Web Attack Tools for Fun and Profit

New Attack Projects
And
Why Should You Volunteer
Why am I up here?

• New Projects
  – Samurai Web Testing Framework
  – Yokoso!
  – Laudanum
  – Social Butterfly

• Benefits of volunteering
  – Different options
  – Lead or join?

• Questions?
Who Am I?

• Senior Security Analyst at InGuardians
• SANS Certified Instructor
  – Author Sec 542 Web Pen-Testing In-Depth
• Project Lead
  – Basic Analysis & Security Engine
    • Intrusion Detection Web Analysis Console
  – Samurai Web Testing Framework
    • LiveCD focused on Web Penetration Tests
  – Yokoso!
    • Infrastructure Fingerprinting via XSS
  – SecTools
    • Collection of Tools (Hping2, Tweety, WebArmor, etc.)
Who is InGuardians, Inc.

• Founded in 2003
• Centered in Washington DC, with offices around the country
  – New Jersey, Chicago, Seattle, Atlanta, Boston
• Vision: We offer world-class information security services utilizing world-class professionals
• Each team member has between 5 and 15 years experience in information security
• Trusted names offering trustworthy advice
• Vendor neutral with no product reselling
• http://samurai.inguardians.com
• Released by
  – Kevin Johnson and Justin Searle
• Team:
  – Frank DiMaggio
• Live Web Pen-Testing Environment
What is Samurai?

- Collection of Tools
- Focused on Web Penetration Testing
- Mainly Open Source tools
- Actively being developed
Major Tools included

- W3AF
  - Web Application Attack & Audit Framework
- Grendel-Scan
  - Web Vulnerability Scanner
- Burp Suite
  - Interception Proxy and Attack Suite
- Fierce Domain Scanner
  - Target Enumeration
- WebScarab
  - Interception Proxy
- Maltego CE
  - Information Gathering and Mapping Tool
- RatProxy
  - Passive Web 2.0 Scanner
- Many Others...
Boot Process

Start Samurai Web Testing Framework in Graphical Mode
Start Samurai Web Testing Framework in Safe Graphical Mode
Install Samurai Web Testing Framework
Check the CD/DVD for defects
Memory Test
Boot the First Hard Disk

Use the ↑ and ↓ keys to select which entry is highlighted. Press enter to boot the selected OS, ‘e’ to edit the commands before booting, or ‘c’ for a command-line.
Boot Continues
GDM Screen

- Authenticate to the Desktop
- Normal User access
- Username: samurai
- Password: samurai
- Root access uses sudo!
Desktop
Using the Tools

- Terminal
- Menu System
Yokoso!

Infrastructure Fingerprinting
Yokoso!

- http://yokoso.inguardians.com
- Focused on Infrastructure Fingerprinting
- Delivered via Cross Site Scripting
- Project Leads:
  - Kevin Johnson & Justin Searle
- Team Member:
  - Frank DiMaggio
Major Pieces

- Proxy Captures
- Fingerprint Requests
- History Lookups
- Controller Additions
Proxy Captures

- Interception Proxy Sessions
- WebScarab is standard
- Remove Private data
  - Placeholders needed
Fingerprint Requests

- Code and/or objects
- Initiate requests to various URLs
- Pre-Authentication
  - Typical
- Post-Authentication
  - If possible
History Lookups

- JavaScript
- Displays a list of URLs
- Determine link color
- Uses Brute Force Techniques
Controller Additions (Kobe)

- Working on adding functions to frameworks
- BEeF is the main focus
  - By Wade Alcorn
  - http://www.bindshell.net
- We are looking into supporting other frameworks
Types of Code

• JavaScript
  – Simple
  – Light-Weight

• Flash Objects
  – More complex
  – Better cross domain support
Laudanum
Laudanum

- Collection of Injectable Files
- Written in Multiple Web Languages
- Provide Pre-Packaged Attacks
  - Heavy Lifting Done For You
- Open Source!
Why Use Laudanum

• More In-Depth Pen-Test
  – Pen-Testing Perfect Storm Webcast
• Leverage Web Issues
• Attack Network Infrastructure
• Better Testing Coverage
What is Provided

• Pre-Packaged Attacks
• Files Written in:
  – PHP
  – ASP
  – ColdFusion
  – JSP
• Controller Application
  – For Third-Party Accessed Files
    • Hooked Browsers
Types of Packaged Attacks

• Command Shell
• LDAP Query Against AD
• DNS Zone Transfers
• Port Scanners
• Web Scanners
• Exploit Delivery
• Proxy Systems
How Do I Inject the Files

• System Access
  – FTP
  – Shell Access
  – Probably have better attacks instead!

• SQL Injection
  – Main Focus of Laudanum
    – select 'Laudanum File Contents' INTO OUTFILE /var/www/html/attack.php
Social Butterfly
Social Butterfly

- Server side application
- Interacts through various APIs
- Runs within the context of the social networking site
- Scope limited for penetration tests
Social Networks
Functions of Social Butterfly

• Social Butterfly has multiple uses
• Information gathering
  – Useful for social engineering
  – Secret question answering
  – Technical data is often exposed
• Browser hooking
  – Again limited by test scope and permission
Volunteering

Fame and Fortune is Waiting
Volunteering

• Benefits:
  – Great Fun
  – Learning Experience
  – Resume Builder

• Cons:
  – Definitely work
  – Attention
Lead or Join?

• **Join:**
  – Joining usually a better start
  – Work with experienced people

• **Lead:**
  – More Control
  – If a project
    • doesn’t exist
    • is dead
Types Needed

- All Skills are needed
- Not just developers
  - Testers
  - Writers
  - Ideas or Sample collectors
Collaboration Systems

• Project Systems
  – Sourceforge
  – Google Code

• Mailing Lists
  – Public
  – Developers

• IRC/IM
Project Idea

• Quick idea for a new project
• Perfect for OWASP due to standard needed
• Standard web testing tool database back end
Web Test Data Store

• Most tools today use their own data store
  – Memory
  – Files
• Build a standard data base for tools to write too
• Allows for sharing information
  – Spider once
  – Share vulns with exploit tools
Sample Project Plan

• Just my idea (Do what you will)
  – Create a SQL Schema
  – Pick some tools to add output to DB
    • Interception proxies would be good first choice
    • Tools that were built for extension are perfect
  – Add functionality to read DB for starting point
• Future feature would be to add support for crash recovery
Questions

kevin@inguardians.com
office: 202.448.8958
cell: 904.403.8024