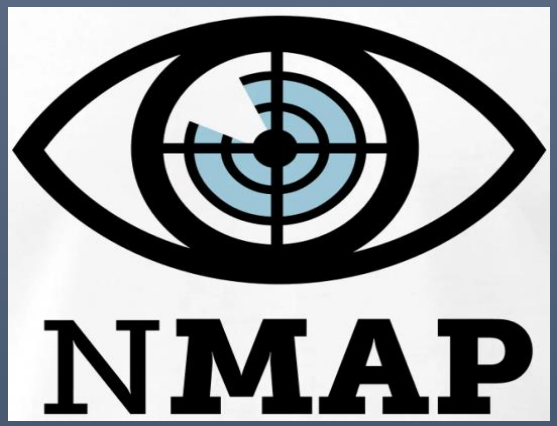


PORTFOLIO 2, Cyber-Security

Asset detection, reconnaissance, and monitoring

Tony (YIT19488399)

Roehampton university | CMP020X305S

Monday, 27 February 2023

INTRODUCTION:

Screenshots will be commented and sketching for better and faster understanding. Friday, 03 of March 2023, in laboratory area and laboratory time is possible to deliver clarifications about this document in person.

I will start from point 2 in requirements A to set out that if gateway in turned off, there are no communication nor networking between hosts on the sandboxed network. And I will demonstrate that host name can be different from association of IPs to names that should be the host names. This is the case for *gateway* and *bitnami* VMs.

Afterwards, I will ping to host names as instructions, and host numbers (only with Zabbix VM), and the outcome should be the same. For requirements B, screenshots have extra *nmap* commands found online. Finally, *nmap* has built in scripts to find vulnerabilities, exploit them, authentication, brute, and more. Many screenshots cover few points from requirements B and original and this paper were produced, being this one (my own) more precise guided.

As "Wow Factor, I participated in few discussions on Moodle. Requirements A and B have some extra content included that is visible on screenshots. Plus I installed Python in Kali and I executed a simple command from file using CLI.

Requirement A: Demonstration Tasks

1. From the **gateway**, demonstrate that you can successfully ping the kali, wordpress, analytics and zabbix host names.

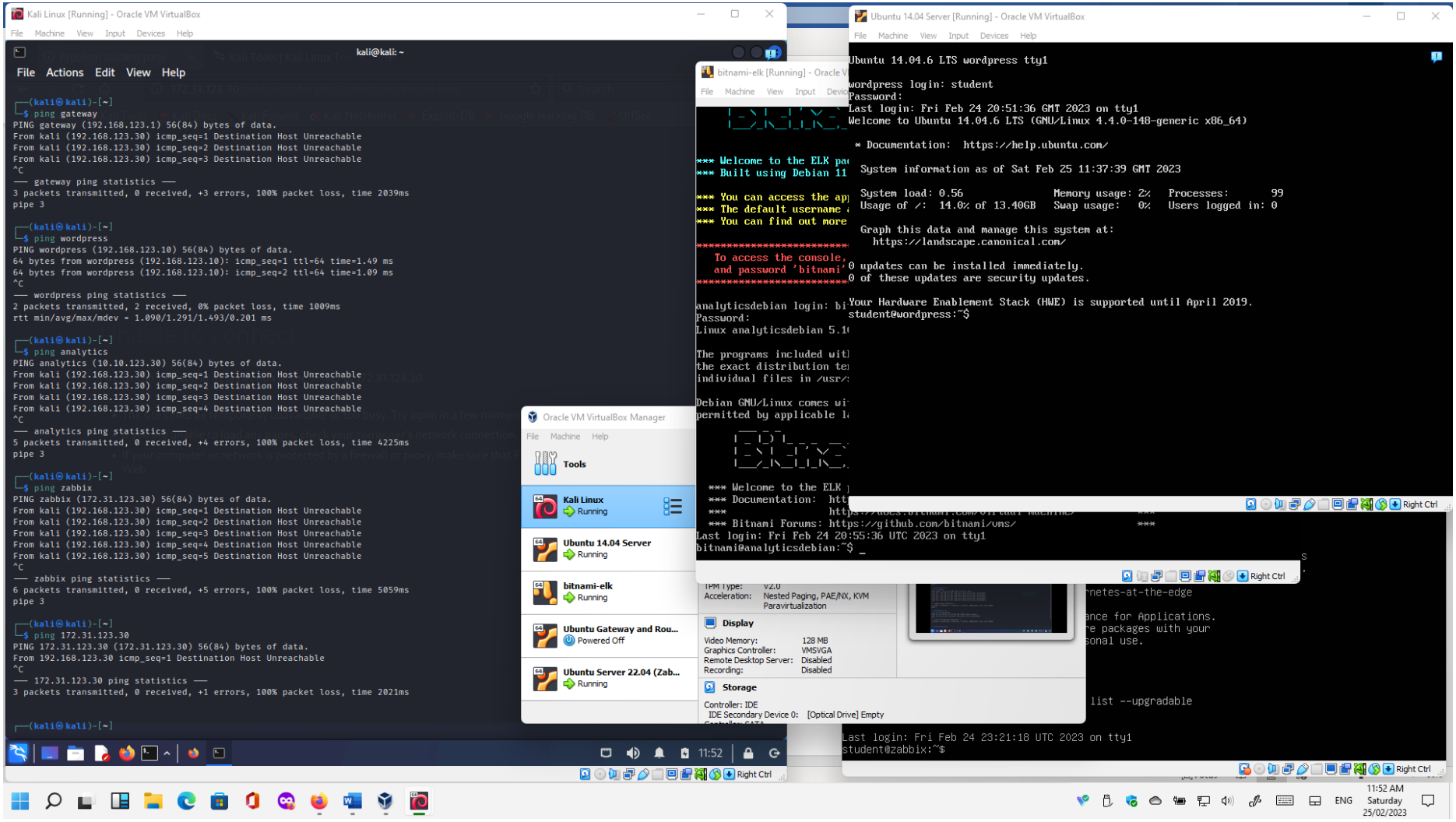
2. From the **kali**, demonstrate that you can successfully ping the gateway, wordpress, analytics and zabbix host names.

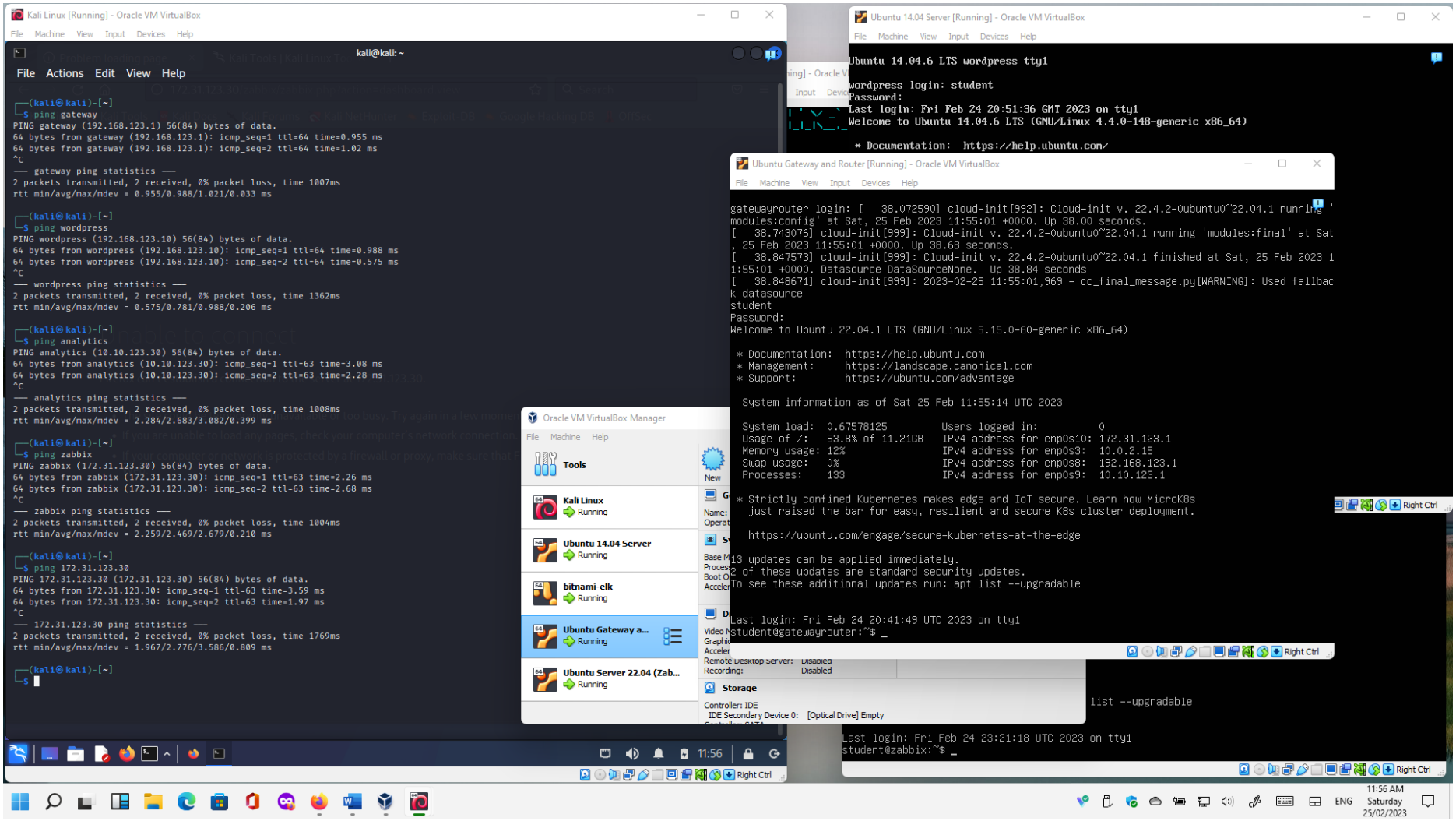
3. From the **wordpress**, demonstrate that you can successfully ping the gateway, kali, analytics and zabbix host names.

4. From the **analytics**, demonstrate that you can successfully ping the gateway, kali, wordpress and zabbix host names.

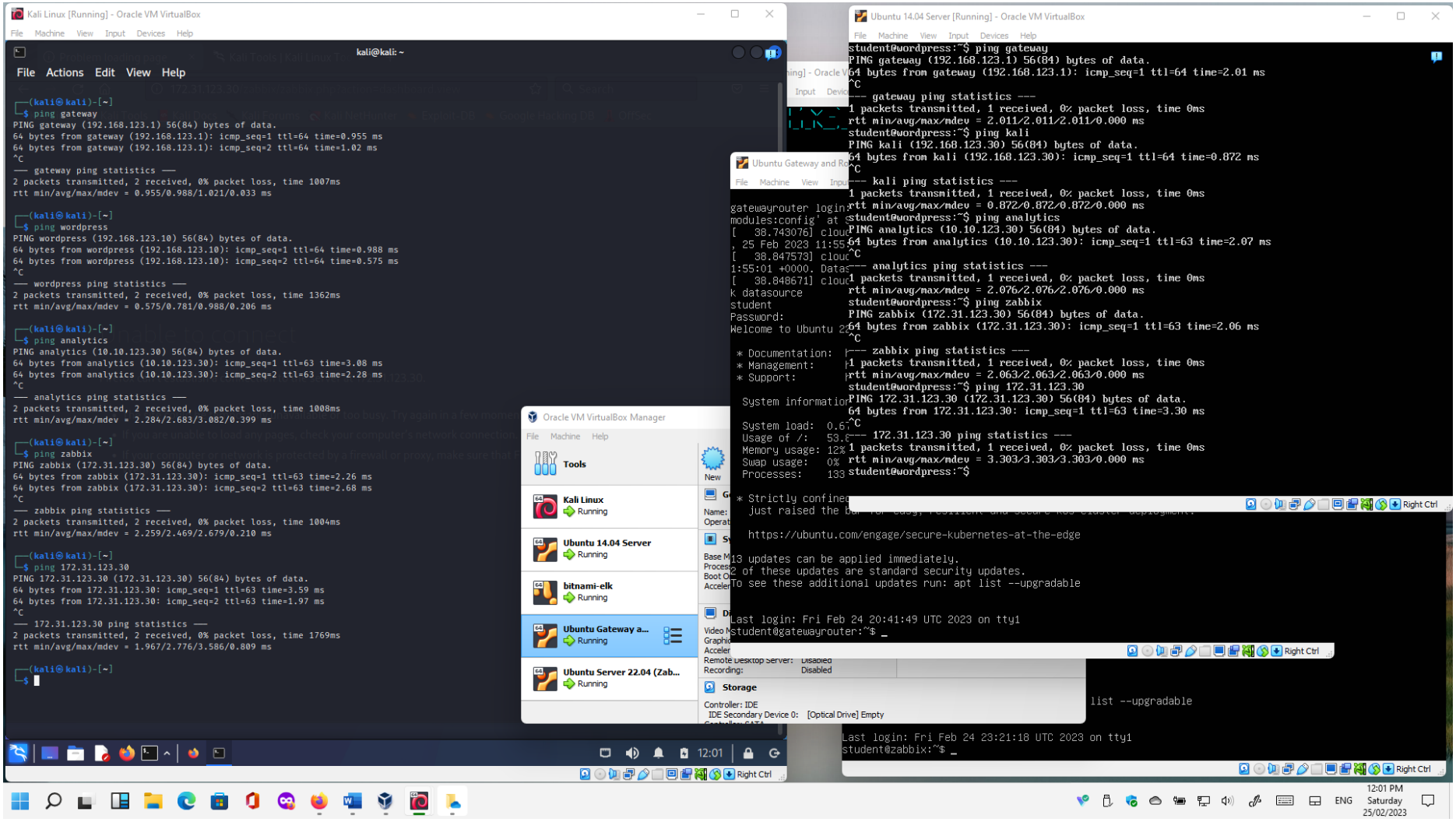
5. From the **zabbix**, demonstrate that you can successfully ping the gateway, kali, wordpress and analytics host names.

2.

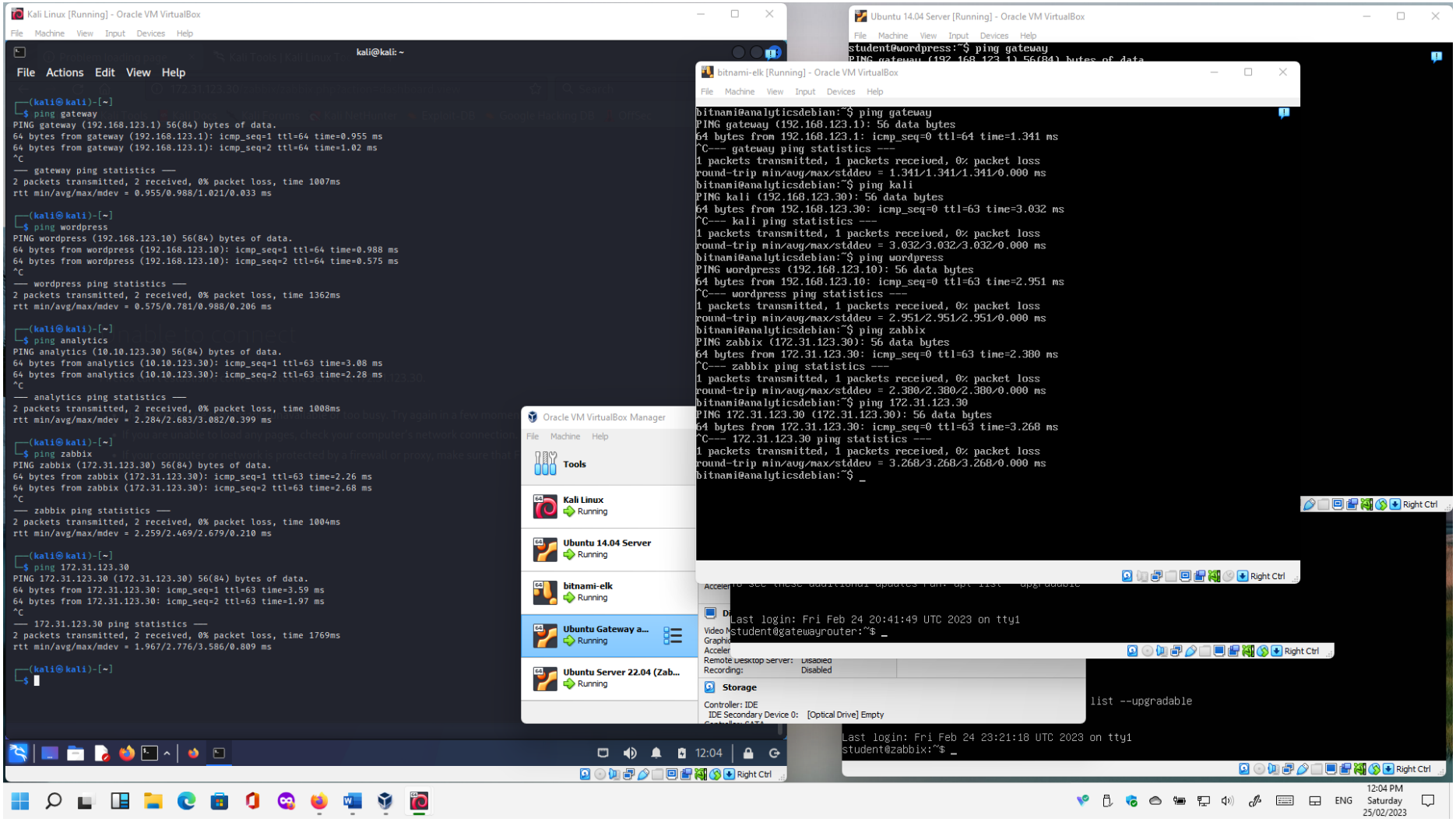

Kali Linux [Running] - Oracle VM VirtualBox
kali@kali: ~
File Actions Edit View Help
ping gateway
PING gateway (192.168.123.1) 56(84) bytes of data.
From kali (192.168.123.30) icmp_seq=1 Destination Host Unreachable
From kali (192.168.123.30) icmp_seq=2 Destination Host Unreachable
From kali (192.168.123.30) icmp_seq=3 Destination Host Unreachable
^C
— gateway ping statistics —
3 packets transmitted, 0 received, +3 errors, 100% packet loss, time 2039ms
pipe 3
ping wordpress
PING wordpress (192.168.123.10) 56(84) bytes of data.
64 bytes from wordpress (192.168.123.10): icmp_seq=1 ttl=64 time=1.49 ms
64 bytes from wordpress (192.168.123.10): icmp_seq=2 ttl=64 time=1.09 ms
^C
— wordpress ping statistics —
2 packets transmitted, 2 received, 0% packet loss, time 1009ms
rtt min/avg/max/mdev = 1.090/1.291/1.493/0.201 ms
ping analytics
PING analytics (10.10.123.30) 56(84) bytes of data.
From kali (192.168.123.30) icmp_seq=1 Destination Host Unreachable
From kali (192.168.123.30) icmp_seq=2 Destination Host Unreachable
From kali (192.168.123.30) icmp_seq=3 Destination Host Unreachable
From kali (192.168.123.30) icmp_seq=4 Destination Host Unreachable
^C
— analytics ping statistics —
5 packets transmitted, 0 received, +4 errors, 100% packet loss, time 4225ms
pipe 3
ping zabbix
PING zabbix (172.31.123.30) 56(84) bytes of data.
From kali (192.168.123.30) icmp_seq=1 Destination Host Unreachable
From kali (192.168.123.30) icmp_seq=2 Destination Host Unreachable
From kali (192.168.123.30) icmp_seq=3 Destination Host Unreachable
From kali (192.168.123.30) icmp_seq=4 Destination Host Unreachable
From kali (192.168.123.30) icmp_seq=5 Destination Host Unreachable
^C
— zabbix ping statistics —
6 packets transmitted, 0 received, +5 errors, 100% packet loss, time 5059ms
pipe 3
ping 172.31.123.30
PING 172.31.123.30 (172.31.123.30) 56(84) bytes of data.
From 192.168.123.30 icmp_seq=1 Destination Host Unreachable
^C
— 172.31.123.30 ping statistics —
3 packets transmitted, 0 received, +1 errors, 100% packet loss, time 2021ms
Oracle VM VirtualBox Manager
Tools
Kali Linux
Running
Ubuntu 14.04 Server
Running
bitnami-elk
Running
Ubuntu Gateway and Rou...
Powered Off
Ubuntu Server 22.04 (Zab...
Running
bitnami-elk [Running] - Oracle V
Welcome to the ELK pa
Built using Debian 11
You can access the ap
The default username
You can find out more
To access the console,
and password 'bitnami'
analyticsdebian login: bi
Password:
Linux analyticsdebian 5.1
The programs included wit
the exact distribution te
individual files in /usr/
Debian GNU/Linux comes wi
permitted by applicable l
Welcome to the ELK
Documentation:
Bitnami Forums: https://github.com/bitnami/vms/
Last login: Fri Feb 24 20:55:36 UTC 2023 on tty1
bitnami@analyticsdebian:~$
Acceleration: Nested Paging, PAE/NX, KVM
Paravirtualization
Display
Video Memory: 128 MB
Graphics Controller: VMSVGA
Remote Desktop Server: Disabled
Recording: Disabled
Storage
Controller: IDE
IDE Secondary Device 0: [Optical Drive] Empty
Ubuntu 14.04 Server [Running] - Oracle VM VirtualBox
Ubuntu 14.04.6 LTS wordpress tty1
wordpress login: student
Password:
Last login: Fri Feb 24 20:51:36 GMT 2023 on tty1
Welcome to Ubuntu 14.04.6 LTS (GNU/Linux 4.4.0-148-generic x86_64)
* Documentation: https://help.ubuntu.com/
System information as of Sat Feb 25 11:37:39 GMT 2023
System load: 0.56 Memory usage: 2% Processes: 99
Usage of /: 14.0% of 13.40GB Swap usage: 0% Users logged in: 0
Graph this data and manage this system at:
https://landscape.canonical.com/
0 updates can be installed immediately.
0 of these updates are security updates.
Your Hardware Enablement Stack (HWE) is supported until April 2019.
student@wordpress:~$
Right Ctrl
netes-at-the-edge
ance for Applications.
e packages with your
sonal use.
list --upgradable
Last login: Fri Feb 24 23:21:18 UTC 2023 on tty1
student@zabbix:~$
11:52
Right Ctrl
ENG
11:52 AM
Saturday
25/02/2023


