Andrew Ma

Lab 11 Part 1

CPE 435

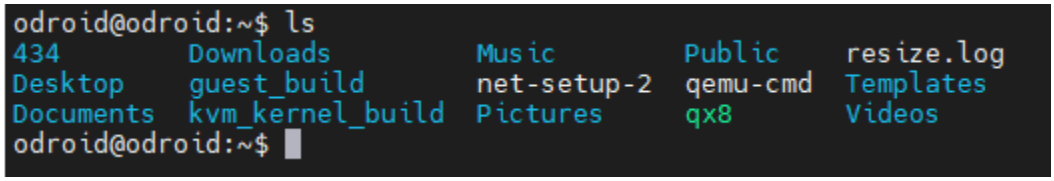
3/29/21

Observations and Answers

Subtask 1

2. echo=172.21.0.6
HOST: odroid50=172.22.4.50

3.



Subtask 2

4. A virtual bridge behaves like a virtual network switch, and it forwards packets between interfaces connected to it.

```
odroid@odroid:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 00:1e:06:32:c7:df
          inet addr:172.22.4.50  Bcast:172.22.255.255  Mask:255.255.0.0
          inet6 addr: fe80::21e:6ff:fe32:c7df/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:7991548 errors:0 dropped:8 overruns:0 frame:0
          TX packets:6506470 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:1490099070 (1.4 GB)  TX bytes:2398144701 (2.3 GB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:352 errors:0 dropped:0 overruns:0 frame:0
          TX packets:352 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1
          RX bytes:41242 (41.2 KB)  TX bytes:41242 (41.2 KB)

tap1      Link encap:Ethernet  HWaddr fe:b5:6d:05:3f:13
          inet6 addr: fe80::fcb5:6dff:fe05:3f13/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:73852 errors:0 dropped:0 overruns:0 frame:0
          TX packets:98304 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:5052105 (5.0 MB)  TX bytes:91847944 (91.8 MB)

virbr0    Link encap:Ethernet  HWaddr fe:b5:6d:05:3f:13
          inet addr:192.168.5.1  Bcast:192.168.5.255  Mask:255.255.255.0
          inet6 addr: fe80::d07c:b6ff:fe2e:e098/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:73852 errors:0 dropped:0 overruns:0 frame:0
          TX packets:61082 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:4018177 (4.0 MB)  TX bytes:89299902 (89.2 MB)
```

5. KVM stands for Kernel-based Virtual Machine, and it is a virtualization module in the Linux kernel that allows the kernel to function as a hypervisor. QEMU is an open source machine emulator and virtualizer that can perform hardware virtualization. QEMU emulates a machine's processor through dynamic binary translation and provides a set of different hardware and device models for the machine.

6.

```
odroid@odroid:~$ ps -aux | grep qemu
root      1659  0.0  0.1   6640  2728 ?        S    Mar11   0:00 sudo /usr/local
/bin/qemu-run
root      1701  0.0  0.0   4124   572 ?        S    Mar11   0:00 /bin/bash -x /u
sr/local/bin/qemu-run
root      1705  1.0 27.2 1280804 555716 ?      Sl   Mar11 318:23 /usr/bin/qemu-s
ystem-arm -M vexpress-a15 -smp 2 -cpu host -enable-kvm -m 512 -kernel /home/odro
id/guest_build/zImage -dtb /home/odroid/guest_build/vexpress-v2p-ca15-tc1.dtb -d
rive file=/home/odroid/guest_build/ubuntu-minimal-16.04.3.img,id=virtio-blk,if=n
one,format=raw -device virtio-blk-device,drive=virtio-blk -net nic -net bridge,b
r=virbr0 -append console=tty1 root=/dev/vda rw rootwait fsck.repair=yes
odroid   13904  0.0  0.0   4020   576 pts/1    S+   04:23   0:00 grep --color=au
to qemu
odroid@odroid:~$
```

