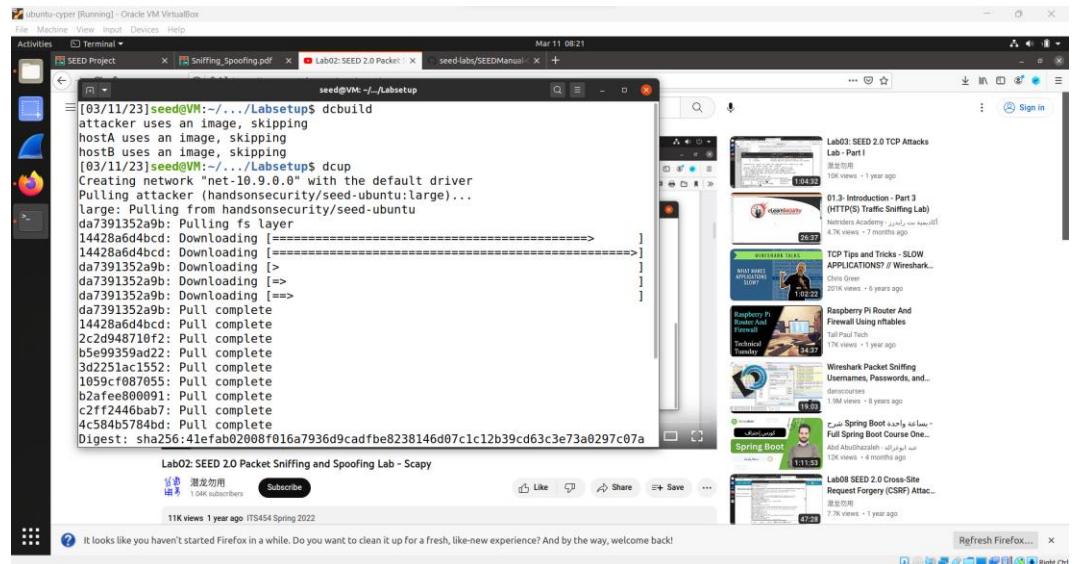


Lab 1- Sniffing and Spoofing Lab

Name: Hamza Abdellah Ahmed

ID: 18P7231

Container Setup and Commands

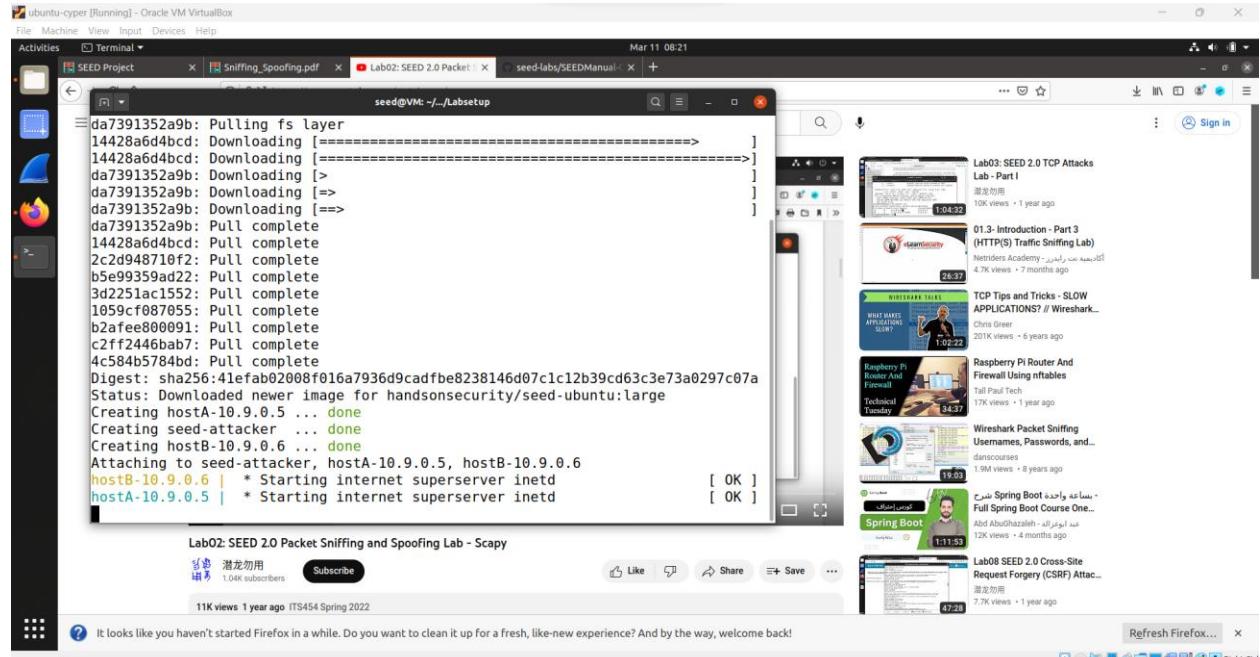


```
[03/11/23]seed@VM:~/.../Labsetup$ dcbuild
attacker uses an image, skipping
hostA uses an image, skipping
hostB uses an image, skipping
[03/11/23]seed@VM:~/.../Labsetup$ dcup
Creating hostA "net-10.9.0.0" with the default driver
Pulling attacker (handsongsecurity/seed-ubuntu:large)...
large: Pulling from handsongsecurity/seed-ubuntu
da7391352a9b: Pulling fs layer
14428a6d4bcd: Downloading [=====]
14428a6d4bcd: Downloading [=====]
da7391352a9b: Downloading [>]
da7391352a9b: Downloading [=]
da7391352a9b: Pull complete
14428a6d4bcd: Pull complete
2c2d948710f2: Pull complete
b5e99359ad22: Pull complete
3d2251ac1552: Pull complete
1059cf087055: Pull complete
b2afee800091: Pull complete
c2ff2446bab7: Pull complete
4c584b5784bd: Pull complete
Digest: sha256:41efab02008f016a7936d9cadfbe8238146d07c1c12b39cd63c3e73a0297c07a

Lab02: SEED 2.0 Packet Sniffing and Spoofing Lab - Scapy
[...]
11K views 1 year ago IT5454 Spring 2022

It looks like you haven't started Firefox in a while. Do you want to clean it up for a fresh, like-new experience? And by the way, welcome back!
```

