Metasploit

ADVANCED COMMAND INJECTION EXPLOITATION:

cmd.exe in the 00's
david d. rude

Affiliated Computer Services
Penetration Tester
www.acs-inc.com

Metasploit
Develop Codes for stuff
www.metasploit.com
Command Injection

**Definition**

*Command injection* is an attack method in which a hacker alters dynamically generated content on a Web page by entering HTML code into an input mechanism, such as a form field that lacks effective validation constraints. A malevolent hacker (also known as a cracker) can exploit that vulnerability to gain unauthorized access to data or network resources. When users visit an affected Web page, their browsers interpret the code, which may cause malicious commands to execute in the users' computers and across their networks.
Command Injection

Uhm...

Really???
Command Injection

Definition
An attack technique used to take advantage of a vulnerability which results in the execution of operating-system commands.
Command Injection

Our Focus
OS Command Injection (to be specific)

Windows Operating Systems

Less useful toolset to work with compared to UNIX, Linux, etc.

Harder to work with post exploitation
Command Injection

Examples

CVE-2009-3845 – HP OpenView NNM Perl CGI

CVE-2008-5516 – gitweb common repository web interface used by open source projects

CVE-2007-3670 – The infamous IE FirefoxURL protocol handler bug Spawned many related issues
Command Injection

**Current Exploits**

Typically a low level of sophistication

Most are for Unix/Linux environments

Most use network related commands for file transfer, etc
Command Injection

Exploitation Considerations

Some Operating Systems only offer a small set of commands

<table>
<thead>
<tr>
<th>Command length limits</th>
<th>XP / Win2k3 / Vista</th>
<th>Win2k</th>
<th>Win95 / 98</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>8191b</td>
<td>2047b</td>
<td>256b</td>
</tr>
</tbody>
</table>

Blind injections
Command Injection

Exploitation Considerations

- Commands available on all Operating System targets
- Common command flags
- Writable/Executable directories
- Metacharacter Filters
**Command Injection**

**Going Beyond Simple Commands**

- Upload binary payloads
- Gives us more options
- More features
- Meterpreter FTW!!!
Command Injection

Network Fu

FTP/TFTP
WScript
Fileshares
Mount Remote Drives
rcp
Command Injection

Pros
- Fast downloads
- Easily scripted
- Low Overhead (no encoding needed)
Command Injection

Cons
- Firewalls
- Web Filters
- Reliability
Command Injection

Non-network Fu

Debug.exe  (Not supported on Windows Vista/7)

WScript
Scripting.FileSystemObject

batch2binary
Command Injection

Pros

Use existing connection

Bypasses firewalls

Works in harsh environments
Command Injection

**Cons**

- Slower downloads (need to use buffering to prevent errors)
- Complex scripting
- Overhead (binary to ASCII conversion)
Command Injection

Designing a Command Stager

Must be reliable

Capable of sending any potential payload

Reuse existing connections (bypass firewalls)

Clean up after itself (Non-persistent)

Stream buffering of data

Reasonably fast
Command Injection

Binary to ASCII Conversion

Could use base64

ASCII representation of hex (0x35 = 0x33 0x35)

Ruby: hex = exe.unpack("H*")[0]

Many options
Command Injection

OS Detection

We can use ‘If exists’ to detect the OS

Check for debug.exe (XP or prior)

Echo a 2048 byte long line to a file (XP)

Echo a < 2048 byte long line to a file (Win2k or prior)

Boot.ini grep/find for a string (XP and prior)
Command Injection

Using Covert Channels

Ping.exe can be used to send messages fairly reliably

Even the harshest of environments typically allow outgoing ICMP

We can use packet size as our status indicator

Using the number of packets to send is overkill
Command Injection

Plan of Attack

The most reliable option is Non-Network Fu

WScript decoder stub (decode a base64 encoded file)

Drop the payload as an executable file and run it

Reverse TCP connections are probably best (Reverse TCP All ports even better)
Command Injection

Demo time!
Command Injection

Code review
Command Injection

Meterpreter FTW!

- An agent which provides a lot of post exploitation capabilities
- Dump Hashes
- Upload/Download files
- Pivoting
- Local Privilege Escalation
Command Injection

Conclusion

Current command injection exploitation techniques are lacking
Reusing existing connections more reliable
WScript is on all windows operating systems
Meterpreter Rocks for post exploitation!
Command Injection

Questions?