A. The Internet, TCP/IP, and LANs
B. Ping sweeps, port scans, traceroutes, & OS fingerprinting
C. An introduction to security issues We’re Here!
   a. Attack Points
      – Human access
      – Physical access
      – LAN access
      – Wireless access
      – Remote (Internet) access
   b. Scanning your site
   c. The law
The Anatomy of an Attack

Introductory Labs – Got them done?

- **Lab #1**: Survey the University of the Pacific
- **Lab #2**: Survey Dave, UOP’s IT security officer
- **Lab #3**: Use Nmap to ping sweep/port scan your own computer (or the lab’s LAN)
- **Lab #4**: Use Nbtenum to capture user data from your own computer (or from the lab’s LAN)
- **Lab #5**: Use SAMInside to capture your own password hashes. Use SamInside and John to crack the passwords
- **Lab #6**: Use Nessus to vulnerability test your own computer (or the lab’s LAN)
- **Lab #7**: Use Ethereal to capture packets on the lab’s LAN
• Now that we know what…
  • Ping sweeps are
  • Port scans are
  • Traceroutes are
  • OS fingerprinting is
• Let’s move on…
So...

What **are** the attack points?

What is being exploited?

**Hint:**

The exploited vulnerabilities are those exploited by the hackers and Internet criminals!
So...

What are the attack points?

What is being exploited?

Hint:

The exploited vulnerabilities are those exploited by the hackers and Internet criminals!

Vulnerable HUMANS!
Vulnerable SERVERS!
Vulnerable CLIENTS!
ATTACK POINTS

1. **Human** access
   - Social engineering

2. **Physical** access
   - Supply chain access
   - Insider access

3. **LAN** access
   - Behind the firewall, but no physical access

4. **Wireless** access

5. **Remote** access
   - Attack via the Internet
1. **The attacker must either:**
   a. Have **physical access** or
   b. Send a message (e.g. email attachment) that exploits a **human** vulnerability or
   c. Know or guess a username and password (i.e. exploit a **configuration** vulnerability or
   d. Send a message (e.g. buffer overflow) that exploits a **server** vulnerability or
   e. Send a message (e.g. from your malicious server) that exploits a **client** vulnerability

2. **The attacker can now:**
   a. Exploit the victim (e.g. download files *from* the target, upload executables *to* the target)
   b. Maintain access (e.g. upload a back door, modify the registry, install a rootkit)
   c. Cover tracks (e.g. delete logs)
The bottom line is this…

1. Exploiting a **Human** vulnerability requires sending the target an executable that he must execute, or enticing the target to visit a malicious website that, for example, asks for a username/password. Or simply guessing a password…

2. Exploiting a **Configuration** vulnerability requires knowing or guessing the vulnerability – for example, a (perhaps default) username and password.

3. Exploiting a **Server Program** vulnerability requires sending the server a malicious message that, for example, causes a buffer overflow and then pushes a shell to the attacker.

4. Exploiting a **Client Program** (e.g. IE) vulnerability requires sending the target an executable that he must execute, or enticing the target to, for example, visit a website that sends a malicious webpage that exploits the target’s browser.
The Target

Remote Offices

Mobile Users

Internet

Human Access

Router-Firewall

Modem

WAP

Mail/SQL

Web Servers

FTP

SSH

Switches

Database Servers

Physical Access

LAN Access

Remote Access

Website Visitors

Wireless Access
HUMAN ACCESS

– Via social engineering
– Via email
  • Spear phishing
– Via malicious websites
  • Spyware/implants
– Via email attachments
  • Trojan/implants
PHYSICAL ACCESS

– If the machine is on…
  • View documents
  • Copy files
  • Retrieve hashed passwords
  • Install tools and rootkits
  • Modify the Registry

– If the machine is off….boot from a CD and …
  • View documents
  • Copy files
  • Retrieve stored password hashes from the hard drive
  • Install tools and rootkits
  • Modify the Registry
  • **You will do all of the above**
“Potential attacks through subversion of hardware or software supply chains can be viewed as another type of insider threat. Access through a hardware supply chain may require development and manufacture of a subverted version of a microelectronic component and a complicated operation to insert the device into the targeted computer, possibly through use of insiders in the supply chain. A software supply chain attack might involve, for example, a subversion embedded in lower-level system software not likely to be evaluated during testing.”

