Hacking Challenges
Have Fun Improving Your Skills

Raúl Siles
Taddong

SANS London 2009
Have Fun Improving Your Skills

"Nintendo English Training: Have Fun Improving Your Skills"
Hacking Challenges

Types:
• 2009:
  – Pen-Test vs. IH
• CtF events:
  – Training
  – Conferences
• EH.net (Don & Ed)
• ...

Goals:
• Improve your...
  – Knowledge
  – Technical skills
• Have Fun! 😊
Hackers for Charity (HFC)

• Johnny Long
• HFC:
  – http://www.hackersforcharity.org
• The Informer:
  – http://ihackcharities.org/category/informer-blog/

hackersforcharity.org
Breaking...

- Trying to get access to GATE’s data net
- Using VoIP phone Ethernet connection
- Windows XP SP3 & BTv4 (pre-final)
- No advanced layer 2 network access protection mechanism
- Intel® PRO/100 VE Network Connection NIC
- Can capture data (Wireshark)
- Cannot send any data!
<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>2009-05-10 07:43:28:671</td>
<td>00:0c:29:0f:c9:30</td>
<td>FF:ff:ff:ff:ff:ff</td>
<td>ARP</td>
<td>who has 172.29.1.1? Tell 172.29.1.201</td>
</tr>
<tr>
<td>3</td>
<td>2009-05-10 07:43:31:426</td>
<td>172.29.1.1</td>
<td>172.29.255.255</td>
<td>ICMP</td>
<td>Echo (ping) request</td>
</tr>
<tr>
<td>4</td>
<td>2009-05-10 07:43:32:706</td>
<td>172.29.255.255</td>
<td>172.29.255.255</td>
<td>ICMP</td>
<td>Echo (ping) request</td>
</tr>
<tr>
<td>5</td>
<td>2009-05-10 07:43:34:801</td>
<td>192.168.1.1</td>
<td>224.0.0.9</td>
<td>RIPV2</td>
<td>Response</td>
</tr>
<tr>
<td>6</td>
<td>2009-05-10 07:43:35:355</td>
<td>192.168.1.1</td>
<td>224.0.0.9</td>
<td>RIPV2</td>
<td>Response</td>
</tr>
<tr>
<td>8</td>
<td>2009-05-10 07:43:36:426</td>
<td>172.29.1.1</td>
<td>255.255.255.255</td>
<td>NTP</td>
<td>NTP Broadcast</td>
</tr>
<tr>
<td>9</td>
<td>2009-05-10 07:43:37:041</td>
<td>172.29.1.1</td>
<td>255.255.255.255</td>
<td>DHCP</td>
<td>DHCP Discover - Transaction ID: 0x53156</td>
</tr>
<tr>
<td>10</td>
<td>2009-05-10 07:43:37:299</td>
<td>172.29.1.1</td>
<td>255.255.255.255</td>
<td>DHCP</td>
<td>DHCP Offer - Transaction ID: 0x53156</td>
</tr>
<tr>
<td>11</td>
<td>2009-05-10 07:43:38:011</td>
<td>172.29.1.1</td>
<td>172.29.255.255</td>
<td>DHCP</td>
<td>DHCP Offer - Transaction ID: 0x53156</td>
</tr>
<tr>
<td>12</td>
<td>2009-05-10 07:43:38:115</td>
<td>172.29.1.1</td>
<td>172.29.1.104</td>
<td>SIP</td>
<td>Status: 200 OK (2 bindings)</td>
</tr>
<tr>
<td>13</td>
<td>2009-05-10 07:43:38:913</td>
<td>172.29.1.1</td>
<td>172.29.1.104</td>
<td>SIP</td>
<td>Status: 200 OK (2 bindings)</td>
</tr>
<tr>
<td>14</td>
<td>2009-05-10 07:43:39:426</td>
<td>172.29.1.1</td>
<td>172.29.255.255</td>
<td>ICMP</td>
<td>Echo (ping) request</td>
</tr>
<tr>
<td>15</td>
<td>2009-05-10 07:43:39:426</td>
<td>172.29.1.1</td>
<td>172.29.255.255</td>
<td>ICMP</td>
<td>Echo (ping) request</td>
</tr>
<tr>
<td>16</td>
<td>2009-05-10 07:43:41:201</td>
<td>172.29.1.1</td>
<td>172.29.255.255</td>
<td>DHCP</td>
<td>DHCP Discover - Transaction ID: 0x53156</td>
</tr>
<tr>
<td>17</td>
<td>2009-05-10 07:43:41:201</td>
<td>172.29.1.1</td>
<td>255.255.255.255</td>
<td>DHCP</td>
<td>DHCP Discover - Transaction ID: 0x53156</td>
</tr>
<tr>
<td>18</td>
<td>2009-05-10 07:43:51:247</td>
<td>00:0.0.0</td>
<td>255.255.255.255</td>
<td>DHCP</td>
<td>DHCP Discover - Transaction ID: 0x53156</td>
</tr>
</tbody>
</table>

