Black Box Penetration Testing

DATASHEET

tracesecurity
Compliance, simplified.

877-275-3009 tracesecurity.com sales@tracesecurity

Don't Be An Easy Target

Your external network includes servers and devices visible to the public. Since anyone can see them, they can provide an easy access point for attackers to breach your systems. If you have even one small vulnerability in your external network, an attacker could exploit that weakness to gain more and more access and potentially compromise your sensitive company information right under your nose.

A Black Box Penetration Test, also known as a "shields up" test, demonstrates how vulnerabilities found on your network devices can provide pathways for an attacker to gain unauthorized access to devices and any private data stored on them.

Know Where You Stand

Our Black Box Penetration Test involves our analyst using various tools and techniques to discover your external IP addresses. They will run a network mapping scan and vulnerability scan against your networks to identify any weaknesses, and then manually attempt to discover any additional vulnerabilities not picked up during scanning. Once one or more vulnerabilities are identified, our analyst will use manual attack methods to exploit them and find how deep a real-world attacker could get.

To demonstrate how exploitable your vulnerabilities are, our analyst will reveal the methods by which they were able to compromise credentials of target systems, gain and maintain access to those systems, and launch pivot attacks to other network devices. We will also provide you with immediate notification of any vulnerabilities that require your immediate attention, along with recommendations on how to address them, before the final report deilvery.

Black Box Penetration Testing Features:

- **Determines weaknesses of external security measures**
- **Manual testing of external networks for vulnerabilities**
- **Utilities tools and techniques used by real-world attackers**
- **Comprehensive report with actionable recommendations for remediation**

Frequently Asked Questions

What is the difference between vulnerability scanning and penetration testing?
Vulnerability Scanning is an automated method that identifies vulnerabilities that may exist on an organization's network. Penetration Testing is by nature more accurate than vulnerability scanning since it actually confirms that a suspected weakness is exploitable.

What is the difference between a Black Box Penetration Test and an External Penetration Test?
The difference between these two types of penetration testing is the discovery of your external network(s). In an EPT, you would give your external IP addresses to our analyst for testing. In a Black Box Penetration Test, our analyst will use tools to discover your external network(s) like an attacker would, giving a better simulation of a real-world attack. If there are any external networks not discovered by our analyst, you have the option to provide any additional external IP addresses to them.

What is the difference between vulnerability scanning and penetration testing?
Vulnerability Scanning is an automated method that identifies vulnerabilities that may exist on an organization's network. Penetration Testing is by nature more accurate than vulnerability scanning since it actually confirms that a suspected weakness is exploitable.

Will this hurt my network?
This is extremely unlikely. We very rarely have any reported problems. We do not attempt any denial of service attacks.

What information does my core provider or IT MSP need to provide during the scoping call?
IP addresses of external interfaces, best times for the automated scans, white-listing process for our IPs, contact information, and domain lockout policy so that we can mitigate the risk of locking out domain users during testing up front.

Are the vulnerability scan results included in the report?
No. If scan results were included, it would be a very long report and there is really no reason to include them. We will often take a screenshot to show the client that scans were run and sometimes the specific vulnerability that we were able to exploit.

What is the Information Security Analyst looking for?
We are looking for system and service level vulnerabilities which can potentially be exploited on systems that can be accessed from the public internet. These vulnerabilities could include out-of-date software versions, insecure system configurations, or other technical flaws. The goal is to identify these exploitable vulnerabilities by attempting to compromise these systems using real-world techniques and provide subsequent recommendations on how to mitigate the confirmed attack methods.

What if x hour(s) of testing isn't enough? Do you stopat x hour(s) if you are still finding things?
We do our best to work with you upfront to identify how long tesing will take. If after the ISA runs their initial port and networking scans and finds a lot more open ports than expected, or is in the middle of testing and realizes they will need significantly more time, they will contact you.