Intro to Penetration Testing

Patrick Laverty
plaverty@rapid7.com | @plaverty9
provwebappsec.com
Who are you?

- Proud CS166 alumnus
- Former Brown/CIS web developer
- Akamai Infosec CSIRT
- Black Hills Infosec Pentester
- Rapid7 Pentester
Hacking

No... just, no.
The Disclaimer

Never “pentest” a system you don’t own or have explicit, written permission to test from its owner.
The Disclaimer

Never “pentest” a system you don’t own or have explicit, written permission to test from its owner.

Don’t call Josh, Bernardo, or Roberto for bail money. You’re on your own.
The Disclaimer

So how do I learn and practice then?
The Disclaimer

So how do I learn and practice then?

Set up a VM with a vulnerable machine

ie. Wordpress, Joomla or Windows XP, or any of a huge list of intentionally vulnerable apps
The Disclaimer

So how do I learn and practice then?

Set up a VM with a vulnerable machine

ie. Wordpress, Joomla or Windows XP, or any of a huge list of intentionally vulnerable apps

(and no, CIS machines don’t count)
Types of Pentesting

- **Network** - ports, protocols, hardware
- **Web Application** - stick with layer 7
- **Physical** - may include SE, or just access
- **Social Engineering** - in person or remote
- **Internal/External** - may want all tests internally
- **Code Review** - literally that
Types of Pentesting

• Black Box

• Gray Box (“Grey”, if you’re Canadian or British)

• White/Crystal
Steps of Pentesting

1. Kick-off, set scope/boundaries
2. Reconnaissance and mapping
3. Scanning
4. Exploitation
5. Persistence
6. Reporting
Kick-off

- Set expectations
- Set scope
- Set time frame/windows
- Set customer contacts
- Get out of jail free card (if necessary)
HACK!

PWN ALL THE THINGS!
Recon and Mapping

- Don’t skimp
- Spider the site, find the open ports/services
- What if admin/root password is in the wild?
- Army vs. Navy
Recon and Mapping

- Check OSINT
- Google/Bing Hacking
- Social Media Sites
- Paste Sites
- Maps

Tool Tip: Recon-NG, Maltego, Google
Scanning

- Point and shoot
- Manually verify - lots of false positives
- Never just give scan report

Tool tip: nmap, Burp, Zap, sqlmap, metasploit, (any of the commercial scanners)
Exploitation

- Now the fun part!
- Overlap between scanning and exploit
- Keep notes!
Persistence

• We’re in, can we stay in?
• Create accounts
• Change passwords
• Create back doors
• Patch/update

Tool tip: Meterpreter, Mimikatz, php shell
Write the Report

• Keep good notes
• Pics or it didn’t happen!
• Explain twice - executive and technical
• Editor, for technical and writing
• No copy/paste from scan report (or other reports)

Tool tip: Serpico
Debrief

• Don’t get to write and run

• Give report, set time for debrief

• Explain findings, answer questions, make edits

• Final sign-off

• $
Where to Learn More?

- **Blogs** - securityweekly.com, pentest-standard.org
- **Books** - Intro to Pentesting (G. Weidman)
- **Twitter** - So many, just search for “pentest”
- **YouTube** - Some good, some bad, some horrendous
- **Classes** - SANS, SecurityTube, with Conferences
- **Conferences** - Source Boston, BSides Boston, Vegas trifecta
- **OWASP Meetings** (ahem) - May 12 and June 9
- **RFCs** - Read the actual source
Ready?

Patrick Laverty
plaverty@rapid7.com
@plaverty9
provwebappsec.com