Assignment 5 – ECE 1155

Rayan Hassan – 4511021

Part 1

Question 1

An example of a threat can cannot be resolved by cryptographic is man in the middle attack. Because it is intercepts and modifies the data that is being communicated. It doesn't matter if it's encrypted or not. The attacker can launch DNS spoofing, therefore sending SYN packets to fill the TCP queue.

Question 2

The DNS server (Domain Name System) basically finds the IP address based off of the URL. DNS spoofing is when an attacker impersonates a DNS server and sends the IP address to the user before the actual/legitimate one does.

Question 3

Transport layer takes care of ensuring reliable transfer of data from the source to the destination. It uses IP address and port numbers to communicate with each user end. Also, it uses segmentation, where the data is basically divided into 2 segments: a header that contains all the necessary information like sequence and acknowledgment numbers, and the data. It also establishes connection between the two ends.

Question 4

(i) Port numbers are used for multiplexing. In fact, when multiple internet applications are using the same network interface card. In order to differentiate between each, they are assigned different port numbers.

(ii) IP addresses are unique for every device, in order to recognize them over the internet and contact them. So they are used to connect devices that send and receive information.

(iii) Data is split into packets, to specify the order of these packet, we use a sequence number. The initial sequence number is randomly generated, and then the order just follows by order.

Question 5

SYN flooding attack is when an attacker sends multiple SYN packets to fill the TCP queue. Basically, when a client sends a SYN packet to the server, it allocates some memory for the connection (half-open connection). So when the attacker does that, there will be no space to store the TCP for any new half-open connection (cannot accept any new SYN packet). So this will cause denial of service, the attacker uses random source IP addresses. We can remedy that by using a keyed hash from the information in the packet using a secret key only known by server. The hash (H) is sent to the client as initial SYN packet, it's called SYN cookie. If the client is legitimate, it will send back H+1. The server will check if the acknowledgment is valid or not. That way, the information about the packet is not stored in the queue (so it's not necessary here), which avoid flooding.

Question 6

HTTP is at the application layer, TCP is at the transport layer. HTTP is a protocol that decides what should be included in the transmitted packets from source to destination depending on client's requests (like if visiting a website). HTTPS uses transport layer security (TLS) which sits between the application layer and the transport layer. It basically deals with unprotected data, and handled encryption, decryption and integrity checks. The channel has the 3 properties: Confidentiality, Integrity and Authentication. So HTTPS is more trusted than HTTP.

Question 7

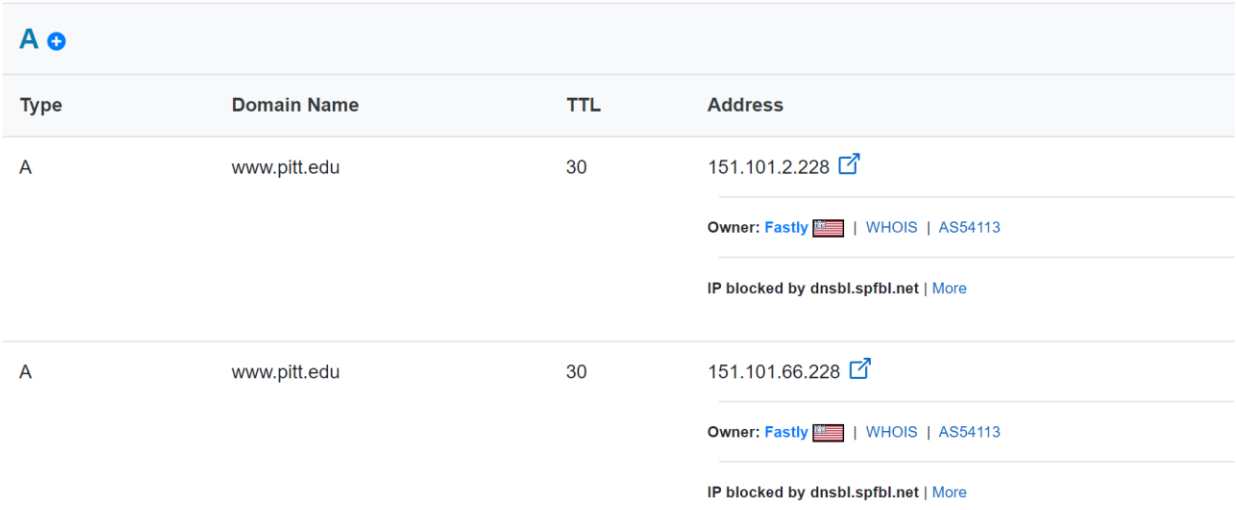
TCP handshake is used to establish the connection between the client and the server. The client sends a SYN packet, the server responds with a SYN-ACK one. The client receives it and sends an acknowledgment packet again ACK to conclude the handshake. TLS handshake on the other hand is used to agree upon cryptographic parameters that need to be used. It happens after the TCP handshake.

