CyberArk DNA™ Technical FAQ

Version 8.1

DNAFAQ 8.1 10/9/2018

What is CyberArk DNA?

CyberArk DNA™ (DNA) is an innovative standalone discovery and audit tool that automatically scans an organization’s network, typically a complex, manual process, for the following:

- Data related to privileged and non-privileged accounts
- Embedded and Hard-coded application credentials
- SSH key exposure
- Potential credential theft risks, including Pass-the-Hash attacks, Pass-the-Ticket and Overpass-the-Hash

The easy-to-use scanner automatically discovers and analyzes any privileged and non-privileged account, then generates a report and visual organizational maps that evaluate the privileged account security status in the organization.

Does CyberArk DNA require a license?

CyberArk DNA requires a license to run. Licenses may limit the number of computers to scan per scan, and include an expiration date.

What technology does CyberArk DNA use?

CyberArk DNA was developed using Microsoft's .NET Framework and designed as a multi-threaded application to expedite scanning.

What does CyberArk DNA scan?

Accounts

CyberArk DNA scans Windows and Unix/Linux/Mac computers. DNA scans each computer and maps the users who can access it, including local and domain users.

On Windows machines, DNA also scans service accounts used in:

- Windows Services Accounts
- Windows Scheduled Tasks

Embedded and Hard-coded Credentials

CyberArk DNA discovers hard-coded credentials in:

- The configuration of data sources in WebSphere and WebLogic servers (on Unix only)
- Connection strings in IIS servers
- Ansible Playbooks (on Unix only)
- Embedded Windows service account credentials
- MSSQL databases
- DevOps

Examples of locations where embedded Windows service account credentials may be found:

- Windows Services Accounts
- Windows Scheduled Tasks
- IIS Application Pool
- IIS Anonymous Authentications
- …and more

SSH Keys

CyberArk DNA discovers Private and Public SSH Keys, and correlates the keys to the relevant accounts discovered in the “Account Scan”.

DNA analyzes all possible SSH Key Trusts to show which account on a certain machine can connect to what account on a remote machine. Using this information, DNA creates an interactive organizational trust map that displays all possible trusts.

Pass-the-Hash Vulnerability

CyberArk DNA detects stored Privileged account password hashes (representations of the password itself). DNA analyzes and presents computers vulnerable to Credential Theft attacks (Pass-the-Hash, Pass-the-Ticket and Overpass-the-Hash), and creates an interactive organizational vulnerability map that displays all possible routes of attacks on the network.

Note:
Scanning for the above mentioned attacks increases bandwidth usage. See below for more details.

Golden Ticket Attack Risk

Using the Pass-the-Hash vulnerability scan, CyberArk DNA can detect possible Golden Ticket attack vectors. DNA presents computers that are vulnerable to Credential Theft attacks which can evolve into a Golden Ticket attack. If the network is vulnerable to a Golden Ticket attack, the vulnerability map will display a Domain Controller icon and all possible routes of attacks to the Domain Controller.

Credential Detection Scan

CyberArk DNA uncovers and reports the endpoints that are most susceptible to credential theft attacks from memory, providing organizations with actionable data that can be used to limit credential theft exposure in a measurable way, by uncovering passwords and derived credentials in LSASS that are vulnerable to common credential harvesting techniques.

Cloud Assets Scan

CyberArk DNA discovers and reports the powerful users, instances and credentials in AWS, helping organizations to understand and quantify privileged account risks in public cloud environments. In addition, CyberArk DNA integrates with AWS Inspector to bring additional information regarding high severity security findings.

What does DNA require?

What type of account is required to perform a scan?

Credentials for Scanning Windows Machines

- Domain Administrator

or,

- Equivalent Domain User:
  - User with read permissions on the Active Directory
  - User with local administrative rights for Windows

> **Note:**
>
> - In Windows Vista or newer, a user who is not a domain Administrator must be a domain user and must belong to the Administrators group or to a group nested within the Administrators group.
> - In older versions of Windows, the domain user can be a member of any privileged group.

Credentials for scanning MSSQL Database Instances

DNA must log onto the database with a domain user that has the **sysadmin** server role.