root 1659 0.0 0.1 6640 2728 ? S Mar11 0:00 sudo /usr/local/bin/qemu-run
root 1701 0.0 0.0 4124 572 ? S Mar11 0:00 /bin/bash -x /usr/local/bin/qemu-run
root 1705 1.0 27.2 1280804 555716 ? Sl Mar11 318:23 /usr/bin/qemu-system-arm -M vexpress-a15 -smp 2 -cpu host -enable-kvm -m 512 -kernel /home/odroid/guest_build/zImage -dtb /home/odroid/guest_build/vexpress-v2p-ca15-tc1.dtb -drive file=/home/odroid/guest_build/ubuntu-minimal-16.04.3.img,id=virtio-blk,if=none,format=raw -device virtio-blk-device,drive=virtio-blk -net nic -net bridge,br=virbr0 -append console=tty1 root=/dev/vda rw rootwait fsck.repair=yes
odroid 13904 0.0 0.0 4020 576 pts/1 S+ 04:23 0:00 grep --color=auto qemu

7. sudo nmap -vvv -oA virbr0_scan -n -T5 -F -e virbr0 192.168.0.0/16

```
Initiating SYN Stealth Scan at 05:22
Scanning 192.168.5.2 [100 ports]
Discovered open port 22/tcp on 192.168.5.2
Warning: 192.168.5.2 giving up on port because retransmission cap hit (2).
Completed SYN Stealth Scan at 05:23, 2.37s elapsed (100 total ports)
Nmap scan report for 192.168.5.2
Host is up, received arp-response (0.0053s latency).
Scanned at 2021-04-01 04:40:29 UTC for 2553s
Not shown: 99 closed ports
Reason: 99 resets
PORT   STATE SERVICE REASON
22/tcp open  ssh     syn-ack ttl 64
MAC Address: 52:54:00:12:34:56 (QEMU virtual NIC)

Read data files from: /usr/bin/../share/nmap
Nmap done: 65536 IP addresses (1 host up) scanned in 2552.94 seconds
           Raw packets sent: 131309 (3.680MB) | Rcvd: 171 (6.584KB)
odroid@odroid:~$
```

8. Guest=192.168.5.2. Port 22 is open

```
odroid@odroid:~$ ssh root@192.168.5.2
root@192.168.5.2's password:
Welcome to Ubuntu 16.04.3 LTS (GNU/Linux 4.13.0 armv7l)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage
Last login: Fri Apr  6 17:03:22 2018 from 192.168.5.1
root@odroid:~#
```

Ports that are open in the machine: 53, 22

```
root@odroid:~# netstat -tulpn
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
PID/Program name
tcp        0      0 127.0.1.1:53            0.0.0.0:*               LISTEN
1460/dnsmasq
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN
1411/sshd
udp        0      0 0.0.0.0:46607           0.0.0.0:*
1460/dnsmasq
udp    49280      0 127.0.1.1:53            0.0.0.0:*
1460/dnsmasq
udp        0      0 0.0.0.0:68              0.0.0.0:*
22442/dhclient
```

Subtask 3

9. ssh odroid@172.22.4.50

```
root@odroid:~# ssh odroid@172.22.4.50
The authenticity of host '172.22.4.50 (172.22.4.50)' can't be established.
ECDSA key fingerprint is SHA256:y8aWbqaO8M4v68C46d9fzW37MV3/VtD+ZQbG4hyqAzg.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '172.22.4.50' (ECDSA) to the list of known hosts.
odroid@172.22.4.50's password:
Permission denied, please try again.
odroid@172.22.4.50's password:
Welcome to Ubuntu 16.04.3 LTS (GNU/Linux 4.9.61+ armv7l)
Last login: Thu Apr  1 04:17:41 2021 from 172.22.0.6
```

10.

```
Yes, somewhat like the movie. I am am0165.
~
~
~
~
~
```

11. /home/odroid on 172.22.4.50

```
odroid@odroid:~$ vi inception_host.txt
odroid@odroid:~$ ls
434          guest_build          net-setup-2  qx8          virbr0_scan.gnmap
Desktop      inception_host.txt   Pictures     resize.log   virbr0_scan.nmap
Documents    kvm_kernel_build     Public       Templates    virbr0_scan.xml
Downloads    Music                qemu-cmd     Videos
odroid@odroid:~$ realpath .
/home/odroid
```

12.

```
odroid@odroid:~$ cat inception_host.txt
Yes, somewhat like the movie. I am am0165.
odroid@odroid:~$
```

