Getting Shells When Metasploit Fails

Presented by:

Ryan Linn

SecTor 2012

Introduction

- Ryan Linn
- Sr Security Consultant
- Network Pen Test Team
- Contributed code to
  - BeEF - Browser Explitation Framework
  - Metasploit
  - Ettercap
- CISSP, CSSLP, OSCP, OSCE, MCSE + Security , CCSP blah blah blah

Why Are We Here

- Metasploit is a useful pen testing tool
- The Meterpreter shell facilitates lots of things
- AV companies are aware of this
- Many are picking up Meterpreter payloads
- But we still want shells
- So what do we do ?
- You're in the right place if you want to find out.

Where We're Headed

- Quick blurb about Metasploit/Meterpreter
- Encoding payloads for AV evasion
- Using winexe to get shells
- Disabling AV
- Executing payloads in memory
- Executing payloads through SQL Server

Metasploit/Meterpreter

- Metasploit
  - Pen Testing/Exploit Development framework
  - Modular
    - Auxiliary – Scanning/Enumeration/Discovery tools
    - Exploitation – Plugable payloads for common exploits
    - Post – Modules to help with post-exploitation
- Meterpreter
  - Specialized shell for use with Metasploit
  - Allows advanced information gathering/traffic routing/ privilege escalation/script execution

Encoding Payloads

- Msfpayload
  - Generate payload from command line
- Msfencode
  - Encode payload from command line
- UPX
  - Pack binaries

Using Winexe

- Command line tool for directly getting shells on remote host
- Spawns a service, then connects to service
- Can use Pass-The-Hash so you don't have to know the password

Disabling AV

- Sc query – List running services
- Tasklist – List running processes
- Net start/stop – start/stop services
- Taskkill – kill processes
  - /IM – Image name (cmd.exe)
  - /PID – Process ID

Executing Payloads in Memory

- Binary never hits disk
- Only thing that will maybe catch us is network av

Getting Shells Through SQL

- Sometimes SMB is disabled
- This lets us use xp_cmdshell to execute commands
- Can disable av/use tftp/etc

Contact Info

- Rlinn@trustwave.com
- Twitter: @sussurro
- Blog: blog.spiderlabs.com

Resources

- Shellcodeexec - https://github.com/inquisb/shellcodeexec
- BackTrack Linux - http://backtrack-linux.org/

Thanks !