BLACKHAWK ALERT

CYBER SECURITY SOLUTIONS

NETWORK PENETRATION TESTING WHITEPAPER

NETWORK PENETRATION TESTING

INTRODUCTION

The network penetration process utilises specialised tools to identify weaknesses in your organization's IT assets, which can be targeted by attackers. These vulnerabilities are inherent flaws that could potentially expose your organization to various threats, including but not limited to ransomware and other unknown risks.

VAPT, short for Vulnerability Assessment and Penetration Testing, encompasses two distinct testing approaches that work together to provide a comprehensive evaluation of vulnerabilities. The VAPT process involves automated vulnerability assessment, human-centric penetration testing, and, in more complex scenarios, red team operations.
Penetration testing is conducted to determine the extent and severity of weaknesses. Its purpose is to identify flaws and demonstrate the potential damage that could occur if they were exploited by a real attacker.
By combining Vulnerability Assessment and Penetration Testing, a detailed examination of flaws across various systems is obtained, providing insights into the potential risks they pose to your organization's cybersecurity.

NETWORK PENETRATION TESTING

In today's constantly evolving landscape of cyber threats, it is crucial to ensure the ongoing safety of your network. Regular vulnerability assessment and penetration testing (VAPT) are essential. By conducting these assessments, you can gain a 360° visibility into your organization's security weaknesses, identify necessary security solutions, and meet compliance requirements such as GDPR, PCI DSS, and ISO 27001.

VAPT is a comprehensive set of services designed to enhance your organization's security by proactively identifying and addressing vulnerabilities before cybercriminals can exploit them. Before embarking on VAPT, it is important to have a clear understanding of the services included within it.

VULNERABILITY ASSESSMENT

The primary component of vulnerability assessment is vulnerability scanning. This process involves identifying, classifying, and addressing security weaknesses, along with offering solutions for risk mitigation.

PENETRATION TESTING

Also known as pen testing, this is an extensive vulnerability assessment that combines human-led techniques with advanced technological approaches to test various layers of an organization's security for vulnerabilities. Penetration testing is conducted across an organization's infrastructure, systems, and applications.

Types of Pen Testing:

- Applying threat intelligence provided by our automated detection solutions.
- Monitoring user behaviour to detect internal threats.
- Understanding how threat actors attack and their preferred vectors of attack.
- Learning and developing their ability to hunt new forms and methods of attack.

To bolster the security of your IT assets, consider the following VAPT services:

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

ENHANCE YOUR NETWORK DEFENCE

In the era of digital transformation, the safety, security, and scalability of your network infrastructure are paramount. A reliable cyber security posture is essential to safeguard against network breaches by cybercriminals. Therefore, conducting network penetration testing is of utmost importance.

Our network penetration service serves as an offensive assessment to identify security vulnerabilities within your network. Through this testing, we expose real-world opportunities that intruders may exploit to compromise systems and networks, gaining unauthorized access to sensitive data or conducting malicious activities.

With our certified team, boasting extensive real-world network penetration testing experience, we help you identify risks across your network, whether internal or external.

Our service utilizes an automated asset discovery system to detect all potential IP-enabled assets, including security solutions, network devices, operating systems, and services. We employ both automated and manual penetration testing techniques to thoroughly assess every element of your network.

Key features of our VAPT service:

- Coverage of 50,000+ vulnerabilities
- SANS/CWE Top 25 Vulnerabilities
- PCI DSS 6.5.1 - 6.5.11 Coverage
- Credentialed/Non-Credentialed Scans
- Internal and External Network Assessments
- Asset Discovery (Host, Network, Services)
- Network Devices (Routers, Switches, Wireless, etc.)
- Security Solutions (Firewalls, Proxies, Email Gateways, etc.)
- Operating Systems (Windows, Linux, MacOS)
- Services (FTP, DHCP, DNS, SSH, SNMP, etc.)
- 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 Testing Methodology
- Compatibility with Common Vulnerabilities and Exposures (CVE)
- Compatibility with Common Weakness Enumeration (CWE)
- Common Vulnerability Scoring System (CVSSv3)
-

By leveraging our network penetration service, you can fortify your network infrastructure, mitigate risks, and ensure the resilience of your organization's digital assets.

