Scan the network using the following tools: i. Hping2 / Hping3

```
root@kali:~# hping3 –A 192.168.0.1
```

```
root@kali:~# hping3 -8 1-600 –S 10.10.50.202
```

```
root@kali:~# hping3 –F –P -U 10.10.50.202
```

Advanced IP Scanner

Ip address of pc

ANGRY ip scanner

Input ip range

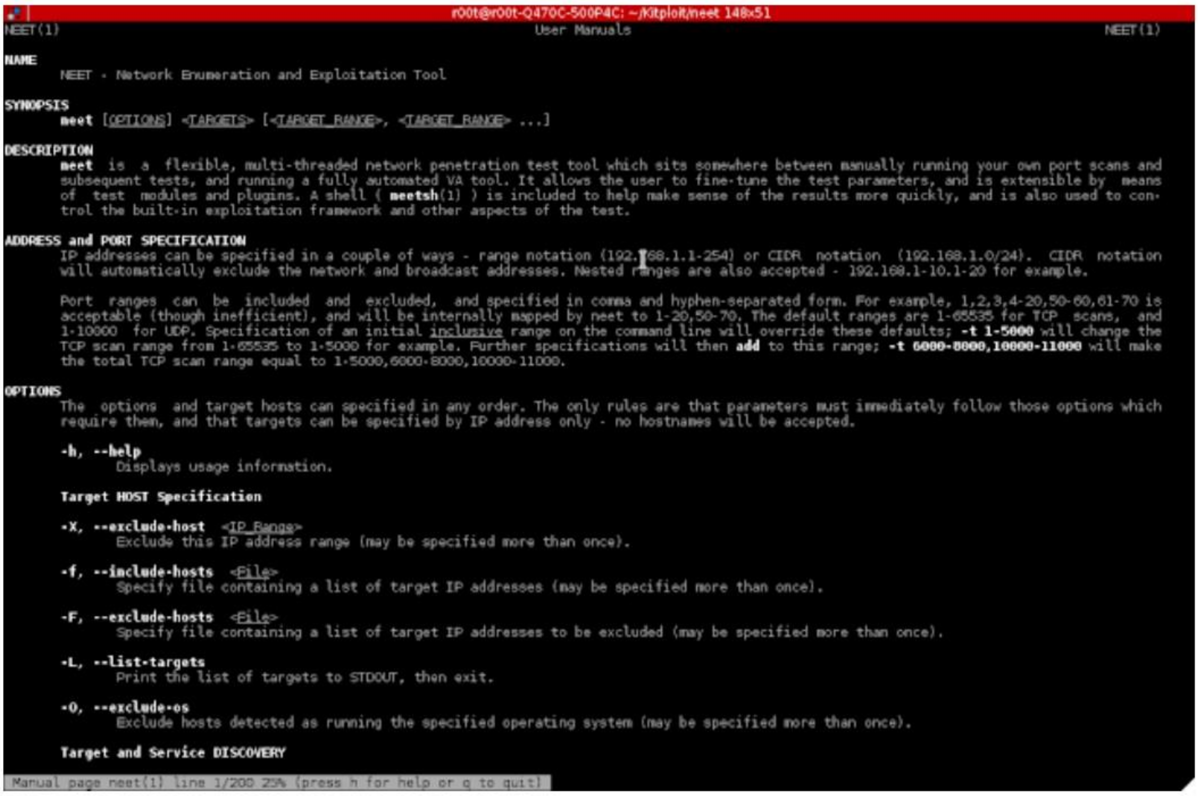
. Masscan

Scan for a selection of ports (-p22,80,445) across a given subnet (192.168.1.0/24): root@kali:~# masscan -p22,80,445 192.168.1.0/24

```
Starting masscan 1.0.3 (http://bit.ly/14GZzcT) at 2014-05-13 21:35:12 GMT -- forced options: -sS -Pn -n --randomize-hosts -v --send-eth
```

```
Scanning 256 hosts [3 ports/host] Discovered open port 22/tcp on 192.168.1.217 Discovered open port 445/tcp on 192.168.1.220 Discovered open port 80/tcp on 192.168.1.230
```

v. NEET



```
r00t@r00t-Q470C-500P4C: ~/Kitploit/neet 148x51
NEET(1)                                        User Manuals                                        NEET(1)

NAME
       NEET - Network Enumeration and Exploitation Tool

SYNOPSIS
       neet [OPTIONS] <TARGETS> [<TARGET_RANGE>, <TARGET_RANGE> ...]

DESCRIPTION
       neet  is  a  flexible, multi-threaded network penetration test tool which sits somewhere between manually running your own port scans and
       subsequent tests, and running a fully automated VA tool. It allows the user to fine-tune the test parameters, and is extensible by  means
       of  test  modules and plugins. A shell ( meetsh(1) ) is included to help make sense of the results more quickly, and is also used to con-
       trol the built-in exploitation framework and other aspects of the test.

ADDRESS and PORT SPECIFICATION
       IP addresses can be specified in a couple of ways - range notation (192.168.1.1-254) or CIDR  notation  (192.168.1.0/24).  CIDR  notation
       will automatically exclude the network and broadcast addresses. Nested ranges are also accepted - 192.168.1-10.1-20 for example.

       Port  ranges  can  be  included  and  excluded,  and specified in comma and hyphen-separated form. For example, 1,2,3,4-20,50-60,61-70 is
       acceptable (though inefficient), and will be internally mapped by neet to 1-20,50-70. The default ranges are 1-65535 for TCP  scans,  and
       1-10000  for UDP. Specification of an initial inclusive range on the command line will override these defaults; -t 1-5000 will change the
       TCP scan range from 1-65535 to 1-5000 for example. Further specifications will then add to this range; -t 6000-8000,10000-11000 will make
       the total TCP scan range equal to 1-5000,6000-8000,10000-11000.

OPTIONS
       The  options  and target hosts can specified in any order. The only rules are that parameters must immediately follow those options which
       require them, and that targets can be specified by IP address only - no hostnames will be accepted.

       -h, --help
              Displays usage information.

       Target HOST Specification

       -X, --exclude-host  <IP_Range>
              Exclude this IP address range (may be specified more than once).

       -f, --include-hosts  <File>
              Specify file containing a list of target IP addresses (may be specified more than once).

       -F, --exclude-hosts  <File>
              Specify file containing a list of target IP addresses to be excluded (may be specified more than once).

       -L, --list-targets
              Print the list of targets to STDOUT, then exit.

       -O, --exclude-os
              Exclude hosts detected as running the specified operating system (may be specified more than once).

       Target and Service DISCOVERY
 Manual page neet(1) line 1/200 25% (press h for help or q to quit)
```

vi. CurrPorts

. Run the application Currports

.Run the HTTP Trojan created in the previous lab

3. For more detail, right click on httpserver.exe and go to properties

Properties are showing more details about tcp connection. 4. Go to Windows 7 machine and initiate the connection as mentioned in the previous lab using aweb browser.

Connection successfully established. 5. Back to Windows Server 2016, Kill the connection.

vii. Colasoft Packet Builder

Colasoft packet builder offers Import and Export options for a set of packets. You can also adda new packet by clicking Add/button. Select the Packet type from the drop-down option. Available options are: - • ARP Packet • IP Packet • TCP Packet • UDP Packet

After Selecting the Packet Type, now you can customize the packet, Select the Network Adapter and Send it towards the destination.

viii. The Dude

input name and status partially down

Advance ip scanner:

Input ip address of another pc click on red button and do force shutdown

Currports

Open currports and Print the repot form _> view then HTML Report-All Items