

110124156

I confirm that I will keep the content of this Lab confidential. I confirm that I have not received any unauthorized assistance in preparing for or writing this Lab. I acknowledge that a mark of 0 may be assigned for copied work.”

Name: Siddharth Samber

Student number: 110124156

LAB 1

Master of Applied Computing

Networking & Data Security

COMP 8677

University of Windsor



University
of Windsor

Submitted By:

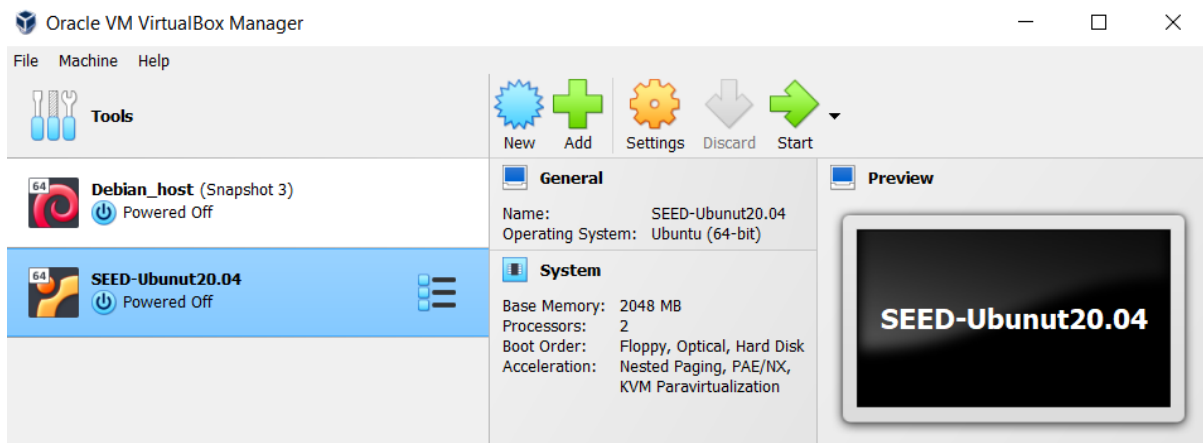
Siddharth Samber

110124156

Submission Date:

23 January 2024

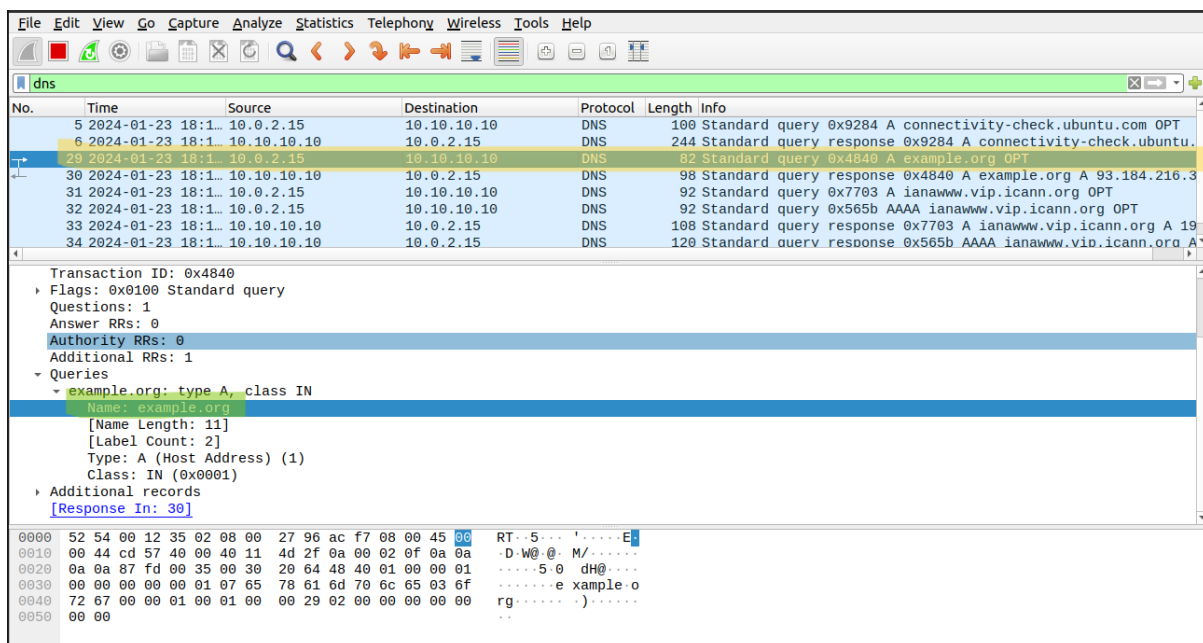
1) SEEDLAB SETUP



SEEDLAB Setup on your computer using Virtual Box has been successfully done.

