Vox Penetration Test: Simulated Cyber Attacks

Vox Pentest

Discover exploitable vulnerabilities and the dangers to your business before a hacker does.

- Discover previously unknown, exploitable vulnerabilities.
- Learn how to mitigate a potential attack.
- Evaluate how a potential threat-actor could gain access.
- Ongoing testing mitigates future issues.
- Assurance of the security of a system.
- Prioritise which flaws to deal with first

Product Overview

In today's digital age, businesses are becoming more reliant on Online and Cloud services to interact with customers and provide products to the public. As a result, the rewards for people who can compromise such organisations digital security are seeing similar increases.

Not only are threats increasing daily, but they are becoming more dynamic in their complexity. This can leave defence technologies exposed – technologies which are, by nature, more static and less dynamic than the threats they face. For this reason, regular penetration tests are essential to any organisation's defensive arsenal.

Penetration tests can be useful for determining:

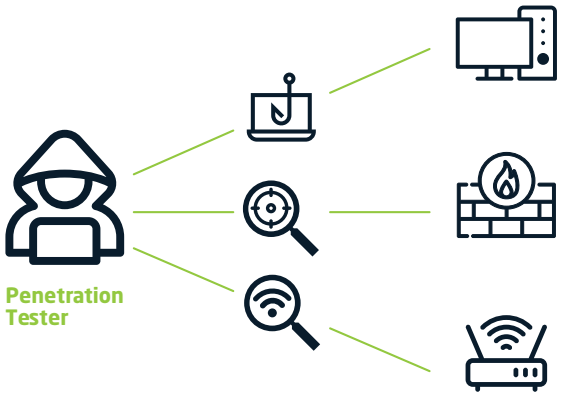
- How well the system tolerates real-world attack patterns.
- The likely level of sophistication an attacker needs to successfully compromise the system.
- Additional countermeasures to mitigate threats against the system.
- The defender's ability to detect attacks and respond appropriately.

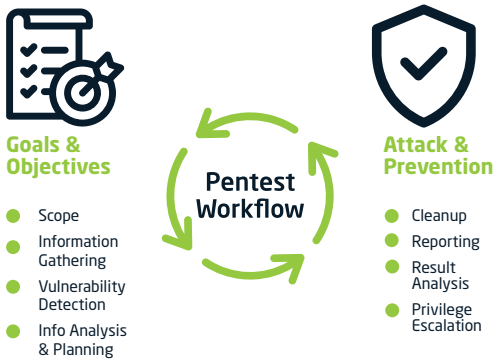
Our methodology is aligned with the Open Web Application Security Project (OWASP) testing guide, as well as a "Top 10" references and vulnerabilities system, ensuring a focused and systematic approach.

The stages involved during testing are:

- Information gathering:
  Determining the type of information that can be gathered from the web application in relation to the perimeter network or system.
- Administrative Interface:
  Investigating the security of administrative functions and interfaces.
- Authentication and Access Control:
  Investigating the authorisation, authentication and access control configurations.
- Configuration Management:
  Investigating the configuration management activities undertaken.
- Input Validation:
  Determining whether the web application can be manipulated by inserting invalid inputs to extract sensitive info or perform unauthorised functions.
- Parameter Manipulation:
  Identifying whether parameters in the web applications can be manipulated to extract sensitive information or perform unauthorised functions.
- Session Management:
  Establishing the session mechanism used and determining any security control weakness.
- Business Logic:
  Determining whether business logic controls can be bypassed.

How it Works





Features and Benefits

Features	Benefits
Gathering Publicly Available Information	Researching the environment using publicly available Data sources (such as search engines and websites) while mapping out the public footprint and pointing out areas of concern.
Network Scanning	Performing automated sweeps of IP addresses from systems provided and/or discovered, both on-network and off-network.
System Profiling	Identification of the operating system and version numbers operating on the system to focus onsubsequent tests
Service Profiling	Identification of the services and applications, as wellas their version numbers operating on the system. This allows for further focus testing on vulnerabilities associated with the identified services discovered.
Vulnerability Identification, Validation and Exploitation	Potential vulnerabilities or control weaknesses applicable to the system are researched, tested and identified. Once these vulnerabilities are identified, they must be validated to minimise errors and false reports which involve attempts to exploit the vulnerability.
Privilege Escalation	Should exploitation of vulnerability be successful, attempts are made to escalate the privileges and obtain "complete control" of the system.

Additional Information

Our testing methodology was developed in line with recommendations from the following sources:

- Open Web Application Security Project (OWASP) Testing Guide version 4.
- OWASP Top 10 2020 – The Ten Most Critical Web Application Security Risks
- Payment Card Industry (PCI) Penetration Testing Guidance (PCI-DSS PTG v1.1)
- Technical Guide to Information Security Testing and Assessment (NIST 800-115)
- MITRE Attack Framework

These recommendations have been combined into a common testing methodology which is agile and can be customised according to various testing scenarios and environments.

About Vox

Innovation and insight combine in Vox - a market leading end-to-end integrated ICT and infrastructure provider and telecommunications company. From data to voice - as well as Cloud, business collaboration and conferencing tools - Vox offers intelligent solutions that connect South Africans to the world, supporting entrepreneurs, customers and commerce, whilst practicing values of integrity, choice and service excellence in all of its dealings. For more information **click here.**

For more information on complementary or alternative products, visit us at vox.co.za

New Business Sales JHB : +27 (0) 87 805 5050
Consumer Support : +27 (0) 87 805 0530
Business Support : +27 (0) 87 805 0500
Email: info@voxtelecom.co.za