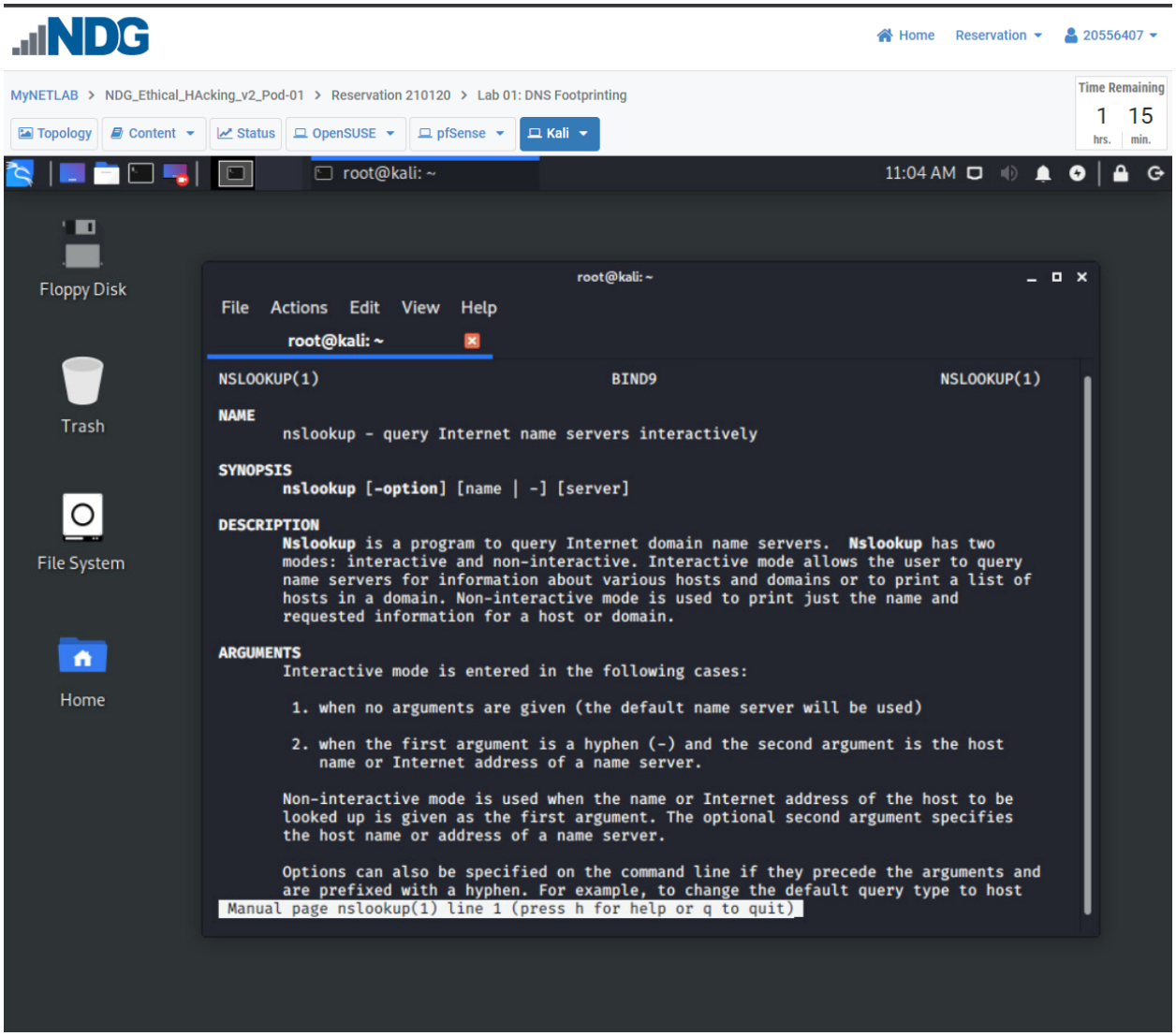
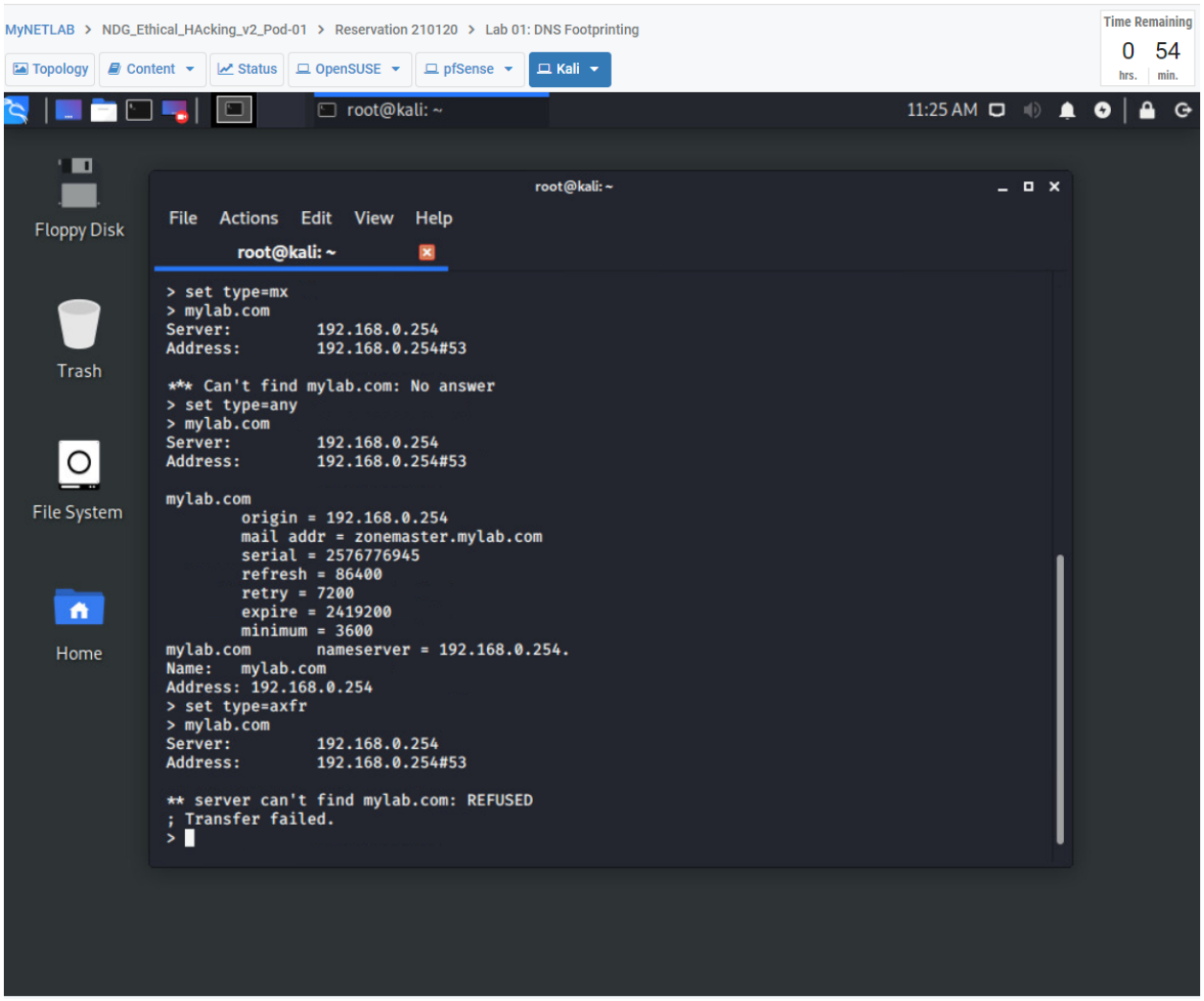
