Trellix

DATA SHEET

External Security Assessment

Protect your critical data, customer information and financial transactions from sophisticated cyber threats with our comprehensive and tailored security measures

Benefits

- Gives you the best of both worlds by performing a penetration test as a subcomponent of the external security assessment
- Enables you to see if your networks and web applications can be penetrated from the outside
- Give you a comprehensive list of all security vulnerabilities on your perimeter network
- Allows your organization to schedule, contract, and execute third-party network assessments more quickly and cost-effectively while still gaining the benefit that comes from using the same commercial scanning tool

At Trellix Guardians, our seasoned consultants bring a wealth of experience and proven methodology to every internet security assessment. By focusing on safeguarding your critical assets from sophisticated cyber threats with our tailored measures, we ensure the highest levels of assurance and business value for our clients.

Our process begins with fortifying internet-connected devices on your network. Guardians consultants meticulously identify and test potential attack points, including live hosts, open ports, and available services. These vulnerabilities are often found in routers, firewalls, DNS servers, web servers, database servers, and even legacy hosts that serve no internet- related business purpose. We concentrate on areas where a compromise would pose the greatest risk to your business while adhering to the policies and regulations that drive the need for security, particularly in
e-commerce and financial services. Our non-disruptive analysis has minimal or no impact on staff and business productivity.

Methodology

A typical external security assessment consists of the following phases:

- Footprinting
- Vulnerability scanning
- Manual vulnerability verification
- Penetration testy
- Vulnerability testing
- Vulnerability analysis
- Provides an executive summary that details trends, architectural, and systemic issues
- Provides a rapid and efficient inventory of the devices, services , and vulnerabilities of internet-connected networks

Footprint Analysis, a key process in network security, and Information Gathering

This phase results in a meticulously detailed blueprint of your company's network and its internet security profile—the two major components to measuring the network's overall risk. This thoroughness ensures a comprehensive security assessment.

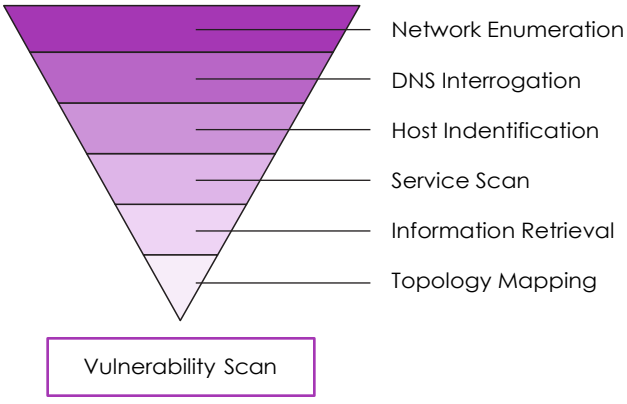
Our consultants' approach footprinting without significant prior knowledge about your company's network. This allows us to achieve thorough mapping and overcome any blind spots you might have.

We gather domain-based names, IP network ranges, and information about hosts, such as operating systems and applications.

Penetration Testing

Our penetration testing offers a thorough examination of internet defenses to help strengthen you network security. Our consultants meticulously analyze internet systems to uncover any weaknesses or vulnerabilities that could be exploited by attackers, with the goal of enhancing the confidentiality, availability, and integrity of internet-connected systems.

Internet Pen Test Methodology



Divided into two essential phases, our penetration testing methodology aims to provide a detailed understanding of your company's network and to recommend effective strategies for protecting your most important assets.

For organizations in need of comprehensive penetration testing, we provide a variety of options, including social engineering, denial-of-service testing, IDS/incident response validation exercises, and more to help fortify your networks against potential threats.

Vulnerability Scanning

The vulnerability scanning phase is a logical continuation of the footprint analysis and information-gathering phase. The information gathered during these initial steps is used to identify vulnerabilities in the system. We then take a systematic approach, chaining multiple, low-risk vulnerabilities to achieve a high level of access to the target network.

Therefore, it is crucial to understand that this vulnerability linking, if not mitigated, can result in the pilfering of sensitive data, such as password

hashes, restricted databases, or the acquisition of specific trophies that your company identifies. This underscores the importance of your role in risk mitigation. This vulnerability linking typically culminates in pilfering sensitive data, such as password hashes, restricted databases, or attaining specific trophies that your company identifies.

Discounted Retesting

Our Guardians consultant's partner with your organization in attaining its strategic security goals. At the conclusion of this engagement, we list all discovered vulnerabilities upon a ranking of high, medium, and low. At a discounted rate, we perform a retest of each of the
discovered vulnerabilities within three months of the completion of your engagement. This allows you to validated that your security remediation efforts resolved all discovered vulnerabilities.

For more information or to schedule a consultation, please contact us at Guardians@Trellix.com