



SEC-C

**Hacking
is HOT**

sec-c.org

Hackers for Hire

Purpose of Presentation:

- How do security professionals work?
- Types of penetration testing
- Common Vulnerabilities
- Game rules

Professional Hacking

Types of Pentests:

- Network Based
- Web Applications
- Information Leak / Espionage
- Code Reviews

Pentesting Overview

- 1) Recon
- 2) Scanning
- 3) PWNING
- 4) Maintaining Access
- 5) Reporting
- 6) Getting Paid

Audit Types

- Blackbox
no information is provided to the tester
to simulate a real attack
- Whitebox
complete knowledge of the network/technology
- Greybox ←
partial details are known to the tester

Real Example: WebApp Pentest

Case Study of a Real Web Application Audit

- The target: Social Network Web Site
- Scope: Find Web Site Vulnerabilities
- Type: Greybox
- Limitations: HTTP vector only, Test dev environment, no DoS, no malware

* Importance of webapp testing

* All names have been changed for privacy

Strategy & Kickoff Meetings

- Sign all legal documents
(non-disclosure, authorization, disclaimers)
- Check we have get-out-of-jail free card
- Do we have emergency contact numbers?
- Ensure network/system admin is on stand-by
- Review time-line
- Pick an executive target ;)

Phase 1: Recon & Profiling

- Server IP Addresses, Ports, Types & version
- Identify Database
- Technology (LAMP, CGI, JSP, .NET...)
- Survey the application
 - page names, URL, function, forms, scripts
- Partner sites?
- Code surfing

Phase 2: Exploiting!

- XSS Vulnerabilities (and sXSS)
- SQL Injections
- Man in the Middle (MITM)
- Session Hijacking
- Command Injections
- Information Disclosure

Cross Site Scripting Dangers

Injecting malicious code on pages to:

- Steal users' info (cookies,password,email)
- Cause users to attack other sites
- Redirect or open phishing sites
- Clickjacking
- Download malicious code
- Hijack browser

SQL Injection Dangers

- Finding DB and server versions (for exploits)
- Host hacking (adding users, programs...)
- Stealing the DB for Credit Cards, emails...
- Manipulating data (eCommerce, records...)
- Loss of business

Command Injection Dangers

Unvalidated input in GET,POST,COOKIE...

- Automated registration (bots, selling...)
- Read files on the host server (password file...)
- Run programs on the server (add user,R-shell)
- Send emails (social engineering,SPAM...)
- DoS / DDoS

Information Disclosure Dangers

Searching comments in code for:

- Employee/Developer Emails (Social E.)
- App Behavior and Function
- Passwords!
- Addresses
- Goodies

Phase 3: Reporting Test Results

Compiling a detailed report containing:

- Scope, Limitation, Method
- App details, Functionality, Technology
- Summary of Test Results
- Detailed Results and process
- Mitigation and Prevention
- Up-selling (we offer training, advice, hardening)

Tools Used

- Brain
- Automated Tools:
nikto, Whisker, OpenVAS, SARA, online...
- Manual Tools:
sqlmap, webscarab, wget, nslookup, nmap,
Firefox Plugins...
- Ubuntu
- Google

Future Business

Web Applications will stay hackable due to:

- Easy to Learn - many entry-level developers repeating same mistakes.
- Lazy / Bad Programming Habits
- Missing / Bad company policies
- Security missing in the Design Stage
- Money

Thank You, to all SEC-C Hackers

© 2008 Roy Firestein

SEC-C.org