The CDE Challenge

Objective: The Acme Corporation ("the Customer") has CyberArk's Privileged Access Management (PAM) Core Suite of software installed and configured and "in production". The customer is having issues that need to be resolved. Additionally, the customer wants more features and functionality that includes adding 2FA using PKI+LDAP; an additional PSM Component server; and creating a load balanced PSM configuration. The customer is also asking for a Security Hardening review on the PAM Component Servers to ensure they have been deployed securely and to CyberArk Best Practices.

General Instructions

1. The CDE Challenge lab represents a customer's production environment and must be treated accordingly. Unauthorized and / or inappropriate modifications to the environment may result in a penalty that will be deducted from your overall score.
2. You will have access to the lab for 1 calendar week, i.e., 7 consecutive days to complete all the objectives and tasks defined herein.
    a. Expect to spend approximately 8 hours to complete.
    b. CDE Challenge labs submitted for review after the 7-day period will be rejected.
3. Review the "CyberArk Partner CDE Challenge and Re-Certification Challenge" document that provides general guidelines, instructions and the retries policy, downloadable from the training website.
4. Refer to CyberArk documentation, the CyberArk Marketplace, or CyberArk Tech Community to complete your tasks.
    a. CyberArk Documentation can be found at https://docs.cyberark.com/Product-Doc/OnlineHelp/Portal/Docs.html
    b. CyberArk Marketplace and Tech Community can be found at https://cyberark-customers.force.com/mplace/
5. You may consult colleagues but no one other than you can configure the provided CyberArk CDE Lab.
6. All questions related to the CDE Challenge must be sent to CDE.Challenge@cyberark.com but no technical assistance will be provided beyond what is included in this guide and the CDE Challenge Lab Guide specific to the CDE Challenge lab.
7. Opening a CyberArk support case requesting assistance with the CDE Challenge may result in the disqualification of the CDE Candidate.
8. Once you have completed the challenge, submit in the CyberArk Learning Management System and upload a text document containing the Skytap Lab URL.
9. Sign in as "VaultAdmin01@acme.corp" to VM COMP01A to access the PVWA.

Assignment Categories

The CDE Challenge will include assignments in the categories described below. A strong emphasis is placed on CyberArk's prescribed security configuration and hardening procedures and what the installation automation scripts perform. Failure to properly diagnose and resolve security hardening parameters will result in an automatic failure of the CDE Challenge.

- Security hardening parameters on CyberArk Components CPM/PVWA
- Disaster Recovery
- Authentication Methods
- LDAP Integration
- PSM Connection Components
- PAM Installation

- PAM Component configuration and optimization

Customer Provided Resources

Your customer has provided the following information to enable configuration and testing of the CyberArk PAM deployment.

ACME Corp Network Environment

Network	Server Name	IP Address
Windows Domain Controller: ***ACME.CORP***	DC01.acme.corp	10.0.0.2
Certificate Authority https://dc01.acme.corp/certsrv	DC01.acme.corp	10.0.0.2
Unix / Linux	CentOS-target	10.0.0.20
CyberArk PAM	Vault01A	10.0.10.1
	Comp01A (PVWA-CPM)	10.0.20.1
	Comp01C (PSM)	10.0.22.1
	Comp01D (PSM)	10.0.23.1
PSM Load Balancer	psm-farm.acme.corp	

CyberArk PAM Software Installation Files and Utilities

1. This lab is a licensed and operational CyberArk PAM core solution v13.2.
2. The ACME Corp lab is a licensed and operational CyberArk PAM core solution v13.2.
    a. The installed version 13.2 of CyberArk Software can be found on the local drive of each CyberArk Component server in ‘C:\CYBR_Files’
3. Utility software is installed on the Windows VM’s for your convenience.
    a. Notepad++ (not on Vault server)
    b. Putty (not on Vault server)
    c. WinSCP (not on Vault server)
    d. Google Chrome (not on Vault server)

Digital Certificates

1. The ACME Corp has installed Certificate Services on the Domain Controller. This is not a recommended configuration and will require users to sign in as a domain user when accessing the PVWA, or certificate revocation list errors will occur.
2. Root certificate of the Skytap Lab Certificate Authority can be downloaded from the ACME Certificate Authority or exported from any domain joined Component Server if required.

3. Digital certificates for Web Hosting and PSM can be found in the folder 'C:\CYBR_Files' on the CyberArk Component servers. Each certificate is password protected. Password = Cyberark1
4. ACME.CORP Certificate Authority can be accessed from any Comp01A Server at URL "**HTTPS://DC01.ACME.CORP/CERTSRV/Default.asp**"

Default Passwords

Note: The default password for all accounts is "**Cyberark1"** unless managed by CyberArk Central Policy Manager (CPM).

The CyberArk built-in Administrator user is managed by the CyberArk CPM.

You have full access to network resources. The customer has provided end usernames for testing and access to the Domain Controller if needed.

