Connection
we solve IT

External Threat Assessment Services

Are You Susceptible to Exploitation from the Outside?

What Is an External Threat Assessment?

In order to determine if your organization is prepared for external cyber attacks, you must periodically perform a series of technical security assessments to probe your defenses and identify weaknesses. Connection's security experts offer the testing services you need to identify vulnerabilities and reduce your organization's risk. Our security services include external penetration testing (ethical hacking), wireless security penetration testing, and social engineering assessments that cover topics ranging from physical access reviews and phishing to phone and deskside-based social engineering.

We Offer Two Types of Ethical Hacking

In order to determine your company's resiliency to external Internet-based attacks, you must conduct the same types of attacks that cyber criminals perform on a daily basis. This testing will determine if you are susceptible to exploitation by these criminals.

- **Black Hat Testing:** Minimal information is provided to Connection. Typically only the target IP addresses are given with no supporting information. Customers are not required to make any adjustments to their security infrastructure to accommodate the testing *(True hacker approach)*.
- **Gray Hat Testing:** Customers provide Connection with detailed information about targets. For example, the customer may provide a target, function, operating system, and other useful information. The customer also allows scanning through their perimeter security infrastructure.

Wireless Penetration Testing

A Wireless Security Assessment determines if your wireless infrastructure is configured appropriately to meet your critical business needs while enforcing your security policies and controls. Connection's security experts will attempt unauthorized access to your network using advanced wireless security testing tools. This will provide a complete risk profile for your wireless networking infrastructure, identifying potential issues related to appropriate coverage (users who cannot connect are experiencing Denial of Service), secure access and authentication controls, proper segmentation between guest and corporate networks, and proper controls for secure application and data access.

Phishing and Social Engineering Testing

Every user in your organization has a responsibility to help protect sensitive and proprietary information. Our Phishing and Social Engineering Testing is a collection of techniques used to assess your employees' susceptibility to social engineering tactics that might influence them to perform certain actions or divulge confidential information.

Our services can:

- Find out what percentage of your staff clicks on HTML links in email messages
- Test employees to determine if they enter information on a fake website

- Perform safe malware phishing experiments to determine the effectiveness of your filters
- Find out whether physical security policies and controls are being enforced
- Test employees to determine their effectiveness and awareness of social engineering attacks, either over the phone or through desk-side visits.

Our assessment emulates the approach used by hackers. We attempt unauthorized access to your network, manually conduct a controlled, real-life attack on your users, and measure their response and actions.

How Can Your Organization Benefit from an External Threat Assessment?

Through a comprehensive, methodical approach to threat testing, our Security Practice experts will uncover vulnerabilities in your environment, expose security weaknesses, and provide recommendations to remedy and better manage your risk.

Our Methods and Practices:

Pre-engagement Planning

Our experts engage with your team 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 contacts for your organization and Connection
- Confirm timeline for testing
- Restrictions for testing are identified and documented (e.g., date and time restrictions and defining stopping points)
- Ensure authorization to conduct testing is verified (e.g., customer owns all IPs)
- Finalize Statement of Work

Intelligence Gathering

Once work commences, the project team is assigned and Connection performs reconnaissance on the customer 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 about the customer
- 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 we use include, but are not limited to:
    - Rapid7 NeXpose
    - Tenable Nessus
    - BeyondTrust Retina

If a Black Hat Test is being conducted, your organization's security appliances can enforce restrictions on the scanning engines that will delay the completion of this phase (e.g., block our scanning IP for 20 minutes).

Threat Modeling

The information gathered during the intelligence phase will be used to develop a plan of attack against the targets. During this stage of the engagement, 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 the Threat Modeling to focus on gaining access to the target systems by bypassing any security restrictions that are put in place by the customer. During this stage of the engagement, the following activities will be conducted:

- 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 these stages of the engagement, 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 providing suggestions for remediation

How Is an External Threat Assessment Scoped?

The scope is determined by collecting data from your organizations on approximate locations and devices. In some cases, a 30-minute scoping call may be required, or a follow-up call scheduled if additional clarification is required.

External Threat Assessment Timeline

The assessment typically runs over a 4–6 week period, from the start of external testing.

Create an Effective Data Protection Plan

In today's security landscape, IT organizations across all industries must navigate a complex set of regulatory, compliance, and business demands. With ever-present security risks, business and technology evolution, and tightening regulations, security compliance can be difficult to achieve and maintain. Our External Threat Assessment can provide you with a better understanding of your organization's current risks and help identify opportunities to protect your sensitive systems data from compromise over the Internet, over your wireless network infrastructure, or through your employees' responses to phishing attempts or sharing of sensitive information from social engineering.

Call an Account Manager to schedule an External Threat Assessment today.

Business Solutions	Enterprise Solutions	Public Sector Solutions
1.800.800.0014	1.800.369.1047	1.800.800.0019

www.connection.com/SecurityPractice

Connection™
we solve IT™