Q2 – Vulnerabilities analysis document

Vulnerability 1

Threat: Mitm

Affected component: mmn15

Module details: Server.py, client.cpp

Vulnerability class: Interception of communication

Description: The attacker intercepts the TCP/IP communication between the client and the server without their knowledge.

Result: Mitm in the protocol provided in Q1 can have several unwanted results:

1. The attacker has the ability to modify the data transmitted between the client and Server.
2. The attacker may impersonate either the client or the server, leading to unauthorized access or deception.
3. The attacker can hijack established sessions between the client and server, potentially gaining unauthorized access to sensitive resources.

Prerequisites: Either the attacker needs to be familiar with the port number and host or they need to be exposed somehow.

Proposed remediation: Encryption – Our program takes Mitm into account and solves it by aes encrypting the messages. In order for both the server and the client to be able to successfully aes encrypt and decrypt the messages, they both need to have the same aes key which should be sent one of the parties(The server in our case). This vulnerability within our proposed remediation is itsel remediated by first sending(The client) an RSA public key to the server which will be used to encrypt the aes key.

Risk:

Damage potential – 6

Reproducibility – 8

Exploitability – 8

Affected users – 9

Discoverability – 6

Vulnerability 2

Threat: Ddos

Affected component: mmn15 – server

Module details: Server.py

Vulnerability class: Service disruption, resource exhaustion, disruption of communication

Description: For each class:

1. overwhelming the server's resources by flooding it with requests.
2. Exhausting the resources of the server and preventing it from handling legitimate user requests.
3. The excessive traffic generated by a DDoS attack disrupts the normal communication flow between the client and server.

Result: For each class:

1. The server becomes slow, unresponsive, or completely unavailable during the attack.
2. Legitimate clients may experience slow response times or be unable to access the service.
3. The excessive traffic generated by a DDoS attack disrupts the normal communication flow between the client and server.

Prerequisites: Compromised devices, malware, or control over a network of systems. Another way it can be done is by having resources and infrastructure to generate a large volume of attack traffic.

Proposed remediation: In our protocol we're limiting the number or requests a client can send to the server to three, meaning that even if a large number of clients will send message simultaneously and the server is overwhelmed, after either receiving an error from the server or no response at all the client's program will terminate.

Risk:

Damage potential – 9

Reproducibility – 8

Exploitability – 7

Affected users – 9

Discoverability – 6