IERG4130 Assignment 3

LAU Long Ching
SID: 1155127347

03/05/2021

Question 1

1)

No, the data from the two client programs will not be mixed on the server side. A TCP packet contains information including the source IP and port, as well as the destination IP and the destination port. The two programs would have different source port since they are assigned by the OS randomly.

2)

Yes, the data from these two client programs will be mixed together on the server side. UDP connections contain only destination ip and port, but not the source one.

Question 2

1)

No, the victim server does not freeze as SYN flooding attacks do not consume all the computation power of victim machine. It fills up the TCB queue so that other machine cannot connect to the victim.

2)

SYN flood attacks do not require the attacker receive a reply from the victim, so there is no need for the attacker to use its real source address. Spoofing the source address both improves anonymity by making it harder to track down the attacker, as well as making it more difficult for the victim to filter traffic based on IP.

3)

if the spoofed source IP address does belong to a running computer, it will receive the SYN packet with acknowledgement from the server. However, since the machine has never initialized the connection request, it knows that something is wrong, so it will reply with a RST packet and close the connection.

4)

No, sending spoofed TCP packet requires a call of the socket () function to create a socket and this require root privilege. We have also tried this in the lab assignment.

Question 3

Assuming there is no protection by the SQL server, We can set `$eid` as `' or 1=1--` and `$passwd` to be anything, so that the query becomes

```
SELECT * FROM employee WHERE eid = '' OR 1=1--  AND password = '';
```

The comment sequence (–) causes the remainder of the query to be ignored, so the statement is equivalent to

```
SELECT * FROM employee WHERE eid = '' OR 1=1;
```

and the login would be bypassed.

Question 4

1)

The first possible attack is DNS spoofing, in which the attacker compromise a DNS server and get the legitimate website to be redirected to a malicious one.

The attacker may also consider cache poisoning, in which physically taking over the DNS settings of the server is not neccessary. Since DNS servers, routers and computers cache DNS records, attackers can insert a forged DNS entry containing an alternative IP destination for the same domain name. The DNS server resolves the domain to the spoofed website, until the cache is refreshed.

2)

Shutdown unneeded DNS resolvers and place them behind a firewall, restrict access to a name server, protect against cache poisoning by using a random source port, randomize query ID, and randomize upper/lower case in domain names. DNS server admins should restrict zone transfers, which is a partial copy of your DNS records. They contain information that is valuable to attackers.

Question 5

1)

This is in fact similar to a task we have done in the lab assignments in which we made the victims modify their profiles without their consent. Cross-Site Request Forgery (CSRF) is an attack that forces an end user to execute unwanted actions on a web application in which they're currently authenticated. If a web server has an XSS vulnerability exposed. The attacker can first inject a malicious script that contains HTTP request to the web server, and then trick the victim into visiting the website that was injected with the payload, either by social engineering or just let them randomly step in.

2)

Confidentiality: The system should ensure that only those who are authorized have access to specific assets and that those who are unauthorized are actively prevented from obtaining access. The CSRF attack allows adversary to access information by sending HTTP requests on behalf of a victim user.

Integrity: The system should ensure that data has not been tampered with and it goes hand in hand with the concept of non-repudiation, in which every action leaves traces and evidence. The CSRF attack allows adversary to send instruction on behalf of the victim, therefore it is difficult to trace who made such instructions.

Availability: The CSRF attack usually do not interfere the availability of server, but if the victim, unfortunately, is the administrator of the web server, then of course the attacker would be able to take down something and make it unavailable.

Question 6

The table contains 2 IP addresses sharing a same MAC address. It is a trace of an ARP attack.

Question 7

TCP session hacking, ARP spoofing, wire-tapping.

Question 8

Not at all. HTTPS will prevent sniffing attacks only. With SSL enabled, there are still chances of session hijacking if there is an XSS vulnerability, or if the attacker has access to the victim's filesystem, the valid session cookie could be retrieved.