Chapter #12: The Pen Test

Outline
- Describe penetration testing, security assessments, and risk management
- Define automatic and manual testing
- List the pen test methodology and deliverables

The Security Assessments
- A security assessment is any test that is performed in order to assess the level of security on a network or system
  - policy and procedure focused
  - it tests whether the organization is following specific standards and policies they have in place

The Pen Test: Putting It All Together
- A vulnerability assessment scans and tests a system or network for existing vulnerabilities but does not intentionally exploit any of them
  - vulnerability assessment is designed to uncover potential security holes in the system and report them to the client for their action
  - it does not fix or patch vulnerabilities, nor does it exploit them — it simply points them out for the client’s benefit
A penetration test, on the other hand, not only looks for vulnerabilities in the system but actively seeks to exploit them. The idea is to show the potential consequences of a hacker breaking in through unpatched vulnerabilities. They are carried out by highly skilled individuals pursuant to an agreement signed before testing begins.

Nothing happens before you have a signed, sealed agreement in place. This agreement should spell out the limitations, constraints, and liabilities between the organization and the penetration test team, and is designed to maximize the effectiveness of the test itself while minimizing operational impact. In many cases, a separate indemnity form releasing you from financial liability is also necessary.

An external assessment analyzes publicly available information and conducts network scanning, enumeration, and testing from the network perimeter, usually from the Internet. An internal assessment is performed from within the organization, from various network access points.

Black-box, white-box, and gray-box testing. Black-box testing occurs when the attacker has no prior knowledge of the infrastructure at all – this testing takes the longest to accomplish and simulates a true outside hacker. White-box testing simulates an internal user who has complete knowledge of the company’s infrastructure. Gray-box testing provides limited information on the infrastructure – sometimes gray-box testing is born out of a black-box test that determines more knowledge is needed.
The red team is the offense-minded group, simulating the bad guys in the world, actively attacking and exploiting everything they can find in your environment. In a traditional war game scenario, the red team is attacking black-box style, given little to no information to start things off.

The blue team, on the other hand, is defensive in nature. They’re not out attacking things – rather, they’re focused on shoring up defenses and making things safe. They usually operate with full knowledge of the internal environment.

Automated Testing Tools

- **Codenomicon**
  - toolkit utilizes a unique “fuzz testing” technique, which learns the tested system automatically

- **Core Impact Pro**
  - tests everything from web applications and individual systems to network devices and wireless

Manual Testing

- **Metasploit**
  - it offers a module called Autopwn that can automate the exploitation phase of a penetration test

- **CANVAS**
  - an automated exploitation system with hundreds of exploits, and a comprehensive, reliable exploit development framework

- Manual testing is still the best choice for a true security assessment
- It requires good planning, design, and scheduling, but it provides the best benefit to the client
**Actions Taken**

- Pre-attack phase
  - reconnaissance and data-gathering efforts
- Attack phase
  - attempting to penetrate the network perimeter, acquire your targets, execute attacks, and elevate privileges
- Post-attack phase
  - lot of cleanup to be done
  - deliverables

**Pre-attack Phase**

- Competitive intelligence, identifying network ranges, checking network filters for open ports
- Running whois, DNS enumeration, finding the network IP address range, and nmap network scanning
- Other tasks include testing proxy servers, checking for default firewall or other network-filtering device installations or configurations, and looking at any remote login allowances/permissions

**Attack Phase**

- Getting past the perimeter, verifying ACLs, crafting packets, use any covert tunnels inside the organization
- Trying XSS, buffer overflows, and SQL injections
- After acquiring specific targets move into password cracking and privilege escalation etc.
- Once you’ve gained access, it’s time to execute your attack code

**Start**

- Typically your test will begin with some form of an in-brief to the management
- an introduction of the team members and an overview of the original agreement
- which tests will be performed, which team members will be performing specific tasks, the timeline for the test etc.
- points of contact, phone numbers, and other information including the “bat phone” number, to be called in the event of an emergency requiring all testing to stop
- thorough review of all expectations for both sides – agreement
### Post-attack Phase 1 - Cleanup

- **Cleanup:**
  - anything that has been uploaded (files or folders)
  - any tools, malware, backdoors, or other attack software
  - don’t forget the Registry—any changes made there need to be reset to the original settings
  - return everything to the pre-test state. Remember, not only are you not supposed to fix anything you find, but you’re also not supposed to create more vulnerabilities for the client

