

HARSHIT 19BCE0382  
ISM CSE3052 (Winter 2021-22 Slot: L5+L6)  
LAB ASSESSMENT 4  
21/03/2022

\$ ifconfig

```
Activities Terminal Mar 21 12:14
root@sjt516scope051: /home/matlab

root@sjt516scope051:/home/matlab# ifconfig
eno1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 10.30.161.61 netmask 255.255.255.0 broadcast 10.30.161.255
    inet6 fe80::fd91:2b71:d252:9cbe prefixlen 64 scopeid 0x20<link>
    ether e8:39:35:46:33:a1 txqueuelen 1000 (Ethernet)
    RX packets 100702 bytes 43652013 (43.6 MB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 46699 bytes 6431492 (6.4 MB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
    device interrupt 20 memory 0xfb000000-fb020000

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 30926 bytes 2689567 (2.6 MB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 30926 bytes 2689567 (2.6 MB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

root@sjt516scope051:/home/matlab#
```

\$ nmap 10.30.161.61

```
Activities Terminal Mar 21 12:15
root@sjt516scope051: /home/matlab

root@sjt516scope051:/home/matlab# nmap 10.30.161.61
Starting Nmap 7.80 ( https://nmap.org ) at 2022-03-21 12:15 IST
Nmap scan report for sjt516scope051 (10.30.161.61)
Host is up (0.0000050s latency).
Not shown: 995 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
53/tcp    open  domain
80/tcp    open  http
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds

Nmap done: 1 IP address (1 host up) scanned in 0.15 seconds
root@sjt516scope051:/home/matlab#
```

\$iptables -F

\$iptables -L

```
Activities Terminal Mar 21 12:17
root@sjt516scope051: /home/matlab

root@sjt516scope051:/home/matlab# iptables -F
root@sjt516scope051:/home/matlab# iptables -L
Chain INPUT (policy ACCEPT)
target    prot opt source               destination

Chain FORWARD (policy ACCEPT)
target    prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target    prot opt source               destination
root@sjt516scope051:/home/matlab#
```

\$git clone <portspooof repo>

```
Activities Terminal Mar 21 12:20
root@sjt516scope051: /home/matlab

root@sjt516scope051:/home/matlab# git clone https://github.com/drk1wi/portspooof.git
Cloning into 'portspooof'...
remote: Enumerating objects: 873, done.
remote: Counting objects: 100% (8/8), done.
remote: Compressing objects: 100% (7/7), done.
remote: Total 873 (delta 1), reused 3 (delta 1), pack-reused 865
Receiving objects: 100% (873/873), 3.30 MiB | 2.24 MiB/s, done.
Resolving deltas: 100% (473/473), done.
root@sjt516scope051:/home/matlab#
```