Kali Linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
kali@kali: ~
File Actions Edit View Help
┌──(kali㉿kali)-[~]
└─$ ping gateway
PING gateway (192.168.123.1) 56(84) bytes of data.
64 bytes from gateway (192.168.123.1): icmp_seq=1 ttl=64 time=0.955 ms
64 bytes from gateway (192.168.123.1): icmp_seq=2 ttl=64 time=1.02 ms
^C
— gateway ping statistics —
2 packets transmitted, 2 received, 0% packet loss, time 1007ms
rtt min/avg/max/mdev = 0.955/0.988/1.021/0.033 ms
┌──(kali㉿kali)-[~]
└─$ ping wordpress
PING wordpress (192.168.123.10) 56(84) bytes of data.
64 bytes from wordpress (192.168.123.10): icmp_seq=1 ttl=64 time=0.988 ms
64 bytes from wordpress (192.168.123.10): icmp_seq=2 ttl=64 time=0.575 ms
^C
— wordpress ping statistics —
2 packets transmitted, 2 received, 0% packet loss, time 1362ms
rtt min/avg/max/mdev = 0.575/0.781/0.988/0.206 ms
┌──(kali㉿kali)-[~]
└─$ ping analytics
PING analytics (10.10.123.30) 56(84) bytes of data.
64 bytes from analytics (10.10.123.30): icmp_seq=1 ttl=63 time=3.08 ms
64 bytes from analytics (10.10.123.30): icmp_seq=2 ttl=63 time=2.28 ms
^C
— analytics ping statistics —
2 packets transmitted, 2 received, 0% packet loss, time 1008ms
rtt min/avg/max/mdev = 2.284/2.683/3.082/0.399 ms
┌──(kali㉿kali)-[~]
└─$ ping zabbix
PING zabbix (172.31.123.30) 56(84) bytes of data.
64 bytes from zabbix (172.31.123.30): icmp_seq=1 ttl=63 time=2.26 ms
64 bytes from zabbix (172.31.123.30): icmp_seq=2 ttl=63 time=2.68 ms
^C
— zabbix ping statistics —
2 packets transmitted, 2 received, 0% packet loss, time 1004ms
rtt min/avg/max/mdev = 2.259/2.469/2.679/0.210 ms
┌──(kali㉿kali)-[~]
└─$ ping 172.31.123.30
PING 172.31.123.30 (172.31.123.30) 56(84) bytes of data.
64 bytes from 172.31.123.30: icmp_seq=1 ttl=63 time=3.59 ms
64 bytes from 172.31.123.30: icmp_seq=2 ttl=63 time=1.97 ms
^C
— 172.31.123.30 ping statistics —
2 packets transmitted, 2 received, 0% packet loss, time 1769ms
rtt min/avg/max/mdev = 1.967/2.776/3.586/0.809 ms
┌──(kali㉿kali)-[~]
└─$
Oracle VM VirtualBox Manager
File Machine Help
Tools
Kali Linux
Running
Ubuntu 14.04 Server
Running
bitnami-elk
Running
Ubuntu Gateway a...
Running
Ubuntu Server 22.04 (Zab...
Running
New
Storage
Controller: IDE
IDE Secondary Device 0: [Optical Drive] Empty
Right Ctrl
Ubuntu 14.04 Server [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Ubuntu 14.04.6 LTS wordpress tty1
wordpress login: student
Password:
Last login: Fri Feb 24 20:51:36 GMT 2023 on tty1
Welcome to Ubuntu 14.04.6 LTS (GNU/Linux 4.4.0-148-generic x86_64)
* Documentation: https://help.ubuntu.com/
Ubuntu Gateway and Router [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
gatewayrouter login: [38.072590] cloud-init[992]: Cloud-init v. 22.4.2-0ubuntu0~22.04.1 running '
modules:config' at Sat, 25 Feb 2023 11:55:01 +0000. Up 38.00 seconds.
[38.743076] cloud-init[999]: Cloud-init v. 22.4.2-0ubuntu0~22.04.1 running 'modules:final' at Sat
, 25 Feb 2023 11:55:01 +0000. Up 38.68 seconds.
[38.847573] cloud-init[999]: Cloud-init v. 22.4.2-0ubuntu0~22.04.1 finished at Sat, 25 Feb 2023 1
1:55:01 +0000. Datasource DataSourceNone. Up 38.84 seconds
[38.848671] cloud-init[999]: 2023-02-25 11:55:01,969 - cc_final_message.py[WARNING]: Used fallbac
k datasource
student
Password:
Welcome to Ubuntu 22.04.1 LTS (GNU/Linux 5.15.0-60-generic x86_64)
* Documentation: https://help.ubuntu.com
* Management: https://landscape.canonical.com
* Support: https://ubuntu.com/advantage
System information as of Sat 25 Feb 11:55:14 UTC 2023
System load: 0.67578125 Users logged in: 0
Usage of /: 53.8% of 11.21GB IPv4 address for enp0s10: 172.31.123.1
Memory usage: 12% IPv4 address for enp0s3: 10.0.2.15
Swap usage: 0% IPv4 address for enp0s8: 192.168.123.1
Processes: 133 IPv4 address for enp0s9: 10.10.123.1
* Strictly confined Kubernetes makes edge and IoT secure. Learn how MicroK8s
just raised the bar for easy, resilient and secure K8s cluster deployment.
https://ubuntu.com/engage/secure-kubernetes-at-the-edge
13 updates can be applied immediately.
2 of these updates are standard security updates.
To see these additional updates run: apt list --upgradable
Last login: Fri Feb 24 20:41:49 UTC 2023 on tty1
student@gatewayrouter:~$
Right Ctrl
list --upgradable
Last login: Fri Feb 24 23:21:18 UTC 2023 on tty1
student@zabbix:~$
Right Ctrl
11:56
Right Ctrl
ENG
11:56 AM
Saturday
25/02/2023

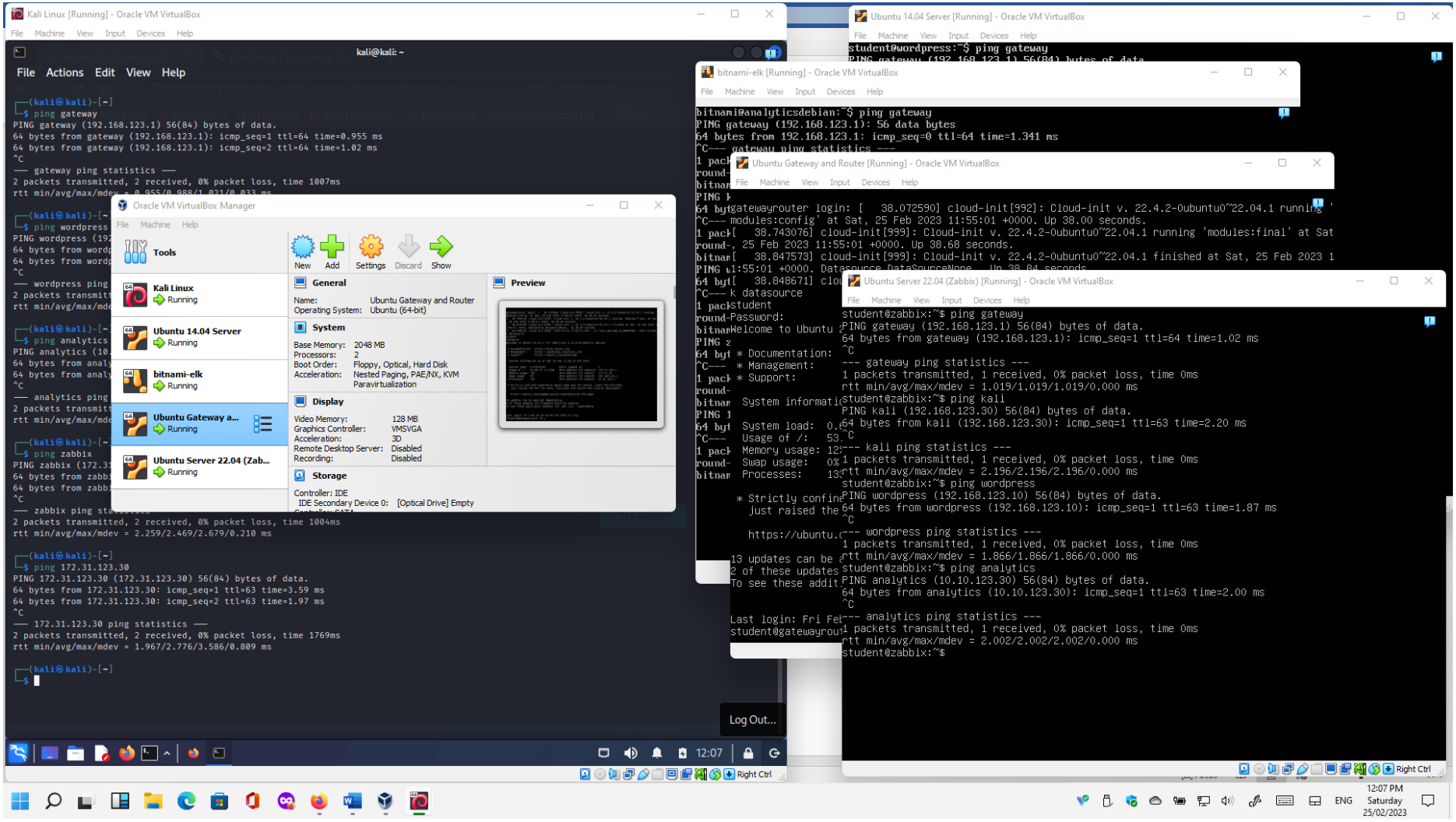
3.


Kali Linux [Running] - Oracle VM VirtualBox
kali@kali: ~
File Actions Edit View Help
Ubuntu 14.04 Server [Running] - Oracle VM VirtualBox
Oracle VM VirtualBox Manager
Tools
Kali Linux
Running
Ubuntu 14.04 Server
Running
bitnami-elk
Running
Ubuntu Gateway a...
Running
Ubuntu Server 22.04 (Zab...
Running
Storage
Controller: IDE
IDE Secondary Device 0: [Optical Drive] Empty
Right Ctrl
12:01 PM
Saturday
25/02/2023

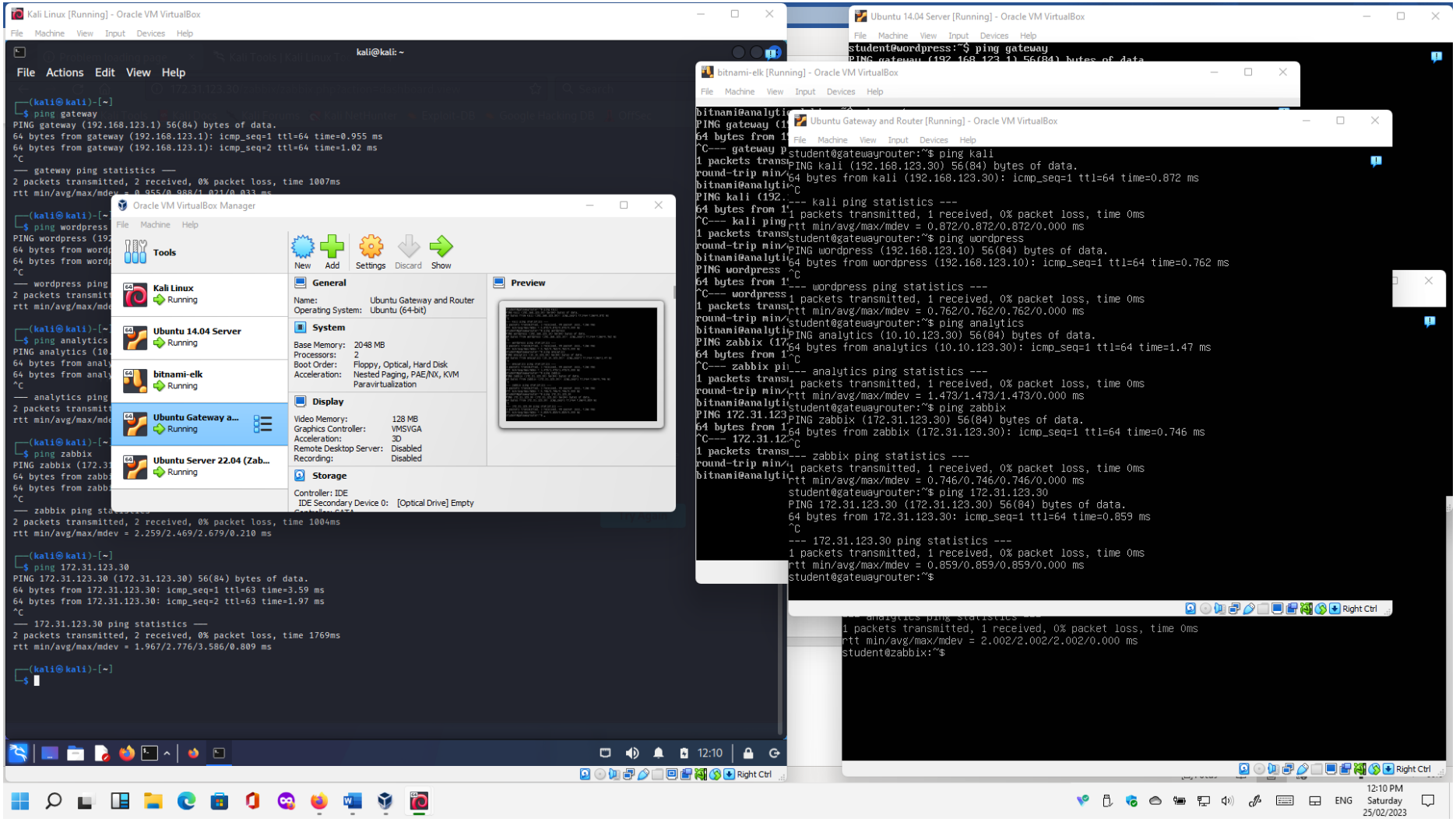
4.


Kali Linux [Running] - Oracle VM VirtualBox
kali@kali: ~
File Actions Edit View Help
(kali㉿kali)-[~]
$ ping gateway
PING gateway (192.168.123.1) 56(84) bytes of data.
64 bytes from gateway (192.168.123.1): icmp_seq=1 ttl=64 time=0.955 ms
64 bytes from gateway (192.168.123.1): icmp_seq=2 ttl=64 time=1.02 ms
^C
— gateway ping statistics —
2 packets transmitted, 2 received, 0% packet loss, time 1007ms
rtt min/avg/max/mdev = 0.955/0.988/1.021/0.033 ms
(kali㉿kali)-[~]
$ ping wordpress
PING wordpress (192.168.123.10) 56(84) bytes of data.
64 bytes from wordpress (192.168.123.10): icmp_seq=1 ttl=64 time=0.988 ms
64 bytes from wordpress (192.168.123.10): icmp_seq=2 ttl=64 time=0.575 ms
^C
— wordpress ping statistics —
2 packets transmitted, 2 received, 0% packet loss, time 1362ms
rtt min/avg/max/mdev = 0.575/0.781/0.988/0.206 ms
(kali㉿kali)-[~]
$ ping analytics
PING analytics (10.10.123.30) 56(84) bytes of data.
64 bytes from analytics (10.10.123.30): icmp_seq=1 ttl=63 time=3.08 ms
64 bytes from analytics (10.10.123.30): icmp_seq=2 ttl=63 time=2.28 ms
^C
— analytics ping statistics —
2 packets transmitted, 2 received, 0% packet loss, time 1008ms
rtt min/avg/max/mdev = 2.284/2.683/3.082/0.399 ms
(kali㉿kali)-[~]
$ ping zabbix
PING zabbix (172.31.123.30) 56(84) bytes of data.
64 bytes from zabbix (172.31.123.30): icmp_seq=1 ttl=63 time=2.26 ms
64 bytes from zabbix (172.31.123.30): icmp_seq=2 ttl=63 time=2.68 ms
^C
— zabbix ping statistics —
2 packets transmitted, 2 received, 0% packet loss, time 1004ms
rtt min/avg/max/mdev = 2.259/2.469/2.679/0.210 ms
(kali㉿kali)-[~]
$ ping 172.31.123.30
PING 172.31.123.30 (172.31.123.30) 56(84) bytes of data.
64 bytes from 172.31.123.30: icmp_seq=1 ttl=63 time=3.59 ms
64 bytes from 172.31.123.30: icmp_seq=2 ttl=63 time=1.97 ms
^C
— 172.31.123.30 ping statistics —
2 packets transmitted, 2 received, 0% packet loss, time 1769ms
rtt min/avg/max/mdev = 1.967/2.776/3.586/0.809 ms
(kali㉿kali)-[~]
$
Oracle VM VirtualBox Manager
Tools
Kali Linux Running
Ubuntu 14.04 Server Running
bitnami-elk Running
Ubuntu Gateway a... Running
Ubuntu Server 22.04 (Zab... Running
Ubuntu 14.04 Server [Running] - Oracle VM VirtualBox
student@wordpress:~$ ping gateway
bitnami-elk [Running] - Oracle VM VirtualBox
bitnami@analyticsdebian:~$ ping gateway
PING gateway (192.168.123.1): 56 data bytes
64 bytes from 192.168.123.1: icmp_seq=0 ttl=64 time=1.341 ms
^C--- gateway ping statistics ---
1 packets transmitted, 1 packets received, 0% packet loss
round-trip min/avg/max/stddev = 1.341/1.341/1.341/0.000 ms
bitnami@analyticsdebian:~$ ping kali
PING kali (192.168.123.30): 56 data bytes
64 bytes from 192.168.123.30: icmp_seq=0 ttl=63 time=3.032 ms
^C--- kali ping statistics ---
1 packets transmitted, 1 packets received, 0% packet loss
round-trip min/avg/max/stddev = 3.032/3.032/3.032/0.000 ms
bitnami@analyticsdebian:~$ ping wordpress
PING wordpress (192.168.123.10): 56 data bytes
64 bytes from 192.168.123.10: icmp_seq=0 ttl=63 time=2.951 ms
^C--- wordpress ping statistics ---
1 packets transmitted, 1 packets received, 0% packet loss
round-trip min/avg/max/stddev = 2.951/2.951/2.951/0.000 ms
bitnami@analyticsdebian:~$ ping zabbix
PING zabbix (172.31.123.30): 56 data bytes
64 bytes from 172.31.123.30: icmp_seq=0 ttl=63 time=2.380 ms
^C--- zabbix ping statistics ---
1 packets transmitted, 1 packets received, 0% packet loss
round-trip min/avg/max/stddev = 2.380/2.380/2.380/0.000 ms
bitnami@analyticsdebian:~$ ping 172.31.123.30
PING 172.31.123.30 (172.31.123.30): 56 data bytes
64 bytes from 172.31.123.30: icmp_seq=0 ttl=63 time=3.268 ms
^C--- 172.31.123.30 ping statistics ---
1 packets transmitted, 1 packets received, 0% packet loss
round-trip min/avg/max/stddev = 3.268/3.268/3.268/0.000 ms
bitnami@analyticsdebian:~$
Right Ctrl
Last login: Fri Feb 24 20:41:49 UTC 2023 on tty1
student@gatewayrouter:~$
Storage
Controller: IDE
IDE Secondary Device 0: [Optical Drive] Empty
list --upgradable
Last login: Fri Feb 24 23:21:18 UTC 2023 on tty1
student@zabbix:~$
12:04
ENG
12:04 PM
Saturday
25/02/2023

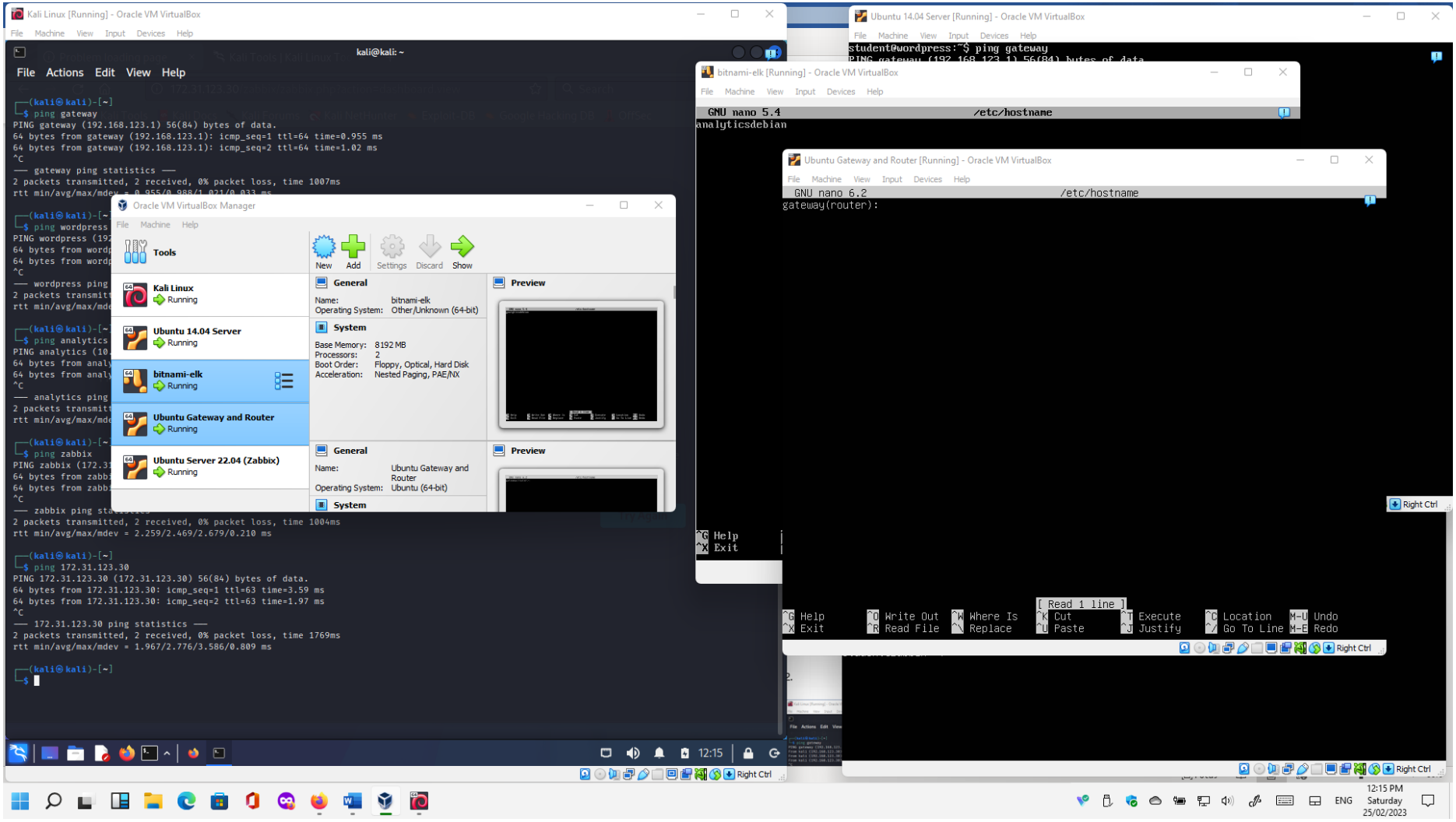
5.

