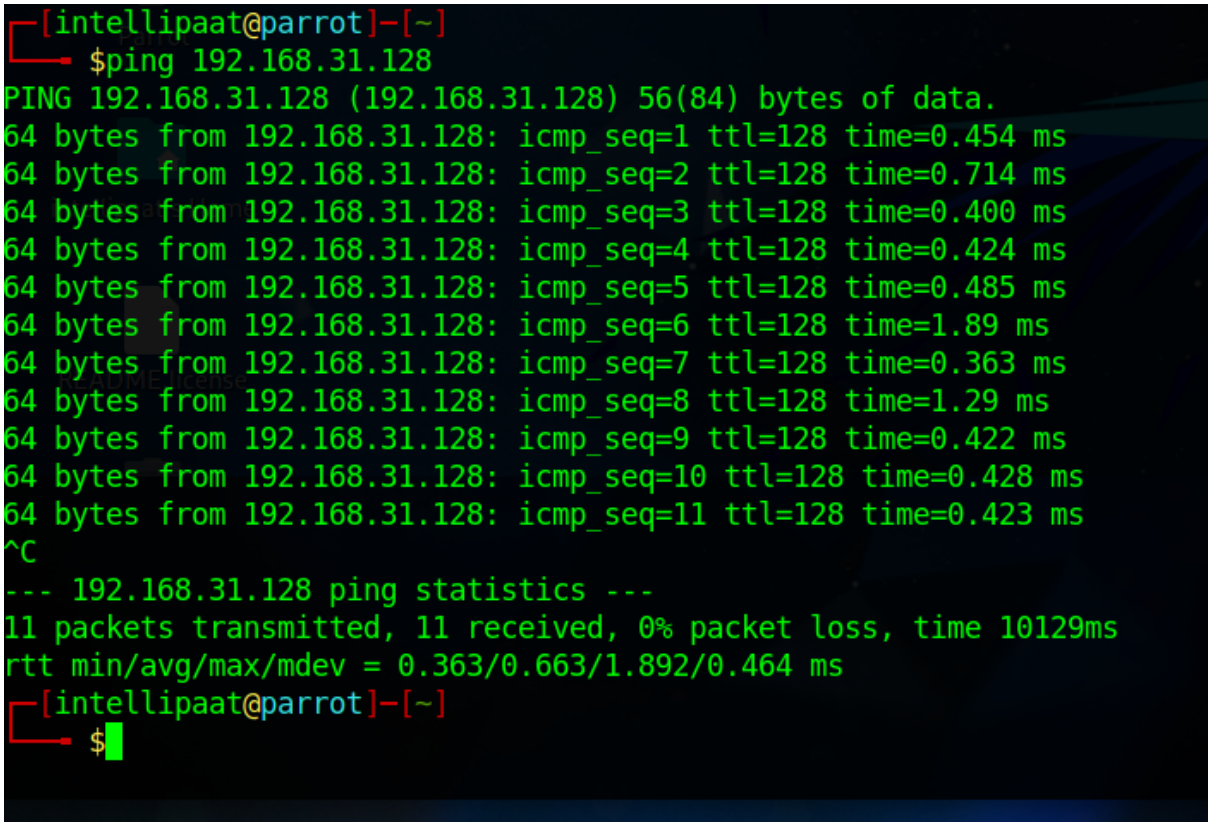
Assignment - Scanning Network

Tasks to be Performed:

1. **Host Discovery Using the 'ping' Command:** Your first task is to perform host discovery on the client's network using the 'ping' command. Provide a detailed explanation of the data you can extract from the results and how this helps in the assignment.

Ans. My target IP address is 192.168.31.128(Win11).



