**ECE404 Introduction to Computer Security**

**Purdue University**

Spring 2020: Midterm-III

**Instructions**

1. Please fill-in the details on this page.
2. This is an open book, open notes exam.
3. Unless otherwise instructed, justify your answers fully.
4. **Answers that are directly copied from the lecture notes will not be accepted**.
5. **Purdue Honor Pledge: As a Boilermaker pursuing academic excellence, I pledge to be honest and true in all that I do.**

**Name** : Dhruv Aggarwal

**Student ID** : 0028896590

**Email** : aggarw45@purdue.edu

**Signature** (For PDFs, use Adobe Reader’s Signature tool. For DOCX files,in Word go to Insert →Shapes→Lines →Scribble) :

# Problem 1 [11 points]

**Scenario:** Suppose you are a network security expert at a company that runs a popular ecommerce website on several servers. You are working from home on your laptop computer because of the social distancing regulations in place due to COVID-19, and your servers are located at an unknown location far away from your home. A colleague alerts you that some parts of the company’s website are taking a longer time to load than usual, and that one of the servers might be at risk of an attack. The IP address for that server is 128.46.144.100. Your goal is to figure out the cause of the slow-down as well as to resolve the problem with the server.

1. You have an account on that server with root privileges. After you enter into the server using ssh, the first thing you decide to check is if the server is under SYN-Flood attack. To do that you plan to use netstat utility. After you run the appropriate command, you get the following output:

tcp 0 0 128.46.144.100:80 140.53.84.24:609 SYN RECV

tcp 0 0 128.46.144.100:80 121.122.42.52:13 SYN RECV

tcp 0 0 128.46.144.100:80 129.12.192.16:48 SYN RECV

tcp 0 0 128.46.144.100:80 121.132.55.21:17 SYN RECV

tcp 0 0 128.46.144.100:80 121.152.212.2:17 SYN RECV

tcp 0 0 128.46.144.100:80 121.21.412.12:13 SYN RECV

tcp 0 0 128.46.144.100:80 124.18.11.10:317 SYN RECV

Observing the output above, you conclude that the server is definitely under a SYN-Flood attack. What would prompt you to reach that conclusion? **[3 pts]**

The reason why I would get to that conclusion is because there is a lot of SYN requests but in a normal three-way handshake there has to be an ACK packet sent which is clearly not being sent.

1. You attempt to thwart the attack by blocking the IP addresses mentioned in the 5th column (i.e., the column that shows the IP addresses of the remote hosts) of the output shown in part (a). But this is not a good strategy. Why? **[3 pts]**

It is not a good strategy because if the forged IP addresses are legitimate, then packet filtering would amount to a DOS to the legitimate users at that server/IP addresses. Example is Amazon. If someone at Amazon blocked Purdue’s IP addresses then no one would be able to reach Amazon at Purdue.

1. You then decide to limit the request for a new connection to one per second. What command would you use to accomplish this? [Hint: use a packet filtering firewall] **[5 pts]**

Sudo iptables -A FORWARD -p tcp –syn -m limit –limit 1/s -j ACCEPT

# Problem 2 [12 points]

1. The DNS hierarchy includes root servers, gTLD servers, and ccTLD servers. What role do each of these servers play when a client first contacts the system? **[5 points]**

The main purpose of the root servers is that it points to the gTLD and the ccTLD server. It is at the top of the hierarchy. When a query is sent to one of the root servers it responds back with the IP address of either of the gTLD server and ccTLD server. The gTLD server is more generic and can hold .com, .edu, .gov etc. The ccTLD servers are more country-specific domains such as .in, .jp etc.

1. What is DNS cache poisoning? How is it done? What aspect of DNS makes it a difficult attack to pull off? **[7 points]**

DNS cache poisoning is the act of entering in the cache a fake IP addresses so that it returns an incorrect response and gets redirected to wrong websites. The way you would do it is first sending out a DNS query with a transaction ID number. If the nameserver to which the DNS query is sent does not contain the IP address it will move forward to query something higher up in the nameserver tree otherwise it returns with a transaction ID number of its own. If the IP addresses and the ID from the remote host are correct the query is legitimate. What makes the DNS difficult is that the transaction ID integer that is 16 bit is randomly generated.

# Problem 3 [9 points]

1. Let’s say I have five computers in a LAN functioning as a server and I want to designate one computer for protecting the LAN with a firewall that will direct traffic destined for port 22 to the other 4 machines . What is the general term for this process? What would be the iptables command for accomplishing this if the IP address of the firewall computer is 128.210.107.65 and the other 4 machines have local IP addresses 10.0.0.1-10.0.0.4? **[5 points]**

The general term for this process is called port forwarding. The iptables command for accomplishing this will be the following.