2) SNIFFING HTTP PACKET

PART A



- Highlighted in **yellow** is DNS **request packet**
- Highlighted in **green** is the **Domain name** of website example.org

110124156

[SEED Labs] enp0s3

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

dns

No.	Time	Source	Destination	Protocol	Length	Info
5	2024-01-23 18:1...	10.0.2.15	10.10.10.10	DNS	100	Standard query 0x9284 A connectivity-check.ubuntu.com OPT
6	2024-01-23 18:1...	10.10.10.10	10.0.2.15	DNS	244	Standard query response 0x9284 A connectivity-check.ubuntu.com OPT
29	2024-01-23 18:1...	10.0.2.15	10.10.10.10	DNS	82	Standard query 0x4840 A example.org OPT
30	2024-01-23 18:1...	10.10.10.10	10.0.2.15	DNS	98	Standard query response 0x4840 A example.org A 93.184.216.34
31	2024-01-23 18:1...	10.0.2.15	10.10.10.10	DNS	92	Standard query 0x7703 A ianawww.vip.icann.org OPT
32	2024-01-23 18:1...	10.0.2.15	10.10.10.10	DNS	92	Standard query 0x565b AAAA ianawww.vip.icann.org OPT
33	2024-01-23 18:1...	10.10.10.10	10.0.2.15	DNS	108	Standard query response 0x7703 A ianawww.vip.icann.org A 19
34	2024-01-23 18:1...	10.10.10.10	10.0.2.15	DNS	120	Standard query response 0x565b AAAA ianawww.vip.icann.org A

Answer RRs: 1
Authority RRs: 0
Additional RRs: 1

Queries

- example.org: type A, class IN
Name: example.org
[Name Length: 11]
[Label Count: 2]
Type: A (Host Address) (1)
Class: IN (0x0001)

Answers

- example.org: type A, class IN, addr 93.184.216.34

Additional records

[Request In: 29]
[Time: 0.003819905 seconds]

0000 08 00 27 96 ac f7 52 54 00 12 35 02 08 00 45 00 ...RT...5...E...
0010 00 54 ec c3 00 00 40 11 6d b3 0a 0a 0a 0a 00 ...T...@...m...
0020 02 0f 00 35 87 fd 00 40 6b c1 48 40 81 80 00 01 ...5...@...k...H...
0030 00 01 00 00 00 01 07 65 78 61 6d 70 6c 65 03 6f ...e...x...a...m...p...l...e...
0040 72 67 00 00 01 00 01 c0 9c 00 01 00 01 00 00 02 rg...
0050 52 00 04 5d b8 d8 22 00 00 29 02 00 00 00 00 00 R...]
0060 00 00

- Highlighted in yellow is DNS response packet
- Highlighted in green is the IP address of website example.org which is 93.184.216.34

PART B

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

dns

No.	Time	Source	Destination	Protocol	Length	Info
5	2024-01-23 18:1...	10.0.2.15	10.10.10.10	DNS	100	Standard query 0x9284 A connectivity-check.ubuntu.com OPT
6	2024-01-23 18:1...	10.10.10.10	10.0.2.15	DNS	244	Standard query response 0x9284 A connectivity-check.ubuntu.com OPT
29	2024-01-23 18:1...	10.0.2.15	10.10.10.10	DNS	82	Standard query 0x4840 A example.org OPT
30	2024-01-23 18:1...	10.10.10.10	10.0.2.15	DNS	98	Standard query response 0x4840 A example.org A 93.184.216.34
31	2024-01-23 18:1...	10.0.2.15	10.10.10.10	DNS	92	Standard query 0x7703 A ianawww.vip.icann.org OPT
32	2024-01-23 18:1...	10.0.2.15	10.10.10.10	DNS	92	Standard query 0x565b AAAA ianawww.vip.icann.org OPT
33	2024-01-23 18:1...	10.10.10.10	10.0.2.15	DNS	108	Standard query response 0x7703 A ianawww.vip.icann.org A 19
34	2024-01-23 18:1...	10.10.10.10	10.0.2.15	DNS	120	Standard query response 0x565b AAAA ianawww.vip.icann.org A

