Hashes in Hi-Res
Unleashing the GPU beasts via CUDA
WHOAMI

3ig0nyohB – Pinoy GreyHat Huk

- Total n00b with guts to talk to l33ts
- Can get drunk with pure milk on the table
- Puked on the garden last BT2
- Survivor – survived BlackDawg's vicious bites
Other credentials

- MIS Manager
- Formerly a scene whore
- Got 3 kids
- Still happily married
- Doing talks for Software Freedom Day (http://softwarefreedomday.org)
Other other credentials

• Church's Tech Support team
• Faith and passion for technology motivated
• Wanting to give back to the community
What's this talk all about

• NEVER EVER MESS AROUND WITH A HACKER. (they learned the lesson the hard way)

• Tackle a little what CUDA is all about

• Demo CUDA enabled tools

• Q&A Later (No l33t questions please ... hehehe)
BacktTrack 4
PGHO Release
• Mails are blocked by RBL
• Sniffed the whole network – wireshark on the gateway
• Analyzed and saved the capture
• An a**hole fed the bosses wrong info
• I'm moonlighting during/after office hours
• Downloading warez
• Called for closed door meet
• Used some SE skillz to win the bosses attention
• Showed the captured packets
<table>
<thead>
<tr>
<th>No.</th>
<th>Time</th>
<th>Source</th>
<th>Destination</th>
<th>Protocol</th>
<th>Info</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>0.0000000</td>
<td>76.13.15.41</td>
<td>172.16.20.32</td>
<td>YMSG</td>
<td>Pager Logout (status=Server Ack)</td>
</tr>
<tr>
<td>140</td>
<td>11.130391</td>
<td>172.16.20.32</td>
<td>76.13.15.41</td>
<td>YMSG</td>
<td>Notify (status=Notify)</td>
</tr>
<tr>
<td>150</td>
<td>12.249896</td>
<td>172.16.20.32</td>
<td>76.13.15.41</td>
<td>YMSG</td>
<td>Y7 Chat Session (status=Default)</td>
</tr>
<tr>
<td>153</td>
<td>12.510653</td>
<td>76.13.15.41</td>
<td>172.16.20.32</td>
<td>YMSG</td>
<td>Y7 Chat Session (status=Server Ack)</td>
</tr>
<tr>
<td>154</td>
<td>12.510799</td>
<td>172.16.20.32</td>
<td>76.13.15.41</td>
<td>YMSG</td>
<td>Message (status=Offline)</td>
</tr>
<tr>
<td>164</td>
<td>13.355084</td>
<td>76.13.15.41</td>
<td>172.16.20.32</td>
<td>YMSG</td>
<td>Picture (status=Server Ack)</td>
</tr>
<tr>
<td>165</td>
<td>13.355784</td>
<td>76.13.15.41</td>
<td>172.16.20.32</td>
<td>YMSG</td>
<td>Picture (status=Default)</td>
</tr>
<tr>
<td>166</td>
<td>16.830057</td>
<td>76.13.15.41</td>
<td>172.16.20.32</td>
<td>YMSG</td>
<td>Keep Alive (status=Default)</td>
</tr>
<tr>
<td>236</td>
<td>47.079333</td>
<td>76.13.15.41</td>
<td>172.16.20.32</td>
<td>YMSG</td>
<td>Status V15 (status=Server Ack)</td>
</tr>
<tr>
<td>247</td>
<td>54.920555</td>
<td>76.13.15.41</td>
<td>172.16.20.32</td>
<td>YMSG</td>
<td>Y6 Status Update (status=Server Ack)</td>
</tr>
<tr>
<td>326</td>
<td>76.321849</td>
<td>76.13.15.41</td>
<td>172.16.20.32</td>
<td>YMSG</td>
<td>Y6 Status Update (status=Server Ack)</td>
</tr>
<tr>
<td>329</td>
<td>76.831789</td>
<td>76.13.15.41</td>
<td>172.16.20.32</td>
<td>YMSG</td>
<td>Keep Alive (status=Default)</td>
</tr>
<tr>
<td>350</td>
<td>87.739313</td>
<td>76.13.15.41</td>
<td>172.16.20.32</td>
<td>YMSG</td>
<td>Notify (status=Server Ack)</td>
</tr>
<tr>
<td>354</td>
<td>88.852999</td>
<td>76.13.15.41</td>
<td>172.16.20.32</td>
<td>YMSG</td>
<td>Message (status=Server Ack)</td>
</tr>
<tr>
<td>356</td>
<td>89.295390</td>
<td>76.13.15.41</td>
<td>172.16.20.32</td>
<td>YMSG</td>
<td>Notify (status=Server Ack)</td>
</tr>
<tr>
<td>359</td>
<td>90.229373</td>
<td>76.13.15.41</td>
<td>172.16.20.32</td>
<td>YMSG</td>
<td>Status V15 (status=Server Ack)</td>
</tr>
<tr>
<td>363</td>
<td>93.934331</td>
<td>172.16.20.32</td>
<td>76.13.15.41</td>
<td>YMSG</td>
<td>Notify (status=Notify)</td>
</tr>
<tr>
<td>374</td>
<td>97.215081</td>
<td>172.16.20.32</td>
<td>76.13.15.41</td>
<td>YMSG</td>
<td>Message (status=Offline)</td>
</tr>
</tbody>
</table>