Iptables -t nat -A PREROUTING -p tcp -d 128.210.107.65 \ -dport 22 -j DNAT –to-destination 10.0.0.1-10.0.0.4

1. Why does the usage of salt in a password hashing scheme make it difficult for an attacker to mount a dictionary attack, even if the attacker knew the salts that were used? **[4 points]**

A salt is a random bit pattern that gets combined with the actual password before it is hashed using a hashing algorithm. The reason that this makes it difficult to mount a dictionary attack is for a few reasons. The first and simple one is that it will make it less likely that any two usernames or any two of whatever you are hashing, have the same password hash associated with them. Another reason is that if you use a different salt for each different value(username) it would make it impossible for any attacker to use a precomputed table to infer the passwords from their hash value. And Lastly I think that using a salt creates way too many possibilities for a password and since a dictionary attack is brute force it will eventually run out of space to compute those values/passwords.

# Problem 4 [16 points]

1. Let’s say you are purchasing something on eBay.com. What role does TLS/SSL play in ensuring this transaction is secure? **[4 points]**

The role it plays is by using certificate authroties. It allows for an authentication between the server and client. This verification is the role that the TLS/SSL play because once they authenticate that it a actual relation then, EBAY will get your card details and be able to process your purchase.

1. Explain at a high level what is accomplished at each phase of an SSL Handshake between two parties for the SSL Handshake protocol. By high level, we mean enough to understand what the two parties are doing in each phase without the need to be precise about the parameters they exchange. **[7 points]**

There are 4 phases of the SSL handshake protocol. The first phase is when the client send the server a client\_hello message to start a relationship between the two. The next phase is when the server has to send the server certificate to the client. This is to validate the server public key. This is called the server\_hello\_done message and usually contains the message along with a ceritificate\_request message to validate the client. The next phase is when the client sends the certificate(if asked for). The client then sends the server a client\_key\_exhchange message that contains a secret session key that has the servers public key encrypted. Then the client sends the server the certificate\_verify message. The last part of the handshaking is when the client sends the server a change\_cipher\_spec message that its copying the one spec into the next. The client sends the server a finished message and that completes the SSL handshake between two parties.

3. Explain the relationship between a socksified client, a SOCKS server, and the outside internet (i.e. how does each of these three entities interact with each other?) **[5 points]**

The first part to this relationship is that the socksified client opens a TCP connection with the socks server’s port. The client then sends a packet suggestion of authentication. If the socks proxy server accepts the packet it responds. Then the client sends the socks proxy server a request to communicate with the outside internet and at what port. If everything is successful then the proxy server will connect to a remote outside internet server.

# Problem 5 [5 points]

1. Assume that a host A decides to use the TOR protocol to send a message anonymously to host E on the internet. The TOR protocol constructs the following circuit from host A to host E:

A → B → C → D → E

Here, nodes B, C, and D are the onion routers (ORs) of the TOR overlay.

While sending messages to nodes in the circuit, each node does not need to share its public RSA key with subsequent nodes in the circuit (e.g. node A does not share its public RSA key with any other nodes, B does not share its key with nodes C, D, and E, node C does not share its key with nodes D and E, etc.).

Explain what makes it possible for TOR to securely transmit messages without a node needing to share its public RSA key with subsequent nodes in the circuit. **[5 points]**

What makes it possible to securely transmit messages without a node needing to share its public RSA key is because of the way this protocol works. When the data is transmitted from A to B it gets encrypted by B’s RSA public key. Now when the data gets moved from A to C it gets encrypted by C’s RSA public key. When B receives that torpacket it generates a control torpacket and since it was meant for node c it is encrypted by c’s public key. The torpacket sent by B to C uses a random number as the circID and now A does not need to know this identifier. Now A and c and calculate the secret key that B is not allowed to c. You use control and relay torpackets to do this.

