



**The NEbraskaCERT Conference:
August 14, 2007**

at the Peter Kiewit Institute's
Scott Conference Center
Omaha, NE USA

Hacking 432

A Discussion of Advanced Techniques

Ron Woerner, CISSP, CEH, CHFI

Thoughts





Guidelines

This is my interpretation and summary and not necessarily the opinion of my employers (past, present, or future).

Not a debate on open source versus commercial software.

Please feel free to ask questions, make comments at any time.

This is **not** a complete list. Help me to complete it.

Thoughts



Actions that Increase Security

Establish policies and procedures

Identify, assess, and manage risks

Change all default user ids and passwords

Ensure proper access control

Harden servers

Turn off all unnecessary services

Apply appropriate patches

Run anti-virus & anti-spyware applications

Train administrators, managers and users

See PCI DSS v1.1

<https://www.pcisecuritystandards.org/tech/index.htm>



What is Hacking?

Definition 1: Asking a lot of questions and refusing to stop asking. A curiosity to discover how something works and why.

Definition 2: Unauthorized use of computer and network resources.

See: [Two Views of Hacking](#)

<http://www.cnn.com/TECH/specials/hackers/qandas/>



Why Hacking?

To best determine the threats and vulnerabilities to a computer system.

To understand what can go wrong in certain circumstances.

To develop strategies for fixing problems.

To develop a balanced risk equation.

Five Phases of an Attack

- Phase 1: Reconnaissance
- Phase 2: Scanning
- Phase 3: Gaining Access
- Phase 4: Maintaining Access
- Phase 5: Covering Attacks and Hiding



Hacking Techniques

Google Hacking


Web Hacking

Vulnerability Hacking

Wireless Hacking

Stupidity Hacking

Social Engineering



Google Hacking

The art of creating complex search engine queries in order to filter through large amounts of search results for information related to **computer security**.
(**Wikipedia**)

Popularized by Johnny Long

See more at:

<http://johnny.ihackstuff.com/ghdb.php>

Google Hacking

- Google Operators:

- Operators are used to refine the results and to maximize the search value. They are your tools as well as hackers' weapons.

- Basic Operators:

+ , - , ~ , . , * , " " , | , OR

- **Advanced Operators:**

- allintext:, allintitle:, allinurl:, bphonebook:, cache:, define:, filetype:, info:, intext:, intitle:, inurl:, link:, phonebook:, related:, rphonebook:, site:, numrange:, daterange

Google Hacking

The screenshot shows the Google Advanced Search page in Microsoft Internet Explorer. The browser window title is "Google Advanced Search - Microsoft Internet Explorer". The address bar shows the URL "http://www.google.ca/advanced_search?hl=en". The page features the Google logo and the text "Advanced Search" with links for "Advanced Search Tips" and "About Google".

The search options are as follows:

- Find results:** Four radio buttons for search criteria: "with all of the words", "with the exact phrase", "with at least one of the words", and "without the words". Each has an associated input field. To the right is a "10 results" dropdown and a "Google Search" button.
- Language:** "Return pages written in" with a dropdown set to "any language".
- File Format:** "Only" dropdown followed by "return results of the file format" and a dropdown set to "Microsoft Excel (.xls)".
- Date:** "Return web pages updated in the" with a dropdown set to "anytime".
- Occurrences:** "Return results where my terms occur" with a dropdown set to "anywhere in the page".
- Domain:** "Only" dropdown followed by "return results from the site or domain" and an input field. Below it is the text "e.g. google.com, .org" and a link "More info".
- SafeSearch:** Two radio buttons: "No filtering" (selected) and "Filter using SafeSearch".

The taskbar at the bottom shows a single open tab titled "Discussions" with a warning icon and the text "Discussions not available on http://www.google.ca/". The system tray shows the "Internet" icon.

