Experiment 07

Study network reconnaissance tools like WHOIS, dig, traceroute, nslookup to gather information about networks and domain registrars.

| Roll No. | 37 |
| --- | --- |
| Name | Mikil Lalwani |
| Class | D15-B |
| Subject | Security Lab |
| LO Mapped | LO3: Explore the different network reconnaissance tools to gather information about networks |

**Aim**:

Study the use of network reconnaissance tools like WHOIS, dig, traceroute, and nslookup to gather information about networks and domain registrars.

**Methods:**

1. traceroute

traceroute command is commonly used to troubleshoot the network. It finds out the delay and pathway to your destination. It determines and reports where is network latency comes from.

It is not installed by default on some Linux Distros, so you can install it using the following command.

sudo apt install traceroute

Syntax:

traceroute <destination>

Where <destination> is the host IP you want to troubleshoot, and its a mandatory parameter for this command.

1. nslookup

nslookup (Name Server Lookup) command used to query DNS to get a domain name, IP address mapping, or DNS records.

Syntax:

nslookup <domainName>

Where <domainName> is the DNS you want to analyze.

1. dig

dig (Domain Information Groper) is another command used to investigate DNS. It is an updated version of nslookup. It performs a DNS Lookup query and displays the response returned from name servers. It is also used to verify DNS mappings, MX records, and other DNS records.

Syntax:

dig <domainName>

Where <domainName> is the DNS you want to analyze.

1. whois

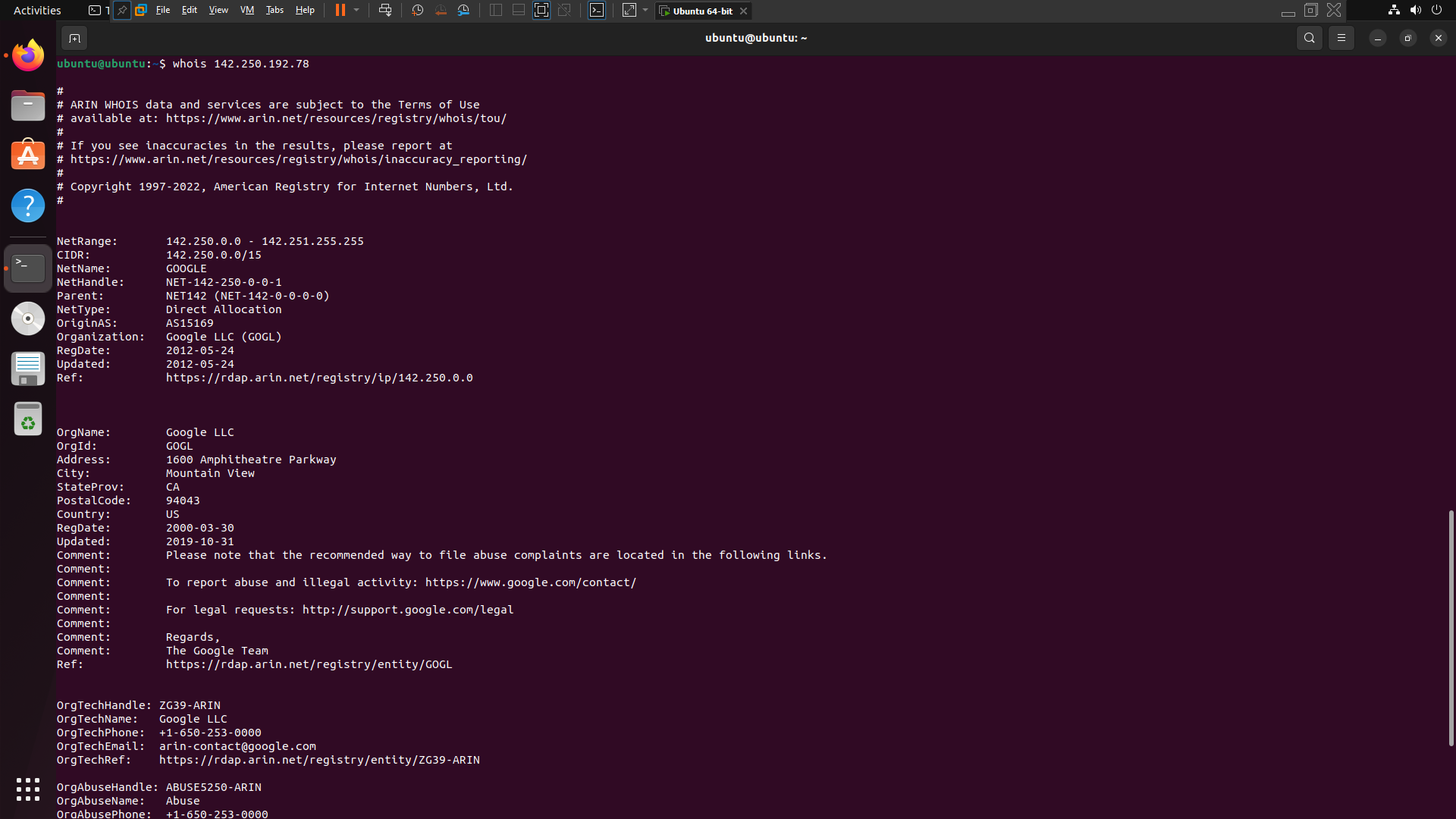
whois command is used to get all the information about a website. You can get all registration and ownership details using it. You need to install the whois package before using it.