13. We are back on the Guest

```
root@odroid:~# ifconfig
eth0      Link encap:Ethernet  HWaddr 52:54:00:12:34:56
          inet addr:192.168.5.2  Bcast:192.168.5.255  Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:245145 errors:0 dropped:0 overruns:0 frame:0
          TX packets:77295 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:99375213 (99.3 MB)  TX bytes:5323506 (5.3 MB)
          Interrupt:36

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:611 errors:0 dropped:0 overruns:0 frame:0
          TX packets:611 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:45652 (45.6 KB)  TX bytes:45652 (45.6 KB)
```

14. We are back on the HOST

```
root@odroid:~# exit
logout
Connection to 192.168.5.2 closed.
odroid@odroid:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 00:1e:06:32:c7:df
          inet addr:172.22.4.50  Bcast:172.22.255.255  Mask:255.255.0.0
          inet6 addr: fe80::21e:6ff:fe32:c7df/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:8410280 errors:0 dropped:8 overruns:0 frame:0
          TX packets:7188898 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:1543605476 (1.5 GB)  TX bytes:2976231634 (2.9 GB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:352 errors:0 dropped:0 overruns:0 frame:0
          TX packets:352 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1
          RX bytes:41242 (41.2 KB)  TX bytes:41242 (41.2 KB)

tap1      Link encap:Ethernet  HWaddr fe:b5:6d:05:3f:13
          inet6 addr: fe80::fcb5:6dff:fe05:3f13/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:77340 errors:0 dropped:0 overruns:0 frame:0
          TX packets:252750 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:5329156 (5.3 MB)  TX bytes:104068072 (104.0 MB)

virbr0    Link encap:Ethernet  HWaddr fe:b5:6d:05:3f:13
          inet addr:192.168.5.1  Bcast:192.168.5.255  Mask:255.255.255.0
          inet6 addr: fe80::d07c:b6ff:fe2e:e098/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:77340 errors:0 dropped:0 overruns:0 frame:0
          TX packets:213142 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:4246396 (4.2 MB)  TX bytes:101362198 (101.3 MB)
```

15. Yes I can see the file

```
odroid@odroid:~$ ls
434         guest_build         net-setup-2  qx8          virbr0_scan.gnmap
Desktop     inception_host.txt  Pictures     resize.log   virbr0_scan.nmap
Documents   kvm_kernel_build    Public       Templates    virbr0_scan.xml
Downloads   Music               qemu-cmd     Videos
odroid@odroid:~$ cat inception_host.txt
Yes, somewhat like the movie. I am am0165.
odroid@odroid:~$
```

Subtask 4

16.

```
odroid@odroid:~$ ssh root@192.168.5.2
root@192.168.5.2's password:
Welcome to Ubuntu 16.04.3 LTS (GNU/Linux 4.13.0 armv7l)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage
Last login: Thu Apr  1 04:54:43 2021 from 192.168.5.1
root@odroid:~#
```

Creating new user am0165

```
root@odroid:~# sudo useradd am0165
useradd: failed to reset the lastlog entry of UID 1000: Structure needs cleaning
root@odroid:~# users
```

Setting password for user am0165

```
root@odroid:~# sudo passwd am0165
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
```

17.

```
root@odroid:~# ssh am0165@192.168.5.2
The authenticity of host '192.168.5.2 (192.168.5.2)' can't be established.
ECDSA key fingerprint is SHA256:8jPDHdWRP5h5E+RWHKwcF9xifelzPbTZNKXlt2vTHTw.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '192.168.5.2' (ECDSA) to the list of known hosts.
am0165@192.168.5.2's password:
Welcome to Ubuntu 16.04.3 LTS (GNU/Linux 4.13.0 armv7l)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.


The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.
```

18.

```
$ realpath .
/home/am0165
$ vi inception_secondguest.txt
$
```

```
Hi this is test
~
~
~
~
~
~
~
```

```
$ cat inception_secondguest.txt
Hi this is test
$
```