About the Attacker Container



```
da7391352a9b: Pulling fs layer
14428a6d4bcd: Downloading [=====]
14428a6d4bcd: Downloading [=====]
da7391352a9b: Downloading [>]
da7391352a9b: Downloading [=]
da7391352a9b: Pull complete
14428a6d4bcd: Pull complete
2c2d948710f2: Pull complete
b5e99359ad22: Pull complete
3d2251ac1552: Pull complete
1059cf087055: Pull complete
b2afee800091: Pull complete
c2ff2446bab7: Pull complete
4c584b5784bd: Pull complete
Digest: sha256:41efab02008f016a7936d9cadfbe8238146d07c1c12b39cd63c3e73a0297c07a
Status: Downloaded newer image for handsongsecurity/seed-ubuntu:large
Creating hostA-10.9.0.5 ... done
Creating seed-attacker ... done
Creating hostB-10.9.0.6 ... done
Attaching to seed-attacker, hostA-10.9.0.5, hostB-10.9.0.6
hostB-10.9.0.6 | * Starting internet superserver inetd
hostA-10.9.0.5 | * Starting internet superserver inetd
[ OK ] [ OK ]

Lab02: SEED 2.0 Packet Sniffing and Spoofing Lab - Scapy
[...]
11K views 1 year ago IT5454 Spring 2022

It looks like you haven't started Firefox in a while. Do you want to clean it up for a fresh, like-new experience? And by the way, welcome back!
```

```
[03/11/23]seed@VM:~/.../Labsetup$ dockps  
acc1afee739 seed-attacker  
165df0779116 hostB-10.9.0.6  
0da75f3d2b1d hostA-10.9.0.5  
[03/11/23]seed@VM:~/.../Labsetup$
```

潜龙勿用
1,04K subscribers

```
[03/11/23]seed@VM-1-1:~/Labssetup$ docksh seed-attacker
root@VM-1-1:~# ifconfig
br-48d86189b02b: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
        inet 10.9.0.1 netmask 255.255.255.0 broadcast 10.9.0.255
                inet6 fe80::2e:3fffe:2e0:6e7 prefixlen 64 scopeid 0x20<link>
                    ether 02:42:e3:25:e0:67 txqueuelen 0 (Ethernet)
                    RX packets 0 bytes 0 (0.0 B)
                    RX errors 0 dropped 0 overruns 0 frame 0
                    TX packets 39 bytes 5974 (5.9 KB)
                    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

docker0: flags=4099<UP,BROADCAST,MULTICAST> mtu 1500
        inet 172.17.0.1 netmask 255.255.0.0 broadcast 172.17.255.255
                ether 02:42:ca:6e:26:e6 txqueuelen 0 (Ethernet)
                    RX packets 0 bytes 0 (0.0 B)
                    RX errors 0 dropped 0 overruns 0 frame 0
                    TX packets 0 bytes 0 (0.0 B)
                    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
        inet 10.0.2.5 netmask 255.255.255.0 broadcast 10.0.2.255
                inet6 fe80::f563:88ff:be2c:6a3d prefixlen 64 scopeid 0x20<link>
                    ether 08:00:27:d5:e6:c8 txqueuelen 1000 (Ethernet)
                    RX packets 229009 bytes 330204115 (330.2 MB)
```

11/17/2012 10:30 AM

```

ubuntu-cyber [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities Terminal Mar 11 08:28
SEED Project Sniffing_Spoofing.pdf Lab02: SEED 2.0 Packet seed-labs/SEEDManual...
seed@VM: ~/Labsetup seed@VM: ~/Labsetup seed@VM: ~/Labsetup seed@VM: ~/Labsetup
root@VM: #/ scapy
INFO: Can't import matplotlib. Won't be able to plot.
INFO: Can't import PyX. Won't be able to use psdump() or pdfdump().
INFO: Can't import python-cryptography v1.7+. Disabled WEP decryption/encryption
. (Dot11)
INFO: Can't import python-cryptography v1.7+. Disabled IPsec encryption/authentication.
WARNING: IPython not available. Using standard Python shell instead.
AutoCompletion, History are disabled.

aSPY//YASa
apyyyyCY/////////YCa
sY//////YSpcs scpCY//Pp
ayp ayyyyyySCP//Pp
AYAsAYYYYYYY//Ps
pCCCCY//p
SPPP//a
/A/
p//Ac
P///YCpc
sccccP//pSP//p
sY/////////y caa
cayCayP//Ya

Welcome to Scapy
Version 2.4.4
https://github.com/secdev/scapy

Have fun!
Craft packets day on earth

We are in France, we say Skappee.
OK? Merci.
-- Sebastien Chabal

11,977 views Jan 19, 2022 IT545 Spring 2022

```

It looks like you haven't started Firefox in a while. Do you want to clean it up for a fresh, like-new experience? And by the way, welcome back!