Frame 1 (102 bytes on wire, 102 bytes captured)
* Internet Protocol, Src: 76.13.15.41 (76.13.15.41), Dst: 172.16.20.32 (172.16.20.32)
* Transmission Control Protocol, Src Port: mnc (5050), Dst Port: tsmcontrol-oms (1158), Seq: 1, Ack: 1, Len: 48
* Yahoo YMSG Messenger Protocol (Pager Logout)

```
0000 00 1f 29 ad ea 66 00 80 ad 71 5a d9 08 00 45 00 .).F... .qz..E.
0010 00 58 3e 09 40 00 30 06 21 30 4c 00 0f 29 ac 10 .x> .O. .Dl...).)
0020 14 20 13 ba 04 84 2d 2b 45 33 fe 84 1d 2e 30 18 ....... E5...P.
0030 ff ff 74 31 00 00 59 4d 53 47 00 0f 00 00 00 1c ...tl_yM 5G....
0040 00 62 00 00 00 00 5f 61 32 37 0c 80 73 63 6d ....... 27...Sem
0050 70 72 69 78 64 00 00 00 34 34 3c 00 80 34 31 39 34 pr:tx:z 44..4194
0060 32 33 39 c0 80 00 239...
```
Accidently? showed a .... hehehehehe
.49..TYPING..1..4..14..13..1..5..
.1..4..14..13..1..5..
.5..4..14..balitaan mo pag okay na yung com ko..97..1..63..;0..64..0..206..2...
.1..4..14..13..1..5..
...
.5..4..14..pickup ko jan..97..1..63..;0..64..0..206..2...
.1..4..14..13..1..5..
300..315..7..10..0..13..1..192..-184112413..197..1XB6g6oMeAAECP4E_
100..213..2..244..3075..283..1..317..1..301..315..303..315..
.5..4..14..D..97..1..63..;0..64..0..206..2...
.1..4..5..97..1..63..;0..64..0..206..2..14..naninigurado lang naman...
500..0...
.49..TYPING..1..4..14..13..0..5...
.49..TYPING..1..4..14..13..1..5...
THE ASSHOLE GOT HIS ASS KICKED
NEVER EVER MESS AROUND WITH A HACKER. They learned their lessons the hard way.
Hashes in Hi-Res
The old times

- Use JTR to break hashes
- Cain and Abel
- Aircrack-NG
- Cowpatty
- Ophcrack+Online Rainbow Tables
Problem with old times

- JTR takes a long time breaking complex/non-dict passwords
- “djohnd” exists but nodes should have similar CPU power – expensive to build
- Aircrack-NG is the same (or used to be the same)
- Cowpatty – space hog
- Online Rainbow tables – Waiting list is as long as people in Divisoria during holiday season
Enter CUDA

• Compute Unified Device Architecture

• CUDA – parallel computing architecture by NVIDIA

• leverages the parallel compute engine in NVIDIA GPUs

• In other words ... It's l33t (but a n00b is talking about it now)
Why CUDA?

• Can break hashes 10 to 15 times using CUDA enabled apps
• Can crack hashes faster when combined with Space-Time-Trade-Off
• Tools are already scattered and being developed to take advantage of this technology
• It's ready to roll on BT4
CUDA Enabled tools

- Multiforcer – MD5, MD4, NTLM/2 brute forcer
- BarsWF (MD5 only) – MD5 bruteforcer for windows
- Pyrit – latest attack tool on Wireless encryptions
- Aircrack-NG now supports CUDA – not enabled by default
Multiforcer Demo
Pyrit
Pyrit + CUDA
Pyrit + cowpatty
Credits

- Encrypted and aphro.ph of PGHO
- **Pureh@te** Of remote-exploit – I used his paper for this talk
- People at aircrack-ng.org
- Bitweasil of cryptohaze.com for multiforcer
- lucas.lueg - author of pyrit
- The whole remote-exploit team
- Church of WiFi congregation
- PINOYGREYHAT.ORG community