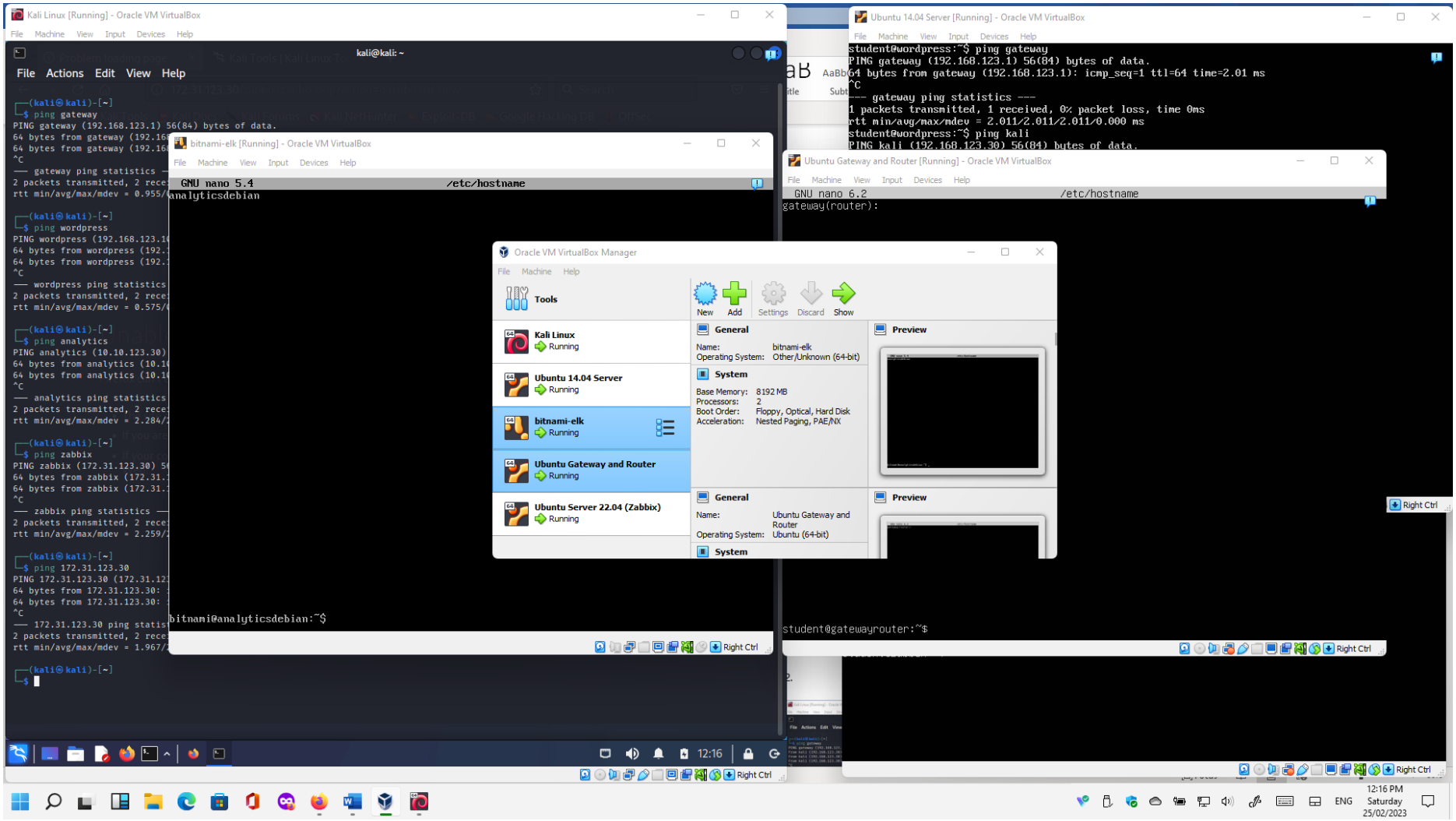

Kali Linux [Running] - Oracle VM VirtualBox
kali@kali: ~
File Actions Edit View Help
Oracle VM VirtualBox Manager
Tools
Kali Linux
Running
Ubuntu 14.04 Server
Running
bitnami-elk
Running
Ubuntu Gateway a...
Running
Ubuntu Server 22.04 (Zab...
Running
General
Name: Ubuntu Gateway and Router
Operating System: Ubuntu (64-bit)
System
Base Memory: 2048 MB
Processors: 2
Boot Order: Floppy, Optical, Hard Disk
Acceleration: Nested Paging, PAE/NX, KVM
Paravirtualization
Display
Video Memory: 128 MB
Graphics Controller: VMSVGA
Acceleration: 3D
Remote Desktop Server: Disabled
Recording: Disabled
Storage
Controller: IDE
IDE Secondary Device 0: [Optical Drive] Empty
Preview
Log Out...
Ubuntu 14.04 Server [Running] - Oracle VM VirtualBox
student@wordpress:~$ ping gateway
bitnami-elk [Running] - Oracle VM VirtualBox
bitnami@analyticsdebian:~$ ping gateway
PING gateway (192.168.123.1): 56 data bytes
64 bytes from 192.168.123.1: icmp_seq=0 ttl=64 time=1.341 ms
Ubuntu Gateway and Router [Running] - Oracle VM VirtualBox
Ubuntu Server 22.04 (Zabbix) [Running] - Oracle VM VirtualBox
student@zabbix:~$ ping gateway
PING gateway (192.168.123.1) 56(84) bytes of data.
64 bytes from gateway (192.168.123.1): icmp_seq=1 ttl=64 time=1.02 ms
--- gateway ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 1.019/1.019/1.019/0.000 ms
student@zabbix:~$ ping kali
PING kali (192.168.123.30) 56(84) bytes of data.
64 bytes from kali (192.168.123.30): icmp_seq=1 ttl=63 time=2.20 ms
--- kali ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 2.196/2.196/2.196/0.000 ms
student@zabbix:~$ ping wordpress
PING wordpress (192.168.123.10) 56(84) bytes of data.
64 bytes from wordpress (192.168.123.10): icmp_seq=1 ttl=63 time=1.87 ms
--- wordpress ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 1.866/1.866/1.866/0.000 ms
student@zabbix:~$ ping analytics
PING analytics (10.10.123.30) 56(84) bytes of data.
64 bytes from analytics (10.10.123.30): icmp_seq=1 ttl=63 time=2.00 ms
--- analytics ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 2.002/2.002/2.002/0.000 ms
student@zabbix:~$
12:07 PM
Saturday
25/02/2023

1.


Kali Linux [Running] - Oracle VM VirtualBox
kali@kali: ~
File Actions Edit View Help
Oracle VM VirtualBox Manager
Tools
Kali Linux
Running
Ubuntu 14.04 Server
Running
bitnami-elk
Running
Ubuntu Gateway a...
Running
Ubuntu Server 22.04 (Zab...
Running
New
Add
Settings
Discard
Show
General
Name: Ubuntu Gateway and Router
Operating System: Ubuntu (64-bit)
System
Base Memory: 2048 MB
Processors: 2
Boot Order: Floppy, Optical, Hard Disk
Acceleration: Nested Paging, PAE/NX, KVM
Paravirtualization
Display
Video Memory: 128 MB
Graphics Controller: VMSVGA
Acceleration: 3D
Remote Desktop Server: Disabled
Recording: Disabled
Storage
Controller: IDE
IDE Secondary Device 0: [Optical Drive] Empty
Preview
Ubuntu 14.04 Server [Running] - Oracle VM VirtualBox
bitnami-elk [Running] - Oracle VM VirtualBox
Ubuntu Gateway and Router [Running] - Oracle VM VirtualBox
Right Ctrl
12:10 PM
Saturday
25/02/2023
ENG

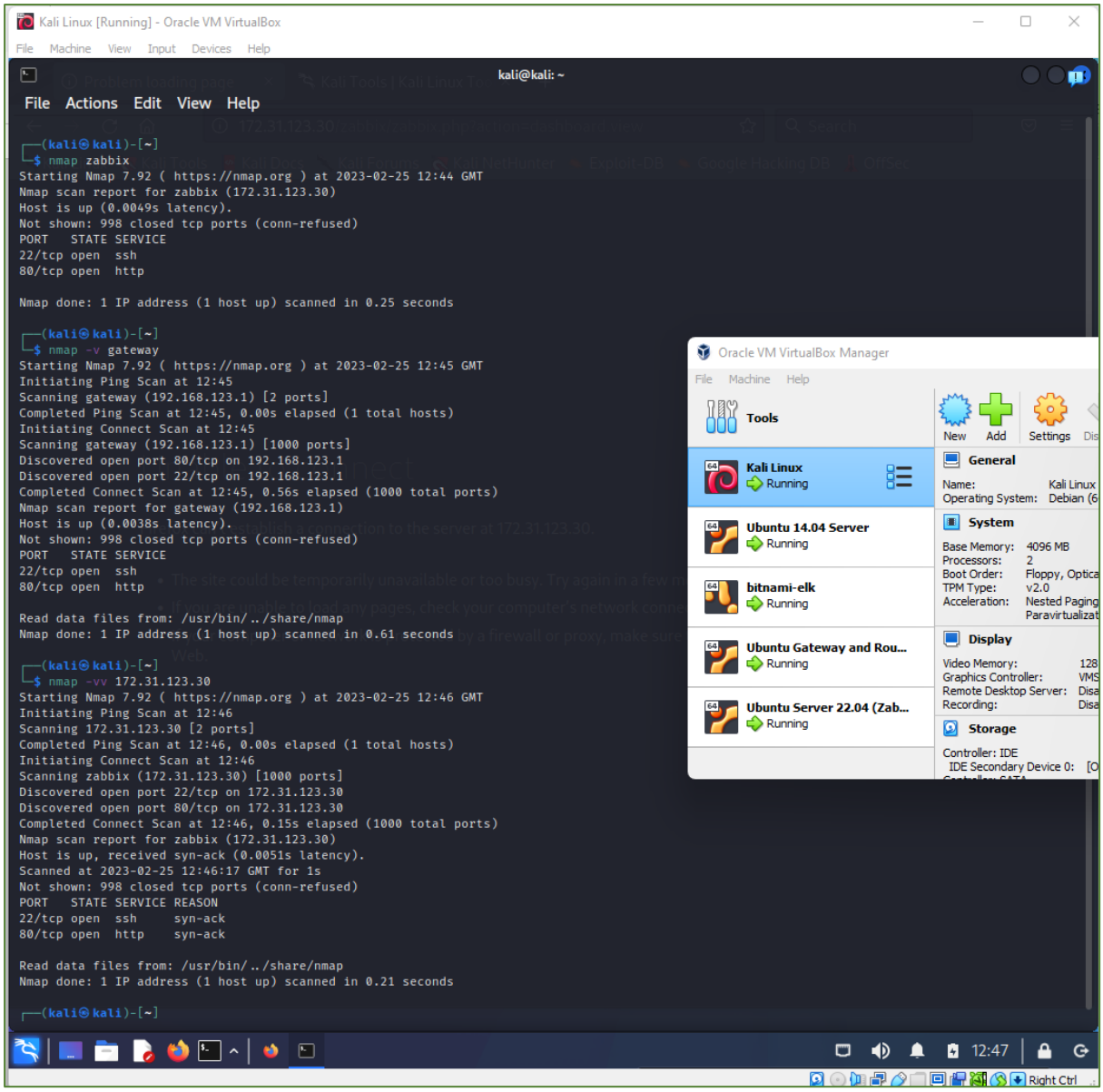
Wow factor demonstration A:

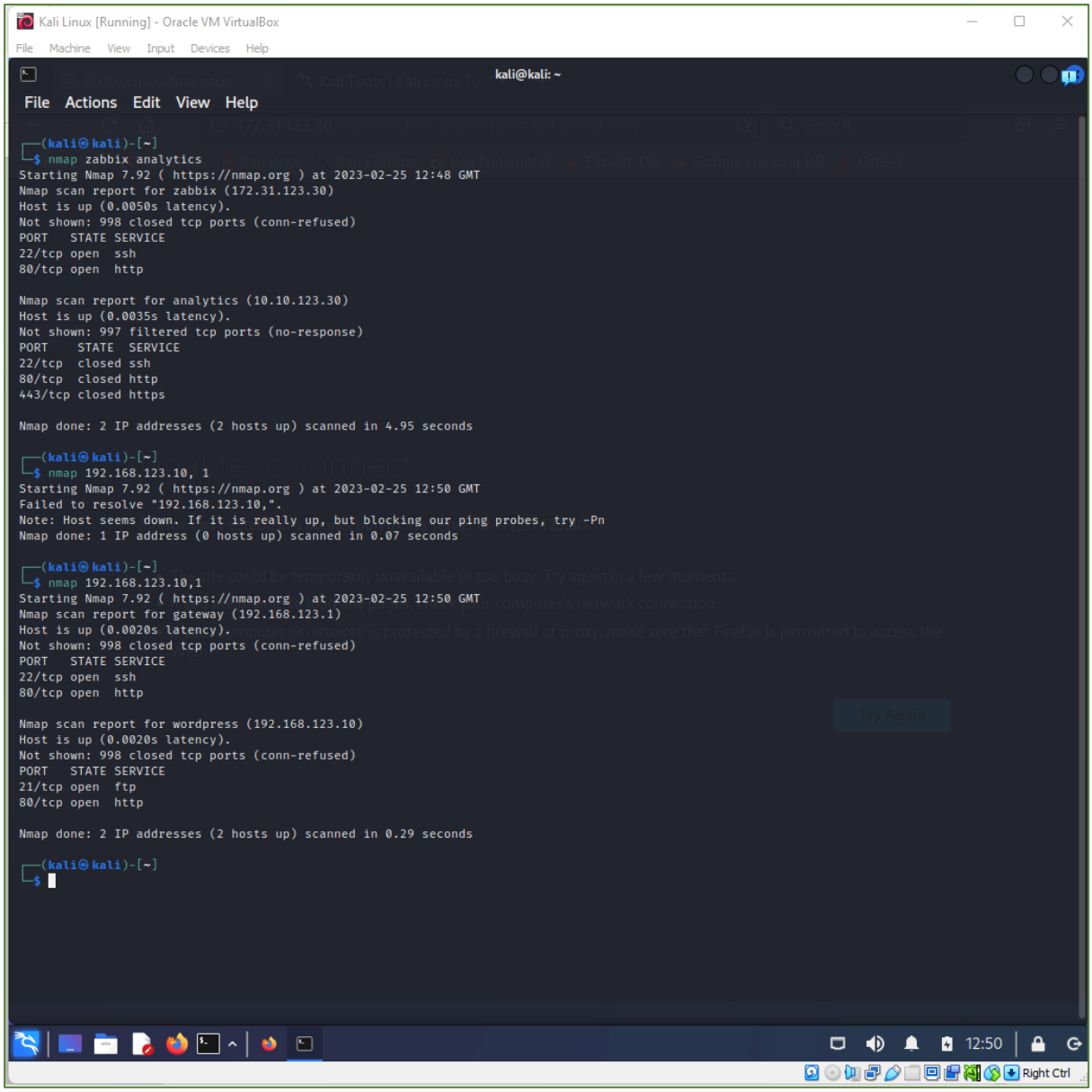


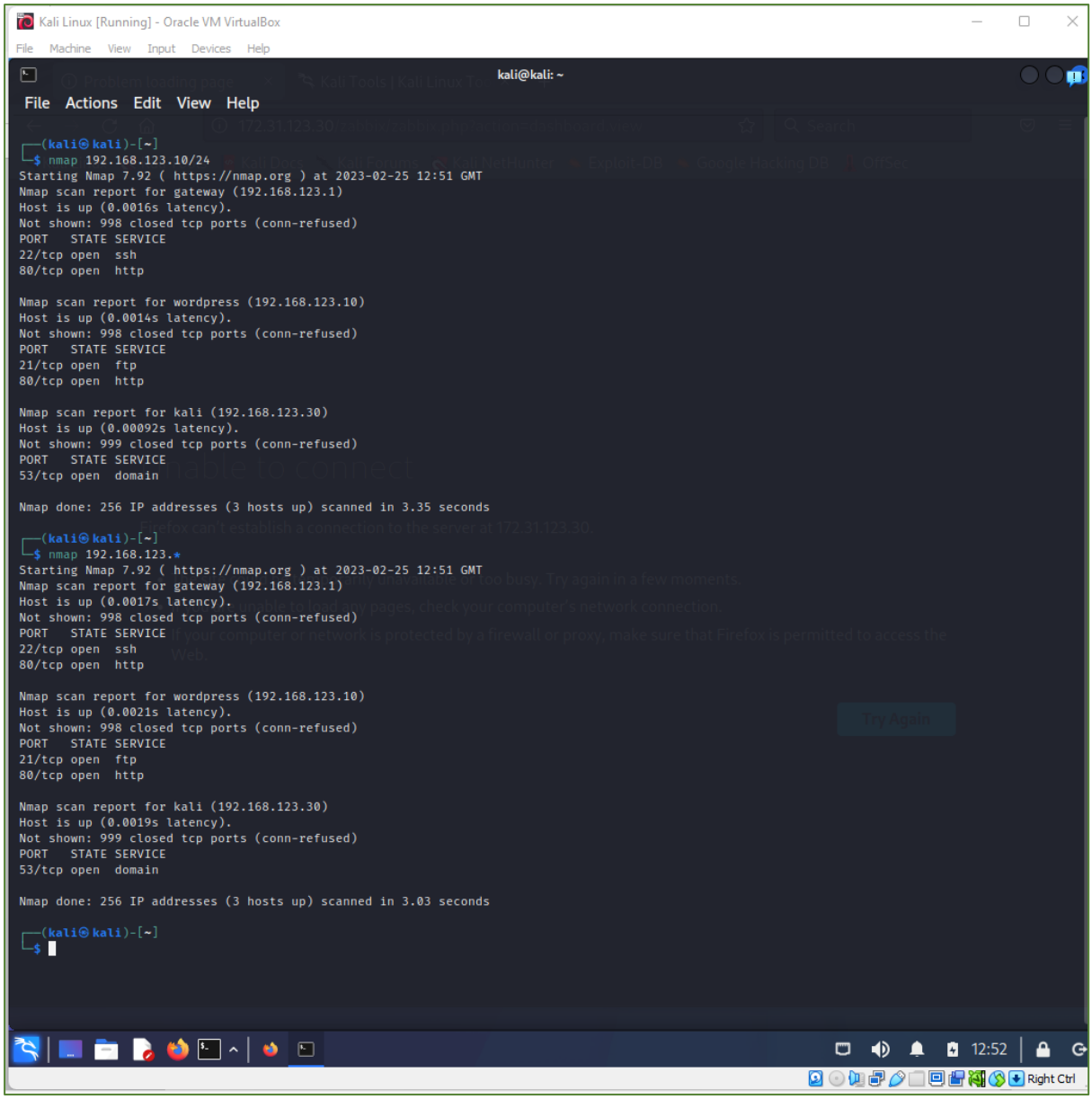

Kali Linux [Running] - Oracle VM VirtualBox
kali@kali: ~
File Actions Edit View Help
bitnami-elk [Running] - Oracle VM VirtualBox
GNU nano 5.4 /etc/hostname
analyticsdebian
bitnami@analyticsdebian:~$
Ubuntu 14.04 Server [Running] - Oracle VM VirtualBox
student@wordpress:~$ ping gateway
PING gateway (192.168.123.1) 56(84) bytes of data.
64 bytes from gateway (192.168.123.1): icmp_seq=1 ttl=64 time=2.01 ms
^C
--- gateway ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 2.011/2.011/2.011/0.000 ms
student@wordpress:~$ ping kali
PING kali (192.168.123.30) 56(84) bytes of data.
Ubuntu Gateway and Router [Running] - Oracle VM VirtualBox
GNU nano 6.2 /etc/hostname
gateway(router):
student@gatewayrouter:~$
Oracle VM VirtualBox Manager
Tools
New Add Settings Discard Show
Kali Linux Running
Ubuntu 14.04 Server Running
bitnami-elk Running
Ubuntu Gateway and Router Running
Ubuntu Server 22.04 (Zabbix) Running
General
Name: bitnami-elk
Operating System: Other/Unknown (64-bit)
System
Base Memory: 8192 MB
Processors: 2
Boot Order: Floppy, Optical, Hard Disk
Acceleration: Nested Paging, PAE/NX
Preview
Name: Ubuntu Gateway and Router
Operating System: Ubuntu (64-bit)
Right Ctrl
12:16
ENG
12:16 PM
Saturday
25/02/2023

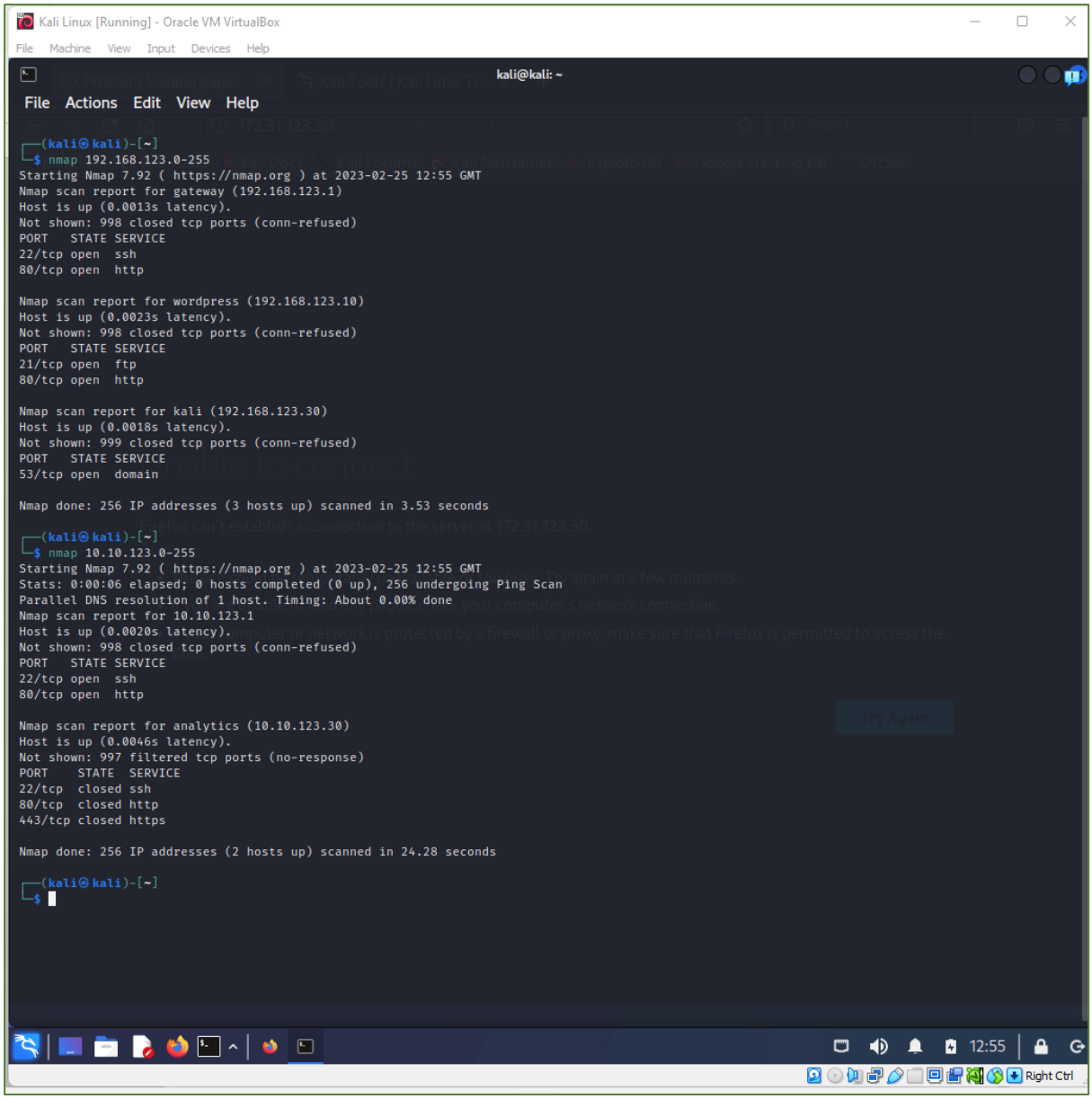
Portfolio Requirement B: Exploring NMAP Commands

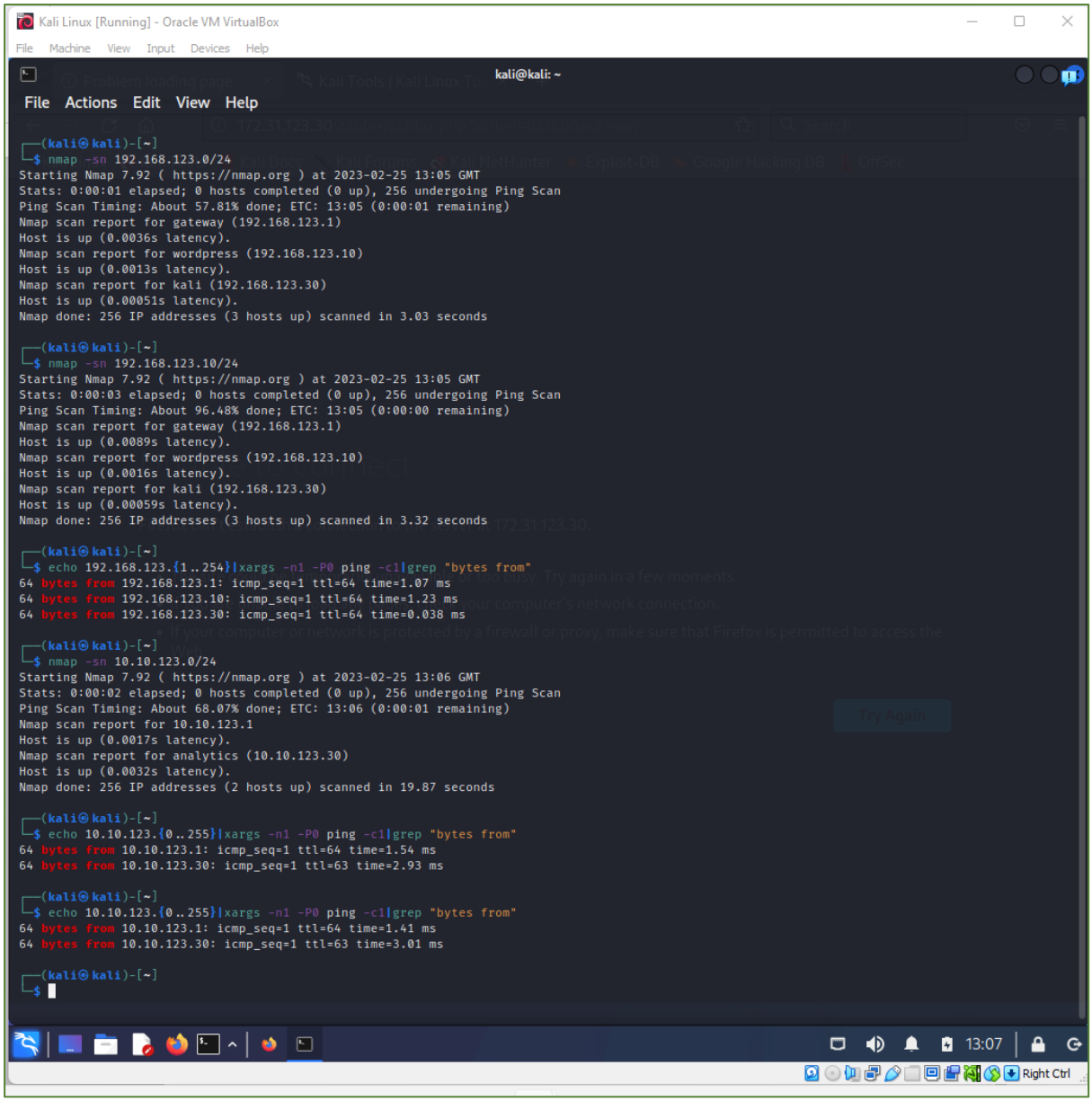
From your Kali virtual machine, test the following **nmap** commands on your sandboxed network. 1 to 16 different commands.