Physical Access

“10 Immutable Laws of Security” @ Microsoft TechNet

Law #3: *If a bad guy has unrestricted physical access to your computer, it's not your computer anymore.*

- He can open the case and replace the BIOS chips.
- He can remove the hard drive from your computer, install it into his computer, and read it.
- He can make a duplicate of your hard drive and take it back to his lair. Once there, he'd have all the time in the world to conduct brute-force attacks, such as trying every possible logon password.
- He can replace your keyboard with one that contains a radio transmitter. He could then monitor everything you type, including your password.

Source:
Attack Points

LAN ACCESS

- View shares on Windows computers
- Grab usernames/privileges on Windows computers
- Grab password hashes on Windows computers
- Hack the ARP (Address Resolution Protocol) process and hijack a session (man-in-the-middle)
  - Ettercap does this
WIRELESS ACCESS

- Fire up your XP SP2 laptop
- “View wireless networks”
- Connect to unprotected networks
  - Fire up Ethereal and observe traffic
- Crack WEP keys with a little effort
- Try to guess WPA keys - more on all this later…

Hacking Wireless Networks For Dummies (For Dummies (Computer/Tech)) (Paperback)

by Kevin Beaver (Author), Peter T. Davis (Author), Devin K. Akin (Foreword) "Wireless local-area networks - often referred to as WLANs or Wi-Fi networks - are all the rage these days..." (more)

Key Phrases: association request packet, wireless network analyzer, unauthorized wireless devices, Network Stumbler, Ethernet Bcpadcast, Hacking For Dummies (more...)

⭐⭐⭐⭐⭐: (6 customer reviews)

List Price: $24.99

Details
REMOTE (INTERNET) ACCESS

- Research
  - Target website
  - Google hacking
  - ARIN (American Registry for Internet Numbers)
  - IP sweeps & port scans
  - Vulnerability (Pen) tests

- Exploit
  - User vulnerabilities
  - Configuration vulnerabilities
  - Client vulnerabilities
  - Server vulnerabilities
The Target

Internet

Remote Offices

Mobile Users

Website Visitors

Remote Access

Human Access

WAP

Router-Firewall

Modem

Switches

Physical Access

Database Servers

Mail/SQL

Web

FTP

SSH

LAN Access

Access

Access
A. The Internet, TCP/IP, and LANs
B. Ping sweeps, port scans, traceroutes, & OS fingerprinting
C. An introduction to security issues
   a. Attack Points
      – Human access
      – Physical access
      – LAN access
      – Wireless access
      – Remote (Internet) access
   b. Scanning your site
   c. The law

We’re Here!
What the Bad Guys Can Find Out

Scanning your site

What can the bad guys find out about you?

– Info gathering tools:
  • Target’s website
  • Google hacking
  • www.arin.net
  • network-tools.com
  • www.netcraft.net
What the Bad Guys Can Find Out

Go to Google Web & Google Groups for…
  ➢ Alliances

Go to Google PPT, Doc, & spreadsheet searches for…
  ➢ Organizational structures

Go to www.sec.gov/edgar/searchedgar/companysearch.html for...
  ➢ Corporate/financial information

Go to www.internic.net or http://network-tools.com for...
  ➢ Contact information & domain names
Google Hacking!

- While Google is a researcher's friend, it is an attacker's dream.

- Many networks are insecure with inadequate security, giving Google access to sensitive information.

- Confidential information, configuration data, password files, and much more are often available.

- Also visit: http://johnny.ihackstuff.com
Google hacking

- Google hacking is the term used when a hacker tries to find exploitable targets and sensitive data by using search engines – using Google, in particular.
- The Google Hacking Database (GHDB) is a database of queries that identify sensitive data. Download at:
  - http://johnny.ihackstuff.com

**Information that the Google Hacking Database identifies:**

- Advisories and server vulnerabilities
- Error messages that contain too much information
- Files containing passwords
- Sensitive directories
- Pages containing logon portals
- Pages containing network or vulnerability data such as firewall logs.
“How to Google Hack Windows Servers”

Available at: http://searchwindowssecurity.techtarget.com/tip/1,289483,sid45_gci1089383,00.html

Google can be used to perform security scans against your public-facing servers -- Windows, IIS, Apache and SQL Server. You can profile servers, find files containing sensitive information and detect "hidden" login pages, server log files and a whole lot more.