Subtask 5

21. sudo nmap -vvv -oA eth0_scan -sn -n -T5 -e eth0 172.22.0.0/16

```
Host is up, received arp-response (0.00062s latency).
MAC Address: 00:02:B3:EF:4F:F9 (Intel)
Nmap scan report for 172.22.255.255 [host down, received no-response]
Read data files from: /usr/bin/../share/nmap
Nmap done: 65536 IP addresses (116 hosts up) scanned in 2308.60 seconds
           Raw packets sent: 131077 (3.670MB) | Rcvd: 267 (7.476KB)
odroid@odroid:~$
```

116 hosts are up

22. To make new scan faster, I will only perform new scan on ports that were detected to be Up from last scan

```
odroid@odroid:~$ grep Up eth0_scan.gnmap | wc -l
116
```

```
odroid@odroid:~$ grep Up eth0_scan.gnmap | awk '{print$2}' > eth0_up_hosts.txt
odroid@odroid:~$
```

For IP Address 172.22.255.20
sudo nmap -vvv -n -T5 -e eth0 172.22.255.20

```
Starting Nmap 7.01 ( https://nmap.org ) at 2021-04-01 07:26 UTC
Initiating ARP Ping Scan at 07:26
Scanning 172.22.255.20 [1 port]
Completed ARP Ping Scan at 07:26, 0.22s elapsed (1 total hosts)
Initiating SYN Stealth Scan at 07:26
Scanning 172.22.255.20 [1000 ports]
Discovered open port 80/tcp on 172.22.255.20
Discovered open port 23/tcp on 172.22.255.20
Discovered open port 22/tcp on 172.22.255.20
Warning: 172.22.255.20 giving up on port because retransmission cap hit (2).
Increasing send delay for 172.22.255.20 from 0 to 5 due to 76 out of 189 dropped probes since last increase.
Completed SYN Stealth Scan at 07:26, 10.46s elapsed (1000 total ports)
Nmap scan report for 172.22.255.20
Host is up, received arp-response (0.0038s latency).
Scanned at 2021-04-01 07:26:12 UTC for 10s
Not shown: 989 closed ports
Reason: 989 resets
PORT      STATE    SERVICE           REASON
22/tcp    open     ssh               syn-ack ttl 64
23/tcp    open     telnet            syn-ack ttl 64
80/tcp    open     http              syn-ack ttl 64
458/tcp   filtered appleqtc          no-response
898/tcp   filtered sun-manageconsole no-response
1700/tcp  filtered mps-raft          no-response
1971/tcp  filtered netop-school      no-response
3260/tcp  filtered iscsi             no-response
6001/tcp  filtered X11:1             no-response
9900/tcp  filtered iua               no-response
15742/tcp filtered unknown           no-response
MAC Address: F8:B1:56:72:58:E9 (Dell)

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 10.90 seconds
           Raw packets sent: 2487 (109.412KB) | Rcvd: 1817 (72.688KB)
```

Ports: 22, 23, 80
OS is Linux

For IP Address 172.22.255.19

```
Starting Nmap 7.01 ( https://nmap.org ) at 2021-04-01 07:36 UTC
Initiating ARP Ping Scan at 07:36
Scanning 172.22.255.19 [1 port]
Completed ARP Ping Scan at 07:36, 0.23s elapsed (1 total hosts)
Initiating SYN Stealth Scan at 07:36
Scanning 172.22.255.19 [1000 ports]
Discovered open port 22/tcp on 172.22.255.19
Discovered open port 80/tcp on 172.22.255.19
Discovered open port 23/tcp on 172.22.255.19
Increasing send delay for 172.22.255.19 from 0 to 5 due to 72 out of 179 dropped probes since last increase.
Warning: 172.22.255.19 giving up on port because retransmission cap hit (2).
Completed SYN Stealth Scan at 07:36, 10.48s elapsed (1000 total ports)
Nmap scan report for 172.22.255.19
Host is up, received arp-response (0.0015s latency).
Scanned at 2021-04-01 07:36:41 UTC for 11s
Not shown: 996 closed ports
Reason: 996 resets
PORT     STATE    SERVICE REASON
22/tcp   open     ssh     syn-ack ttl 64
23/tcp   open     telnet  syn-ack ttl 64
80/tcp   open     http    syn-ack ttl 64
3260/tcp filtered iscsi   no-response
MAC Address: F8:B1:56:64:2C:63 (Dell)

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 10.94 seconds
           Raw packets sent: 2466 (108.488KB) | Rcvd: 1863 (74.528KB)
```

Ports: 22, 23, 80
OS is Linux

23.