Username	**Group Membership**	**Password**	**Domain or Server**	**Description**
Administrator	N/A	Managed	n/a	CyberArk built-in Administrator
Administrator@acme.corp	Domain Admins	Cyberark1	acme.corp	Built-in Domain Administrator
Admin01-05	Domain Admins			**Admin01 is managed** by the CPM and used as a reconcile account
VaultAdmin01-05	CyberArk Vault Admins WindowsAdmins			Local Administrator on all Component Servers
Auditor01-05	CyberArk Vault Auditors			CyberArk Auditors
WinAdmin01-05	CyberArk Vault Users			CyberArk End users
LinuxUser01-05	CyberArk Vault Users			CyberArk End users
LinuxAdmin01-05	CyberArk Vault Users			CyberArk End users
OracleAdmin01-05	CyberArk Vault Users			CyberArk End users

[1] VaultAdmin01@acme.corp account should be used to sign in to all Comp01 servers.

PSM Connection Components In Use

Connection Component	**Target Address**	**Managed Accounts**

PSM-RDP	Comp01c.acme.corp	1. Admin01@acme.corp 2. Admin02-05 can be added if needed for testing 3. Localadmin01@comp01c.acme.corp
PSM-SSH	10.0.0.20	• Root • Root01-05 can be added if needed for testing
PSM-PrivateArkClient (desired)	10.0.10.1	• Administrator
PSM-SQLPlus	10.0.0.20	• dba01 • dba01-05 can be added if needed for testing

Assigned Tasks

- Troubleshoot and resolve the outstanding issues identified by the customer.

Category: PAM Installation – Privileged Session Manager

Category: Security hardening parameters on CyberArk Components

- The ACME Corp wants fault tolerance for their PSM implementation. The ACME Network Administrator has configured a load balancer for this purpose. The load balanced pool includes PSM servers COMP01C and COMP01D. PSM v13.2 is installed and configured on COMPO1C as a standalone PSM server.
- All features and functions enabled on the existing PSM server must also be supported by the new PSM server. The COMP01D server is a Microsoft Windows 2019 server joined to the ACME.CORP domain.
  - Install a 2nd PSM Server on COMP01D server to CyberArk standards for configuration and hardening. Ensure the ACME Corp standard for execution policy is maintained and CyberArk recommended configuration is applied. Accept the defaults except for the following requirements when installing PSM on COMP01D.
    - CyberArk PAM software can be found in the **"C:\CYBR_Files"** directory.

- Secure RDP Connections with SSL
  - Do not configure API Gateway
  - Do not enable PKI authentication
  - Reduce Win Certificate Wait Time
  - Ensure all phases of PSM hardening are applied, including the CyberArk hardening GPO.
    - The CyberArk PSM GPO is already linked to the ACME.CORP\Servers\CyberArk\PSM Organizational Unit

        - COMP01D resides in the \Computer's container in the ACME.CORP domain and must be moved to the target OU post PSM install.
    - Disable support for Web Applications and Enable PSM users to print PSM sessions.
- The Network Admin provided a CNAME, "psm-farm.acme.corp" to represent the load balanced pool of PSM servers, i.e., comp01c.acme.corp and comp01d.acme.corp.
- Individual password protected (*Cyberark1*) certificates configured with Subject Alternative Names or SAN's can be found locally on the COMP01C and COMP01D servers in the **"C:\CYBR_Files"** directory with a .PFX file name extension.
- Configure active platforms with names beginning with ACME that are enabled for session management to take advantage of the Load Balanced PSM Server Pool.
- Test PSM Connection Component functionality on COMP01D and the Load Balanced configuration.
- ACME Corp auditors need to review all logs created as a result of the CyberArk PSM installation. Create a new folder "C:\CYBR_Files\Logs.
    - Copy or move all relevant logs to "C:\CYBR_Files\Logs" that were created during the installation and configuration of the PSM server.

Category: Security hardening parameters on CyberArk Components

- The CPM and PVWA are co-hosted on the Windows Server COMP01A at the ACME Corp. The component server has been hardened using CyberArk Installation Automation scripts + GPO enforcement as required by CyberArk.
    - After the installation, configuration and hardening of the CyberArk Component Servers, ACME Administrators discover that the 'CyberArk Password Manager' and 'CyberArk Central Policy Manager Scanner' services will not start.
    - Troubleshoot and resolve to CyberArk hardening standards any issues preventing CyberArk services from running.

Category: Security hardening parameters on CyberArk Components

- When CyberArk PAM was initially installed, all hardening scripts and recommended procedures were followed. ACME Corp management wants to be sure the system remains compliant with CyberArk recommendations and Best Practices.
    - Perform a security review on the CyberArk Components CPM and PVWA to ensure they are hardened per CyberArk documented prescriptive guidance.
    - Resolve any issues identified.

Category: Authentication Methods

- The ACME Corp Chief Information Security Officer is demanding 2 factor authentications for the CyberArk Users group.
    - Enable PKI Authentication at the PVWA
    - When signed into server Comp01a, the VaultAdmin01 user has a valid certificate in the Windows Personal Certificate Store that can be used for testing PKI authentication.

- Enable 2 factor Authentication using PKI+LDAP/S
- Ensure the default authentication method at the PVWA is PKI.