\$/configure

\$make

\$make install

```
Activities Terminal Mar 21 12:21
root@sjt516scope051: /home/matlab/portspooof

root@sjt516scope051:/home/matlab# ./configure && make && sudo make install
bash: ./configure: No such file or directory
root@sjt516scope051:/home/matlab# ls
18bn10025.pdf.ps  BCE001  closed.py  Downloads  examples.desktop  gh.o  nano.save  portspooof  q.c  Templates  Videos
a.out            BCE002  Desktop   dsa         gfff.cpp          'invalid path>'  NetBeansProjects  projectc  'queue 1.c'  'Untitled1.cpp'
a.c.save         BCE003  DEVANG    DSALABCAT   gh                 'invalid path>.layout'  p.c               pt        shatayu      'Untitled1.pdf'
a.out           clo.py  Documents eclipse-workspace gh.cpp            Music
root@sjt516scope051:/home/matlab# cd portspooof
root@sjt516scope051:/home/matlab/portspooof# ./configure && make && sudo make install
checking for a BSD-compatible install... /usr/bin/install -c
checking whether build environment is sane... yes
checking for a thread-safe mkdir -p... /bin/mkdir -p
checking for gawk... no
checking for mawk... mawk
checking whether make sets $(MAKE)... yes
checking build system type... x86_64-pc-linux-gnu
checking host system type... x86_64-pc-linux-gnu
checking for g++... g++
checking whether the C++ compiler works... yes
checking for C++ compiler default output file name... a.out
checking for suffix of executables...
checking whether we are cross compiling... no
checking for suffix of object files... o
checking whether we are using the GNU C++ compiler... yes
checking whether g++ accepts -g... yes
checking for style of include used by make... GNU
checking dependency style of g++... gcc3
checking for gcc... gcc
checking whether we are using the GNU C compiler... yes
checking whether gcc accepts -g... yes
checking for gcc option to accept ISO C89... none needed
checking dependency style of gcc... gcc3
checking whether gcc and cc understand -c and -o together... yes
checking whether make sets $(MAKE)... (cached) yes
checking how to run the C preprocessor... gcc -E
checking for grep that handles long lines and -e... /bin/grep
checking for egrep... /bin/grep -E
checking for ANSI C header files... yes
checking for sys/wait.h that is POSIX.1 compatible... yes
checking for sys/types.h... yes
checking for sys/stat.h... yes
checking for stdlib.h... yes
checking for string.h... yes
checking for memory.h... yes
checking for strings.h... yes
checking for inttypes.h... yes
```

```
Activities Terminal Mar 21 13:06
root@sjt516scope051: /home/matlab/portspoo

root@sjt516scope051: /home/matlab/portspoo x matlab@sjt516scope051: ~

config.status: creating src/Makefile
config.status: creating tools/Makefile
config.status: creating src/config.h
config.status: src/config.h is unchanged
config.status: executing depfiles commands
root@sjt516scope051:/home/matlab/portspoo# make
Making all in src
make[1]: Entering directory '/home/matlab/portspoo/src'
make all-am
make[2]: Entering directory '/home/matlab/portspoo/src'
make[2]: Leaving directory '/home/matlab/portspoo/src'
make[1]: Leaving directory '/home/matlab/portspoo/src'
Making all in tools
make[1]: Entering directory '/home/matlab/portspoo/tools'
make[1]: Nothing to be done for 'all'.
make[1]: Leaving directory '/home/matlab/portspoo/tools'
make[1]: Entering directory '/home/matlab/portspoo'
make[1]: Nothing to be done for 'all-am'.
make[1]: Leaving directory '/home/matlab/portspoo'
root@sjt516scope051:/home/matlab/portspoo# make install
Making install in src
make[1]: Entering directory '/home/matlab/portspoo/src'
make[2]: Entering directory '/home/matlab/portspoo/src'
test -z "/usr/local/bin" || /bin/mkdir -p "/usr/local/bin"
/usr/bin/install -c portspoo '/usr/local/bin'
make[2]: Nothing to be done for 'install-data-am'.
make[2]: Leaving directory '/home/matlab/portspoo/src'
make[1]: Leaving directory '/home/matlab/portspoo/src'
Making install in tools
make[1]: Entering directory '/home/matlab/portspoo/tools'
make[2]: Entering directory '/home/matlab/portspoo/tools'
test -z "/usr/local/etc" || /bin/mkdir -p "/usr/local/etc"
/usr/bin/install -c -m 644 portspoo.conf portspoo_signatures '/usr/local/etc'
make[2]: Nothing to be done for 'install-data-am'.
make[2]: Leaving directory '/home/matlab/portspoo/tools'
make[1]: Leaving directory '/home/matlab/portspoo/tools'
make[1]: Entering directory '/home/matlab/portspoo'
make[2]: Entering directory '/home/matlab/portspoo'
make[2]: Nothing to be done for 'install-exec-am'.
make[2]: Nothing to be done for 'install-data-am'.
make[2]: Leaving directory '/home/matlab/portspoo'
make[1]: Leaving directory '/home/matlab/portspoo'
root@sjt516scope051:/home/matlab/portspoo#
```

\$ iptables -t nat -A PREROUTING -i eth0 -p tcp -m tcp -m multiport --dports 1:21,23:79,8

```
Activities Terminal Mar 21 12:57
root@sjt516scope051: /home/matlab/portspoo

root@sjt516scope051: /home/matlab/portspoo x matlab@sjt516scope051: ~

root@sjt516scope051:/home/matlab/portspoo# iptables -t nat -A PREROUTING -i eth0 -p tcp -m tcp -m multiport --dports 1:21,23:79,8
root@sjt516scope051:/home/matlab/portspoo#
```

\$portspooft -c /usr/local/etc/portspooft.conf -s /usr/local/etc/portspooft\_signatures

```
Activities Terminal Mar 21 13:10
root@sjt516scope051: /usr/local/etc
root@sjt516scope051: /usr/local/etc# portspooft -c /usr/local/etc/portspooft.conf -s /usr/local/etc/portspooft_signatures
-> Using user defined configuration file /usr/local/etc/portspooft.conf
-> Using user defined signature file /usr/local/etc/portspooft_signatures
```

```
Activities Terminal Mar 21 13:13
matlab@sjt516scope051: ~
root@sjt516scope051: /usr/local/etc
matlab@sjt516scope051:~$ nmap 10.30.161.61
Starting Nmap 7.80 ( https://nmap.org ) at 2022-03-21 13:13 IST
Nmap scan report for sjt516scope051 (10.30.161.61)
Host is up (0.000095s latency).
Not shown: 994 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
53/tcp    open  domain
80/tcp    open  http
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
4444/tcp  open  krb524

Nmap done: 1 IP address (1 host up) scanned in 0.05 seconds
matlab@sjt516scope051:~$
```