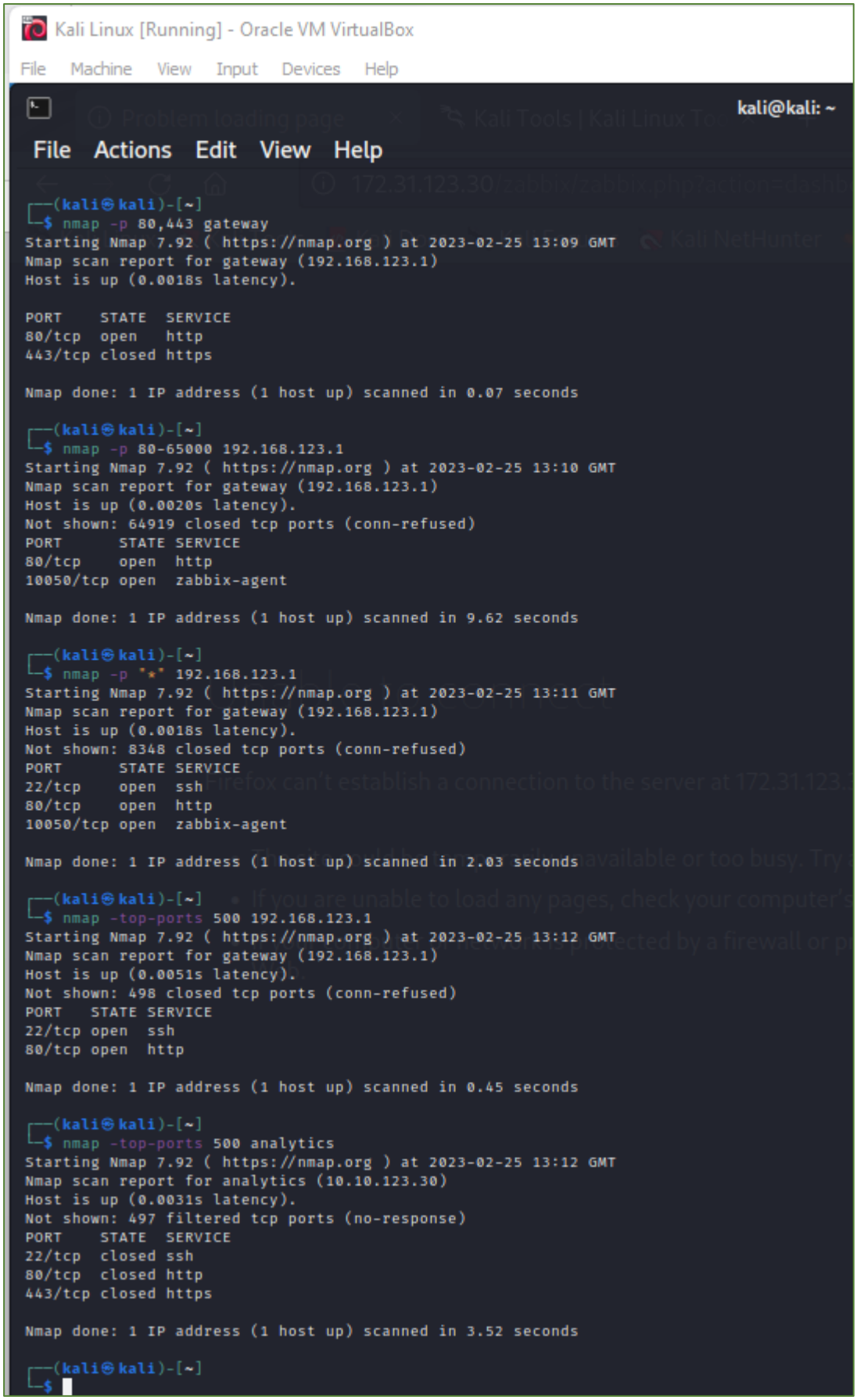

Kali Linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
kali@kali: ~
File Actions Edit View Help
┌──(kali㉿kali)-[~]
└─$ nmap zabbix
Starting Nmap 7.92 (https://nmap.org) at 2023-02-25 12:44 GMT
Nmap scan report for zabbix (172.31.123.30)
Host is up (0.0049s latency).
Not shown: 998 closed tcp ports (conn-refused)
PORT STATE SERVICE
22/tcp open ssh
80/tcp open http
Nmap done: 1 IP address (1 host up) scanned in 0.25 seconds
┌──(kali㉿kali)-[~]
└─$ nmap -v gateway
Starting Nmap 7.92 (https://nmap.org) at 2023-02-25 12:45 GMT
Initiating Ping Scan at 12:45
Scanning gateway (192.168.123.1) [2 ports]
Completed Ping Scan at 12:45, 0.00s elapsed (1 total hosts)
Initiating Connect Scan at 12:45
Scanning gateway (192.168.123.1) [1000 ports]
Discovered open port 80/tcp on 192.168.123.1
Discovered open port 22/tcp on 192.168.123.1
Completed Connect Scan at 12:45, 0.56s elapsed (1000 total ports)
Nmap scan report for gateway (192.168.123.1)
Host is up (0.0038s latency).
Not shown: 998 closed tcp ports (conn-refused)
PORT STATE SERVICE
22/tcp open ssh
80/tcp open http
Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 0.61 seconds
┌──(kali㉿kali)-[~]
└─$ nmap -vv 172.31.123.30
Starting Nmap 7.92 (https://nmap.org) at 2023-02-25 12:46 GMT
Initiating Ping Scan at 12:46
Scanning 172.31.123.30 [2 ports]
Completed Ping Scan at 12:46, 0.00s elapsed (1 total hosts)
Initiating Connect Scan at 12:46
Scanning zabbix (172.31.123.30) [1000 ports]
Discovered open port 22/tcp on 172.31.123.30
Discovered open port 80/tcp on 172.31.123.30
Completed Connect Scan at 12:46, 0.15s elapsed (1000 total ports)
Nmap scan report for zabbix (172.31.123.30)
Host is up, received syn-ack (0.0051s latency).
Scanned at 2023-02-25 12:46:17 GMT for 1s
Not shown: 998 closed tcp ports (conn-refused)
PORT STATE SERVICE REASON
22/tcp open ssh syn-ack
80/tcp open http syn-ack
Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 0.21 seconds
┌──(kali㉿kali)-[~]
Oracle VM VirtualBox Manager
File Machine Help
Tools
New Add Settings
Kali Linux
Running
Ubuntu 14.04 Server
Running
bitnami-elk
Running
Ubuntu Gateway and Rou...
Running
Ubuntu Server 22.04 (Zab...
Running
General
Name: Kali Linux
Operating System: Debian (6
System
Base Memory: 4096 MB
Processors: 2
Boot Order: Floppy, Optica
TPM Type: v2.0
Acceleration: Nested Paging
Paravirtualizat
Display
Video Memory: 128
Graphics Controller: VMS
Remote Desktop Server: Disa
Recording: Disa
Storage
Controller: IDE
IDE Secondary Device 0: [O
12:47
Right Ctrl


Kali Linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
kali@kali: ~
File Actions Edit View Help
┌──(kali㉿kali)-[~]
└─$ nmap zabbix analytics
Starting Nmap 7.92 (https://nmap.org) at 2023-02-25 12:48 GMT
Nmap scan report for zabbix (172.31.123.30)
Host is up (0.0050s latency).
Not shown: 998 closed tcp ports (conn-refused)
PORT STATE SERVICE
22/tcp open ssh
80/tcp open http
Nmap scan report for analytics (10.10.123.30)
Host is up (0.0035s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT STATE SERVICE
22/tcp closed ssh
80/tcp closed http
443/tcp closed https
Nmap done: 2 IP addresses (2 hosts up) scanned in 4.95 seconds
┌──(kali㉿kali)-[~]
└─$ nmap 192.168.123.10, 1
Starting Nmap 7.92 (https://nmap.org) at 2023-02-25 12:50 GMT
Failed to resolve "192.168.123.10,".
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 0.07 seconds
┌──(kali㉿kali)-[~]
└─$ nmap 192.168.123.10,1
Starting Nmap 7.92 (https://nmap.org) at 2023-02-25 12:50 GMT
Nmap scan report for gateway (192.168.123.1)
Host is up (0.0020s latency).
Not shown: 998 closed tcp ports (conn-refused)
PORT STATE SERVICE
22/tcp open ssh
80/tcp open http
Nmap scan report for wordpress (192.168.123.10)
Host is up (0.0020s latency).
Not shown: 998 closed tcp ports (conn-refused)
PORT STATE SERVICE
21/tcp open ftp
80/tcp open http
Nmap done: 2 IP addresses (2 hosts up) scanned in 0.29 seconds
┌──(kali㉿kali)-[~]
└─$
12:50
Right Ctrl


Kali Linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
kali@kali: ~
File Actions Edit View Help
(kali㉿kali)-[~]
$ nmap 192.168.123.10/24
Starting Nmap 7.92 (https://nmap.org) at 2023-02-25 12:51 GMT
Nmap scan report for gateway (192.168.123.1)
Host is up (0.0016s latency).
Not shown: 998 closed tcp ports (conn-refused)
PORT STATE SERVICE
22/tcp open ssh
80/tcp open http
Nmap scan report for wordpress (192.168.123.10)
Host is up (0.0014s latency).
Not shown: 998 closed tcp ports (conn-refused)
PORT STATE SERVICE
21/tcp open ftp
80/tcp open http
Nmap scan report for kali (192.168.123.30)
Host is up (0.00092s latency).
Not shown: 999 closed tcp ports (conn-refused)
PORT STATE SERVICE
53/tcp open domain
Nmap done: 256 IP addresses (3 hosts up) scanned in 3.35 seconds
(kali㉿kali)-[~]
$ nmap 192.168.123.*
Starting Nmap 7.92 (https://nmap.org) at 2023-02-25 12:51 GMT
Nmap scan report for gateway (192.168.123.1)
Host is up (0.0017s latency).
Not shown: 998 closed tcp ports (conn-refused)
PORT STATE SERVICE
22/tcp open ssh
80/tcp open http
Nmap scan report for wordpress (192.168.123.10)
Host is up (0.0021s latency).
Not shown: 998 closed tcp ports (conn-refused)
PORT STATE SERVICE
21/tcp open ftp
80/tcp open http
Nmap scan report for kali (192.168.123.30)
Host is up (0.0019s latency).
Not shown: 999 closed tcp ports (conn-refused)
PORT STATE SERVICE
53/tcp open domain
Nmap done: 256 IP addresses (3 hosts up) scanned in 3.03 seconds
(kali㉿kali)-[~]
$
12:52
Right Ctrl

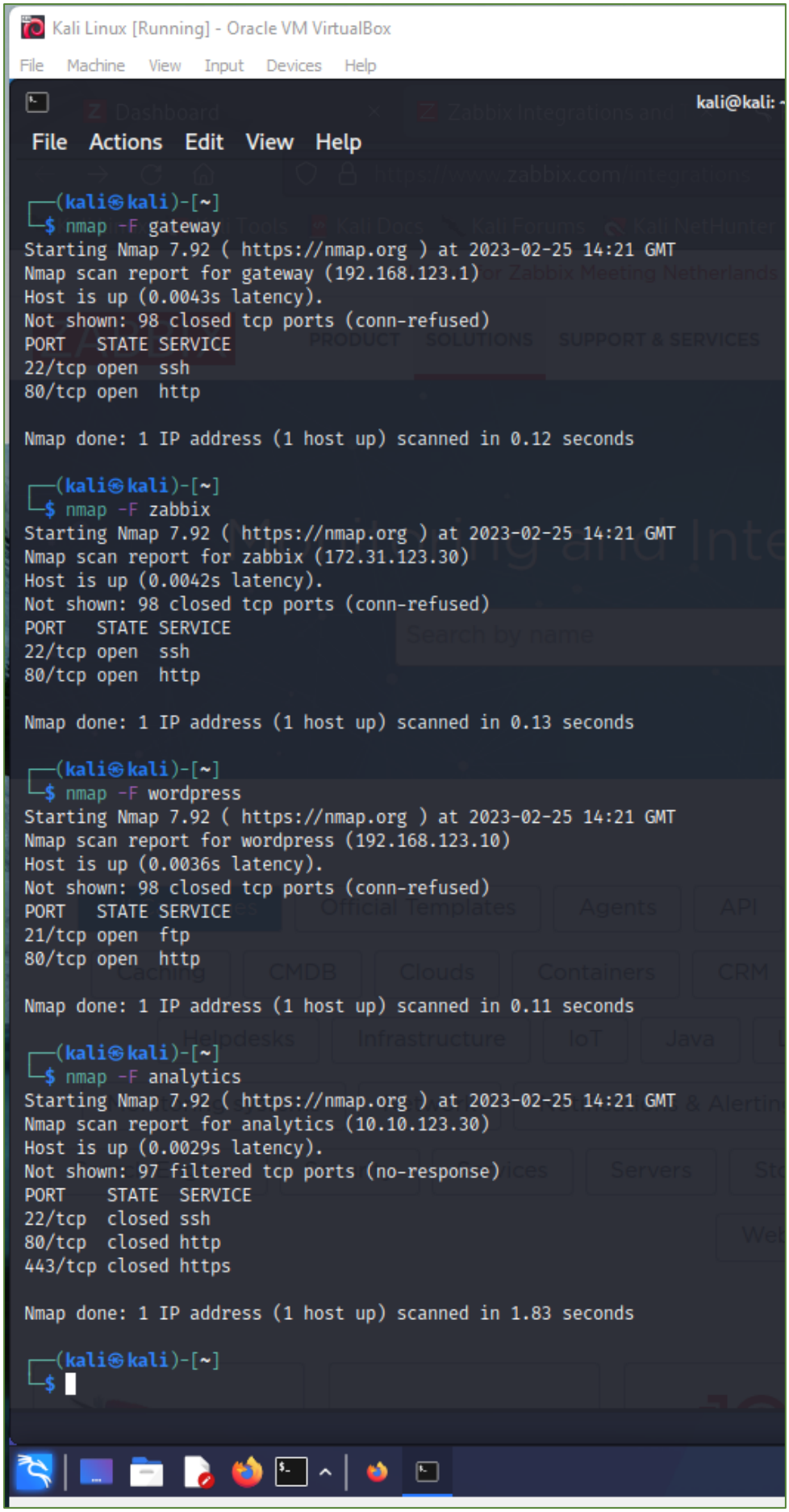

Kali Linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
kali@kali: ~
File Actions Edit View Help
┌──(kali㉿kali)-[~]
└─$ nmap 192.168.123.0-255
Starting Nmap 7.92 (https://nmap.org) at 2023-02-25 12:55 GMT
Nmap scan report for gateway (192.168.123.1)
Host is up (0.0013s latency).
Not shown: 998 closed tcp ports (conn-refused)
PORT STATE SERVICE
22/tcp open ssh
80/tcp open http
Nmap scan report for wordpress (192.168.123.10)
Host is up (0.0023s latency).
Not shown: 998 closed tcp ports (conn-refused)
PORT STATE SERVICE
21/tcp open ftp
80/tcp open http
Nmap scan report for kali (192.168.123.30)
Host is up (0.0018s latency).
Not shown: 999 closed tcp ports (conn-refused)
PORT STATE SERVICE
53/tcp open domain
Nmap done: 256 IP addresses (3 hosts up) scanned in 3.53 seconds
┌──(kali㉿kali)-[~]
└─$ nmap 10.10.123.0-255
Starting Nmap 7.92 (https://nmap.org) at 2023-02-25 12:55 GMT
Stats: 0:00:06 elapsed; 0 hosts completed (0 up), 256 undergoing Ping Scan
Parallel DNS resolution of 1 host. Timing: About 0.00% done
Nmap scan report for 10.10.123.1
Host is up (0.0020s latency).
Not shown: 998 closed tcp ports (conn-refused)
PORT STATE SERVICE
22/tcp open ssh
80/tcp open http
Nmap scan report for analytics (10.10.123.30)
Host is up (0.0046s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT STATE SERVICE
22/tcp closed ssh
80/tcp closed http
443/tcp closed https
Nmap done: 256 IP addresses (2 hosts up) scanned in 24.28 seconds
┌──(kali㉿kali)-[~]
└─$
12:55
Right Ctrl

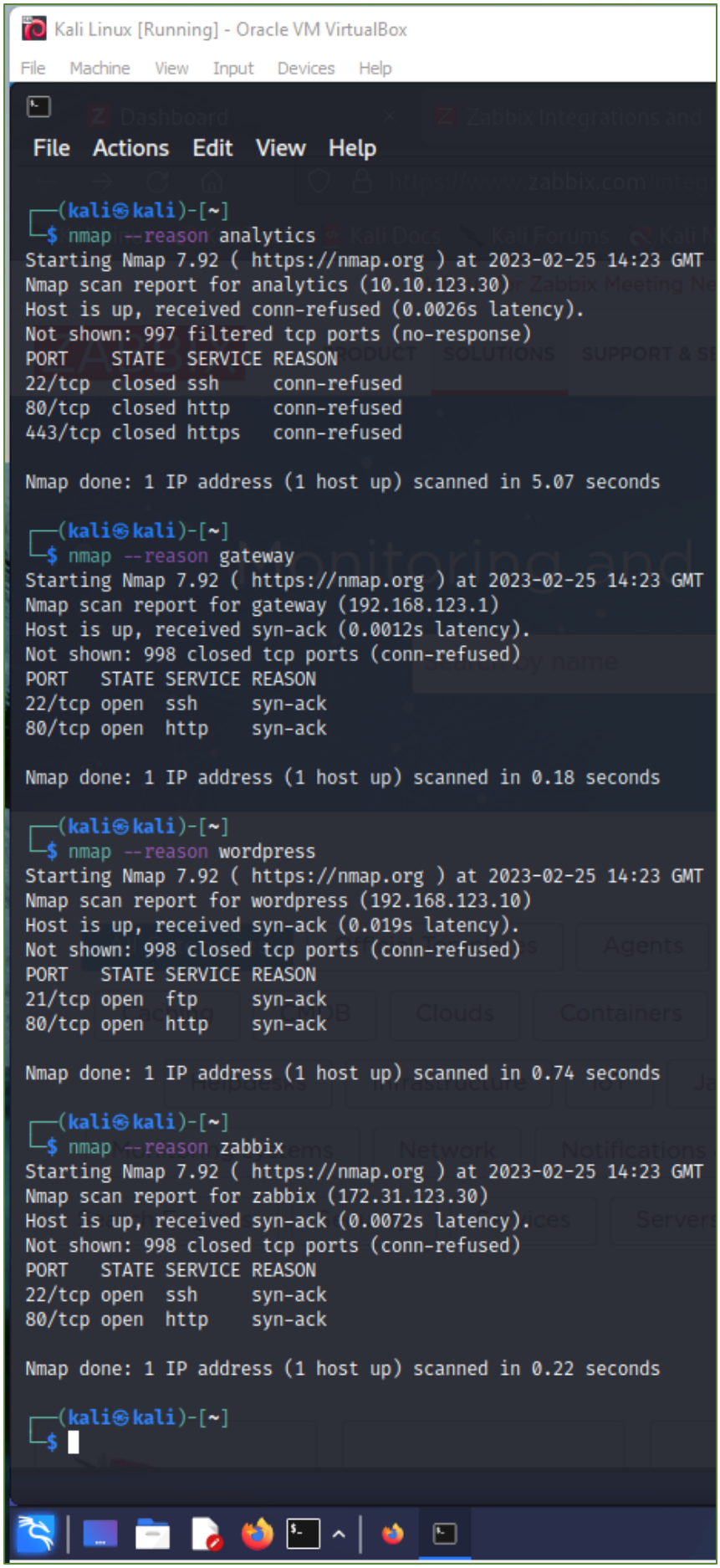

Kali Linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
kali@kali: ~
File Actions Edit View Help
┌──(kali㉿kali)-[~]
└─$ nmap -sn 192.168.123.0/24
Starting Nmap 7.92 (https://nmap.org) at 2023-02-25 13:05 GMT
Stats: 0:00:01 elapsed; 0 hosts completed (0 up), 256 undergoing Ping Scan
Ping Scan Timing: About 57.81% done; ETC: 13:05 (0:00:01 remaining)
Nmap scan report for gateway (192.168.123.1)
Host is up (0.0036s latency).
Nmap scan report for wordpress (192.168.123.10)
Host is up (0.0013s latency).
Nmap scan report for kali (192.168.123.30)
Host is up (0.00051s latency).
Nmap done: 256 IP addresses (3 hosts up) scanned in 3.03 seconds
┌──(kali㉿kali)-[~]
└─$ nmap -sn 192.168.123.10/24
Starting Nmap 7.92 (https://nmap.org) at 2023-02-25 13:05 GMT
Stats: 0:00:03 elapsed; 0 hosts completed (0 up), 256 undergoing Ping Scan
Ping Scan Timing: About 96.48% done; ETC: 13:05 (0:00:00 remaining)
Nmap scan report for gateway (192.168.123.1)
Host is up (0.0089s latency).
Nmap scan report for wordpress (192.168.123.10)
Host is up (0.0016s latency).
Nmap scan report for kali (192.168.123.30)
Host is up (0.00059s latency).
Nmap done: 256 IP addresses (3 hosts up) scanned in 3.32 seconds
┌──(kali㉿kali)-[~]
└─$ echo 192.168.123.{1..254}|xargs -n1 -P0 ping -c1|grep "bytes from"
64 bytes from 192.168.123.1: icmp_seq=1 ttl=64 time=1.07 ms
64 bytes from 192.168.123.10: icmp_seq=1 ttl=64 time=1.23 ms
64 bytes from 192.168.123.30: icmp_seq=1 ttl=64 time=0.038 ms
┌──(kali㉿kali)-[~]
└─$ nmap -sn 10.10.123.0/24
Starting Nmap 7.92 (https://nmap.org) at 2023-02-25 13:06 GMT
Stats: 0:00:02 elapsed; 0 hosts completed (0 up), 256 undergoing Ping Scan
Ping Scan Timing: About 68.07% done; ETC: 13:06 (0:00:01 remaining)
Nmap scan report for 10.10.123.1
Host is up (0.0017s latency).
Nmap scan report for analytics (10.10.123.30)
Host is up (0.0032s latency).
Nmap done: 256 IP addresses (2 hosts up) scanned in 19.87 seconds
┌──(kali㉿kali)-[~]
└─$ echo 10.10.123.{0..255}|xargs -n1 -P0 ping -c1|grep "bytes from"
64 bytes from 10.10.123.1: icmp_seq=1 ttl=64 time=1.54 ms
64 bytes from 10.10.123.30: icmp_seq=1 ttl=63 time=2.93 ms
┌──(kali㉿kali)-[~]
└─$ echo 10.10.123.{0..255}|xargs -n1 -P0 ping -c1|grep "bytes from"
64 bytes from 10.10.123.1: icmp_seq=1 ttl=64 time=1.41 ms
64 bytes from 10.10.123.30: icmp_seq=1 ttl=63 time=3.01 ms
┌──(kali㉿kali)-[~]
└─$
13:07
Right Ctrl

