Skillz H@ck1ng Challenge Example 1: When Trinity Hacked the IRS D-Base

digg this storyDiscuss in Forums {mos_smf_discuss:Examples}by Ed Skoudis, May 2003

The Scene: A neo-gothic dance club playing pulsing music. Trinity, played by Carrie-Anne Moss, approaches Neo, played by Keanu Reeves. Trinity: "Hello Neo."
Neo: "How do you know that name?"
Trinity: "I know a lot about you."
Neo: "Who are you?"
Trinity : "My name's Trinity."
Neo: "Trinity...THE Trinity? The one who hacked the IRS D-Base?"
Trinity: "That was a long time ago."
Neo: "Jesus."
Trinity : "What?"
Neo: "I just thought...you were a guy."
Trinity: "Most guys do."- Dialogue from the movie, The Matrix

A long time ago, Nicholas Reagan Ipher was the chief of security at the IRS. Nick was flummoxed. An attacker had penetrated his computer system and rifled through several tax returns. The bad guy appeared to be looking for the postal addresses and phone numbers of several young, hot-shot computer programmers. Now, Nick was a pretty solid mainframe administrator, but he wasn't very well versed in TCP/IP or database administration. He was too proud to admit it, but he was out of his league with this type of hack.

In the aftermath of the attack, Nick found himself staring face to face with an agent assigned to this case of computer burglary.

"I don't need your help! I've got this case solved," lied Nick."Is that right?" asked the agent.

"Absolutely. Gloria, our grandmotherly database administrator, pulled the logs and gave me the user input submitted by the attacker. I asked Gloria for help in deciphering them, but she told me she was an Oracle person, not a SQL-Server expert. I had to go through the user input logs myself."

The agent was growing impatient. "So, what have you got?" he asked.

Nick answered, "Well, look at this first set of user input:irsfile.asp?username='test';+exec+master..xp_cmdshell+'ping+209.171.43.28';--

See the word 'ping' in there? Looks like a Chinese name to me. I think the Chinese Government was behind this thing."

"Oh really?" smiled the bemused agent.

Nick continued, "And this other user input is especially interesting:
irsfile.asp?username='test'+UNION+SELECT+name,1,'1',1,'1'+FROM+irs_dbase..syso bjects+WHERE+xtype+=+'U';--

See the word 'UNION'? Probably an inside job, perpetrated by one of our own workers in the employee union." Of course, Nick was making all of this up on the spot, trying to show the agent that he had the case under control. Nick had always fancied himself an actor.

"And this final set of user input gives us some especially useful information:
irsfile.asp?username='Trinity'+UNION+SELECT+phone_number+FROM+irs_dbase..accou
nt+WHERE+taxpayer_lastname+=+'Anderson';--

See, the attacker calls himself 'Trinity'. With a name like that, I'll bet this guy is either a religious extremist or a spy looking for nuclear secrets, or even both!" shouted Nick, impressed by his own logic.

The agent responded, "So, Mr. Ipher, you believe this crime was perpetrated by a religious group… that has infiltrated our employee union… looking for nuclear secrets… on behalf of the Chinese Government?"

"Sure do. I have a knack for this stuff," said Nick, quite happy with himself.

The agent shook his head in disgust as he left the room to find out what had really happened in this case. The agent ordered his men to keep a watchful eye over Nicholas Ipher. While Nick was indeed a fool, Agent Smith felt that his creative conniving just might be useful someday.

Questions:1) What type of attack had Trinity really launched against the IRS?2) What was the real purpose of the first set of user input, and how does it function?3) What was the real purpose of the second user input, and how does it function?4) What was the real purpose of the third user input, and how does it function?See the list of winners and their entries in the Skillz: Examples Forum.Originally Published at http://www.counterhack.net/when_trinity_hacked_the_irs_d-.html