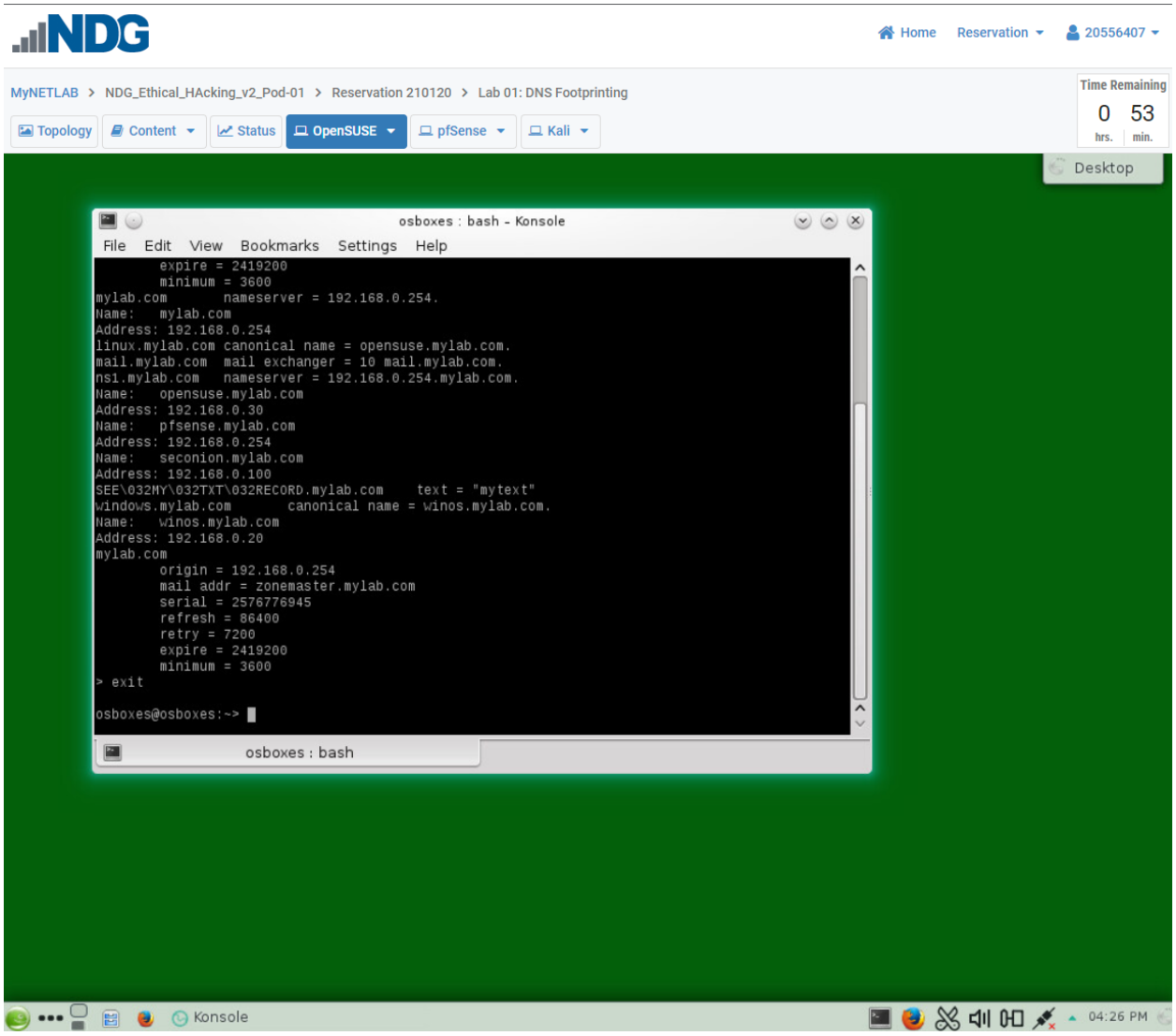
Jason Palmeri
CS53C
Lab 01
Timothy Ryan

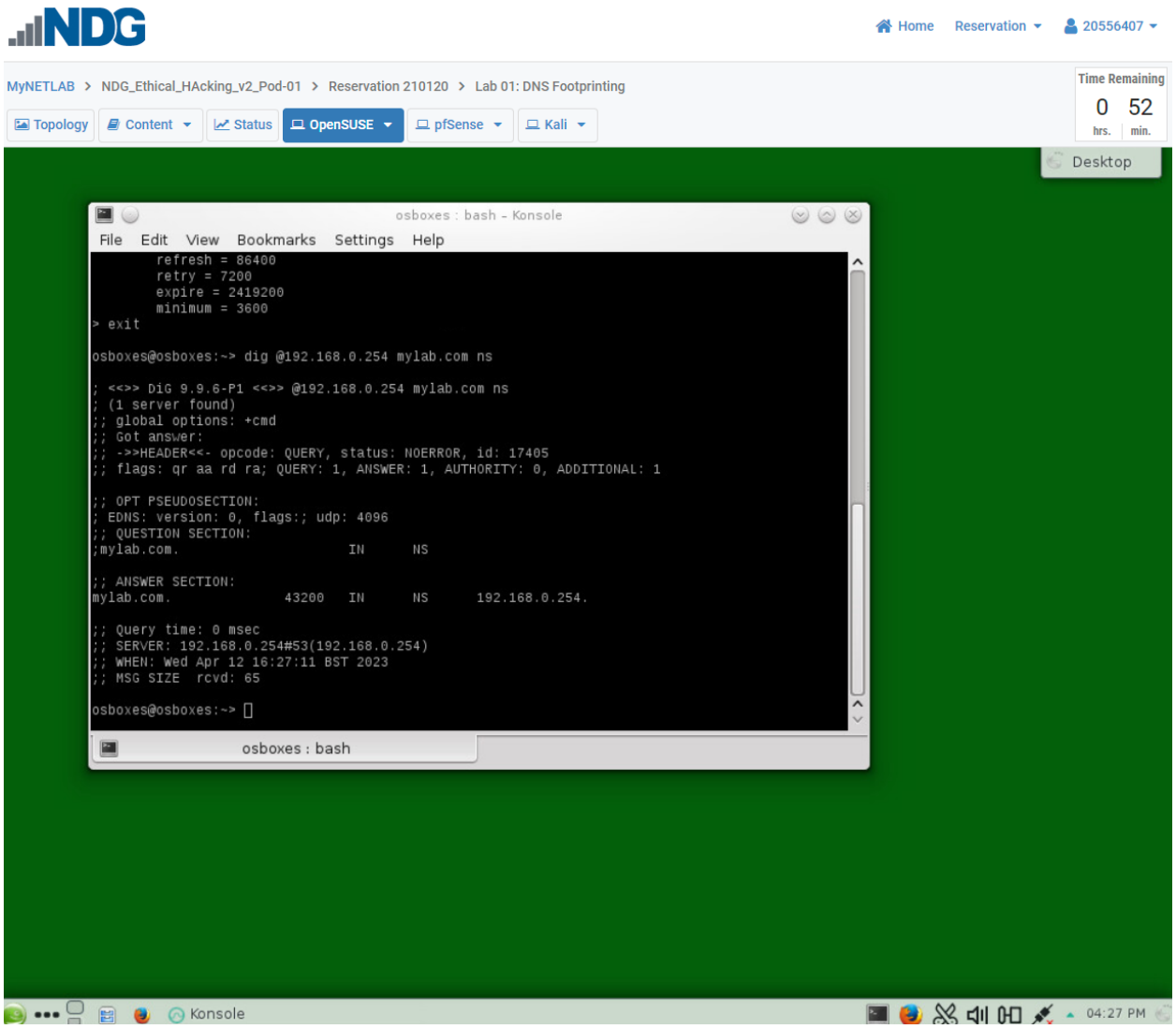
Lab 01: DNS Footprinting

1. Footprinting using nslookup




MyNETLAB > NDG_Ethical_HAcking_v2_Pod-01 > Reservation 210120 > Lab 01: DNS Footprinting
Time Remaining
0 hrs. 54 min.
