

Prison Break - Breaking, Entering and Decoding

Hello! Ed Skoudis here... with a new challenge written by my friend, Raul Siles. You may remember Raul as the victor in such challenges as Lord of the Ring Zero and When Trinity Hacked the IRS D-Base. Raul has whipped up a doozy of a challenge here, all based on the TV show Prison Break. In this challenge, you'll work to thwart the sinister plans of The Company, an ominous, faceless group bent on world domination. To win, you'll have to do some network trouble shooting, plot a clever hack, and perform some file and packet analysis, all skills that are extremely useful for security pros. As always, we'll choose three winners: the best technical one, a creative entry that is also technically correct, and a random draw. Even if you don't know all the answers or can only guess, submit an entry with what you do have, and you'll be entered in that random draw. Winners will receive signed copies of my book, Counter Hack Reloaded. All entries are due by August 31, 2009. Have fun with Raul's challenge!

--Ed Skoudis

EthicalHacker.net Challenge Master

Author of Counter Hack Reloaded, Co-Founder, InGuardians, SANS Fellow

del.icio.us

[Discuss in Forums {mos_smf_discuss:July 2009 - Prison Break}](#)

PRISON BREAK – BREAKING, ENTERING & DECODING

By Raul Siles

www.raulsiles.com

July 2009

After their "Prison Break" (wikipedia entry) escape from the Fox River State Penitentiary, brothers Michael Scofield and Lincoln Burrows find themselves ready to achieve their lifelong goal: to unmask The Company, an almost unknown group of multinationals influencing world governments and whose power stretches all the way to the White House. The Company's main goal is to maintain control over the country's economy. The brother's mission is to obtain and decode Scylla, a portable data device containing critical and invaluable information about alternative forms of energy.

Breaking

Michael and his team were on a desperate mission to get a hold of Scylla. They were so close that they could almost smell it. Michael called his brother Lincoln, who was located in an abandoned warehouse in the port of Los Angeles used as an improvised operations center. Michael asked Lincoln to get help from Roland, the team computer hacker.

Michael explained that they were trying to get access to a data network, but their attempts to get in were not working. "We are in an office cubicle inside GATE's corporate headquarters building. GATE is a sales company, and the entry point to The Company headquarters. Both GATE and The Company share some core network and general infrastructure between buildings. After finding what looks like a VoIP phone on a desk, we unplugged it and connected our laptop to the same Ethernet cable."

"Wait a second." Lincoln transferred the cell phone to Roland, so he could gather all the details. Michael continued, "We have a standard x86-based laptop running Windows XP SP3. We see link-light on our laptop network card, and, although we can capture traffic using Wireshark, we cannot transmit any packets. Roland, we need to know what's going on right now. I cannot understand it, as I always use this laptop to capture traffic and get network access on other networks all the time. Based on our initial recon and intelligence gathering, GATE doesn't have any NAC/NAP systems or a similar advanced layer 2 network access protection mechanisms. It seems we are in a pretty standard switched network. But, we cannot send any data!"

Roland asked Michael about the laptop network card model, and requested a screenshot of a packet capture plus the output of a few commands: the network address details, a ping to the potential local router, and the local ARP cache.

"The network card is an Intel® PRO/100 VE Network Connection," Michael clarified. "We started with no IP address, just capturing traffic. As you can see in the packet dump, it seems there are multiple logical networks on the same physical segment, 192.168.1.0/24 and 172.29.0.0/16. I tried to get connectivity by requesting a DHCP address, as shown in frame 17, but I got no response."

[Click on picture for larger image](#)

Michael continued, "I also tried to set a fixed IP address of 192.168.1.17, which you can see in frame 23. But when I ping the default gateway, 192.168.1.1, I get no response... and the strange thing is that I cannot even get its MAC address in the local ARP cache. It seems like it's not sending ARP replies, although I can see other traffic coming from it, and it looks like it is talking to other systems on this same network."

[Click on picture for larger image](#)

Roland asked, "You have that Backtrack 4 pre-final VM that we include in all of our jumpkits, right?" Michael confirmed, "Sure do. We're always prepared for these missions."

"Hey, think about what is going on and what we can do to get network access. I'll call you in an hour," Michael rushed.

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?

Entering

A week later, Michael was at that same GATE cubicle talking to Sara, "Roland was instrumental in getting us this far. But that rat, the only techie we were assigned for this mission, betrayed us. He's out of the picture now. We need a replacement, and we need one ASAP!"