TABLE OF CONTENTS

• Why use Google to scan for security vulnerabilities
• Google tools for automated hacking tests
• Google queries for manual hacking tests
• Four steps to safeguard Windows data from Google hackers
Hello,

Listing 5. Importing default Drupal SQL database.
For:
C:\eclipse\workspace\drupal_development> mysql -u drupal_user -p drupal_db < database/database.4.1.mysql

I received the following answer:
ERROR 1045 (28000): Access denied for user 'drupal_user'@'localhost' (using password: YES)

Could someone give me a hint, please?
I am stuck here with this tutorial.

The password is correct. It worked for:
C:\Documents and Settings\Administrator> mysql -u root -p mysql

Thanks,
Adrian
Google - Search IBM’s website for PPT presentations…

**Embedded Concatenative**
File Format: Microsoft Powerpoint 97 - View as HTML

**Business Position Model**
File Format: Microsoft Powerpoint 97 - View as HTML
IBM logo must not be moved, added to, or altered in any way. Background should not be modified. Title/subtitle/confidentiality line ...
www.developer.ibm.com/.../$file/decision_support_plan_completed_example_09012003.ppt - Similar pages
More Google Hacking

Google - Search IBM’s website for Word documents…

[doc] do you know anything about "exclusive lock waits". there are some ...
File Format: Microsoft Word 6 - View as HTML

do you know anything about "exclusive lock waits". there are some locks that last 
forever... and i cannot reach some records in MSEG table. what shoul i do... ...
www-912.ibm.com/s_dir/SAPDiscuss.nsf/0/635c48630b33c07686256a42002865df/$FILE/3elge1.doc -
Supplemental Result - Similar pages

[doc] IBM Authorized Business Partner
File Format: Microsoft Word 97 - View as HTML
IBM Authorized Value Partner. Solution Register Form. IBM
More Google Hacking

Google - Search IBM’s website for spreadsheets.
More Google Hacking

Spreadsheets I found...

<table>
<thead>
<tr>
<th>EMPLOYEE</th>
<th>GROSS WAGE</th>
<th>EMPLOYEE</th>
<th>GROSS WAGE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Abigail Almon</td>
<td>$140.00</td>
<td>Robert Ficker</td>
<td>$800.00</td>
</tr>
<tr>
<td>Debra Almon</td>
<td>$53,477.24</td>
<td>Sherri Ficker</td>
<td>$17,400.92</td>
</tr>
<tr>
<td>Donna Baker</td>
<td>$27,621.51</td>
<td>Jeanne Finney</td>
<td>$140.00</td>
</tr>
<tr>
<td>Raymond Bernier</td>
<td>$70.00</td>
<td>Catherine Fitzgerald</td>
<td>$7,416.62</td>
</tr>
<tr>
<td>Lisa Begley</td>
<td>$1,900.00</td>
<td>Lee Fitzgerald</td>
<td>$14,080.14</td>
</tr>
<tr>
<td>Janine Beck</td>
<td>$29,685.96</td>
<td>Maria Foley</td>
<td>$70.00</td>
</tr>
<tr>
<td>Theresa Blades</td>
<td>$17,789.00</td>
<td>Lisa Forsyth</td>
<td>$34,046.05</td>
</tr>
<tr>
<td>Andy Blake</td>
<td>$1,966.16</td>
<td>Janet Fortin</td>
<td>$140.00</td>
</tr>
<tr>
<td>Denise Bissonnette</td>
<td>$8,383.07</td>
<td>Gine Genest</td>
<td>$46,028.07</td>
</tr>
<tr>
<td>Kristine Boardman</td>
<td>$36,366.22</td>
<td>Deborah Gobell</td>
<td>$49,370.06</td>
</tr>
<tr>
<td>Robin Bolton</td>
<td>$630.00</td>
<td>James Gough</td>
<td>$46,106.66</td>
</tr>
<tr>
<td>Jennifer Bolster</td>
<td>$325.80</td>
<td>Sonja Gonzalez</td>
<td>$45,816.01</td>
</tr>
<tr>
<td>Corey Brackett</td>
<td>$13,827.20</td>
<td>Diane Gray</td>
<td>$46,873.06</td>
</tr>
<tr>
<td>Scott Brown</td>
<td>$43,570.06</td>
<td>Marian Guidoboni</td>
<td>$1,500.00</td>
</tr>
<tr>
<td>Jason Butler</td>
<td>$47,000.16</td>
<td>Mary Hale</td>
<td>$45,448.14</td>
</tr>
<tr>
<td>Margaret Callahan</td>
<td>$3,010.00</td>
<td>Brenda Hamel</td>
<td>$175.00</td>
</tr>
<tr>
<td>Cheryl Catanaro</td>
<td>$44,680.95</td>
<td>Benjamin Hayes</td>
<td>$140.00</td>
</tr>
<tr>
<td>Frances Chickering</td>
<td>$1,200.00</td>
<td>Danielle Hill</td>
<td>$70.00</td>
</tr>
</tbody>
</table>

