Video: Abusing Windows Remote Management (WinRM) with Metasploit

Entire Webcast Now Available!!

In this technical webinar for penetration testers originally delivered on Dec 4, 2012, David Maloney discussed how you can use Windows Remote Management and Windows Remote Shell to obtain a session on a host while avoiding detection through anti-virus solutions. Participants learned:

• Capabilities of Windows Remote Management (WinRM) and Windows Remote Shell (WinRS)

• Discovering hosts running these services

• Brute forcing the services to obtain passwords

• Running WMI Queries and running commands

• Getting and migrating shells to a more persistent process

David Maloney, a Software Engineer on Rapid7’s Metasploit team, is responsible for development of core features for the commercial Metasploit editions. Before Rapid7, he worked as a Security Engineer and Penetration Tester at Time Warner Cable and as an Application Security Specialist for a global insurance company. David has been a long-time community contributor to the Metasploit Framework. He is one of the founders of Hackerspace Charlotte and is an avid locksport enthusiast.

Discuss in Forums {mos_smf_discuss:Special Events}

In addition to the video of the entire presentation and Q&A embedded below, we've also made the presenter's slide deck available for download here.

Thanks to Rapid7 for sponsoring this webcast. Don't forget to try Rapid7 Products for FREE!!

Download NEXPOSE

Download Metasploit

Rapid7 NeXpose, which received the highest rating of “Strong Positive” in Gartner’s Marketscope for Vulnerability Assessment 2011, leverages one of the largest vulnerabilities databases to identify vulnerabilities that represent the greatest threat to your organization

Metasploit Pro is enterprise-grade software for security professionals who specialize in penetration testing and require an advanced solution for multi-level attacks that enables them to get deeper into networks more efficiently. Rapid7 offers a free, fully featured trial version of Metasploit Pro for you to download.

With more than one million unique downloads in the past year, the free and open source Metasploit Framework is the

world’s most popular exploit development and penetration testing platform.

As the Metasploit Project sponsor, and in cooperation with the open source community, Rapid7 is continuously expanding the exploit library and creating a broader platform with publicly available exploits, helping organizations to stay ahead of the changing threat landscape.

The Metasploit Framework enables:

- Network security professionals to perform penetration tests
- System administrators to verify patch installations
- Software developers to perform regression testing

The Metasploit Framework enables you to:

- Distinguish real threats from false positives to speed and simplify remediation
- Prioritize penetration tests based on automated vulnerability scans
- Pinpoint exploitable vulnerabilities in networks, operating systems, Web applications and databases
- Add standard and custom exploits for pen-testing real-time