



Breaking Things with Ruby



NCC Group Plc
Manchester Technology
Centre Oxford Road
Manchester
M1 7EF
www.nccgroup.com



Rory McCune
Consultant

Tel: +44 (0) 161 209 5200

e-mail: Rory.mccune@nccgroup.com

The Corporate Stuff



·NCC Group

- Pen Testing for 10 years.
- Customers in all sectors.
- One of the largest security teams in the UK.
- The largest CHECK teams in the UK.

·Personal Overview

- 14 years in IT and IT Security.
- Penetration Tester.
- Chapter leader for OWASP Scotland.

What Penetration testing Isn't



Overview – What Penetration Testing Is



- Review the Security of just about anything
 - Web applications
 - Server Operating Systems
 - Databases
 - Custom Application Code
 - Wireless Networks
 - Cash machines
 - . . .
- Essentially we test Assumptions about security

Why Ruby?

- Fits well with Pen testing
- Short time-frames
 - Values developer time over runtime speed
- Varied requirements
 - Flexibility (eg, open classes) is important
- Cross-Platform support
 - Hacking from my phone is fun :)

A Day in the Life

- Classic Pen. Testing consists of a number of phases
 - Scanning
 - Exploitation
 - Post-Exploitation
 - Reporting
- Let's walk through the stages and see where ruby can help.

Scanning

- Assessing what services are available
- De-facto tool of choice – NMAP
 - Quickly assess what the attack surface is
 - Additional scripts give us more information about the target
- XML output (common for most tools)
 - Ruby-nmap (<http://rubynmap.sourceforge.net>) allows us to quickly parse the output and do further processing
 - Also possible to import results to Metasploit...

Interlude - Metasploit

- Largest ruby-based Penetration testing project (that I'm aware of)
- Excluding external dependencies
 - ~ 250,000 LOC
- Covers a lot of ground
 - Exploit development
 - Network Testing
 - Web App testing
 - ...
- Far more than just db_autopwn!

Important Note

Never Run hacking tools against
systems you don't own

Exploitation 1 - Server

- Metasploit allows for rapid development of “traditional” vulnerabilities.
- On networks where patching isn't up to date, these are a great option for easy access.
- Good example – MS08-067

Demo Time!

Exploitation 2 - Client side attacks

- Becoming a much more popular method for attackers
- Combined with “social engineering” can get great results
- Again Metasploit can help automate the process
- Use Metasploit to generate “malicious” PDFs
- Encoding to bypass Anti-Virus.

Demo Time!

Exploitation 3 - Databases

- Another area to test
- Usually the goal for an attacker is to get access to information (eg, credit card details, credentials etc)
- Those are almost always stored in.... databases.
- A number of ways of getting access here too!

Demo Time!

Post Exploitation

- What to do with all those lovely shells
- Meterpeter
 - Very advanced payload
- Very friendly for ruby users

Demo Time!

Reporting & Organisation

- An unfortunate part of every penetration test is...
- Someone wants a report at the end
- Ruby/Rails has us covered here too
- Dradis project (<http://dradisframework.org>)
 - Rails app designed for sharing information in Pen. Test teams and easing the reporting process
 - Imports from common test tools (eg, nmap/nessus)

Convenience Methods – AKA Monkeypatches

- Making use of Rubys open classes.
- Projects like rbkb and Ronin.
- Adding commonly used penetration testing tasks
- String
 - Adds methods like “urlenc” which URL encodes a string
 - “entropy” - rough calculation of entropy in a string
 - “md5” - calculate hashes of strings
- File
 - “strings” - pull printable strings from binary files.
- URL
 - “query_params”
 - “has_sqli?” !

Where to get More information?

- Metasploit
 - <http://www.metasploit.com> - kinda obvious!
 - <http://www.offensive-security.com/metasploit-unleashed> - Free training course for Metasploit
 - <http://carnal0wnage.attackresearch.com><http://www.darkoperator.com> - blogs with lots of good Metasploit info.
- Pen Testing
 - http://www.owasp.org/index.php/Category:OWASP_Testing_Project - OWASP testing guide.
 - <http://www.isecom.org/osstmm/> - Open Source Security Testing Methodology Manual.

Questions?