Using Scapy to Sniff and Spoof Packets

```

ubuntu-cyber [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities Terminal Mar 11 08:31
SEED Project Sniffing_Spoofing.pdf Lab02: SEED 2.0 Packet its545/labs/lab02 at master Usage - Scapy 2.5.0.docx seed-labs/SEEDManual...
seed@VM: ~/Labsetup seed@VM: ~/Labsetup seed@VM: ~/Labsetup seed@VM: ~/Labsetup
ccaaCS

>>> a=ip()
Traceback (most recent call last):
  File "<console>", line 1, in <module>
NameError: name 'ip' is not defined
>>> a=IP()
>>> a.show()
###[ IP ]##
version= 4
ihl= None
tos= 0x0
len= None
id= 1
flags=
frag= 0
ttl= 64
proto= hopopt
chksum= None
src= 127.0.0.1
dst= 127.0.0.1
\options\

>>>
11,977 views Jan 19, 2022 IT545 Spring 2022

```

It looks like you haven't started Firefox in a while. Do you want to clean it up for a fresh, like-new experience? And by the way, welcome back!

ubuntu-cyber [Running] - Oracle VM VirtualBox

Activities Terminal Sniffing_Spoofing.pdf Lab02: SEED 2.0 Packet its454/labs/lab02 at master Usage — Scapy 2.5.0. do seed-labs/SEEDManual

```
[seed@VM: ~]# dockps
accdfafee739 seed-attacker
165df0779116 hostB-10.9.0.6
0da75f3d2b1d hostA-10.9.0.5
[seed@VM: ~]# ls
dockercfg volumes
[seed@VM: ~]# cd volumes
[seed@VM: ~]# touch template.py
[seed@VM: ~]# touch start.py
[seed@VM: ~]#
```

ubuntu-cyber [Running] - Oracle VM VirtualBox

Activities Terminal Sniffing_Spoofing.pdf Lab02: SEED 2.0 Packet its454/labs/lab02 at master Usage — Scapy 2.5.0. do seed-labs/SEEDManual

```
>>> exit()
root@VM: ~]# ls
bin dev home lib32 libx32 mnt proc run srv tmp var
boot etc lib lib64 media opt root sbin sys usr volumes
root@VM: ~]# cd volumes
root@VM: /volumes# ls
start.py template.py
root@VM: /volumes# python3 start.py
##[ IP ]##
version = 4
ihl = None
tos = 0x0
len = None
id = 1
flags =
frag = 0
ttl = 64
proto = hopopt
chksum = None
src = 127.0.0.1
dst = 127.0.0.1
\options \
root@VM: /volumes#
```

11,977 views Jan 19, 2022 ITS454 Spring 2022

It looks like you haven't started Firefox in a while. Do you want to clean it up for a fresh, like-new experience? And by the way, welcome back!

ubuntu-cyber [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

Activities Terminal Sniffing_Spoofing.pdf Lab02: SEED 2.0 Packet... its454/labs/lab02 at ma... Usage — Scapy 2.5.0. do... seed-labs/SEEDManual... Mar 11 08:42

```
seed@VM: ~/Labsetup
proto      = hopopt
chksum    = None
src       = 127.0.0.1
dst       = 127.0.0.1
\options   \

root@VM:/volumes# chmod a+x start.py
root@VM:/volumes# ./start.py
###[ IP ]###
version    = 4
ihl       = None
tos       = 0x0
len       = None
id        = 1
flags     =
frag      = 0
ttl       = 64
proto     = hopopt
chksum    = None
src       = 127.0.0.1
dst       = 127.0.0.1
\options   \

root@VM:/volumes#
```

1.04:32

Lab02: SEED 2.0 TCP Attacks
Lab - Part I
10K views • 1 year ago

01.3- Introduction - Part 3
(HTTP(S) Traffic Sniffing Lab)
NetDev Academy - نیت دیو آکادمی
4.7K views • 7 months ago

TCP Tips and Tricks - SLOW
APPLICATIONS? // Wireshark...
Chris Greer
Chris Greer - چریس گریر
20K views • 6 years ago

Raspberry Pi Router And
Firewall Using nftables
Technical Tuesday
Tall Paul Tech
Tall Paul Tech - پال تال
17K views • 1 year ago

Wireshark Packet Sniffing
Usernames, Passwords, and...
anscources
1.9M views • 8 years ago

Spring Boot 2.0 اندروید و سایه -
Full Spring Boot Course One...
Abd AbduGhazaleh - عابد عبد الغزاله
12K views • 4 months ago

Lab08 SEED 2.0 Cross-Site
Request Forgery (CSRF) Attack...
置龙勿用
11,977 views Jan 19, 2022 IT5454 Spring 2022

Like Share Save ...

1.04:32

Refresh Firefox... x

It looks like you haven't started Firefox in a while. Do you want to clean it up for a fresh, like-new experience? And by the way, welcome back!

ubuntu-cyber [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

Activities Terminal task1.py template.py Mar 11 08:47

```
seed@VM: ~/Labsetup
seed@VM: ~/volumes
seed@VM: ~/Labsetup
seed@VM: ~/Labsetup

[03/11/23]seed@VM:~/.../Labsetup$ dockeps
accdlafee739 seed-attacker
165df0779116 hostB-10.9.0.6
0da75f3d2b1d hostA-10.9.0.5

[03/11/23]seed@VM:~/.../Labsetup$ ls
docker-compose.yml volumes

[03/11/23]seed@VM:~/.../Labsetup$ cd volumes
[03/11/23]seed@VM:~/.../volumes$ touch template.py
[03/11/23]seed@VM:~/.../volumes$ touch start.py
[03/11/23]seed@VM:~/.../volumes$ ll
total 8
-rwxrwxr-x 1 seed seed 65 Mar 11 08:38 start.py
-rw-rw-r-- 1 seed seed 687 Mar 11 08:34 template.py
[03/11/23]seed@VM:~/.../volumes$ touch task1.{1..4}.py
[03/11/23]seed@VM:~/.../volumes$ ls
start.py task1.1.py task1.2.py task1.3.py task1.4.py template.py
[03/11/23]seed@VM:~/.../volumes$
```

Python 3 Tab Width: 8 Ln 10, Col 35 INS

ab03: SEED 2.0 TCP Attacks
ab - Part I
10K views • 1 year ago

1.3- Introduction - Part 3
(HTTP(S) Traffic Sniffing Lab)
NetDev Academy - نیت دیو آکادمی
7K views • 7 months ago

TCP Tips and Tricks - SLOW
APPLICATIONS? // Wireshark...
Chris Greer
Chris Greer - چریس گریر
10K views • 6 years ago

Raspberry Pi Router And
Firewall Using nftables
Technical Tuesday
Tall Paul Tech
Tall Paul Tech - پال تال
7K views • 1 year ago

Wireshark Packet Sniffing
Usernames, Passwords, and...
anscources
1.9M views • 8 years ago

Spring Boot 2.0 اندروید و سایه -
Full Spring Boot Course One...
Abd AbduGhazaleh - عابد عبد الغزاله
2K views • 4 months ago

ab08 SEED 2.0 Cross-Site
Request Forgery (CSRF) Attack...
置龙勿用
7K views • 1 year ago

Refresh Firefox... x

It looks like you haven't started Firefox in a while. Do you want to clean it up for a fresh, like-new experience? And by the way, welcome back!