Google Hacking

■ Basic Operators

- (~) search synonym:
Example: ~food
- Return the results about food as well as recipe, nutrition and cooking information
- (.) a single-character wildcard:
Example: m.trix
- Return the results of M@trix, matrix, metrix.....
- (*) any word wildcard

Google Hacking

- Advanced Operators: “Filetype:”
 - Filetype: extension_type
 - Find documents with specified extensions
 - Example: *Budget filetype: xls*

Google Hacking

- Advanced Operators “Intitle:”
 - Intitle: search_term
 - Find search term within the title of a Webpage
 - Allintitle: search_term1 search_term2 search_term3
 - Find multiple search terms in the Web pages with the title that includes all these words
 - These operators are specifically useful to find the directory lists
 - Example – Find directory list:
Intitle: Index.of “parent directory”

Google Hacking

- Advanced Operators “Inurl:”
 - Inurl: search_term
 - Find search term in a Web address
 - Allinurl: search_term1 search_term2 search_term3
 - Find multiple search terms in a Web address
 - Examples:
 - Inurl: cgi-bin
 - Allinurl: cgi-bin password

Google Hacking

- Advanced Operators: “Cache:”
 - Cache: URL
 - Find the old version of Website in Google cache
 - Sometimes, even the site has already been updated, the old information might be found in cache
 - Examples:
 - Cache: www.certconf.org



Google Hacking

- Transparent Proxy
 - Use Google translation tool to surf blocked sites

Google Hacking

- Google, Friend or Enemy?
 - Google is everyone's best friend (yours or hackers)
 - Information gathering and vulnerability identification are the tasks in the first phase of a typical hacking scenario
 - Passive, stealth and huge data collection
 - Google can do more than search
 - Have you used Google to audit your organization today?

Google Hacking

■ Protect Your Data

- Keep patching your systems and applications
- Keep your sensitive data off the Web apply authentication
 - (RSA, Clientless VPN)
- Disable directory browsing
- Google hack your Website
- Consider removing your site from Google's index:
<http://www.google.com/remove.html>.
- Use a robots.txt file to against Web crawlers:
<http://www.robotstxt.org>.



Internet Hacking

Information exposure

- Google hacking

- Public information

 - Netcraft – <http://news.netcraft.com/>

 - Wayback maching –
<http://www.archive.org/>

- Error messages



Web Hacking

Web 2.0 applications on the rise.

Apps using web browser for interface.

75% of all hacks are again web applications.

Over 80% of attacks target port 80.

Web Hacking – OWASP Top 10

http://www.owasp.org/index.php/Top_10_2007

- Cross Site Scripting (XSS)
- Injection Flaws
- Malicious File Execution
- Insecure Direct Object Reference
- Cross Site Request Forgery (CSRF)
- Information Leakage & improper Error Handling
- Broken Authentication and Session Management
- Insecure Cryptographic Storage
- Insecure Communications
- Failure to Restrict URL Access

Web Testing Tools

There are three main classes of software security testing tools:

2. application scanning tools,
3. proxy-based tools, and
4. automated penetration-testing tools.

“Fancy tools aren’t enough. Automated testing tools can’t replace smart QA people. Just as attackers use tools and their own expertise, you need to combine tools and expertise to fight them.” [Forrester View]

<http://www.expresscomputeronline.com/20060306/management02.shtml>

Web Testing Tools

- Microsoft
 - Fiddler HTTP Debugging Proxy (<http://www.fiddlertool.com/fiddler/>)
 - IE Developer Toolbar (<http://www.microsoft.com/downloads/details.aspx?familyid=e59>)
- OWASP (<http://www.owasp.org/index.jsp>)
 - WebGoat & WebScarab
- Nikto (<http://www.cirt.net/code/nikto.shtml>)
 - Web vulnerability scanner and library.
- Syhunt Sandcat (<http://www.syhunt.com/section.php?id=sandcat>)



Web Testing Tools

Bayden Systems' (<http://www.bayden.com/>)

TamperIE – HTTP form-tampering

Bayden IEToys – Dictionary, Encyclopedia, & Google lookup, HMTL Source, IE7 Clear Tracks, Linkify

Sandboxes / Playgrounds

HTTP Sandbox (<http://www.bayden.com/sandbox/>)

HTTPS Sandbox (<https://www.fiddlertool.com/sandbox/>)



Messing Around / Manual techniques

URL manipulation

- Directory Traversal

- Predictable Resource Location

Login tampering

Error message handling

Cookies and cached pages

Unvalidated Input

- Never trust input from a user
- Malicious user can tamper with anything and try to:
 - Cause errors to occur and give up info
 - Buffer overflow
 - Modify parameters
- Common attacks:
 - Modifying URL
 - SQL Injection
 - Cross Site Scripting
 - Session hijacking with cookie modification
 - Hidden input fields

Broken access control

■ Types of attacks:

- Insecure ID (guess IDs)
- Forced browsing past access control checks
 - “/client” is checked for access control
 - “/client/client1/data” is not
 - If someone guesses the full URL....
- Path traversal (../../../../)
- File permissions (OS permission + web server permission)
- Client side caching
 - Airport terminals
 - Internet cafes



Web Testing – Demo

Sandboxes / Playgrounds

HTTP Sandbox (<http://www.bayden.com/sandbox/>)

HTTPS Sandbox (<https://www.fiddlertool.com/sandbox/>)



Vulnerability Hacking

Scanning for known OS and application vulnerabilities.

