ARANCIA

UNCOVER AND REMEDIATE YOUR SECURITY GAPS

PENETRATION TESTING SERVICES

ARANCIA'S PENETRATION TESTING SERVICES

Arancia's penetration testing services empower security leaders to proactively identify and address vulnerabilities across your critical infrastructure, web applications, APIs, mobile apps, and OT/IoT systems. Our team of certified professionals leverages industry-leading methodologies and advanced tools to simulate real-world attacks, exposing weaknesses before malicious actors can exploit them.

WHY PENETRATION TESTING IS CRUCIAL

In today's ever-evolving threat landscape, a single security breach can have devastating consequences. Penetration testing provides a critical line of defense by:

PROACTIVE DEFENSE

Penetration testing helps identify and remediate vulnerabilities before they can be exploited by malicious actors.

REGULATORY COMPLIANCE

Regular testing ensures compliance with industry standards and regulations, protecting your business from legal and financial penalties.

RISK MITIGATION

By understanding potential threats, you can implement effective countermeasures, minimizing the risk of data breaches and cyber-attacks.

WHY CHOOSE US?

Threat-Focused Approach

We utilize a robust threat modeling process to tailor testing scenarios to the specific risks facing your organization.

Meticulous Process

Our structured approach ensures a comprehensive assessment, encompassing planning, reconnaissance, scanning, exploitation, post-exploitation, and detailed reporting.

Industry Expertise

Our team holds industry-recognized certifications and possesses in-depth knowledge of the latest vulnerabilities and attack vectors.

Advanced Techniques

We employ cutting-edge tools and methodologies to deliver thorough and accurate assessments.

OUR APPROACH: THREAT MODELLING

1 SCOPE

We define the testing scope to ensure relevance and applicability to your systems and applications.

2 REAL-WORLD SCENARIOS

We evaluate potential threats based on realistic scenarios related to your environment.

3 LIMITATIONS

We consider barriers such as firewalls and other security measures that may impact threat exploitation.