# Problem 6 [20 points]

1. Is the following statement True or False? “In a C program, if I use a malloc call in a declaration of a buffer, that buffer cannot overflow.” Please justify your answer. **[4 points]**

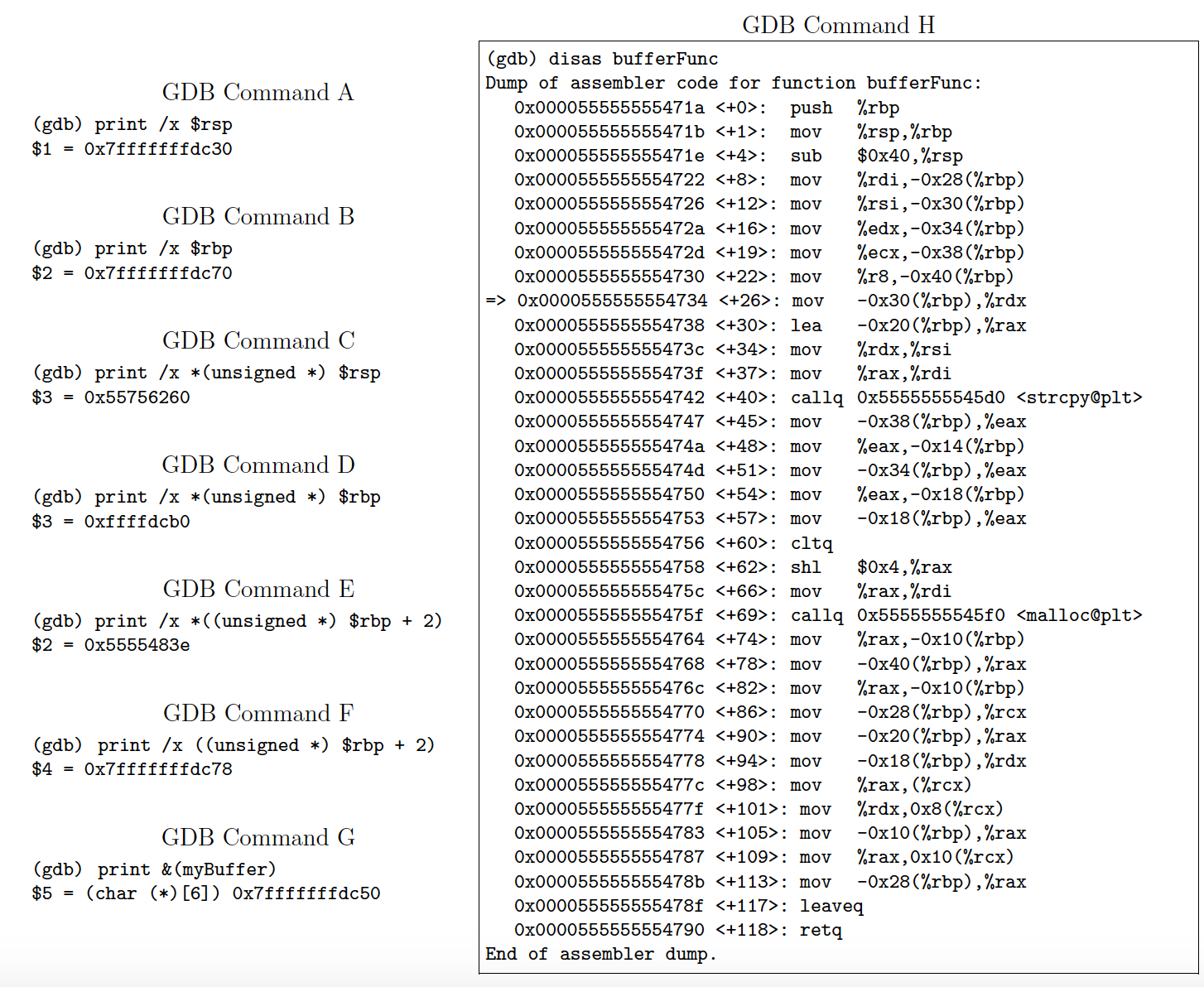
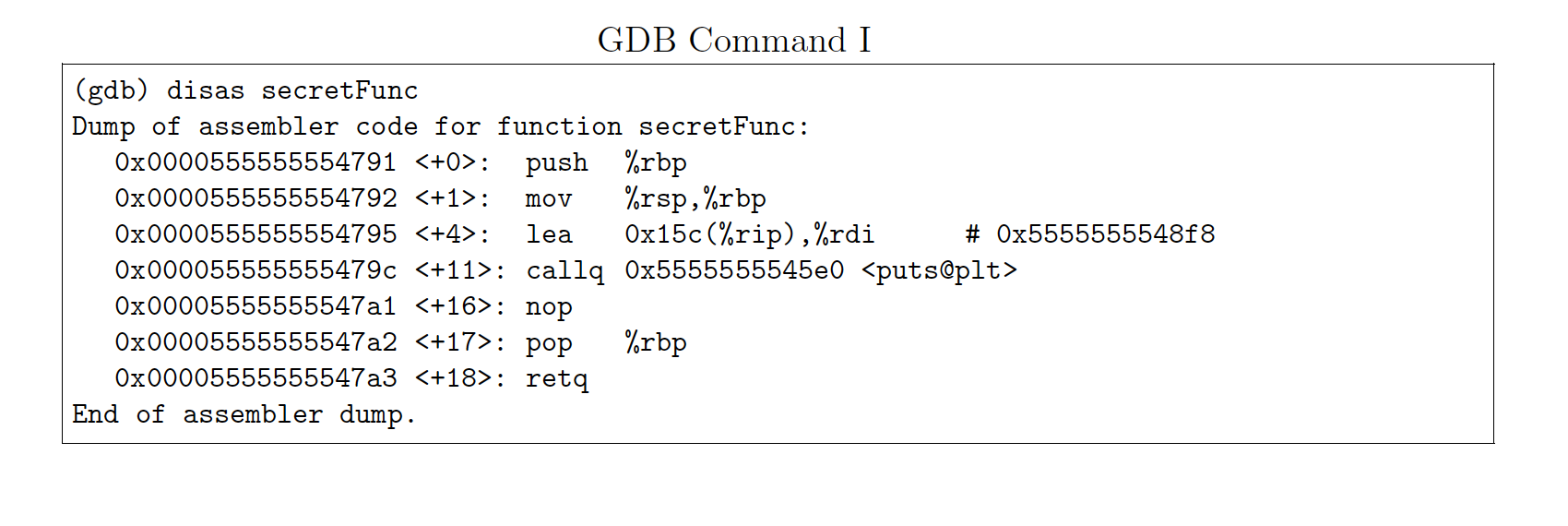
This statement is false. This is because malloc is done in the heap. In the heap when the size of the information exceeds the memory allocated for the object at that location you will have a buffer overflow. Now while this is harder to do in the heap then the stack it is possible.

