Pen Test Summit 2009

Concluding Remarks

Ed Skoudis

~~Stuff We've Gotta Play With~~ In-Depth Lab Analysis

- New Metasploit features
  - Set up a lab, follow HD's tweets (@hdmoore), and try experiments each weekend on new functionality
  - Meterpreter script-a-palooza
  - Experiment with dev version in lab, consider use in real tests
- Gain experience with Jason Ostrum's tools to get prep for increased VoIP work (or just general internal network assessments)
  - UCsniff, ACE, and LiveDVD, etc.
  - Why don't almost all internal assessments include at least some VoIP tests?

~~More Stuff We've Gotta Play With~~ More In-Depth Lab Analysis

- Check out Josh Wright's VistaRFmon and other Vista Wireless Power Tools, bluetooth search, and Chaka Kahn
- Think about methodology for operationalizing click-jacking into web app pen tests
- Recon should now *always* include image retrieval from target website (and more) and exiftool for doc metadata, a la hax0rthematrix
- Grendel-scan 1.1 – gotta download it ASAP
- Can't wait to get my hands on Valsmith's phishing tools

Additional Thoughts

- Metasploit isn't just an exploitation framework…
  - It is a full-blown attack framework and research environment
  - Lots of automation – autopwn, browser autopwn, Meterpreter scripts
- New tools are automating much more of our traditional attack work
  - But, don't fall into the trap of thinking that pen testing is now easy. Point and click, fire and forget, drop an auto-gen'ed report, send invoice… NOT!
  - The truth is… You have to be more NINJA than ever
  - Automation is freeing pen testers to focus on some really clever and creative attacks
  - Our job is to mimic real-world attacks to determine business risks and help prioritize resources
  - It's all about business value… and humans are needed for that
- Manual human interaction is still incredibly important
  - Thanks, David Byrne and Eric Duprey, for your rant!
  - Subtle attacks, combined attacks, web app attacks, business logic flaws…
  - And, Jeremiah's comments are a good challenge for us to keep it real

Exploiting the "Unfixable"

- Number of service-based exploits is diminishing
  - But not dead yet – MS08-067 and more
  - But, transition is clearly underway to client-side, wireless, targeting users (phishing), etc.
- As pen testers, we're increasingly pushing on edge cases, to exploit the "unfixable"
  - Phishing and duping users, inherent wireless flaws, protocol vulnerabilities, Windows design errors, business logic flaws, etc.
  - Sure… there are *some* preventative defenses here, but it's not just a simple patch or reconfig
  - But, what does it really show if our results include only those things that can't be fixed traditionally?
  - Are we really providing business value if we do that?

Answer: Heck Yeah!

- We are still providing value
- Remember, not all defenses are preventative
  - Some are associated with detection, response, and eradication
- "Unfixable" findings can shed light on where better defense-in-depth is needed, as well as improved monitoring
- And… it might also show where the target organization is already pwned
  - Turning a pen test into incident response on the fly
  - We may see a lot more of that kind of transformation in the future

Business Value

- And business value is where we really have to focus
- Actionable, verified, high-quality results
  - Thanks to Ron Dilley and Toby Kohlenberg, for your rants
- Prioritized, report in a consistent and understandable fashion
- In some ways, we have to take back the term "Penetration Test" from those who have sullied its meaning

And, Finally, Thank You!

- Thank you to all of the speakers for their time and insights
- Thank you to the attendees, who fulfilled my promise of asking good questions
- And, don't forget the 2010 Pen Test Summit!
  - Already working on the agenda!
  - Be on the lookout for details