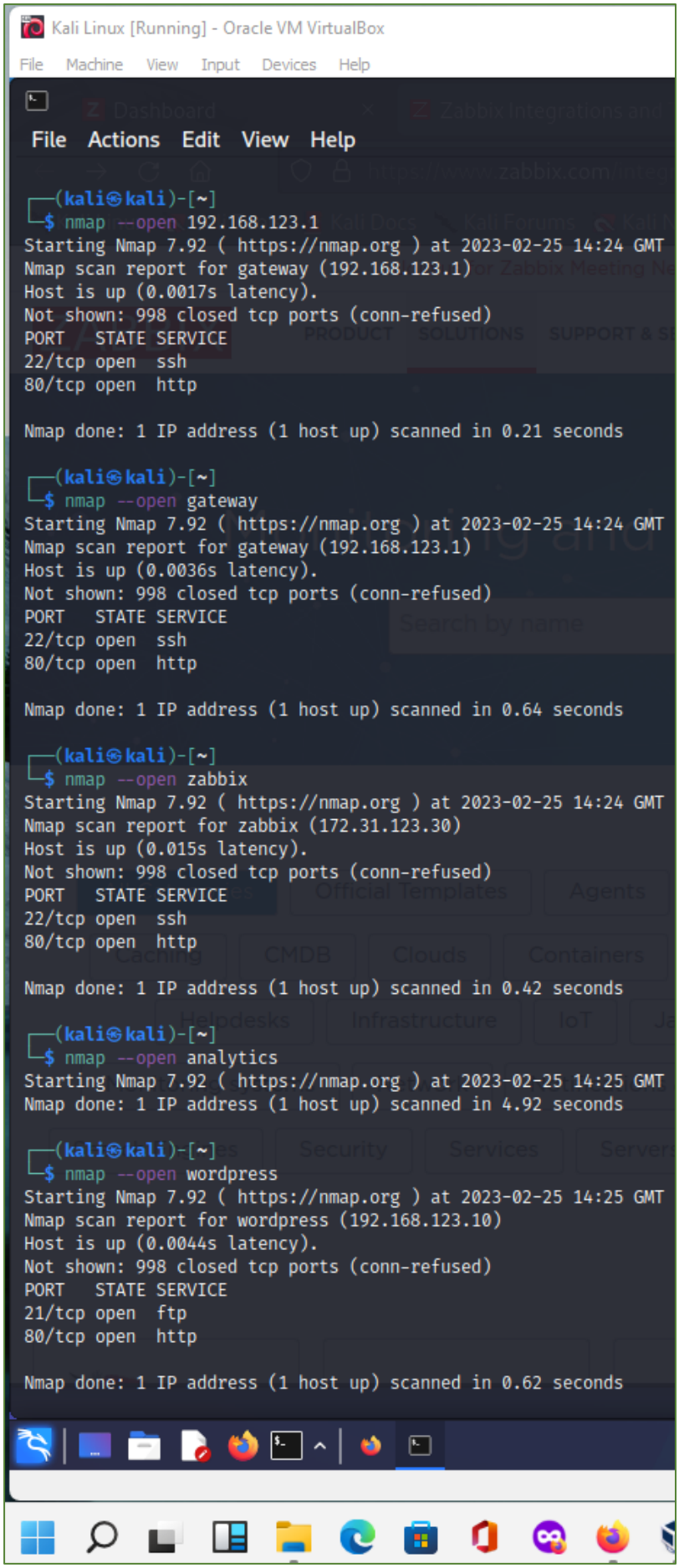

Kali Linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
kali@kali: ~
File Actions Edit View Help
┌──(kali㉿kali)-[~]
└─$ nmap -p 80,443 gateway
Starting Nmap 7.92 (https://nmap.org) at 2023-02-25 13:09 GMT
Nmap scan report for gateway (192.168.123.1)
Host is up (0.0018s latency).
PORT STATE SERVICE
80/tcp open http
443/tcp closed https
Nmap done: 1 IP address (1 host up) scanned in 0.07 seconds
┌──(kali㉿kali)-[~]
└─$ nmap -p 80-65000 192.168.123.1
Starting Nmap 7.92 (https://nmap.org) at 2023-02-25 13:10 GMT
Nmap scan report for gateway (192.168.123.1)
Host is up (0.0020s latency).
Not shown: 64919 closed tcp ports (conn-refused)
PORT STATE SERVICE
80/tcp open http
10050/tcp open zabbix-agent
Nmap done: 1 IP address (1 host up) scanned in 9.62 seconds
┌──(kali㉿kali)-[~]
└─$ nmap -p "*" 192.168.123.1
Starting Nmap 7.92 (https://nmap.org) at 2023-02-25 13:11 GMT
Nmap scan report for gateway (192.168.123.1)
Host is up (0.0018s latency).
Not shown: 8348 closed tcp ports (conn-refused)
PORT STATE SERVICE
22/tcp open ssh
80/tcp open http
10050/tcp open zabbix-agent
Nmap done: 1 IP address (1 host up) scanned in 2.03 seconds
┌──(kali㉿kali)-[~]
└─$ nmap -top-ports 500 192.168.123.1
Starting Nmap 7.92 (https://nmap.org) at 2023-02-25 13:12 GMT
Nmap scan report for gateway (192.168.123.1)
Host is up (0.0051s latency).
Not shown: 498 closed tcp ports (conn-refused)
PORT STATE SERVICE
22/tcp open ssh
80/tcp open http
Nmap done: 1 IP address (1 host up) scanned in 0.45 seconds
┌──(kali㉿kali)-[~]
└─$ nmap -top-ports 500 analytics
Starting Nmap 7.92 (https://nmap.org) at 2023-02-25 13:12 GMT
Nmap scan report for analytics (10.10.123.30)
Host is up (0.0031s latency).
Not shown: 497 filtered tcp ports (no-response)
PORT STATE SERVICE
22/tcp closed ssh
80/tcp closed http
443/tcp closed https
Nmap done: 1 IP address (1 host up) scanned in 3.52 seconds
┌──(kali㉿kali)-[~]
└─$


Kali Linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
File Actions Edit View Help
(kali㉿kali)-[~]
$ nmap -sO 192.168.123.1
You requested a scan type which requires root privileges.
QUITTING!
(kali㉿kali)-[~]
$ sudo su
[sudo] password for kali:
Sorry, try again.
[sudo] password for kali:
(root㉿kali)-[/home/kali]
nmap -sO 192.168.123.1
Starting Nmap 7.92 (https://nmap.org) at 2023-02-25 13:15 GMT
Stats: 0:00:04 elapsed; 0 hosts completed (1 up), 1 undergoing IPProto Scan
IPProto Scan Timing: About 6.88% done; ETC: 13:15 (0:00:41 remaining)
Warning: 192.168.123.1 giving up on port because retransmission cap hit (10).
Stats: 0:00:28 elapsed; 0 hosts completed (1 up), 1 undergoing IPProto Scan
IPProto Scan Timing: About 22.02% done; ETC: 13:17 (0:01:39 remaining)
Stats: 0:02:44 elapsed; 0 hosts completed (1 up), 1 undergoing IPProto Scan
IPProto Scan Timing: About 65.48% done; ETC: 13:19 (0:01:26 remaining)
Nmap scan report for gateway (192.168.123.1)
Host is up (0.0010s latency).
Not shown: 249 closed n/a protocols (proto-unreach)
PROTOCOL STATE SERVICE
1 open icmp
2 open|filtered igmp
6 open tcp
17 open udp
103 open|filtered pim
128 open|filtered sscopmce
136 open|filtered udplite
MAC Address: 08:00:27:6A:7C:8B (Oracle VirtualBox virtual NIC)
Nmap done: 1 IP address (1 host up) scanned in 299.79 seconds
(root㉿kali)-[/home/kali]
nmap -sO gateway
Starting Nmap 7.92 (https://nmap.org) at 2023-02-25 13:20 GMT
Warning: 192.168.123.1 giving up on port because retransmission cap hit (10).
Nmap scan report for gateway (192.168.123.1)
Host is up (0.00097s latency).
Not shown: 250 closed n/a protocols (proto-unreach)
PROTOCOL STATE SERVICE
1 open icmp
2 open|filtered igmp
6 open tcp
17 open udp
103 open|filtered pim
136 open|filtered udplite
MAC Address: 08:00:27:6A:7C:8B (Oracle VirtualBox virtual NIC)
Nmap done: 1 IP address (1 host up) scanned in 287.92 seconds
(root㉿kali)-[/home/kali]
nmap -sO zabbix
Starting Nmap 7.92 (https://nmap.org) at 2023-02-25 13:25 GMT
Warning: 172.31.123.30 giving up on port because retransmission cap hit (10).
Nmap scan report for zabbix (172.31.123.30)
Host is up (0.0020s latency).
Not shown: 246 closed n/a protocols (proto-unreach)
PROTOCOL STATE SERVICE
1 open icmp
2 open|filtered igmp
6 open tcp
17 open udp
47 open|filtered gre
79 open|filtered wb-expak
103 open|filtered pim
121 open|filtered smp
136 open|filtered udplite
220 open|filtered unknown
Nmap done: 1 IP address (1 host up) scanned in 300.73 seconds
(root㉿kali)-[/home/kali]
#

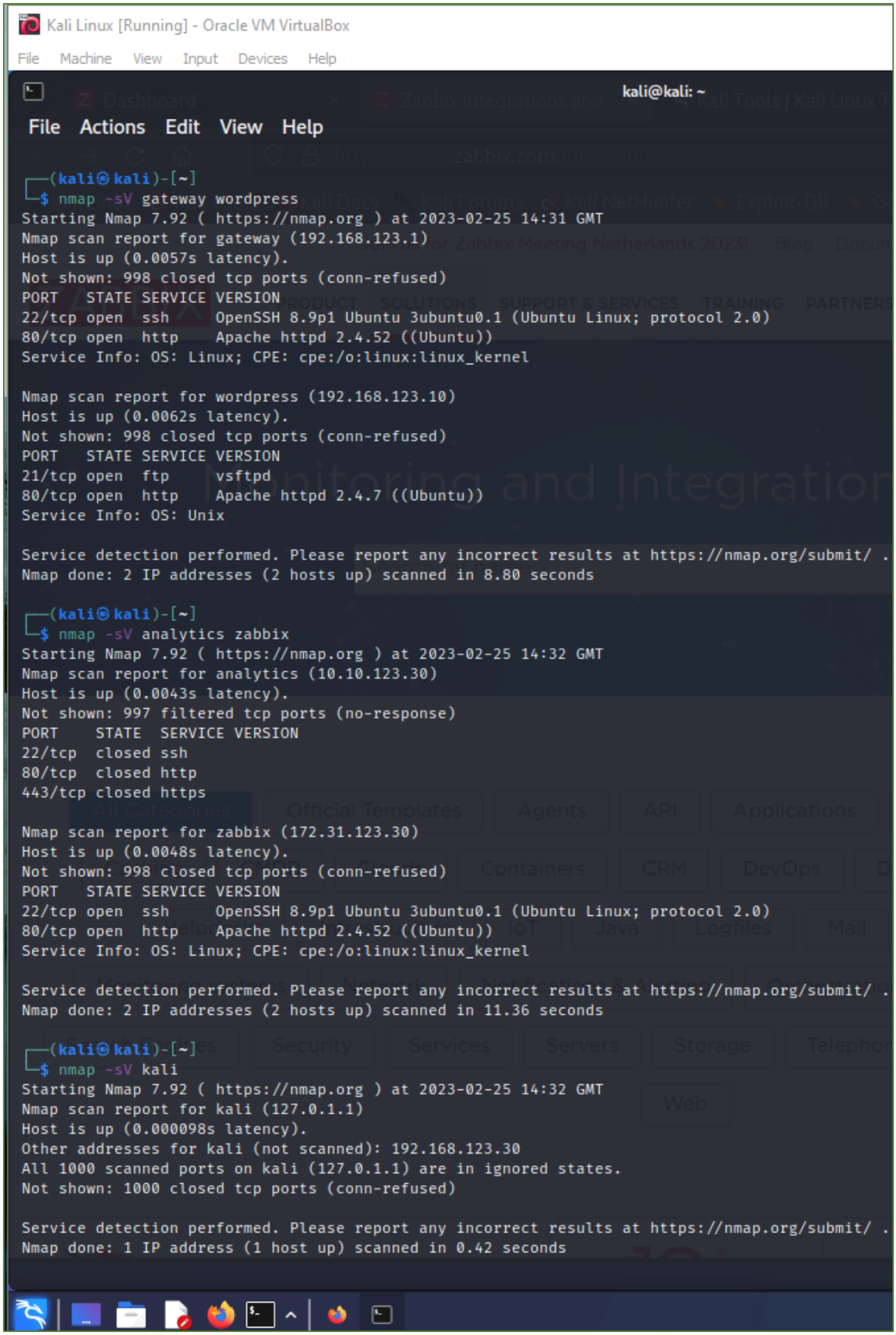
```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sT 192.168.123.1
Starting Nmap 7.92 ( https://nmap.org ) at 2023-02-25 13:57 GMT
Nmap scan report for gateway (192.168.123.1)
Host is up (0.0039s latency).
Not shown: 998 closed tcp ports (conn-refused)
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http
MAC Address: 08:00:27:66:0A:6D (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.92 seconds

┌──(root㉿kali)-[/home/kali]
└─# nmap -p T:80 gateway
Starting Nmap 7.92 ( https://nmap.org ) at 2023-02-25 13:57 GMT
Nmap scan report for gateway (192.168.123.1)
Host is up (0.0020s latency).

PORT   STATE SERVICE
80/tcp open  http
MAC Address: 08:00:27:6A:7C:8B (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.22 seconds

┌──(root㉿kali)-[/home/kali]
└─# nmap -sU gateway
Starting Nmap 7.92 ( https://nmap.org ) at 2023-02-25 13:57 GMT
Stats: 0:00:10 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan
UDP Scan Timing: About 2.04% done; ETC: 14:05 (0:07:59 remaining)
Stats: 0:10:03 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan
UDP Scan Timing: About 57.64% done; ETC: 14:15 (0:07:23 remaining)
Nmap scan report for gateway (192.168.123.1)
Host is up (0.0011s latency).
All 1000 scanned ports on gateway (192.168.123.1) are in ignored states.
Not shown: 1000 closed udp ports (port-unreach)
MAC Address: 08:00:27:C2:1A:1A (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 1087.05 seconds

┌──(root㉿kali)-[/home/kali]
└─# nmap -p U:53 gateway
Starting Nmap 7.92 ( https://nmap.org ) at 2023-02-25 14:18 GMT
WARNING: Your ports include "U:" but you haven't specified UDP scan with -sU.
WARNING: a TCP scan type was requested, but no tcp ports were specified.  Skipping this scan type.
Nmap scan report for gateway (192.168.123.1)
Host is up (0.0010s latency).
MAC Address: 08:00:27:6A:7C:8B (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.14 seconds

┌──(root㉿kali)-[/home/kali]
└─# nmap -p U:53,79,113,T:21-80,443,8080 zabbix
Starting Nmap 7.92 ( https://nmap.org ) at 2023-02-25 14:18 GMT
WARNING: Your ports include "U:" but you haven't specified UDP scan with -sU.
Nmap scan report for zabbix (172.31.123.30)
Host is up (0.0069s latency).
Not shown: 60 closed tcp ports (reset)
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http

Nmap done: 1 IP address (1 host up) scanned in 0.24 seconds

┌──(root㉿kali)-[/home/kali]
└─# nmap -p U:53,79,113,T:21-80,443,8080 gateway
Starting Nmap 7.92 ( https://nmap.org ) at 2023-02-25 14:18 GMT
WARNING: Your ports include "U:" but you haven't specified UDP scan with -sU.
Nmap scan report for gateway (192.168.123.1)
Host is up (0.0010s latency).
Not shown: 60 closed tcp ports (reset)
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http
MAC Address: 08:00:27:6A:7C:8B (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.22 seconds
```

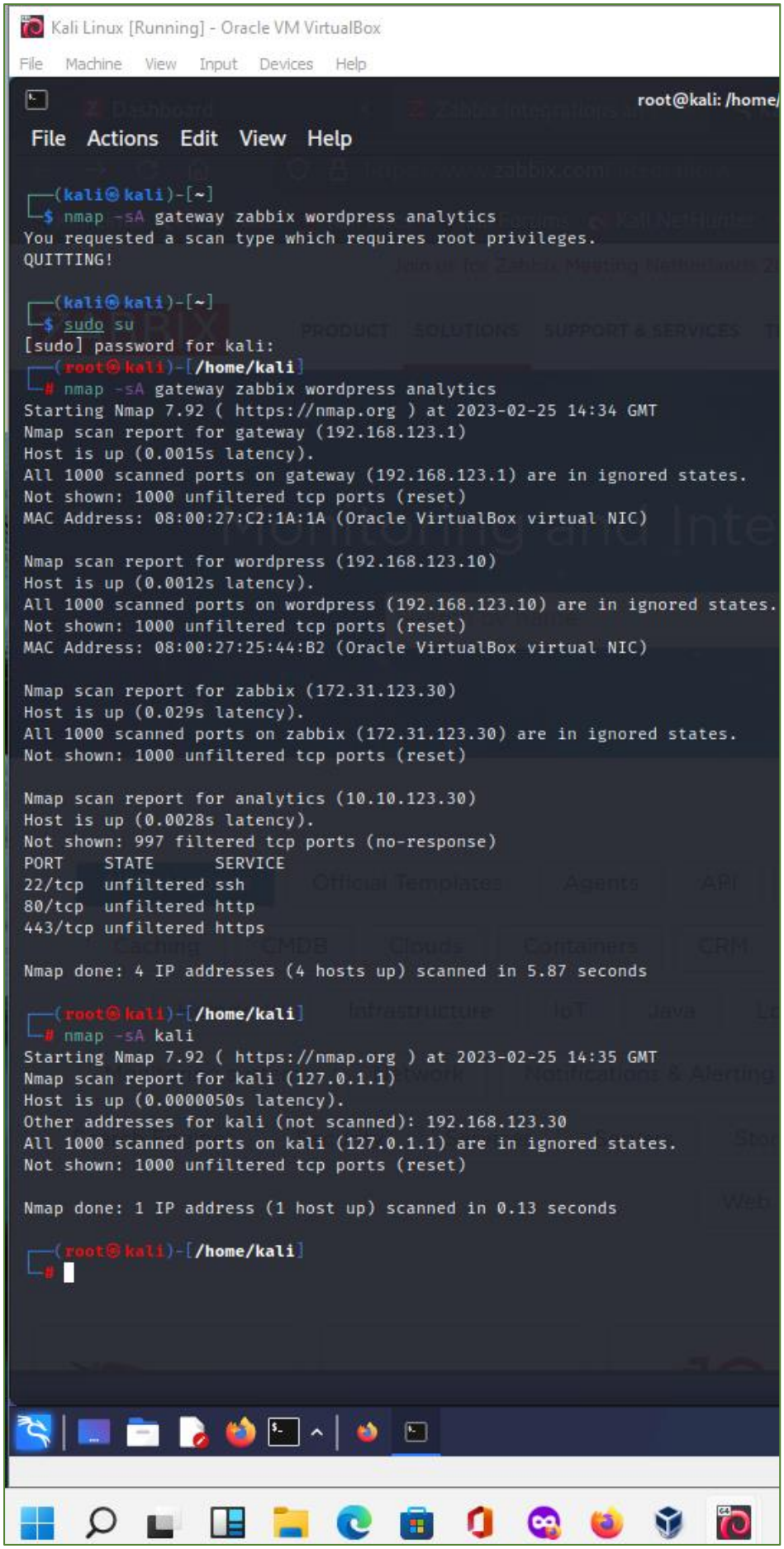

Kali Linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
kali@kali: ~
File Actions Edit View Help
(kali㉿kali)-[~]
$ nmap -F gateway
Starting Nmap 7.92 (https://nmap.org) at 2023-02-25 14:21 GMT
Nmap scan report for gateway (192.168.123.1)
Host is up (0.0043s latency).
Not shown: 98 closed tcp ports (conn-refused)
PORT STATE SERVICE
22/tcp open ssh
80/tcp open http
Nmap done: 1 IP address (1 host up) scanned in 0.12 seconds
(kali㉿kali)-[~]
$ nmap -F zabbix
Starting Nmap 7.92 (https://nmap.org) at 2023-02-25 14:21 GMT
Nmap scan report for zabbix (172.31.123.30)
Host is up (0.0042s latency).
Not shown: 98 closed tcp ports (conn-refused)
PORT STATE SERVICE
22/tcp open ssh
80/tcp open http
Nmap done: 1 IP address (1 host up) scanned in 0.13 seconds
(kali㉿kali)-[~]
$ nmap -F wordpress
Starting Nmap 7.92 (https://nmap.org) at 2023-02-25 14:21 GMT
Nmap scan report for wordpress (192.168.123.10)
Host is up (0.0036s latency).
Not shown: 98 closed tcp ports (conn-refused)
PORT STATE SERVICE
21/tcp open ftp
80/tcp open http
Nmap done: 1 IP address (1 host up) scanned in 0.11 seconds
(kali㉿kali)-[~]
$ nmap -F analytics
Starting Nmap 7.92 (https://nmap.org) at 2023-02-25 14:21 GMT
Nmap scan report for analytics (10.10.123.30)
Host is up (0.0029s latency).
Not shown: 97 filtered tcp ports (no-response)
PORT STATE SERVICE
22/tcp closed ssh
80/tcp closed http
443/tcp closed https
Nmap done: 1 IP address (1 host up) scanned in 1.83 seconds
(kali㉿kali)-[~]
$


