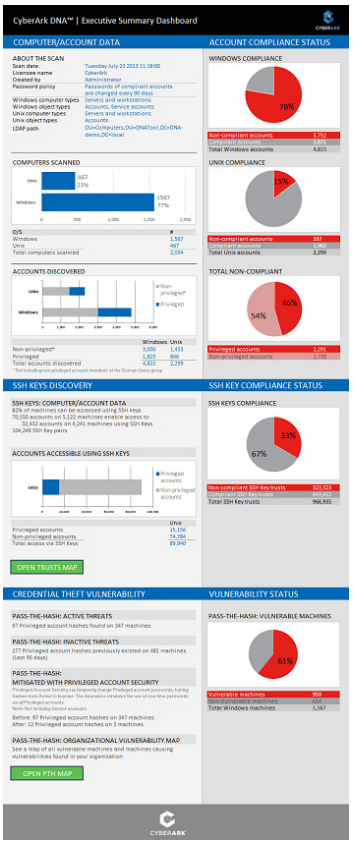
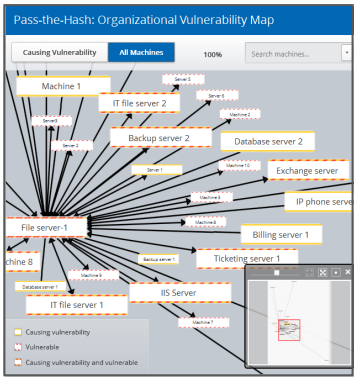
Discovery & Audit

Scan your network with CyberArk DNA™ to:

- Discover where privileged accounts exist
- Clearly assess privileged account security risks
- Identify all privileged passwords, SSH keys, and password hashes
- Collect reliable and comprehensive audit information



Sample Executive Summary Dashboard



Visual maps of password hashes and SSH Key trusts enhance visibility

The Challenge

Privileged accounts are the pathway to a company's most valuable data and are therefore compromised in the majority of advanced and internal attacks. Managing and securing privileged accounts begins with gaining visibility into the risks associated with privileged accounts including:

Privileged Account volume – Typically, there are three to four times the number of privileged accounts than the number of employees in an organization. These accounts exist in every piece of hardware and software in an organization including but not limited to information system administrator or super-user accounts, scripts and application accounts, select business user accounts and corporate social media accounts. The sheer volume of privileged accounts represents a significant security vulnerability to organizations.

Privileged Credential status – The security of privileged accounts is highly determined by the status (strength, age, etc) of the privileged credentials that enable access to these all-powerful accounts. To implement security measures, organizations frequently set credential management policies such as rotating passwords every 90 days. Outdated and static credentials that are not compliant with such policies are at a greater risk of being compromised. Privileged credentials are found in a variety of forms including:

- **Passwords** – Old and static passwords introduce significant risk of compromised credentials. Many compliance regulations recommend frequent password rotation, especially for the most critical accounts in an organization.
- **SSH keys** – Stored throughout a network, SSH keys pose a major challenge to security teams because these privileged credentials can be easily created without a record, and are difficult to track, manage or control..
- **Password hashes** – Passwords are frequently hashed and stored on local machines for user convenience by the operating system, but attacks such as Pass-the-Hash leverage these vulnerable password hashes in order to execute a credential theft attack, impersonate employees, and access valuable assets and data.

Discovering, auditing and understanding vulnerabilities in privileged accounts and credentials across the network can address specific challenges associated with:

Security & Risk Management: If the full extent of the risk is not understood, security and IT teams are not armed with the information they need to mitigate risks associated with privileged accounts.

Audit & Compliance: When an organization does not have clear visibility into their privileged account environment, they can unknowingly be noncompliant with internal policies and risk failing regulatory compliance audits due to a lack of reliable information that is required to meet regulations.

Project Planning: Once an organization is focused on securing privileged accounts, estimating budget and resources required to implement a solution is difficult without a clear view of the problem.

