External Security Assessment

Don’t Make it Easy

When attempting to breach networks, attackers will work to identify vulnerabilities, starting with minimally intrusive techniques, in order to prevent detection. Freely available tool kits can assist the attacker in automating this research as well as allowing the attacker to exploit vulnerabilities.

There is a lot of publicly available information about your organization – configuration details about your domain and email, information about users within your organization, and servers that are exposed to the outside world. For someone trying to get access to your data, this information can provide a playbook to attacking your organization. Just as important, properly configuring and securing these externally-facing components shows that you are security-conscious and will cause attackers to try elsewhere. Don't be the low-hanging fruit.

What We’ve Noticed

In an External Security Assessment (ESA), our team collects and reports public information easily obtained by attackers and ensures your external systems follow configuration best practices. We use a layered approach that combines an external network assessment, email configuration checks, domain configuration checks, and open source information gathering. Each of these works together to give you a full picture of your external vulnerabilities too keep you off the radar of attackers. To get started, you don’t need to install any software or equipment – we can check everything remotely and provide a report on the findings.

After testing, we provide easy-to-implement recommendations that your managed service provider or IT staff can handle with your existing environment.

An External Security Assessment Includes:

- ✓ **Email Configuration Checks**
- ✓ **Domain Configuration Checks**
- ✓ **External Network Testing**
- ✓ **Open Source Information Gathering**

Frequently Asked Questions

What's the difference between an External Security Assessment and an External Penetration Test?

An external security assessment collects and reports on your organization's publicly available information to give you an understanding of what an attacker could use in a cyberattack. An external penetration test involves manual exploitation of vulnerabilities found on your external network.

What types of information are you looking for during this assessment?

From an information gathering standpoint, we are looking for publicly available company information - things like employee names, phone numbers, and email addresses. We also perform configuration check of your email set-up including the use of DomainKeys and SPF records. In addition to those, our ISAs will perform vulnerability scanning of your organization’s externally facing IP addresses in order to identify any weaknesses and if there are any, we will provide detailed recommendations to mitigate these issues.

What do you need from me to perform this assessment?

We need your external IP address(es) and domain names to complete the assessment.

How often should we perform this test?

We recommend that you perform this once per year, or if there is any significant change to your externally facing IT environment.

Could there be any denial of service during testing?

No, we have never experienced any denial of service when performing this assessment.

tracesecurity

Practical, worry-free cybersecurity.