Task 1.1: Sniffing Packets

A screenshot of a Linux desktop environment (Ubuntu) running in Oracle VM VirtualBox. The desktop has a dark theme. On the left is a dock with icons for a terminal, file manager, and browser. A central dock shows several open windows: a terminal window titled 'ubuntu-cyber [Running] - Oracle VM VirtualBox' with a command-line interface, a text editor window titled 'task1.py' containing Python code for packet sniffing, and a browser window showing a YouTube search results page for 'SEED Manual'. The browser window has a sidebar with recommended videos.

```
#!/usr/bin/env python3
from scapy.all import *
# The interface can be found with
# 'docker network ls' in the VM
# or 'ifconfig' in the container
pkt = sniff(iface='br-48d86189b02b', filter='icmp', prn=print_pkt)
```

A screenshot of a Linux desktop environment (Ubuntu) running in Oracle VM VirtualBox. The desktop has a dark theme. On the left is a dock with icons for a terminal, file manager, and browser. A central dock shows several open windows: a terminal window titled 'ubuntu-cyber [Running] - Oracle VM VirtualBox' with a command-line interface, a text editor window titled 'task1.py' containing Python code for packet sniffing, and a browser window showing a YouTube search results page for 'SEED Manual'. The browser window has a sidebar with recommended videos.

```
[03/11/23]seed@VM:~/.../Labsetup$ docksh hostA-10.9.0.5
root@0da75f3d2b1d:/# ping 10.9.0.6
PING 10.9.0.6 (10.9.0.6) 56(84) bytes of data.
64 bytes from 10.9.0.6: icmp_seq=1 ttl=64 time=0.080 ms
64 bytes from 10.9.0.6: icmp_seq=2 ttl=64 time=0.092 ms
64 bytes from 10.9.0.6: icmp_seq=3 ttl=64 time=0.060 ms
64 bytes from 10.9.0.6: icmp_seq=4 ttl=64 time=0.058 ms
64 bytes from 10.9.0.6: icmp_seq=5 ttl=64 time=0.066 ms
64 bytes from 10.9.0.6: icmp_seq=6 ttl=64 time=0.063 ms
64 bytes from 10.9.0.6: icmp_seq=7 ttl=64 time=0.126 ms
64 bytes from 10.9.0.6: icmp_seq=8 ttl=64 time=0.072 ms
^C
--- 10.9.0.6 ping statistics ---
8 packets transmitted, 8 received, 0% packet loss, time 7174ms
rtt min/avg/max/mdev = 0.058/0.077/0.126/0.021 ms
root@0da75f3d2b1d:/#
```

ubuntu-cyber [Running] - Oracle VM VirtualBox

Activities Terminal Mar 11 08:51

seed@VM: ~/Labsetup

```
seed@VM: ~/Labsetup seed@VM: ~/volumes seed@VM: ~/Labsetup seed@VM: ~/Labsetup
start.py task1.1.py task1.2.py task1.3.py task1.4.py template.py
root@VM:/volumes# chmod a+x task1.1.py
root@VM:/volumes# ./task1.1.py
###[ Ethernet ]###
dst      = 02:42:0a:09:00:06
src      = 02:42:0a:09:00:05
type     = IPv4
###[ IP ]###
version  = 4
ihl      = 5
tos      = 0x0
len      = 84
id       = 6801
flags    = DF
frag     = 0
ttl      = 64
proto    = icmp
checksum = 0xbfc
src      = 10.9.0.5
dst      = 10.9.0.6
\options \
###[ ICMP ]###
type     = echo-request
code    = 0
chksum  = 0x284
```

潜龙勿用 1.04K subscribers Subscribe Like Share Save ...

11,977 views Jan 19, 2022 IT5454 Spring 2022

It looks like you haven't started Firefox in a while. Do you want to clean it up for a fresh, like-new experience? And by the way, welcome back!

Refresh Firefox... Right Ctrl

ubuntu-cyber [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help Mar 11 08:58

Activities Terminal Mar 11 08:58

seed@VM: ~/Labsetup

```
seed@VM: ~/Labsetup seed@VM: ~/volumes seed@VM: ~/Labsetup seed@VM: ~/Labsetup
exit
root@VM:/volumes# task1.1.py
###[ Ethernet ]###
dst      = 02:42:0a:09:00:06
src      = 02:42:0a:09:00:05
type     = IPv4
###[ IP ]###
version  = 4
ihl      = 5
tos      = 0x0
len      = 84
id       = 49610
flags    = DF
frag     = 0
ttl      = 64
proto    = icmp
checksum = 0x64c2
src      = 10.9.0.5
dst      = 10.9.0.6
\options \
###[ ICMP ]###
type     = echo-request
code    = 0
chksum  = 0x284
```

Task 1.1B. Usually, when we sniff packets, we are only interested certain types of packets. We can do that by setting filters in sniffing. Scapy's filter use the BPF (Berkeley Packet Filter) syntax; you can find the callback function print_pkt() will be run after the packet. Run the program with the filter. After that, run the program again, but

It looks like you haven't started Firefox in a while. Do you want to clean it up for a fresh, like-new experience? And by the way, welcome back!