Credentials for Scanning Unix/Linux Machines

- To scan Unix/Linux machines, the following credentials are required:
  - User with root permissions for Unix/Linux

  It is possible to configure DNA to scan with users who authenticate with a password as well as users who authenticate with SSH keys. For more information, refer to Appendix E: Importing a File in the DNA User Guide.
- To scan Unix/Linux machines connected via an Active Directory bridge, use the Active Directory as a source. The following credentials are required:
  - Domain Administrator with root permissions on Unix/Linux machines

  or,
  - Equivalent Domain User:
    - User with read permissions on the Active Directory
    - User with root permissions for Unix/Linux

> **Note:**
>
> - To scan using the Active Directory as a source, your organization must use an Active Directory bridge solution. For example, Centrify DirectControl.

When scanning Unix/Linux machines with accounts other than root, DNA requires the use of sudo to run commands. Hence, the administrative user account(s) configured to scan with DNA must have permissions to run sudo on the scanned Unix/Linux machines.

For more information, see *Configuring Root Permissions Using the Sudoers File* in the CyberArk DNA User Guide.

Note:
Currently, DNA supports the following sudo-replacement solutions:

- CA Privileged Identity Manager/ControlMinder using the sesudo command
- Centrify Access Manager/DirectAudit using the dzdo command

About the Scan

Will the scan burden my network or affect the performance of my DCs or target computers?

The CyberArk DNA **Account Scan** consumes low network bandwidth and uses insignificant network and CPU resources on the Active Directory DCs and target machines.

The CyberArk DNA **SSH Keys Scan** consumes low network bandwidth. To discover Private SSH keys on each machine, DNA searches the configured paths for the files. As a result, target machines may experience an increase in CPU usage during the scan, which usually varies between a few seconds and up to a few minutes (single core machines are not supported and will therefore not be scanned, due to high total CPU usage).

The CyberArk DNA **Pass-the-Hash Vulnerability Scan** consumes insignificant network resources against the Active Directory DCs and a total network bandwidth as described in the table below. Due to environmental limitations, target machines running Windows versions prior to Vista, may experience an increase in CPU usage during the scan, which usually varies between a few seconds and up to a few minutes (single core machines are not supported and will therefore not be scanned, due to high total CPU usage).

Pass-the-Hash Scan	Average MB/s	Maximum MB/s
1 thread	3 MB/s	7 MB/s
10 threads	11 MB/s	40 MB/s
25 threads	23 MB/s	70 MB/s

Best-practices for scanning with DNA

As a best practice, it is recommended to plan the scan on your network by considering the following parameters:

- **Network utilization** – Consider the current network utilization as well as the added utilization that DNA may introduce.
- **Potential bottlenecks** – Consider any potential bottlenecks, e.g. routers, switches, single interface/channel/link/pipe with potentially sensitive or loaded connections, servers with overloaded CPUs, etc.

Scanning machines connected to a LAN

When running DNA on machines connected to a LAN (e.g. a switched network), it is recommended to use the default thread value (the default value of 10 threads assumes a 1 Gb/s switched network).

To decrease network utilization, configure the number of threads that DNA uses to a lower number, see DNA User Guide for instructions.

Scanning machines connected to a WAN

When running DNA on machines connected via a WAN link (i.e. using a single interface/channel/uplink/pipe), it is recommended to set the threads to a safe and conservative value of 1 or 2, since it is the nature of single interface connections to be highly utilized at all times.

How do I run CyberArk DNA?

Does CyberArk DNA require installation?

CyberArk DNA is a standalone tool and does not require installation. It can be run on any Windows 7, 2008 or 2012 operating system with .NET 4.5.2 Framework and with 1 GB free space.

Does CyberArk DNA make any changes to the machine it is run from?

CyberArk DNA *does not make changes* to the machine it is run from, except for a registry change in the current user hive to be able to store the EULA acceptance, and for writing report and log files.

Does CyberArk DNA make any changes to the scanned DCs or target computers?

CyberArk DNA performs the network scan in *read-only mode* by default. It makes no changes to the Active Directory or target computers.

Note:
The discovery of SSH keys on Windows machines is not read-only. This discovery feature is disabled by default and must be enabled manually.

How does it work?

Where does CyberArk DNA store the credentials?

CyberArk DNA stores the credentials used for scanning in memory. It does not save them in any other way.

