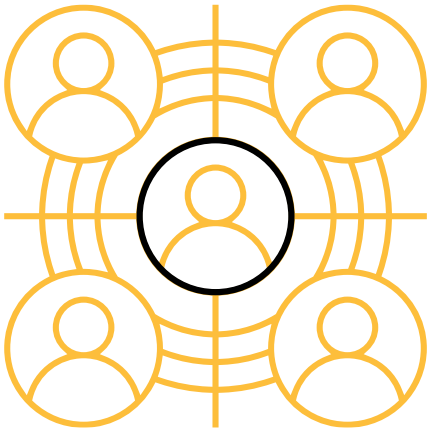
Lodestone

SERVICE BRIEF FOR

PENETRATION TESTING



Lodestone Penetration Testing thoroughly assesses the effectiveness of your organization's security controls, both internal and external, and identifies weaknesses that could result in a future compromise. We cover both your external network boundary, where all devices and services directly connected and exposed to the Internet reside, and your internal network boundary, where all of your connected devices reside behind a firewall.

Our engineers use industry-standard penetration testing tactics, techniques, and procedures (TTPs) and methodologies to identify vulnerabilities that could be a common entry point for a threat actor, and those that could provide the most information to a threat actor that manages to infiltrate your environment.

Internal or external Penetration Testing performed by Lodestone's Offensive Security Services team equips your organization with actionable findings that can be used to strengthen your security posture and reduce your attack surface. Using TTPs actual threat actors use in the wild, the Lodestone's engineers will help you identify vulnerabilities and missing security controls that could put your company at risk of compromise or unauthorized access to internal resources.

We are with you every step of the way to inform you of any critical findings that require immediate action and ensure that testing does not interrupt your critical business functions. We ensure the findings and their impacts are clearly defined for your future remediation efforts.

BENEFITS

- Reduction of your internal and external attack surfaces by remediating identified vulnerabilities to mature the security posture of your organization.
- Assist your organization with maintaining compliance with a number of business standards and reputations, such as the Health Information Portability and Accountability Act (HIPAA) and the Payment Card Industry Data Security Standard (PCI-DSS).
- Knowledge that will enable you to create an optimized roadmap for allocating your security budget, protecting your company's image and reputation, and communicating the importance of addressing cybersecurity risks to key stakeholders and executives.

METHODOLOGY

The Penetration Testing is comprised of these primary phases:

- Testing Scope – We work with you to determine the scope of the external and internal environments and narrow down what the penetration test will cover. For external environments, this may include email portals, web applications, VPN portals, or file-sharing applications. For internal testing, this may include certain subnets and internal services that will either be in scope or out of scope for testing.
- Reconnaissance and OSINT – Lodestone uses automated tools and manual research to gather information passively. Reconnaissance is the first step in vulnerability assessments and penetration tests and is crucial for any adversary seeking entry into an organization. It includes searching for Internet-facing servers, web applications, subdomains, employee information, physical addresses, phone numbers, email accounts, credentials, and any other information that could be used to enter the network.
- Target Enumeration – In this stage, testers begin to enumerate the services running on open ports discovered from open-source intelligence (OSINT). These services are researched to gain information from the open service and formulate attack paths and potential methods for exploitation.
- Vulnerability Detection – From the engagement scope, different tools are utilized by our engineers to enumerate potential vulnerabilities on externally facing hosts.
- Exploitation
  - Findings uncovered from target enumeration and vulnerability detection are tested to see if they can be exploited as they would be by a threat actor. We identify which vulnerabilities are false positives that do not threaten your organization.
  - Lodestone engineers use any successfully exploited vulnerabilities to determine what information they can access and use this access to escalate privileges, exfiltrate data, and pivot to other devices and services.
- Reporting – All findings will be compiled into a report that includes details on our methodology and the testing performed, key findings, and recommendations for remediation.
- Report Review – We provide our clients at least two weeks to review the reports and formulate any questions or requests for clarification. At the end of every engagement, a report review call is scheduled to ensure that all of your concerns are addressed.

ENGAGEMENT ARTIFACTS

The following artifacts will be obtained by our team as part of the assessment:

- List of internal IP address ranges
- List of external IP address ranges
- Usernames and passwords for credentialed scanning
- Screenshots and information used for deliverables

DURATION AND DELIVERABLES

A penetration test varies in duration based on the size of your environment, the number of systems, and findings, but typically takes two to three weeks. It can be delivered on-premises or remotely.

Lodestone will provide the following deliverables to you as part of the engagement:

	Weekly Status Reporting – Lodestone will provide a weekly or bi-weekly status report to the project sponsor once the kickoff call is complete. Lodestone can accommodate your preferred communications, including via phone call or email.
	Executive Summary Report – Lodestone will provide a high-level report on the engagement, findings, and any recommendations, if applicable.
	Final Report – After the engagement completion, Lodestone will provide a final report that details the engagement, findings, and recommendations for mitigating the findings.

Connect with us:
www.lodestone.com
320 East Main Street, Lewisville, TX 75057, USA
Tel: +1-203-307-4984
info@lodestone.com

Lodestone is a global cybersecurity firm committed to helping clients prevent and investigate security incidents. It is comprised of top talent from private industry, government, intelligence, and law enforcement specializing in incident response, digital forensics, offensive security, risk management, and threat detection.