Internetworking exercise

Offensive Technologies 2021
Matteo Franzil <matteo.franzil+github@gmail.com>

December 11, 2021

1 Solution

This exercise was solved as the following. First, I inspected the created nodes from the web interface:

```
pc162 NWworkstation1 pc3060 Ubuntu-EDU up [...]
pc177 NWrouter pc3060 Ubuntu-EDU up [...]
pc179 ISrouter pc3060 Ubuntu-EDU up [...]
pc181 SWrouter pc3060 Ubuntu-EDU up [...]
pc201 SWworkstation1 pc3060 Ubuntu-EDU up [...]
```

Code 1 Code found in the DeterLAB web interface.

The grey names are the names of the nodes of the experiment in which we're going to install our network configuration.

Second, I ssh-ed into the control plane and uploaded the script file (`working-demo.sh`). The script file was written by combining data from the exercise page on DeterLAB (https://www.isi.deterlab.net/file.php?file=/share/shared/Internetworking), which provides network configuration information step-by-step, into a single, whole file. Indeed, the first time I executed the exercise, I first did it step by step, but kept the executed commands and then condensed it into the script.

First, the script pings `/share/shared/Internetworking/showcabling` in order to retrieve the configuration set up by DeterLAB (the so known "wired connections):

```
$ /share/shared/Internetworking/showcabling Franzil-Iworking offtech

NWworkstation1 eth5 <- is "wired" to -> NWrouter eth5
NWrouter eth3 <- is "wired" to -> ISrouter eth2
ISrouter eth1 <- is "wired" to -> SWrouter eth5
SWworkstation1 eth3 <- is "wired" to -> SWrouter eth3
```

Code 2 Obtaining the network cabling setup.

These are then filtered and saved as PATH variables in order to keep them at hand.

Then, I chose some subnets to apply to the nodes. This is the network I obtained:

```
 NW-workstation
       | .1
[10.0.100.0/28]
       | .2
      NW-r
       | .1
[2.0.100.0/28]
       | .2
```

```
     IS-r
      | .1
[3.0.100.0/28]
      | .2
     SW-r
      | .1
[10.0.400.1/28]
      | .2
 SW-workstation
```

Code 3 Simplified diagram of the network.

Only `.1` and `.2` IPs were assigned, with the logic that southbound (i.e. facing south on the DeterLAB exercise page and in the above diagram) interfaces would get `.1`, northbound interfaces would get `.2`. So as an example, the northwest workstation has a single southbound interface, and is thus numbered `10.0.100.1`. This is also reflected in the script by the interface names saved in the variables.

Then, the script proceeds to apply the network configuration as required the exercise (IP addresses; routing; blocking of private addresses; NAT; port-forwarding). I decided to use the newer `ip` commands instead of the `ifconfig` ones as it is now recommended to use the formers.

For five times, the script saves the configuration to a `sh` file and, using the ability to share the home folder between DeterLAB nodes, does an `ssh` to each machine and applies it as a superuser (thus avoiding a sudo for each command).

2 Example outputs

This section contains some example outputs presented during the execution of the exercise. For example, this is what happens when pinging the two workstation with private address blocking enabled:

```
root@nwrouter:~# tcpdump -nnti eth3 icmp
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth3, link-type EN10MB (Ethernet), capture size 262144 bytes
IP 10.0.100.1 > 10.4.100.2: ICMP echo request, id 17109, seq 51, length 64
IP 10.0.100.1 > 10.4.100.2: ICMP echo request, id 17109, seq 52, length 64
IP 10.0.100.1 > 10.4.100.2: ICMP echo request, id 17109, seq 53, length 64
IP 10.0.100.1 > 10.4.100.2: ICMP echo request, id 17109, seq 54, length 64
```

Code 4 TCPdump with private address blocking.

On the other hand, this is when NAT is enabled and the workstations ping each other using their router's IP:

```
IP 2.0.100.1 > 3.0.100.2: ICMP echo request, id 19365, seq 391, length 64
IP 3.0.100.2 > 2.0.100.1: ICMP echo reply, id 19365, seq 391, length 64
IP 2.0.100.1 > 3.0.100.2: ICMP echo request, id 19365, seq 392, length 64
IP 3.0.100.2 > 2.0.100.1: ICMP echo reply, id 19365, seq 392, length 64
IP 2.0.100.1 > 3.0.100.2: ICMP echo request, id 19365, seq 393, length 64
IP 3.0.100.2 > 2.0.100.1: ICMP echo reply, id 19365, seq 393, length 64
```

Code 5 Pinging each other with NAT.

