Keeping the Credential 'Chain of Custody' Intact - CyberArk and PenTera Integration

Jan 13, 2020
By Ran Tamir - PCYSYS

In legal terms, the process of transferring evidence from one place to another is handled in a vigilant manner - the chain of custody. The purpose is to ensure that the evidence remains untainted or tampered with, and is in fact related to the alleged crime. The smallest crack in the process can result in setting a criminal free, or worse, convicting an innocent man as guilty.

When it comes to cyber security and access to the IT network, the evidence being transferred in the 'chain of custody' comes in the shape of credentials. With the continuous growth of cyber attacks on organizations originating from phishing campaigns, the way credentials are transferred and the access given between applications and processes can create an opportunity for an attacker if it is not maintained properly.

Whether for development, finance, security or others, every application added to the network requires credentials, which then require access to different components of the network in order to run and perform their purpose. As the network grows, it becomes increasingly difficult to keep track of which applications have access to what and where, thus beginning the uncertainty of the strength and posture of the network configurations.

Organizations that deploy the CyberArk Privileged Access Security Solution understand the importance of a privileged access and credential management solution that focuses squarely on risk reduction. Credentials are secured through the CyberArk vault, eliminating the need to store privileged credentials, passwords, keys, etc. within the native solution code.

The "Threat" of a Manual Penetration Test

The purpose of a penetration test is to test an organization's security controls, understand the state of its cyber security posture and where to focus remediation efforts. The way it is widely conducted today, 1-3 times a year by third-party individuals, does not provide a continuously accurate view of the dynamic network controls while using privileged credentials as part of the test project.

Get the CyberArk Integration Datasheet

When running what/if scenarios, the goal is to learn where certain credentials can lead to within the network. The tester is explicitly given the credentials to a specific app or workstation and follows the "kill chain" as far as it can go. For example, can a compromised computer (originating from a weaponized resume document) in the HR department, laterally move to the Finance department?

To test this use case, one would give the pen-testing professional, the HR network's admin credentials. The same may apply to test if a compromised dev-environment workstation could potentially breach the operational compute clusters.

The root of the problem remains in the need for the pen-testers to use privileged credentials. In most cases, these are written on a piece of paper, or worse (if possible), sent via another insecure app. Once again, the 'chain of custody' is lost, as will be the accurate status of cyber security posture. Do you know where the credentials are going?

Ironically, an activity that comes to reduce vulnerabilities generates a few vulnerabilities in itself. That is until automation and integration join together to prevent that from happening.

Automating network penetration testing enables security teams to continually improve the consistency of their cyber security posture over time. They can test their environment on a self-service basis in a secure manner.

Pcysys' automated penetration-testing platform, PenTera, enables continuous risk validation and focused remediation on damage-baring vulnerabilities. After automatically scanning and enumerating an organization's network and applying a broad range of pen-testing techniques, PenTera generates an automatic attack summary report that visually illustrates the "attack story" from the hacker's perspective, pointing to the security practices that require improvement and the business-focused vulnerabilities that need remediation.

Get the CyberArk Integration Datasheet

Securely Enable Continuous Enterprise Penetration Testing

The PenTera™ integration with CyberArk Application Access Manager, part of the CyberArk Privileged Access Security Solution, is designed to provide a robust penetration testing solution that gives security teams the power of a red team while protecting privileged accounts. This integration enables the retrieval of user credentials, as part of an authenticated and automated penetration testing scenario run. It is also designed to ensure the integrity and confidentiality of high-privilege credentials while conducting penetration test risk validation exercises.

Penetration tests can be performed without exposing sensitive information to non-authorized third-party personnel and without adding further risk of credential leakage or compromise, always maintaining the 'chain of custody'.