## ? EASY (10 Questions)

**Q1.** What is the primary purpose of Network Load Balancing (NLB)?
A. Data encryption
B. Distribute client traffic across servers
C. Backup servers
D. DNS resolution

**Q2.** Which Windows feature provides built-in load balancing?
A. Failover Clustering
B. NLB
C. Hyper-V Replica
D. DFS

**Q3.** Which OSI layer does NLB primarily operate on?
A. Layer 2
B. Layer 3
C. Layer 4
D. Layer 7

**Q4.** Which NLB mode uses a shared MAC address?
A. Multicast
B. Unicast
C. Anycast
D. Broadcast

**Q5.** Which Windows security feature protects against malware?
A. Windows Defender
B. DHCP
C. NLB
D. IPAM

**Q6.** What is the default firewall in Windows 10/11?
A. Norton Firewall
B. Windows Firewall
C. IPsec only
D. UFW

**Q7.** Which component stores user credentials in AD?
A. SYSVOL
B. NTDS.DIT
C. Registry
D. Event Logs

**Q8.** Which security principle limits user permissions?
A. Full control

B. Least privilege
C. Role explosion
D. Trust delegation

**Q9.** Which NLB configuration requires a dedicated NIC?
A. Multicast
B. Unicast
C. IGMP
D. Virtual

**Q10.** Which Windows feature encrypts disk data?
A. EFS
B. BitLocker
C. IPsec
D. NTFS ACL

---

## □ MEDIUM (15 Questions)

**Q11.** Which NLB component distributes traffic using hashing?
A. Cluster IP
B. Port rules
C. Host priority
D. Affinity

**Q12.** Which affinity mode keeps client requests on the same server?
A. None
B. Single
C. Network
D. Random

**Q13.** Which scenario best suits NLB?
A. Database clustering
B. Web servers
C. File servers
D. Domain controllers

**Q14.** Which Windows security feature isolates applications?
A. AppLocker
B. Credential Guard
C. Device Guard
D. Sandbox

**Q15.** Which AD attack exploits excessive privileges?
A. Phishing

B. Privilege escalation
C. ARP poisoning
D. DNS tunneling

**Q16.** Which tool enforces application whitelisting?
A. BitLocker
B. AppLocker
C. Defender
D. NLB

**Q17.** Which NLB limitation exists compared to failover clustering?
A. No scalability
B. No stateful failover
C. No redundancy
D. No security

**Q18.** Which Windows feature protects LSASS credentials?
A. Secure Boot
B. Credential Guard
C. EFS
D. SmartScreen

**Q19.** Which attack targets NTLM hashes?
A. Pass-the-Hash
B. Golden Ticket
C. SQL Injection
D. DoS

**Q20.** Which protocol secures network traffic at OS level?
A. SSL
B. TLS
C. IPsec
D. FTP

**Q21.** Which NLB setting defines traffic handling priority?
A. Port rule priority
B. Host priority
C. Cluster name
D. Affinity

**Q22.** Which security practice prevents lateral movement?
A. Single admin account
B. Tiered admin model
C. Shared passwords
D. Disabled auditing

**Q23.** Which Windows feature logs security events?
A. Task Scheduler
B. Event Viewer
C. Performance Monitor
D. Services

**Q24.** Which service must run for BitLocker network unlock?
A. DNS
B. DHCP
C. Windows Deployment Services
D. TPM

**Q25.** Which firewall rule type allows only specific traffic?
A. Allow all
B. Block all
C. Inbound allow rule
D. Outbound deny rule

---

## 🟥 HARD (15 Questions)

**Q26.** Why is NLB not recommended for stateful applications?
A. Low bandwidth
B. No session persistence by default
C. Poor encryption
D. Limited nodes

**Q27.** Which NLB mode can cause switch flooding?
A. IGMP multicast
B. Multicast
C. Unicast
D. VLAN

**Q28.** Which AD security risk arises from stale admin accounts?
A. Disk failure
B. Unauthorized access
C. DNS corruption
D. Replication delay

**Q29.** Which Windows security feature enforces kernel-mode code integrity?
A. AppLocker
B. Device Guard
C. BitLocker
D. Defender

**Q30.** Which misconfiguration commonly weakens AD security?
A. DNS scavenging
B. Excessive group membership
C. Multiple DCs
D. SYSVOL replication

**Q31.** Why should NLB nodes be monitored continuously?
A. Licensing compliance
B. Detect node failure and imbalance
C. Improve DNS
D. Increase storage

**Q32.** Which attack exploits forged Kerberos tickets?
A. Pass-the-Hash
B. Golden Ticket
C. Brute force
D. DoS

**Q33.** Why is SMB signing recommended?
A. Faster file access
B. Prevent MITM attacks
C. Reduce bandwidth
D. Improve compression

**Q34.** Which Windows feature restricts credential theft during boot?
A. Secure Boot
B. BitLocker
C. Defender
D. Firewall

**Q35.** Which NLB configuration improves multicast efficiency?
A. Disable affinity
B. Enable IGMP
C. Use unicast only
D. Single NIC

**Q36.** Why should services not run as Domain Admin?
A. Slower performance
B. Increased attack surface
C. License violation
D. Backup issues

**Q37.** Which Windows security log tracks logon failures?
A. Application
B. System

C. Security
D. Setup

**Q38.** Which practice improves enterprise Windows hardening?
A. Disable updates
B. Baseline security templates
C. Shared admin passwords
D. Disable firewall

**Q39.** Which high-availability alternative provides true failover?
A. NLB
B. DNS round robin
C. Failover clustering
D. IPAM

**Q40.** Which combined approach best secures Windows servers?
A. Antivirus only
B. Firewall only
C. Defense-in-depth
D. Open access