SENTINEL®

ALWAYS LEADING

Mobile Access PEN Test

Sentinel penetration test experts will test your remote worker security now!

The COVID-19 pandemic has thrust us into a situation where working from home is not only supported by organizations, but mandated by federal and state governments. The rush to support mass amounts of remote workers has pressured many organizations to compromise their cyber security governance and protection in the name of expediency. It has also strained technology suppliers, forcing some organizations to compromise their standards and accept inferior solutions so workers can be productive at home. Adding to these challenges, cyber criminals are acutely aware that security standards and protection have been weakened in order to address the immediacy of access, so they are actively attempting to compromise your systems today!

Sentinel's Remote Access PEN Test challenges an organization's security posture from a remote worker perspective. Our expert penetration testers take on the role of one of your remote workers in order to uncover your areas of risk and help with hardening your systems as quickly as possible. We approach your systems from the standpoint of a compromised endpoint with access to your VPN, and will identify and exploit any visible holes within your security infrastructure. This will test your protection, detection, and response to a cyber threat entering your enterprise from a home worker and moving laterally to monetize the attack or steal your data. This is done without disruption and in parallel to your workers' continued productivity.

Sentinel experts, armed with first-hand experience in your network, will provide immediate recommendations for preventing an attack. These recommendations include practical actions to **swiftly secure your mobile workforce, often leveraging currently available no cost protection and detection technologies**. The results will help your organization establish a preventative security approach and continued work from home productivity with a much lower risk of data exfiltration, destruction, and/or successful ransomware attack.

Service Overview

- **Recon** – Sentinel's penetration testing experts will review your systems from the VPN, review resources, and identify weaknesses.
- **Attack** – Experts will perform ethical and non-intrusive penetration testing, not only identifying systems for vulnerabilities but exploiting identified weaknesses.
- **Report** – A final report will be presented, findings reviewed, and remediation recommended for the immediate, near-term and long-term security posture of your organization.

Benefits:

- Provide remote workers with **in-office levels of productivity during the COVID-19** pandemic and remain at home government orders
- **Rapidly Identify areas of risk** in your remote access infrastructure using lateral movement through your network systems
- Active penetration testing will help **determine your weaknesses without disruption**, moving beyond simply identifying vulnerabilities and reporting
- Assessment results presented with **real examples and explanations** of what a hacker with malicious intent could compromise within your enterprise
- Learn from Sentinel experts about available solutions to **protect you NOW!**

Confidential information property of Sentinel Technologies

HOW IT WORKS

Sentinel provides this service in a rapid manner and simply requires access to your VPN service as if a typical remote user. We will assume the position of a compromised end user with VPN access to your systems. Once connected to your network, Sentinel experts perform a remote access PEN test including:

Phase 1 — Reconnaissance

At this stage, our experts explore your systems looking at what is visible within your enterprise. Our ethical penetration testers may perform vulnerability reviews, brute-force attacks, or use other common (and not so common) means to attempt to identify the weakest points with highest probability of critical access.

Phase 2 — Attack (Gentle Penetration Testing)

Once reconnaissance is complete, Sentinel's PEN testers will actively perform simple and advanced hacking techniques on your systems. Intended to be non-disruptive, our experts will attempt to gain access to critical systems, move laterally, and also try to expose ourselves to detection in place to "test" your detection technologies or services.

Phase 3 — Reporting and Results

Sentinel experts are highly likely to penetrate one or many of your internal systems with VPN access. Using the results of the test, Sentinel will report on what your remote access risks are and what type of exposure exists from a criminal hacker's perspective. This insight is critical in assessing your risk, determining immediate and near-term remediation, and making the best protection and detection investments to support your mobile workforce today.

ENGAGEMENT DETAILS

Sentinel has put together an express mobility worker penetration testing engagement in order to meet the IT challenges surrounding the COVID-19 threat. This service includes:

- Quote, contract, and scope for remote worker penetration testing
- Initiation call to begin the service to ensure a full understanding of the scope and expectations of the engagement
- Over the coming days, Sentinel will non-disruptively perform this service against your systems without creating any actual damage or outages
- Sentinel will rapidly provide a report and review over a conference bridge
- Express reporting will provide actionable insights to help you protect your assets immediately

Mobility PEN Testing Investment $6,800

Contact Sentinel today to schedule your engagement!

Confidential information property of Sentinel Technologies

Sentinel Advisory Services

Sentinel's Advisory experts are available to assist with the following related services and can define custom executive services engagements to meet your cyber security needs.

SECURITY ASSESSMENT

Experts from Sentinel examine your organization's current security posture to provide insights and recommend improvements intended to significantly mitigate any risks

VULNERABILITY ASSESSMENT

A program that detects and classifies any weaknesses throughout your company's system, network and applications where an attack might occur, and calculates the efficacy of countermeasures

PENETRATION TESTING

An authorized tester attempts to gain access to protected resources and data contained within your system, network, or applications to uncover security flaws that could be exploited in a legitimate attack

IT SECURITY GOVERNANCE

Sentinel analyzes your infrastructure and framework to ensure all security components and strategies align with business objectives, comply with current regulations, and provide proper oversight to manage risk