Refresh Firefox... Right Ctrl

ubuntu-cyper [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

Activities Terminal Mar 11 09:29

seed@VM: ~/Labsetup

```
[03/11/23]seed@VM:~/.../Labsetup$ docksh hostB-10.9.0.6
root@165df0779116:~# telnet 10.9.0.5
Trying 10.9.0.5...
Connected to 10.9.0.5.
Escape character is '^].
Ubuntu 20.04.1 LTS
0da75f3d2b1d login: seed
Password:
Welcome to Ubuntu 20.04.1 LTS (GNU/Linux 5.4.0-54-generic x86_64)

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

This system has been minimized by removing packages and content that are
not required on a system that users do not log into.

To restore this content, you can run the 'unminimize' command.
Last login: Sat Mar 11 14:25:48 UTC 2023 from 0da75f3d2b1d on pts/5
seed@0da75f3d2b1d:~$
```

11,977 views Jan 19, 2022 IT5454 Spring 2022

It looks like you haven't started Firefox in a while. Do you want to clean it up for a fresh, like-new experience? And by the way, welcome back!

Refresh Firefox... Right Ctrl

ubuntu-cyper [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

Activities Terminal Mar 11 09:29

seed@VM: ~/Labsetup

```
seed@VM:~/.../Labsetup$ ./task1.1.py
^Croot@VM:/volumes# python3 task1.1.py
^Croot@VM:/volumes# ./task1.1.py
^Croot@VM:/volumes# ./task1.1.py
###[ Ethernet ]###
dst      = 02:42:0a:09:00:05
src      = 02:42:0a:09:00:06
type     = IPv4
###[ IP ]###
version  = 4
ihl      = 5
tos      = 0x10
len      = 60
id       = 29
flags    = DF
frag     = 0
ttl      = 64
proto    = tcp
chksum   = 0x2673
src      = 10.9.0.6
dst      = 10.9.0.5
\options \
###[ TCP ]###
sport    = 53640
```

11,977 views Jan 19, 2022 IT5454 Spring 2022

It looks like you haven't started Firefox in a while. Do you want to clean it up for a fresh, like-new experience? And by the way, welcome back!

Refresh Firefox... Right Ctrl

ubuntu-cyper [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

Activities Terminal Sniffing_Spoofing.pdf Lab02: SEED 2.0 Packet its454/labs/lab02 at master Usage — Scapy 2.5.0. do seed-labs/SEEDManual...

seed@VM: ~/_/Labsetup Mar 11 09:38

```
seed@VM: ~/_/L... seed@VM: ~/_/V... seed@VM: ~/_/La... seed@VM: ~/_/La... seed@VM: ~/_/La...
Ubuntu 20.04.1 LTS
0da75f3d2b1d login: seed
Password:
Welcome to Ubuntu 20.04.1 LTS (GNU/Linux 5.4.0-54-generic x86_64)

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

This system has been minimized by removing packages and content that are
not required on a system that users do not log into.

To restore this content, you can run the 'unminimize' command.
Last login: Sat Mar 11 14:25:48 UTC 2023 from 0da75f3d2b1d on pts/5
seed@0da75f3d2b1d:~$ exit
logout
Connection closed by foreign host.
root@165df0779116:/# ping 128.230.0.11
PING 128.230.0.11 (128.230.0.11) 56(84) bytes of data.
^C
--- 128.230.0.11 ping statistics ---
2 packets transmitted, 0 received, 100% packet loss, time 1002ms
root@165df0779116:/#
```

11,977 views Jan 19, 2022 ITS454 Spring 2022

It looks like you haven't started Firefox in a while. Do you want to clean it up for a fresh, like-new experience? And by the way, welcome back!

Refresh Firefox... Right Ctrl

ubuntu-cyper [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

Activities Terminal Sniffing_Spoofing.pdf Lab02: SEED 2.0 Packet its454/labs/lab02 at master Usage — Scapy 2.5.0. do seed-labs/SEEDManual...

seed@VM: ~/_/Labsetup Mar 11 09:39

```
seed@VM: ~/_/L... seed@VM: ~/_/V... seed@VM: ~/_/La... seed@VM: ~/_/La... seed@VM: ~/_/La...
Display all 736 possibilities? (y or n)
root@VM:/volumes# ./task1.1.py
###[ Ethernet ]###
dst      = 02:42:e3:25:e0:67
src      = 02:42:0a:09:00:06
type     = IPv4
###[ IP ]###
version  = 4
ihl      = 5
tos      = 0x0
len      = 84
id       = 6176
flags    = DF
frag     = 0
ttl      = 64
proto    = icmp
checksum = 0x9789
src      = 10.9.0.6
dst      = 128.230.0.11
options   \
###[ ICMP ]###
type     = echo-request
code    = 0
checksum = 0x8600
```

11,977 views Jan 19, 2022 ITS454 Spring 2022

It looks like you haven't started Firefox in a while. Do you want to clean it up for a fresh, like-new experience? And by the way, welcome back!

Refresh Firefox... Right Ctrl

Task 1.2: Spoofing ICMP Packets

The screenshot shows a Linux desktop environment with a terminal window and a Firefox browser window.