Credentials such as Hash and passwords that are found using the Credential Detection scan are not saved at all, anywhere. DNA only sends an indication of their existence and password length (when available) back to the report.

Does CyberArk DNA make any changes to SSH Keys? Does DNA download the discovered SSH Keys?

DNA performs the scan in read-only mode and does not make any changes to the SSH Keys or the SSH client/server configuration files. For Unix scans, DNA does not download discovered SSH Keys.

Note:
The discovery of SSH keys on Windows machines is not read-only, and SSH keys need to be securely downloaded from the scanned machine to the scanning machine. This discovery feature is disabled by default and must be enabled manually.

Does CyberArk DNA access any password hashes on the workstations, servers or the domain controller?

DNA does not access any hashes, passwords or any sensitive information on scanned machines. DNA performs the scan in read-only mode and does not write to the scanned machines.

What type of data does CyberArk DNA access during the scan?

CyberArk DNA accesses account data, machine data, SSH keys, configuration files, memory (LSASS) and event log data found on machines during the scan.

Does CyberArk DNA create or expose hashes on scanned machines during the scan?

CyberArk DNA uses protocols and methods that do not leave hashes on scanned machines, and, therefore, do not cause machines any vulnerabilities.

What does the DNA Obfuscation tool do?

In order to share information with CyberArk in a secure manner, CyberArk provides the DNA Obfuscation tool. This tool obfuscates every protected data value (account/group name, description, file path, key, machine address, service name and account, etc.) by hashing it with SHA256 one-way hash, so after the obfuscation no-one (including CyberArk) can see the actual values.

Why does the DNA Credential detection scan return no results?

The DNA Credentials Detection Scan scans both LSASS and SAM credentials. Customers who implement LSA Protection protect the LSASS from being accessed by external programs, which results in empty scan results on the LSASS as SAM is not protected by this mechanism and will retrieve the detected hashes. For more information about LSA protection: https://technet.microsoft.com/en-us/library/dn408187(v=ws.11).aspx

Why can’t I select scan with AWS Inspector security findings?

Make sure the AWS Inspector is installed in the selected region. If it is not, access the AWS Inspector console and make the required changes.

What are SPN and why are they risky?

In addition to regular service accounts in Windows, some services authenticate using Kerberos and are registered in the Active Directory Domain. These accounts have an additional attribute called the Service Principal Name (SPN). Regardless of the domain function level or the host’s version, SPNs that are registered under a user account use an old encryption suite (RC4-HMAC) to secure the user’s Hash in the user ticket.

Since requesting a ticket is a legitimate action for every user in the domain, by cracking the SPN ticket that is returned from the request, an attacker could efficiently escalate privileges by creating Silver Tickets or simply impersonate the service account by logging in with the appropriate credentials.

CyberArk DNA can discover all defined Domain Service Accounts according to their Service Principal Name (SPN) attribute.

What type of performance can I expect from CyberArk DNA?

The following CyberArk benchmark shows typical CyberArk DNA performance. The scan was performed on a Windows 7 computer using 25 threads. The Windows machines were scanned using separate processes and the Unix/Linux machines were scanned using one main process.

Windows Scan

For Windows:	
Total number of computers scanned	10,000
Computers scanned successfully	4,375 (44%)
Computers failed partially (4%)	5,625 (56%)
Computers failed to scan (14%)	0
Total number of unique accounts discovered during the scan	321,903
Total number of accounts discovered during the scan	521,250
Total number of Service accounts discovered during the scan	184,375
Total scan time (at worst case)	2 hours, 52 minutes

Windows – with Pass-the-Hash Scan

For Windows – with Pass-the-Hash Scan:	
Total number of computers scanned	10,000
Computers scanned successfully	4,375 (44%)
Computers failed partially	5,625 (56%)
Computers failed to scan	0
Total number of unique accounts discovered during the scan	321,904
Total number of accounts discovered during the scan	523,125
Total number of Service accounts discovered during the scan	184,375
Total scan time (at worst case)	8 hours, 46 minutes

Unix/Linux Scan

For Unix/Linux:	
Total number of computers scanned	10,000
Computers scanned successfully	9,762
Computers failed to scan (2%)	238
Total number of accounts discovered during the scan	281,935
Total number of Service accounts discovered during the scan	184,375
Total scan time (at worst case)	8 hours, 55 minutes

