Penetration Testing
What is penetration testing?

- Attempt to bypass security controls.
- Expose weaknesses
- Show how an actual attacker might gain access
- Demonstrate the severity of security issues
Different Styles of Pentesting

Black box
   Tester has no knowledge of system

White box
   Tester has full knowledge of system

This can include:
   Network map, source code, firewalls, etc...
Different Styles of Pentesting

Overt Pentesting - Tester works with the security team and they are warned ahead of time (often White box)

Covert Pentesting - Security team is unaware a test will be taking place. Used to assess responsiveness (often Black box)
Stages of Penetration Test

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

Discuss the goal of the test

Agree on the **scope** for the penetration test

Educate client on what to expect
Intelligence Gathering

Public Information sources
- whois
- NSLookup
- Company/agency website
- Google
Intelligence Gathering

Network mapping
Port scanning
Host enumeration
Operating System Detection

let's talk about nmap...
Intelligence Gathering

DEMO!
Intelligence Gathering

- Attacker
- Windows XP SP2
- Windows 7

Questions: ? ?
Threat Modeling

What are you going to attack?

What are the valuable targets?

How can you evade detection?

What will real attackers do?
Vulnerability Analysis

Port scanning and OS fingerprinting can identify known vulnerabilities

Reverse engineer software to find bugs

Bypass poorly configured security systems

Check web applications for XSS, SQLi, etc.
Exploitation

The fun part!
Exploitation

Demo!
Exploitation

- Attacker
- Windows XP SP2
  - OWNED!
- Windows 7

??
Pre-engagement Interactions
Intelligence Gathering
Threat Modeling
Vulnerability Analysis
Exploitation
Post Exploitation
Reporting
Post Exploitation

Attacker

Win XP

DC

Win 7

Mail

Win 7
Pivoting

- Attacker
- Win XP
- Win 7
- DC
- Mail
- Win 7
Post Exploitation

"Pass-the-Hash" - NTLM protocol used by Windows doesn't require plaintext password

Token Impersonation - Windows Active Directory uses Kerberos single-sign-on to authenticate users

Social Engineering - Trick an employee into helping us
Demo!
Post Exploitation

- Attacker
- Win XP
- Win 7
- DC
- Mail
- Win 7
The least interesting, but **most important** part of the test!
Reporting

Report should include:

- Executive Summary
- Presentation
- Technical findings

The goal is to improve overall security, not just patch bugs!