***You've Been Hacked! A Valentine's Day Challenge* (or… *You've Got Sleepless Mail in Seattle*)**

By Ed Skoudis, Author of the book *Malware: Fighting Malicious Code*

Ed Skoudis has created a Valentine's Day Crack the Hacker Challenge *for you to solve. Inspired by cheesy romantic comedy movies, this challenge lets you analyze a computer attack, formulate answers to four questions, and get a chance to win a copy of Ed's* Counter Hack *book.   Submit your answers to febchallenge@counterhack.net by February 29, 2004, and Ed will select three winners from the best entries.*

Meg and Tom were in love… or at least a close facsimile thereof. For, you see, they had never actually met face to face. Theirs was a love that was entirely online, the world of the electron and the switch, the beauty of the baud.

Their romance began in a chat room a few years back while the two were discussing that sappy movie about rival bookstore owners falling in love via e-mail and Instant Messaging. Or was it the romantic comedy about the insomniac in Seattle? It doesn't really matter, as most of those movies have pretty much the same plot.

To communicate their love notes, Tom and Meg's messaging client of choice was AOL Instant Messenger™ (AIM). While shy in real life, they were completely open in their chats, sharing their most intimate secrets. Although Meg often found him lovable but goofy, Tom fancied himself a real techno-Casanova. He'd often type in classic love poems he had found on the Internet, pretending that he himself had written the odes to her. Unfortunately for Tom, Meg would simply Google up the verses to see their true author. On Valentine's Day, Tom sent this message to Meg:

> And yet, by heaven, I think my love as rare
> As any she belied with false compare.

Meg giggled and responded, "Oh, Tom, don't be so silly… You just swiped that from Shakespeare!"

To protect their secret communications, they both configured AIM with its strictest privacy settings. In fact, Meg, the more technically astute of the duo, went even further by installing a digital certificate in her chat client, hoping to encrypt their conversations. Tom did not have a certificate, but was very reassured to see the little lock icon next to Meg's name in his Buddy List when he chatted with her.

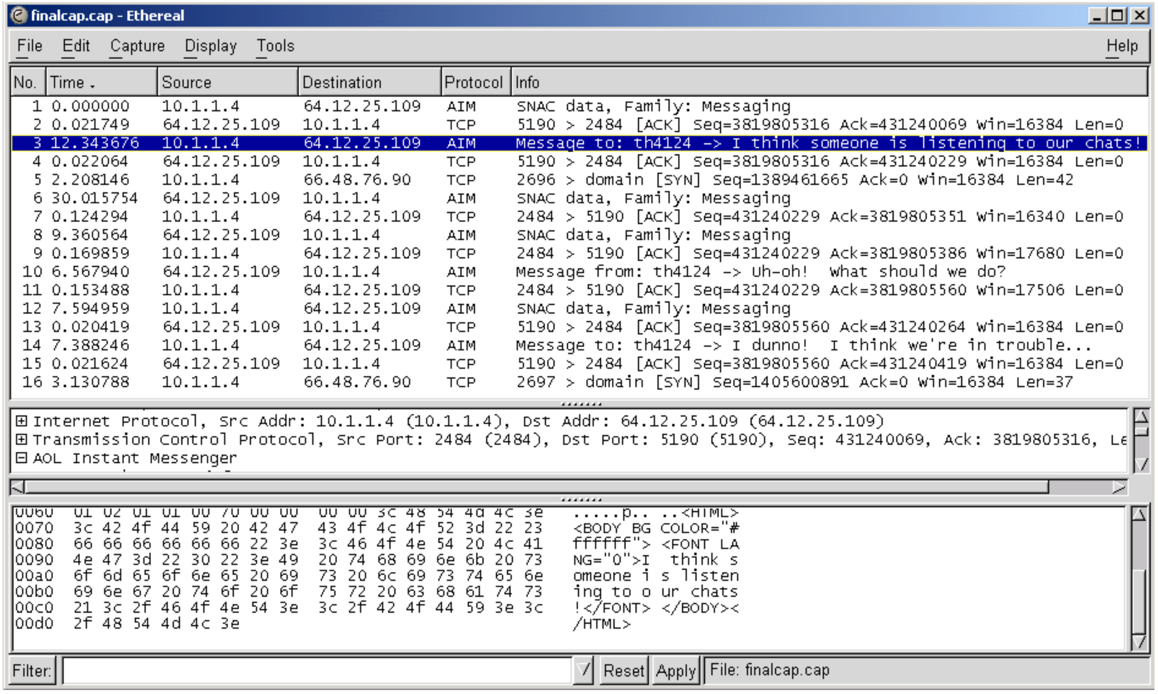
And suddenly, as with any contrived romance created merely as a plot device, their special relationship faced its biggest challenge yet: an interloper snooping on their chats. On the evening of Valentine's Day, Meg received this Instant Message from someone named Th3R3alShak3sp3ar3:

> Meg, I can't believe you wrote this line…

‘Oh, Tom, don’t be so silly… You just swiped that from Shakespeare!’
You should leave that dork and get a better man like me!

Meg’s eyes opened wide as she realized that an intruder had been able to see the contents of their chat sessions! Meg shuddered as she pondered the other, less innocuous chats that she and Tom had shared.

