NMAPING SECURITY SOLUTIONS

Penetration Testing services

Realise your resilience

Find your weak points before someone else does

Motivated cybercriminals will do whatever they can to break into your systems; penetration testing replicates this behaviour through controlled ethical hacking that tests the strength of your security controls.
NMAPING SECURITY SOLUTIONS Penetration Testing Services are consultant-led security assessments which seek out security vulnerabilities in your systems, networks, or applications that an attacker could exploit.
We have a comprehensive range of testing services to meet any situation from wireless to network, web application to active directory, and many more.

We Promise

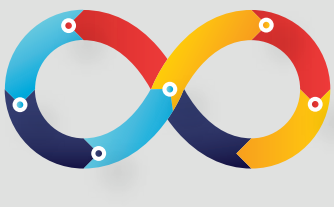
Work with you to ensure you receive the most appropriate assessment for your situation. You can explore our services in greater depth with one of our experts who will recommend which ones would be suitable for your organisation's circumstances, business objectives and obligations. Our penetration testing services are CREST

Penetration Testing Services

Web Application Penetration Testing

Mobile Application Penetration Testing

API Penetration Testing



DevSecOps

Network Penetration Testing

Cloud Penetration Testing

1. Web Application Penetration Testing

What is it?

The Web Application Testing is a comprehensive assessment of your web applications following the Open Web Application Security Project (OWASP) Top 10 testing methodology. The assessment can be carried out from following perspectives.

Black Box Assessment - Taking on the position of an anonymous malicious threat a ctor, the penetration tester is provided only the URL of the application. If there is a signup or registration element to the application this can also be included in the scope of work.

Grey Box Assessment – Representing a threat to the application from an authorised user, the penetration tester is provided with access to the application, but no information on its architecture, user base or the technologies used.

White Box Assessment – the penetration tester is provided with access to the application, full details of its architecture, user rights assignment and the technologies used to build it.

What We cover?