Question 8

TLS handshake basically determines the cryptographic method to be uses, a shared secret key used for symmetric encryption and another one used to form a method authentication code (HMAC).

Question 9

The IP address provided in the given question didn't work. I looked up my DNS lookup tool and found out that the IP address for www.pitt.edu is actually 151.101.2.228, as show in the picture below:



A

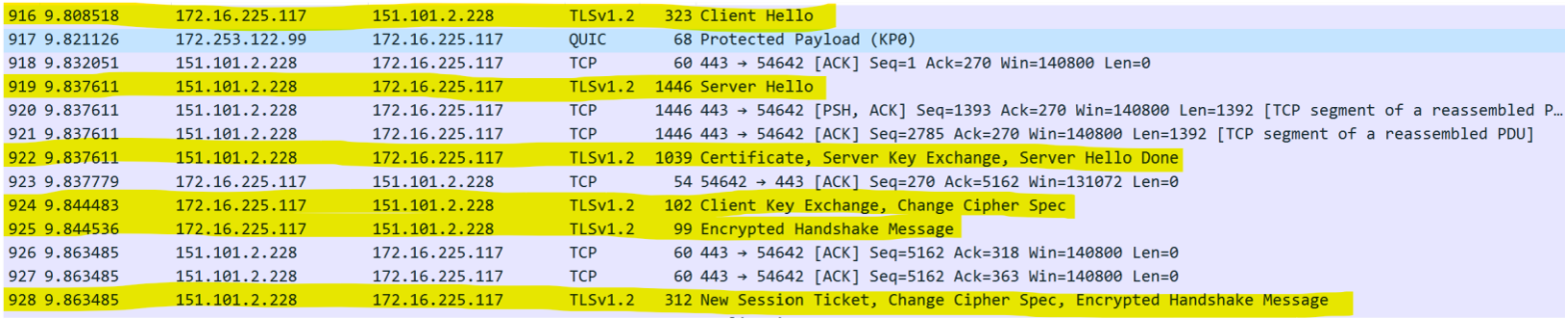
Type	Domain Name	TTL	Address
A	www.pitt.edu	30	151.101.2.228 Owner: Fastly | WHOIS | AS54113 IP blocked by dnsbl.spfbl.net | More
A	www.pitt.edu	30	151.101.66.228 Owner: Fastly | WHOIS | AS54113 IP blocked by dnsbl.spfbl.net | More

That made sense because I was actually able to find it among the packet in Wireshark, whereas with the provided IP address (136.142.34.104) I wasn't able to find it. Even after I tried the URL many times and used different browsers just in case.

```
913 9.785930    172.16.225.117  151.101.2.228   TCP     66 54642 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
914 9.806094    151.101.2.228   172.16.225.117  TCP     66 443 → 54642 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1396 SACK_PERM=1 WS=512
915 9.806272    172.16.225.117  151.101.2.228   TCP     54 54642 → 443 [ACK] Seq=1 Ack=1 Win=131072 Len=0
```

This is the TCP handshake, we can tell that in the first packet, the client (in this case me) is sending SYN to the server (which is www.pitt.edu) and seq = 0. The latter responds by sending back a SYN-ACK packet where ACK = 1. Finally, the client sends an ACK packet, and as shown seq = 1 (seq + 1).