Kali Linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
File Actions Edit View Help
(kali㉿kali)-[~]
$ nmap --reason analytics
Starting Nmap 7.92 (https://nmap.org) at 2023-02-25 14:23 GMT
Nmap scan report for analytics (10.10.123.30)
Host is up, received conn-refused (0.0026s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT STATE SERVICE REASON
22/tcp closed ssh conn-refused
80/tcp closed http conn-refused
443/tcp closed https conn-refused
Nmap done: 1 IP address (1 host up) scanned in 5.07 seconds
(kali㉿kali)-[~]
$ nmap --reason gateway
Starting Nmap 7.92 (https://nmap.org) at 2023-02-25 14:23 GMT
Nmap scan report for gateway (192.168.123.1)
Host is up, received syn-ack (0.0012s latency).
Not shown: 998 closed tcp ports (conn-refused)
PORT STATE SERVICE REASON
22/tcp open ssh syn-ack
80/tcp open http syn-ack
Nmap done: 1 IP address (1 host up) scanned in 0.18 seconds
(kali㉿kali)-[~]
$ nmap --reason wordpress
Starting Nmap 7.92 (https://nmap.org) at 2023-02-25 14:23 GMT
Nmap scan report for wordpress (192.168.123.10)
Host is up, received syn-ack (0.019s latency).
Not shown: 998 closed tcp ports (conn-refused)
PORT STATE SERVICE REASON
21/tcp open ftp syn-ack
80/tcp open http syn-ack
Nmap done: 1 IP address (1 host up) scanned in 0.74 seconds
(kali㉿kali)-[~]
$ nmap --reason zabbix
Starting Nmap 7.92 (https://nmap.org) at 2023-02-25 14:23 GMT
Nmap scan report for zabbix (172.31.123.30)
Host is up, received syn-ack (0.0072s latency).
Not shown: 998 closed tcp ports (conn-refused)
PORT STATE SERVICE REASON
22/tcp open ssh syn-ack
80/tcp open http syn-ack
Nmap done: 1 IP address (1 host up) scanned in 0.22 seconds
(kali㉿kali)-[~]
$

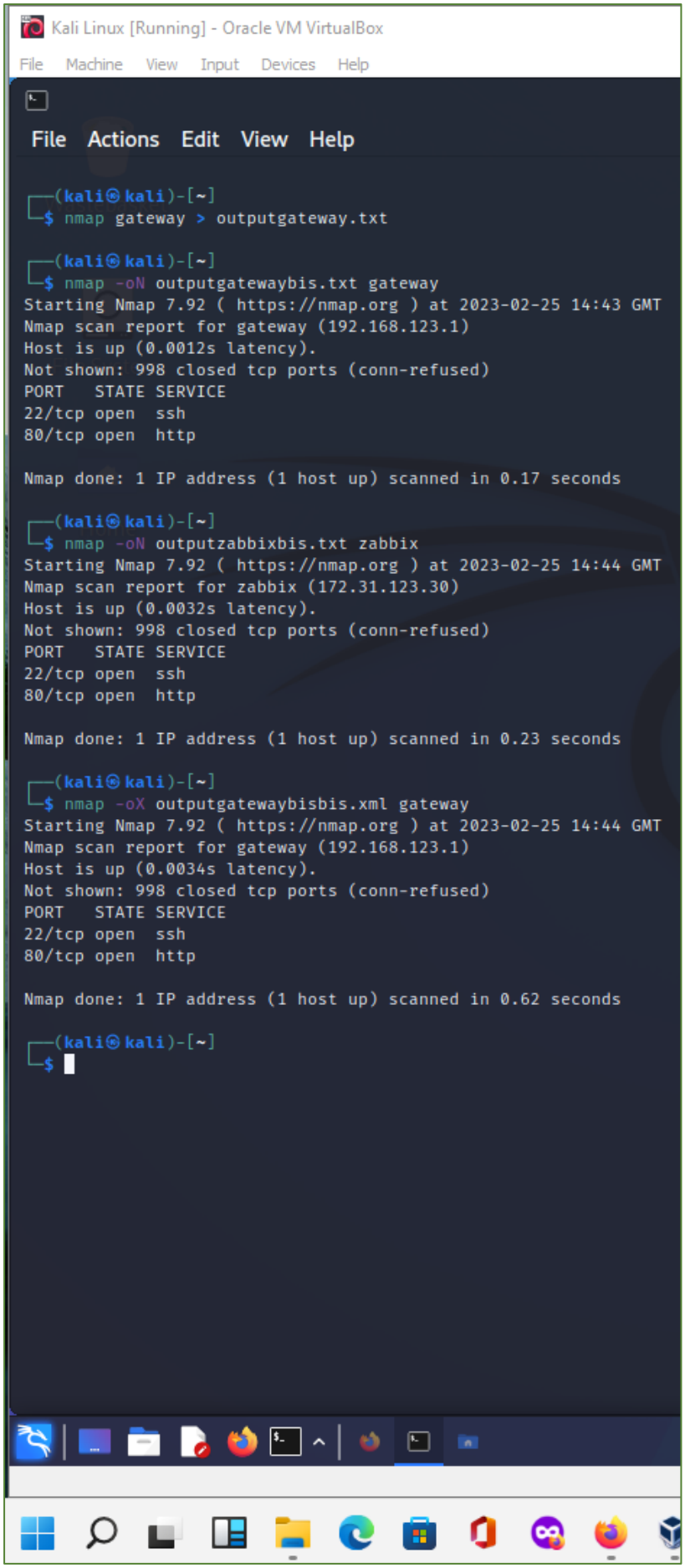

Kali Linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
File Actions Edit View Help
┌──(kali㉿kali)-[~]
└─$ nmap --open 192.168.123.1
Starting Nmap 7.92 (https://nmap.org) at 2023-02-25 14:24 GMT
Nmap scan report for gateway (192.168.123.1)
Host is up (0.0017s latency).
Not shown: 998 closed tcp ports (conn-refused)
PORT STATE SERVICE
22/tcp open ssh
80/tcp open http
Nmap done: 1 IP address (1 host up) scanned in 0.21 seconds
┌──(kali㉿kali)-[~]
└─$ nmap --open gateway
Starting Nmap 7.92 (https://nmap.org) at 2023-02-25 14:24 GMT
Nmap scan report for gateway (192.168.123.1)
Host is up (0.0036s latency).
Not shown: 998 closed tcp ports (conn-refused)
PORT STATE SERVICE
22/tcp open ssh
80/tcp open http
Nmap done: 1 IP address (1 host up) scanned in 0.64 seconds
┌──(kali㉿kali)-[~]
└─$ nmap --open zabbix
Starting Nmap 7.92 (https://nmap.org) at 2023-02-25 14:24 GMT
Nmap scan report for zabbix (172.31.123.30)
Host is up (0.015s latency).
Not shown: 998 closed tcp ports (conn-refused)
PORT STATE SERVICE
22/tcp open ssh
80/tcp open http
Nmap done: 1 IP address (1 host up) scanned in 0.42 seconds
┌──(kali㉿kali)-[~]
└─$ nmap --open analytics
Starting Nmap 7.92 (https://nmap.org) at 2023-02-25 14:25 GMT
Nmap done: 1 IP address (1 host up) scanned in 4.92 seconds
┌──(kali㉿kali)-[~]
└─$ nmap --open wordpress
Starting Nmap 7.92 (https://nmap.org) at 2023-02-25 14:25 GMT
Nmap scan report for wordpress (192.168.123.10)
Host is up (0.0044s latency).
Not shown: 998 closed tcp ports (conn-refused)
PORT STATE SERVICE
21/tcp open ftp
80/tcp open http
Nmap done: 1 IP address (1 host up) scanned in 0.62 seconds

```
┌──(kali㉿kali)-[~]
└─$ nmap -O gateway
TCP/IP fingerprinting (for OS scan) requires root privileges.
QUITTING!

┌──(kali㉿kali)-[~]
└─$ sudo su
[sudo] password for kali:
┌──(root㉿kali)-[/home/kali]
└─# nmap -O gateway
Starting Nmap 7.92 ( https://nmap.org ) at 2023-02-25 14:26 GMT
Nmap scan report for gateway (192.168.123.1)
Host is up (0.0012s latency).
Not shown: 998 closed tcp ports (reset)
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http
MAC Address: 08:00:27:66:0A:6D (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 4.X|5.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5
OS details: Linux 4.15 - 5.6
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 4.94 seconds

┌──(root㉿kali)-[/home/kali]
└─# nmap -O wordpress
Starting Nmap 7.92 ( https://nmap.org ) at 2023-02-25 14:27 GMT
Nmap scan report for wordpress (192.168.123.10)
Host is up (0.00082s latency).
Not shown: 998 closed tcp ports (reset)
PORT   STATE SERVICE
21/tcp open  ftp
80/tcp open  http
MAC Address: 08:00:27:25:44:B2 (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.9
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 1.87 seconds

┌──(root㉿kali)-[/home/kali]
└─# nmap -O kali
Starting Nmap 7.92 ( https://nmap.org ) at 2023-02-25 14:27 GMT
Nmap scan report for kali (127.0.1.1)
Host is up (0.000097s latency).
Other addresses for kali (not scanned): 192.168.123.30
All 1000 scanned ports on kali (127.0.1.1) are in ignored states.
Not shown: 1000 closed tcp ports (reset)
Too many fingerprints match this host to give specific OS details
Network Distance: 0 hops

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 1.96 seconds

┌──(root㉿kali)-[/home/kali]
└─# nmap -O zabbix
Starting Nmap 7.92 ( https://nmap.org ) at 2023-02-25 14:27 GMT
Nmap scan report for zabbix (172.31.123.30)
Host is up (0.0023s latency).
Not shown: 998 closed tcp ports (reset)
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http
Device type: general purpose
Running: Linux 4.X|5.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5
OS details: Linux 4.15 - 5.6
Network Distance: 2 hops

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 2.10 seconds
```


Kali Linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
kali@kali: ~
File Actions Edit View Help
┌──(kali㉿kali)-[~]
└─$ nmap -sV gateway wordpress
Starting Nmap 7.92 (https://nmap.org) at 2023-02-25 14:31 GMT
Nmap scan report for gateway (192.168.123.1)
Host is up (0.0057s latency).
Not shown: 998 closed tcp ports (conn-refused)
PORT STATE SERVICE VERSION
22/tcp open ssh OpenSSH 8.9p1 Ubuntu 3ubuntu0.1 (Ubuntu Linux; protocol 2.0)
80/tcp open http Apache httpd 2.4.52 ((Ubuntu))
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
Nmap scan report for wordpress (192.168.123.10)
Host is up (0.0062s latency).
Not shown: 998 closed tcp ports (conn-refused)
PORT STATE SERVICE VERSION
21/tcp open ftp vsftpd
80/tcp open http Apache httpd 2.4.7 ((Ubuntu))
Service Info: OS: Unix
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 2 IP addresses (2 hosts up) scanned in 8.80 seconds
┌──(kali㉿kali)-[~]
└─$ nmap -sV analytics zabbix
Starting Nmap 7.92 (https://nmap.org) at 2023-02-25 14:32 GMT
Nmap scan report for analytics (10.10.123.30)
Host is up (0.0043s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT STATE SERVICE VERSION
22/tcp closed ssh
80/tcp closed http
443/tcp closed https
Nmap scan report for zabbix (172.31.123.30)
Host is up (0.0048s latency).
Not shown: 998 closed tcp ports (conn-refused)
PORT STATE SERVICE VERSION
22/tcp open ssh OpenSSH 8.9p1 Ubuntu 3ubuntu0.1 (Ubuntu Linux; protocol 2.0)
80/tcp open http Apache httpd 2.4.52 ((Ubuntu))
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 2 IP addresses (2 hosts up) scanned in 11.36 seconds
┌──(kali㉿kali)-[~]
└─$ nmap -sV kali
Starting Nmap 7.92 (https://nmap.org) at 2023-02-25 14:32 GMT
Nmap scan report for kali (127.0.1.1)
Host is up (0.000098s latency).
Other addresses for kali (not scanned): 192.168.123.30
All 1000 scanned ports on kali (127.0.1.1) are in ignored states.
Not shown: 1000 closed tcp ports (conn-refused)
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 0.42 seconds


Kali Linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
root@kali: /home/
File Actions Edit View Help
┌──(kali㉿kali)-[~]
└─$ nmap -sA gateway zabbix wordpress analytics
You requested a scan type which requires root privileges.
QUITTING!
┌──(kali㉿kali)-[~]
└─$ sudo su
[sudo] password for kali:
┌──(root㉿kali)-[/home/kali]
└─# nmap -sA gateway zabbix wordpress analytics
Starting Nmap 7.92 (https://nmap.org) at 2023-02-25 14:34 GMT
Nmap scan report for gateway (192.168.123.1)
Host is up (0.0015s latency).
All 1000 scanned ports on gateway (192.168.123.1) are in ignored states.
Not shown: 1000 unfiltered tcp ports (reset)
MAC Address: 08:00:27:C2:1A:1A (Oracle VirtualBox virtual NIC)
Nmap scan report for wordpress (192.168.123.10)
Host is up (0.0012s latency).
All 1000 scanned ports on wordpress (192.168.123.10) are in ignored states.
Not shown: 1000 unfiltered tcp ports (reset)
MAC Address: 08:00:27:25:44:B2 (Oracle VirtualBox virtual NIC)
Nmap scan report for zabbix (172.31.123.30)
Host is up (0.029s latency).
All 1000 scanned ports on zabbix (172.31.123.30) are in ignored states.
Not shown: 1000 unfiltered tcp ports (reset)
Nmap scan report for analytics (10.10.123.30)
Host is up (0.0028s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT STATE SERVICE
22/tcp unfiltered ssh
80/tcp unfiltered http
443/tcp unfiltered https
Nmap done: 4 IP addresses (4 hosts up) scanned in 5.87 seconds
┌──(root㉿kali)-[/home/kali]
└─# nmap -sA kali
Starting Nmap 7.92 (https://nmap.org) at 2023-02-25 14:35 GMT
Nmap scan report for kali (127.0.1.1)
Host is up (0.0000050s latency).
Other addresses for kali (not scanned): 192.168.123.30
All 1000 scanned ports on kali (127.0.1.1) are in ignored states.
Not shown: 1000 unfiltered tcp ports (reset)
Nmap done: 1 IP address (1 host up) scanned in 0.13 seconds
┌──(root㉿kali)-[/home/kali]
└─#


root@kali: /home/kali
File Actions Edit View Help
┌──(root㉿kali)-[/home/kali]
└─# nmap -sS gateway
Starting Nmap 7.92 (https://nmap.org) at 2023-02-25 14:36 GMT
Nmap scan report for gateway (192.168.123.1)
Host is up (0.0011s latency).
Not shown: 998 closed tcp ports (reset)
PORT STATE SERVICE
22/tcp open ssh
80/tcp open http
MAC Address: 08:00:27:66:0A:6D (Oracle VirtualBox virtual NIC)
Nmap done: 1 IP address (1 host up) scanned in 0.53 seconds
┌──(root㉿kali)-[/home/kali]
└─# nmap -sS analytics zabbix wordpress
Starting Nmap 7.92 (https://nmap.org) at 2023-02-25 14:36 GMT
Nmap scan report for analytics (10.10.123.30)
Host is up (0.0030s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT STATE SERVICE
22/tcp closed ssh
80/tcp closed http
443/tcp closed https
Nmap scan report for zabbix (172.31.123.30)
Host is up (0.0034s latency).
Not shown: 998 closed tcp ports (reset)
PORT STATE SERVICE
22/tcp open ssh
80/tcp open http
Nmap scan report for wordpress (192.168.123.10)
Host is up (0.027s latency).
Not shown: 998 closed tcp ports (reset)
PORT STATE SERVICE
21/tcp open ftp
80/tcp open http
MAC Address: 08:00:27:25:44:B2 (Oracle VirtualBox virtual NIC)
Nmap done: 3 IP addresses (3 hosts up) scanned in 6.27 seconds
┌──(root㉿kali)-[/home/kali]
└─# tor-resolve google.com
Command 'tor-resolve' not found, but can be installed with:
apt install tor
Do you want to install it? (N/y)y
apt install tor
Reading package lists ... Done
Building dependency tree ... Done
Reading state information ... Done
Some packages could not be installed. This may mean that you have
requested an impossible situation or if you are using the unstable
distribution that some required packages have not yet been created
or been moved out of Incoming.
The following information may help to resolve the situation:
The following packages have unmet dependencies:
libc6-dev : Breaks: binutils (< 2.38) but 2.37-10.1 is to be installed
E: Error, pkgProblemResolver::Resolve generated breaks, this may be caused by held packages.
┌──(root㉿kali)-[/home/kali]
└─# tor-resolve google.com
Command 'tor-resolve' not found, but can be installed with:
apt install tor
Do you want to install it? (N/y)y
apt install tor
Reading package lists ... Done
Building dependency tree ... Done
Reading state information ... Done
Some packages could not be installed. This may mean that you have


Kali Linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
File Actions Edit View Help
┌──(kali㉿kali)-[~]
└─$ nmap gateway > outputgateway.txt
┌──(kali㉿kali)-[~]
└─$ nmap -oN outputgatewaybis.txt gateway
Starting Nmap 7.92 (https://nmap.org) at 2023-02-25 14:43 GMT
Nmap scan report for gateway (192.168.123.1)
Host is up (0.0012s latency).
Not shown: 998 closed tcp ports (conn-refused)
PORT STATE SERVICE
22/tcp open ssh
80/tcp open http
Nmap done: 1 IP address (1 host up) scanned in 0.17 seconds
┌──(kali㉿kali)-[~]
└─$ nmap -oN outputzabbixbis.txt zabbix
Starting Nmap 7.92 (https://nmap.org) at 2023-02-25 14:44 GMT
Nmap scan report for zabbix (172.31.123.30)
Host is up (0.0032s latency).
Not shown: 998 closed tcp ports (conn-refused)
PORT STATE SERVICE
22/tcp open ssh
80/tcp open http
Nmap done: 1 IP address (1 host up) scanned in 0.23 seconds
┌──(kali㉿kali)-[~]
└─$ nmap -oX outputgatewaybisbis.xml gateway
Starting Nmap 7.92 (https://nmap.org) at 2023-02-25 14:44 GMT
Nmap scan report for gateway (192.168.123.1)
Host is up (0.0034s latency).
Not shown: 998 closed tcp ports (conn-refused)
PORT STATE SERVICE
22/tcp open ssh
80/tcp open http
Nmap done: 1 IP address (1 host up) scanned in 0.62 seconds
┌──(kali㉿kali)-[~]
└─$

Wow factor Req. B (build in scripts from *nmap*):

[1] [2] [3] [4] [5]

Bibliography

[1] [Online]. Available: https://www.tecmint.com/use-nmap-script-engine-nse-scripts-in-linux/ .

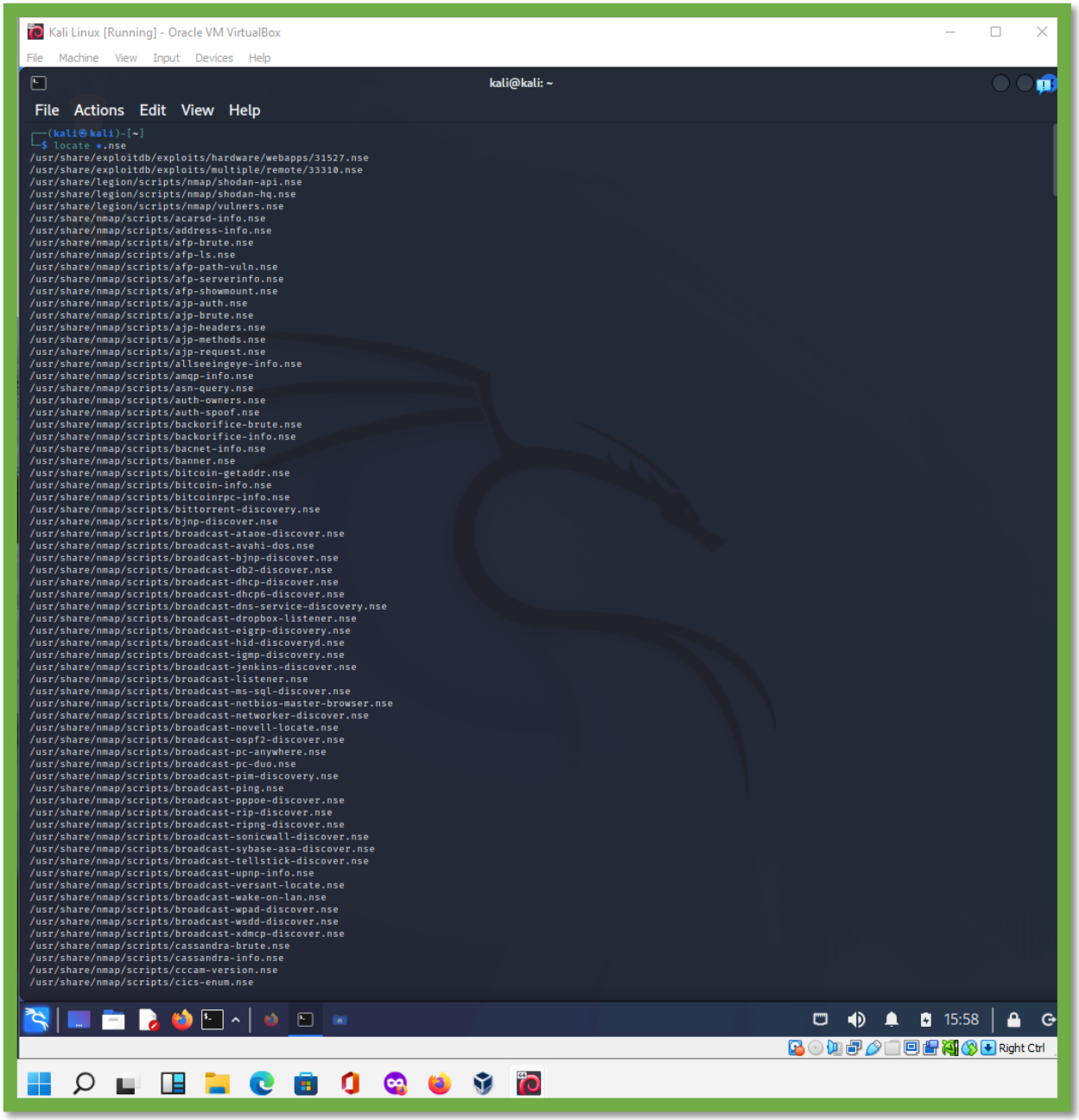
[2] [Online]. Available: https://securitytrails.com/blog/nmap-scripts-nse .