FREMONT SCHOOL DISTRICT PAYROLL 2004-2005
More Google Hacking

Spreadsheets I found…

[Image of a web browser showing a spreadsheet with the following data:

<table>
<thead>
<tr>
<th>Check Number</th>
<th>Check Date</th>
<th>Employee Number</th>
<th>Gross Pay</th>
</tr>
</thead>
<tbody>
<tr>
<td>9011803</td>
<td>11/4/2004</td>
<td>6</td>
<td>2,009.11</td>
</tr>
<tr>
<td>9011763</td>
<td>11/4/2004</td>
<td>13</td>
<td>2,022.07</td>
</tr>
<tr>
<td>9011833</td>
<td>11/4/2004</td>
<td>15</td>
<td>940.80</td>
</tr>
<tr>
<td>9011765</td>
<td>11/4/2004</td>
<td>19</td>
<td>1,828.00</td>
</tr>
<tr>
<td>9011766</td>
<td>11/4/2004</td>
<td>21</td>
<td>1,495.20</td>
</tr>
<tr>
<td>9011770</td>
<td>11/4/2004</td>
<td>22</td>
<td>2,526.40</td>
</tr>
<tr>
<td>9011771</td>
<td>11/4/2004</td>
<td>24</td>
<td>996.80</td>
</tr>
<tr>
<td>14372</td>
<td>11/4/2004</td>
<td>25</td>
<td>1,422.31</td>
</tr>
<tr>
<td>9011817</td>
<td>11/4/2004</td>
<td>26</td>
<td>2,291.20</td>
</tr>
</tbody>
</table>

MRCA Payroll Disbursement
November 2004]
More Google Hacking

Spreadsheets I found…

![Excel Spreadsheet](http://www.hoosierdata.in.gov/docs/2q2005Q.xls)

**Indiana Covered Employment and Payrolls**

<table>
<thead>
<tr>
<th>County</th>
<th>Monthly Employment</th>
<th>Quarterly Payroll</th>
<th>Average Weekly Earnings</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>April</td>
<td>May</td>
<td>June</td>
</tr>
<tr>
<td>1</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>7</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>14.550</td>
<td>14.790</td>
<td>14.940</td>
</tr>
<tr>
<td>9</td>
<td>177.620</td>
<td>179.390</td>
<td>176.120</td>
</tr>
<tr>
<td>10</td>
<td>41.340</td>
<td>41.440</td>
<td>41.720</td>
</tr>
<tr>
<td>11</td>
<td>2.490</td>
<td>2.520</td>
<td>2.480</td>
</tr>
<tr>
<td>12</td>
<td>4.130</td>
<td>4.140</td>
<td>4.160</td>
</tr>
<tr>
<td>13</td>
<td>17.620</td>
<td>17.860</td>
<td>17.930</td>
</tr>
<tr>
<td>14</td>
<td>3.020</td>
<td>3.130</td>
<td>3.300</td>
</tr>
<tr>
<td>15</td>
<td>5.170</td>
<td>5.260</td>
<td>5.380</td>
</tr>
<tr>
<td>16</td>
<td>15.760</td>
<td>15.840</td>
<td>15.780</td>
</tr>
<tr>
<td>17</td>
<td>43.570</td>
<td>44.030</td>
<td>44.460</td>
</tr>
<tr>
<td>18</td>
<td>7.470</td>
<td>7.490</td>
<td>7.540</td>
</tr>
<tr>
<td>19</td>
<td>10.940</td>
<td>11.060</td>
<td>11.210</td>
</tr>
<tr>
<td>20</td>
<td>2.240</td>
<td>2.280</td>
<td>2.240</td>
</tr>
<tr>
<td>21</td>
<td>10.740</td>
<td>10.870</td>
<td>10.520</td>
</tr>
<tr>
<td>22</td>
<td>14.480</td>
<td>14.850</td>
<td>14.690</td>
</tr>
<tr>
<td>23</td>
<td>12.400</td>
<td>12.470</td>
<td>12.530</td>
</tr>
</tbody>
</table>

