SharkStriker

Data Sheet

Network Penetration Testing

Decoding VAPT

The vulnerability assessment process involves the use of vulnerability assessment tools that identify vulnerabilities in your organization's IT assets, which have the potential to be exploited by attackers. These are systemic flaws that can leave your organization exposed to both known and unknown threats such as ransomware and more.

What is VAPT?

VAPT stands for Vulnerability Assessment and Penetration Testing (VAPT) and the acronym contains two types of testing approaches, which together offer a comprehensive vulnerability evaluation. The VAPT process includes automated vulnerability assessment, human-centric penetration testing and in certain complex scenarios, also involved red team operations

Penetration testing is used to identify the extent of weaknesses and their severity. The job of a penetration test is to find flaws and show you how damaging it could be if it is exploited by a real attacker.

Together, both Vulnerability Assessment and Penetration Testing offer a drill down view of the various flaws across different systems and their potential to put your organization's cybersecurity at risk

Necessity of VAPT

Cybercriminals are using strategies and tactics that are constantly evolving. In order to ensure your network remains safe at all times, it is imperative that it goes through periodic vulnerability assessment and testing.

Apart from delivering a 360° visibility into organizational security weaknesses and throwing light on the necessary security solution, VAPT also supports your need to meet compliances such as **GDPR, PCI DSS and ISO 27001**

Our VAPT Services

VAPT is a collection of services that make your organization more secure by identifying and addressing vulnerabilities before cybercriminals can find them. Before an organization gets started on VAPT, it is imperative they have a better idea of the services that are a part of VAPT

Vulnerability Assessment

The principal component of vulnerability assessment is vulnerability scanning; as the phrase suggests, it helps in identifying, classifying and addressing security weakness. It can also include offering solutions for risk mitigation.

Penetration Testing

Also called pen testing, this is a comprehensive vulnerability assessment that integrates human-led techniques with an advanced-tech enabled approach to test various layers of an organization's security for vulnerabilities. This test is conducted across an organization's infrastructure, systems and applications.

Types of pen testing:

- Network
- Web Application
- Mobile Application
- API
- IoT Device

Diverse VAPT Services

Reliable Security Assessment

Bolster the Security of your IT Assets:

- Web Application VAPT Service
- Mobile App VAPT Service
- Network VAPT Service
- API VAPT Service
- IOT VAPT Service

Network Penetration Testing

Fortify your network defense with our unassailable network penetration service that identifies both internal and external network vulnerabilities and experience the benefit of a secure and robust network infrastructure.

Digital transformation depends on safe, secure, and scalable network infrastructure. The strength of this infrastructure is a reliant on a dependable cyber security posture. All organizations must ensure that cybercriminals aren't able to breach their network, which makes network penetration testing of paramount importance.

It is an offensive assessment to identify security vulnerabilities in the network. Testing will expose real-world opportunities for intruders to be able to compromise systems and networks in such a way that allows for unauthorized access to sensitive data or even take-over systems for malicious purposes.

Our certified team with extensive, real-world network penetration testing experience will help you identify risks across your network, whether internal or external network.

Comprehensive Coverage

Service leverages automated asset discovery system to discover all possible IP enabled assets such as security solutions, network devices, various operating systems and services. Automated and manual penetration testing system penetrates every element of the network.

- Coverage of 50000+ Vulnerabilities
- SANS / CWE Top 25 Vulnerabilities
- PCI DSS 6.5.1 – 6.5.11 Coverage
- Credentiated / Non-Credentiated Scan
- Internal and External Network
- Asset Discovery (Host, Network, Services)
- Network Devices (Router, Switches, Wireless etc.)
- Security Solutions (Firewall, Proxy, Email Gateway etc.)
- Operating Systems (Windows, Linux, MacOS)
- Services (FTP, DHCP, DNS, FTP, SSH, SNMP etc.)

SharkStriker Methodology

Testing Methodology

- OWASP Testing Guide
  NIST SP 800-115 Technical Guide to Information Security Testing and Assessment
- PCI DSS Information Supplement: Penetration Testing Guidance
- FedRAMP Penetration Test Guidance
- ISACA's How to Audit GDPR

Reporting Standards

- Common Vulnerabilities and Exposures (CVE) Compatible
- Common Weakness Enumeration (CWE) Compatible
- Common Vulnerability Scoring System (CVSSv3)

	Essentials	Professional	Enterprise	Ultimate
SCOPE				
Internal & External Network Scan	✓	✓	✓	✓
Non-credentialed scan	✓	✓	✓	✓
Credentialed scan	✓	✓	✓	✓
Automated Penetration Testing	✓	✓	✓	✓
Manual Penetration Testing by Experts	2 experts	2+ experts	2+ experts	3+ experts
Zero False Positive	✓	✓	✓	✓
OSCP Certfied Tester	✓	✓	✓	✓
SLA	3-5 Days	5 -8 Days	8-12 Days	12-15 Days
VULNERABILITIES SCAN				
Coverage of 50K+ Vulnerabilities	✓	✓	✓	✓
Host Operating System (OS)	✓	✓	✓	✓
Database	✓	✓	✓	✓
Network (Router / Switch / Access Point etc.)	✓	✓	✓	✓
Security (Firewall / Proxy / Email Gateway etc.)	✓	✓	✓	✓
Services (FTP, DHCP, DNS, NTP, SSH, SNMP etc.)	✓	✓	✓	✓
Host Discovery	✓	✓	✓	✓
Network Discovery	✓	✓	✓	✓
Service Discovery	✓	✓	✓	✓
Unpatched Systems	✓	✓	✓	✓
Weak Communication Protocols	✓	✓	✓	✓
Backdoors	✓	✓	✓	✓
Denial of Service	✓	✓	✓	✓
Brute force attacks	✓	✓	✓	✓
CWE/SANS TOP 25	✓	✓	✓	✓
PCI DSS 6.5.1-6.5.11 FULL COVERAGE	✓	✓	✓	✓
REPORTING				
Reproduction Steps	✓	✓	✓	✓
Web, PDF, JSON, XML and CSV Formats	✓	✓	✓	✓
Remediation Guidelines	✓	✓	✓	✓
Compliance Report	✓	✓	✓	✓
CVE, CWE and CVSSv3 Scores	✓	✓	✓	✓
ACCESS TO SECURITY CONSULTANT				
24/7 Access to Security Consultant	✓	✓	✓	✓