Topology
Content
Status
OpenSUSE
pfSense
Kali
root@kali: ~
11:25 AM
Floppy Disk
Trash
File System
Home
root@kali: ~
File Actions Edit View Help
root@kali: ~
> set type=mx
> mylab.com
Server: 192.168.0.254
Address: 192.168.0.254#53
** Can't find mylab.com: No answer
> set type=any
> mylab.com
Server: 192.168.0.254
Address: 192.168.0.254#53
mylab.com
origin = 192.168.0.254
mail addr = zonemaster.mylab.com
serial = 2576776945
refresh = 86400
retry = 7200
expire = 2419200
minimum = 3600
mylab.com nameserver = 192.168.0.254.
Name: mylab.com
Address: 192.168.0.254
> set type=axfr
> mylab.com
Server: 192.168.0.254
Address: 192.168.0.254#53
** server can't find mylab.com: REFUSED
; Transfer failed.
>


NDG
Home
Reservation
20556407
MyNETLAB > NDG_Ethical_HAcking_v2_Pod-01 > Reservation 210120 > Lab 01: DNS Footprinting
Time Remaining
0 hrs. 53 min.
Topology
Content
Status
OpenSUSE
pfSense
Kali
Desktop
osboxes : bash - Konsole
File Edit View Bookmarks Settings Help
expire = 2419200
minimum = 3600
mylab.com nameserver = 192.168.0.254.
Name: mylab.com
Address: 192.168.0.254
linux.mylab.com canonical name = opensuse.mylab.com.
mail.mylab.com mail exchanger = 10 mail.mylab.com.
ns1.mylab.com nameserver = 192.168.0.254.mylab.com.
Name: opensuse.mylab.com
Address: 192.168.0.30
Name: pfsense.mylab.com
Address: 192.168.0.254
Name: seconion.mylab.com
Address: 192.168.0.100
SEE\032MY\032TXT\032RECORD.mylab.com text = "mytext"
windows.mylab.com canonical name = winos.mylab.com.
Name: winos.mylab.com
Address: 192.168.0.20
mylab.com
origin = 192.168.0.254
mail addr = zonemaster.mylab.com
serial = 2576776945
refresh = 86400
retry = 7200
expire = 2419200
minimum = 3600
> exit
osboxes@osboxes:~>
osboxes : bash
Konsole
04:26 PM


NDG
Home
Reservation
20556407
MyNETLAB > NDG_Ethical_HAcking_v2_Pod-01 > Reservation 210120 > Lab 01: DNS Footprinting
Time Remaining
0 hrs.
52 min.
Topology
Content
Status
OpenSUSE
pfSense
Kali
Desktop
osboxes : bash - Konsole
File Edit View Bookmarks Settings Help
refresh = 86400
retry = 7200
expire = 2419200
minimum = 3600
> exit
osboxes@osboxes:~> dig @192.168.0.254 mylab.com ns
; <<>> DiG 9.9.6-P1 <<>> @192.168.0.254 mylab.com ns
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 17405
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1
;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;mylab.com. IN NS
;; ANSWER SECTION:
mylab.com. 43200 IN NS 192.168.0.254.
;; Query time: 0 msec
;; SERVER: 192.168.0.254#53(192.168.0.254)
;; WHEN: Wed Apr 12 16:27:11 BST 2023
;; MSG SIZE rcvd: 65
osboxes@osboxes:~>
osboxes : bash
Konsole
04:27 PM