Penetration Testing 101

@Bugg - never done a pen-test

What is a Pen-Test?

Attempting to gain access to resources **without** knowledge of user-names, passwords and other **normal means of access.**

-SANS

Pen-Test vs Hacking

The main thing that separates a penetration tester from an attacker is **permission**.

The penetration tester will have permission from the owner of the computing resources that are being tested….

–SANS

What is the goal?

To **increase** the **security** of the computing resources being tested.

–SANS

Internal vs External

External tests target the assets of a company that are **visible on the Internet….**

Internal testing gives a tester access to an application behind its firewall and simulates an **attack by a malicious insider**.

Pentesting Steps

1) Scoping/Planning
2) Recon
3) Scanning
4) Exploit Vulns
5) Analysis/**Report**
6) Debrief Client

1 – Scoping/Planning

- **What they want** vs how much time that would take
- The systems to be addressed and the **testing methods** to be used.

2 – Recon

- **Gathering intelligence** to better understand how a target works and its potential vulnerabilities.
- Network, domain names, mail server, hosts, employees, email scheme, etc...

3 – Scanning

- **Port-Scanning**
  - Nmap
- **Vuln-Scanning**
  - Nessus
- **Wireless Scanning**
  - Wireshark/Aircrack

4 – Exploit Vulns

- Cross-site scripting, SQL injection, backdoors, escalating privileges, stealing data, intercepting traffic, etc., **to understand the damage you can cause.**

5 – Analysis & Report

- **Specific vulnerabilities** that were exploited
- **Sensitive data** that was accessed
- The amount of **time** the pen tester was able to remain in the system **undetected**
- **How to** configure a client’s security solutions to **patch vulnerabilities** and protect against future attacks

6 – Debreif Client

- **Go over entire report with client**
- Make sure client has all their questions answered

Questions?

Sources:

- https://www.sans.org/reading-room/whitepapers/analyst/penetration-testing-assessing-security-attackers-34635
- http://www.timothydeblock.com/eis/72
- https://www.irongeek.com/
- https://www.coresecurity.com/content/penetration-testing
- https://www.veracode.com/security/penetration-testing
- https://www.pcisecuritystandards.org/documents/Penetration_Testing_Guidance_March_2015.pdf