The following screenshot shows the TLS handshake (highlighted)



916	9.808518	172.16.225.117	151.101.2.228	TLSv1.2	323 Client Hello
917	9.821126	172.253.122.99	172.16.225.117	QUIC	68 Protected Payload (KP0)
918	9.832051	151.101.2.228	172.16.225.117	TCP	60 443 → 54642 [ACK] Seq=1 Ack=270 Win=140800 Len=0
919	9.837611	151.101.2.228	172.16.225.117	TLSv1.2	1446 Server Hello
920	9.837611	151.101.2.228	172.16.225.117	TCP	1446 443 → 54642 [PSH, ACK] Seq=1393 Ack=270 Win=140800 Len=1392 [TCP segment of a reassembled P…
921	9.837611	151.101.2.228	172.16.225.117	TCP	1446 443 → 54642 [ACK] Seq=2785 Ack=270 Win=140800 Len=1392 [TCP segment of a reassembled PDU]
922	9.837611	151.101.2.228	172.16.225.117	TLSv1.2	1039 Certificate, Server Key Exchange, Server Hello Done
923	9.837779	172.16.225.117	151.101.2.228	TCP	54 54642 → 443 [ACK] Seq=270 Ack=5162 Win=131072 Len=0
924	9.844483	172.16.225.117	151.101.2.228	TLSv1.2	102 Client Key Exchange, Change Cipher Spec
925	9.844536	172.16.225.117	151.101.2.228	TLSv1.2	99 Encrypted Handshake Message
926	9.863485	151.101.2.228	172.16.225.117	TCP	60 443 → 54642 [ACK] Seq=5162 Ack=318 Win=140800 Len=0
927	9.863485	151.101.2.228	172.16.225.117	TCP	60 443 → 54642 [ACK] Seq=5162 Ack=363 Win=140800 Len=0
928	9.863485	151.101.2.228	172.16.225.117	TLSv1.2	312 New Session Ticket, Change Cipher Spec, Encrypted Handshake Message

In the beginning, we can see that the client is sending “Client hello” and then the server responds with “Server hello”. Then, the server sends “Certificate”, “Server Key exchange” and “Server Hello Done”. In our case, the client didn’t send back “Certificate”, “Server Key exchange” and “Certificate verify”, but that’s fine it’s simply because the server didn’t request it. Finally, they both send “Change Cipher sec” to each other and the handshake is done.

The encryption suite is shown in the following screenshot

```
   Cipher Suites Length: 32
v  Cipher Suites (16 suites)
      Cipher Suite: TLS_AES_128_GCM_SHA256 (0x1301)
      Cipher Suite: TLS_AES_256_GCM_SHA384 (0x1302)
      Cipher Suite: TLS_CHACHA20_POLY1305_SHA256 (0x1303)
      Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 (0xc02b)
      Cipher Suite: TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f)
      Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 (0xc02c)
      Cipher Suite: TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030)
      Cipher Suite: TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256 (0xcca9)
      Cipher Suite: TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 (0xcca8)
      Cipher Suite: TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013)
      Cipher Suite: TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014)
      Cipher Suite: TLS_RSA_WITH_AES_128_GCM_SHA256 (0x009c)
      Cipher Suite: TLS_RSA_WITH_AES_256_GCM_SHA384 (0x009d)
      Cipher Suite: TLS_RSA_WITH_AES_128_CBC_SHA (0x002f)
      Cipher Suite: TLS_RSA_WITH_AES_256_CBC_SHA (0x0035)
      Cipher Suite: TLS_EMPTY_RENEGOTIATION_INFO_SCSV (0x00ff)
```

We can see that the encryption algorithms used are AES (128 bits) with SHA256, AES (256 bits) with SHA384, RSA with AES (128 bits and 256 bits, with SHA).

We can tell that TCP connection is established after the server sends ACK packet, and TLS handshake begins (because we know that TLS handshake happens after TCP handshake).

Part 2

Question 10

a) Packet Filter Firewall controls traffic based on the information in the packet header, without looking into the application data. So it takes the source and destination IP addresses into consideration and their port numbers. Also, it doesn't take the state of the packets into consideration (stateless firewall). The advantages of the Packet Filter Firewall are that it's fast and simple, also it is not specific to any application and is transparent to users. Disadvantages are that it can't block certain content if the application is allowed, and it is a stateless firewall.