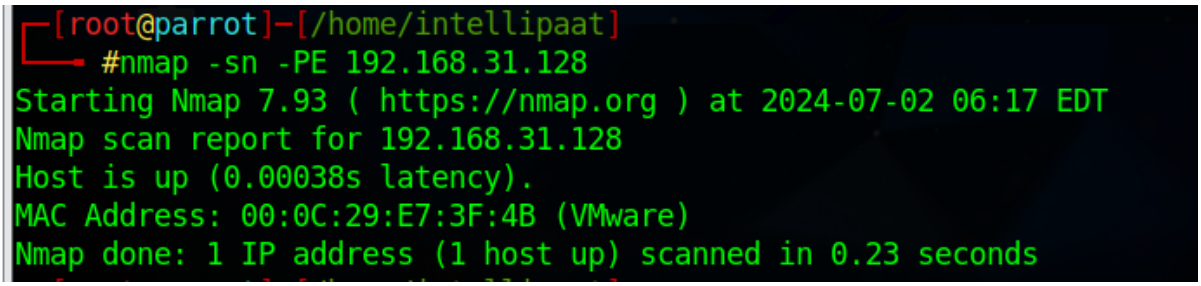
Above we can see that as soon as we ping to target packets are sent from attacking device which is of 64 bytes(8bits=1byte) . Main idea of pinging is to check if the device is active or not. To check weather its active, we transmit packets and if we receive the packets without any loss, that means the device is active and ready to get attacked. There are two concepts ARP (Address Resolution Protocol) and ICMP (Internet Control Message Protocol) protocol, in simple words ARP is used when we are discovering target MAC address for the first time, ICMP is used once the target is discovered to send Clearly above we can see out of 11 packets sent, it received all the packets without loss. TTL means time to live i:e total time the data packet can survive, exceeding the ttl with no response results in expiring of packet. Time is 10129ms means total time taken for the whole process to take place.

2. **Comprehensive Port Scan:** Now, you need to conduct a comprehensive and non-intrusive port scan on the specified target IP address. Outline the steps you would take, including the choice of tools and software. Explain the reasons for using non-intrusive methods.

Ans. Tools used is Nmap. Non intrusive port scan or no port scan is kind of passive attack where we don't want aggressively scan the target. This method is kind of pinging which also tell weather the host is active or not.

Pinging using Nmap for basic details.

Step1: Enter the command **nmap-sn -PE <ip address>**



We are pinging using ICMP to target host, lets decode above command. **-sn** = pinging,

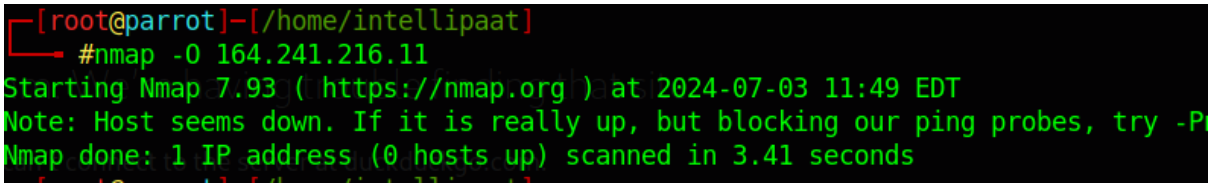
-PE =using icmp, **IP addr** =192.168.31.128. This method tell us weather the host Is up or not which in this case is up and also displays the **MAC** address which is **00:0C:29:E7:3F:4B** and also displays it is VMware which is true as we are using VMware software.

3. **OS Discovery and Ethical/Legal Considerations**: Perform OS discovery on the network you do not own or manage. Discuss the ethical and legal considerations that security professionals should be aware of and adhere to during this process.

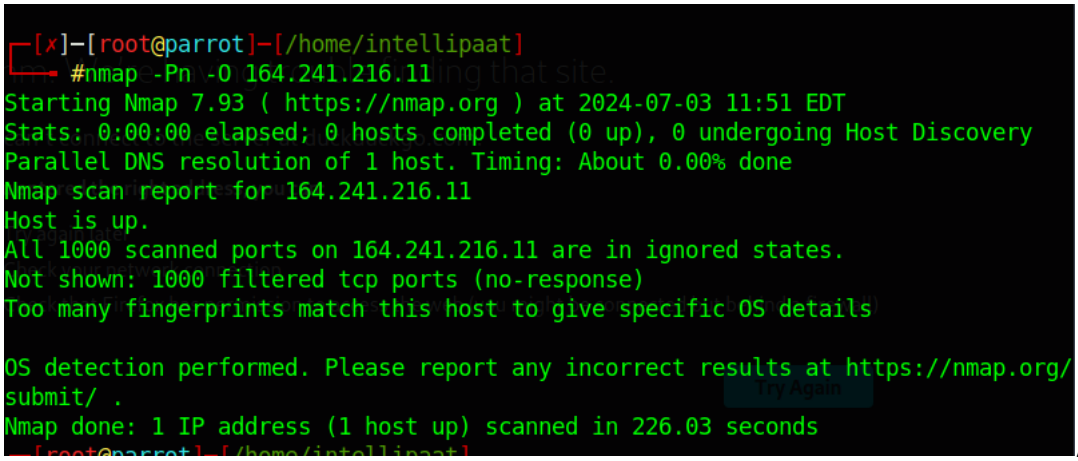
Ans. For this , I will be using certifiedhacker.com to Perform OS discovery on the network which does not managed by me. This site is used by all the freshers to test our skills as it its meant for ethically hacking. First we will see how we discover the OS and then followed by discussion on ethical and legal consideration.

