CyberArk DNA Scanner – Setup & Analysis Documentation

1. CyberArk DNA Overview & Purpose

CyberArk DNA (Discovery & Audit) scans systems (Windows/Linux) to uncover privileged accounts, misconfigurations, SSH keys, and vulnerabilities. It identifies credential exposure risks and produces visual maps and summary reports.

Reference: CyberArk DNA Datasheet

2. Licensing & Scope

DNA requires a valid license with limited usage on Windows/Linux machines. It is run from a network-reachable host using a standalone executable.

Reference: CyberArk Documentation

3. Deployment and Input Options

- Active Directory (OU-based) discovery
- Manual host/IP import using CSV

4. Network and Firewall Requirements

For Windows scans, the following ports must be allowed: 88, 135, 137, 138, 389, 445, 49153–49156.

ICMP (ping) is optional. DNS resolution and protocol-level access (WMI/SMB) are mandatory.

Reference: DNA Ports and Protocols

5. Authentication and Privileges

Windows: Domain admin account

Linux: SSH-based access with sudo/root rights

Credential format: Provided through the DNA tool during scanning.

6. AWS/Azure Considerations

Cloud servers (e.g., EC2) must be domain-joined for AD-based scans.

Reference: AWS EC2 DNA Requirements

7. Timeout Configuration & Troubleshooting

Modify timeouts in configuration for resolving common errors (DNAPR199E, etc).

References:
- DNA Error Reference

8. Test Plan Outline

1. Install DNA tool on test machine
2. Import test AWS servers (OU or CSV)
3. Validate port access
4. Ensure DNS connectivity
5. Use valid domain/SSH credentials
6. Run test scan and collect data
7. Compare with BeyondTrust output
8. Report and recommend next steps

9. References for Further Reading

- CyberArk Datasheet
- DNA Error Codes
- Required Ports
- Cloud Scanning Requirements