

# Penetration Testing

# Penetration Testing Execution Standard (PTES)

- “Penetration Testing is a way to simulate the methods that an attacker might use to circumvent security controls and gain access to a system.”<sup>1</sup>

PTES, baseline fundamentals for performing a penetration test –

<http://www.pentest-standard.org/>

• <sup>1</sup>Kennedy, David, et. al. *Metasploit: The Penetration Tester's Guide*. San Francisco: No Starch Press, 2011. Print.



# PTES Phases

1. Pre-Engagement
2. Intelligence Gathering
3. Threat Modeling
4. Vulnerability Analysis
5. Exploitation
6. Post Exploitation
7. Reporting

# Pre-Engagement

- Discussing the scope and terms of the penetration test with your client
  - Convey the goals of the penetration test
  - -use this opportunity to discuss what will happen, the expectations of a full scale penetration test
  - - what will be tested – the need for total access to get a complete report

# Intelligence Gathering

- - Gather information about the organization (social media, Google hacking, etc)
- - Start to probe the organization for ports with blocking (use a disposable IP address,
  - you will be blocked if this is turned on)
- Test any Web Applications

Note: perform scans from an IP address range that cannot be traced back to you or your team. The initial probing can be performed from anywhere (except at your team's office!).

# Threat Modeling

- Using the information acquired in the intelligence gathering.
- Look at the organization as an adversary and determine
  - -where the threats are coming from,
  - -what form they may take
  - -and what they are after.

# Vulnerability Analysis

- You will use all the previous information from prior phases
- This is a detailed analysis taking into account port and vulnerability scans, banner grabbing, and information from intelligence gathering.

# Exploitation

- The “glam” part of the penetration test
- Often brute force (not very “glam”) instead of precision
- Separates the “good” and the “bad” testers –
  - “Bad” testers will fire off massive onslaught of exploits
  - “Good” testers will perform only exploits expected to succeed based on info gathered
- Creating “noise” with massive exploits and hoping for a result is not the way!



# Post Exploitation

- After you have compromised one or more systems (there are many more to come)
- -Targets specific systems
- -Identifies critical infrastructure
- -Targets information or data of value to the company
- Start with systems that will present the most business impact to the company if breached

# Post Exploitation

- Take the time to determine what systems do and their different user roles
- Ex: suppose you compromise a domain? Big deal.
- What else could you do in terms of the systems that the business uses? Backdoor code on a financial application? What about their payroll system? Intellectual property?

# Reporting

- Most important element of the penetration test
- Include at least:
  - Executive Summary
  - Executive Presentation
  - Technical Findings
    - Used by the client to remediate security holes
    - Be sure to warn the client about the thinking that fixing the hole solves the whole problem. Ex: sql injection vulnerability – they fix their problem, but have they addressed any 3<sup>rd</sup> party applications that are connected?

# Types of Penetration Tests

- Overt Penetration Testing

- You work with the organization to identify the potential security threats
  - Advantages: full access without blocks, detection doesn't matter, access to insider knowledge
  - Disadvantages: don't get the opportunity to test incident response

- Covert Penetration Testing

- Performed to test the internal security team's ability to detect and respond to an attack
  - Advantages: Test incident response, most closely simulates a true attack
  - Disadvantages: Costly, time consuming, require more skill
  - Note: because of cost of covert – most will target only one vulnerability, the one with easiest access – gaining access undetected is key

# Vulnerability Scanners

- Automated tools used to identify security flaws
  - 1. Fingerprint a target's operating system
  - 2. Take one OS identified, use scanner to determine if vulnerabilities exist
- Although Vulnerability Scanners play an essential role in Penetration Testing, a penetration test CANNOT be completed automated! Most penetration testers with years of experience rarely use vulnerability scanners – they rely more on their knowledge and experience – business knowledge is also a key factor.

# PTES Methodology

- You can use PTES or another methodology to perform a penetration test.
- More important to have a standard, repeatable process that you follow.
- OCD wins the prize!