Method-1(Nmap)

Step 1: In command line terminal enter nmap -O 164.214.216.11.As we can see that it couldn't detect any host OS and shows host me be down. It also shows solution of using -Pn before -O.



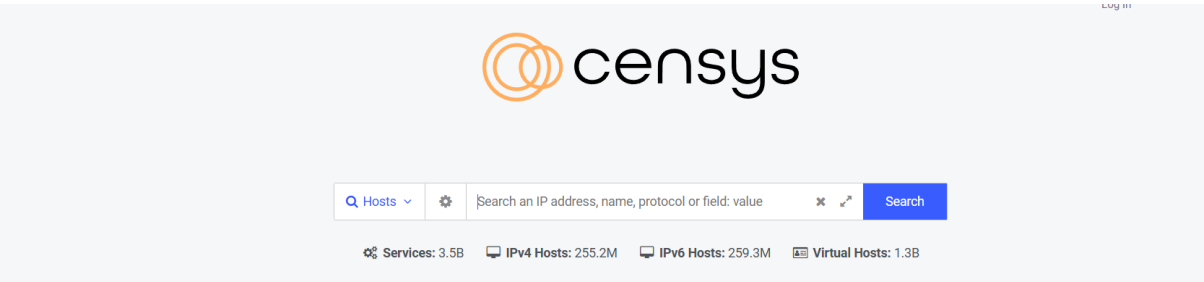
Step-2:



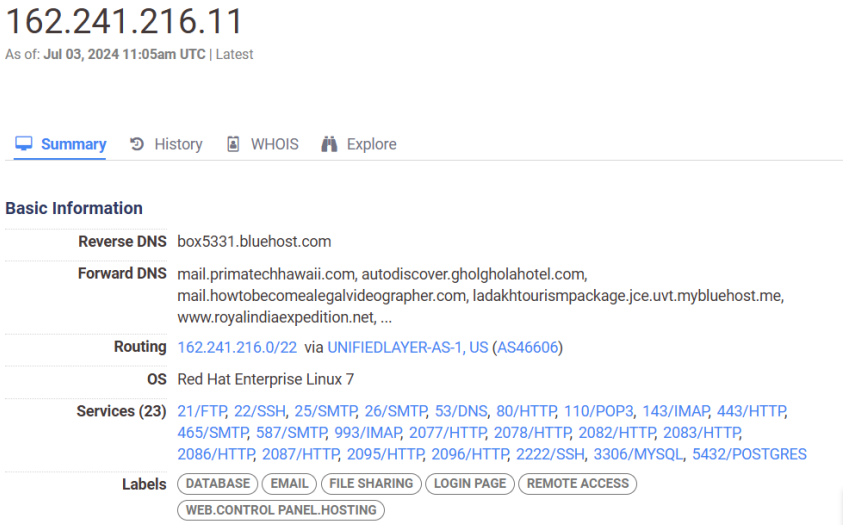
After entering nmap -Pn -O 164.241.216.11 , we can detect that host is up but nothing more could be known about OS. So we will try Method 2 which is using censys website.

Method-2

Step 1: First, search **censys.io** on your browser as we are about to use this website to discover target OS.



Step 2: Enter the target website certifiedhacker.com IP address and click enter.



Finally we get the result, where we can identify the OS used is **Red Hat Enterprise Linux 7**. **Final result**- **Linux OS** is detected.

Ethical Consideration:-

- **Authorization**: This refers to the need for explicit permission from the organization or individual who owns the system or network being tested. Without proper authorization, a penetration tester is effectively engaging in unethical hacking.
- **Transparency**: Ethical hackers must be transparent to their clients about their methodology, tools, and techniques. This means that they should not keep any aspect of their testing methodology a secret and must fully disclose their methods to their clients.
- **Confidentiality**: Organizations and penetration testers must ensure that the data collected during the penetration testing exercise is kept confidential and not shared with unauthorized parties.
- **Responsibility**: Organizations must ensure that their penetration testing exercise is conducted in a responsible and professional manner, and that no harm is caused to their employees, customers, or stakeholders during the process.

