

Prison Break - Breaking, Entering and Decoding - Answers and Winners

Hello, challenge fans! This is Raul Siles, author of the "Prison Break - Breaking, Entering and Decoding" EH-Net challenge, here to announce the answers and winners for this tough competition. BTW, the answers for this challenge were released to The Informer subscribers a few days ago. EH-Net had teamed with The Informer; in Johnny Long words, "(It is) a fund raising effort run by Hackers For Charity. It is designed to give subscribers a "backstage pass" to the world of Information Security. For \$54 per year, subscribers get early, exclusive access to all sorts of goodies donated by the top names in the INFOSEC world. The industry's most recognized names will post blog entries here before they even post them to their own sites." The EH-Net contribution will be the answers to the Skillz Challenges a few days before they are revealed on EH-Net.

The main goal of this challenge was to improve your pen-testing skills by devising an attack strategy to achieve multiple goals, such as dealing with a VoIP 802.1q (VLAN) scenario, squeeze the Windows and Metasploit meterpreter capabilities to sniff traffic, and decode and analyze HTTPS traffic. You became very creative, with different assumptions and answers, covering a variety of strategies and tools.

del.icio.us

Discuss in Forums {mos_smf_discuss:July 2009 - Prison Break}

And now for the details...

By Raul Siles

www.raulsiles.com

October 2009

Most submissions mentioned MAC filtering as the most probable reason for the lack of network connectivity in Question 1. Although it was an option, the scenario described a very common behavior on 802.1q-enabled (VLAN) switched networks, such as VoIP environments, especially when 802.1q header information is not available on the sniffer. Unfortunately, nobody paid attention to the specific network card model mentioned by Michael Scofield. This section tried to emphasize how important it is to have your pen-testing laptop and gear ready for action. Having VLAN support, for both capture and injection, is a must nowadays in switched network environments.

Let's jump into the core of the challenge, Questions 2 and 3. Network traffic can be captured on the target system

by using Windump (already uploaded; as some entries missed the fact that some tools were already available on the target system). However, the main mistake made by most submissions was not meeting its requirements: Winpcap, the packet capture library, has to be installed in order for this Windows sniffer to run. Some entries realized that and suggested the installation of the standard Winpcap library (which by the way met the file size constraints of the environment), but they didn't consider that it does not include silent install capabilities anymore. Surprisingly, only Eugenio Delfa mentioned MicroOLAP, the capture library used by the new Meterpreter sniffer module. Read the end of Answer 3 and Appendix A for more details about how HD Moore unconsciously affected the design of this challenge. BTW, nobody mentioned netmon as an option (http://www.inguardians.com/pubs/Vista_Wireless_Power_Tools-Wright.pdf).

During the step-by-step approach, a few submissions mixed up some of the Windump command line switches. The most common mistake was the assumption that Windump stops automatically when the `-C` option is used. Also, there was some confusion about other switches such as the units to `-C` (millions of bytes), the difference between `-L` and `-D`, `-s` and `-C`, etc. Robert Kesterson went very deep into the math about how much traffic to capture and how to setup Windump's options accordingly, paying attention to the minor details. Great work!

Most of the top entries opted to use a pure cmd.exe shell versus just the current meterpreter session. My main concern with that approach is that it will spawn a new cmd.exe process visible on the OS process table from Task Manager.

Dmitry questioned the USB hack due to the constraints imposed by Vista on the autorun capabilities. Good catch! Roland's USB hack can be a reality depending on the target system setup and the user response to Vista's autorun popup the first time an autorun-enabled device is connected. Additionally, while the challenge was taking place, Microsoft released (August 25, 2009) a new update to the AutoPlay functionality in Windows.

Regarding the last two Questions, 4 & 5, multiple answers identified the certificate and key on the backup.zip file, and therefore, decrypted the SSL/TLS traffic and gathered details about the target environment. Most people used Wireshark to decrypt the traffic, although a couple of people suggested the use of ssldump instead. Apart from the capture file, it is possible to gather details from the digital certificate, as Keith Lee did. Sandro Guly Zaccarini found a glitch in the Matrix on the web server timestamp header: Sat, 30 May 2009, while the traffic was captured on May 18, 2009. Excellent catch! ;)

In order to get the passphrase for the Scylla code used that week, Google was of great help for lot of people. Surprisingly, Kelvin Lomboy was even able to find the MD5 value through Google (from a website review site) and even mapped it to the passphrase. That info was not available in Google by the time I wrote the challenge and checked :) The purpose here was to give free rein to your imagination. Starting with the real evidence (the code), the top entries were capable of identifying the passphrase, identifying what the application does; this replicates crazy ideas web developers sometimes have.

The bonus question (not covered on purpose on the official answers) allowed people to point out multiple good defensive approaches to raise the bar, such as the usage of white-listing software to limit the executable files on the system, the importance of protecting your SSL keys, the availability of group policy settings to limit the USB hack and to lock down systems to prevent unauthorized software installs, how to limit reverse connections through proxies (not always effective) or at least detect them, the need to tune your IDS/IPS and firewall policy (especially using egress filtering), the importance of switches (with port security enabled) vs. hubs, host integrity checking tools to detect the installation of new software, and promiscuous mode detection capabilities. Of course, the best option is to avoid the attacker getting administrative-level access to the target system in the first place.

Finally, I enjoyed the creativity for the selection of the capture filenames, such as Eric Irvin “michael_jackson_thriller.flv” or rvs “gretchen.mp4” (plus his multiple Prison Break references). Definitely, rvs non-technical answer to question 5 was the funniest and most original one: "Since Tea-bag was around and they were very mindfull keys were given to different members such as Sucre, Linc, Michael, Sara and Mahone. They can't disclose it while the rat is around." LOL!

And now for the answers...

The “Prison Break – Breaking, Entering & Decoding” challenge answers are contained in a single PDF file (27 pages) plus three associated screencasts below.

BTv4 802.1q (VLAN) Setup

BTv4 802.1q (VLAN) setup from siles on Vimeo.

Metasploit Meterpreter Windump/Winpcap Sniffer

Metasploit meterpreter Windump/Winpcap sniffer from siles on Vimeo.

Metasploit Meterpreter Built-in Sniffer Module

Metasploit meterpreter built-in sniffer module from siles on Vimeo.

And now for the winners...

There was a tough competition between the two winners, but finally, Justin got the technical slot due to its awesome answer and the additional investigation on the web server images. Dmitry got the creative slot with his very solid answer, several interactions with the Windows firewall and UAC on the target system, and a custom Visual Basic script to decompress ZIP files natively. The main drawback with this excellent approach to decompress files is that it may display the window with the decompression progress in the target system desktop.

Technical Winner is Justin Kinney. See his entry [HERE](#).

Creative Winner is Dmitry Akselrod (Ketchup). His submission is [HERE](#).

And our Random Winner is Roger Crane.

Honorable mentions go to Keith Lee (the next entry near the winner positions), Robert Kesterson, Eugenio Delfa, and Kelvin Lomboy for their solid work, thorough responses, and analysis.

All three winners will receive signed copies of Ed Skoudis' book, Counter Hack Reloaded. Congrats and keep up the good work!