CORNICE NETWORKS

NETWORK PENETRATION TESTING

DATASHEET

What is Automated Penetration Testing?

vPenTest is **Cornice Networks** automated network penetration testing platform that combines the knowledge, methodology, processes, and toolsets of a team of security consultants into a single, deployable platform for organizations of all sizes. We help organizations to perform a penetration test within their environment at any given time, satisfying both compliance requirements as well as meeting security best practices. This platform is automated by vPenTest and is based on a framework that continuously improves over time.

Traditionally, organizations have to face several challenges when seeking a penetration test, including availability, experience and background, as well as low quality deliverables that fail to effectively communicate the critical issues and remediation strategies that organizations need to adhere to in order to reduce their overall cyber risk. Through several years of experience, certifications, industry contributions including numerous tools, vPenTest solves a critical need for organizations in an ever-changing threat landscape.

- ➔ No more scheduling conflicts.
- ➔ A full-blown penetration test, whenever you need, however often you need.
- ➔ Developed on a framework and methodology that changes and improves as the industry threats increase.
- ➔ Backed by 10+ years of experienced and OSCP, CISSP, CEH, and OSCE certified consultants.

vPenTest helps organizations solve an ongoing challenge of meeting compliance, achieving security best practices, and researching multiple vendors to compare numerous factors to meet their offensive security needs.

BACKED BY EXPERTS

Combining the knowledge, skills, logic, and toolsets of numerous certified security consultants into one platform, vPenTest is the perfect solution to consistently satisfy your organization's needs for quality results.

REAL-TIME ACTIVITY TRACKING

An important step to assessing your organization's risk is the ability to detect and respond to malicious activities occurring within your environment. vPenTest creates a separate log file for every single activity that is performed so you can correlate our activities with your monitoring and logging solutions.

MEET COMPLIANCE & BEST PRACTICES

By having the ability to perform a quality network penetration test whenever you want and however often you want, your organization can be assured that it will continuously meet security best practices and compliance regulations.

CORNICE NETWORKS

Our Penetration Testing Methodology

vPenTest combines multiple methodologies that were once manually conducted into an automated fashion to consistently provide maximum value to organizations.

EGRESS FILTERING TESTING

Automatically perform egress filtering to ensure that your organization is effectively restricting unnecessary outbound traffic. Unrestricted outbound access can allow a malicious actor to exfiltrate data from your organization's environment using traditional methods and unmonitored ports.

AUTHENTICATION ATTACKS

Upon the discovery of user account credentials, vPenTest will automatically attempt to validate those credentials and determine where they are most useful. This is a common process executed by both malicious attackers and penetration testers and is performed during privilege escalation.

PRIVILEGE ESCALATION & LATERAL MOVEMENT

Using a valid set of credentials, vPenTest will attempt to identify valuable areas within your organization. This is conducted through a variety of methods, including the use of vPenTest's Leprechaun tool which assists in identifying where sensitive targets are.

DATA EXFILTRATION

Critical data leaving your organization is an extremely serious concern. If access to confidential and/or sensitive data can be attained, vPenTest will simulate and log this activity to help your organization tighten areas that should restrict data exfiltration.

SIMULATED MALWARE

With elevated access, vPenTest will attempt to upload malicious code into remote systems in an attempt to test the organization's end-point anti-malware controls.

REPORTS AVAILABLE WITHIN 48 HOURS

Our detailed deliverables will allow your network staff to cross reference our activities with monitoring and alerting controls.

We offer two different network penetration testing services to guide your organization to a better security posture and program.

INTERNAL NETWORK PENETRATION TESTING

Using a device connected to your internal environment, our consultants will discover security vulnerabilities present within the internal network environment. These activities simulate that of a malicious attacker.

EXTERNAL NETWORK PENETRATION TESTING

Assuming the role of a malicious attacker from the public Internet, our consultants will identify security flaws within your external network environment. These flaws can include patching, configuration, and authentication issues.