Packet Crafting

In this lab, students will use the **Hping3** utility to perform various packet crafting tasks. The objective is developing basic packet crafting skills needed by ethical hackers and security auditors.

Reminder: you can get help on using hping3 by typing **hping3 –h** or by typing **man hping3**. Man allows accessing the command's manual. Arrow keys allow navigating through the manual and pressing **q** allows returning back to the command-line.

Objectives:

Lab1 – Quick startup to hping3 usage
Lab2 – Target port scanning using hping3
Lab3 – Host Discovery using hping3
Lab4 – Other useful tests using hping3

Lab1 – Quick startup to hping3 usage

1) Start both of your virtual machines Kali Linux and Windows
2) Login to your Windows virtual machine and make sure your firewall is disabled
3) Login to your Kali Linux virtual machine
4) Double-click the Terminal to open a shell (i.e. a Command Prompt)
5) Now start Wireshark to capture packets that we'll be crafting
6) When you get the prompt, type **hping3 -h** followed by the ENTER key again
7) You should get the syntax for hping3 along with its options
8) Use the scroll bar to read the information and answer the following questions:

Q1. Use the appropriate option to check the version of hping3 that you are using. Write down your answer. Version: _____ Year that the version was developed / released: _____.

Q2. Which of the options allows sending packets with bad IP checksum to a target?
Answer: _____.

Q3. You want to use the hping3 utility to send a TCP FIN packet to a target computer. What hping3 option could do that? Answer: _____.

Q4. Type **hping3 192.168.56.102** followed by the ENTER key to check if the computer is reachable. Is the target live (i.e. reachable)? Yes No.

Q5. What was the higher layer protocol used in the packets sent in Q4?
Answer: _____.

9) Type **hping3 193.188.67.51 193.188.67.52** followed by the ENTER key. Based on the result, answer the following two questions.

Q5. Why won't this command work? Answer: _____.

Q6. Based on the previous question, which of the two computers is connected to the Internet?
Answer: _____.

Lab2 – Target port scanning using hping3

1) Perform a TCP SYN Scan on target

a. hping3 –S 192.168.56.102 –c 1

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

Q2. What must be adjusted to send a TCP SYN packet to port 135?
Answer: _____.

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

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

a. hping3 –A 192.168.56.102 –c 1 –p 445

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

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

a. hping3 –R 192.168.56.102 –c 1 –p 445

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

Q6. How can we send more than one crafted packet?
Answer: _____.

Q7. How can we perform a TCP XMAS Scan?
Answer: _____.

4) Perform a UDP Scan on target

a. hping3 -2 192.168.56.102 -p 53 -c 1

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

Q9. Continue to the same packet capture, Why do you think Wireshark stated this sent packet as "Malformed Packet"?
Answer: _____.

Q10. Also, what was the ICMP packet reply's Type _____ and Code _____ Numbers?
Answer: _____.

Lab3 – Host Discovery using hping3

1) Perform an ICMP Ping on target

a. hping3 –1 192.168.56.102 –c 1

Q1. Based on the Wireshark capture for this traffic, what was the type of ICMP packet sent and received?
Answer: _____.

Q2. What is the packet size of the IP layer _____ and the ICMP layer _____?

2) Perform a TCP Ping on target (sending 5 packets)

a. hping3 –p 135 –c 5 192.168.56.102 -S

Q3. Based on the Wireshark capture for this traffic, what was the type of flags set in the target's reply? Answer: _____.

Q4. Is there any difference between the TCP Ping we just crafted and the TCP SYN packet we did in Lab2 part1 and why?
Answer: _____.

3) Perform a UDP Ping on target

a. hping3 -2 –p 445 –c 1 192.168.56.102

Q5. Is there any difference between the UDP Ping we just crafted and the UDP SYN packet we did in Lab2 part4 and why?
Answer: _____.

Lab4 – Other useful tests using hping3

1) Capture (Sniffing) all HTTP Traffic

a. hping3 -9 HTTP -I eth0

Q1. If you opened your browser and accessed any website, could you see any output displayed by hping3? Answer: _____.

2) Performing a Classical SYN Flood Attack

a. hping3 -S 192.168.56.102 -a 172.16.1.10 -p 135 --flood

Q2. Based on the Wireshark capture for this traffic, how many packets were transmitted _____ and how many were received _____?

Q3. Why did you receive that number of packets only? Answer: _____.

Q4. What is the "-a" hping3 option used for? Answer: _____.

3) Sending your name as data loaded onto an ICMP packet

a. hping3 -1 192.168.56.102 -e "YOUR NAME" -p 135

Q5. How can you capture this traffic on the destination/target?
Answer: _____.

Q6. In what layer did you find your name?
Answer: _____.

Q7. What was the size of that layer and why?
Answer: _____.

Q8. What must be adjusted to send your name using a UDP packet?
Answer: _____.

Q9. In what layer did you find your name?
Answer: _____.

Q10. What was the size of that layer and why?
Answer: _____.

Turning in Your Lab Work

Email the answers to me as an attachment. Send the message to **bsc@ashememery.com** with a subject line of **Hping3 Lab From** *Your Name*. Send a Cc to yourself.