

Brady Bunch Boondoggle

Challenge Extended until March 16!

Dearest challenge fans,

We've got a special treat for you this time around. Josh Wright of InGuardians has created a simply fantastic challenge based on the beloved 1970's TV show, The Brady Bunch. I grew up watching the Brady's crazy antics again and again in re-runs, and love how Josh has interweaved the show's lore throughout his challenge. But, even if you aren't into the Bradys, there is so much gee-whiz technical awesomeness here, you really should work through this one, my friends. Josh's funk is multi-layered, and there is a bunch to be learned by all of us from this one. Don't skip it or be intimidated by it... just start working your way through it, carefully and methodically, and enjoy all of the beautiful twists and turns Josh has crafted. I honestly think this is one of our best challenges yet!

As usual, we'll have three prizes: one for the best technical answer, one for the most creative answer that is technically correct, and one random draw winner. You must submit something to qualify for the random draw, so send in even partially completed answers. Winners will receive signed copies of my book, Counter Hack Reloaded. All entries are due by March 9, 2009 March 16, 2009.

--Ed Skoudis

Co-Founder, InGuardians, SANS Fellow, EthicalHacker.net Challenge Master, Author of Counter Hack Reloaded, Josh Wright Fan

del.icio.us

Discuss in Forums {mos_smf_discuss:Feb 2009 - Brady Bunch Boondoggle}

here

by Joshua Wright

A disaster is nearly averted when Greg and Peter disrupt a business meeting where Mike and Carol are attempting to woo new Spanish-speaking clients. Peter, having pretended to be Phil Packer, Greg's classmate and double-date partner, is recounting the evening's events after being caught taking their dates out to the same restaurant as Mike and Carol.

In his best disapproving tone, Mike asks Peter what valuable lessons he learned today.

"Boy, I really learned something," Peter says. "One, you act your age, and two, you don't try to be something you're not." Peter hesitates, deep in thought, adding "Three, you find out in advance what restaurant your Mom and Dad are going to, and go someplace else!"

"This isn't a joking matter, Peter," Mike replies. "Your antics tonight could have caused the firm to lose Mr. and Mrs. Calderone as new clients."

"Straight to your room, Peter," Carol instructs, pointing up the stairs.

"Yes, Mom," Peter bemoans, and heads to his room.

Banished to his room, Peter seeks consolation with his brothers Greg and Bobby, and sisters, Marcia, Jan and Cindy.

"Sorry to get you in such trouble Pete," Greg says.

"Yeah," adds Marcia. "We hope Dad doesn't lose his new clients."

"If he does, it could get him fired," Jan announces.

"And if Dad loses his job, then we'll have to sell the house," Cindy says.

"If Mom and Dad have to sell the house, we'll have to move," Peter says.

"Go to a new school," adds Bobby.

"Make new friends," adds Jan.

"But Jan," Marcia points out, "you don't have any friends."

"Wait, I got it," exclaims Peter, snapping his fingers. "We could use our hacking skills to give Dad a raise. That would solve all our problems!"

In agreement, the kids decide to break into the payroll system at Mike's office. Peter, obviously the smartest of the bunch, dolls out the responsibilities.

"Greg, we'll need a way to get access to the network in Dad's office. Can you take care of that?"

"Groovy Pete, I got just the thing," Greg says.

"Marcia, your job is to build a list of valid usernames we can target. Jan, you come up with a dictionary wordlist we can use. Bobby, we need you to do the dumpster diving to find a network diagram and anything about their system policies. Cindy..."

"Ahhh-chooo," Cindy sneezes.

"CINDY!" the gang choruses.

"Sorry, I have the sniffles." Cindy says.

Greg was the best choice for getting network access since he still worked for Mike's office doing office cleaning. Returning to the office, Greg plants a wireless access point inside Mike's office, then leaves for his date with Randi Peterson.

Meanwhile, Bobby has returned from a successful visit to Mike's office dumpster, producing a network diagram for Phillips Design, Inc. Greg identified the location of the planted access point in red:

Unfortunately, Bobby's pants became soiled in the search, so he decides to wash them himself to avoid suspicion. This plan backfires, however, with an unfortunate incident in using the washing machine.

The next day, Mike and Mr. Phillips, Mike's boss, have been discussing recent events in the office.

"Mike, as you know we have been going through our PCI 1.2 compliance assessment. This morning, our consulting firm performed the quarterly assessment of wireless devices and discovered no unauthorized devices, giving us a pass mark for section 11.1. They included this screen-shot in the report:

"That's great news Mr. Phillips."

"Thanks for your support Mike. To reward you, I'm assigning you to a new project where you'll design a building for a friend of the firm, a perfume heiress, who wants you to design her a new factory with some... unusual specifications."

On the day of the hack, Jan, Marcia, Greg and Peter drive to the parking lot of Mike's office. Using a high-gain directional antenna, Peter is able to get access to the office network through Greg's malicious access point. He then proceeds to enumerate the accessible targets.

Peter asks, "Marcia, what did you find out about valid usernames?"

"We definitely want to target Mr. Phillips account, "mphilips." He's the only one with access to the human resources system. Well, him, and George Glass." Marcia casts a glance at Jan.

"Sounds good. Jan, did you build that dictionary wordlist?"

"Uhh, well, I didn't get far," Jan laments.

"Show us what you have Jan," Peter insists.

"Nice work Jan," Marcia teases.

"Don't worry Jan, it doesn't look like that's going to work anyway. I've got a different idea," Peter says. Diligently tapping away, Peter works his hacking magic until he's satisfied. "Ok, Dad gets his raise, and we get to stay in the house. Now, Greg, do you think I have a shot at another date with Linda?"

Unknown to the kids, a stowaway was hidden in the trunk of the family station wagon. This stowaway had a grudge against the kids, and used his own antenna and wireless packet capture tools to record the entire hacking session.

The stowaway was cousin Oliver.

Making his way back to the Brady's house, Oliver sought out Mr. Brady to tattle on the kids.

"I'm glad you came to tell me Oliver, but remember, it's not nice to tattle," Mr. Brady admonished. "And, I'm an architect, and I don't know how to make heads or tails of this information. Who do you think can help us?"

You are called on to help analyze the packet capture information available here. Help Mr. Brady and Oliver figure out what kind of trouble the kids got into by answering the following questions:

1. What SSID is used for the kids' rogue AP?
2. How were the kids able to access Greg's rogue access point even though it was not detected during Mr. Phillips PCI compliance assessment?
3. How did Peter compromise the target system? (hint: no previously undisclosed exploits were used; remember, this was 1973, which would have made it a -12775-day exploit)

BONUS QUESTION: What steps did Peter take to change Mike's salary after compromising the target? What is Mike's new salary?

Hint: A tool that you may find useful is "wlan2eth", which converts a libpcap file from a wireless link type to an Ethernet link type. It is sometimes necessary to convert packet captures to an Ethernet link to work with applications that don't support the wireless link type. WLan2eth is available at <http://www.willhackforsushi.com/Offensive.html>.

Submit your answers to skillz0209@ethicalhacker.net with the subject line "Skillz Submission" by March 9, 2009 for a chance to win an autographed copy of my book, 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)