In the terminal window, the code for task1.2.py is displayed:

```
#!/usr/bin/env python3
from scapy.all import *
a = IP()
a.dst = '1.2.3.4'
b = ICMP()
p = a/b
ls(a)
send(p)
```

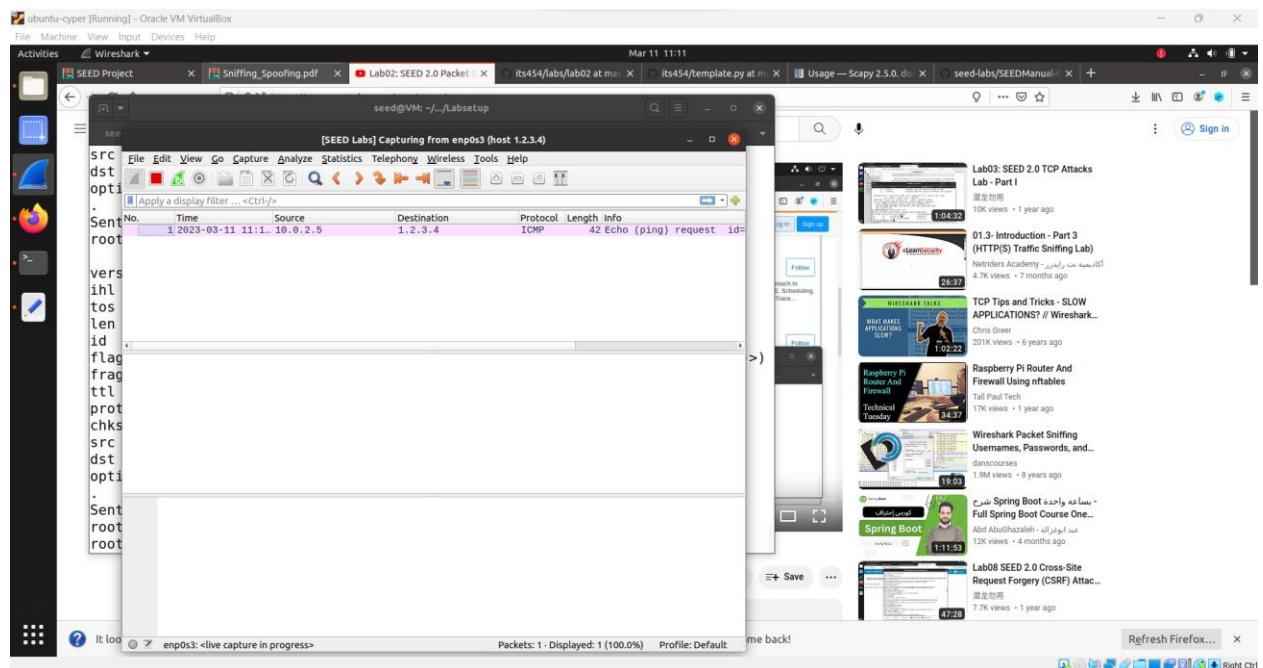
In the Firefox browser window, the YouTube channel "seed-labs" is open, showing the "SEED Manual" playlist. The first video in the list is "Lab03: SEED 2.0 TCP Attacks Lab - Part I".

The screenshot shows a Linux desktop environment with a terminal window and a Firefox browser window.

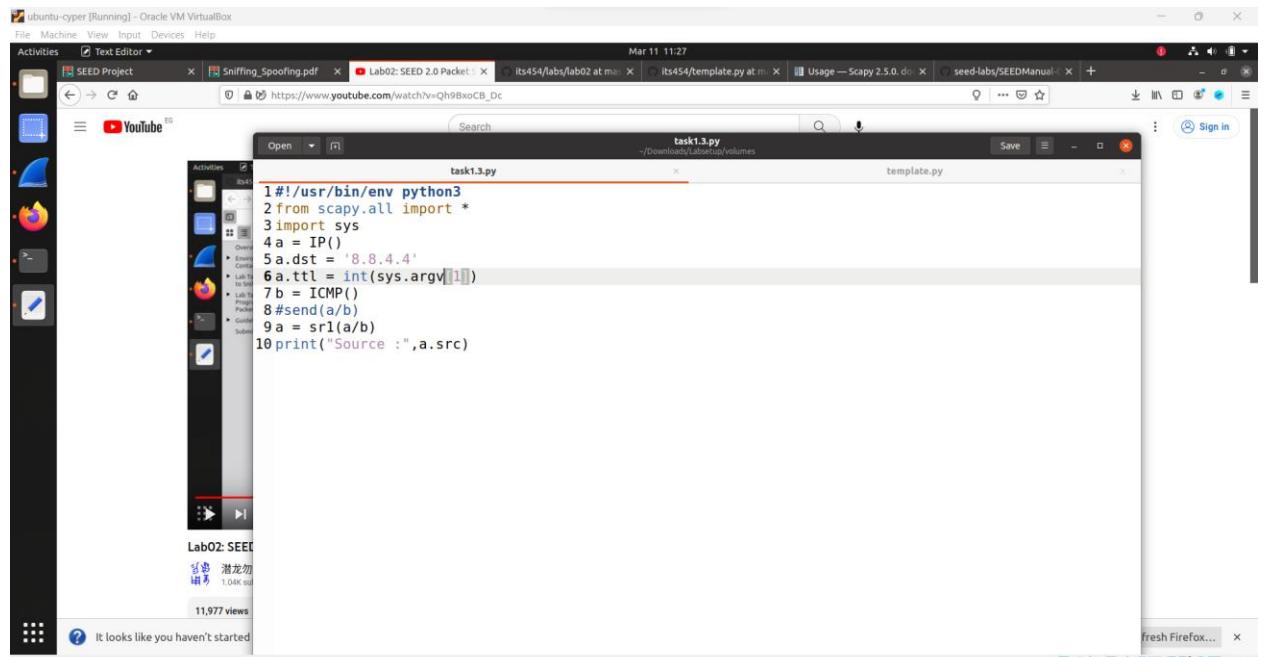
In the terminal window, the code for task1.2.py is displayed:

```
#!/usr/bin/env python3
from scapy.all import *
a = IP()
a.dst = '1.2.3.4'
b = ICMP()
p = a/b
ls(a)
send(p)
```

In the Firefox browser window, the YouTube channel "seed-labs" is open, showing the "SEED Manual" playlist. The first video in the list is "Lab03: SEED 2.0 TCP Attacks Lab - Part I".