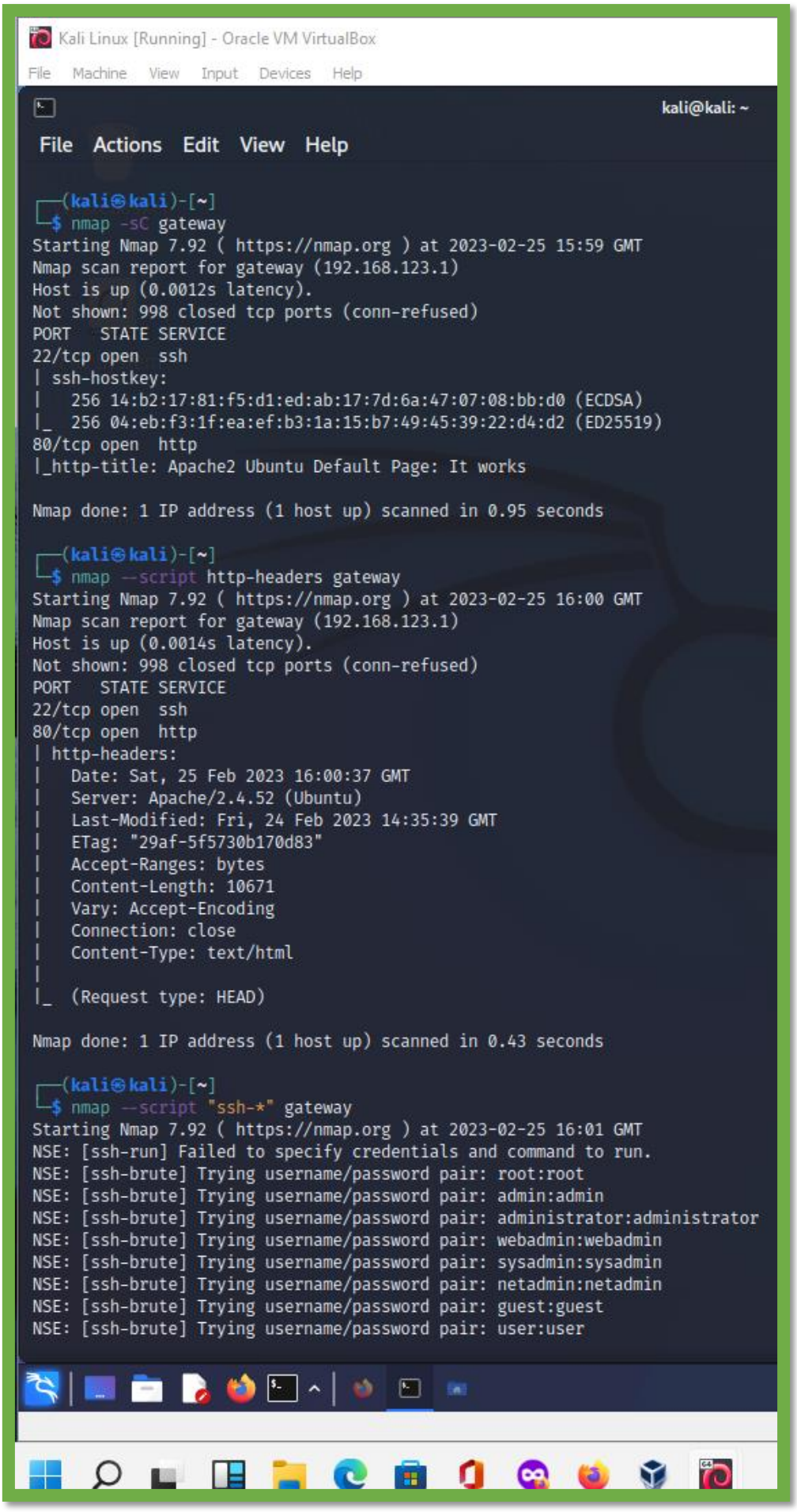
[3] [Online]. Available: https://www.cybervie.com/blog/nmap-and-useful-nse-scripts/ .

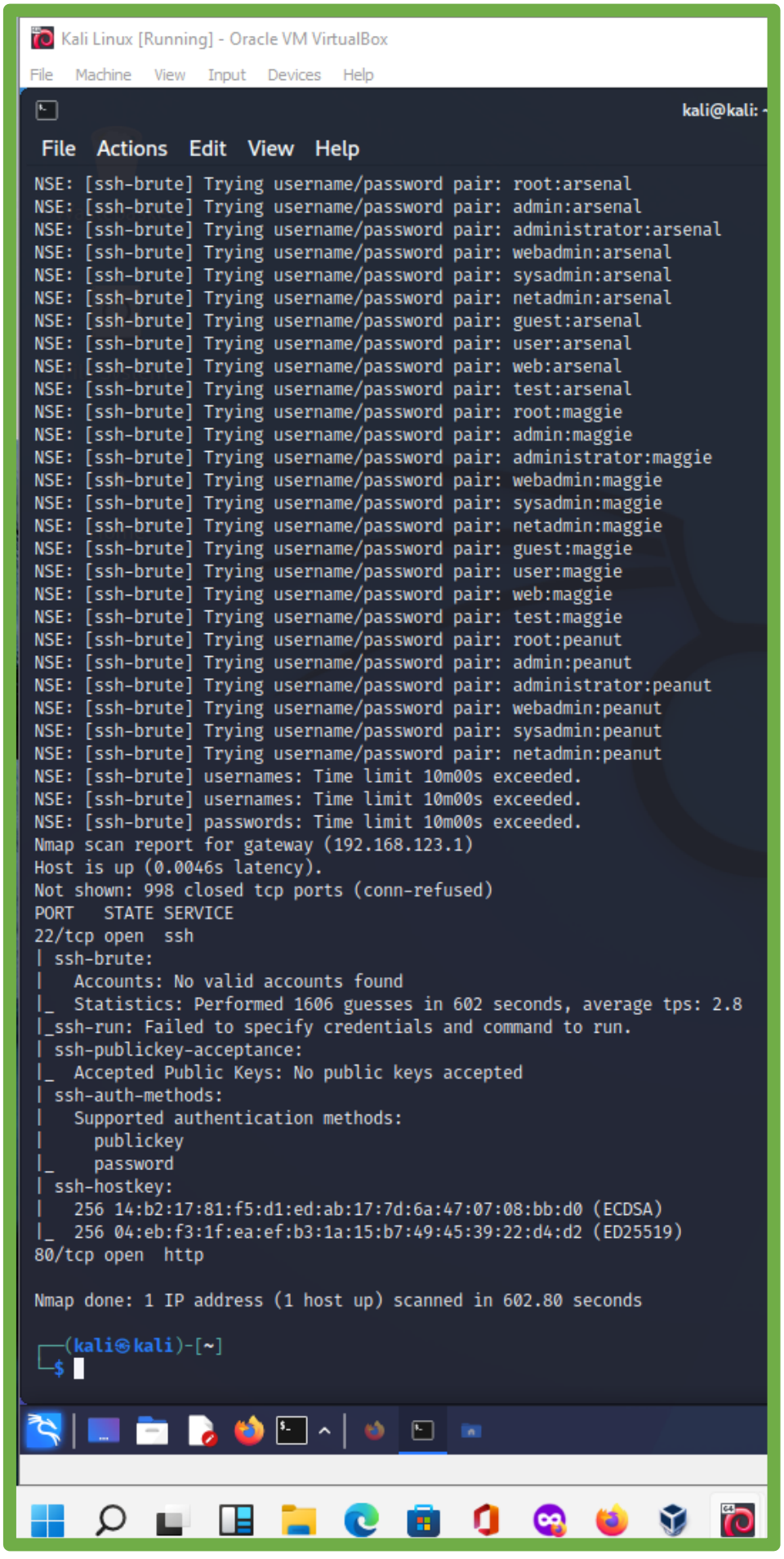
[4] [Online]. Available: https://nmap.org/book/nse-usage.html .

[5] [Online]. Available: https://www.shellhacks.com/find-active-computers-local-network-linux/.

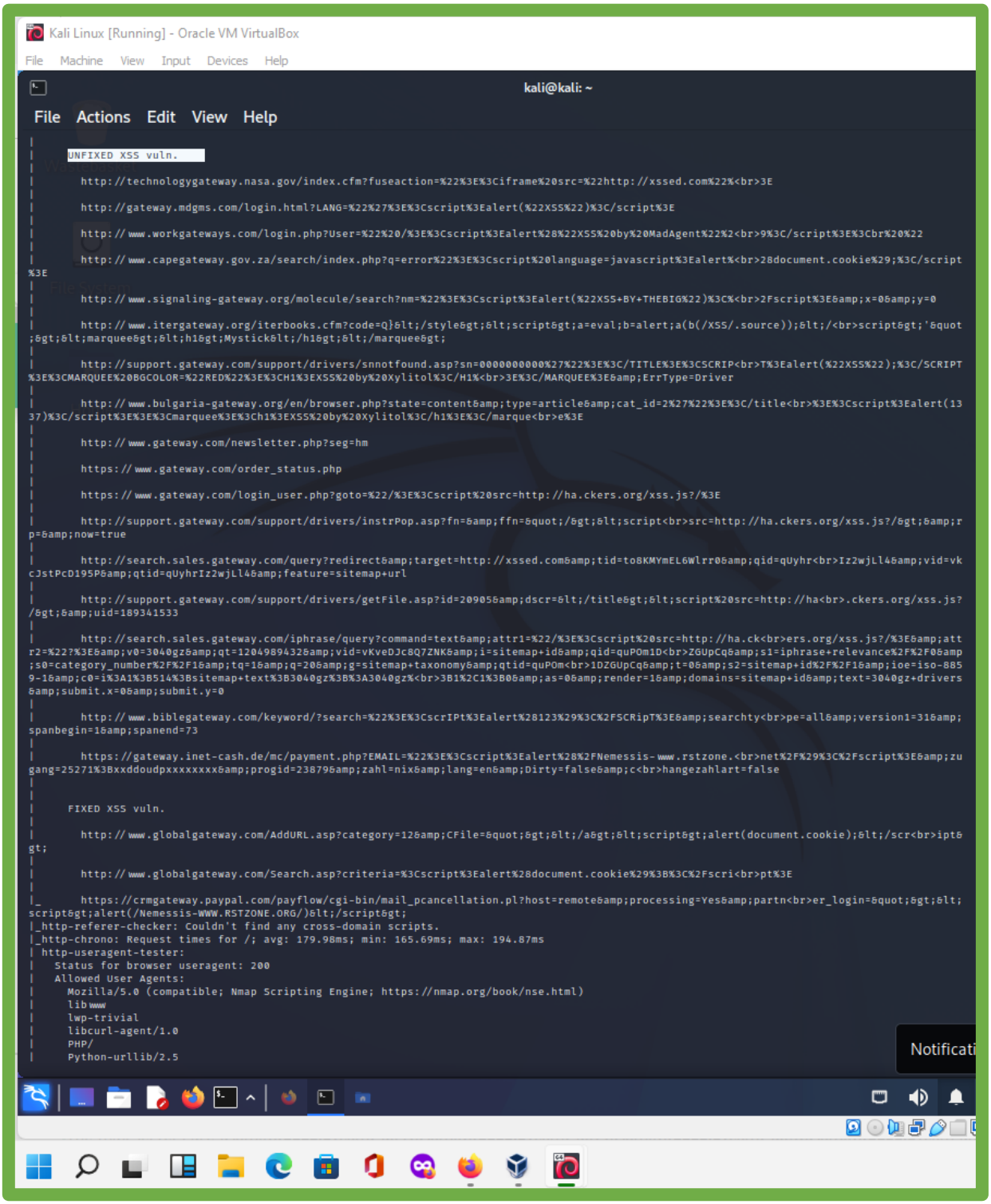
[6] [Online]. Available: https://www.shellhacks.com/find-active-computers-local-network-linux/.


Kali Linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
kali@kali: ~
File Actions Edit View Help
┌──(kali㉿kali)-[~]
└─$ locate *.nse
/usr/share/exploitdb/exploits/hardware/webapps/31527.nse
/usr/share/exploitdb/exploits/multiple/remote/33310.nse
/usr/share/legion/scripts/nmap/shodan-api.nse
/usr/share/legion/scripts/nmap/shodan-hq.nse
/usr/share/legion/scripts/nmap/vulners.nse
/usr/share/nmap/scripts/acarsd-info.nse
/usr/share/nmap/scripts/address-info.nse
/usr/share/nmap/scripts/afp-brute.nse
/usr/share/nmap/scripts/afp-ls.nse
/usr/share/nmap/scripts/afp-path-vuln.nse
/usr/share/nmap/scripts/afp-serverinfo.nse
/usr/share/nmap/scripts/afp-showmount.nse
/usr/share/nmap/scripts/ajp-auth.nse
/usr/share/nmap/scripts/ajp-brute.nse
/usr/share/nmap/scripts/ajp-headers.nse
/usr/share/nmap/scripts/ajp-methods.nse
/usr/share/nmap/scripts/ajp-request.nse
/usr/share/nmap/scripts/allseeingeye-info.nse
/usr/share/nmap/scripts/amqp-info.nse
/usr/share/nmap/scripts/asn-query.nse
/usr/share/nmap/scripts/auth-owners.nse
/usr/share/nmap/scripts/auth-spoof.nse
/usr/share/nmap/scripts/backorifice-brute.nse
/usr/share/nmap/scripts/backorifice-info.nse
/usr/share/nmap/scripts/bacnet-info.nse
/usr/share/nmap/scripts/banner.nse
/usr/share/nmap/scripts/bitcoin-getaddr.nse
/usr/share/nmap/scripts/bitcoin-info.nse
/usr/share/nmap/scripts/bitcoinrpc-info.nse
/usr/share/nmap/scripts/bittorrent-discovery.nse
/usr/share/nmap/scripts/bjnp-discover.nse
/usr/share/nmap/scripts/broadcast-ataoe-discover.nse
/usr/share/nmap/scripts/broadcast-avahi-dos.nse
/usr/share/nmap/scripts/broadcast-bjnp-discover.nse
/usr/share/nmap/scripts/broadcast-db2-discover.nse
/usr/share/nmap/scripts/broadcast-dhcp-discover.nse
/usr/share/nmap/scripts/broadcast-dhcp6-discover.nse
/usr/share/nmap/scripts/broadcast-dns-service-discovery.nse
/usr/share/nmap/scripts/broadcast-dropbox-listener.nse
/usr/share/nmap/scripts/broadcast-eigrp-discovery.nse
/usr/share/nmap/scripts/broadcast-hid-discoveryd.nse
/usr/share/nmap/scripts/broadcast-igmp-discovery.nse
/usr/share/nmap/scripts/broadcast-jenkins-discover.nse
/usr/share/nmap/scripts/broadcast-listener.nse
/usr/share/nmap/scripts/broadcast-ms-sql-discover.nse
/usr/share/nmap/scripts/broadcast-netbios-master-browser.nse
/usr/share/nmap/scripts/broadcast-networker-discover.nse
/usr/share/nmap/scripts/broadcast-novell-locate.nse
/usr/share/nmap/scripts/broadcast-ospf2-discover.nse
/usr/share/nmap/scripts/broadcast-pc-anywhere.nse
/usr/share/nmap/scripts/broadcast-pc-duo.nse
/usr/share/nmap/scripts/broadcast-pim-discovery.nse
/usr/share/nmap/scripts/broadcast-ping.nse
/usr/share/nmap/scripts/broadcast-pppoe-discover.nse
/usr/share/nmap/scripts/broadcast-rip-discover.nse
/usr/share/nmap/scripts/broadcast-ripng-discover.nse
/usr/share/nmap/scripts/broadcast-sonicwall-discover.nse
/usr/share/nmap/scripts/broadcast-sybase-asa-discover.nse
/usr/share/nmap/scripts/broadcast-tellstick-discover.nse
/usr/share/nmap/scripts/broadcast-upnp-info.nse
/usr/share/nmap/scripts/broadcast-versant-locate.nse
/usr/share/nmap/scripts/broadcast-wake-on-lan.nse
/usr/share/nmap/scripts/broadcast-wpad-discover.nse
/usr/share/nmap/scripts/broadcast-wsdd-discover.nse
/usr/share/nmap/scripts/broadcast-xdmcp-discover.nse
/usr/share/nmap/scripts/cassandra-brute.nse
/usr/share/nmap/scripts/cassandra-info.nse
/usr/share/nmap/scripts/cccam-version.nse
/usr/share/nmap/scripts/cics-enum.nse
15:58
Right Ctrl

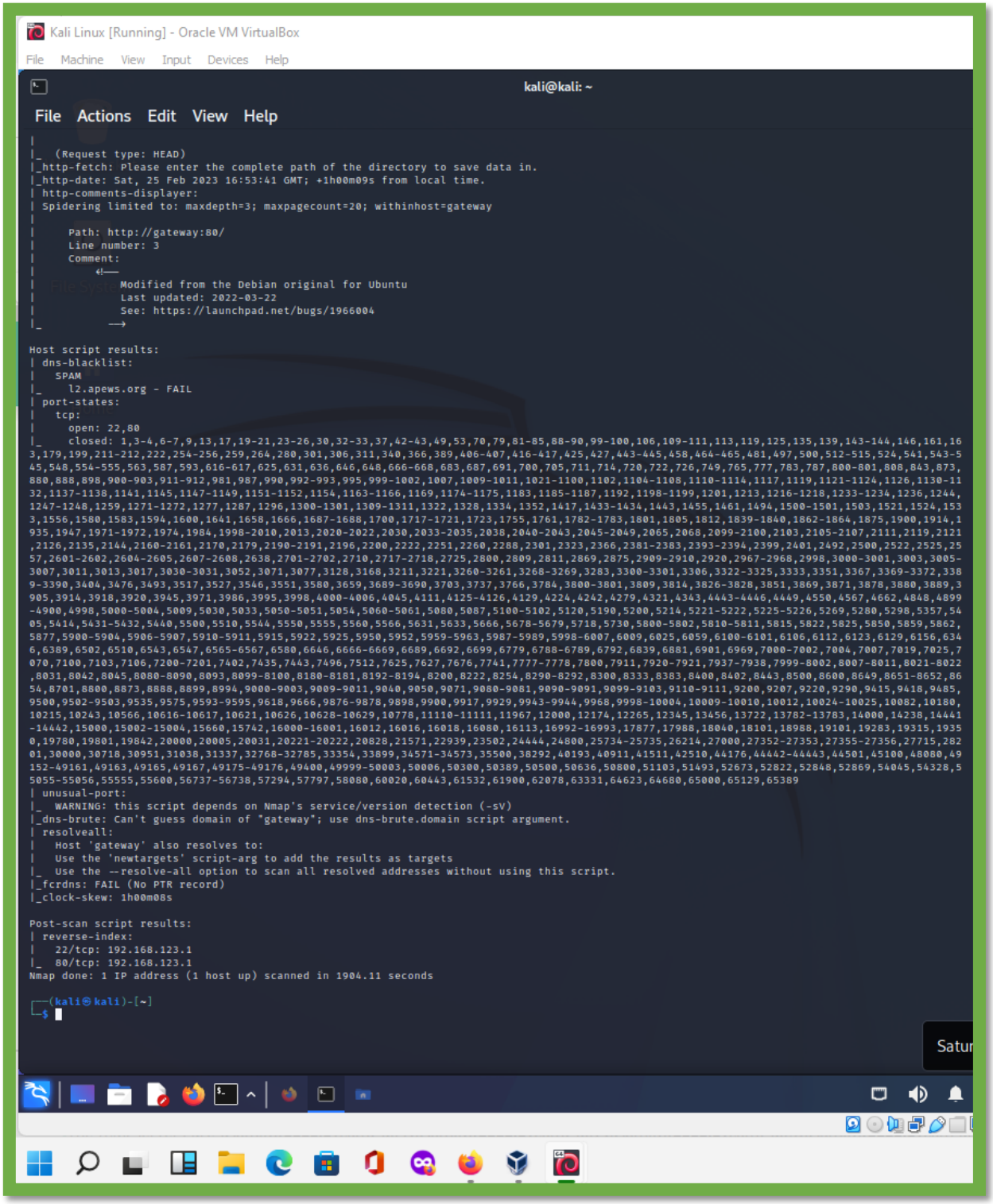

Kali Linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
kali@kali: ~
File Actions Edit View Help
┌──(kali㉿kali)-[~]
└─$ nmap -sC gateway
Starting Nmap 7.92 (https://nmap.org) at 2023-02-25 15:59 GMT
Nmap scan report for gateway (192.168.123.1)
Host is up (0.0012s latency).
Not shown: 998 closed tcp ports (conn-refused)
PORT STATE SERVICE
22/tcp open ssh
| ssh-hostkey:
| 256 14:b2:17:81:f5:d1:ed:ab:17:7d:6a:47:07:08:bb:d0 (ECDSA)
|_ 256 04:eb:f3:1f:ea:ef:b3:1a:15:b7:49:45:39:22:d4:d2 (ED25519)
80/tcp open http
|_http-title: Apache2 Ubuntu Default Page: It works
Nmap done: 1 IP address (1 host up) scanned in 0.95 seconds
┌──(kali㉿kali)-[~]
└─$ nmap --script http-headers gateway
Starting Nmap 7.92 (https://nmap.org) at 2023-02-25 16:00 GMT
Nmap scan report for gateway (192.168.123.1)
Host is up (0.0014s latency).
Not shown: 998 closed tcp ports (conn-refused)
PORT STATE SERVICE
22/tcp open ssh
80/tcp open http
| http-headers:
| Date: Sat, 25 Feb 2023 16:00:37 GMT
| Server: Apache/2.4.52 (Ubuntu)
| Last-Modified: Fri, 24 Feb 2023 14:35:39 GMT
| ETag: "29af-5f5730b170d83"
| Accept-Ranges: bytes
| Content-Length: 10671
| Vary: Accept-Encoding
| Connection: close
| Content-Type: text/html
|
|_ (Request type: HEAD)
Nmap done: 1 IP address (1 host up) scanned in 0.43 seconds
┌──(kali㉿kali)-[~]
└─$ nmap --script "ssh-*" gateway
Starting Nmap 7.92 (https://nmap.org) at 2023-02-25 16:01 GMT
NSE: [ssh-run] Failed to specify credentials and command to run.
NSE: [ssh-brute] Trying username/password pair: root:root
NSE: [ssh-brute] Trying username/password pair: admin:admin
NSE: [ssh-brute] Trying username/password pair: administrator:administrator
NSE: [ssh-brute] Trying username/password pair: webadmin:webadmin
NSE: [ssh-brute] Trying username/password pair: sysadmin:sysadmin
NSE: [ssh-brute] Trying username/password pair: netadmin:netadmin
NSE: [ssh-brute] Trying username/password pair: guest:guest
NSE: [ssh-brute] Trying username/password pair: user:user