172.22.255.20

```
odroid@odroid:~$ sudo nmap -vvv -n -T5 -O -e eth0 172.22.255.20

Starting Nmap 7.01 ( https://nmap.org ) at 2021-04-01 07:42 UTC
Initiating ARP Ping Scan at 07:42
Scanning 172.22.255.20 [1 port]
Completed ARP Ping Scan at 07:42, 0.23s elapsed (1 total hosts)
Initiating SYN Stealth Scan at 07:42
Scanning 172.22.255.20 [1000 ports]
Discovered open port 23/tcp on 172.22.255.20
Discovered open port 22/tcp on 172.22.255.20
Discovered open port 80/tcp on 172.22.255.20
Warning: 172.22.255.20 giving up on port because retransmission cap hit (2).
Increasing send delay for 172.22.255.20 from 0 to 5 due to 77 out of 192 dropped probes since last increase.
Completed SYN Stealth Scan at 07:42, 10.24s elapsed (1000 total ports)
Initiating OS detection (try #1) against 172.22.255.20
Retrying OS detection (try #2) against 172.22.255.20
Nmap scan report for 172.22.255.20
Host is up, received arp-response (0.0016s latency).
Scanned at 2021-04-01 07:42:49 UTC for 15s
Not shown: 991 closed ports
Reason: 991 resets
PORT     STATE    SERVICE    REASON
7/tcp    filtered echo       no-response
22/tcp   open     ssh        syn-ack ttl 64
23/tcp   open     telnet     syn-ack ttl 64
80/tcp   open     http       syn-ack ttl 64
616/tcp  filtered sco-sysmgr no-response
1033/tcp filtered netinfo    no-response
1049/tcp filtered td-postman no-response
3260/tcp filtered iscsi      no-response
5357/tcp filtered wsdapi     no-response
MAC Address: F8:B1:56:72:58:E9 (Dell)
OS fingerprint not ideal because: Timing level 5 (Insane) used
Aggressive OS guesses: Linux 3.1 (94%), Linux 3.2 (94%), AXIS 210A or 211 Network Camera (Linux 2.6.17) (94%), HP P2000 G3 NAS device (94%), Android 4.1 (Linux 3.4) (92%), Android 4.1.2 (92%), Andro
id 4.3 (92%), Android 4 (92%), Android 5.0.2 (92%), Android 5.1 (92%)
No exact OS matches for host (test conditions non-ideal).
TCP/IP fingerprint:
SCAN(V=7.01%E=4%D=4/1%OT=22%CT=1%CU=43877%PV=Y%DS=1%DC=D%G=N%M=F8B156%TM=60657988%P=arm-unknown-linux-gnueabihf)
SEQ(SP=101%GCD=1%ISR=10F%TI=Z%CI=Z%TS=7)
OPS(O1=M23C6ST11NW7%O2=M23C6ST11NW7%O3=M23C6NNT11NW7%O4=M23C6ST11NW7%O5=M23C6ST11NW7%O6=M23C6ST11)
WIN(W1=4774%W2=4774%W3=4774%W4=4774%W5=4774%W6=4774)
ECN(R=Y%DF=Y%T=40%W=478C%O=M23C6NNSNW7%CC=Y%Q=)
T1(R=Y%DF=Y%T=40%S=O%A=S+%F=AS%RD=0%Q=)
T2(R=N)
T3(R=N)
T4(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)
T5(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)
T6(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)
T7(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)
U1(R=Y%DF=N%T=40%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)
IE(R=Y%DFI=N%T=40%CD=S)

Uptime guess: 65.519 days (since Mon Jan 25 19:16:15 2021)
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=257 (Good luck!)
IP ID Sequence Generation: All zeros

Read data files from: /usr/bin/../share/nmap
OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 16.48 seconds
           Raw packets sent: 2537 (116.844KB) | Rcvd: 1908 (81.212KB)
```