NETWORK PENETRATION TESTING SERVICES

TIERS	ESSENTIALS	PROFESSIONAL	ENTERPRISE	ULTIMATE
	UP TO 25 IPS	UP TO 50 IPS	UP TO 100 IPS	UP TO 200 IPS
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 Certified Tester	✓	✓	✓	✓
SLA	5-7 days	8-10 days	12-14 days	15-17 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	✓	✓	✓	✓

SCOPE (CONTINUED)				
Backdoors	✓	✓	✓	✓
Denial of Service	✓	✓	✓	✓
Brute force attacks	✓	✓	✓	✓
CWE/SANS TOP 25				
CWE-22: Path Traversal	✓	✓	✓	✓
CWE-89: SQL Injection	✓	✓	✓	✓
CWE-78: Command injection	✓	✓	✓	✓
CWE-89: Blind SQL Injection	✓	✓	✓	✓
CWE-79: Stored XSS	✓	✓	✓	✓
CWE-90: LDAP Injection	✓	✓	✓	✓
CWE-79: Reflected XSS	✓	✓	✓	✓
CWE-91: XML Injection	✓	✓	✓	✓
CWE-79: DOM-Based XSS	✓	✓	✓	✓
CWE-93: CRLF Injection	✓	✓	✓	✓
CWE-94: Code Injection	✓	✓	✓	✓
CWE-113: HTTP Response splitting	✓	✓	✓	✓
CWE-94: AJAX Injection	✓	✓	✓	✓
CWE-200: Information Exposure	✓	✓	✓	✓
CWE-94: JSON Injection	✓	✓	✓	✓
CWE-255: Credentials Management	✓	✓	✓	✓
CWE-97: SSI injection	✓	✓	✓	✓
CWE-284: Improper Access Control	✓	✓	✓	✓
CWE-98: Remote/Local PHP File Inclusion	✓	✓	✓	✓
CWE-287: Authentication Bypass	✓	✓	✓	✓
CWE-345: Insufficient Verification of Data Authenticity	✓	✓	✓	✓
CWE-352: Cross-site request forgery (CSRF)	✓	✓	✓	✓
CWE-384: Session Fixation	✓	✓	✓	✓
CWE-400: Resource Exhaustion	✓	✓	✓	✓
CWE-434: Arbitrary File Upload	✓	✓	✓	✓
CWE-502: Deserialization of Untrusted Data	✓	✓	✓	✓
CWE-521: Weak Password Requirements	✓	✓	✓	✓

CWE/SANS TOP 25 (CONTINUED)				
CWE-601: Open Redirect	✓	✓	✓	✓
CWE-611: Improper Restriction of XML External Entity Reference (XXE)	✓	✓	✓	✓
CWE-613: Insufficient Session Expiration	✓	✓	✓	✓
CWE-643: XPath Injection	✓	✓	✓	✓
CWE-804: Guessable CAPTCHA	✓	✓	✓	✓
CWE-799: Improper Control of Interaction Frequency	✓	✓	✓	✓
CWE-918: Server-Side Request Forgery (SSRF)	✓	✓	✓	✓
CWE-942: Overly permissive Cross-domain Whitelist	✓	✓	✓	✓
PCI DSS 6.5.1-6.5.11 FULL COVERAGE				
Injection Flaws	✓	✓	✓	✓
Many other "High" Risk Vulnerabilities	✓	✓	✓	✓
Buffer Overflows	✓	✓	✓	✓
Cross-Site Scripting (XSS)	✓	✓	✓	✓
Insecure Cryptographic Storage	✓	✓	✓	✓
Improper Access Control	✓	✓	✓	✓
Insecure Communications	✓	✓	✓	✓
Cross-Site Request Forgery (CSRF)	✓	✓	✓	✓
Improper Error Handling	✓	✓	✓	✓
Broken Authentication and Session Management	✓	✓	✓	✓
REPORTING				
Reproduction Steps	✓	✓	✓	✓
Web, PDF, JSON, XML and CSV Formats	✓	✓	✓	✓
Remediation Guidelines	✓	✓	✓	✓
Compliance Report	✓	✓	✓	✓
CVE, CWE and CVSSv3 Scores	✓	✓	✓	✓
COVERAGE				
24/7 Access to Security Consultant	✓	✓	✓	✓