Connection
we solve IT

PENETRATION TESTING SERVICES

Find Flaws in Your Security Before They Do

Why Consider a Penetration Test?

In today's security landscape, IT organizations across all industries must navigate a complex set of regulatory, compliance, and business demands. With ever-present and evolving security threats, business and technology evolution, and tightening regulations, security compliance can be difficult to achieve and maintain.

In order to identify whether your organization is prepared against external threats, you must periodically perform technical security testing to probe your defenses and identify weaknesses. Connection offers Penetration Testing to help you identify flaws in your infrastructure, as well as the recommendations to reduce your organization's risk.

Why Test?

In order to determine your company's resiliency to attacks, you must periodically perform the same types of attacks that cyber-criminals perform daily. This "ethical hacking" will determine if your defenses are susceptible to exploitation. Connection's Penetration Testing Services are focused on a true hacker–based approach. This means minimal information is provided to Connection. Typically, only the target IP addresses are given with no supporting information and you are not required to make any adjustments to your security infrastructure to accommodate the testing.

What Value Does a Penetration Test Provide?

Our Penetration Testing Services can provide you with a better understanding of your organization's current risks to attack and compromise. Connection will utilize a comprehensive and methodical approach to security testing. Our Security Practice experts use industry-leading tools and techniques to uncover vulnerabilities in your environment that could expose security weaknesses that an attacker would leverage to compromise your systems, data, and services. We document and prioritize the risks we uncover, as well as provide recommendations to remedy and better manage your risk.

Methods and Practices:

Pre-Engagement Planning

Our experts engage with you to determine success criteria, the type of testing to be conducted, and to identify any areas of focus. The following pre-engagement activities will be conducted:

- Determine size of the environment
- Document the scope of the engagement
- Introduce points of contact
- Confirm timeline for testing
- Identify and document restrictions for testing (e.g., date and time restrictions and defining stopping points)
- Ensure authorization to conduct testing is verified (e.g. ownership of IP's)
- Finalize SOW

Intelligence Gathering

Once work commences, the project team is assigned and Connection performs reconnaissance to gain as much information as possible. This information will be utilized in later stages of the engagement. During this phase, the following activities will be conducted:

- Open source intelligence gathering
    - Utilizing online public resources to gain information
- Network and service enumeration
    - Using tools such as network vulnerability scanners to identify live hosts, enumerate open ports, and identify network services and versions. The scanners employed include but are not limited to:
        - Rapid7's NeXpose
        - Tenable's Nessus
        - Beyond Trust's Retina

Threat Modeling

The information gathered during the intelligence phase will be used to develop a plan of attack against the targets. During this stage, the following activities will be conducted:

- Information is documented and classified (e.g., assets are identified as primary or secondary targets)
- Vulnerabilities are identified and documented
- Services and service versions are researched for known exploits

Exploitation

This phase of the engagement uses Threat Modeling to focus on gaining access to the target systems, bypassing any security restrictions that have been put in place. This stage includes the following activities:

- Exploits for vulnerabilities are identified and documented
  - Exploits can be identified by the following techniques:
    - Pre-built (e.g., Metasploit or Core Impact modules)
    - Manually built or scripted
- Identified exploits are executed against the target systems

Post-Exploitation and Reporting

The final stages of the engagement include the post-exploitation and reporting activities. During this stage the following activities will be conducted:

- False positives for vulnerabilities are identified and eliminated
- Successful exploits are identified and classified by criticality
- A comprehensive report is developed, detailing all activities and suggestions for remediation

How Is a Penetration Test Scoped?

The scope is determined by collecting data on approximate locations and devices. In some cases, a follow-up call may be required for additional clarification. Once the scope is completed, a SOW will be provided for signature. The document contains the work tasks, deliverables, and terms and conditions necessary for this security testing.

Penetration Test Timeline

This assessment typically takes three to six weeks from the start of testing to the completion and delivery of the final report. Times may vary depending on your environment's size and availability.

How Do I Engage the Connection Security Practice?

Reach out to your Account Team. They will work with the Security Practice Service Managers to scope and finalize the project. Scoping sometimes requires a site-standard sizing sheet that you will need to complete and return. In some instances, a short call may be required to clarify testing parameters. Once the effort is scoped, a Service Manager will provide a SOW for you to review and sign. Once the testing and report are complete, the Security Practice Service Managers will work with your Account Team to coordinate a meeting to review the report and discuss best-in-class remediation for any identified issues.

For more information about the comprehensive services Connection offers, contact your Account Team today.

Connection®
we solve IT®

1.800.998.0067
www.connection.com/Services