172.22.255.19

```
odroid@odroid:~$ sudo nmap -vvv -n -T5 -O -e eth0 172.22.255.19

Starting Nmap 7.01 ( https://nmap.org ) at 2021-04-01 07:39 UTC
Initiating ARP Ping Scan at 07:39
Scanning 172.22.255.19 [1 port]
Completed ARP Ping Scan at 07:39, 0.23s elapsed (1 total hosts)
Initiating SYN Stealth Scan at 07:39
Scanning 172.22.255.19 [1000 ports]
Discovered open port 23/tcp on 172.22.255.19
Discovered open port 22/tcp on 172.22.255.19
Discovered open port 80/tcp on 172.22.255.19
Warning: 172.22.255.19 giving up on port because retransmission cap hit (2).
Increasing send delay for 172.22.255.19 from 0 to 5 due to 79 out of 196 dropped probes since last increase.
Completed SYN Stealth Scan at 07:39, 10.26s elapsed (1000 total ports)
Initiating OS detection (try #1) against 172.22.255.19
Retrying OS detection (try #2) against 172.22.255.19
Nmap scan report for 172.22.255.19
Host is up, received arp-response (0.0018s latency).
Scanned at 2021-04-01 07:39:02 UTC for 15s
Not shown: 990 closed ports
Reason: 990 resets
PORT     STATE    SERVICE REASON
22/tcp   open     ssh     syn-ack ttl 64
23/tcp   open     telnet  syn-ack ttl 64
80/tcp   open     http    syn-ack ttl 64
705/tcp  filtered agentx  no-response
1030/tcp filtered iad1    no-response
3260/tcp filtered iscsi   no-response
8333/tcp filtered bitcoin no-response
9415/tcp filtered unknown no-response
25734/tcp filtered unknown no-response
54328/tcp filtered unknown no-response
MAC Address: F8:B1:56:64:2C:63 (Dell)
OS fingerprint not ideal because: Timing level 5 (Insane) used
Aggressive OS guesses: Linux 3.1 (94%), Linux 3.2 (94%), AXIS 210A or 211 Network Camera (Linux 2.6.17) (94%), HP P2000 G3 NAS device (94%), Android 4.1.1 (92%), Android 5.0.2 (92%), Android 5.1 (92
%), Linux 2.6.32 (92%), Linux 3.0 - 3.2 (92%), Linux 3.10 (92%)
No exact OS matches for host (test conditions non-ideal).
TCP/IP fingerprint:
SCAN(V=7.01%E=4%D=4/1%OT=22%CT=1%CU=30720%PV=Y%DS=1%DC=D%G=N%M=F8B156%TM=606578A5%P=arm-unknown-linux-gnueabihf)
SEQ(SP=103%GCD=1%ISR=106%TI=Z%CI=Z%TS=7)
OPS(O1=M23C6ST11NW7%O2=M23C6ST11NW7%O3=M23C6NNT11NW7%O4=M23C6ST11NW7%O5=M23C6ST11NW7%O6=M23C6ST11)
WIN(W1=4774%W2=4774%W3=4774%W4=4774%W5=4774%W6=4774)
ECN(R=Y%DF=Y%T=40%W=478C%O=M23C6NNSNW7%CC=Y%Q=)
T1(R=Y%DF=Y%T=40%S=O%A=S+%F=AS%RD=0%Q=)
T2(R=N)
T3(R=N)
T4(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)
T5(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)
T6(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)
T7(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)
U1(R=Y%DF=N%T=40%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)
IE(R=Y%DFI=N%T=40%CD=S)

Uptime guess: 65.516 days (since Mon Jan 25 19:16:20 2021)
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=259 (Good luck!)
IP ID Sequence Generation: All zeros

Read data files from: /usr/bin/../share/nmap
OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
```

