Jad_AbouNajem_solution

1. 203.0.113.8 and 150.200.0.1 can be assigned to hosts.
2. ARP finds the MAC address by broadcasting a request for a given IP.
3. DHCP uses UDP, server listens on port 67.
4. a+b-> Hubs are multi-port repeaters, while bridges sit between Hub-connected hosts and know which hosts are on which side, which solves the hub issue(unwanted hosts receiving packets), and routers facilitate connections between network + connect to the internet.

Task 3:

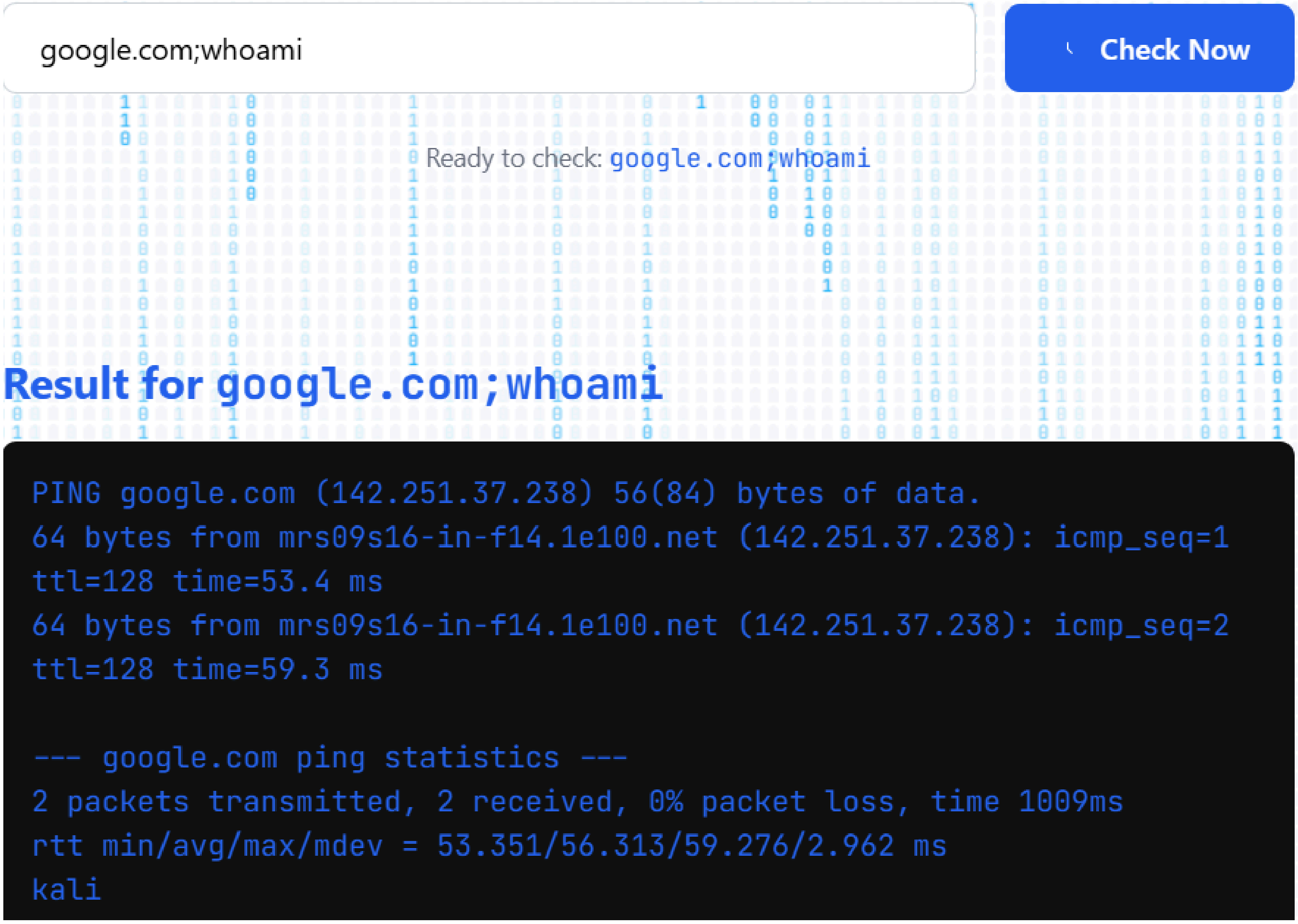
windows OS:

```
PING google.com (142.251.37.238) 56(84) bytes of data. 64 bytes from mrs09s16-in-f14.1e100.net (142.251.37.238): icmp_seq=1 ttl=128 time=154 ms 64 bytes from mrs09s16-in-f14.1e100.net (142.251.37.238): icmp_seq=2 ttl=128 time=82.2 ms --- google.com ping statistics --- 2 packets transmitted, 2 received, 0% packet loss, time 999ms rtt min/avg/max/mdev = 82.159/117.995/153.832/35.836 ms
```

Kali terminal:

```
192.168.216.1 - - [26/Jul/2025 11:45:23] "GET / HTTP/1.1" 200 -
192.168.216.1 - - [26/Jul/2025 11:45:23] "GET /static/logo.png HTTP/1.1" 200 -
192.168.216.1 - - [26/Jul/2025 11:45:24] "GET /favicon.ico HTTP/1.1" 404 -
192.168.216.1 - - [26/Jul/2025 11:46:03] "GET /api/run?host=google.com HTTP/1.1" 200 -
192.168.216.1 - - [26/Jul/2025 11:46:37] "GET /api/run?host=1.1.1.1 HTTP/1.1" 200 -
```

Vulnerability:



Ready to check: google.com;whoami

Result for google.com;whoami

```
PING google.com (142.251.37.238) 56(84) bytes of data.
64 bytes from mrs09s16-in-f14.1e100.net (142.251.37.238): icmp_seq=1
ttl=128 time=53.4 ms
64 bytes from mrs09s16-in-f14.1e100.net (142.251.37.238): icmp_seq=2
ttl=128 time=59.3 ms

--- google.com ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1009ms
rtt min/avg/max/mdev = 53.351/56.313/59.276/2.962 ms
kali
```

the app has an injection vulnerability as shown in the above image, when I inputed ;whoami after google.com we can see "kali" as a displayed output.

As a solution input should be securely validated and sanitized, and we can introduce a whitelist of inputs .