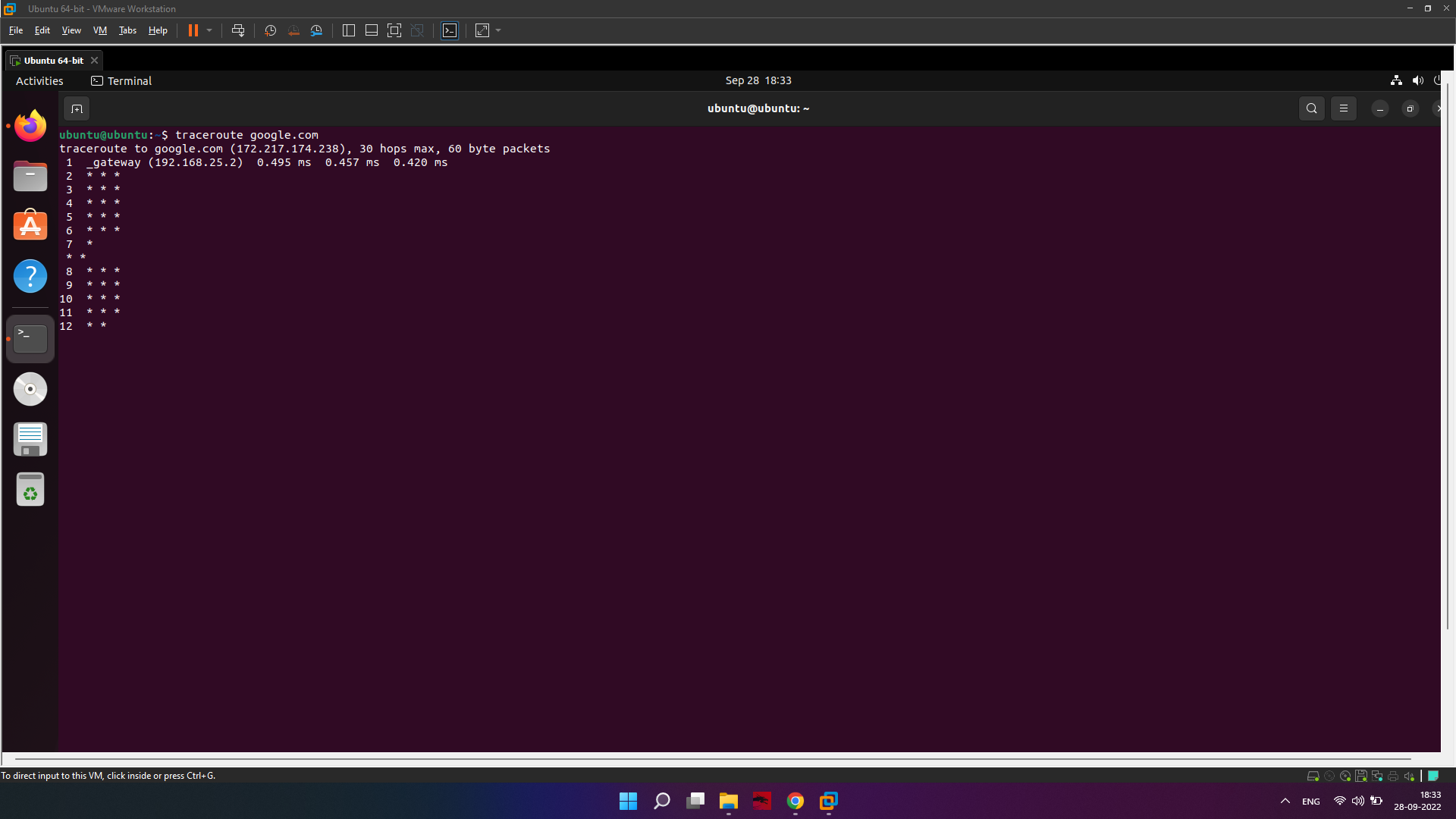
