Ethic ec

Home Services ▾ Order

Infrastructure Security Testing

Fortify your network infrastructure against external and internal vulnerabilities.

Contact Us

Infrastructure Security Testing

Protect your infrastructure from potential breaches with our customized testing options:

Automated External Infrastructure Vulnerability Scanning

- Efficient scans to identify vulnerabilities in external infrastructure.
- Price: €300/day | Duration**:** 1 day per 50 IPs (including reporting).
- Get a full analysis of detected vulnerabilities with expert advice on remediation.

External Infrastructure Penetration Testing

- Simulates real-world external attacks to identify exploitable vulnerabilities and misconfigurations.
- Price: €600 (2 days) minimum | Duration**:** 2 days for up to 50 IPs + €300/day for additional scope.
- Includes both automated and manual testing from an external attacker's perspective, with a comprehensive vulnerability report and remediation recommendations.

Internal Infrastructure Penetration Testing

- Simulates attacks from within your network to expose deeper issues.
- Price: €900 (3 days) minimum | Duration**:** Minimum 3 days (scope defined in kick-off meeting).
- In-depth testing using internal access and insights into your infrastructure's security posture.

Order Now

Explore Service Details

	Automated Vulnerability Scanning	**External Infrastructure Penetration Testing**	**Internal Infrastructure Penetration Testing**
Prerequisites	IP Addresses	IP Addresses	IP Addresses, VPN access, User credentials, Infrastructure Insights
Test Type	Automated	Automated and Manual	Automated and Manual with Internal Knowledge
Actions	Identify and Report vulnerabilities	Identify, Exploit and Report vulnerabilities	Identify, Exploit and Report vulnerabilities
Used Tools	Nessus, Nmap	Nessus, Nmap, Metasploit, Crackmapexec, Hydra, Impacket, Snmpwalk, Netcat, etc.	Nessus, Nmap, Metasploit, Crackmapexec, Responder, Hydra, Impacket, Snmpwalk, Netcat, Mimikatz, Bloodhound, **PingCastle,** Rubeus, Powershell scripts, psexec, etc.
Covered Vulnerabilities	• Outdated software and patch management issues. • Misconfigured services and protocols. • Weak or default credentials on network devices. • Open ports and services exposing sensitive information. • SSL/TLS configuration issues. • Publicly known vulnerabilities (CVE-based scanning).	All the vulnerabilities from the Automated Vulnerability Scanning plus the following: • Weak perimeter defenses, such as misconfigured firewalls or VPNs. • Exploitable open ports and services. • Credential brute-forcing on exposed services (e.g., SSH, RDP). • Insecure file-sharing protocols (SMB, FTP, etc.). • Publicly exposed sensitive data or misconfigured DNS settings. • Vulnerabilities in web server configurations or hosted applications. • Exploitable vulnerabilities in third-party software or systems. • Inadequate email security configurations (e.g., SPF, DKIM, DMARC).	All the vulnerabilities from the Automated Vulnerability Scanning and External Infrastructure Penetration Testing plus the following: • Sensitive information exposure in file shares or internal applications. • Insufficient network segmentation. • Insecure protocol usage (e.g., outdated SMB or Telnet). • Lateral movement vulnerabilities, such as unprotected admin shares or misconfigured RDP. • Weak or outdated encryption on internal communications. • Privilege escalation opportunities (e.g., misconfigured services or applications). • Insecure Active Directory configurations, such as weak Kerberos policies or mismanaged group permissions.

			• Credential harvesting and reuse attacks (e.g., NTLMv2 relay, pass-the-hash, pass-the-ticket).
Reporting	Comprehensive Report with Automated findings with expert review and remediation guidance.	Comprehensive Report with vulnerability details, exploit paths, risk assessment, and Remediation Recommendations.	Comprehensive Report with vulnerability details, exploit paths, risk assessment, and Remediation Recommendations.
Duration	24 hours / 50 IPs	48 hours / 50 IPs	72 hours minimum (depending on the company size)
Price	€300/24 hours	€600 (2 days) minimum + €300/additional day	€900 (3 days) minimum + €300/additional day

Order Now

Order Now

Order Now

Step-by-Step Process

1. Order Service Request

The client orders a "Service Request" by completing the contact form, providing the details of the resources in scope, a brief project description, and contact information.

2. Scope Review & Kick-Off (if applicable)

We review the Service Request and, if necessary, schedule a 30-minute kick-off meeting to discuss the effort estimation, project timeline, and details regarding the in-scope resources. For Black-Box tests, we can proceed directly to the next step.

3. Contract and Payment

Once the details are agreed upon, we send the client a contract and invoice. After the contract is signed and payment is received, we begin the testing phase.

4. Testing Execution

Our expert team conducts a combination of automated and manual tests, simulating real-world attack scenarios to uncover vulnerabilities and assess security posture.

5. Report Delivery

Upon completion, you'll receive a comprehensive report detailing identified vulnerabilities, their severity levels, and actionable recommendations to enhance your security.

Subscribe to our newsletter

Email address

Your email address

Submit

Contact

office@ethicsec.com

Hours

Mon-Fri: 9am-5pm

Socials