



Vanguard
Global Ltd.

Information Security

Penetration testing

Uncover Hidden Vulnerabilities and Confidently Secure your Applications and Network with our Comprehensive Penetration Testing Service & Reports.

What is a Penetration Test?

- A Penetration Test (also known as *Ethical Hacking*) is an authorised hacking attempt targeting an organisation's IT infrastructure, applications and staff, with the aim of gaining access into its virtual assets. The purpose of this test is to harden security defences by eliminating vulnerabilities and advising on areas that are susceptible for compromise.

Scope of the Service

- **Applications**

Our Application Testing covers Mobile Applications, Web Applications, and Web Services.

- **Networks**

Our Network Testing examines the security stance and procedures around network assets.



Benefits to Executive Management

- Independently verify your organisation's security posture and processes
- Reduce risk and incorporate Information Security into your organisation's overall risk management policy
- Avoid the high cost, legal ramifications, and damage to reputation that can result from information loss
- Leverage good security practices as a competitive advantage
- Ensure compliance with PCI DSS and other security standards
- Incorporate business objectives into your overall security program. Security management is fast becoming the domain of executive management, not just the internal IT team.



Network Penetration Testing

YOUR INFRASTRUCTURE IS A LUCRATIVE TARGET FOR HACKERS.

CAN YOUR NETWORK WITHSTAND AN ATTACK?

What is a Network Penetration Test?

- A Network Penetration Test is an authorised hacking attempt designed to uncover and exploit network vulnerabilities and gain access to an organization's information assets. The testing process is followed by a comprehensive report prioritising vulnerabilities and outlining actionable mitigation strategies.

Benefits of Network Penetration Testing

- Harden network security and maintain a proactive security posture
- Test the resilience of your network architecture and validate security configurations
- Reduce risk, and avoid the high costs, legal ramifications, and damage to reputation that may result from information loss
- Ensure compliance with PCI DSS and other security standards
- Detect misconfigured systems and identify your organisation's IT footprint on the internet
- Allow network engineers to leverage our expertise, make informed decisions, and follow best practices
- Validate resilience to malware, viruses, and worm propagation
- Detect access control vulnerabilities
- Reduce time and costs associated with managing false positives



Our scope for Network Penetration Testing



External



Wireless



Internal

EXTERNAL NETWORK PENETRATION TESTING

- EXPENDITURE ON ADDING ANOTHER SECURITY LAYER TO PROTECT YOUR NETWORK CAN BE FUTILE IF THE FUNDAMENTALS – CONFIGURATIONS, PATCHING, AND ARCHITECTURE – ARE VULNERABLE.
- A PENETRATION TEST WILL DETECT AND ELIMINATE THE VULNERABILITIES IN YOUR NETWORK.

What is an External Penetration Test?

- An External Penetration Test is an authorised hacking attempt against an organisation's internet facing servers such as web and email servers and ecommerce sites.
- This test is aimed at hardening the external facing network against attackers attempting to compromise vulnerable hosts from outside an organisation's perimeter.



Benefits of External Penetration Testing

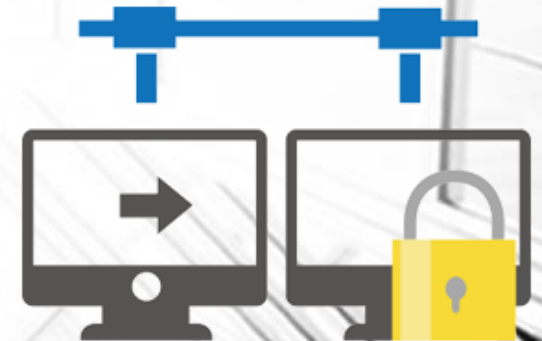
- Reduce risk to business continuity and the cost of being non-compliant
- Provide management with a proof of exploit, which outlines the assets that an attack can compromise
- Avoid the costs of adding unnecessary security layers before receiving an independent attestation on the effectiveness of current systems
- Detect known vulnerabilities and discover unknown vulnerabilities which may be exploited to access privileged information
- Audit external security monitoring procedures and test your incident response tactics
- Detect installations which are non-compliant with your internal policy and which may serve as a pivot for external attackers
- Harden systems and network against host compromise
- Get independent security verification of your organization's internet facing presence

Internal Network Penetration Testing

- An Internal Penetration Test will harden your IT Systems against attacks that can compromise your information and the integrity of your network.

What is an Internal Penetration Test?

- Internal Penetration Testing is an authorised internal hacking attempt aimed at identifying and exploiting vulnerabilities within an organization's perimeter defenses.
- Testers are typically given onsite access through an Ethernet cable (similar to the way employees or contractors could connect to an internal environment). They then attempt to escalate privileges and gain access to critical information.
- For certain environments, such as data centers, we can supply specific jump posts that we use to test remotely via your organisation's VPN access.



