SOLUTION BRIEF

Uncover Potential Security Gaps with FortiGuard Penetration Testing Services

Executive Summary

Threat actors are continually looking for holes in an organization's security "armor" to gain an initial foothold on the network. Security gaps are lurking in every enterprise's environment, ranging from a misconfigured service or application, a known or unknown vulnerability, or a login using credentials posted to the dark web. Regardless of which gaps exist, malicious actors are adept at finding and exploiting even the slightest weakness.

With the FortiGuard Penetration Testing Service, you'll gain an understanding of the previously unknown vulnerabilities and weaknesses in your environment that a threat actor could easily use to find their way into your organization's network. By getting a better picture of what the threat actor may be able to leverage, you can then prioritize your remediation efforts around these discovered gaps.

Fortinet data shows that over the last five years, unique exploit detections are up 68%, making detecting and remediating known and unknown vulnerabilities much more important.[1]

What Is the FortiGuard Penetration Testing Service?

The FortiGuard Penetration Testing Service is a specialized assessment our team conducts on networks, systems, and applications to identify unknown vulnerabilities that an adversary could exploit. Penetration testing mimics real-world attacks to pinpoint potential ways that threat actors might impact the confidentiality, integrity, or availability of your networks, systems, and applications. When conducting a penetration test, our team of experts uses various tools and techniques commonly utilized by attackers to detect vulnerabilities and test the resilience of your organization's network.

Penetration Testing Focus Areas

During penetration tests, our team can focus on a variety of areas, such as:

Focus Area	
Internal Networks	Our team is equipped to conduct internal network penetration testing to evaluate threats to your organization's internal network and devices. These assessments are scoped based on the number of IP addresses included.
External Networks	External network penetration testing focuses on the external, or internet-facing, systems your organization makes available, including web servers, database servers, network devices, and other network-based equipment. These assessments are scoped based on the number of IP addresses included.
Web Applications	The FortiGuard Web Application Vulnerability Penetration Test focuses on one or more web applications with the goal of identifying known and previously unknown vulnerabilities within the application. The test also evaluates the ability to use discovered vulnerabilities to further penetrate the organization. It looks for areas where somebody could compromise the confidentiality, availability, or integrity of systems or data. These assessments are scoped based on the number of your organization's web applications.
Mobile Applications	The FortiGuard Mobile Application Penetration Test focuses on one or more mobile applications with the goal of identifying either known or unknown vulnerabilities within the application. The test also evaluates the ability to use discovered vulnerabilities to further penetrate the organization. It looks for areas where somebody could compromise the confidentiality, availability, or integrity of systems or data. These assessments are scoped based on the number of your organization's mobile applications.

> Nearly 57% of organizations that the FortiGuard Incident Response team has assisted have failed to apply patches to known vulnerabilities within a reasonable time frame.[2]

How the Assessment Works

There are several methodologies our team uses when conducting the penetration test. The approach we take is primarily based on the information shared with our team of testers. The main methodologies we rely on include:

- **Black box penetration testing**: In a black box assessment, the assessor has no prior knowledge of the organization's IT infrastructure. This type of penetration testing is often used to test the security of an organization's external-facing assets.
- **White box penetration testing**: In a white box assessment, the assessor has full knowledge of the organization's IT infrastructure. This type of penetration testing is often used to test the security of an organization's internal assets.
- **Grey box penetration testing**: A grey box assessment is a black-and-white box penetration testing hybrid. The assessor has some knowledge of the organization's IT infrastructure but not as much as having full visibility as they would with a white box test.

Schedule Your Penetration Test Today

Penetration tests are an essential part of any organization's security program. With a FortiGuard Penetration Test, you can comprehensively understand your security posture, discover where gaps exist, and prioritize and plug the "holes" in your enterprise's security armor before they're used for nefarious purposes.

Contact us to learn more about FortiGuard Penetration Tests or to schedule your assessment.

[1] Douglas Jose Pereira dos Santos, "Key Findings from the 1H 2023 FortiGuard Labs Threat Report," Fortinet, August 7, 2023.

[2] "Global Threat Landscape Report: A Semiannual Report by FortiGuard Labs," Fortinet, February 21, 2023.

FORTINET

www.fortinet.com

October 3, 2023 4:12 PM

2345421-0-0-EN