Security test as per OWASP standards

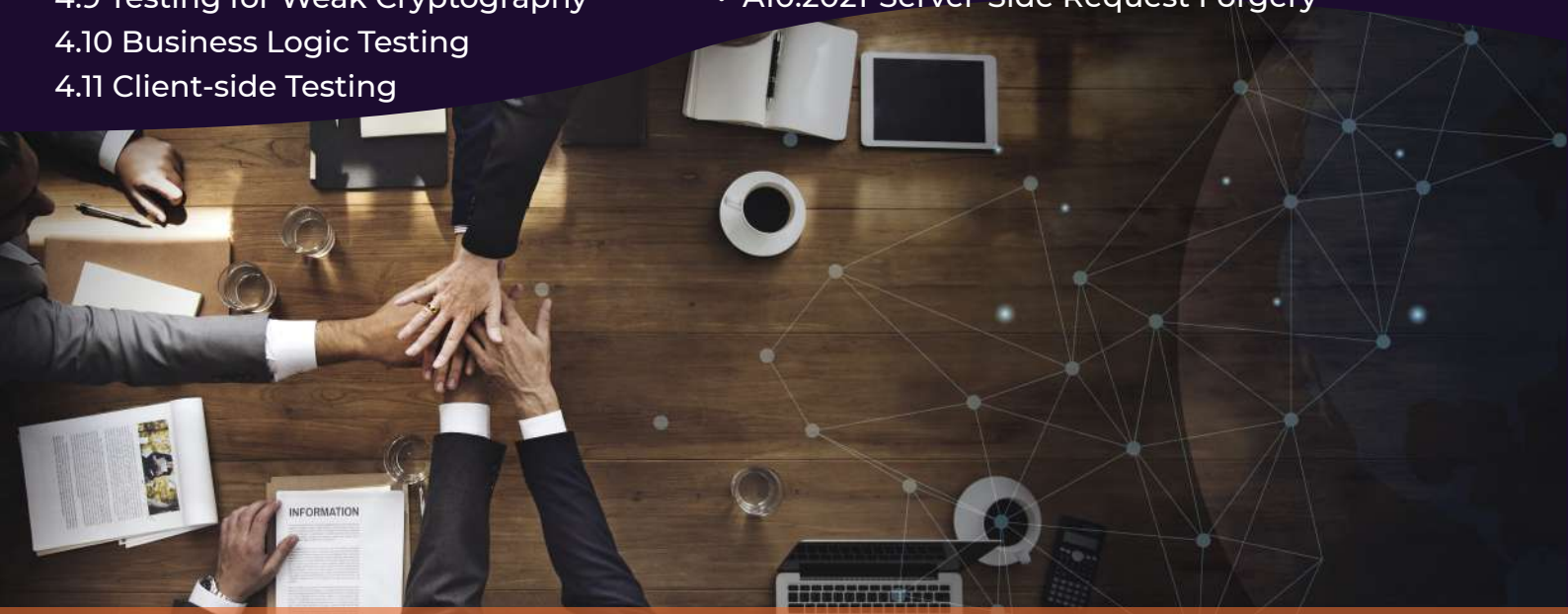
We cover

4.1 Information Gathering
4.2 Configuration and Deployment Management Testing
4.3 Identity Management Testing
4.4 Authentication Testing
4.5 Authorization Testing
4.6 Session Management Testing
4.7 Input Validation Testing
4.8 Testing for Error Handling
4.9 Testing for Weak Cryptography
4.10 Business Logic Testing
4.11 Client-side Testing

We cover

TOP 10 OWASP attacks

- A01:2021-Broken Access Control
- A02:2021-Cryptographic Failures
- A03:2021-Injection
- A04:2021-Insecure Design
- A05:2021-Security Misconfiguration
- A06:2021-Vulnerable and Outdated Components
- A07:2021-Identification and Authentication Failures
- A08:2021-Software and Data Integrity Failures
- A09:2021-Security Logging and Monitoring Failures
- A10:2021-Server-Side Request Forgery



We prepare the report as per the industry compliance standards like PCI DSS, HIPPA, ISO27001..etc

What is the output from this assessment?

A full technical report will include the following:

- Executive Summary – explanation of the vulnerabilities encountered, the risk they pose to your organisation, whether the objective was completed and recommendations of any remedial action that should be taken
- Summary of Findings – a table of all vulnerabilities noted during the assessment, the vulnerability title, its risk rating, and the vulnerability's current state

Detailed Findings:

The vulnerability's risk rating

– The system, URL or process that contains the vulnerability
– How the vulnerability was exploited
– The risk posed to the organisation
– Full technical details of how to replicate the vulnerability
– Remediation advice

When evaluating the overall risk rating for each vulnerability, the following factors will be considered

Impact – the impact that exploitation of this vulnerability will have on the business or organisation

- Risk – the risk posed to the organisation if this vulnerability was exploited
- Likelihood – the likelihood that this vulnerability could be exploited

Each vulnerability will have a remediation recommendation, which will include either:

- Official fix, such as a firmware upgrade for hardware, or a patch for a publicly disclosed vulnerability
- When there is no official fix a workaround can be used
- Process improvement for when exploitation of vulnerability is caused by a business process

BENEFITS:

Unbiased Testing:
By engaging in an indpedendant 3 rd party to complete the webapplication penetration test your organisation will be guaranteed of a report that is free from bias and internal politics.

Discover Unknown Vulnerabilities:
Understand the areas of weakness your organisation faces through the use of web applications with a in-depth analysis of the business risks and business impacts.

Reduced Risk:
Improve your organisation's defences by decreasing the number of existing vulnerablitlites before being discovered by a threat actor with malicious intent

2. Mobile Application Penetration Testing

What is it?

Mobile testing will examine and identify security vulnerabilities in mobile applications built for smart phones or tablets. The assessment encompasses the complete mobile application and any server-side APIs the application uses. It is also recommended that the application's source code is provided as this improves both the quality of findings and any recommendations.

Does this involve exploitation of vulnerabilities?

Yes. Identified vulnerabilities will be exploited to demonstrate the risk posed where possible.

Approach

The first attack phase consists of manual testing using a range of tools and techniques. The tools used include network monitoring, man-in-the-middle proxies, and reverse engineering tools. The precise tests that are performed will vary depending on the nature of the application. Typically, these will include:

- Analysis of data stored on the mobile device
- Analysis of transport layer security
- Analysis of the use of cryptography within the application
- Analysis of any binary protections that may be in place
- Validation of authentication and session management
- Source code review
- OWASP Top Ten Mobile Risks

The second attack phase consists of manual and automated testing of the server-side end point of a client-server mobile application. The tools used include network scanners, automated testing tools, and man-in-the-middle proxies.

