Penetration Testing Guidance

Andreas Bohman

CISO at Central Washington University
10,250 students
Eight state-wide campuses
150 Majors & 11 Varsity Teams
2,500 graduates each year
Great Northwest Athletic Conference – NCAA DIV II
Agenda

• Setting the Stage
• What is Penetration Testing?
• Why Penetration Testing?
• Attack Vectors and Scoping
• Approach and Methodology
• Tools of the Trade
• Compliance vs. Business Risk
• Policies and Procedures
• Conclusion
What will this technical track session not teach you?
Images: Vårdförbundet, Viking Electronics, and Engadget.com
What is Penetration Testing?

“Penetration testing is security testing in which assessors mimic real-world attacks to identify methods for circumventing the security features of an application, system, or network.”

- NIST SP 800-115
Why Do Penetration Testing?

“The intent of a penetration test is to simulate a real-world attack situation with a goal of identifying how far an attacker would be able to penetrate into an environment.”

- PCI DSS v3.0
VIDEO
What is Penetration Testing?

Port Scanning

Vulnerability Assessment
Why Penetration Test?

Data Breach

Establish Baseline

Images: Flickr Creative Commons and Wikimedia Commons
Why Penetration Test?

Security Controls  Compliance

Images: Flickr Creative Commons and Wikimedia Commons
Attack Vectors and Scoping
Attack Vectors and Scoping
Approach and Methodology

NIST 800-115

Penetration Testing Execution Standard (PTES)
NIST 800-115

Image: National Institute of Standards and Technology (NIST), SP 800-115
Approach and Methodology

NIST 800-115

Image: National Institute of Standards and Technology (NIST), SP 800-115
Penetration Testing Execution Standard (PTES)

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

Images: Flickr Creative Commons and TrustedSec
Approach and Methodology

Covert vs. Overt

Images: Flickr Creative Commons and Wikimedia Commons
Approach and Methodology

Internal vs. External

Images: Brisk Info Sec
Tools of the Trade
Penetration Testing Execution Standard (PTES)

1. Pre-Engagement Interactions
2. Intelligence Gathering
3. Threat Modeling
4. Vulnerability Analysis
5. Exploitation
6. Post Exploitation
7. Reporting
Payment Card Industry Data Security Standard (PCI DSS)
Requirement 11.3: Implement a methodology for penetration testing

- Includes testing from both inside and outside the network
  - Includes review and consideration of threats and vulnerabilities experienced in the last 12 months

- Includes coverage for the entire CDE perimeter and critical systems
  - Specifies retention of penetration testing results and remediation activities results.

- Defines application-layer penetration tests to include, at a minimum, the vulnerabilities listed in Requirement 6.5
  - Is based on industry-accepted penetration testing approaches (for example, NIST SP800-115)

- Includes testing to validate any segmentation and scope-reduction

- Defines network-layer penetration tests to include components that support network functions as well as operating systems
June 30, 2015
Policies and Procedures

Policy

A policy typically described as a set of procedures to achieve goals. The term is often used in a technical sense to describe a procedure that is formally recognized and enforced.

Whereas a policy describes the protocols that contain the rules.
Hack yourself...

...before the attackers do!