The Real Deal

24. Hydra is a parallelized network login cracker that can attack many protocols. New modules can be added to it. Attackers can use Hydra to gain unauthorized access to systems remotely. Some protocols Hydra supports include SMTP, RDP, Telnet, SSH v1 and v2, LDAP, MS-SQL, MySQL, VNC, FTP, and more. We can pass a userlist or password list for cracking or guessing valid login/password pairs. I won't use hydra for immoral or illegal purposes.

```
root@kali:~# hydra -h
Hydra v7.6 (c)2013 by van Hauser/THC & David Maciejak - for legal purposes only

Syntax: hydra [[[-l LOGIN|-L FILE] [-p PASS|-P FILE]] | [-C FILE]] [-e nsr] [-o FILE] [-t TASKS] [-M FILE [-T TA

Options:
  -R        restore a previous aborted/crashed session
  -S        perform an SSL connect
  -s PORT   if the service is on a different default port, define it here
  -l LOGIN or -L FILE  login with LOGIN name, or load several logins from FILE
  -p PASS  or -P FILE  try password PASS, or load several passwords from FILE
  -x MIN:MAX:CHARSET  password bruteforce generation, type "-x -h" to get help
  -e nsr    try "n" null password, "s" login as pass and/or "r" reversed login
  -u        loop around users, not passwords (effective! implied with -x)
  -C FILE   colon separated "login:pass" format, instead of -L/-P options
  -M FILE   list of servers to be attacked in parallel, one entry per line
  -o FILE   write found login/password pairs to FILE instead of stdout
  -f / -F   exit when a login/pass pair is found (-M: -f per host, -F global)
  -t TASKS  run TASKS number of connects in parallel (per host, default: 16)
  -w / -W TIME  waittime for responses (32s) / between connects per thread
  -4 / -6   prefer IPv4 (default) or IPv6 addresses
  -v / -V / -d  verbose mode / show login+pass for each attempt / debug mode
  -U        service module usage details
  server    the target server (use either this OR the -M option)
  service   the service to crack (see below for supported protocols)
  OPT       some service modules support additional input (-U for module help)

Supported services: asterisk afp cisco cisco-enable cvs firebird ftp ftps http[s]-{head|get} http[s]-{get|post}-

Hydra is a tool to guess/crack valid login/password pairs - usage only allowed
for legal purposes. This tool is licensed under AGPL v3.0.
The newest version is always available at http://www.thc.org/thc-hydra
These services were not compiled in: sapr3 oracle.

Use HYDRA_PROXY_HTTP or HYDRA_PROXY - and if needed HYDRA_PROXY_AUTH - environment for a proxy setup.
E.g.:  % export HYDRA_PROXY=socks5://127.0.0.1:9150 (or socks4:// or connect://)
       % export HYDRA_PROXY_HTTP=http://proxy:8080
       % export HYDRA_PROXY_AUTH=user:pass

Examples:
  hydra -l user -P passlist.txt ftp://192.168.0.1
  hydra -L userlist.txt -p defaultpw imap://192.168.0.1/PLAIN
  hydra -C defaults.txt -6 pop3s://[fe80::2c:31ff:fe12:ac11]:143/TLS:DIGEST-MD5
```

25.

```
-bash-4.2$ ssh odroid@172.22.4.50
odroid@172.22.4.50's password:
Welcome to Ubuntu 16.04.3 LTS (GNU/Linux 4.9.61+ armv7l)
Last login: Thu Apr  1 06:14:22 2021 from 192.168.5.2
odroid@odroid:~$
```

26. We could use a password wordlist and bruteforce since we have the username. Or we can find a vulnerability in SSH.

27.

```
odroid@odroid:~$ cat password.txt
a
b
c
d
e
f
g
h
i
j
odroid
odroid@odroid:~$
```

28.

```
odroid@odroid:~$ hydra -l am0165 -P password.txt ssh://192.168.5.2 -s 22
Hydra v8.1 (c) 2014 by van Hauser/THC - Please do not use in military or secret
service organizations, or for illegal purposes.

Hydra (http://www.thc.org/thc-hydra) starting at 2021-04-01 08:01:01
[WARNING] Many SSH configurations limit the number of parallel tasks, it is reco
mmended to reduce the tasks: use -t 4
[DATA] max 11 tasks per 1 server, overall 64 tasks, 11 login tries (l:1/p:11), ~
0 tries per task
[DATA] attacking service ssh on port 22
[22][ssh] host: 192.168.5.2   login: am0165   password: odroid
1 of 1 target successfully completed, 1 valid password found
Hydra (http://www.thc.org/thc-hydra) finished at 2021-04-01 08:01:12
odroid@odroid:~$
```

```
odroid@odroid:~$ ssh am0165@192.168.5.2
am0165@192.168.5.2's password:
Welcome to Ubuntu 16.04.3 LTS (GNU/Linux 4.13.0 armv7l)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage
Last login: Thu Apr  1 06:23:38 2021 from 192.168.5.2
$
```

