

## Serenity Hack - Answers & Winners

Before I thank Mr. Matthew Carpenter for his excellent work, let me thank the EH-Net members and readers for being patient. Between our regular work duties, a trip to Vegas for Black Hat and DefCon, and organizing our inaugural effort, ChicagoCon, we were all a little behind schedule. Now that Matt's first venture in challenge land is complete, he now has a good idea of what Ed and the Intelguardians crew go through on a regular basis. It's truly not an easy task to go through all of those entries and pick winners, but pick them he has.

And now for the bad news... Ed is one tired puppy. So we are going to take a break for a little while. Only a month or so to give Ed an opportunity to catch up on his own life. So I guess we'll all have to be on our best behavior as we give the Intelguardians a well deserved rest after more than a year of new challenges. But I'm not sure Ed knows how to do that as he asks (hint for the next challenge), "I'm scared Don, will I dream?"

Cheers to our host, Ed Skoudis of Intelguardians

& Author of Counter Hack Reloaded

[del.icio.us](#) [Slashdot](#) [It!](#)

[Discuss in Forums {mos\\_smf\\_discuss:June 07 - Serenity Hack}](#)

Sponsored by ChicagoCon 2007

Serenity Hack

Answers & Winners

By Matthew Carpenter

It was really hard to decide who won in each category for this one! So many correct answers, and even a handful of exceptional ones made it really tough! Exceptional bunch of submissions, and many first-time submitters, all of which were very good!

As a reminder, the questions to this challenge are as follows:

1. What tool did Kaylee use to remove the malware? How could she find the process, kill it and keep it from starting?
2. What was the code snippet most likely used for and what was the bot's control password?
3. Describe how you could discover the commands the bot would accept and their basic functionality?
4. (Extra Credit) What is the meaning of the password?

Our Creative Winner is...

The hardest part was deciding to award the creative to answer Andrew Laman, not Brian Finn.

Brian did an amazing job answering the questions using a discussion between the three dead dudes, Wash, Mr. Universe, and Shepherd Book, getting the answers correct (even getting closest of all on the Extra Credit) in such a creative fashion. Andrew's submission was both artistic and technically instructive, showing good "in-character" interactions between the crew members and very effectively integrating technical displays as would be seen when sitting at the console. His solution is here.

Our Technical Winner is...

The Technical winner was nearly as hard to judge, with many good answers...

However, Phillip Ames simply went above and beyond in all aspects. He skipped the easy (and very powerful) answer of using Process Explorer and Autoruns (and various other SysInternals tools) to eradicate the malware, and showed a little bit o' hard-core old-school, choosing the command-line SysInternals tools, and kindly including the links for us to get them (this is, after all, a teaching mechanism). I personally prefer to use the GUI tools, even though I'm a CLI-nut, because ProcessExplorer and Autoruns just spit out exceptionally well laid-out information. Also, the ability to mask signed-Microsoft binaries and look for unsigned programs quickly eliminates a lot of the noise.

Phillip then goes on to help the reader \*write\* an ASM tool to decipher the password and walks the reader through getting at it. The inclusion of GDB usage gets him extra points, although pragmatically it may have been more direct simply to make the call to glibc's printf(). Including the call to

printf() was far more advanced than required for this challenge (as was most of his response)

Phillip's third answer was just as good, wrapping up his win for the technical answer. See his solution is here.

What about that Extra Credit Question?

And what, you may ask, was the extra credit? So glad you asked...

The PAX released into the air on Miranda was supplemented by only allowing PAX TV the ability to broadcast there. Terraforming is an awfully long process with nothing to entertain but PAX TV, on which the steamiest show was Family Ties which featured a beautiful girl named Mallory Keaton. And, of course, since Nathan Fillion looks \*very much\* like Mallory's boyfriend on Family Ties, it's no wonder the Reavers chased them down... out of jealousy. (IMDB lists her real boyfriend as Nick Moore. Ed and I have been playing with a theory that Nathan Fillion used a different stage name back then, since IMDB doesn't list a picture... Sorry, no Google or IMDB points for that one, you had to watch the show to get the extra credit... old farts rule!)

#### Honorable Mention

I know this is not required, but there were several entries that deserved Honorable Mention. These are mostly in no particular order:

Brian Finn - exceptional discussion between Wash, Book, and Mr. Universe, I really enjoyed the bits about how much cooler it was to die by a sword than a "stupid beam". Many other great allusions to the movie which I loved. It hurt not to pick your answer. Very nice...

Greg Tiernan - told me the answer to number 2 and then told me I was mistaken and gave me a little challenge of my own!

Evan Anderson - Great hex2ascii.py tool! I had already written a similar tool, also in python. Nice...

Candid Wueest - Very good writeup, including a reference to delete-on-next-boot if necessary to remove the malware! You exhibit a good amount of malware-experience in your writing!

Benny Tsai - Excellent first answer, particularly indicating ProcessExplorer tricks like looking for packed images and processes/dlls with suspicious or no names/description/company name/version.

In the random draw category, the winner is:

Jonathan Austin

Congratulations to all and thanks again for all of your efforts. Each winner gets an autographed copy of one of Ed and Lenny' book, Malware: Fighting Malicious Code, congratulating you on your victory and amazing abilities!

For the picture above and some other cool Serenity and Firefly inspired backgrounds,

visit [The Sci-Fi Desktop Wallpaper Web](#).