Serenity Hack

Hello, Challenge fans! The Intelguardians crew is back this month with another challenge to tickle your fancy and bake your noodle. This month, Matthew Carpenter takes the helm, penning a challenge based on the movie Serenity. Shockingly, a recent SFX magazine poll found that Serenity had overcome Star Wars as the most popular Sci-Fi movie among its readers. It’s amazing what someone can accomplish with a bot-net voting in these on-line polls… Isn’t it, Matt? I hope you enjoy the challenge, as you help the Serenity crew thwart a nasty bot-net to escape the Reavers and the Alliance.

Remember, as always, we’ll award three prizes: One for the best technical answer, one for the most creative answer that is technically correct, and one awarded to a winner chosen randomly. Thus, if you can’t answer all of the questions, still send something in to qualify for the random winner. This month’s prize is my book, Malware: Fighting Malicious Code, which I authored with Lenny Zeltser.

--Ed Skoudis, Intelguardians

Author, Counter Hack Reloaded

del.icio.us Slashdot It!

Discuss in Forums {mos_smf_discuss:June 07 - Serenity Hack}

Sponsored by ChicagoCon 2007

Serenity Hack

By Matthew Carpenter

Wash: "I am a leaf on the wind! Watch how I soar..."

The battle stage is set! The "enlightened" Alliance army is eagerly awaiting the arrival of their prey, one small "Firefly"-class spaceship named "Serenity". Serenity is carrying two fugitives whom the Alliance must reclaim at all costs: a telepathic named River Tam and her big brother Simon, who gave up a promising career in medicine and spent his entire

fortune to break River out of an Alliance black-ops facility.

Malcom "Mal" Reynolds, captain of Serenity, and his crew are attempting to reach the broadcasting station of "Mr. Universe" who can take over screens in over 30 worlds and play videos on them. They have discovered a video indicating egregious Alliance behavior that resulted in the death of an entire planet and the creation of Reavers, each one a real-life version of the "boogieman", and your worst nightmare. Mal's former lieutenant Zoey, her husband and pilot Wash, gunslinger Jayne, and the ship's mechanic Kaylee are now fighting to take back their lives. The Alliance has destroyed any settlement known to be friendly toward Serenity's crew, and threatens to kill them all.

The Alliance army is waiting just inside of an ion cloud that surrounds Mr. Universe's planet, disrupting operation of any radar.

Meanwhile, Serenity is high-tailing it to Mr. Universe's planet not only because they want to alert the 'Verse to the Alliance's atrocities, but because they are being chased by an entire legion of Reavers who seem to think Serenity looks good enough to eat....

Serenity breaks through the ion cloud and continues directly toward the Alliance ships. The assassin assigned by the Alliance to capture the Tams chuckles as he comments to the captain of his ship, "They're not even changing course." Immediately following Serenity, the Reaver fleet comes through the ion cloud. Their fleet is the biggest and scariest collection of mishmash ships, most running without core containment (which would kill normal folk, just like in Star Trek), torn up and 'modified', just like the Reavers' faces.

Meanwhile, on board Serenity...

Mal: "Chicken's come home to roost."

Wash: "It's ok! I am a leaf on the wind!"

Mal: "What does that mean!?"

Wash: "It means I'm about to die a horrible and sudden death!"

Serenity begins to weave in and out of the madness as all-out war ensues between the Alliance fleet and the Reavers,

who would rather eat their victims alive. Alliance firepower meets Reaver improvisation as ships are destroyed in new and interesting ways. A strange beam appears just over Serenity's bough.

Mal: "Looks like we 'roused the interest of somebody..."

Zoey: "Must be Reaver. That beam ain't Alliance."

Mal: "Whatever it is, just don't get hit by..."

WHAM! The ship lurches as the beam collides with it.

Mal: "Aiishe!" <muttering curses in Mandarin> "I thought I just told you not to get hit by it! What in the 'Verse am I payin' you for, Wash!?"

Wash: "Uh.. could you wait to kill me until after we regain control of the ship?"

Zoey: "What's the matter honey?"

Mal: "Yeah, honey! What's the matter?"

Serenity begins a spiral toward the ground

Wash: "After that beam hit us, I lost all control."

<Mal hits the intercom button>

Mal: "Kaylee? What's going on?"

Kaylee: "It looks like the nav-computer may have a problem, Cap'n. After that last hit, CPU utilization went crazy and network traffic went ape. I think we may have one o' them malware programs running. It's on the bridge so I'll be there in a jiffy."

Kaylee arrives on the bridge with a USB thumb drive that she plugs into the nav-computer. Mal can just make out "SysIn..." on a label partly covered up with engine grime.

Kaylee: "Yep, it looks like we got malware. I think it's communicating with other ships over wireless! Why anyone installed Windows on the nav-computer is beyond me."

Mal snaps to attention at hearing that. Kaylee continues working while quietly continuing, "Everyone knows that everyone runs Linux for navigating ships! The software just works better. Never ride on a ship navved by Windows. They fall right outta the sky."