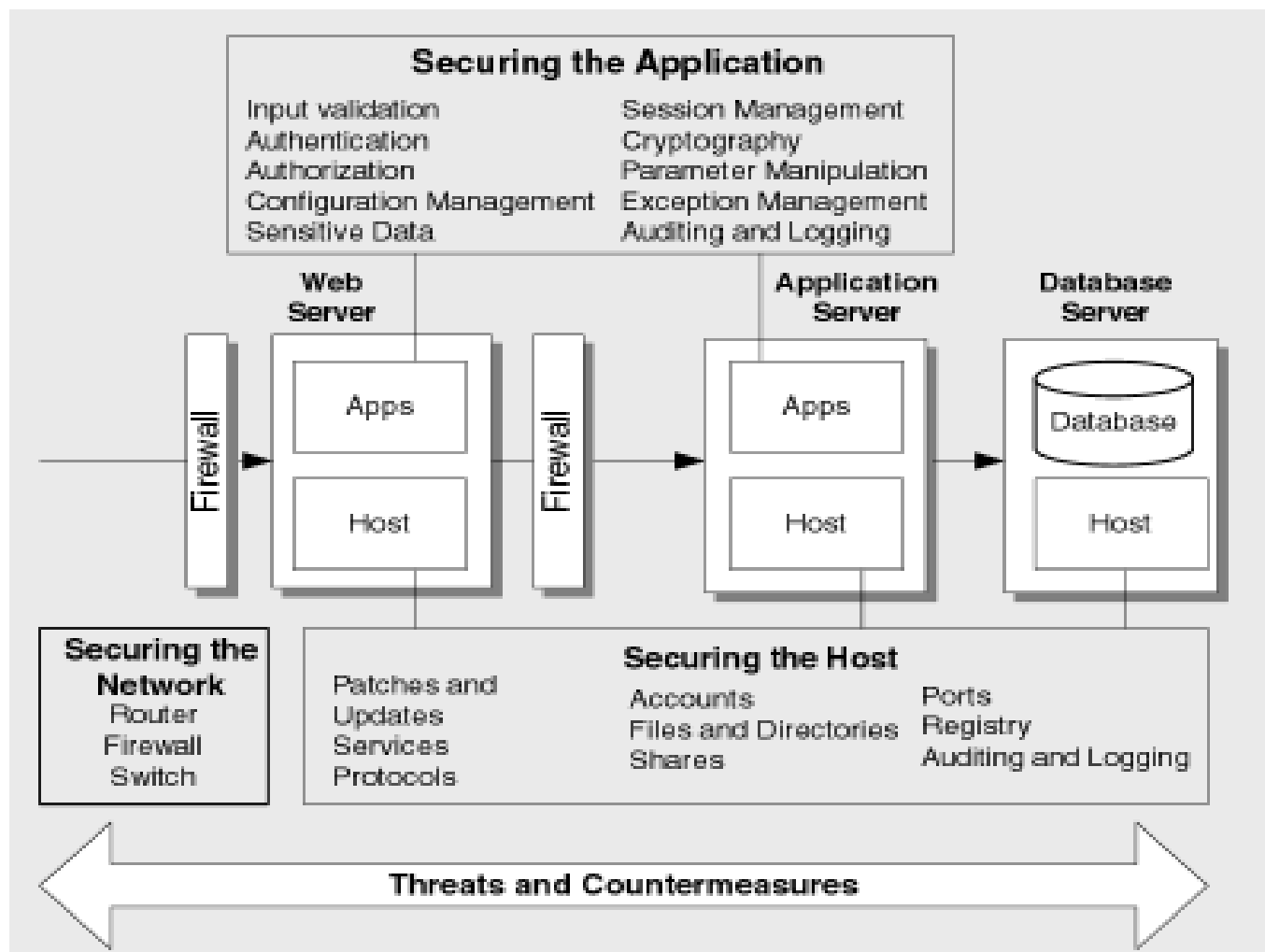
Free Security Tools

- Nmap (<http://www.insecure.org/nmap/>)
 - An open source utility for network exploration or security auditing.
- Nessus (<http://www.nessus.org/>)
 - The premier Open Source vulnerability assessment tool.
- Netcat (<http://www.securityfocus.com/tools/137>)
 - The network swiss army knife.
- Dsniff (<http://naughty.monkey.org/~dugsong/dsniff/>)
 - A collection of tools for network auditing and penetration testing.