Legal Consideration:-

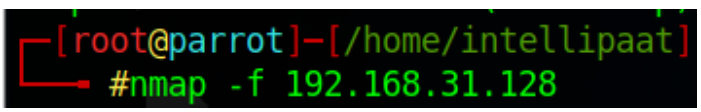
- **Compliance**: Organizations must ensure that their penetration testing exercise complies with all applicable laws and regulations, including data protection laws, privacy laws, and intellectual property laws.
- **Liability**: Organizations must consider the potential liability that may arise from the penetration testing exercise, including any damage caused to the network or systems as a result of the testing, or real-world implications that might be tied to those systems.
- **Documentation**: Organizations must maintain detailed records of their penetration testing exercise, including the scope of the test, the methods used, and the results obtained.

4. **Scanning Beyond IDS and Firewall:** Conduct a scan beyond the Intrusion Detection System (IDS) and Firewall. Provide a report of all the outcomes, including vulnerabilities and potential risks that may have been missed by these security measures.

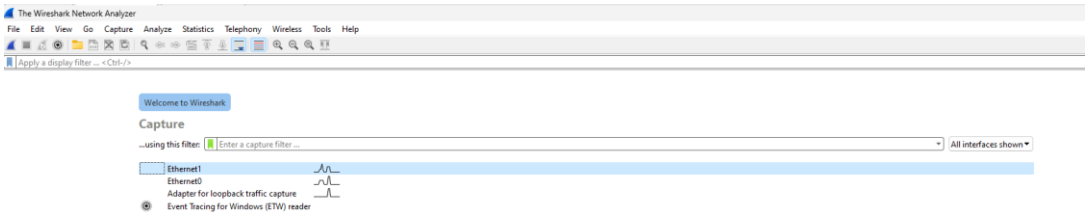
Ans. Method1-Sending Fragments to scan beyond IDS and firewall

- Fragmented scans divide packets into smaller fragments, making it harder for IDS to reassemble and analyze them.
- IDS may miss fragmented packets, allowing attackers to explore beyond the firewall.

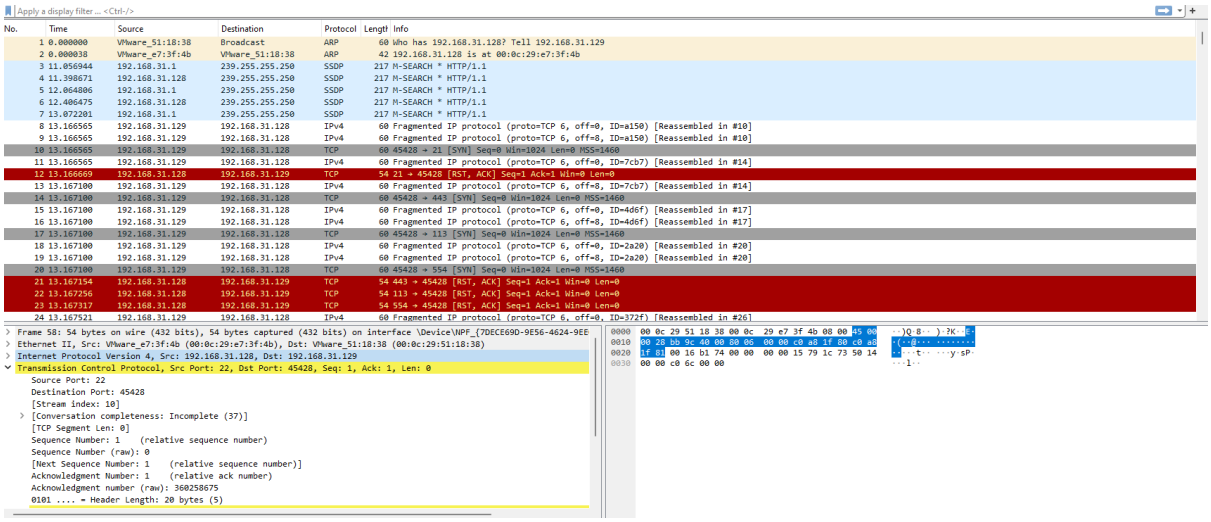
Step1: Turn on terminal in parrot os, Enter this command nmap -f 192.168.31.128.