Transaction ID: 0x4840
Flags: 0x0100 Standard query
Questions: 1
Answer RRs: 0
Authority RRs: 0
Additional RRs: 1

Queries

- example.org: type A, class IN
Name: example.org
[Name Length: 11]
[Label Count: 2]
Type: A (Host Address) (1)
Class: IN (0x0001)

Additional records

[Response In: 30]

0000 52 54 00 12 35 02 08 00 27 96 ac f7 08 00 45 00 ...RT...5... '...E...
0010 00 44 cd 57 40 00 40 11 4d 2f 0a 0a 02 0f 0a 0a ...D...W...@...M.../
0020 0a 0a 87 fd 00 35 00 30 20 64 48 40 01 00 00 01 ...5...@...dh...
0030 00 00 00 00 00 01 07 65 78 61 6d 70 6c 65 03 6f ...e...x...a...m...p...l...e...
0040 72 67 00 00 01 00 01 00 00 29 02 00 00 00 00 00 rg...
0050 00 00

- Highlighted in yellow is IP address of our machine which is 10.0.2.15
Explanation: Source address of request packet is IP address of our machine
- Highlighted in green is the IP address of DNS Server which is 10.10.10.10
Explanation: destination address of request packet is IP address of DNS server.
- Highlighted in purple is the domain name of our server

[SEED Labs] enp0s3

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

dns

No.	Time	Source	Destination	Protocol	Length	Info
5	2024-01-23 18:1...	10.0.2.15	10.10.10.10	DNS	100	Standard query 0x9284 A connectivity-check.ubuntu.com OPT
6	2024-01-23 18:1...	10.10.10.10	10.0.2.15	DNS	244	Standard query response 0x9284 A connectivity-check.ubuntu.
29	2024-01-23 18:1...	10.0.2.15	10.10.10.10	DNS	82	Standard query 0x4840 A example.org OPT
30	2024-01-23 18:1...	10.10.10.10	10.0.2.15	DNS	98	Standard query response 0x4840 A example.org A 93.184.216.3
31	2024-01-23 18:1...	10.0.2.15	10.10.10.10	DNS	92	Standard query 0x7703 A ianawww.vip.icann.org OPT
32	2024-01-23 18:1...	10.0.2.15	10.10.10.10	DNS	92	Standard query 0x565b AAAA ianawww.vip.icann.org OPT
33	2024-01-23 18:1...	10.10.10.10	10.0.2.15	DNS	108	Standard query response 0x7703 A ianawww.vip.icann.org A 19
34	2024-01-23 18:1...	10.10.10.10	10.0.2.15	DNS	120	Standard query response 0x565b AAAA ianawww.vip.icann.org A

Answer RRs: 1
 Authority RRs: 0
 Additional RRs: 1
 Queries
 - example.org: type A, class IN
 Name: example.org
 [Name Length: 11]
 [Label Count: 2]
 Type: A (Host Address) (1)
 Class: IN (0x0001)
 Answers
 - example.org: type A, class IN, addr 93.184.216.34
 Additional records
 [Request In: 29]
 [Time: 0.003819905 seconds]

```

0000 08 00 27 96 ac f7 52 54 00 12 35 02 08 00 45 00  ...RT...5...E.
0010 00 54 ec c3 00 00 40 11 6d b3 0a 0a 0a 0a 0a 00  .T...@.m.....
0020 02 0f 00 35 87 fd 00 40 6b c1 48 40 81 80 00 01  ...5...@k.H@...
0030 00 01 00 00 00 01 07 65 78 61 6d 70 6c 65 03 6f  ....e xample.o
0040 72 67 00 00 01 00 01 c0 0c 00 01 00 01 00 00 02  rg.....
0050 52 00 04 5d b8 d8 22 00 00 29 10 00 00 00 00 00  R...].
0060 00 00
  
```

- 1) Highlighted in **yellow** is **IP address of DNS Server**. Which is 10.10.10.10
Explanation: Source address of response packet is IP address of DNS server
- 2) Highlighted in **green** is the **IP address of our Machine**. Which is 10.0.2.15
Explanation: Destination address of response packet is IP address of our machine
- 3) Highlighted in **purple** is the **IP address of our server** which is 93.104.216.34
Explanation : Answer contains IP address of server

CONCLUSION

Sniffing of DNS request and response packets and setup of SEEDLAB successfully completed.