SSH Key Scan

SSH Key Scan:	
Total number of computers scanned	10,000
Windows machines scanned successfully	3205
Unix machines scanned successfully	6434
Computers failed to scan (0%)	0.036% (361)
Total number of Windows accounts discovered during the scan	114,727
Total number of Unix accounts discovered during the scan	352,427
Total number of unique accounts accessible using SSH Keys	6,411
Total number of unique SSH Key Pairs	138
Total number of SSH Key Trusts	121,956,225
Total scan time	2 days, 52 minutes

Websphere and WebLogic Hard Coded Credentials Scan

Websphere and WebLogic Hard Coded Credentials Scan:	
Total number of computers scanned	10,000
Windows machines scanned successfully	0
Unix machines scanned successfully	8,654
Computers failed to scan (0%)	0.041% (410)
Total number of Websphere/WebLogic servers discovered during the scan	10,000
Total number of applications discovered during the scan	1,060,000
Total number of hard coded credentials discovered during the scan	2,140,000
Total number of target systems at risk	1,400
Total scan time	21 hours

Which network protocols does CyberArk DNA require?

To enable CyberArk DNA to function properly, the following network protocols are required:

- For Windows scanning:
  - Windows File and Print Sharing
  - Windows Management Instrumentation (WMI)
  - NetBIOS
  - Ports: 88, 135, 137, 138, 139, 389/636, 445, 49153, 49155-49156 (required for Windows Services scanning)
- For Windows scanning without using Cygwin:
  - 4431
- For Unix/Linux scanning:
  - SSH
  - Ports: By default 22 and can be configured to other ports
- For Cloud scanning:
  - HTTPS
  - Port: 443

Note:
Make sure the above protocols are enabled on all of the target computers you want to scan and that firewalls do not block this type of traffic.

What does DNA use each required port for?

Port	DNA uses the port for ...
88	This is the KDC services (only relevant to domain controllers) and should be accessible both through network- and host-based firewalls.
135, 137, 138 (typically also 139)	These are the NetBIOS ports that should be open on host-based firewalls.
389/636	This is the LDAP service (only relevant to domain controllers) and should be accessible both through networ and host-based firewalls.
445	This is SMB/TCP and should be open on host-based firewalls.
49153, 49155-49156	These are ephemeral ports.

Which service(s) are expected to be listening on these ports?

Port	DNA uses the port for ...
49153	To communicate (in TCP) with the remote computer.
49155-49156	To retrieve the list of services from the remote computer.

DNA on Unix/Linux

Which Unix/Linux commands does CyberArk DNA use?

Platform	Command
Linux:	uname, ls, test, cat, lastlog, getent, grep, wc, find, xargs, ssh-keygen, echo, rm, date, hostname, ifconfig, sh
AIX:	uname, ls, test, cat, lsdev, grep, wc, ssh-keygen, echo, rm, istat, hostname, ifconfig, sh
Solaris:	uname, echo, test, cat, getent, grep, psrinfo, wc, find, xargs, ssh-keygen, ls, rm, truss, hostname, ifconfig, sh

Notes:

Note:

- When configuring the sudoers file to enable root access for a non-root account, include all the commands above.
- In order to calculate the Public SSH key fingerprint, DNA has to create a temporary file. The “rm” command is then used to delete this temporary file.

Which Unix/Linux files are read by the DNA scan?

In a Unix/Linux scan, DNA scans for configuration files on the target-scanned machine. These file paths depend on the Unix/Linux flavor.

The following list shows an example of the configuration files that DNA scans on a Linux system:

- /etc/passwd
- /etc/group
- /etc/shadow
- /etc/sudoers
- /etc/ssh/sshd_config
- /etc/syslog.conf
- /etc/rsyslog.conf
- /etc/syslog-ng/syslog-ng.conf

Which methods of Data Protection does DNA use?

When scanning Unix/Linux machines, CyberArk DNA connects to the scanned machines via SSH, using the provided credentials. All the SSH traffic is encrypted, by default, which protects the data in transit. DNA uses an underlying AES encryption algorithm to protect data at rest.

