1. Describe the purpose of the Govern (GV) function in establishing a network security posture. Using a Service Provider (ISP) as an example, illustrate how GV.RM (Risk Management Strategy) defines the threshold for "acceptable" latency versus packet loss during a DDoS mitigation event, and how these influences Protect (PR)configurations like Rate Limiting.

2. Describe the Identify (ID) function with a focus on Asset Management (ID.AM). Explain how using a network scanner (e.g., Nmap or Nessus) to discover "Shadow IT" (unauthorized switches or IoT devices) informs the Risk Assessment process and triggers specific VLAN tagging or port security actions in the Protect (PR) function.

3. Outline the Protect (PR) and Detect (DE) functions. Focus on Identity and Access Management (IAM) and Security Continuous Monitoring (DE.CM). In a scenario where an IDS/IPS flags a "North-South" traffic spike (e.g., 5GB of encrypted data leaving the network at 3 AM), discuss how this differs from static firewall rules (PR) and how it leads to Respond (RS) activities.

4. Discuss the Respond (RS) and Recover (RC) functions. Provide a technical example of Mitigation (RS.MI) by black holing a compromised IP address on a router, followed by an RC.RP (Recovery Planning) session to implement Infrastructure as Code (IaC) for faster automated redeployment of clean network configs.

5. After a corporate merger that integrates two disparate Autonomous Systems (AS), what is the immediate priority for the network governance team under GV.OC (Organizational Context)? Specify how defining the unified "Trust Boundary" guides the integration of new routing tables and firewall policies.

6. Explain the three contexts of NIST SP 800-160 (Problem, Solution, Trustworthiness). Provide an example of defining stakeholder needs for a Military-grade VPN in the Problem Context, emphasizing why "Security by Design" is critical for preventing side-channel attacks.

7. Describe the Solution Context in NIST SP 800-160. Using the design of a DMZ (Demilitarized Zone) for a public web server, explain how the choice of a Triple-Homed Firewall architecture addresses the requirement of network isolation defined in the Problem Context.

8. Outline the Trustworthiness Context. Discuss the role of Security Authorization (A&A) and penetration testing in proving that a newly implemented Zero Trust Architecture (ZTA) actually restricts lateral movement as intended.

9. A network team wants to deploy a Software-Defined Network (SDN) immediately. What critical step involving Threat Modeling must occur in the Problem Context before the control plane is configured? Discuss the risks of an unauthenticated controller.

10. A monitoring system flags a vulnerability in a core Layer 3 Switch. Describe the systematic process triggered (Risk Assessment → Solution Context patching → Trustworthiness verification) and explain why traceability between the security requirement and the firmware version is essential.

11. Explain A01:2025 Broken Access Control. In a network administration context, discuss how a failure to implement Role-Based Access Control (RBAC) on a router's Management Interface (SSH) could lead to an unauthorized user gaining "Enable" or "Root" privileges.

12. Describe A03:2025 Software Supply Chain Failures. Focus on the risks of using unverified Firmware or Docker Images in a production environment. Provide an example of a compromised "npm" package and how Software Composition Analysis (SCA) mitigates this.

13. Discuss A05:2025 Injection. While usually associated with web forms, explain how Command Injection can occur in a network device's web-based GUI (e.g., a ping-test utility) and how input sanitization prevents it.

14. Explain A10:2025 Mishandling of Exceptional Conditions. Describe a scenario where a Stateful Firewall runs out of memory (RAM) and "Fails Open" (allowing all traffic). Discuss mitigations such as Resource Quotas and High Availability (HA) pairs.

15. A network uses an outdated SSL/TLS library on its VPN concentrator. Identify which OWASP category this falls under (A03: Software Supply Chain Failures) and discuss the mitigation steps, including Virtual Patching via a WAF or IPS.

16. Explain the MITRE ATT&CK Enterprise Matrix. Describe the Reconnaissance tactic (TA0043) specifically using Active Scanning (T1595). How does an adversary use "Port Scanning" to map the network attack surface?

17. Describe the Initial Access tactic (TA0001). Focus on Exploit Public-Facing Application (T1190) (e.g., an unpatched VPN portal). List the risks to the internal network and mitigations like Network Segmentation.

18. Outline the Persistence tactic (TA0003). Discuss how an adversary might use a Scheduled Task (T1053) or a hidden VPN Tunnel to maintain access. Explain how this differs from the initial breach.

19. Discuss Privilege Escalation (TA0004) in a Windows Domain environment. Provide an example of Token Impersonation (T1134) and how it allows a standard user to become a Domain Admin. Recommend mitigations such as Credential Guard.

20. Scenario Analysis: An adversary performs LLMNR/NBT-NS Poisoning (T1557.001) (Reconnaissance/Access), followed bypass-the-Hash (T1550.002) (Lateral

Movement). Map these to their tactics, explain the network-level sequence, and recommend defenses like disabling LLMNR and enforcing SMB Signing.