Is this part of AD or not — Sanitized (Exam-safe)

Note: This is a sanitized, exam-safe triage reference. It contains generic commands, a port→service table, and high-level checks for identifying Active Directory environments. All walkthroughs, PoCs, external links, and machine-specific identifiers have been removed.

Step 1: Initial Nmap Scan (quick triage)

```
nmap -sC -sV -Pn -T4 -oN scan.txt <IP>  # fast service/version scan
```

Step 2: Common ports → service → AD relevance (triage table)

Port	Service	AD relevance / notes
53	DNS	May indicate DNS; often present on Domain Controllers
88	Kerberos	AD-related; Kerberos traffic typically on DCs
135	RPC	Windows RPC - useful indicator of Windows host
139	NetBIOS-SSN	Legacy Windows sharing (NetBIOS)
389	LDAP	AD-related directory service
445	SMB	Windows file sharing; often on DCs or Windows hosts
3268	GlobalCatalog	Global Catalog service usually on DCs
5985/5986	WinRM	WinRM (HTTP/HTTPS) often present in AD environments; useful for post-exploitation if credentials a

Step 3: Hostname & Domain Detection (high-level checks)

- Check NetBIOS/SMB info and share names for NETLOGON, SYSVOL (indicates DC)
- Look for domain-like hostnames (examples: containing 'corp', 'domain', or common DC naming patterns)
- Enumerate visible shares and directory names (document findings)
- Record any domain names returned by directory/hostname queries

Step 4: Kerberos responsiveness (indicator)

- Probe Kerberos port (88) to check if the service is responding. A response suggests Kerberos is active (likely AD).
- If Kerberos responds, prioritize AD-focused enumeration checks.

Step 5: Logic & Indicators

- Multiple Windows hosts + domain names + LDAP/Kerberos => Likely Active Directory environment
- Single machine, no domain signs, no Kerberos/LDAP => Likely standalone Windows host
- Presence of NETLOGON or SYSVOL shares is a strong DC indicator

Fast rule-of-thumb

Multiple Win boxes + domain names + LDAP/88 => Active Directory
Only one target + no domain signs => Standalone

Source: user-provided notes, sanitized for exam use. This file contains only generic triage guidance and command templates; no walkthroughs, PoCs, or machine-specific identifiers are included.