CSCD27 – Network Security

Shih-Chin Liang 11/28/2014

Question 1: Course Feedback

Send it to you via email.

Question 2: So, You Want to be a Hacker?

A) If the default stack-protector has not been turned off, then a warning message *** stack smashing detected ***: will appeared and the program will be terminated.
B)The inputs are as follows:
Name?
Shih-Chin Liang01234567890123456789012345678901234567890123456789012345678901234iz
62 characters in total
Mark?
99
Rubric?

Cool :)</br><object width="400" height="270" data="https://s3.yimg.com/os/en_us/Games/Yahoo/web_bouncing-balls/bouncing.swf"></object>
First, I tried to convert 31337 to Hexadecimal which is 7A69. Then, I convert the hex value back to string which is zi. Secondly, by trial and error I know the total space I have to input before I reach the memory space for auth is 60. I noticed the behaviour of the stack, they read my input in the opposite direction. So, the string that I would like to put into the memory space of auth should be iz. Due to the stack orientation and observation, that's why overflowing the variable name will overwrite the memory space of auth.
C)No, when the stack grows "down", the buffer overflow attack on the local variable can overwrite the return address. Consider the call stack orientation(http://en.wikipedia.org/wiki/File:Call_stack_layout.svg), if it oriented upward, the attacker can simply perform buffer overflow attack on the parameters to overwrite the return address. Thus, changing the stack orientation doesn't protect the stack-based buffer-overflow attacks. In addition, when I have the ability to overwrite the return address, I could have the ability to redirect to some other place on the stack and screwed things up.

Question 3: Abuse of Set-UID File Permissions

Yes, you should be able to do it. The commands you used are as follows
cp /bin/sh sh
chmod 4755 sh
mv sh /cmshome/liangs11/hacked
history -c

Assuming I have preset my desired folder in this case, hacked, to be writable and executable and liangs11 folder is executable(chmod go+x . in home folder) before I launch the attack. This will works because basically, I just copy the shell of the victim and set the uid bit of the copied shell. So, when I run the shell in the terminal, the Unix system will think the victim is running it due to the set uid bit. So, I have access to the victim's directories and all of his/her privileges. Due to the fact that I moved to my home directory, I could then revoke the write privilege such that no one other than me can delete the shell. The victim has no way of knowing it because the history -c options delete all the history of terminal in that terminal session. In addition, based on my testing, the total time spend for this attack is 43 seconds including setting the privilege of my home folder and the desired folder, hacked.

Question 4: Web Security

Partner: Carmen Flores(Utorid: floresc4) Sorry, I noticed I forget to add a bracket in line 12 for sql injection patch at the last minute. It's very late. I don't want to wake my partner up to re-submit. Thus, I'm submitting a new one with the extra bracket as diff.txt. Sorry, for the inconvenient.

Question 5: Web Security

A)The attacker can first go to the IP address-block lookup tools such as db-ip.com to find out Prof. Luddite's Ip address. Then, go on the Bell tech support website to figure out the factory default password for Bell's router which in this case is admin and admin. By assumption, the attacker is familiar with netcat. Thus, the attacker can use the tool to find the available/proper port number to get in which is 80. After going into the router the attacker can use netcat -k option to change the proxy setting such that redirection will happen or the attacker can change the DNS server from 8.8.8.8 to a malicious DNS the attacker has control of by `http://IPaddress/set?dns=whatever` provided in the question(after authentication) and performs the desired attack(redirection). Note: The attack is possible because the remote administration is enabled.

B)From the hint in FAQ, we can assume the default admin username-password is also valid for authenticating the Wifi access point(Bell123 as shown in fugure). Thus, by the fact that the attacker is outside of Prof. Luddite's house, the attacker can just connect to the network and the rest is the same as part A) except the way to connect the admin interface is now by `http://192.168.2.1/` not the IP address of the router.

C)reference : `crypto.stanford.edu/dns/dns-rebinding.pdf`

It could be done by DNS rebinding.

Since the attacker has full control of the website, therefore when the DNS query first request the website, the attacker could just send the malicious java script to instruct Prof. Luddite's browser to connect back to (youvyou.com). Then, bind the Ip address of the host name to Prof. Luddite's Ip address. When the script issues a second request to (youvyou.com), the server will reject it and force the browser to re-connect to the binded address which is itself. This will trick the browser to believe they all belong to the same origin because they share a host name. By same origin policy, this allows the attacker to read back the responses. From here on, the attacker can just do the same thing as part A).

Question 6: Denial of Service

A)The ISP can simply just forge the TCP reset bit and set it to 1. This will disrupt the TCP connection by fooling the receiving computer to end the TCP connection. In other words, this will kill the TCP connection immediately. In order for the forging to work, the ISP has to disguise itself to be one of the connection endpoints with proper IP and port numbers, and other relevant TCP header's values such as sequence number. Also, send it to the victim before the sender. This could easily been done because ISP distributed your traffic. They have this kind of access easily.
Interesting fact: The most famous ISP that use this type of attack is Comcast, and the software they used is from a software company from Canada called Sandvine.
B) According to rfc4953 from the IETF, there are five different solutions to deal with this type of attack in transport layer and network layer. However, all solutions required other extension such as MD5 or re-interpret/modified the use of different TCP's header value(s). In other word, the client and server have to come to an agreement on some policy. As a conclusion, there isn't a build-in TCP/IP protocol suite to prevent this type of attack.
C)Yes, the attacker must have computer access in the LAN to be able to monitor the traffic. As mentioned in A), the attacker must has access to the proper IP address and port number, and other relevant TCP header's values to perform TCP spoofing attack.
D)No, the reason being is that SSL is in application layer which is above transport layer. Although, the data is encrypted, but TCP headers aren't. The same attack can still applies.