Free Security Tools

- Metasploit Framework (<http://framework.metasploit.com/>)
 - An advanced open-source platform for developing, testing, and using exploit code.”
 - Four steps:
 1. Choose a platform/application
 2. Choose an exploit
 3. Choose a shell code
 4. Exploit

Fixing the Problems



Wireless Hacking

- Kismet (<http://www.kismetwireless.net/>)
A 802.11(a/b/g) network sniffer and network dissector
- Network Stumbler (<http://netstumbler.com/>)
- AirSnort (<http://airsnort.shmoo.com/>)
- Aircrack (<http://www.aircrack-ng.org/doku.php>)



Stupidity Hacking

People will always be the weakest link.

Mistakes will always lead the way.

Boredom is second.

Your job is to protect the innocent and
keep honest people honest.



Fraud

Access

Knowledge

Intent



Social Engineering

“The art and science of getting people to comply to your wishes.” (Bernz 2)

“Getting needed information (for example, a password) from a person rather than breaking into a system” (Berg).

Social Engineering

Preys on qualities of human nature:

- The desire to be helpful
- The tendency to trust people
- The fear of getting into trouble

The sign of a truly successful social engineer is they receive information or access without raising any suspicion.

Plausibility + Dread + Novelty = Compromise



Social Engineering

Perception is reality

Opinions tend to become facts.

People generally want to meet your expectations.

Every action human beings take is motivated either out of a need to avoid pain or the desire to gain pleasure – or both.



Persuasion Techniques

A social engineer will

- Misrepresent their objectives to trigger acceptance without thinking.
- Make statements at the outset that triggers a strong emotion such as:
 - Excitement
 - Fear

Technology is only a tool for manipulation.

Bernz's Social Engineering Tips

<http://www.defcon.tv/docs/social-engineering/tips.html>

- Be professional
- Be calm
- Know your mark
- Do not try to fool a superior scammer
- Plan your escape
- Try to be a woman
- Manipulate the less fortunate, the unaware and the stupid
- Use a team if you can



Resources – Past NebraskaCERT Conference Presentations

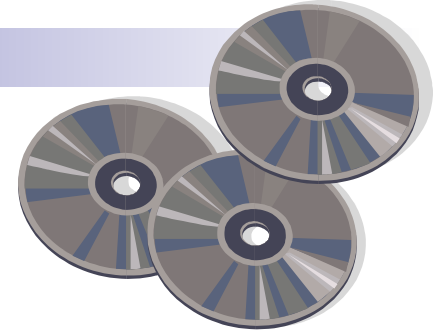
- Fiddling with Fiddler - Testing Web Applications v
- Compromising Wetware - Plugging the Human Le
- Free Security
- Google Hacking
- Acting the Part: Required Non-Technical Skills fo

Free Security Tools – Lists



- Top 75 Security Tools(<http://sectools.org/>)
- Network Security Toolkit
(<http://www.networksecuritytoolkit.org/nst/links.html>)
- S–T–D (<http://s-t-d.org/tools.html>)
- Home PC Firewall Guide
(<http://www.firewallguide.com/>)

Free Security Tools – Bootable CDs



- Network Security Toolkit [NST] (<http://www.networksecuritytoolkit.org/>)
- Trinux (<http://trinux.sourceforge.net/>)
- Knoppix (<http://www.knoppix.org/>)
- Backtrack (<http://www.remote-exploit.org/>)
- Pentoo (<http://www.pentoo.ch/>)
- Helix (<http://www.e-fense.com/helix/>)

See SecurityDistro.com (<http://www.securitydistro.com/>)

Questions



Conclusion

- Be aware of what's available
- Use your (free) resources
- Go out and play
- Join a community:
<http://community.securitycatalyst.com/forums/index.php>
- Share with others
- Do no harm

Thoughts





**THANK
YOU!**

Ron Woerner