Michael quickly summed up the situation while showing the hacking laptop screen. "We were able to get physical access to the General's desktop computer inside The Company headquarters building for a couple of minutes. We plugged in an autorun-enabled USB thumb-drive prepared by Roland, and got a reverse shell connection back to us with high privileges on the box. In the process, we also copied a pair of hacking tools for further scanning and sniffing." Michael showed the screen of his MacBook hacking laptop running a couple of VMware Fusion guest machines, specifically Backtrack 4 Pre-final (BTv4) and Windows XP. "As you all can see, the terminal with the reverse connection from the desktop computer is running on BTv4."

...

```
[*] Transmitting intermediate stager for over-sized stage...(191 bytes)
```

```
[*] Sending stage (2650 bytes)
```

```
[*] Sleeping before handling stage...
```

```
[*] Uploading DLL (75787 bytes)...
```

```
[*] 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

```
meterpreter >
```

The following diagram illustrates the network topology they face:

"We had to break in to The Company physically, because their firewall doesn't allow any inbound traffic from GATE's network. Fortunately, General Jonathan Krantz does not like personal constraints, so there is no outbound filtering from the General's network," Michael explained. "Our goal now is to capture the remote traffic going through the General's network, in particular tomorrow at 09:00."

"Why?" asked Sucre, Michael's best friend and a trusted team member.

Michael took a deep breath to provide all the details, "Every day at 09:00, always right on time, the General connects to a server from his laptop, and enters a Scylla validation code. This code is valid for a week and is generated by a tool on his laptop, getting as input a passphrase that is based on some files stored on the server. The code unlocks Scylla and provides access to its information using the associated passphrase. After validating the code, the General uses it to check how many times and who has used the validation code during the previous 24 hours."

"As far as we know, the network traffic generated by the General's laptop can be captured from his desktop computer easily, given that a hub connects both." It looked like an easy deal. "However, there is a network IDS that monitors all traffic from remote networks to that network segment. If we need any additional tools, take into account that we can only upload and download a single file, one in each direction, and each file must be bigger than 524,288 bytes (half a Meg) and smaller than 10 Mbytes. Yeah, I know the upload constraint imposed by the IDS is strange, but the infrastructure is set up to detect small file transfers, even within the same TCP session. If we break the rules, our presence will be detected," Michael reiterated. "As you all know, it is crucial to avoid being detected. Also, we must avoid leaving any traces of our actions on the compromised systems. If we need any tool, tell Lincoln, and he will download it," Michael confirmed.

"Michael, have you tried the recently released sniffer module for Meterpreter?" Sucre suggested. Michael confirmed, "Yes, that is the first thing we tried. However, it failed. We don't know exactly why; perhaps it's due to some sort of host-based IPS running on the system and detecting the associated DLL. We definitely need to come up with another approach that does not involve that new module."

Challenge Question 2: What tool should Lincoln download, if any, to be able to capture traffic on the desktop computer?

Challenge Question 3: 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.

Decoding (the Scylla validation code)

As a result of the previous step, a packet capture file was collected at 09:00 the next day. This PCAP file is an extract of the full capture file, where non-relevant packets, such as ARP frames, have been removed.

The team was about to leave the building to analyze this network traffic capture in-depth, when Sara pointed out, "Michael, have you gathered the file from the desktop computer Roland got really excited about?" Michael realized he didn't, turned back, put his hand into the desk drawer, and grabbed a USB drive containing the following ZIP file. "Here it is! We don't know what exactly this is but Roland got crazy when he found it after searching around on the desktop computer file system. He mentioned something about a backup. Sara, you're right; this may help with our analysis."

Finally, Michael emphasized: "We need to be back as soon as we have any idea of what the contents of the traffic are and, even better, what the validation code and associated passphrase for this week are. I have a feeling we will need the passphrase used by the General to generate the unlock code required to get full access to Scylla."

Challenge Question 4: 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.

Challenge Question 5: What are the validation code and input passphrase used by the General to generate the Scylla validation code for this week?

BONUS QUESTION: Briefly describe your recommendations about how The Company could have detected and defended against the tactics you described in your answer to Question 3.

NOTE: Prison Break image obtained from http://www.shockya.com/news/wp-content/uploads/prison_break_ver4_poster.jpg

Submit your answers to skillz0709 (at) ethicalhacker.net with the subject line "Skillz Submission" by August 31, 2009 for a chance to win an autographed copy of Counter Hack Reloaded. The autograph will congratulate you on your prowess in mastering this challenge! We'll choose three winners, as usual, one in each of the three following categories:

- Best Technical Answer
- Best Creative Answer (that is also technically correct)
- Random Draw (Anyone can win, so send in a response, any response... it doesn't matter)

