DETECT ON-PREM PRIVILEGED ACCOUNT RISK AND VULNERABILITIES WITH CYBERARK ZBANG

FREE Open Source Tool

INTRODUCTION

Many organizations today exist in a hybrid cloud environment whereby many critical Tier0 applications and data continue to reside in traditional on-premises environments. Beyond traditional unmanaged privileged accounts and credentials such as local admin accounts, domain admin accounts, application and database accounts, there are many other (non-traditional) privileged risks and vulnerabilities that need to be addressed to mitigate the risk of a cyber attack. The CyberArk zBang tool is an open source tool designed to create an in-depth risk assessment that automates and unifies manual scans that uncover privileged access security risk across on-premises environments. Developed by the CyberArk Threat Research Labs team, the tool assists security teams in scanning their networks to discover and visualize critical risks associated with privileged accounts and credentials.

HIGHLIGHTS

- Identify potential attack vectors and improve the security of the network
- The tool only requires a domain-level user account with read-only permissions to execute a scan
- Standard execution time on a network with 1,000 machines is approximately 7 minutes~
- The tool is a free open source solution: https://github.com/cyberark/zBang

WHAT'S COVERED IN A SCAN

zBang is comprised of 5 different scanning modules:

1. **ACLight Scan:** The scan allows for the review of privileged accounts that might not be part of the organization's known privileged groups, but still have very sensitive permissions.
2. **Skeleton Key Scan:** The Skeleton Key is a form of malware that infects domain controllers and allows an infiltrator persistence within the network. An infected domain controller will allow the infiltrator access to every domain account with a preset back doored password set by the malware.
3. **SID History Scan:** The SID history attribute is an attribute that can be assigned to each domain account and can be used in case of migration of an account between two trusted domains. The attribute can be manipulated by attackers to escalate privileges.
4. **RiskySPNs Scan:** The tool scans the domain controller for deployed services running with high privileged human accounts. Those services can be targeted by an infiltrating attacker to extract credentials and utilize the privileged account for malicious purposes.
5. **Mystique Scan:** The scan discovers risky delegation configurations in the network. Risky delegation configurations have potential to be abused by attackers.

1	Scan Name	**ACLight**
	Main Value	**Discover the most privileged accounts that need to be protected**
	Scan Output	Visualized results of the discovered privileged accounts, including Shadow Admins with direct sensitive ACL permission assignments. Each account will be presented in a graph with its permissions.
	CyberArk Recommendations	Three questions that must be answered on every discovered account: 1. Is the account recognized? An attacker could create his own new stealthy admin accounts. 2. Does the account really need the highest privileges over the entire domain? The network should be managed with "least privilege" methodology. 3. Is the account properly secured? Privileged accounts need end-to-end protection: strong passwords with frequent rotation, session monitoring, audit trail of activities, etc.
2	Scan Name	**Skeleton Key**
	Main Value	**Discover infected DCs**
	Scan Output	Visualized list of infected domain controllers with the Skeleton Key malware (if it exists).
	CyberArk Recommendations	If the scan finds an infected DC, it is crucial to initiate an incident response process.
3	Scan Name	**SID History**
	Main Value	**Discover hidden privileged in secondary SID of domain accounts**
	Scan Output	Visualized list of accounts with SID history (secondary SID)
	CyberArk Recommendations	If the scan discovers a privileged secondary SID, the need for this SID needs to be verified. If there's a legitimate need, this account should be prioritized for onboarding and management within CyberArk. Especially if the account's secondary SID is privileged and the main SID is not. This is a well-known attack method that's often leveraged for obtaining persistency in the target network and performing malicious actions in a stealthy manner.
4	Scan Name	**RiskySPNs**
	Main Value	**Discover weak configurations of SPNs that might lead to credential theft of Domain Admins**
	Scan Output	Visualized list of risky services and accounts.
	CyberArk Recommendations	All discovered user accounts that have SPN (service registered user account) should be secured. If the account becomes compromised, so does its registered service. Converting the SPN to be registered under a machine account instead of a user account should be considered. Moreover, if a privileged account has an SPN (e.g. Domain Admin account), the registration of the SPN (the service) should be converted to a non-privileged account. In this scenario, an attacker can easily request a TGS (Kerberos ticket) for that SPN and then brute force the ticket's encryption. The extracted key is the password of that SPN's domain admin privileged account. This is a powerful attack method for adversaries to perform privilege escalation in the target network.
5	Scan Name	**Mystique**
	Main Value	**Discover risky delegation configurations in the network**
	Scan Output	Visualized list of the domain's delegation options and their risks.
	CyberArk Recommendations	Delegation permissions in the network need to be reviewed. Are the delegation permissions really necessary? Disable old and unused delegation accounts. More specifically, check the risky delegation types of "Unconstrained" and "Constrained with Protocol Transition." Convert "Unconstrained" delegation to "Constrained" delegation so it will be permitted only for specific needed services. The "Protocol Transition" type of delegation should be revalidated and disabled if possible.

EXECUTION REQUIREMENTS

1. Run zBang from a domain joined machine (any Windows OS version).
2. Run zBang with any domain user, the scans does not require any extra privileges as the tool only performs read only queries to the domain controller.
3. PowerShell Version 3 or above and .NET 4.5 (note: it's by default in Windows 8/2012 and above).

TAKE THE NEXT STEP

CyberArk zBang is one of many complimentary scanning solutions to help uncover your organization's level of privileged risk. The tool can be leveraged to enable Security and Red teams to uncover additional attack vectors across the network, as well as help support the business case for implementing a privileged access security program. Get started today by contacting your local CyberArk Customer Success Representative, or by accessing the Quick Start Guide on GitHub: https://github.com/cyberark/zBang

©CyberArk Software Ltd. All rights reserved. No portion of this publication may be reproduced in any form or by any means without the express written consent of CyberArk Software. CyberArk®, the CyberArk logo and other trade or service names appearing above are registered trademarks (or trademarks) of CyberArk Software in the U.S. and other jurisdictions. Any other trade and service names are the property of their respective owners. U.S., 09.19. Doc. 396730052

CyberArk believes the information in this document is accurate as of its publication date. The information is provided without any express, statutory, or implied warranties and is subject to change without notice.