1. Discuss the role of Windows Firewall in Windows Server and how to configure it.

ANS-Windows Firewall in Windows Server acts as a host-based firewall,
Filtering inbound/outbound traffic based on rules to enhance security. It blocks unauthorized access,
Allows essential services (e.g., RDP, HTTP), and supports stateful inspection, logging,
And integration with Group Policy for domain-wide control. It operates in three profiles: Domain, Private, Public.
Configuration steps:

(a)Open Windows Defender Firewall with Advanced Security (wf.msc).
(b)Enable firewall for desired profiles.
(c)Create Inbound/Outbound Rules: Specify program/port/protocol/action (allow/block).
(d)Use Predefined rules for common services (e.g., File Sharing).
(e)Apply via netsh advfirewall commands or PowerShell (New-NetFirewallRule).
(f)Monitor via Event Viewer (Microsoft-Windows-Windows Firewall).

2. What is Network Address Translation (NAT) in Windows Server, and how do you configure it?

ANS-Network Address Translation (NAT) in Windows Server enables multiple internal devices to share a public IP using the
Routing and Remote Access Service (RRAS).
It translates private IPs to public ones for outbound traffic and routes responses back,
Conserving IPs and hiding internal topology.
Configuration steps:

(a)Install RRAS role via Server Manager.
(b)Run Routing and Remote Access console (rrasmgmt.msc).
(c)Right-click server → Configure and Enable Routing and Remote Access → Select NAT.
(d)Choose public interface (internet-facing NIC).
(e)Select private interface; enable Basic firewall.
(f)Configure services (e.g., DNS/DHCP forwarding if needed).

3. Explain the concept of Dynamic Host Configuration Protocol (DHCP) and how to configure it in Windows Server 2016.

ANS-Dynamic Host Configuration Protocol (DHCP) automatically assigns IP addresses, subnet masks, gateways,
DNS servers, and other settings to clients, reducing manual configuration and preventing conflicts.
Configuration in Windows Server 2016:

(a)Install DHCP Server role via Server Manager.
(b)Run Post-install: Authorize server in Active Directory (dhcpmgmt.msc).
(c)Create a Scope: Right-click IPv4 → New Scope → Define IP range (e.g.,

192.168.1.100–200), exclusions,
Lease duration (default 8 days).
(d)Configure Scope Options: 003 Router, 006 DNS Servers, 015 Domain Name.
(e)Activate scope.
(f)Use PowerShell: Add-DhcpServerv4Scope -Name "LAN" -StartRange 192.168.1.100 -EndRange 192.168.1.200 -SubnetMask 255.255.255.0.

4.Describe the process of configuring DNS (Domain Name System) in Windows Server.

ANS-
DNS resolves hostnames to IPs and vice versa, enabling name-based network access.

Configuration in Windows Server:

(a)Install DNS Server role via Server Manager.
(b)Open DNS Manager (dnsmgmt.msc).
(c)Create Forward Lookup Zone (Primary/AD-integrated): Right-click → New Zone → Define zone name (e.g., corp.example.com).
(d)Add records: A (host IP), CNAME (alias), MX (mail), SRV (services).
(e)For reverse: New Reverse Lookup Zone → Enter network ID (e.g., 192.168.1).
(f)Configure Forwarders (Root Hints or ISP DNS) for external resolution.
(g)Enable DNSSEC for security if needed.

5. What is Server Manager, and how do you use it to manage servers in Windows Server?

ANS-Server Manager is a central MMC console in Windows Server for managing local and remote servers from one interface.
Usage:

(a)Open Server Manager (auto-starts or via Start menu).
(b)Add servers: Manage → Add Servers → Find by name/IP/DNS; import from AD.
(c)View Dashboard for alerts, performance, events.
(d)Manage Roles/Features: Select server → Add/Remove Roles (e.g., AD DS, DHCP).
(e)Monitor Events, Services, Performance per server.
(f)Run Best Practices Analyzer (BPA) for compliance.
(g)Group servers into Server Pools for bulk actions.

6. Discuss the role of Remote Desktop Services (RDS) in Windows Server 2016 or 2019 and how to configure it.

ANS-Remote Desktop Services (RDS) in Windows Server 2016/2019 enables centralized desktop/app delivery via RD Session Host,
RD Gateway, RD Web Access, and RD Licensing.
Configuration steps:

(a)Install RDS role via Server Manager.
(b)Run Add Roles Wizard: Select Quick Start (single server) or Standard Deployment.
(c)Deploy: Session Host (hosts sessions), Connection Broker (load balancing), Web

Access (HTML5 portal),
Gateway (secure external access).
(d)Create Session Collection: Publish RemoteApps/Desktops.
(e)Install RDS CALs in RD Licensing Manager.
(f)Configure Group Policy: Enable RDP, set security (NLA).
(g)Use PowerShell: New-RDSessionDeployment.