impact of a potential security breach and to isolate critical systems.

35. **How do you manage risk in OT security?**
Risk management in OT security involves assessing threats, vulnerabilities, and impacts, and implementing mitigation strategies to protect critical assets.

36. **What is a cyberattack surface in OT?**
The cyberattack surface includes all potential points of entry into an OT system, such as network connections, software vulnerabilities, and physical access points.

37. **What is OT security compliance?**
OT security compliance refers to adherence to industry standards and regulations (e.g., NIST, ISA/IEC 62443) designed to protect critical infrastructure from cyber threats.

38. **What is data loss prevention (DLP) in OT?**
DLP refers to technologies and strategies used to monitor and prevent unauthorized access, use, or transmission of sensitive data within OT systems.

39. **What are best practices for securing remote access in OT?**
Best practices include using VPNs, multi-factor authentication, and strict access controls to limit and monitor remote access to OT systems.

Operation Technology - Top 50 Questions

40. **What is a patch management policy for OT?**
A patch management policy ensures that OT systems are regularly updated with security patches to address vulnerabilities without disrupting operations.

41. **What is a man-in-the-middle (MITM) attack in OT?**
A MITM attack involves intercepting and altering communications between two OT systems, potentially compromising data integrity or control.

42. **How do you secure control networks in OT?**
Securing control networks involves network segmentation, implementing firewalls, using intrusion detection systems (IDS), and regular security audits.

43. **What is threat hunting in OT security?**
Threat hunting in OT involves proactively searching for signs of malicious activity or vulnerabilities within the network before they can cause damage.

44. **What is incident response in OT security?**
Incident response in OT security involves preparing for, detecting, and responding to security incidents in OT systems to minimize the impact of attacks.

45. **What is a security operations center (SOC) in OT?**
A SOC in OT monitors and analyzes security events across OT environments, detecting and responding to threats in real-time.

46. **What is endpoint security in OT?**
Endpoint security in OT involves securing devices (e.g., controllers, workstations) that interact with industrial control systems from malware and unauthorized access.

47. **How do you test OT system security?**
OT system security testing involves penetration testing, vulnerability scanning, and risk assessments to identify potential threats and weaknesses.

48. **What is cybersecurity insurance for OT systems?**
Cybersecurity insurance for OT systems helps cover costs related to data breaches, cyberattacks, and operational disruptions in critical infrastructure.