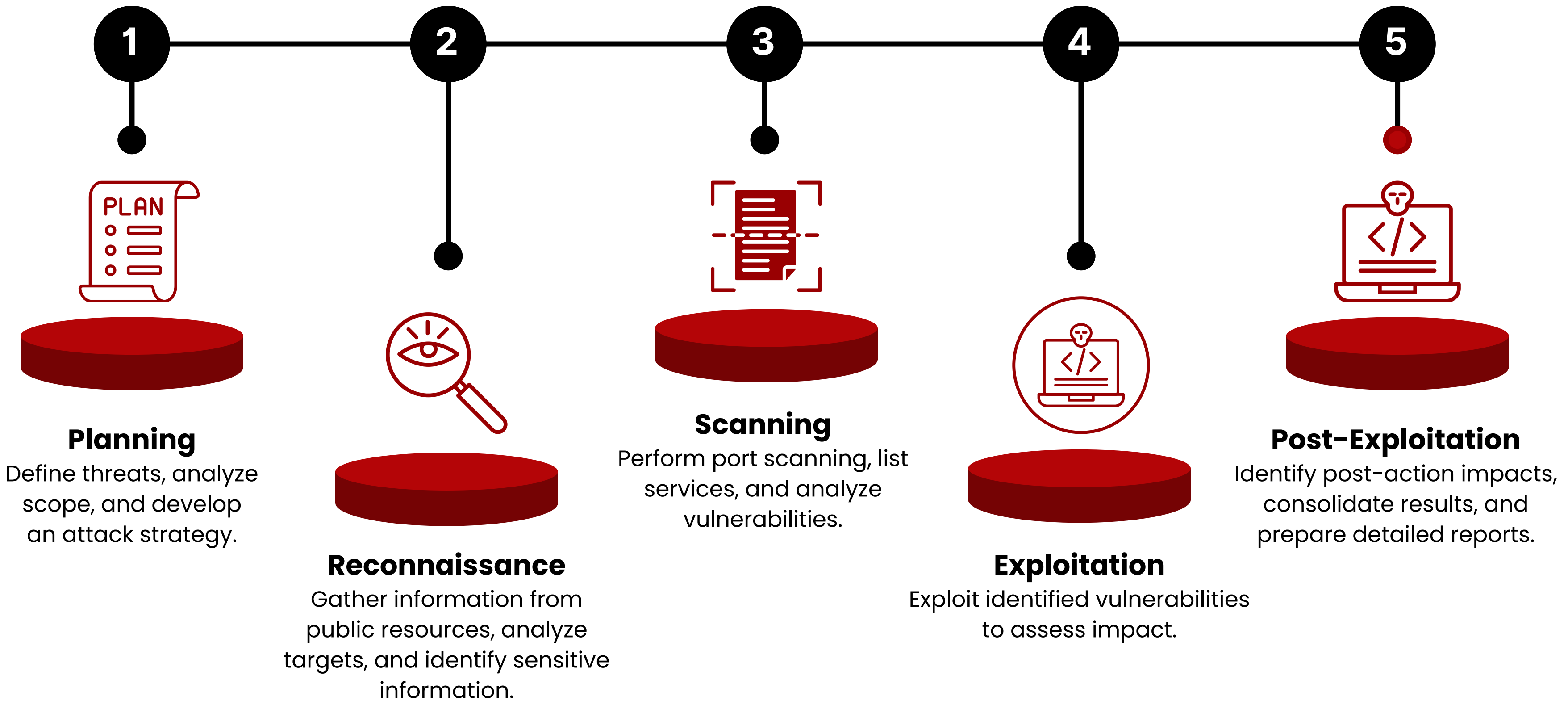
4 MOTIVATIONS

We assess potential threat motivations, including financial gain and access to sensitive data.

5 COMMON THREAT EXAMPLES

Internal employees, external cybercriminals, untrusted visitors, outsourced employees, and more.

PEN TEST PROCESS



1 **Planning**
Define threats, analyze scope, and develop an attack strategy.

2 **Reconnaissance**
Gather information from public resources, analyze targets, and identify sensitive information.

3 **Scanning**
Perform port scanning, list services, and analyze vulnerabilities.

4 **Exploitation**
Exploit identified vulnerabilities to assess impact.

5 **Post-Exploitation**
Identify post-action impacts, consolidate results, and prepare detailed reports.

TYPES OF TESTING

Blackbox Testing

Performing a security test without prior knowledge of the internal workings of the target system, representing an unauthenticated test.

Whitebox Testing

Conducting an internal assessment with complete knowledge of the system's architecture and source code, representing an authenticated test.

Greybox Testing

Conducting a security test with partial knowledge of the target system, focusing on specific areas of interest, representing an authenticated test.

PENETRATION TESTING SERVICES

- **Web Application Penetration Testing:** Our skilled team identifies and exploits vulnerabilities in web applications using industry-leading tools and manual testing techniques.
    - **Common Vulnerabilities Tested Based on OWASP Top 10 Items like:** Broken Access Control, Cryptographic Failures, Injection, Insecure Design, Security Misconfiguration, Vulnerable and Outdated Components, Identification and Authentication Failures, Software and Data Integrity Failures, Security Logging and Monitoring Failures, Server-Side Request Forgery (SSRF).
- **Network Penetration Testing:** Our experts utilize advanced tools to discover and exploit weaknesses in your network infrastructure and security controls.
    - **Common Vulnerabilities Tested:** Open ports, Weak passwords, Misconfigured firewalls, Insecure remote access, Unsecured wireless networks, and more.
- **API Penetration Testing:** We assess the security of your APIs, identifying vulnerabilities that could lead to unauthorized access or data breaches.
- **Mobile Application Penetration Testing:** Our team evaluates your mobile applications for vulnerabilities specific to the Android and iOS platforms.
- **Operational Technology (OT) & Internet of Things (IoT) Penetration Testing:** We assess the security of your OT/IoT systems to ensure they are resilient against cyberattacks.
- **SAST/DAST:** We provide Static Application Security Testing (SAST) and Dynamic Application Security Testing (DAST) to identify vulnerabilities at different stages of your software development lifecycle.
- **Code Reviews:** Our team conducts in-depth code reviews to uncover security flaws, ensuring your applications are robust and secure.

ARANCIA

Protect Your Organization, Proactively.
Contact Arancia today to discuss your penetration testing needs and gain a comprehensive understanding of your security posture.