Practical 3

Thursday, 11 August 2022 11:56 AM

ISEC3002 Penetration Testing and Defence
Workshop 3

The purpose of this workshop is to practice packet crafting with Scapy and Hping. Both tools should be available on Kali. In order to check your results please make sure that you are using Wireshark to capture the packets generated by your work.
Finally, the common target for the exercises below is the machine named ***Aldruhn***.

Exercise 1.
Provide the command to create the TCP header of a packet named "mypac" with the source port 443 and destination port 80.
mypac = IP() / TCP(sport=443, dport=80)
Provide the command to display the contents of mypac. Do you notice anything interesting about the port description?
mypac.show()
Update the command from (i) to use 53 as the source port and 135 as the destination port.
mypac /= / TCP(sport=53, dport=135)

Exercise 2.
Provide the command to send an ICMP packet to the IP address of *Aldruhn* with a payload containing the text string "My Message".
send(IP(dst = "192.168.2.12" / ICMP() / b"My Message")
Examine the packet created by your command. How many bytes does the actual message use?
10 bytes

Exercise 3.
Provide the command to send and receive TCP packets to the IP address of *Aldruhn* with the destination ports 80, 88, 443. How would you display the results?
ans, unans = sr(IP(dst="192.168.2.12") / TCP(dport=[80,88,443]))
ans.show()
unans.show()

Exercise 4.
Provide the command to do a SYN scan on the ports 22, 80, 88, 145, 443, 1433, 3389 (target is again Aldruhn machine).
Modify your previous command to add a source port of 53.
sr1(IP(dst="192.168.2.12") / TCP(dport=[22,80,88,145,443,1433,3389], flags='S'))
sr1(IP(dst="192.168.2.12") / TCP(sport=53,dport=[22,80,88,145,443,1433,3389], flags='S'))

Exercise 5.
Provide the command to create a DNS packet that sends a query asking for the DNS Question record for www.yahoo.com.

```
dnsPacket = IP(dst="1.1.1.1") / UDP(dport=53) / DNS(rd=1,
qd=DNSQR(qname='www.yahoo.com'))
```

Exercise 6.

Provide the HPING command to send TCP packets to the IP address *Aldruhn*, on port 80 with the flags SYN, ACK.

```
sudo hping3 192.168.2.12 -p 80 -S -A
```

Exercise 7.

Provide the HPING command to send 200 ACK TCP packets to *Aldruhn*, port 88. The packets should be sent every 0.05 of a second.

```
sudo hping3 -c 200 -A 192.168.2.12 -p 88 --interval u50000
```

Exercise 8.

Provide the command to do a port scan on the first 1024 ports of the *Aldruhn* machine.

```
sudo hping3 --scan 0-1024 -S 192.168.2.12
```

Exercise 9.

Provide the HPING command to send spoofed UDP packets from IP address of your machine to the IP address of Aldruhn.

```
sudo hping3 -a 1.2.3.4 --udp 192.168.57.7
```

Exercise 10.

Provide the HPING command to send ICMP timestamp requests to the IP *Aldruhn*.

```
sudo hping3 --icmp-ts 192.168.57.7
```

Exercise 11.

Provide the command that will send 10 ICMP packets to yahoo.com.

```
sudo hping3 -c 100 --icmp yahoo.com
```

Exercise 12.

Provide the command to send and receive only the answers of 5 packets with TTL values ranging from 1 to 5, from a randomized source, with the flags SYN and ACK set to the IP address of *Aldruhn*.

```
sudo hping3 -c 5 -t 5 --rand-source -S -A 192.168.57.7
```