### Post-attack Phase 2 - Deliverables

- Provide the client with information they need to make their network safer and more secure (template)
  - an executive summary of the organization’s overall security posture (if you are testing under the auspices of FISMA, DIACAP, RMF, HIPAA, or some other standard, this summary will be tailored to the standard)
  - the names of all participants and the dates of all tests
  - a list of findings, usually presented in order of highest risk
  - an analysis of each finding and recommended mitigation steps (if available)
  - log files and other evidence from your toolset – this evidence should include tons of screenshots, because that’s what customers seem to want

### Guides

- [VulnerabilityAssessment.co.uk](http://VulnerabilityAssessment.co.uk) has been promoting a pen test walkthrough methodology
  - [SANS guide](http://SANS guide)

### Methodologies

- Open Source Security Testing Methodology
- Information Systems Security Assessment Framework
- Open Web Application Security Project Testing
- Web Application Security Consortium Threat Classification
- Penetration Testing Execution Standard
Blind: does not require any prior knowledge about the target system. However, the target is informed before the execution of an audit scope. Ethical hacking and war gaming are examples of blind type testing. This kind of testing is also widely accepted because of its ethical vision of informing a target in advance.

Double blind: an auditor neither requires any knowledge about the target system, nor is the target informed before the test execution. Black box auditing and penetration testing are examples of double blind testing. Most of the security assessments today are carried out using this strategy, thus putting a real challenge for the auditors to select the best of breed tools and techniques in order to achieve their required goal.

Gray box: an auditor holds limited knowledge about the target system and the target is also informed before the test is executed. Vulnerability assessment is one of the basic examples of gray box testing.

Double gray box: similar to gray box testing, except that the time frame for an audit is defined and there are no channels and vectors being tested. White box audit is an example of double gray box testing.

Tandem: the auditor holds minimum knowledge to assess the target system and the target is also notified in advance, before the test is executed (Examples: crystal box and in-house audit).

Reversal: an auditor holds full knowledge of the target system and the target will never be informed of how and when the test will be conducted.
Information Systems Security Assessment Framework (ISSAF)
- It bridges the gap between the technical and managerial view of security testing by implementing the necessary controls to handle both areas.
- It enables the management to understand the existing risks that float over an organization's perimeter defenses and reduces them proactively by identifying the vulnerabilities that may affect the business integrity.

Open Web Application Security Project Testing (OWASP)
- Testing web applications against OWASP top ten security risks ensures that the most common attacks and weaknesses are avoided and the confidentiality, integrity, and availability of an application is maintained.
- The OWASP community has developed a number of security tools that focus on the automated and manual web application tests: WebScarab, Wapiti, JBroFuzz, and SQLiX, which are also available under the Kali Linux operating system.

Open Web Application Security Project Testing
- OWASP Testing Guide provides you with technology-specific assessment details; e.g., Oracle vs. MySQL.
- Encourages secure coding practices by integrating security tests at each stage of development ensuring that the production application is robust, error-free, and secure.
- It provides industry-wide acceptance and visibility - the top ten security risks can also be aligned with other web application security assessment standards helping to achieve more than one standard at a time with a little more effort.

Web Application Security Consortium Threat Classification
- Provides technology-specific threat classification for each type of application (e.g., JavaScript, Web, Java, etc.).
- Aligns OWASP and other web application security assessment standards with established industry-wide metrics.
Penetration Testing Execution Standard

- Penetration Testing Execution Standard

Insider Threats

- Pure insider
  - an employee with all the rights and access associated with being employed by the company
  - already have access to the facility (card or badge) and a logon to get access to the network
  - their privileges are often assigned at a higher level than are actually required to get their work done

- Insider associate
  - someone with limited authorized access, such as a contractor, guard, or cleaning services person
  - they aren't employees of the company, and they do not need or have full access, but they have physical access to the facility
  - they're not allowed network access
  - physical records are sometimes accessible, plethora of dumpster-diving material, but physical access to a system usually guarantees a hacker, given enough time, can access what she needs

- Insider affiliate
  - a spouse, friend, or client of an employee who uses the employee's credentials to gain access
  - the key is the credentials used to do it – for all intents and purposes
  - to the network, physical access restriction areas, and any computer she grabs hold of the intruder is a trusted insider
Insider Threats

- Outside affiliate
  - someone who is outside the organization, unknown and untrusted, who uses an open access channel to gain access to an organization’s resources
  - if it’s an employee or someone who knows the employee, it’s an insider — if it’s not, it’s an outsider

There is no 100 percent secure system, and there is nothing that is foolproof!

Stay Alert!