Benefits of Internal Penetration Testing

- Reduce risk to business continuity and the cost of being non-compliant
- Ensure compliance with PCI DSS and other security standards
- Harden your network against information leakage through current or terminated employees, or through data that may be available online
- Detect installations which are non-compliant with your organisation's internal policy, and which may serve as a pivot for external attackers
- Provide management with a proof of exploit, which outlines the assets that an attack can compromise.
- Avoid adding unnecessary security layers before receiving an independent attestation on the effectiveness of current systems
- Detect known vulnerabilities and discover unknown vulnerabilities, which may be exploited to access privileged information
- Audit security monitoring procedures and test your incident response tactics



Wireless Penetration Testing

An insecure Wi-Fi network opens up your organisation to a myriad of attacks that could compromise your critical information.

What is a Wireless Penetration Test?

- A Wireless Penetration test is an authorised hacking attempt, which is designed to detect and exploit vulnerabilities in security controls employed by a number of wireless technologies and standards, misconfigured access points, and weak security protocols.



Benefits to your business

- Ensure Compliance with PCI DSS and other security standards
- Audit security monitoring procedures and incident response tactics
- Detect vulnerabilities, misconfigured wireless devices, and rogue access points
- Reduce the risk and legal ramifications of a business breach
- Harden the wireless access path to your internal network
- Get independent security verification – of encryption and authentication policies – for devices interacting with your wireless network
- Prevent unauthorised use of your wireless network as a pivot for cyber attacks, which may be traced back to your organisation
- Provide management with a proof of exploit, which outlines the assets that an attack can compromise; such as, compromising critical data or gaining administrative level rights over routers and switches



Application Penetration Testing

Application Penetration Testing provides the highest level of assurance that an application is secure. We can also scan applications for vulnerabilities throughout development and provide guidance on best security practices.

Our scope for Application Penetration Testing



Mobile Application



Web Application

Application development best practices

- Information Security must be addressed from the onset of application development and all the way to production. Unfortunately, tight deadlines often mean that security is left as an afterthought. This leaves applications vulnerable to cyber attacks that may compromise intellectual property and critical data.
- Whether your application is live or in the planning and development phase, we can provide the testing required to ensure that your application is secure.



Benefits of Application Penetration Testing

- Ensure Compliance with PCI DSS and other security standards
- Reduce the risk and legal ramifications of a data breach, which may be caused by security flaws
- Verify alignment with OWASP, and ensure that the most common exploitation mechanisms are addressed
- Ensure encryption methodologies meet security standards before data is stored in your database
- Test crucial aspects of application security, such as: user roles, privilege escalation, password-based access controls and data authentication
- Get a threat model and actionable recommendations for your developers to follow during development, or when implementing upgrades
- Gain competitive advantage by implementing quality control over application security, and ensure the production of secure applications for internal or commercial distribution



Mobile Application Penetration Testing

- THREATS ALREADY RAMPANT ON WEB APPLICATIONS CAN BE EQUALLY EFFECTIVE ON NATIVE MOBILE APPLICATIONS, WITH CROSS SITE SCRIPTING (XSS) STILL TOPPING THE LIST.

What is a mobile application Penetration Test?

- A Mobile Application Penetration Test is an authorized and simulated hacking attempt against a native mobile application such as Android, Windows, and iOS. The purpose of this test is to identify and exploit vulnerabilities in an application, and the way it interacts and transfers data with the backend systems.



Web Application Penetration Testing

- UNTESTED APPLICATIONS REMAIN THE MOST COMMON POINT OF ATTACK ON AN ORGANISATION.
- WEB APPLICATION VULNERABILITIES HAVE RESULTED IN THE THEFT OF MILLIONS OF CREDIT CARDS, AND COMPROMISED CRITICAL INFORMATION FOR ORGANISATIONS AND END USERS.

What is a web application Penetration Test?

- A Web Application Penetration test is an authorised hacking attempt on open source and custom web applications. The aim of this test is to identify and exploit vulnerabilities relating to: authorisation, security configuration and data protection mechanisms.



Vulnerability Scanning & Assessment

SECURE YOUR ORGANISATION & SATISFY COMPLIANCE REQUIREMENTS

The only way to prevent hackers from exploiting weaknesses in your corporate defenses,
is to scan for vulnerabilities before they do.

What is a Vulnerability Assessment?


- Vulnerability Assessment is a process that scans for and identifies security holes within a network or communications infrastructure. Discovery is followed by prioritisation of vulnerabilities and provision of guidelines for counter measures.



Scope of the service

 Network Vulnerability Scanning

 Web Application Vulnerability Scanning

 Wireless Vulnerability Scanning