What We cover?

We cover TOP 10 OWASP attacks

- M1: Improper Platform Usage
- M2: Insecure Data Storage
- M3: Insecure Communication
- M4: Insecure Authentication
- M5: Insufficient Cryptography
- M6: Insecure Authorization
- M7: Client Code Quality
- M8: Code Tampering
- M9: Reverse Engineering
- M10: Extraneous Functionality

We prepare the report as per the industry compliance standards like PCI DSS, HIPPA, ISO27001

3. API Penetration Testing

What is it?

The full form of API is Application Programming Interface. API is defined as a **software code that helps two different software's to communicate and exchange data with each other**
Like any software, **APIs can be compromised and your data can be stolen.** Since APIs serve as conduits that reveal applications for third-party integration, they are susceptible to attacks.

What We cover?

OWASP API Security Top 10 attacks

- API1:2019 - Broken Object Level Authorization
- API2:2019 - Broken User Authentication
- API3:2019 - Excessive Data Exposure
- API4:2019 - Lack of Resources & Rate Limiting
- API5:2019 - Broken Function Level Authorization
- API6:2019 - Mass Assignment
- API7:2019 - Security Misconfiguration
- API8:2019 – Injection
- API9:2019 - Improper Assets Management
- API10:2019 - Insufficient Logging & Monitoring

4.DevSecOps

What is it?

A transformational shift which incorporates secure culture, practices, and tools to drive visibility, collaboration, and agility of security into each phase of the DevOps pipeline

Governance

Establish security 'guardrails' and monitor results

- Redesign the operational & compliance framework
- Establish shared metrics to evaluate progress

Improve security and quality

- Increase deployment success rate
- Reduce meantime to resolve incidents
- Reduce number of open security defects

People

Break down silos between security and DevOps teams and instill cyber awareness

- Incorporate security staff in DevOps teams
- Have security teams brief dev and ops teams on current threats / exploits/breaches

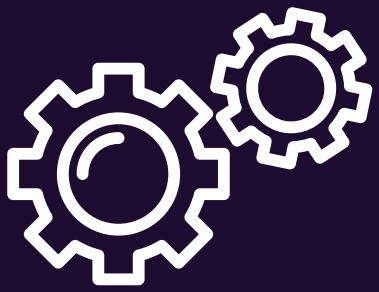
Improve time to market

- Increase production deployment frequency
- Greater speed of deployment

Process

Orchestrate an integrated process flow and drive 'in- line' risk rationalized feedback

- Asset inventory and risk awareness
- Integrated backlog and pipeline
- Security telemetry and incident response



Improve compliance feedback

- Reduction in open compliance findings
- Decrease time from audit request to evidence delivery

Technology

Automate recurring security tasks and harden the development pipeline

- Automate secure application development
- Protect the toolchain and infrastructure

Improve productivity

- More story points per sprint

SDLC Process

Requirements → Design → Development → Testing → Deployment

Secure SDLC Process

Risk Assessment → Threat Modeling & Design Review → Static Analysis → Security Testing & code Review → Security Assessment & Secure Configuration

BENEFITS:

Unbiased Testing:
By engaging in an indpedendant 3rd party to complete the web- application penetration test your organisation will be guaranteed of a report that is free from bias and internal politics

Discover Unknown Vulnerabilities:
Understand the areas of weakness your organisation faces through the use of web applications with a in-depth analysis of the business risks and business impacts

Reduced Risk:
Improve your organisation's defences by decreasing the number of existing vulnerablitlites before being discovered by a threat actor with malicious intent

5. Network Penetration Testing

What is it?

Network penetration tests simulate attacks to an organization's systems, networks, applications, or data. Network penetration testing identifies risks within the network before those risks can be exploited by unauthorized users.