1. Let’s say a canary with a value of ***0xc69b05c8*** is used to detect if a buffer overflow attack has occurred in the execution of a program. Would an attacker still be able to mount a buffer overflow attack despite the presence of this canary? Explain why or why not. **[4 points]**

I think an attacker would still be able to mount a buffer overflow attack despite the presence of this canary because this specific hex value doesn’t have a null byte. Since it doesn’t have a null byte when trying to use strcpy, there is no null byte and it will be able to use gets to get past the new line character. Therefore a buffer overflow attack would still be possible and this canary would not be able to terminate the execution of the program.

1. Let’s say there is a C program with a buffer overflow vulnerability in the function *bufferFunc(...)* with the variable *char myBuffer[6]* due to the use of the *strcpy(...)* function to copy user input into *myBuffer*. An attacker wants to exploit this vulnerability to execute the function *secretFunc(...)*. In order to craft a string to mount the attack, the program is run with **gdb**. On the following pages are some **gdb** commands along with their respective outputs at a breakpoint right before the vulnerability (you are allowed to use a Hexadecimal to Decimal converter for the addresses). Using this information, create a string that could potentially be used to enter *secretFunc(...).* Be sure to explain how you came up with the string and refer to the GDB commands that helped you craft the string. **[12 points]**

I think that the string is “A” \* 24\x91\x47\x55\x55. I think this is it because in the gdb commands we look at the first push address of the secretFunc. I used 24 A’s to pad because we want to fix the first 24 characters. The last 4 bytes come from the first address of the secret function. We want to target that x91\x47\x55\x55 for the overflow. The only gdb command I really used was I which was the dias secretFunc.

****

# C:\Users\Constantine\Downloads\93511610_2647694092110763_2796084109821083648_n.png

# 

# Problem 7 [18 points]

1. Why is it important for a virus to check if a file has been already infected? **[4 points]**

It is important for a virus to check if a file has already been infected because if they don’t check and there is already a virus then the size of the infected file could grow and become huge. The way they check is by looking at a signature which is usually left by the virus.

1. Why are IRC servers chosen by botnet creators for communication between servers and bots? **[3 points]**

IRC servers are chosen by botnet creators for communications between servers and bots because it is likely to go undetected if they use the C&C server. This because the C&C server uses a standard protocol and it becomes difficult for packet sniffers to figure out there is something wrong in the network. IRC is the protocol they chose based on the mode of communication.

