Assignment 2

William Mak

November 07 2014

1 Course Feedback

See Email

2 So, You Want to be a Hacker?

A If the marker had not turned off the default stack-protector and the the user enters a string over certain length then they would observe an error stating:

```
*** stack smashing detected ***: ./marker terminated
======= Backtrace: =========
```

etc...

B The string values I used were:

```
Name: aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaiz
Mark: hi
Rubric: hellooooooooo
```

The important part of the Name variable are the last two characters. This is because the 34^{th} character causes an overflow to occur. An overflow occurs because the way auth and name are stored causes auth to be 60 bytes away so we can just set it to 'iz'

C No. In this particular case it would have been protected. Because the user would write in the opposite direction from auth. But if 'char name[34]‘ came before ‘int auth=0‘ then it would still be possible.

3 Abuse of Set-UID File Permissions

I would add my public key to the users authorized keys located at $HOME/.ssh/authorized_keys. Unless they check this file regularly they will not be able to notice me doing this. And I would be able to ssh into their account any time I want.

4 Web Security

See attached files for answers to A, D, E

5 Wifi Router Vulnerabilities

A For this attack as an attacker I would first use db-ip.com to find all possible Canadian addresses if I knew about this vulnerability with Bell. Or if the screenshot is from his router then I would know that I can go on 76.65.189.43. I would then use netcat to send the following request. request(http://192.168.2.1/login?u=adminp=admin). The ones that do I would then send a new DNS server. With my new DNS server I would have the google ip redirect to my kim.dot.com.

B Sitting outside of the professor's condo the attacker would be able to send TCP packets to the router with a different source address. And because the attacker would be right next to the router their address would remain unchanged. Now the attacker can send the same requests as before and modify the DNS

C A hacker could very easily inject some malicious javascript into youvyou.com that would authenticate with the administrative account. And then aftewards modify the DNS server yet again to set google to be kim.dot.com

6 Denial of Service

A For this attack I would send a TCP packet into the network-connection with the reset flag set to one. This way the other computer will think that the connection is no longer working.

B It's well known that TCP does not have a builtin defense against spoofing of TCP resets(RST). For example in 2007 after Comcast decided to do this attack on their users a RFC was released detailing the failings of rfc https://tools.ietf.org/html/rfc4953

C Yes provided that they can monitor the network and determine things such as the sequence number. And that they can spoof their IP. If they cannot do either one of these things then it would not be possible for them to conduct a similar account

D No Subscribers will not be able to protect themselves even if they use SSL encrypted packets. This is because the attackers can target either client or server.