Mal: "Who installed gorramn Windows on my boat!?"

Jayne (who is a manly man): "Simmer down Mal! There was good reasons fer runnin' Windows!" <under his breath> "Latest version o' Donkey Kong don't run on nuthin' else."

Mal: "I thought we was real clear about bringin' Windows 'board my boat!"

Jayne: "Chill Mal, sheesh, you'd think we hurt yer ship."

Mal: "You did hurt my ship..." <more profanity in Mandarin> "...and to play some lousy games!? My boat don't crash. If she crashes, you crashed her!"

A very tense minute passes as the crew attempts to hold down their lunch, spinning out of control.

Kaylee: "Found it! Give me a second...."

<The ship slowly stops spinning and some control returns to the console.>

Kaylee: "There. It was a nasty mean piece of malware. Give me a minute and I'll tell you what it does."

Mal: "Why aren't we flyin' right yet?"

Wash: "It seems we've taken some huge damage during the fall."

Jayne: "Yeah, felt like people been usin' us for target shootin'!"

Kaylee, with Zoey looking over her shoulder, picks apart the malware.

Kaylee: "Here it is. Yep. Looks like it was an IRC bot that allowed someone to control the nav-computer from over the wireless net. Likely that beam was some sort of new attack vector er sumthin'."

<A pause in Kaylee's speaking>

Kaylee: "Oooh! Look at this, Cap'n!"

Zoey and Mal look over Kaylee's shoulders as she points out the following code. Wash, meanwhile, is attempting to "glide" Serenity down into a landing pattern.

```
MOV BL, 0x4d

MOV [EAX + 0x00], BL

MOV BL, 0x21

MOV [EAX + 0x0d], BL

MOV BL, 0x73

MOV [EAX + 0x09], BL

MOV BL, 0x61

MOV [EAX + 0x01], BL

MOV BL, 0x6f

MOV [EAX + 0x04], BL

MOV BL, 0x6c
```

MOV [EAX + 0x03], BL

MOV BL, 0x74

MOV [EAX + 0x0c], BL

MOV BL, 0x79

MOV [EAX + 0x06], BL

MOV BL, 0x72

MOV [EAX + 0x05], BL

MOV BL, 0x57

MOV [EAX + 0x07], BL

MOV BL, 0x61

MOV [EAX + 0x08], BL

MOV BL, 0x6c

MOV [EAX + 0x02], BL

```
MOV BL, 0x48

MOV [EAX + 0x0a], BL

MOV BL, 0x6f

MOV [EAX + 0x0b], BL
```

Mal: "Uh.. ok. Great then. Wash! How are we doin'?"

Wash: "Not sure, Mal."

Mal: "Give me worst case."

Wash (in perfect deadpan): "Oh God, oh God, we're all gonna die?"

Mal: "Fine. Just get us on the ground."

Wash: "Oh, that part will happen pretty definitely."

Mal looks up in awe to see Alliance ships crashing into each other. Kaylee giggles.

Zoey: "Cap'n, Kaylee's found a way to control a whole lotta the other ships up there. It seems we weren't the only ones hit by this malware. Lots of Alliance, too, and even some Reavers. Reavers controlling other Reaver's ships. Sounds

appropriate."

Mal: "Good. Keep 'em off our tail while we..."

CRASH! Serenity lands <ahem> safely except for busted landing gear, one lost engine, and a lot of peripheral damage (no, the printer didn't break), but all the crew seem to have survived.

Questions:

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 snippit 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?

Epilogue:

With the message broadcast to as many worlds as possible and the Alliance facing difficulties, Serenity's crew would be left alone for the time being. Mal is sitting in the pilot's seat, the crew having worked feverishly to repair the damaged Serenity, about to take off and get back to work.

Mal: "So, you gonna ride shotgun with me, help me fly?"

River: "That's the plan."

Mal: "Think you can work out...." <thunder of engines as River takes off>

Mal: "...ok. Clearly some aptitude... It ain't all buds and charts, little albatross. Know what the first rule of flying is? Well I suppose you do since you already know what I'm about to say."

River: "I do, but I like to hear you say it."

Mal: "Love.... You can learn all the math in the ‘Verse, but if you take a boat in the air that you don't love... shake you up just as sure as the turn of the worlds. Love keeps 'er in the air when she oughta fall down. Tells ya she's hurtin' 'fore she keels... Makes her a home."

River: "Storms getting worse..."

Mal: "We'll pass through it soon enough."

They pass through the clouds and into the sunshine, a beautiful picture by any measure. Serenity breaks orbit as some panel flies off and smacks the reader in the face with a loud <THWACK>.

Mal: "What was that!?"

Please read Matt's challenge, compose your answers, and e-mail them to skillz0607@ethicalhacker.net with the Subject: 'Skillz Submission' by July 23, 2007. By the end of July, Matt will choose three winners, one from each of these categories:

- Best technical answer
- Most creative and technically correct answer
- Random draw from all answers submitted, correct, incorrect, complete, partially complete, etc.

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.