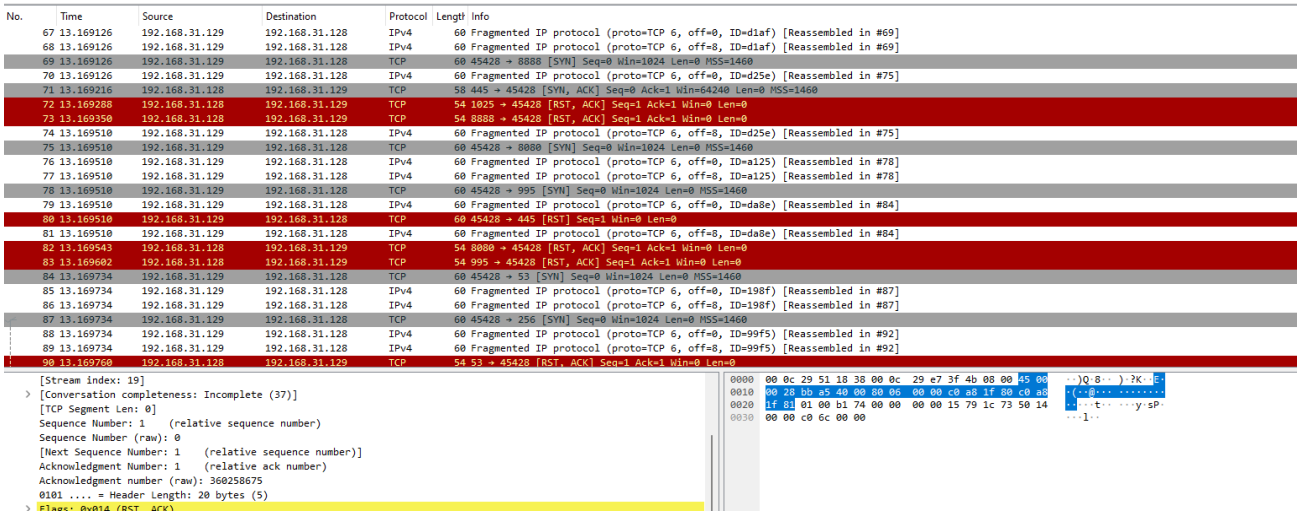


Step2. Parallelly open Wireshark app in windows vm ,click the ethernet 1 or 0, which in my case is ethernet0 as its is the name of the target IP.



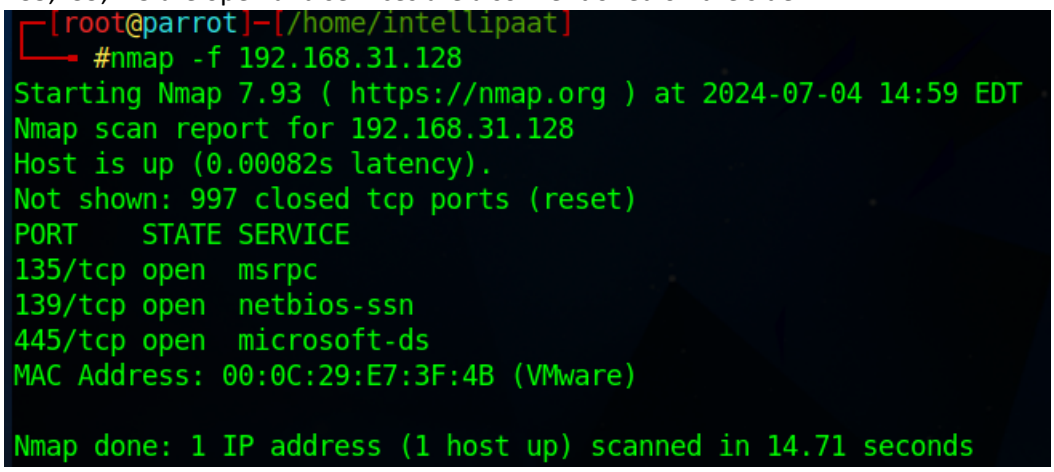
Step 3. Double click on enthernet0 to start analysing. We can observe that Wireshark has started receiving fragments ,it clearly shoes source ip and destination ip.