On the other hand, Stateful Firewall tracks the state of traffic by monitoring all the connection interactions until it gets closed. It examines files, record related packets and understands the context packets by maintaining a connection state table. Pros is that it has more information to inspect so it's more accurate and secure. In fact, for instance if it finds that the same external IP address is being request at multiple ports, then it blocks further requests because it assumes it's a port scan. Also, it reduces the chance for IP spoofing because it allows packets that belong to an existing connection. Cons is that it takes more time than Packet Filter Firewall

Both Packet Filter and Stateful Firewall don't look into the application data. This is not the case with Application Proxy Firewall. Client's connection ends at proxy and another one is initiated from the proxy to the destination host. Proxy Firewall simulates the behaviour of a protected application on the inside network and so it only allows safe data. The advantage is that it's more secure than packet filtering. Disadvantages are that it needs additional overhead on each connection.

b) Default accept is when access is permitted unless expressly denied. However, default deny is when access is denied unless expressly allowed. This is exactly like fail-safe principle, where access is denied unless specified otherwise.

c) Ingress filtering inspects incoming traffic to prevent attacks from the outside network. However, egress filtering inspects the outgoing network traffic and prevents user from internal network to access outside network.

d) Firewall should be placed between the internet, and the trusted networks and the DMZ (demilitarized zone). That way it blocks undesired data coming from the internet. Firewalls are used to protect DMZ and the internal networks. So in addition, firewalls are placed between trusted networks and intranet.

Question 11

Intrusion detection is a function (hardware or software) that analyses information from the network and identifies possible security intrusions.

Question 12

Signature-based intrusion detection uses a set of known malicious data patterns and compares them with current behaviour to see if they match. If they do, then they're probably malicious. On the other hand, anomaly detection basically uses machine learning (AI) to collect the data that relates to the

behaviour of legitimate users. That way, it analyses the current observed behaviour to see if it matches with the legitimate users' behaviour or not.

Question 13

A false positive is when a normal, legitimate behaviour is confused with a malicious use. However, false negatives (or miss detection) occur when malicious activity looks like normal activity and therefore is not detected.

Question 14

The base rate fallacy is when we want to have more data in order to explain intrusions, but we don't want intrusions to happen. The challenge is that intrusions are rare events so it is hard to have enough data. So Bayesian detection rate (probability of intrusion knowing that there is alert) is low if base rate (probability of intrusion) is low.

Question 15

Honeypots are used to lure attackers. So it attracts attackers to learn attack patterns

Question 16

P(intrusion) = **p(I) = 0.0001** so **P(no I) = 0.9999**

a) True positive rate: P(alert | intrusion) = **p(A | I) = 900/1000 = 0.9**

False negative rate = 1 – true positive rate = 1 – 0.9 = **p(no A|I) = 0.1**

b) false positive rate P(Alert | no Intrusion) = **p(A|no I) = 0.001**

Bayesian rate = $\frac{P(I)P(A|I)}{P(I)P(A|I)+P(no\ I)P(A|no\ I)} = \frac{0.0001\times0.9}{0.0001\times0.9+0.9999\times0.001} = 0.08257$

c) p(A| no I) = 0.0001

$$\frac{P(I)P(A|I)}{P(I)P(A|I) + P(no\ I)P(A|no\ I)} = \frac{0.0001 \times 0.9}{0.0001 \times 0.9 + 0.9999 \times 0.0001} = 0.4737$$

P(A |no I) = 0.00001

$$\frac{P(I)P(A|I)}{P(I)P(A|I) + P(no\ I)P(A|no\ I)} = \frac{0.0001 \times 0.9}{0.0001 \times 0.9 + 0.9999 \times 0.00001} = 0.9$$

P(A|no I) = 0.000001

$$\frac{P(I)P(A|I)}{P(I)P(A|I) + P(no\ I)P(A|no\ I)} = \frac{0.0001 \times 0.9}{0.0001 \times 0.9 + 0.9999 \times 0.000001} = 0.989$$

We can see that the Bayesian rate increases drastically as we decrease the false positive rate. So the probability of having an alert knowing that there is an intrusion increases as the probability of getting an alert with no intrusion decreases. It makes sense because if P(A|no I) is very low then the system is more accurate and so it better detects an intrusion (so P(A|I) is higher). Mathematically speaking, it also makes sense because the denominator is smaller.