Solution

CyberArk Discovery & Audit™ is a patent-pending, standalone, easy to use tool that exposes the magnitude of the privileged account security challenge. The solution provides a comprehensive view of an organization's privileged account environment including:

- All privileged accounts on the network
- Privileged passwords and their current status
- SSH key pairs and orphan keys and associated status including age, encryption characteristics, compliance status and trust relationships throughout the organization
- Privileged accounts vulnerable to Pass-the-Hash attacks, their locations on the network, and all possible attack routes

Discovery & Audit

Running a DNA scan is a straightforward, automated process that does not require the installation of any agents on the local or target systems and consumes very low bandwidth. With this fast, accessible assessment tool, IT and security administrators can gain a detailed view into the quantity, status and vulnerability of each privileged account, all on an intuitive user interface.

CyberArk DNA answers questions such as:

- On which network servers do privileged accounts eixst?
- Which accounts have escalated privileges?
- How many SSH keys and orphan keys exist in the environment?
- Which machines and accounts on the network can be accessed using SSH Keys, and from where?
- Which privileged accounts are not in compliance with company policy? (i.e. password has not been changed in over 90 days)
- Did an external contractor or 3rd party add a privileged account to a server?
- Do "backdoor" accounts exist on products that have been decommissioned
- How many and which machines on the network are vulnerable to Pass-the-Hash attacks?

Features

CyberArk DNA provides key capabilities including:

- **Simple to use, non-intrusive scanning** – A straightforward three-step process scans an entire directory for privileged, shared and generic accounts on workstations and servers without the need to install anything on the network.
- **Detailed reporting** – A detailed report provides a 'single version of the truth' about all existing privileged accounts, passwords, SSH keys and Pass-the-Hash vulnerabilities and the status of each.
- **Graphical presentation of results** – An Executive Summary Dashboard presents a clear, concise view of privileged account risk and compliance status.
- **Pass-the-Hash vulnerability map** – A clear diagram of network machines storing privileged password hashes demonstrates how an attacker can leverage the Pass-the-Hash attack to travel the network and reach a target machine.
- **SSH key trust map** – A visual display of all SSH keys (including orphan SSH keys) illustrates the trust relationships that enable access to privileged accounts.
- **Targeted Alerting** – A report flags and alerts on audit findings that indicate a problem, such as mismanaged privileged accounts, out-of-policy passwords, orphaned SSH keys, and Pass-the-Hash vulnerabilities.
- **Powerful scanning with minimal performance impact** – A multi-threaded application design expedites scanning, consuming low network bandwidth and using insignificant network and CPU resources on the Active Directory Domain Controllers and target machines. All scans are performed in read-only mode, without changing anything in the environment.

Benefits

Identify extent of risk by discovering every single privileged account and its status
Fast, accurate reporting on privileged account numbers and status enables organizations to immediately pinpoint unknown or improperly managed privileged accounts and act quickly to address any issues.

Understand vulnerabilities to specific cyber security threats
The identification of privileged password hashes provides key insights into Pass-the-Hash vulnerabilities, improving mitigation planning and implementation.

Save valuable audit preparation time and cost
Auditors gain a reliable, correlated and comprehensive view of the state of privileged accounts, eliminating complex mapping and manual discovery of this information, which is often difficult and time consuming to gather.

Gain visibility into the privileged account problem and solution
A clear and reliable view of the magnitude and status of privileged accounts creates a better understanding of the problem, leading to a more operational approach to planning, budgeting and deploying a solution.

Implement a comprehensive solution CyberArk's market-leading Privileged Account Security solution offers a comprehensive solution for privileged account controls, monitoring, management and intelligence. This end-to-end solution begins with the critical function of auditing and discovering all privileged accounts on the network.

Specifications

CyberArk DNA™ runs on

- Windows 7

Both 32-bit and 64-bit versions are available for all platforms

Supported Target Systems

Windows Workstations:

- Windows 2000
- Windows XP
- Windows Vista
- Windows 7
- Windows 8

Windows Servers:

- Windows 2000
- Windows 2003
- Windows 2008
- Windows 2012

Unix:

- RHEL 4-6
- Solaris Intel 10
- SUSE
- Fedora
- Oracle
- CentOS

Network Protocols

Windows:

- Windows File and Print Sharing
- Windows (WMI)

Unix:

- SSH
- SFTP

Sample Data Scanned

- Windows and Unix Accounts
- Domain Accounts
- Local Accounts
- Windows Service Accounts:
- Windows Services
- Scheduled Tasks