Source: [Indiana Workforce Development](http://www.hoosierdata.in.gov/docs/2q2005Q.xls)
Google Hacking

I Googled: “place of death” ssn
And 49,00 hits like this one:
What the Bad Guys Can Find Out

The Wayback Machine: Go to http://www.archive.org and then type in a URL. Here’s King’s website history:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Pages</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>2</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Year</th>
<th>2003</th>
<th>2004</th>
<th>2005</th>
<th>2006</th>
<th>2007</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pages</td>
<td>4</td>
<td>3</td>
<td>2</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>Oct 14, 2003</td>
<td>Dec 11, 2004</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Dec 23, 2003</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
What the Bad Guys Can Find Out

*Interesting information on individuals might be found at:*

- www.monster.com
- www.hotjobs.com
- Google’s Groups

*Search on:*

“Top secret security clearance”
What the Bad Guys Can Find Out

When the attacker runs ping sweeps, port scans, and vulnerability tests, he needs:

- Owned IP address ranges
  - www.arin.net (American Registry for Internet Numbers)
- Name server names & IP addresses
  - http://network-tools.com (DNS records)
- Other server IP addresses (Web, email, SQL)
  - http://www.netcraft.net
What the Bad Guys Can Find Out

Enter: google or: university of the pacific or: ibm
The IP addresses Google owns

<table>
<thead>
<tr>
<th>Organization</th>
<th>AS Number</th>
<th>Type</th>
<th>Address Range</th>
</tr>
</thead>
<tbody>
<tr>
<td>Google Inc.</td>
<td>AS15169</td>
<td></td>
<td>15169</td>
</tr>
<tr>
<td>Google Inc.</td>
<td>AS36039</td>
<td></td>
<td>36039</td>
</tr>
<tr>
<td>Google Inc.</td>
<td>AS36040</td>
<td></td>
<td>36040</td>
</tr>
<tr>
<td>Google Inc.</td>
<td>AS15169</td>
<td></td>
<td>15169</td>
</tr>
<tr>
<td>Google Inc.</td>
<td>AS36039</td>
<td></td>
<td>36039</td>
</tr>
<tr>
<td>Google Inc.</td>
<td>AS36040</td>
<td></td>
<td>36040</td>
</tr>
<tr>
<td>Google Incorporated</td>
<td>AS36384</td>
<td></td>
<td>36384</td>
</tr>
<tr>
<td>Google Incorporated</td>
<td>AS36385</td>
<td></td>
<td>36385</td>
</tr>
<tr>
<td>Google Inc. GOOGLE</td>
<td>NET-216-239-32-0-1</td>
<td></td>
<td>216.239.32.0 - 216.239.63.255</td>
</tr>
<tr>
<td>Google Inc. GOOGLE</td>
<td>NET-64-233-160-0-1</td>
<td></td>
<td>64.233.160.0 - 64.233.181.255</td>
</tr>
</tbody>
</table>

Click here for address and POC
Address and POC (admin info):
ARIN Information

- Address: Used for wireless scanning (war driving)
- Telephone Number: Used for social engineering
- Contact Name: Used for social engineering
2. To get contact & name server info, go to http://network-tools.com, check “Network Lookup.” **Enter:** target, click **Submit**. No checks!
2. The Network-Tools results came straight from ARIN...
What the Bad Guys Can Find Out

Name Server Information: http://network-tools.com

- Check “DNS Records,” enter target name, click “Submit”

No checks!
What the Bad Guys Can Find Out

To get a list of UOP’s web servers, go to www.netcraft.com and, under “What’s that site running?..., Enter: .uop.edu

Include the period!
What the Bad Guys Can Find Out

If your target is Google, enter: .google.com. You get a list of all 144 of Google’s web servers – and their OSs (all Linux)!

![Netcraft page showing search results for .google.com](image-url)
Others can scan **YOU** remotely!

More on this in your **homework** (www.grc.com).

In Part 4, we continue with:
**How Others Scan You!**