1. What is a content delivery network (CDN)? What makes it secure against DDoS attacks? **[6 points]**

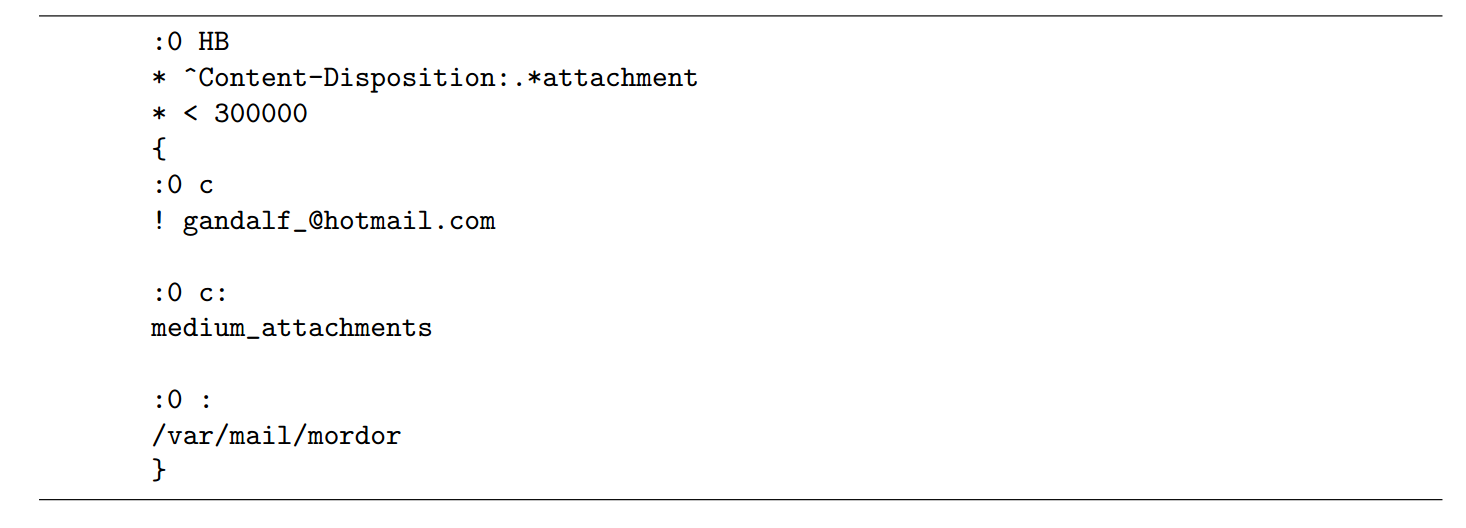
A content delivery network is a network of customer facing proxy servers that deliver the content which is used for load balancing on an enterprise level. The reason they are secure against DDoS attacks is because they isolate the origin servers. The origin servers have their own content to the CDN proxy servers through different tunnels in which DDoS attacks became a lot harder.

1. Let’s say an Autonomous System (AS) falls victim to a DDoS attack. In relation to its network neighborhood, explain the actions the AS would take to mitigate this attack.

**[5 points]**

The actions that the AS would do is to redirect the traffic. So the AS would instantly change and reroute the traffic to something longer and by then there can be filters applied so that the attack is mitigated.

|  |  |
| --- | --- |
| **Problem 8** | **[9 points]** |
| 1. What does the following spam filter recipe do? | **[5 points]** |



It is a non-delivering recipe. The first line means that the recipe will be applied to both the head and the body. The next line is checking to see if there is an attachment. The \* < 300000 checks that the total length of the email is less than 300000 bytes. The :O c means that a copy of this email will be processed by this recipe while the original email will be processed by the remaining recipes. The ! gandalf\_hotmail.com line means to forward the email to that email address. The next line means to copy all messages into a folder called medium attachments and the last line means to hold all incoming mail until this is processed in a folder called mordor. So to summarize it checks if there is an attachment and makes sure that the email is less than 300000 bytes and then sends a copy to Gandalf and sends the content into a local folder called medium attachments and then holds incoming mail in a mordor folder until every recipe is processed.

2. Betty Bitdiddle is upset with her friend Ben Bitdiddle because she says he sent her an email message with a virus. This email was in fact not sent by Ben but by an enemy of Betty. If a friend of Betty and Ben had access to all parts of the email, what information could their friend use to clear Ben’s name and show he didn’t actually send it? **[4 points]**

The way he can try to clear ben’s name is by you look at a few things. In the email you can look at the return path and then the received line will have an ip address. You can go on an iptracker to see where that IP is. Another thing you can do is in the Received: from line you can see the IP address there and if it’s the same IP as where the domain directly received the email but 2 different locations you also know it was a spam email.

## (If you need extra space, you can use this page)