What type of sudo-replacement solutions can DNA use?

DNA supports the following sudo-replacement solutions:

- CA Privileged Identity Manager/ControlMinder – This solution contains the ‘sesudo’ command.
- Centrify Access Manager/DirectAudit – This solution contains the ‘dzdo’ command.

DNA will automatically determine whether or not the above sudo-replacement solutions exist on the scanned machine and, if they do, will automatically use them.

Making sense of the Executive Report numbers

Machine/Account Data – Accounts Discovered

Privileged Accounts

Find out the total number of privileged accounts that were discovered by adding up the number of privileged domain accounts and the number of privileged local accounts.

You can do this in the 'Windows Scan' sheet.

To view the number of discovered privileged domain accounts:

1. Filter all the domain accounts (Account Type=domain:*) that are privileged (Account Category=Privileged Personal / Privileged Shared).
2. Remove duplicates according to Account Name and Account Type.
3. Remove the 'Domain Users' group.

To view the number of discovered privileged local accounts:

1. Filter all the local accounts (Account Type=Local) that are privileged (Account Category=Privileged Personal / Privileged Shared).
2. Remove duplicates according to Computer Name and Account Name.

Non-Privileged Accounts

Find out the total number of accounts that were discovered by adding up the number of domain accounts and local accounts.

Find out the number of non-privileged accounts that were discovered by subtracting the number of privileged accounts from the total number of accounts that were discovered.

You can do this in the 'Windows Scan' sheet.

To view the number of discovered domain accounts:

1. Filter all the domain accounts (Account Type=domain:*).
2. Remove the 'Domain Users' group.
3. Remove duplicates according to Account Name and Account Type.

To view the number of discovered local accounts:

1. Filter all the local accounts (Account Type=Local).
2. Remove duplicates according to Computer Name and Account Name.

Machine/Account Data – least privilege risk - Windows business users

Privileged business users - Workstations

Find out the number of privileged business users on workstations by adding up the number of local privileged users and domain privileged users (unique).

In the 'Windows Scan' sheet:

1. Filter all Workstation privileged accounts (Machine Type=Workstation, Account Category=Privileged Personal/Privileged Shared)
2. Count the number of local accounts (Account Type=Local) except the local Administrator user
3. Filter the number of Domain accounts (Account Type=Domain*) except the Domain Users group
4. Remove duplicates from the user name
5. Add the number of users from sections 2 and 4 to total the number of Privileged Business users on workstations.

Non-Privileged business users - Workstations

Find out the number of non-privileged business users on workstations by adding up the number of local non-privileged users and domain non-privileged users (unique).

In the 'Windows Scan' sheet:

1. Filter all Workstation non-privileged accounts (Machine Type=Workstation, Account Category=Non-Privileged Personal/Non-Privileged Shared)
2. Count the number of local accounts (Account Type=Local)
3. Filter the number of Domain accounts (Account Type=Domain*) except the Domain Users group
4. Remove duplicates from the user name
5. Add the number of users from sections 2 and 4 to total the number of Non-Privileged Business users on workstations.

Privileged business users - Servers

Find out the number of privileged business users on servers by adding up the number of local privileged users and domain privileged users (unique).

In the 'Windows Scan' sheet:

1. Filter all Server privileged accounts (Machine Type=Server, Account Category=Privileged Personal/Privileged Shared)
2. Count the number of local accounts (Account Type=Local) except the local Administrator user
3. Filter the number of Domain accounts (Account Type=Domain*) except the Domain Users group
4. Remove duplicates from the user name

5. Summing the number of users from section 2 and 4 will result with the number of Privileged Business users on servers.

Non-Privileged business users - Servers

Find out the number of non-privileged business users on servers by adding up the number of local non-privileged users and domain non-privileged users (unique).

In the ‘Windows Scan’ sheet:

1. Filter all Server non-privileged accounts (Machine Type=Server, Account Category=Non-Privileged Personal/Non-Privileged Shared)
2. Count the number of local accounts (Account Type=Local)
3. Filter the number of Domain accounts (Account Type=Domain*) except the Domain Users group
4. Remove duplicates from the user name
5. Summing the number of users from section 2 and 4 will result with the number of Non-Privileged Business users on servers.