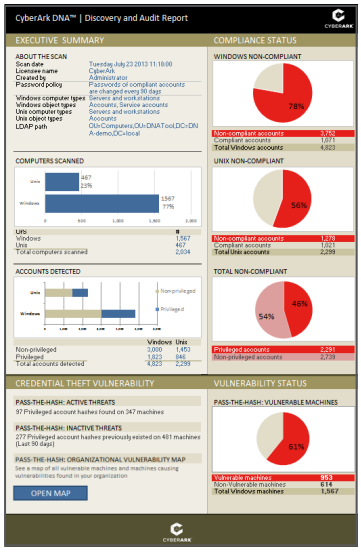
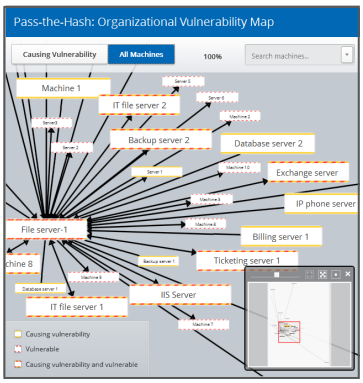
Discovery & Audit

Scan your network with CyberArk DNA™ to:

- Discover where privileged accounts exist
- Clearly assess privileged account security risks
- Identify machines vulnerable to Pass-the-Hash attacks
- Collect reliable and comprehensive audit information



Sample Executive Summary Dashboard for easy identification and insight of issues



Sample Organizational Vulnerability Map for a visual representation of Pass-the-Hash vulnerabilities

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 locating all accounts and understanding the security risks and vulnerabilities associated with each account. However, this continuous process of identifying and securing all privileged accounts in an organization presents a real challenge due to the high volume of accounts, employee turnover and lack of historical records and documentation.

Typically, there are two to three more shared and privileged accounts than users in an organization. With the understanding that shared accounts exist everywhere—desktops, laptops, servers, databases, security and network devices, virtual machines, application code, web-based interfaces—the process of finding every account across the entire network is nearly impossible without a tool designed to locate and identify such accounts. Compounding the problem is the fact that employees and contractors managing these accounts change roles and leave the company, often taking important knowledge with them. Even the best efforts to document and track privileged accounts in an organization can leave some undiscovered whether they resulted from a merger or acquisition or are legacy accounts that have never been documented.

Understanding where privileged accounts are located and how many exist is only the first step in understanding the risks and vulnerabilities associated with the accounts. Old, static passwords as well as password hashes stored on machines across the network introduce significant risk of compromised credentials. For example, attacks such as Pass-the-Hash leverage these vulnerable password hashes in order to execute an attack and access valuable assets and data. As a result, a complete understanding of the privileged account security problem requires a full scan of the network to locate accounts, accompanied by an audit of credentials and storage of password hashes.

Discovering, auditing and understanding vulnerabilities in privileged accounts 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 and Compliance:** When an organization does not have a clear understanding of the volume and location of privileged accounts, auditors lack the reliable information they need to complete an audit.
- **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 & Key Benefits

CyberArk's Discovery & Audit (CyberArk DNA™) is a patent-pending, standalone, easy to use tool that exposes the magnitude of the privileged account security challenge. The solution provides a complete list of all privileged accounts on the network, a status report on the associated passwords as well as identifies machines vulnerable to attacks such as Pass-the-Hash.

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 privilege account, all on an intuitive reporting and user interface.

CyberArk DNA answers questions such as:

- On which network servers do privileged accounts exist?
- Which accounts have escalated privileges?
- Which privileged accounts are not in compliance with company policy? (i.e. password has not been changed in over 60 days)
- Did an external contractor or 3rd party add a privileged user 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?
- How can an attack be carried out in my organization?
- What is causing my machines to be vulnerable to Pass-the-Hash and how can I reduce the risk?

Access to a comprehensive report of the privileged accounts, credentials and vulnerabilities enables IT and security teams to effectively manage and secure privileged accounts. Security risks are identified quickly resulting in faster mitigation and reduced damage to the business. Audits are streamlined and more comprehensive. Overall knowledge of the privileged account threat landscape is better understood in preparation for employing a privileged account security solution.

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.
- **Graphical presentation of results –** An Executive Summary Dashboard presents a clear, concise view of privileged account risk and compliance status.
- **Detailed reporting –** A detailed report provides a 'single version of the truth' about all existing privileged accounts and Pass-the-Hash vulnerabilities and the status of each and every account.
- **Pass-the-Hash vulnerability map –** A clear diagram of network machines storing privileged password hashes illustrates how an attacker can leverage the Pass-the-Hash attack to travel the network and reach a target machine.
- **Targeted Alerting –** A report flags and alerts on audit findings that indicate a problem, such as mismanaged privileged accounts, 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

Cyber-Ark'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

Supported Target Systems for Scanning

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

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