29.

```
odroid@odroid:~$ hydra -l root -P password.txt ssh://192.168.5.2 -s 22
Hydra v8.1 (c) 2014 by van Hauser/THC - Please do not use in military or secret
service organizations, or for illegal purposes.

Hydra (http://www.thc.org/thc-hydra) starting at 2021-04-01 08:01:44
[WARNING] Many SSH configurations limit the number of parallel tasks, it is reco
mmended to reduce the tasks: use -t 4
[DATA] max 11 tasks per 1 server, overall 64 tasks, 11 login tries (l:1/p:11), ~
0 tries per task
[DATA] attacking service ssh on port 22
[22][ssh] host: 192.168.5.2   login: root   password: odroid
```

30.
```
odroid@odroid:~$ ssh root@192.168.5.2
root@192.168.5.2's password:
Welcome to Ubuntu 16.04.3 LTS (GNU/Linux 4.13.0 armv7l)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage
Last login: Thu Apr  1 06:18:59 2021 from 192.168.5.1
root@odroid:~#
```

31.
```
odroid@odroid:~$ exit
logout
Connection to 172.22.4.50 closed.
-bash-4.2$
```

32.
```
-bash-4.2$ vim password.txt
-bash-4.2$ cat password.txt
a
b
c
d
e
f
g
h
i
j
yslavrin
-bash-4.2$
```

Hydra wasn't part of path, so I had to find hydra program

```
-bash-4.2$ find / -name hydra -type f 2>/dev/null
/export/odroid/odroid21/usr/bin/hydra
/export/odroid/odroid48/usr/bin/hydra
/export/odroid/odroid64/usr/bin/hydra
/export/odroid/odroid33/usr/bin/hydra
^C
```

But the problem is each of these binaries were compiled with ARM

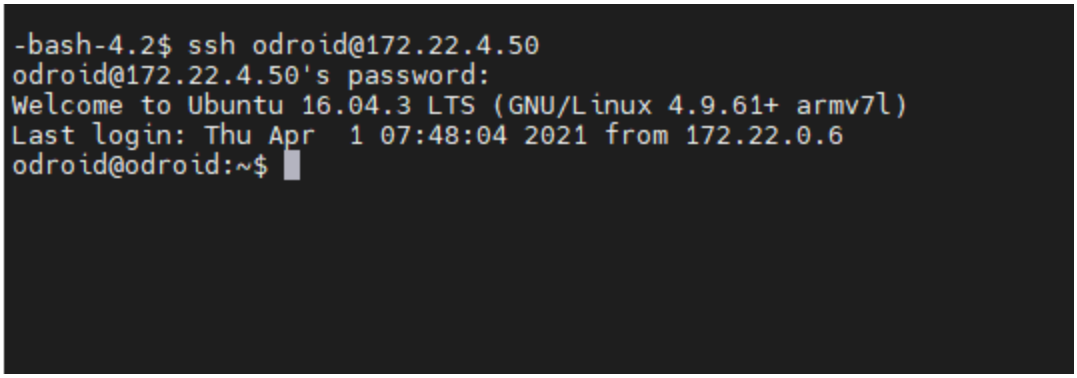
```
-bash-4.2$ /export/odroid/odroid81/usr/bin/hydra
/lib/ld-linux-armhf.so.3: No such file or directory
-bash-4.2$
```

So I had to download from https://github.com/vanhauser-thc/thc-hydra

Then run ./configure; make

But, I couldn't install the libssh libraries needed for ssh

```
-bash-4.2$ hydra -l odroid -P password.txt ssh://172.22.4.50 -s 22
bash: hydra: command not found...
-bash-4.2$
```

33. 
-bash-4.2$ ssh odroid@172.22.4.50
odroid@172.22.4.50's password:
Welcome to Ubuntu 16.04.3 LTS (GNU/Linux 4.9.61+ armv7l)
Last login: Thu Apr 1 07:48:04 2021 from 172.22.0.6
odroid@odroid:~$