Later that evening, Meg decided to investigate what had happened. With only the chat program running on her Windows 2000 Professional laptop, Meg ran the Ethereal sniffer to look at the traffic leaving her machine. She signed into AIM and started a session with Tom. She sent him a message saying, “I think someone is listening to our chats!” While conversing with Tom, Meg observed this output from the sniffer:



```
No. Time .     Source        Destination   Protocol Info
  1 0.000000   10.1.1.4      64.12.25.109  AIM      SNAC data, Family: Messaging
  2 0.021749   64.12.25.109  10.1.1.4      TCP      5190 > 2484 [ACK] Seq=3819805316 Ack=431240069 Win=16384 Len=0
  3 12.343676  10.1.1.4      64.12.25.109  AIM      Message to: th4124 -> I think someone is listening to our chats!
  4 0.022064   64.12.25.109  10.1.1.4      TCP      5190 > 2484 [ACK] Seq=3819805316 Ack=431240229 Win=16384 Len=0
  5 2.208146   10.1.1.4      66.48.76.90   TCP      2696 > domain [SYN] Seq=1389461665 Ack=0 Win=16384 Len=42
  6 30.015754  64.12.25.109  10.1.1.4      AIM      SNAC data, Family: Messaging
  7 0.124294   10.1.1.4      64.12.25.109  TCP      2484 > 5190 [ACK] Seq=431240229 Ack=3819805351 Win=16340 Len=0
  8 9.360564   64.12.25.109  10.1.1.4      AIM      SNAC data, Family: Messaging
  9 0.169859   10.1.1.4      64.12.25.109  TCP      2484 > 5190 [ACK] Seq=431240229 Ack=3819805386 Win=17680 Len=0
 10 6.567940   64.12.25.109  10.1.1.4      AIM      Message from: th4124 -> Uh-oh!  What should we do?
 11 0.153488   10.1.1.4      64.12.25.109  TCP      2484 > 5190 [ACK] Seq=431240229 Ack=3819805560 Win=17506 Len=0
 12 7.594959   10.1.1.4      64.12.25.109  AIM      SNAC data, Family: Messaging
 13 0.020419   64.12.25.109  10.1.1.4      TCP      5190 > 2484 [ACK] Seq=3819805560 Ack=431240264 Win=16384 Len=0
 14 7.388246   10.1.1.4      64.12.25.109  AIM      Message to: th4124 -> I dunno!  I think we're in trouble...
 15 0.021624   64.12.25.109  10.1.1.4      TCP      5190 > 2484 [ACK] Seq=3819805560 Ack=431240419 Win=16384 Len=0
 16 3.130788   10.1.1.4      66.48.76.90   TCP      2697 > domain [SYN] Seq=1405600891 Ack=0 Win=16384 Len=37
```

```
⊞ Internet Protocol, Src Addr: 10.1.1.4 (10.1.1.4), Dst Addr: 64.12.25.109 (64.12.25.109)
⊞ Transmission Control Protocol, Src Port: 2484 (2484), Dst Port: 5190 (5190), Seq: 431240069, Ack: 3819805316, Le
⊟ AOL Instant Messenger
```

```
0060  01 02 01 01 00 70 00 00  00 00 3c 48 54 4d 4c 3e   .....p.. ..<HTML>
0070  3c 42 4f 44 59 20 42 47  43 4f 4c 4f 52 3d 22 23   <BODY BG COLOR="#
0080  66 66 66 66 66 66 22 3e  3c 46 4f 4e 54 20 4c 41   ffffff"> <FONT LA
0090  4e 47 3d 22 30 22 3e 49  20 74 68 69 6e 6b 20 73   NG="0">I  think s
00a0  6f 6d 65 6f 6e 65 20 69  73 20 6c 69 73 74 65 6e   omeone i s listen
00b0  69 6e 67 20 74 6f 20 6f  75 72 20 63 68 61 74 73   ing to o ur chats
00c0  21 3c 2f 46 4f 4e 54 3e  3c 2f 42 4f 44 59 3e 3c   !</FONT> </BODY><
00d0  2f 48 54 4d 4c 3e                                  /HTML>
```

Meg was completely shocked to see her AIM traffic in clear text! She had gone to all of the trouble to enable privacy and even installed a security certificate, yet her innermost secrets were being dribbled naked on the Internet. Feeling so violated, Meg and Tom both wondered whether they’d have to call off their relationship, forced to live aimlessly without each other.

Help our star-crossed lovers solve this dilemma and get a chance to win a copy of the book Counter Hack by answering the following questions:

1) Why hadn’t the privacy settings in Tom’s AIM client or the digital certificate in Meg’s client encrypted their connection?

2) How can Meg and Tom employ an encrypted protocol for communication using AIM? What other chat programs offer better security features?

3) Given the evidence presented in the narrative above, which system had the attacker most likely compromised: Meg's computer, Tom's computer, a machine on a network sitting between Meg and Tom, or AOL's messaging system itself? Why?

4) What steps should Meg and Tom take next to deal with the bad guy and eradicate him from their lives?

Remember, please send your answers to febchallenge@counterhack.net by February 29, 2004. The best three answers, as judged by Ed, will receive a copy of Ed's book, *Counter Hack: A Step-by-Step Guide to Computer Attacks and Defenses*. Also, all winning answers will be posted at www.counterhack.net, guaranteeing the winners a small amount of worldwide fame and a sure resume builder.

Finally, with Valentine's Day on its way, why not buy your sweetie the ultimate romantic gift – a copy of Ed's brand-new book, *Malware: Fighting Malicious Code*? Filled with tips for preventing, detecting, and responding to malicious software, this book is sure to add spark to your romance this Valentine's Day.