

## Lab Assignment-2

K.Anirudh  
AP21110011342

**1)The Command Used for the SYN attack for a domain(apache2 server) is**

`Hping3 10.0.92.128 -S -flood`

**Q1.Based on the Wireshark capture for this traffic, what was the destination port used?**

A. The destination port for the following SYN attack is port 0. This is the best way to do 'hide ping'

**Q2. What must be adjusted to send a TCP SYN packet to port 135?**

A. To change the TCP SYN Packet to port 135 we need to add the -p parameter and specify the port as 135. The command would look like `'hping3 10.0.92.128 -S -flood -p 135'`

**Q3. What must be adjusted to send a TCP SYN packet to series of ports (ex: start from 80)?**

A.To send the packets from the series of ports that starts with the port 80 we need to add the -s parameter where it indicates that it is starting port. The Command would look like `hping3 10.0.92.128 -S -flood -p ++80`

**2)Perform a TCP ACK Scan on target (port 445)**

**Q4. Based on the Wireshark capture for this traffic, what was the flag type of the target's reply?**

**Answer:**RST flag

**3. Perform a TCP RST Scan on target (port 445)**

**Q5. Based on the Wireshark capture for this traffic, what was the flag type of the targets reply?**

**Answer:** No Reply

**Q6. How can we send more than one crafted packet?**

**Answer:** By using the Flood Attack

**Q7. How can we perform a TCP XMAS Scan?**

Answer: we can set the TCP XMAS Scan by adding the -x parameter. The full command is **hping3 10.0.92.128 -X -flood**

**4. Perform a UDP Scan on target**

**Q8. Based on the Wireshark capture for this traffic, what was the higher layer protocol used?**

Answer: DNS

**Q9. Continue to the same packet capture, Why do you think Wireshark stated this sent packet as “Malformed Packet”?**

Answer: Because the packet may be using Incorrect Protocol or someone Intercepted the packet and changed the response and checksum error occurs because of that and therefore the Packet is termed as Malformed Packet.

**Q10. Also, what was the ICMP packet reply’s Type \_\_\_\_\_ and Code \_\_\_\_\_ Numbers?**

Answer: 3(Destination Unreachable) Code 3(Port Unreachable)

**5. Perform an ICMP Ping on target**

**Q11. Based on the Wireshark capture for this traffic, what was the type of ICMP packet sent and received?**

Answer:

The ICMP sent is Type 8(Echo(Ping) Request) and the ICMP received is Type 0(Echo(Ping) request)

**Q12. What is the packet size of the IP layer \_\_\_\_\_ and the ICMP layer \_\_\_\_\_?**

Answer: IP Layer 66 bytes and ICMP layer 42 bytes

**6. Perform a TCP Ping on target (sending 5 packets)**

**Q13. Based on the Wireshark capture for this traffic, what was the type of flags set in the target’s reply?**

Answer: RST,ACK

**Q14. Is there any difference between the TCP Ping we just crafted and the TCP SYN packet we did in Lab2 part1 and why?**

Answer: The TCP Ping is one type of the DDOS attack where the ICMP echo request has been sent to the sever in large amounts of the data and the server cannot able to send the ICMP Echo Reply whereas the SYN Flooding attack is also the same type of the attack but instead of the ICMP we will send the SYN requests/

