Penetration Testing Cheat Sheet 2024

What is Penetration testing?

Penetration testing is a simulated cyberattack aimed at identifying and exploiting vulnerabilities in systems, networks, or applications to assess their security posture and resilience against real-world threats.

Types of Penetration Tests:

External Testing

Targets internet-visible assets like websites and servers.

Internal Testing

Simulates internal threats, assessing potential damage.

Web Application Testing

Identifies vulnerabilities in web apps, APIs, and servers.

Wireless Testing

Evaluates WLAN security and related protocols (Bluetooth, ZigBee).

Mobile Application Testing

Finds vulnerabilities in mobile apps on smartphones and tablets.

When to Conduct a Penetration Test:

- After Significant Changes to Your IT Infrastructure
- Regularly Scheduled Intervals **(at least once annually)**
- In Response to New Threats
- Compliance Requirements
- Prior to Launch of New Services

The 5 Stages of a Penetration Test:

1. **Reconnaissance:** Gather essential info about systems (Black, White, Grey Box Testing).
2. **Scanning:** Use tools to find vulnerabilities like open ports and services.
3. **Vulnerability Assessment:** Identify and analyze vulnerabilities using collected data.
4. **Exploitation:** Actively attempt to exploit identified vulnerabilities.
5. **Reporting:** Produce a detailed report with findings and recommendations.

Essential Pen-Testing Tools:

OP Innovate WASP

Continuous penetration testing with attack surface management (ASM).

Network Scanning

Nmap, Wireshark, Aircrack-ng, Cobalt Strike

Vulnerability Scanning

Nessus, OpenVAS.

Social Engineering

Social Engineer Toolkit (SET).

Password Cracking

John the Ripper, Hashcat.

Exploitation Frameworks

Metasploit.

OP Innovate's Penetration Testing as a Service (PTaaS):

OP Innovate's PTaaS offering combines expert manual penetration testing with cutting-edge automated testing and Attack Surface Management (ASM) to enable continuous security for applications.

With routine pen test sprints conducted by a CREST-certified offensive security team and the innovative WASP platform providing continuous scanning and reconnaissance, you can stay one step ahead of cyber threats while maximizing your resources.

Get in touch now to get started 👉👉👉

www.op-c.net

contactus@op-c.net

+972 54-677-6338