Furthermore, some screenshots are included in the next pages.

```
root@swworkstation1:~# ip r
default via 192.168.1.254 dev eth4 proto dhcp src 192.168.1.201 metric 1024
2.0.100.0/28 via 10.4.100.1 dev eth3
3.0.100.0/28 via 10.4.100.1 dev eth3
10.0.100.0/28 via 10.4.100.1 dev eth3
10.4.100.0/28 dev eth3 proto kernel scope link src 10.4.100.2
192.168.0.0/22 dev eth4 proto kernel scope link src 192.168.1.201
192.168.1.254 dev eth4 proto dhcp scope link src 192.168.1.201 metric 1024
root@swworkstation1:~# ping 10.4.100.1
PING 10.4.100.1 (10.4.100.1) 56(84) bytes of data.
64 bytes from 10.4.100.1: icmp_seq=1 ttl=64 time=0.332 ms
64 bytes from 10.4.100.1: icmp_seq=2 ttl=64 time=0.382 ms
^C
--- 10.4.100.1 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1007ms
rtt min/avg/max/mdev = 0.332/0.357/0.382/0.025 ms
root@swworkstation1:~# ping 3.0.100.1
PING 3.0.100.1 (3.0.100.1) 56(84) bytes of data.
64 bytes from 3.0.100.1: icmp_seq=1 ttl=63 time=0.610 ms
64 bytes from 3.0.100.1: icmp_seq=2 ttl=63 time=0.520 ms
^C
--- 3.0.100.1 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1023ms
rtt min/avg/max/mdev = 0.520/0.565/0.610/0.045 ms
root@swworkstation1:~# ping 2.0.100.
ping: 2.0.100.: Name or service not known
root@swworkstation1:~# ping 2.0.100.1
PING 2.0.100.1 (2.0.100.1) 56(84) bytes of data.
64 bytes from 2.0.100.1: icmp_seq=1 ttl=62 time=1.35 ms
64 bytes from 2.0.100.1: icmp_seq=2 ttl=62 time=1.01 ms
^C
--- 2.0.100.1 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1001ms
rtt min/avg/max/mdev = 1.017/1.188/1.359/0.171 ms
root@swworkstation1:~# ping 10.0.100.1
PING 10.0.100.1 (10.0.100.1) 56(84) bytes of data.
64 bytes from 10.0.100.1: icmp_seq=1 ttl=62 time=1.23 ms
64 bytes from 10.0.100.1: icmp_seq=2 ttl=62 time=1.27 ms
^C
--- 10.0.100.1 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1001ms
rtt min/avg/max/mdev = 1.238/1.257/1.277/0.040 ms
root@swworkstation1:~# ping 10.0.100.1
PING 10.0.100.1 (10.0.100.1) 56(84) bytes of data.
```

Figure 1 Example of pings passing through to all other four machines from the southwest workstation.