Task 1.3: Traceroute



A screenshot of a Firefox browser window. The address bar shows the URL as seed@VM: ~/.Labsetup. The main content area displays a terminal session on a Kali Linux VM. The terminal output is as follows:

```
root@VM:/volumes# ./task1.3.py 1
Traceback (most recent call last):
  File "./task1.3.py", line 6, in <module>
    a.ttl = int(sys.argv[1])
AttributeError: module 'sys' has no attribute 'arg'
root@VM:/volumes# ./task1.3.py 1
Begin emission:
Finished sending 1 packets.
.*
Received 2 packets, got 1 answers, remaining 0 packets
Source : 10.0.2.1
root@VM:/volumes# ./task1.3.py 2
Begin emission:
Finished sending 1 packets.
.*
Received 2 packets, got 1 answers, remaining 0 packets
Source : 192.168.1.1
root@VM:/volumes# ./task1.3.py 3
Begin emission:
Finished sending 1 packets.
.*
Received 2 packets, got 1 answers, remaining 0 packets
Source : 41.234.148.1
root@M:/volumes#
```

Below the terminal, there is a "Subscribe" button with 1,04K subscribers. To the right of the terminal, a video player is open, showing a video titled "Lab03: SEED 2.0 TCP Attacks Lab - Part1" by NetRiders Academy. The video has 10K views and was posted 1 year ago. The video thumbnail shows a person speaking. Below the video player, there are other video thumbnails from the same channel, including "01.3 - Introduction - Part 3 (HTTP(S) Traffic Sniffing Lab)" and "TCP Tips and Tricks - SLOW APPLICATIONS!! // Wireshark...". Further down, there are more thumbnails for "Raspberry Pi Router And Firewall Using iftables", "Wireshark Packet Sniffing Usernames, Passwords, and...", and "Spring Boot - مراجعة كاملة لـ Full Spring Boot Course One...". At the bottom of the browser window, a message says "It looks like you haven't started Firefox in a while. Do you want to clean it up for a fresh, like-new experience? And by the way, welcome back!" and a "Refresh Firefox..." button.

Task 1.4: Sniffing and-then Spoofing

ubuntu-cyber [Running] - Oracle VM VirtualBox

```
Received 2 packets, got 1 answers, remaining 0 packets
Source : 41.234.148.1
root@VM:/volumes# ^C
root@VM:/volumes# chmod a+x task1.4.py
root@VM:/volumes# ./task1.4
bash: ./task1.4: No such file or directory
root@VM:/volumes# ./task1.4.py
^Croot@VM:/volumes# ./task1.4.py
Original Packet.....
Source IP : 10.9.0.5
Destination IP : 1.2.3.4
Spoofed Packet.....
Source IP : 1.2.3.4
Destination IP : 10.9.0.5
Original Packet.....
Source IP : 10.9.0.5
Destination IP : 1.2.3.4
Spoofed Packet.....
Source IP : 1.2.3.4
Destination IP : 10.9.0.5
Original Packet.....
Source IP : 10.9.0.5
```

Lab02: SEED 2.0 Packet Sniffing and Spoofing Lab - Scapy

潜龙勿用
1.04K subscribers

Like

11,977 views Jan 19, 2022 IT5454 Spring 2022

It looks like you haven't started Firefox in a while. Do you want to clean it up for a fresh, like-new experience? And

```
task1.3.py
env python3
all import *

def(pkt):
    and print out icmp echo request packet
    in pkt and pkt[ICMP].type == 8:
        print("Original Packet.....")
        print("Source IP : ", pkt[IP].src)
        print("Destination IP :", pkt[IP].dst)

    spoof an icmp echo reply packet
    swap srcip and dstip
    ip = IP(src=pkt[IP].dst, dst=pkt[IP].src, ihl=pkt[IP].ihl)
    ip = ICMP(type=0, id=pkt[ICMP].id, seq=pkt[ICMP].seq)
    data = pkt[Raw].load
    newpkt = ip/icmp/data

    print("Spoofed Packet.....")
    print("Source IP : ", newpkt[IP].src)
    print("Destination IP :", newpkt[IP].dst)

    ((newpkt, verbose=0)
     ip and host 1.2.3.4'
24#print("filter: {}\\n".format(filter))
25 pkt = sniff(iface = 'br-48d86189b02b' ,filter=filter, prn=spoof_pkt)
```

ubuntu-cyber [Running] - Oracle VM VirtualBox

```
File Machine View Input Devices Help
Activities Terminal Mar 11 11:49
seed@VM: ~-/Labsetup
From 10.9.0.5 icmp_seq=6 Destination Host Unreachable
^C
--- 10.9.0.99 ping statistics ---
7 packets transmitted, 0 received, +6 errors, 100% packet loss, time
pipe 4
root@0da75f3d2b1d:/# exit
exit
^C

c[03/11/23]seed@VM:~/.../Labsetup$ ^C
[03/11/23]seed@VM:~/.../Labsetup$ docksh hostA-10.9.0.5
root@0da75f3d2b1d:/# ping 10.9.0.99
PING 10.9.0.99 (10.9.0.99) 56(84) bytes of data.
From 10.9.0.5 icmp_seq=1 Destination Host Unreachable
From 10.9.0.5 icmp_seq=2 Destination Host Unreachable
From 10.9.0.5 icmp_seq=3 Destination Host Unreachable
^C
--- 10.9.0.99 ping statistics ---
5 packets transmitted, 0 received, +3 errors, 100% packet loss, time
pipe 4
root@0da75f3d2b1d:/# 
```