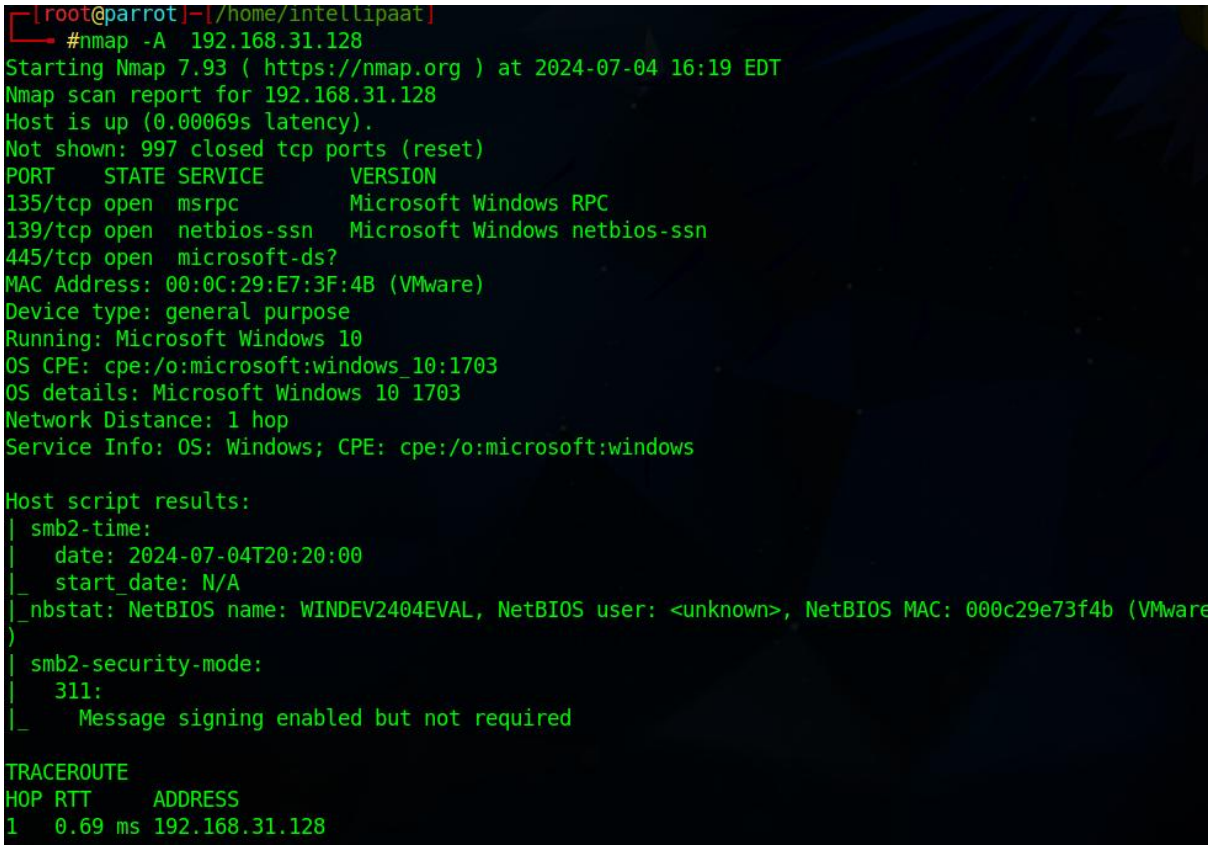
Step 4:After nmap running the command, it will show what all port are open with service. Below

135,139,445 are open and services are also mentioned on the side.



5. Network Scan Using Wireshark: Create a step-by-step tutorial on how to use Wireshark to carry out a basic network scan. Demonstrate how to locate open ports on a target machine as an example.

Ans. Step1.



6.Generating a Comprehensive Report: After completing the tasks mentioned above, generate a comprehensive report summarizing your findings, including vulnerabilities, risks, and recommendations for improving the network's security.

----------Ignore----------

```
┌──(root㉿kali)-[/home/kali]
└─# hping3 --flood --rand-source 137.74.187.101 --data 1000000000
HPING 137.74.187.101 (eth0 137.74.187.101): NO FLAGS are set, 40 headers + 51712 data bytes
hping in flood mode, no replies will be shown
^C
── 137.74.187.101 hping statistic ──
9026 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
```

Offline for Maintenance

Our apologies for the inconvenience, but this site is temporarily offline for maintenance (usually nightly backups at 8:00 AM UTC). If this lasts longer than 60 minutes, please feel free to email us or contact us on Discord.

— HackThisSite.org