Frame 17 (342 bytes on wire, 342 bytes captured)

Ethernet II, src: 00:0c:29:12:34:aa (00:0c:29:12:34:aa), Dst: ff:ff:ff:ff:ff:ff (ff:ff:ff:ff:ff:ff)

Internet Protocol, src: 0.0.0.0 (0.0.0.0), Dst: 255.255.255.255 (255.255.255.255)

User Datagram Protocol, src Port: 68 (68), Dst Port: 67 (67)

Bootstrap Protocol, src: 192.168.1.1, Dst: 192.168.1.1

Protocol: bootp (bootstrap), 300 bytes

Packets: 30 Displayed: 30 Marked: 0

Profile: Default
Challenge Question 1

What is the most probable reason Michael could not get network connectivity from the desk Ethernet jack?

What actions should the team take to determine exactly what is going on, collect full traffic captures, and gain full access to the network?
Solution 1

• Wireshark’s documentation Wiki:
  “When capturing on a VLAN, you won't necessarily see the VLAN tags in packets. ... **It depends on the NIC, the NIC firmware, the driver, and the alignment of the moon and planets**”

• Windows registry tweaks (Intel NIC)
Solution 1

# modprobe 8021q
# cd vlan
# ./vconfig add eth0 20
# ifconfig eth0.20 up
Entering...

- Access to General’s desktop computer (USB drive)
- Reverse connection back (to BTv4)
- Copy a couple of hacking tools
- Firewall:
  - Deny inbound traffic
  - Allow outbound traffic (from General’s)
- Capture traffic on General’s desktop
The Setup

- **Hacking laptop**
  - GATE’s network
  - Switch
  - Core Network
  - Firewall
    - Firewall doesn’t allow inbound connections. It only allows outbound connections from the General’s network.

- **The Company**
  - General’s desktop
  - General’s laptop
  - Hub
  - IDS
  - Scylla Codes server
  - Reverse connection

- **General’s network**

- **Servers network**
[*] Upload completed.
[*] Meterpreter session 1 opened (hacking:443 -> general-desktop:1705)

```
msf exploit(handler) > sessions -i 1
[*] Starting interaction with 1...
meterpreter > getuid
Server username: GENERAL-DESKTOP\Administrator
meterpreter > sysinfo
Computer: GENERAL-DESKTOP
OS : Windows Vista (Build 6002, Service Pack 2).
meterpreter > pwd
C:\
meterpreter > cd Scylla
meterpreter > ls
Listing: C:\Scylla

Mode Size Type Last modified Name
---- ---- ---- ------------------ ----
40777/rwxrwxrwx 0    dir  Sun May 17 10:29:09 -0900 2009  ..
100777/rwxrwxrwx 569344 fil  Sun May 17 10:29:09 -0900 2009 WinDump.exe
```
Challenge Questions 2 & 3

What tool should Lincoln download, if any, to be able to capture traffic on the desktop computer?

Starting with the reverse connection from the desktop computer, describe a step-by-step approach that could be applied prior to 09:00 the next day in order to capture the network traffic on the remote network and get a capture file for further in-depth analysis. Make sure your approach follows Michael's advice to avoid detection.
Solution 2 & 3

- The easy way... using the “new” Metasploit built-in Meterpreter sniffer module
- You can read the hard way on the official solution to the challenge
... Decoding

- Analyze captured traffic:  
  - Capture.pcap
- Extra file:  
  - Backup.zip
Challenge Questions 4 & 5

Help the team complete this aspect of their mission by analyzing the packet capture file collected on the desktop computer and provide detailed information about the environment. Your response should at least include the type of network traffic collected, details about the General’s laptop computer, details about the Scylla Codes server plus any other server available, and provide the names and contents of the files stored on the server the input passphrase is based on.