Lab02: SEED 2.0 Packet Sniffing and Spoofing Lab - Scapy

潜龙勿用
1.04K subscribers

Like

11,977 views Jan 19, 2022 IT5454 Spring 2022

It looks like you haven't started Firefox in a while. Do you want to clean it up for a fresh, like-new experience? And

```
task1.4.py
#!/usr/bin/env python3
from scapy.all import *
from scapy.layers.inet import ICMP, IP

def spoof_pkt(pkt):
    # sniff and print out icmp echo request packet
    if ICMP in pkt and pkt[ICMP].type == 8:
        print("Original Packet.....")
        print("Source IP : ", pkt[IP].src)
        print("Destination IP :", pkt[IP].dst)

    # spoof an icmp echo reply packet
    # swap srcip and dstip
    ip = IP(src=pkt[IP].dst, dst=pkt[IP].src, ihl=pkt[IP].ihl)
    icmp = ICMP(type=0, id=pkt[ICMP].id, seq=pkt[ICMP].seq)
    data = pkt[Raw].load
    newpkt = ip/icmp/data

    print("Spoofed Packet.....")
    print("Source IP : ", newpkt[IP].src)
    print("Destination IP :", newpkt[IP].dst)

    send(newpkt, verbose=0)
    filter = 'icmp and host 10.9.0.99'
24#print("filter: {}\\n".format(filter))
25 pkt = sniff(iface = 'br-48d86189b02b' ,filter=filter, prn=spoof_pkt)
```

```
[ubuntu-cyber [Running] - Oracle VM VirtualBox]
File Machine View Input Devices Help
Activities Terminal Mar 11 11:50
seed@VM:~/.../Labsetup$ docksh hostA-10.9.0.5
root@0da75f3d2b1d:/# ping 10.9.0.99
PING 10.9.0.99 (10.9.0.99) 56(84) bytes of data.
From 10.9.0.5 icmp_seq=1 Destination Host Unreachable
From 10.9.0.5 icmp_seq=2 Destination Host Unreachable
From 10.9.0.5 icmp_seq=3 Destination Host Unreachable
^C
--- 10.9.0.99 ping statistics ---
5 packets transmitted, 0 received, +3 errors, 100% packet loss, time 4097ms
pipe 4
root@0da75f3d2b1d:/# ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=64 time=43.6 ms
64 bytes from 8.8.8.8: icmp_seq=1 ttl=64 time=62.1 ms (DUP!)
64 bytes from 8.8.8.8: icmp_seq=2 ttl=64 time=18.6 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=64 time=45.7 ms (DUP!)
^C
--- 8.8.8.8 ping statistics ---
3 packets transmitted, 3 received, +2 duplicates, 0% packet loss, time 2002ms
rtt min/avg/max/mdev = 18.641/38.354/62.136/16.186 ms
ping: write error
root@0da75f3d2b1d:/#

```

Lab02: SEED 2.0 Packet Sniffing and Spoofing Lab - Scapy

潜水勿用
1.04K subscribers

Like

11,977 views Jan 19, 2022 IT5454 Spring 2022

It looks like you haven't started Firefox in a while. Do you want to clean it up for a fresh, like-new experience? And

```
task1.3.py
env python3
all import *

pkt:
    and print out icmp echo request packet
    in pkt and pkt[ICMP].type == 8:
        print("Original Packet.....")
        print("Source IP : ", pkt[IP].src)
        print("Destination IP : ", pkt[IP].dst)

        spoof an icmp echo reply packet
        vap srcip and dstip
        = IP(src=pkt[IP].dst, dst=pkt[IP].src, ihl=pkt[IP].ihl)
        o = ICMP(type=0, id=pkt[ICMP].id, seq=pkt[ICMP].seq)
        a = pkt[Raw].load
        okt = ip/icmp/data

        print("Spoofed Packet.....")
        print("Source IP : ", newpkt[IP].src)
        print("Destination IP : ", newpkt[IP].dst)

        (newpkt, verbose=0)
        print("filter: {}\\n".format(filter))
        25 pkt = sniff(iface = 'br-48d86189b02b', filter=filter, prn=spoof_pkt)
```

```
[ubuntu-cyber [Running] - Oracle VM VirtualBox]
File Machine View Input Devices Help
Activities Terminal Mar 11 11:51
seed@VM:~/.../Labsetup$ ./task1.4.py
^Croot@VM:~/volumes# ./task1.4.py
^Croot@VM:~/volumes# ./task1.4.py
^Croot@VM:~/volumes# ./task1.4.py
Original Packet.....
Source IP : 10.9.0.5
Destination IP : 8.8.8.8
Spoofed Packet.....
Source IP : 8.8.8.8
Destination IP : 10.9.0.5
Original Packet.....
Source IP : 10.9.0.5
Destination IP : 8.8.8.8
Spoofed Packet.....
Source IP : 8.8.8.8
Destination IP : 10.9.0.5
Original Packet.....
Source IP : 10.9.0.5
Destination IP : 8.8.8.8
Spoofed Packet.....
Source IP : 8.8.8.8
Destination IP : 10.9.0.5

```

Lab02: SEED 2.0 Packet Sniffing and Spoofing Lab - Scapy

潜水勿用
1.04K subscribers

Like

11,977 views Jan 19, 2022 IT5454 Spring 2022

It looks like you haven't started Firefox in a while. Do you want to clean it up for a fresh, like-new experience? And

```
task1.4.py
env python3
all import *

pkt:
    and print out icmp echo request packet
    in pkt and pkt[ICMP].type == 8:
        print("Original Packet.....")
        print("Source IP : ", pkt[IP].src)
        print("Destination IP : ", pkt[IP].dst)

        spoof an icmp echo reply packet
        vap srcip and dstip
        = IP(src=pkt[IP].dst, dst=pkt[IP].src, ihl=pkt[IP].ihl)
        o = ICMP(type=0, id=pkt[ICMP].id, seq=pkt[ICMP].seq)
        a = pkt[Raw].load
        okt = ip/icmp/data

        print("Spoofed Packet.....")
        print("Source IP : ", newpkt[IP].src)
        print("Destination IP : ", newpkt[IP].dst)

        (newpkt, verbose=0)
        print("filter: {}\\n".format(filter))
        25 pkt = sniff(iface = 'br-48d86189b02b', filter=filter, prn=spoof_pkt)
```