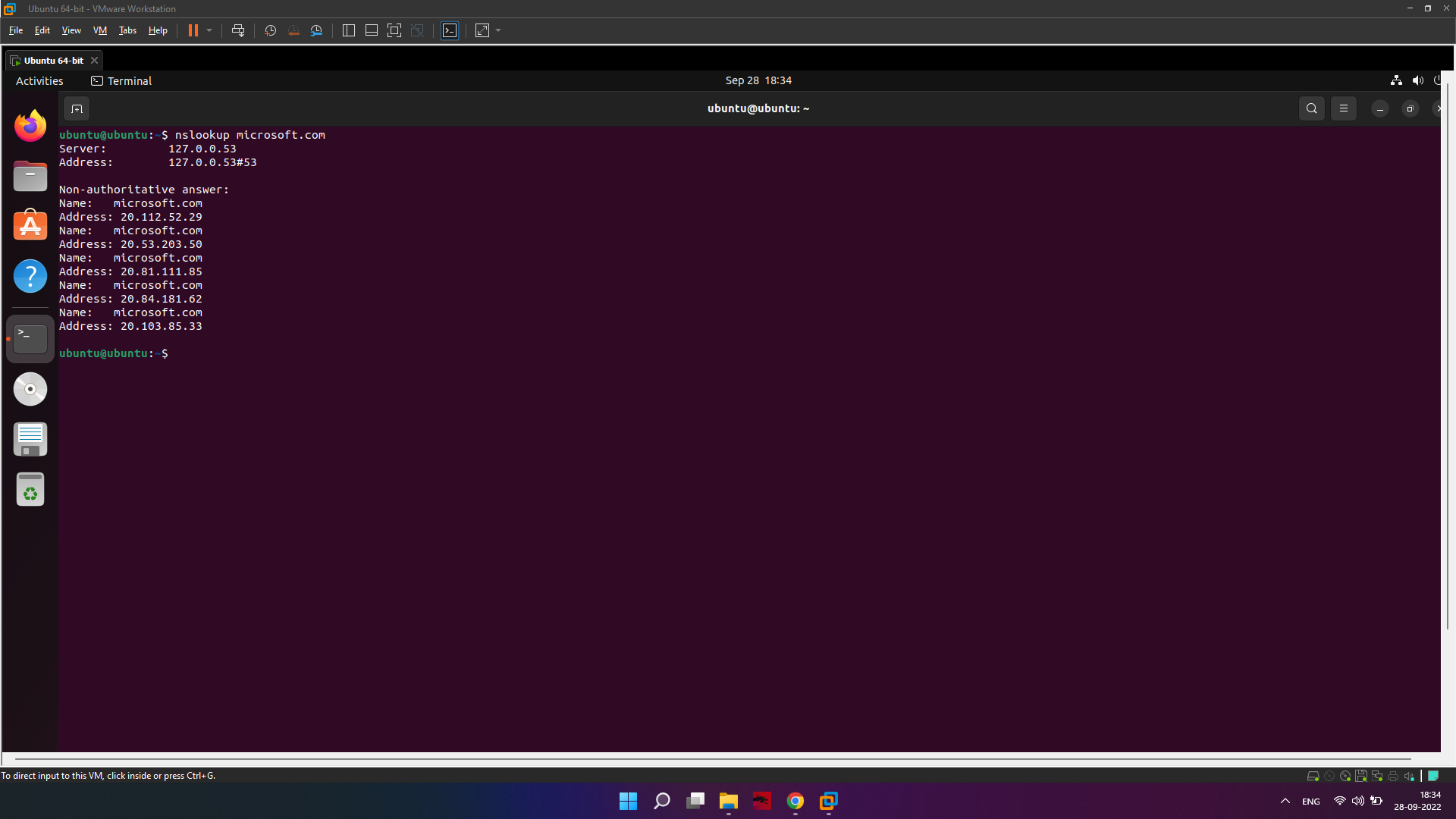
sudo apt install whois