What are the validation code and input passphrase used by the General to generate the Scylla validation code for this week?
Solution 4 & 5

• Wireshark “Statistics” menu(s)
• Decrypt SSL/TLS
  – RSA keys list:
    10.10.20.94,443,http,E:\server.key
• IP’s, Hosts, User-Agent, Server, links, images, files (.zip), web pages...
• Export HTTP objects

6189db841f01413a05a53b7135137a17
Questions (w/o Google) 😊

I will use Google before asking dumb questions. I will use Google before asking dumb questions. I will use Google before asking dumb questions. I will use Google before asking dumb questions. I will use Google before asking dumb questions. I will use Google before asking dumb questions. www.mrburns.nl before asking dumb questions. I will use Google before asking dumb questions. I will use Google before asking dumb questions. I will use Google before asking dumb questions. I will use Google before asking dumb questions. I will use Google before asking dumb questions. I will use Google before asking dumb questions. I will use Google before asking dumb questions. I will use Google before asking dumb questions. I will use Google before asking dumb questions. I will use Google before asking dumb questions. I will use Google before asking dumb questions. I will use Google before asking dumb questions. I will use Google before asking dumb questions. I will use Google before asking dumb questions. I will use Google before asking dumb questions. I will use Google before asking dumb questions. I will use Google before asking dumb questions. I will use Google before asking dumb questions. I will use Google before asking dumb questions. I will use Google before asking dumb questions. I will use Google before asking dumb questions. I will use Google before asking dumb questions. I will use Google before asking dumb questions. I will use Google before asking dumb questions. I will use Google before asking dumb questions. I will use Google before asking dumb questions. I will use Google before asking dumb questions. I will use Google before asking dumb questions. I will use Google before asking dumb questions. I will use Google before asking dumb questions. I will use Google before asking dumb questions. I will use Google before asking dumb questions. I will use Google before asking dumb questions. I will use Google before asking dumb questions. I will use Google before asking dumb questions. I will use Google before asking dumb questions. I will use Google before asking dumb questions. I will use Google before asking dumb questions. I will use Google before asking dumb questions. I will use Google before asking dumb questions. I will use Google before asking dumb questions. I will use Google before asking dumb questions. I will use Google before asking dumb questions. I will use Google before asking dumb questions. I will use Google before asking dumb questions. I will use Google before asking dumb questions. I will use Google before asking dumb questions. I will use Google before asking dumb questions. I will use Google before asking dumb questions. I will use Google before asking dumb questions. I will use Google before asking dumb questions. I will use Google before asking dumb questions. I will use Google before asking dumb questions. I will use Google before asking dumb questions. I will use Google before asking dumb questions. I will use Google before asking dumb questions. I will use Google before asking dumb questions. I will use Google before asking dumb questions. I will use Google before asking dumb questions. I will use Google before asking dumb questions. I will use Google before asking dumb questions. I will use Google before asking dumb questions. I will use Google before asking dumb questions. I will use Google before asking dumb questions. I will use Google before asking dumb questions. I will use Google before asking dumb questions. I will use Google before asking dumb questions. I will use Google before asking dumb questions. I will use Google before asking dumb questions. I will use Google before asking dumb questions. I will use Google before asking dumb questions. I will use Google before asking dumb questions. I will use Google before asking dumb questions. I will use Google before asking dumb questions. I will use Google before asking dumb questions. I will use Google before asking dumb questions. I will use Google before asking dumb questions. I will use Google before asking dumb questions. I will use Google before asking dumb questions. I will use Google before asking dumb questions. I will use Google before asking dumb questions. I will use Google before asking dumb questions. I will use Google before asking dumb questions. I will use Google before asking dumb questions. I will use Google before asking dumb questions. I will use Google before asking dumb questions. I will use Google before asking dumb questions. I will use Google before asking dumb questions. I will use Google before asking dumb questions. I will use Google before asking dumb questions. I will use Google before asking dumb questions. I will use Google before asking dumb questions. I will use Google before asking dumb questions. I will use Google before asking dumb questions. I will use Google before asking dumb questions. I will use Google before asking dumb questions. I will use Google before asking dumb questions. I will use Google before asking dumb questions. I will use Google before asking dumb questions. I will use Google before asking dumb questions. I will use Google before asking dumb questions. I will use Google before asking dumb questions. I will use Google before asking dumb questions. I will use Google before asking dumb questions. I will use Google before asking dumb questions. I will use Google before asking dumb questions. I will use Google before asking dumb questions. I will use Google before asking dumb questions. I will use Google before asking dumb questions. I will use Google before asking dumb questions. I will use Google before asking dumb questions. I will use Google before asking dumb questions. I will use Google before asking dumb questions. I will use Google before asking dumb questions. I will use Google before asking dumb questions. I will use Google before asking dumb questions. I will use Google before asking