## 7. Perform a UDP Ping on target

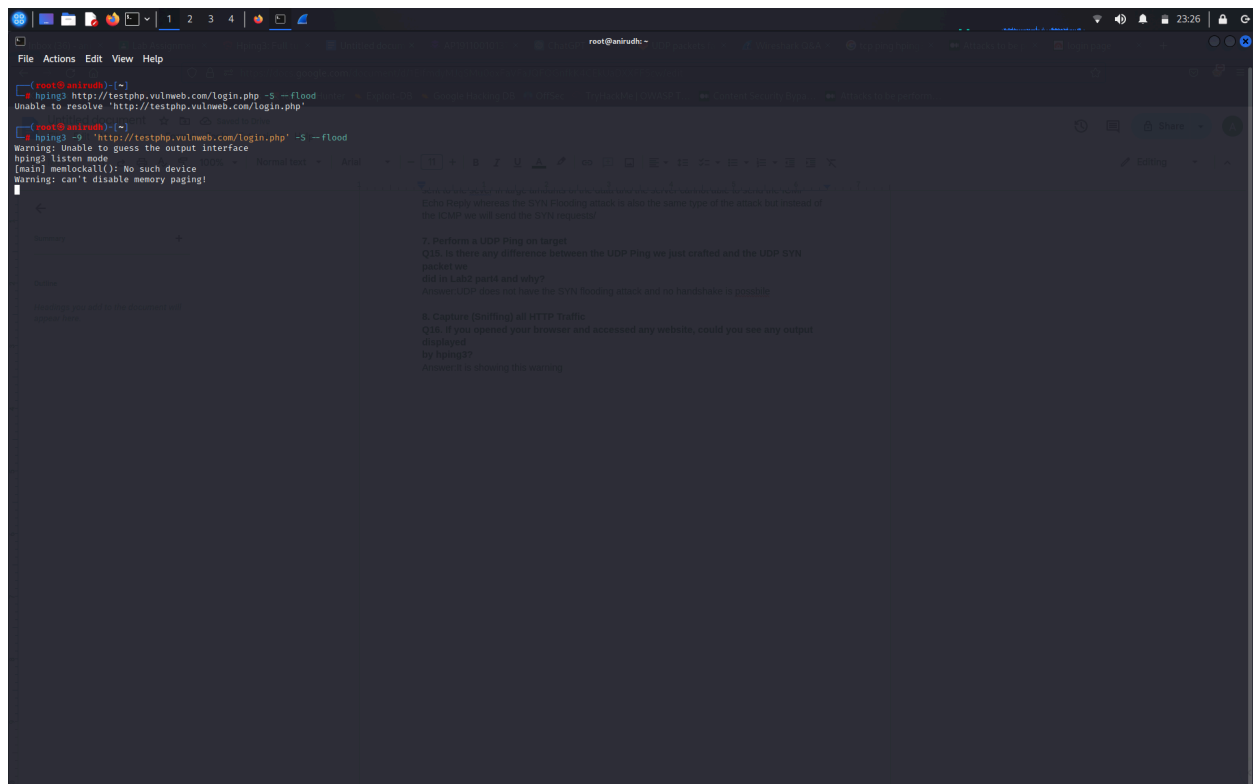
**Q15. Is there any difference between the UDP Ping we just crafted and the UDP SYN packet we did in Lab2 part4 and why?**

Answer:UDP does not have the SYN flooding attack and no handshake is possible

## 8. Capture (Sniffing) all HTTP Traffic

**Q16. If you opened your browser and accessed any website, could you see any output displayed by hping3?**

Answer:It is showing this warning



```
root@anirudh: ~  
[root@anirudh]# hping3 http://testphp.vulnweb.com/login.php -S --flood  
Unable to resolve 'http://testphp.vulnweb.com/login.php'  
[root@anirudh]# hping3 -S http://testphp.vulnweb.com/login.php -S --flood  
warning: Unable to guess the output interface  
hping3 listen mode  
[main] memlockall(): No such device  
warning: can't disable memory paging!
```

7. Perform a UDP Ping on target  
Q15. Is there any difference between the UDP Ping we just crafted and the UDP SYN packet we did in Lab2 part4 and why?  
Answer:UDP does not have the SYN flooding attack and no handshake is possible

8. Capture (Sniffing) all HTTP Traffic  
Q16. If you opened your browser and accessed any website, could you see any output displayed by hping3?  
Answer:It is showing this warning

## 9. Performing a Classical SYN Flood Attack

**Q17. Based on the Wireshark capture for this traffic, how many packets were transmitted**

\_\_\_\_\_ and how many were received  
\_\_\_\_\_?

Answer: Packets:72787 Displayed:72787(100.00%)

**Q18. Why did you receive that number of packets only?**

Answer:Because of the SYN flood attack which continuously send the packets irrespective of the 3-way Handshake

**Q19. What is the “-a” hping3 option used for?**

**Answer:** It is used to spoof the source IP address