XERVANT

verifying **TRUST**

CYBER SECURITY

when asked by the FBI why they did it, the number one answer given by hackers was

"BECAUSE I COULD"

Often times people think that they are safe from cyber attack because they rationalize that no one would have an interest in their information. Unfortunately, there are numerous reasons why an organization may become the target of an attack including something as simple as an open door.

So how do you know if you have an open door? That's where we can help. We have identified three primary entry points that external attackers typically use to gain unauthorized access to your systems: *Web Applications*, *Networks*, and *People*. Each of these entry points offer a would-be attacker potential access to your confidential data, so it is important to know that you can trust them to be secure. So how do you know if you can trust them? That's easy, trust, but verify. We offer the services to help validate the real-world security of all three of these areas so that you can trust with confidence.

Web Applications

Many modern web sites include functionality that utilizes data from back end systems and databases. Although beneficial to the end users, these types of sophisticated applications have the potential to provide would-be attackers with direct access to your confidential data.

Networks

A firewall is a great defensive tool for your network, but what if it isn't configured properly? What if your servers and switches have not been properly patched? What if you are using unsecured TCP ports? These are just a few of many ways that a network could become an unauthorized entry point for a would-be attacker.

People

Rarely do you hear someone mention people when they talk about information security, but people represent one of the largest potential risks to most organizations. An attack on one or more of your employees who lacks security consciousness can expose your most valued assets to your attackers, or even worse, your competitors.

Web Application Penetration Test

A web application penetration test is a great way to assess the real-world security of your web-based resources. By evaluating the security of a deployed web site, we are able to simultaneously verify the security posture of the critical elements such as the integration between components, deployment configuration, and unsafe coding practices related to authentication, authorization, session management, data storage, information exposure, and other coding related issues. This type of comprehensive security assessment is essential for any company that has already deployed or plans to deploy a modern web site.

Our Approach

We analyze your web application/web site from the vantage point of the external attacker using a combination of automated testing tools and personal inspection by a certified information security expert. We not only look at the common entry points that hackers typically use to gain unauthorized access, but we also systematically evaluate your site for other potential entry points providing a comprehensive security assessment strategy. Once we have completed our assessment, we provide a detailed report outlining any discovered vulnerabilities and the recommended remediation steps that need to be taken in order to properly secure your site.

What does it include?

Our web application penetration testing service is a comprehensive, real-world security assessment which includes:

- Assessment by a certified information security expert.
- Scanning for an array of vulnerabilities and common attack surfaces such as:
  - Improper/Unsafe Data Handling (Cookies, Query Strings, Hidden Fields)
  - SQL Injection/Script Injection
  - Cross Site Scripting (XSS)
  - Information Disclosure
  - Security Misconfiguration
- Scanning for platform-specific vulnerabilities.
- Assessment of authentication/authorization techniques.
- A detailed assessment report outlining any discovered vulnerabilities and the recommended remediation steps.

External Network Penetration Test

Our external network penetration test is designed to evaluate the effectiveness of security at the outer edge of your network. This type of assessment typically answers questions related to which services you expose beyond your firewall and if those services are properly secured. In addition, a network penetration test is also a great way to identify unauthorized rouge services such as a personal gaming server, personal web site, or other unauthorized services that are utilizing network based resources at your expense. Performing this type of security assessment on an ongoing basis is a great way to proactively maintain the first line of defense in your information security efforts.

Our Approach

We analyze your network from the vantage point of the external attacker using a combination of automated testing tools and personal inspection by a certified information security expert. The primary assessment involves identifying all of the open TCP ports, checking them for known vulnerabilities, and validating the appropriateness of the services being exposed. Once we have completed our assessment, we provide a detailed report outlining any discovered vulnerabilities and the recommended remediation steps that need to be taken in order to properly secure your network and firewall.

What does it include?

Our external network penetration testing service is a comprehensive, real-world security assessment which includes:

- Assessment by a certified information security expert.
- Identification of all open TCP ports.
- Scanning of all 65,535 available ports on each identified public IP address.
- Scanning for firewall-specific vulnerabilities.
- Scanning for open service-specific vulnerabilities.
- Validation of appropriateness for questionable open ports.
- Recommendations for alternative configurations to minimize security issues while still providing the required authorized services.
- A detailed assessment report outlining any discovered vulnerabilities and the recommended remediation steps.

Social Engineering Assessment

A social engineering assessment is all about evaluating the security of your people by attempting to lure them into taking some unsafe action or divulging sensitive information. Admittedly, this type of assessment is entrenched in deception, but unfortunately, that is one of the favorite tools used by some of the world's most notorious hackers. Think about it this way: is it easier to break into a network and bypass the intrusion detection system or simply convince an employee to reveal a password or other sensitive information? People are often the weakest link in any security strategy and a social engineering assessment is a great way to verify the security consciousness of your team.

Our Approach

We analyze the security awareness of the targeted employee(s) from the vantage point of the external attacker by compiling readily available data into an assessment profile. This profile may include information from social media outlets, search engines, and other sources and is used to develop attack scenarios that are likely to be successful. We then execute a multi-layered attack on the target through some type of direct communication (email, social media, telephone, etc). Once we have completed our assessment, we provide a detailed report outlining any successful attack scenarios and the recommended remediation steps required to enhance the effective security of your people.

What does it include?

Our social engineering assessment service is a comprehensive, real-world security assessment which includes:

- Assessment by a certified information security expert.
- Customer defined employee targeting method (you can define the specific employees to be targeted or allow us to define the targets blindly).
- Target profile data collection from search engines, social media, and other readily available sources.
- Password analysis based on the collected profile data.
- Highly targeted attack scenarios which are specifically designed to simulate real-world attacks.
- A detailed assessment report outlining any successful attack scenarios and the recommended remediation steps.
- Complete confidentiality and professionalism.

XERVANT

Xervant Cyber Security
29520 Community Road
Albemarle, NC 28001
(704) 984-4986
info@xervant.com
www.xervant.com

CYBER SECURITY