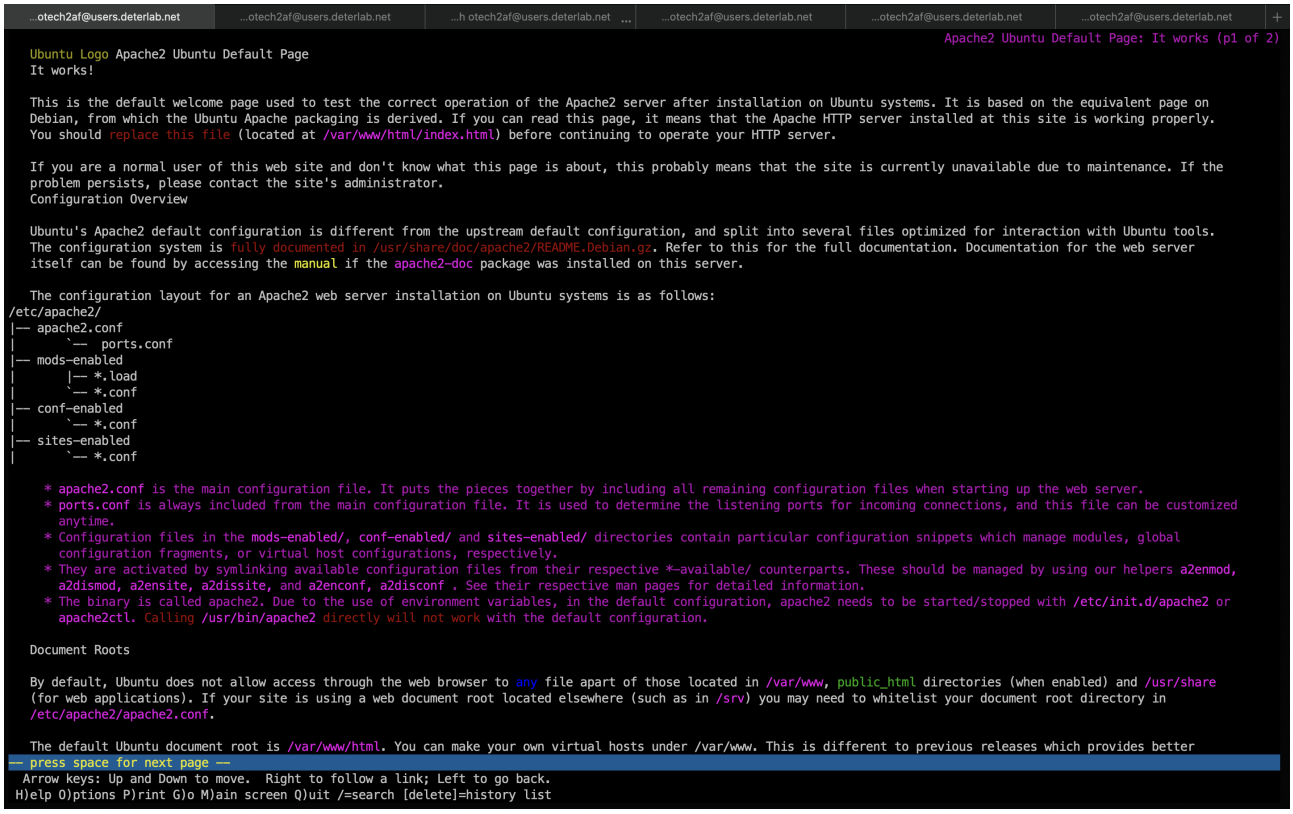

Figure 2 Final result of the exercise, yielding the Apache web server visualized with the Lynx web browser.

```
root@swrouter:~# tcpdump -nnti eth5
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth5, link-type EN10MB (Ethernet), capture size 262144 bytes
LLDP, length 232: EHP18e
IP 2.0.100.1.43028 > 3.0.100.2.80: Flags [S], seq 1725720234, win 64240, options [mss 1460,sackOK,TS val 943619465 ecr 0,nop,wscale 7], length 0
IP 3.0.100.2.80 > 2.0.100.1.43028: Flags [S.], seq 3207567789, ack 1725720235, win 65160, options [mss 1460,sackOK,TS val 3724135591 ecr 943619465,nop,wscale 7], length 0
IP 2.0.100.1.43028 > 3.0.100.2.80: Flags [.], ack 1, win 502, options [nop,nop,TS val 943619467 ecr 3724135591], length 0
IP 2.0.100.1.43028 > 3.0.100.2.80: Flags [P.], seq 1:256, ack 1, win 502, options [nop,nop,TS val 943619467 ecr 3724135591], length 255: HTTP: GET / HTTP/1.0
IP 3.0.100.2.80 > 2.0.100.1.43028: Flags [.], ack 256, win 508, options [nop,nop,TS val 3724135593 ecr 943619467], length 0
IP 3.0.100.2.80 > 2.0.100.1.43028: Flags [P.], seq 1:3441, ack 256, win 508, options [nop,nop,TS val 3724135594 ecr 943619467], length 3440: HTTP: HTTP/1.1 200 OK
IP 3.0.100.2.80 > 2.0.100.1.43028: Flags [F.], seq 3441, ack 256, win 508, options [nop,nop,TS val 3724135595 ecr 943619467], length 0
IP 2.0.100.1.43028 > 3.0.100.2.80: Flags [.], ack 1449, win 501, options [nop,nop,TS val 943619471 ecr 3724135594], length 0
IP 2.0.100.1.43028 > 3.0.100.2.80: Flags [.], ack 2897, win 501, options [nop,nop,TS val 943619471 ecr 3724135594], length 0
IP 2.0.100.1.43028 > 3.0.100.2.80: Flags [.], ack 3441, win 497, options [nop,nop,TS val 943619472 ecr 3724135594], length 0
IP 2.0.100.1.43028 > 3.0.100.2.80: Flags [F.], seq 256, ack 3442, win 501, options [nop,nop,TS val 943619473 ecr 3724135595], length 0
IP 3.0.100.2.80 > 2.0.100.1.43028: Flags [.], ack 257, win 508, options [nop,nop,TS val 3724135598 ecr 943619473], length 0
```

Figure 3 TCPdump result of the Lynx-Apache connection.