Designed to mimic attacks from multiple network perspectives

- COMMON TARGETS
- SOFTWARE
- MAIL SERVERS
- NETWORK ARCHITECTURES
- WIRELESS DEVICES
- FIRE WALLS
- COMPUTER SYSTEMS

External Network Pentest

External penetration testing targets vulnerabilities within an organization's perimeter systems such as web applications, websites, email servers, or other systems accessible from the internet. A security professional assumes the role of an outside attacker trying to gain unauthorized access to sensitive organizational data. These tests are used to determine external threats to the organization.

Internal Network Pentest

Internal penetration testing targets vulnerabilities from within an organization. A penetration tester assumes the role of an attacker who has already gained access to your network and exploits vulnerabilities within an organization's internal security architectures. These tests are used to determine internal threats to the organization, including malicious threats and accidental breaches.

What is the output from this assessment?

A full technical report will include the following:

- **Executive Summary – explanation of the vulnerabilities encountered, the risk they pose to your organisation, whether the objective was completed and recommendations of any remedial action that should be taken.**
- **Summary of Findings – a table of all vulnerabilities noted during the assessment, the vulnerability title,its risk rating, and the vulnerability's current state.**
- **Detailed Findings:**
  - The vulnerability's risk rating
  - The system, URL or process that contains the vulnerability
  - How the vulnerability was exploited
  - The risk posed to the organisation
  - Full technical details of how to replicate the vulnerability
  - Remediation advice
- Appendices – vulnerability output that was noted in the engagement

When evaluating the overall risk rating for each vulnerability, the following factors will be considered:

- Impact – the impact that exploitation of this vulnerability will have on the business or organisation
- Risk – the risk posed to the organisation if this vulnerability was exploited
- Likelihood – the likelihood that this vulnerability could be exploited

Each vulnerability will have a remediation recommendation, which will include either:

- Official fix, such as a firmware upgrade for hardware,or a patch for a publicly disclosed vulnerability
- When there is no official fix a workaround can be used
- Process improvement for when exploitation of a vulnerability is caused by a business process

6. Cloud Penetration Testing

What is it?

Cloud penetration testing is a form of security assessment conducted on an environment hosted by a cloud service provider such as Amazon's AWS or Microsoft Azure. Cloud pen testing is designed to gauge the effectiveness of security controls and identify, safely exploit and help to remediate vulnerabilities before they are compromised by malicious adversaries.

Our Approach

As part of our proven methodology, Nmaping security experts:

- Work with you to understand the scope of the specific cloud-hosted environment to be evaluated.
- Conduct targeted reconnaissance to assess the attack surface of externally exposed systems and services.
- Attempt to exploit identified vulnerabilities using a combination of publicly available exploits and commercial penetration testing tools. Our experts then conduct realistic attack simulations using internally developed exploits and tools to mirror the latest attacker behaviors as seen on the frontlines.

Summary of engagement phases

Engagement outcomes

- **Executive briefing.** Overview of the service scope and critical findings for executive and senior level management
- **Technical briefing.** Engagement details that enable you to recreate the findings for future and recurring assessment
- **Risk analysis report.** Fact-based risk analysis to confirm the critical findings are relevant to your specific cloud environment
- **Actionable recommendations.** Strategic and technical recommendations for both immediate and long-term improvements to your cloud security program

BENEFITS:

Identify specific cloud-hosted attack surface risks in your specific environment

Validate security vulnerabilities in your cloud environment before an attacker exploits them

Understand the latest cloud security threats facing your organization based on front line incident response experience

Harden your cloud environment with actionable, strategic recommendations based onreal-world incidents

Assess your cloud security detection and prevention capabilities through real-world simulation exercises

ABOUT Nmaping

Nmaping is an award-winning provider of cybersecurity services, bringing innovative thought leadership to the ever-evolving cybersecurity marketplace. Leveraging our tenacious curiosity, we aim to operate at the forefront of the industry. Through our research and innovation centres, Nmaping provides threat led services that span technical assurance, consulting and managed detection and response offerings.

We are driven by a desire to build and deliver the best cybersecurity propositions in the industry and stay abreast of the evolving legislative and regulatory cybersecurity landscape. This helps our clients to prioritise their cybersecurity risks, enabling them to focus on the activities that are core to their business.

www.nmaping.com

sales@nmaping.com

+91 8977793634

No,103, Raj towers, Ayyappa society
madhapur Hyderabad 500081