EC-Council Licensed Penetration Tester

Methodology: Rules of Engagement

Penetration Tester:			
Organization:			
Date:		**Location:**	

Penetration Testing Rules of Engagement

Overview:

Security Assessment needs vary from agency to agency. The XSECURITY Penetration Testing Team (XSECURITY) offers several services that can assist COMPANY X in securing their information technology assets. Each of these services requires some degree of support from the COMPANY X (system information, access to agency personnel or facilities, system/network connections, etc.). Penetration testing tools and techniques can be invasive, however, so there needs to be a clear level of understanding of what an assessment entails, what support is required for assessments, and what potential effect each type of assessment may have.

Use of Tools

The Penetration testing activities performed by the XSECURITY Penetration Testing Team include scanning network assets with specific penetration testing tools. These tools check system configurations, default settings, security settings/updates, network and workstation services, open ports, and other specific vulnerabilities that might be utilized by intruders or unauthorized staff to undermine or bypass the security of an agency's network. They do not access user files, data files, or other personal/confidential files, only network/workstation files associated with system configurations and security. The XSECURITY does perform 'penetration testing' – that is, test how deep into your network an intruder can go, retrieve confidential information, or change system configurations. Our scans determine what vulnerabilities exist within the agency network with fully exploiting those vulnerabilities. The purpose of a network penetration testing is to enable system administrators to better protect systems and ensure the quality of service.

Required Support from Company X

COMPANY X selects the penetration testing service, or combination of services, that best meet their needs. While there is some analytical and methodological overlap in some penetration testing services, there is significant difference between others. COMPANY X support will therefore vary depending on the combination of services selected. In all cases, however, we will need a signed document giving us authorization to perform the selected penetration testing.

Internal penetration testing: Since this is performed onsite, the client needs to provide network connections (IP address, subnet mask, default gateway, preferred DNS server) and

accounts for the scanning machines. Specific network information, such as IP range, types of devices, and network services is also required.

External penetration testing: The client must provide specific network information including IP ranges, devices types and services.

Modem Sweep: The client must provide a list of phone/fax/modem numbers to test.

Password Assessment: Copies of the appropriate password files will be required in order to assess password strength.

Physical Assessment: The client must provide information regarding physical assets to protect, current agency security policies and procedures, and arrange access to the facility for the team.

Corporate Security Culture Assessment: The XSECURITY Penetration Testing Team will need the client's location and permission to enter the premises unannounced. This assessment is best done without prior knowledge by the client's staff.

Potential Impact or Effect

With regards to Internal and External penetration testing all the tools used by the XSECURITY are obtained from trusted resources. These tools are designed to discover vulnerabilities and not to undermine the system they are assessing. The only disruption to a network might be a temporary denial of service through port scanning, but this is very unlikely. (In fact, we have never caused a denial of service on any machine without giving ample warning.)

A Password Assessment requires only a few minutes of the network administrator's time and does not involve the network itself. Furthermore, we only use a copy of the files to reduce the impact on system resources and lessen the possibility of harming the system. These assessment tools used are from trusted resources, as well.

A Modem Sweep is generally performed at night or on the weekend when the staff is out of the office. To be most effective, however, the sweep should be done during normal office hours, since unauthorized modems will not be found when a host machine is turned off (at night or on weekends). The impact from a Modem Sweep is only a temporary inconvenience for staff members who answer their phone. Even so, the dialer program imitates fax tones to disguise the phone sweep.

A Physical Assessment will at worst be a minor disruption for a client's staff, similar to having non-employees visiting the office.

The Corporate Security Culture Assessment entails observing the security awareness of agency personnel. This necessitates having XSECURITY members enter the client's location in an inconspicuous way. Little disruption of normal work can be expected.

XSECURITY Consideration Checklist		
YES	**NO**	**DESCRIPTION**
		Has the XSECURITY taken reasonable precautions to ensure that its own employees or the staff of any subcontractor will not take advantage of the opportunity afforded them by the testing assignment to later initiate an unsanctioned attack against the client?
		Is the XSECURITY acceptable to the organization's insurance underwriter (if any)?
		Does the XSECURITY agree to be bound by clearly defined (and documented) terms of engagement?
		Does the XSECURITY provide any kind of compensation if they, as a result of their testing activities, significantly disrupt the normal operation of the system being tested?
		Does the XSECURITY provide any kind of compensation (or guarantee) if they fail to detect a security hole that is later successfully exploited by an intruder?
		Does the contract with the XSECURITY specify what types of tests will be conducted? Examples would be ping sweeps, port scans, simulated distributed denial-of-service attacks, file share scans, application source code reviews, submitting system commands via application input data, and so on.
		Does the contract with the XSECURITY specify whether the XSECURITY will include recommendations on how to fix any detected vulnerability?
		Does the XSECURITY also offer a consulting service for implementing any recommendations they might make?
		Is the XSECURITY willing to divulge what testing tools (and versions) they will use to conduct their tests?
		Does the contract specify what head-start information (if any) will be provided to the XSECURITY prior to commencement of the assessment? Examples include a complete list of network addresses used by the target site, specific version numbers of the system software installed on the target site, or a list of services running on the servers located closest to the perimeter firewall.
		Does the contract with the XSECURITY specify the duration of the testing effort and under what circumstances may testing be terminated, suspended, or extended?
		If the testing is to be done remotely, have additional tests been scheduled that will test the security of the Web site from an internal attacker?