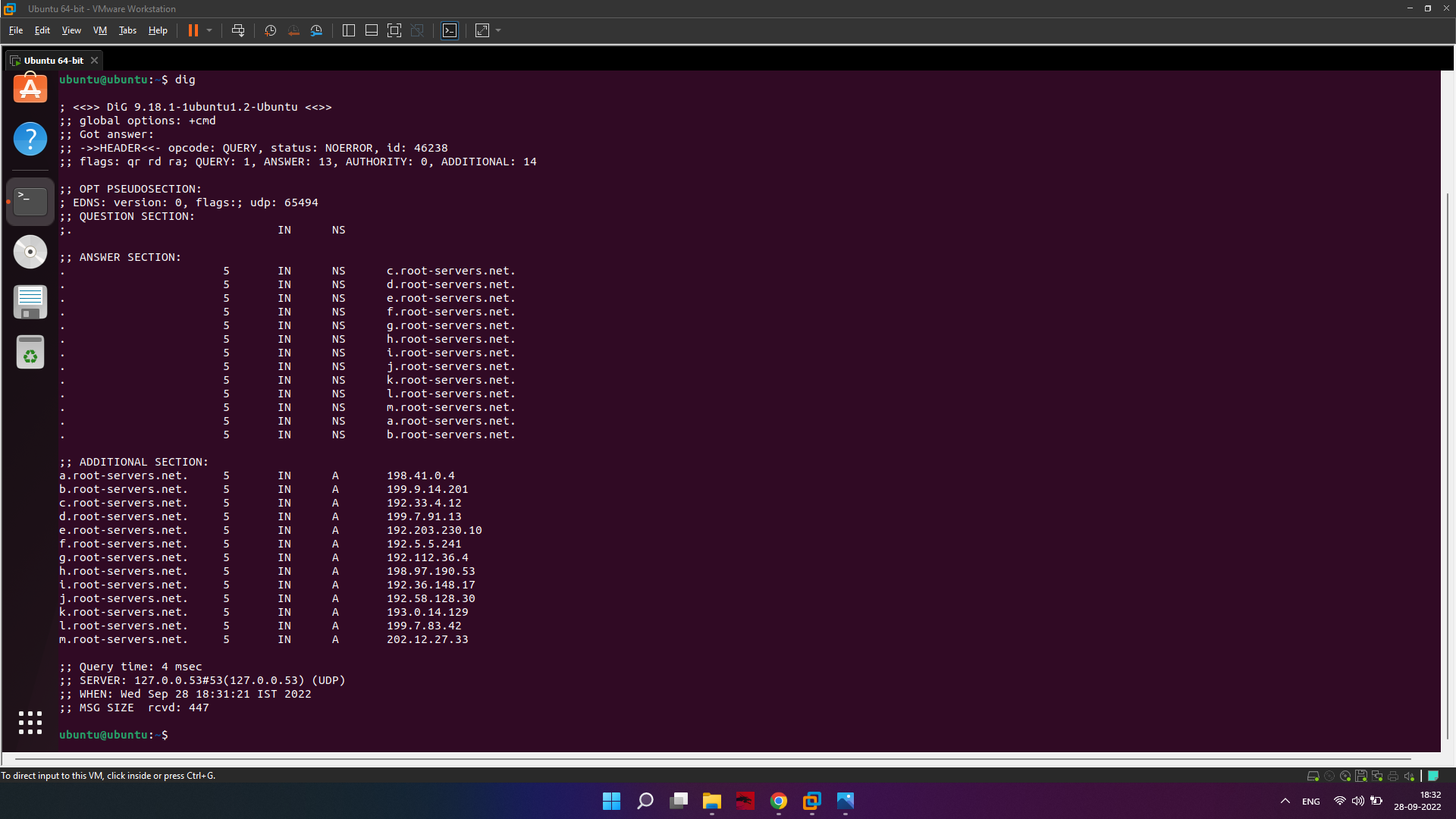
Syntax:

whois <website>

**Results**:







**Conclusion**:

Thus we have successfully used network reconnaissance tools to gather information about networks and domain registrars.