dumb questions. I will use Google before asking dumb questions. I will use Google before asking dumb questions. I will use Google before asking dumb questions. I will use Google before asking dumb questions. I will use Google before asking dumb questions. I will use Google before asking dumb questions. I will use Google before asking dumb questions. I will use Google before asking dumb questions. I will use Google before asking dumb questions. I will use Google before asking dumb questions. I will use Google before asking dumb questions. I will use Google before asking dumb questions. I will use Google before asking dumb questions. I will use Google before asking dumb questions. I will use Google before asking dumb questions. I will use Google before asking dumb questions. I will use Google before asking dumb questions. I will use Google before asking dumb questions. I will use Google before asking dumb questions. I will use Google before asking dumb questions. I will use Google before asking dumb questions. I will use Google before asking dumb questions. I will use Google before asking dumb questions. I will use Google before asking dumb questions. I will use Google before asking dumb questions. I will use Google before asking dumb questions. I will use Google before asking dumb questions. I will use Google before asking dumb questions. I will use Google before asking dumb questions. I will use Google before asking dumb questions. I will use Google before asking dumb questions. I will use Google before asking dumb questions. I will use Google before asking dumb questions. I will use Google before asking dumb questions. I will use Google before asking dumb questions. I will use Google before asking dumb questions. I will use Google before asking dumb questions. I will use Google before asking dumb questions. I will use Google before asking dumb questions. I will use Google before asking dumb questions. I will use Google before asking dumb questions. I will use Google before asking dumb questions. I will use Google before asking dumb questions. I will use Google before asking dumb questions. I will use Google before asking dumb questions. I will use Google before asking dumb questions. I will use Google before asking dumb questions. I will use Google before asking dumb questions. I will use Google before asking dumb questions. I will use Google before asking dumb questions. I will use Google before asking dumb questions. I will use Google before asking dumb questions. I will use Google before asking dumb questions. I will use Google before asking dumb questions. I will use Google before asking dumb questions. I will use Google before asking dumb questions. I will use Google before asking dumb questions. I will use Google before asking dumb questions. I will use Google before asking dumb questions. I will use Google before asking dumb questions. I will use Google before asking dumb questions. I will use Google before asking dumb questions. I will use Google before asking dumb questions. I will use Google before asking dumb questions. I will use Google before asking dumb questions. I will use Google before asking dumb questions. I will use Google before asking dumb questions. I will use Google before asking dumb questions. I will use Google before asking dumb questions. I will use Google before asking dumb questions. I will use Google before asking dumb questions. I will use Google before asking dumb questions. I will use Google before asking dumb questions. I will use Google before asking dumb questions. I will use Google before asking dumb questions. I will use Google before asking dumb questions. I will use Google before asking dumb questions. I will use Google before asking dumb questions. I will use Google before asking dumb questions. I will use Google before asking dumb questions. I will use Google before asking dumb questions. I will use Google before asking dumb questions. I will use Google before asking dumb questions. I will use Google before asking dumb questions. I will use Google before asking dumb questions. I will use Google before asking dumb questions. I will use Google before asking dumb questions. I will use Google before asking dumb questions. I will use Google before asking dumb questions. I will use Google before asking dumb questions. I will use Google before asking dumb questions. I will use Google before asking dumb questions. I will use Google before asking dumb questions. I will use Google before asking dumb questions. I will use Google before asking dumb questions. I will use Google before asking dumb questions. I will use Google before asking dumb questions. I will use Google before asking dumb questions. I will use Google before asking dumb questions. I will use Google before asking dumb questions. I will use Google before asking dumb questions. I will use Google before asking dumb questions. I will use Google before asking dumb questions. I will use Google before asking dumb questions. I will use Google before asking dumb questions. I will use Google before asking dumb questions. I will use Google before asking dumb questions. I will use Google before asking dumb questions. I will use Google before asking dumb questions. I will use Google before asking dumb questions. I will use Google before asking dumb questions. I will use Google before asking dumb questions. I will use Google before asking dumb questions. I will use Google before asking dumb questions. I will use Google before asking dumb questions. I will use Google before asking dumb questions. I will use Google before asking dumb questions. I will use Google before asking dumb questions. I will use Google before asking dumb questions. I will use Google before asking dumb questions. I will use Google before asking dumb questions. I will use Google before asking dumb questions. I will use Google before asking dumb questions.
Contact Info

Taddong
www.taddong.com

RaDaJo
www.radajo.com

Raúl Siles
www.raulsiles.com
raul@raulsiles.com
References

  – http://www.ethicalhacker.net/content/view/268/2/
  – http://www.ethicalhacker.net/content/view/278/2/
• “Prison Break – Official Answers”. Raul Siles.
• Ed’s Hacking Challenges:
  – http://counterhack.net/Counter_Hack/Challenges.html
  – http://www.ethicalhacker.net/content/category/2/12/2/