INTERNAL PENETRATION TESTING

WHY CHOOSE MOBIUS BINARY?

Threats don't just come from the outside. Internal security gaps can pose significant risks, whether from insider threats, compromised credentials, or lateral movement within your network. Mobius Binary's Internal Penetration Testing simulates real-world attack scenarios to identify vulnerabilities before they can be exploited, helping you strengthen your security posture from within.

- **Expert Security Team –** Our specialists hold top certifications, including **OSCP, CREST CRT, GPEN, and eWPTX.**
- **Global Expertise –** With over 200 projects completed across 16+ countries, we bring extensive experience in securing diverse IT environments.
- **CREST Accredited –** We adhere to the highest industry standards in ethical hacking and security testing.
- **Industry-Leading Standards –** Testing methodologies based on **MITRE ATT&CK, NIST, and PTES frameworks.**
- **Tailored Attack Scenarios –** We design test scenarios customised to your specific business risks and industry challenges.
- **Real-World Threat Simulation –** Our penetration testers replicate the latest attack techniques used by cybercriminals.
- **Comprehensive Reporting –** Beyond identifying vulnerabilities, we provide clear insights with practical remediation steps.

WHAT IS INTERNAL PENETRATION TESTING?

Internal Penetration Testing assesses your internal IT environment, including workstations, servers, databases, Active Directory, and internal applications. Our security experts emulate the tactics of real-world attackers who have bypassed perimeter defences to evaluate how easily they could escalate privileges, exfiltrate sensitive data, or disrupt business operations.

CLEARLY SECURE. GLOBALLY TRUSTED. ALWAYS ONE STEP AHEAD.

MOBIUS BINARY
Clearly secure

CREST PEN TEST

Email: info@mobiusbinary.com | **Website:** mobiusbinary.com

INTERNAL PENETRATION TESTING

OUR APPROACH: A STEP-BY-STEP ATTACK SIMULATION

At Mobius Binary, we follow a structured, industry-recognised methodology to assess your internal security defences thoroughly:

1. **Initial Foothold –** From a non-domain joined machine, we attempt to gain initial access to your internal network using attacks such as default credentials, Pass-the-Hash, poisoning, or other attack vectors.
2. **Lateral Movement –** Once an initial foothold is obtained, we simulate an attacker's ability to move across systems, escalating access to critical resources.
3. **Privilege Escalation –** We test privilege escalation techniques to assess whether attackers could elevate their access to administrative levels.
4. **Domain Compromise –** We evaluate the risk of full domain compromise, determining whether attackers can seize control of key infrastructure components.

We adhere to globally recognised frameworks, including CREST, MITRE ATT&CK, PTES, NIST, and OSSTMM, ensuring industry-leading quality in security testing.

KEY BENEFITS:

PROACTIVE RISK MANAGEMENT	From a non-domain joined machine, we attempt to gain initial access to your internal network using attacks such as default credentials, Pass-the-Hash, poisoning, or other attack vectors.
REGULATORY & COMPLIANCE ALIGNMENT	Satisfy security requirements for frameworks like ISO 27001, PCI DSS, GDPR, and more.
ENHANCED INSIDER THREAT DETECTION	Strengthen monitoring and response against malicious insiders or compromised accounts.
IMPROVED NETWORK SEGMENTATION	Ensure that lateral movement within your network is restricted and controlled.
STRENGTHENED ENDPOINT & USER SECURITY	Test workstation and user security to prevent unauthorised privilege escalation.

GET STARTED WITH MOBIUS BINARY TODAY

Your internal security is as critical as your external defences. Whether you require a one-time assessment or ongoing security testing, Mobius Binary is ready to help you stay ahead of emerging threats.

SECURE YOUR DIGITAL BOUNDARIES.

MOBIUS BINARY
Clearly secure

CREST PEN TEST

Email: info@mobiusbinary.com | **Website:** mobiusbinary.com