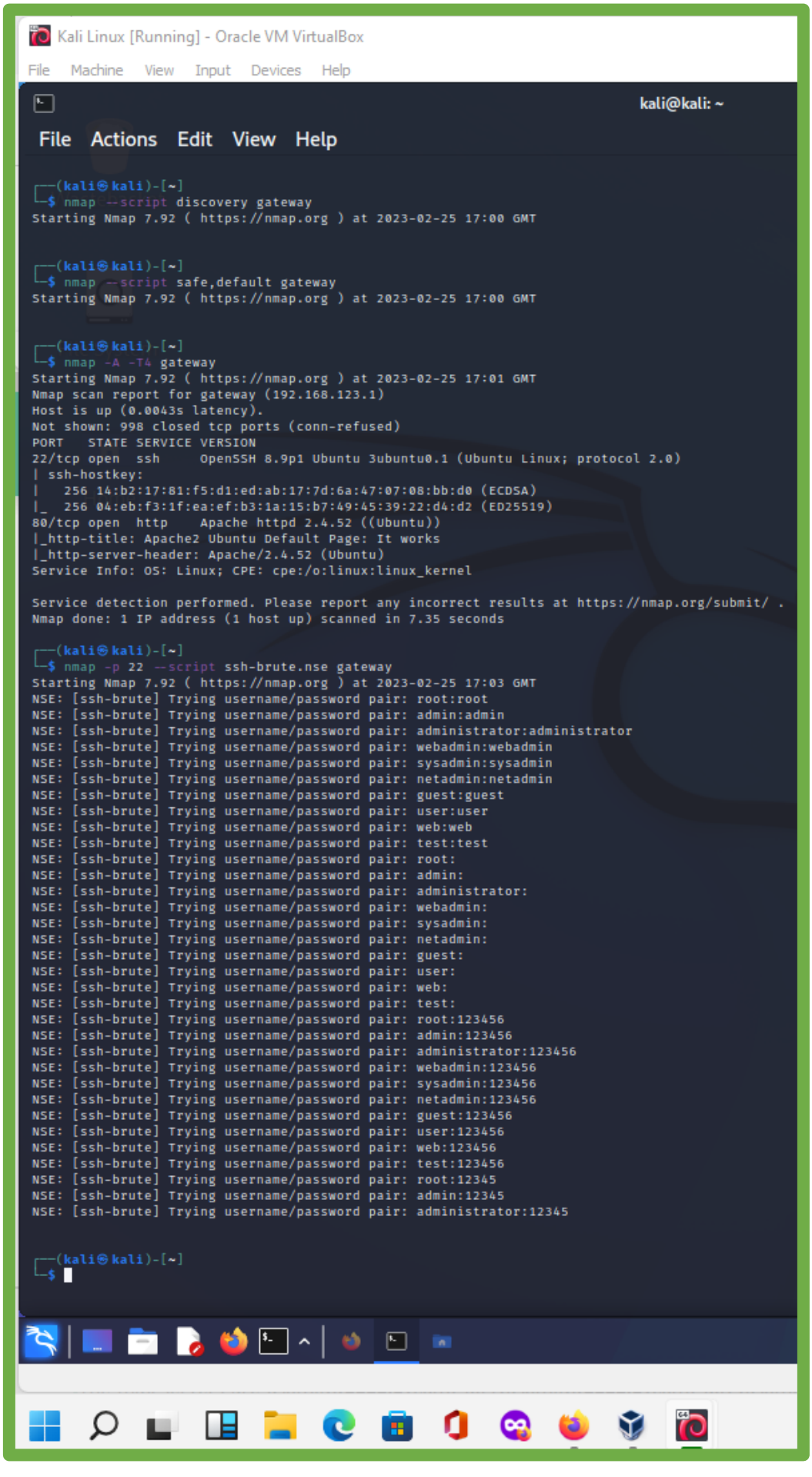

Kali Linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
kali@kali:
File Actions Edit View Help
NSE: [ssh-brute] Trying username/password pair: root:arsenal
NSE: [ssh-brute] Trying username/password pair: admin:arsenal
NSE: [ssh-brute] Trying username/password pair: administrator:arsenal
NSE: [ssh-brute] Trying username/password pair: webadmin:arsenal
NSE: [ssh-brute] Trying username/password pair: sysadmin:arsenal
NSE: [ssh-brute] Trying username/password pair: netadmin:arsenal
NSE: [ssh-brute] Trying username/password pair: guest:arsenal
NSE: [ssh-brute] Trying username/password pair: user:arsenal
NSE: [ssh-brute] Trying username/password pair: web:arsenal
NSE: [ssh-brute] Trying username/password pair: test:arsenal
NSE: [ssh-brute] Trying username/password pair: root:maggie
NSE: [ssh-brute] Trying username/password pair: admin:maggie
NSE: [ssh-brute] Trying username/password pair: administrator:maggie
NSE: [ssh-brute] Trying username/password pair: webadmin:maggie
NSE: [ssh-brute] Trying username/password pair: sysadmin:maggie
NSE: [ssh-brute] Trying username/password pair: netadmin:maggie
NSE: [ssh-brute] Trying username/password pair: guest:maggie
NSE: [ssh-brute] Trying username/password pair: user:maggie
NSE: [ssh-brute] Trying username/password pair: web:maggie
NSE: [ssh-brute] Trying username/password pair: test:maggie
NSE: [ssh-brute] Trying username/password pair: root:peanut
NSE: [ssh-brute] Trying username/password pair: admin:peanut
NSE: [ssh-brute] Trying username/password pair: administrator:peanut
NSE: [ssh-brute] Trying username/password pair: webadmin:peanut
NSE: [ssh-brute] Trying username/password pair: sysadmin:peanut
NSE: [ssh-brute] Trying username/password pair: netadmin:peanut
NSE: [ssh-brute] usernames: Time limit 10m00s exceeded.
NSE: [ssh-brute] usernames: Time limit 10m00s exceeded.
NSE: [ssh-brute] passwords: Time limit 10m00s exceeded.
Nmap scan report for gateway (192.168.123.1)
Host is up (0.0046s latency).
Not shown: 998 closed tcp ports (conn-refused)
PORT STATE SERVICE
22/tcp open ssh
| ssh-brute:
| Accounts: No valid accounts found
|_ Statistics: Performed 1606 guesses in 602 seconds, average tps: 2.8
|_ssh-run: Failed to specify credentials and command to run.
| ssh-publickey-acceptance:
|_ Accepted Public Keys: No public keys accepted
| ssh-auth-methods:
| Supported authentication methods:
| publickey
|_ password
| ssh-hostkey:
| 256 14:b2:17:81:f5:d1:ed:ab:17:7d:6a:47:07:08:bb:d0 (ECDSA)
|_ 256 04:eb:f3:1f:ea:ef:b3:1a:15:b7:49:45:39:22:d4:d2 (ED25519)
80/tcp open http
Nmap done: 1 IP address (1 host up) scanned in 602.80 seconds
(kali㉿kali)-[~]
$


Kali Linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
kali@kali: ~
File Actions Edit View Help
┌──(kali㉿kali)-[~]
└─$ nmap --script "not vuln" gateway
Starting Nmap 7.92 (https://nmap.org) at 2023-02-25 16:22 GMT
Pre-scan script results:
| targets-asn:
|_ targets-asn.asn is a mandatory parameter
|_http-robtex-shared-ns: *TEMPORARILY DISABLED* due to changes in Robtex's API. See https://www.robtex.com/api/
|_hostmap-robtex: *TEMPORARILY DISABLED* due to changes in Robtex's API. See https://www.robtex.com/api/
Nmap scan report for gateway (192.168.123.1)
Host is up (0.0037s latency).
Not shown: 998 closed tcp ports (conn-refused)
Bug in http-security-headers: no string output.
PORT STATE SERVICE
22/tcp open ssh
| ssh-publickey-acceptance:
|_ Accepted Public Keys: No public keys accepted
|_banner: SSH-2.0-OpenSSH_8.9p1 Ubuntu-3ubuntu0.1
| ssh2-enum-algos:
| kex_algorithms: (10)
| server_host_key_algorithms: (4)
| encryption_algorithms: (6)
| mac_algorithms: (10)
|_ compression_algorithms: (2)
| ssh-auth-methods:
| Supported authentication methods:
| publickey
|_ password
|_ssh-run: Failed to specify credentials and command to run.
| ssh-hostkey:
| 256 14:b2:17:81:f5:d1:ed:ab:17:7d:6a:47:07:08:bb:d0 (ECDSA)
|_ 256 04:eb:f3:1f:ea:ef:b3:1a:15:b7:49:45:39:22:d4:d2 (ED25519)
| ssh-brute:
| Accounts: No valid accounts found
|_ Statistics: Performed 22 guesses in 1807 seconds, average tps: 0.3
80/tcp open http
|_http-devframework: Couldn't determine the underlying framework or CMS. Try increasing 'httpspider.maxpagecount' value to spider more pages.
| http-errors:
| Spidering limited to: maxpagecount=40; withinhost=gateway
| Found the following error pages:
|
| Error Code: 404
|_ http://gateway:80/manual
|_http-slowloris: false
|_http-mobileversion-checker: No mobile version detected.
|_http-config-backup: ERROR: Script execution failed (use -d to debug)
| http-vhosts:
|_128 names had status 200
|_http-server-header: Apache/2.4.52 (Ubuntu)
|_http-title: Apache2 Ubuntu Default Page: It works
|_citrix-brute-xml: FAILED: No domain specified (use ntdomain argument)
| http-sitemap-generator:
| Directory structure:
| /
| Other: 1
| /icons/
| png: 1
| Longest directory structure:
| Depth: 1
| Dir: /icons/
| Total files found (by extension):
|_ Other: 1; png: 1
| http-xssed:
|
| UNFIXED XSS vuln.
|
| http://technologygateway.nasa.gov/index.cfm?fuseaction=%22%3E%3Ciframe%20src=%22http://xssed.com%22%
3E
|
| http://gateway.mdgms.com/login.html?LANG=%22%27%3E%3Cscript%3Ealert(%22XSS%22)%3C/script%3E
|
| http://www.workgateways.com/login.php?User=%22%20/%3E%3Cscript%3Ealert%28%22XSS%20by%20MadAgent%22%2
9%3C/script%3E%3Cbr%20%22

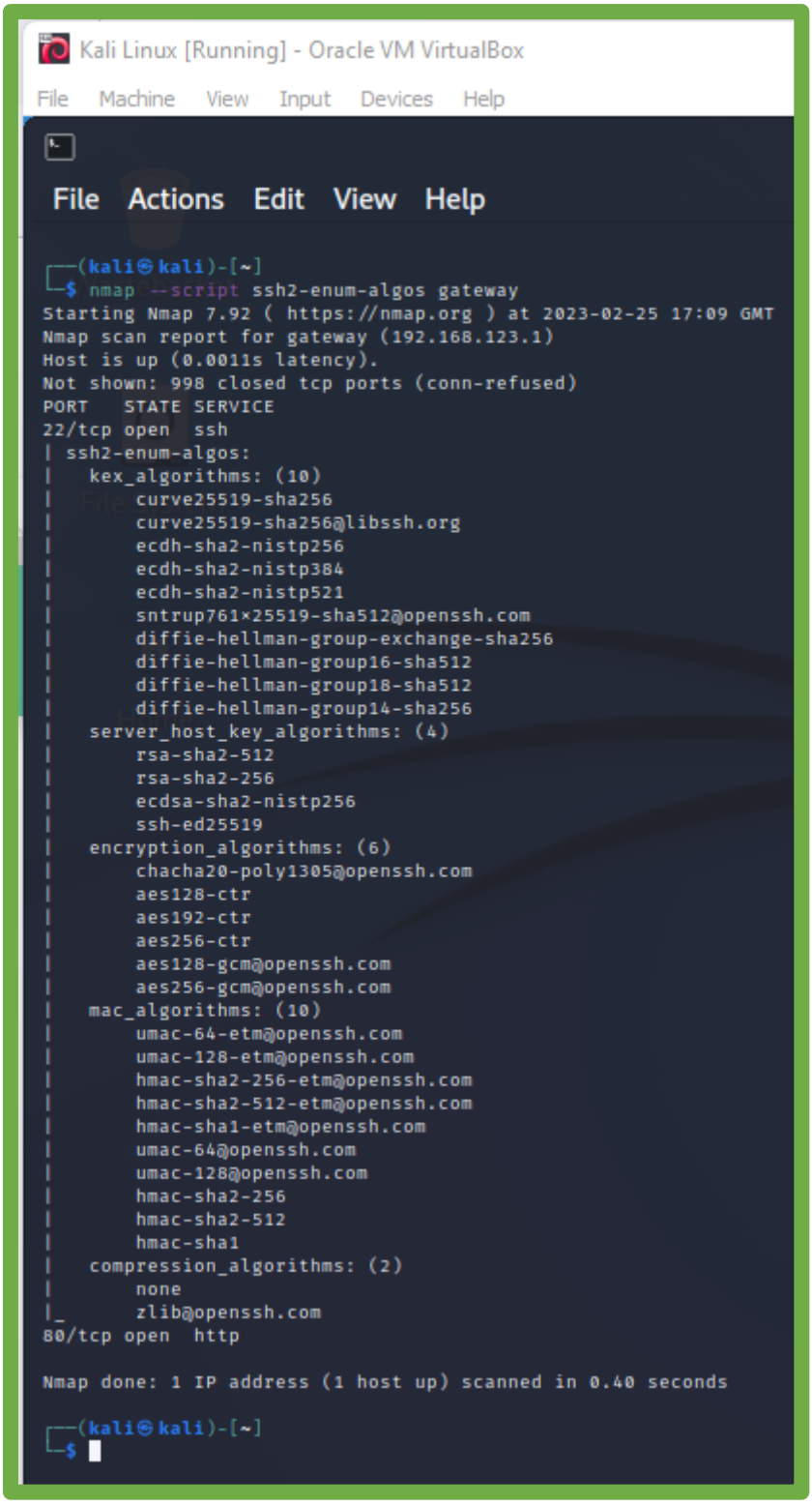

Kali Linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
kali@kali: ~
File Actions Edit View Help
UNFIXED XSS vuln.
http://technologygateway.nasa.gov/index.cfm?fuseaction=%22%3E%3Ciframe%20src=%22http://xssed.com%22%
3E
http://gateway.mdgms.com/login.html?LANG=%22%27%3E%3Cscript%3Ealert(%22XSS%22)%3C/script%3E
http://www.workgateways.com/login.php?User=%22%20/%3E%3Cscript%3Ealert%28%22XSS%20by%20MadAgent%22%2
9%3C/script%3E%3Cbr%20%22
http://www.capegateway.gov.za/search/index.php?q=error%22%3E%3Cscript%20language=javascript%3Ealert%
28document.cookie%29;%3C/script%3E
http://www.signaling-gateway.org/molecule/search?nm=%22%3E%3Cscript%3Ealert(%22XSS+BY+THEBIG%22)%3C%
2Fscript%3E&x=0&y=0
http://www.itergateway.org/iterbooks.cfm?code=Q}</style><script>a=eval;b=alert;a(b(/XSS/.source));</
script>'"><marquee><h1>Mystick</h1></marquee>
http://support.gateway.com/support/drivers/snnotfound.asp?sn=0000000000%27%22%3E%3C/TITLE%3E%3CSCRIP
T%3Ealert(%22XSS%22);%3C/SCRIPT%3E%3CMARQUEE%20BGCOLOR=%22RED%22%3E%3CH1%3EXSS%20by%20Xylitol%3C/H1%
3E%3C/MARQUEE%3E&ErrType=Driver
http://www.bulgaria-gateway.org/en/browser.php?state=content&type=article&cat_id=2%27%22%3E%3C/title
%3E%3Cscript%3Ealert(1337)%3C/script%3E%3E%3Cmarquee%3E%3Ch1%3EXSS%20by%20Xylitol%3C/h1%3E%3C/marque
e%3E
http://www.gateway.com/newsletter.php?seg=hm
https://www.gateway.com/order_status.php
https://www.gateway.com/login_user.php?goto=%22/%3E%3Cscript%20src=http://ha.ckers.org/xss.js?/%3E
http://support.gateway.com/support/drivers/instrPop.asp?fn=&ffn="/><script
src=http://ha.ckers.org/xss.js?/>&rp=&now=true
http://search.sales.gateway.com/query?redirect&target=http://xssed.com&tid=to8KMYmEL6Wlrr0&qid=qUyhr
Iz2wjLl4&vid=vkcJstPcD195P&qtid=qUyhrIz2wjLl4&feature=sitemap+url
http://support.gateway.com/support/drivers/getFile.asp?id=20905&dscr=</title><script%20src=http://ha
.ckers.org/xss.js?/>&uid=189341533
http://search.sales.gateway.com/iphrase/query?command=text&attr1=%22/%3E%3Cscript%20src=http://ha.ck
ers.org/xss.js?/%3E&attr2=%22?%3E&v0=3040gz&qt=12049894326&vid=vKveDJc8Q7ZNK&i=sitemap+id&qid=quPOm1D
ZGUpCq&s1=iphrase+relevance%2F%2F0&s0=category_number%2F%2F1&tq=1&q=20&g=sitemap+taxonomy&qtid=quPOm
1DZGUpCq&t=0&s2=sitemap+id%2F%2F1&ioe=iso-8859-1&c0=i%3A1%3B514%3Bsitemap+text%3B3040gz%3B%3A3040gz%
3B1%2C1%3B0&as=0&render=1&domains=sitemap+id&text=3040gz+drivers&submit.x=0&submit.y=0
http://www.biblegateway.com/keyword/?search=%22%3E%3CscrIPt%3Ealert%28123%29%3C%2FSCRipT%3E&searchty
pe=all&version1=31&spanbegin=1&spanend=73
https://gateway.inet-cash.de/mc/payment.php?EMAIL=%22%3E%3Cscript%3Ealert%28%2FNemessis-www.rstzone.
net%2F%29%3C%2Fscript%3E&zugang=25271%3Bxxddoudpxxxxxxxx&progid=23879&zahl=nix&lang=en&Dirty=false&c
hangezahlart=false
FIXED XSS vuln.
http://www.globalgateway.com/AddURL.asp?category=12&CFile="><script>alert(document.cookie);</scr
ipt>
http://www.globalgateway.com/Search.asp?criteria=%3Cscript%3Ealert%28document.cookie%29%3B%3C%2Fscri
pt%3E
https://crmgateway.paypal.com/payflow/cgi-bin/mail_pcancellation.pl?host=remote&processing=Yes&partn
er_login="><script>alert(/Nemessis-WWW.RSTZONE.ORG/)</script>
|_http-referer-checker: Couldn't find any cross-domain scripts.
|_http-chrono: Request times for /; avg: 179.98ms; min: 165.69ms; max: 194.87ms
| http-useragent-tester:
| Status for browser useragent: 200
| Allowed User Agents:
| Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)
| lib www
| lwp-trivial
| libcurl-agent/1.0
| PHP/
| Python-urllib/2.5
Notificati

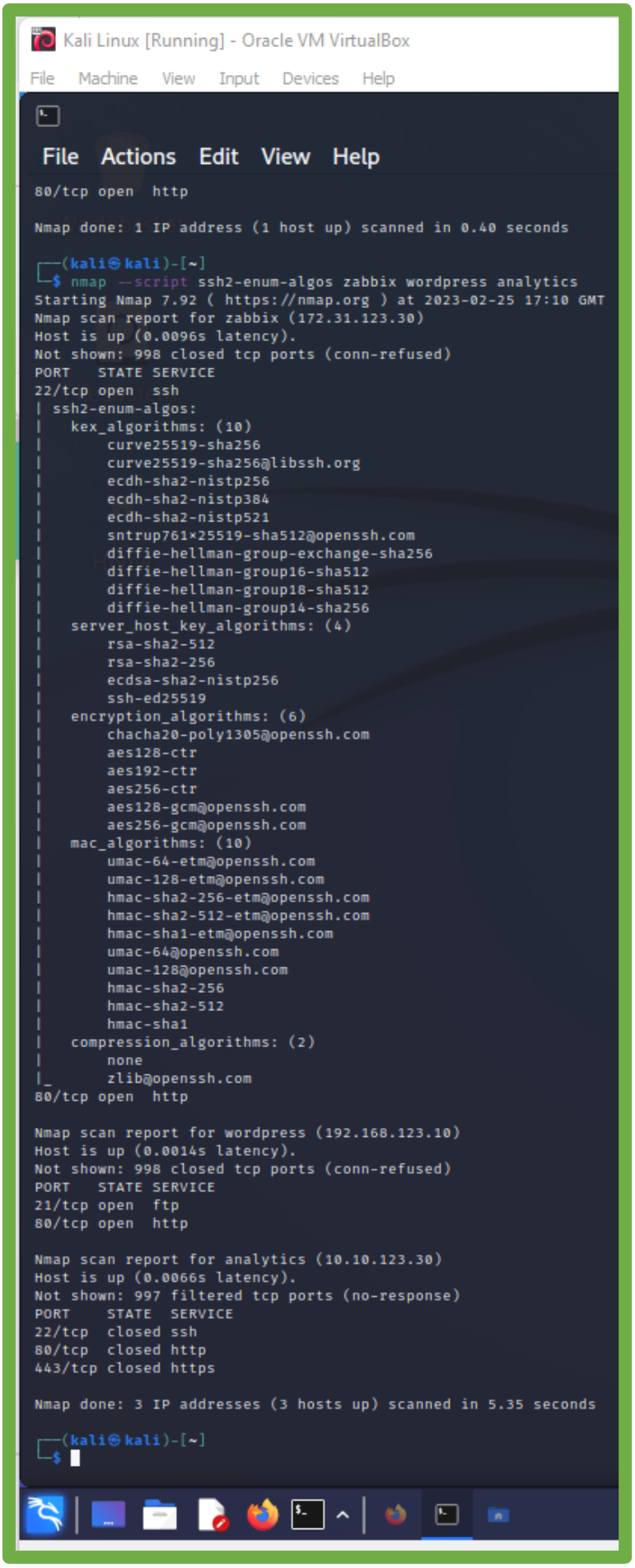

Kali Linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
kali@kali: ~
File Actions Edit View Help
| lwp-trivial
| libcurl-agent/1.0
| PHP/
| Python-urllib/2.5
| GT::WWW
| Snoopy
| MFC_Tear_Sample
| HTTP::Lite
| PHPCrawl
| URI::Fetch
| Zend_Http_Client
| http client
| PECL::HTTP
| Wget/1.13.4 (linux-gnu)
|_ WWW-Mechanize/1.34
| http-brute:
|_ Path "/" does not require authentication
|_http-feed: Couldn't find any feeds.
| http-headers:
| Date: Sat, 25 Feb 2023 16:53:37 GMT
| Server: Apache/2.4.52 (Ubuntu)
| Last-Modified: Fri, 24 Feb 2023 14:35:39 GMT
| ETag: "29af-5f5730b170d83"
| Accept-Ranges: bytes
| Content-Length: 10671
| Vary: Accept-Encoding
| Connection: close
| Content-Type: text/html
|
|_ (Request type: HEAD)
|_http-fetch: Please enter the complete path of the directory to save data in.
|_http-date: Sat, 25 Feb 2023 16:53:41 GMT; +1h00m09s from local time.
| http-comments-displayer:
| Spidering limited to: maxdepth=3; maxpagecount=20; withinhost=gateway
|
| Path: http://gateway:80/
| Line number: 3
| Comment:
| <!--
| Modified from the Debian original for Ubuntu
| Last updated: 2022-03-22
| See: https://launchpad.net/bugs/1966004
|_ -->
Host script results:
| dns-blacklist:
| SPAM
|_ l2.apews.org - FAIL
| port-states:
| tcp:
| open: 22,80
|_ closed: 1,3-4,6-7,9,13,17,19-21,23-26,30,32-33,37,42-43,49,53,70,79,81-85,88-90,99-100,106,109-111,113,119,125,135,139,143-144,146,161,163,179,199,211-212,222,254-256,259,264,280,301,306,311,340,366,389,406-407,416-417,425,427,443-445,458,464-465,481,497,500,512-515,524,541,543-545,548,554-555,563,587,593,616-617,625,631,636,646,648,666-668,683,687,691,700,705,711,714,720,722,726,749,765,777,783,787,800-801,808,843,873,880,888,898,900-903,911-912,981,987,990,992-993,995,999-1002,1007,1009-1011,1021-1100,1102,1104-1108,1110-1114,1117,1119,1121-1124,1126,1130-1132,1137-1138,1141,1145,1147-1149,1151-1152,1154,1163-1166,1169,1174-1175,1183,1185-1187,1192,1198-1199,1201,1213,1216-1218,1233-1234,1236,1244,1247-1248,1259,1271-1272,1277,1287,1296,1300-1301,1309-1311,1322,1328,1334,1352,1417,1433-1434,1443,1455,1461,1494,1500-1501,1503,1521,1524,1533,1556,1580,1583,1594,1600,1641,1658,1666,1687-1688,1700,1717-1721,1723,1755,1761,1782-1783,1801,1805,1812,1839-1840,1862-1864,1875,1900,1914,1935,1947,1971-1972,1974,1984,1998-2010,2013,2020-2022,2030,2033-2035,2038,2040-2043,2045-2049,2065,2068,2099-2100,2103,2105-2107,2111,2119,2121,2126,2135,2144,2160-2161,2170,2179,2190-2191,2196,2200,2222,2251,2260,2288,2301,2323,2366,2381-2383,2393-2394,2399,2401,2492,2500,2522,2525,2557,2601-2602,2604-2605,2607-2608,2638,2701-2702,2710,2717-2718,2725,2800,2809,2811,2869,2875,2909-2910,2920,2967-2968,2998,3000-3001,3003,3005-3007,3011,3013,3017,3030-3031,3052,3071,3077,3128,3168,3211,3221,3260-3261,3268-3269,3283,3300-3301,3306,3322-3325,3333,3351,3367,3369-3372,3389-3390,3404,3476,3493,3517,3527,3546,3551,3580,3659,3689-3690,3703,3737,3766,3784,3800-3801,3809,3814,3826-3828,3851,3869,3871,3878,3880,3889,3905,3914,3918,3920,3945,3971,3986,3995,3998,4000-4006,4045,4111,4125-4126,4129,4224,4242,4279,4321,4343,4443-4446,4449,4550,4567,4662,4848,4899-4900,4998,5000-5004,5009,5030,5033,5050-5051,5054,5060-5061,5080,5087,5100-5102,5120,5190,5200,5214,5221-5222,5225-5226,5269,5280,5298,5357,5405,5414,5431-5432,5440,5500,5510,5544,5550,5555,5560,5566,5631,5633,5666,5678-5679,5718,5730,5800-5802,5810-5811,5815,5822,5825,5850,5859,5862,5877,5900-5904,5906-5907,5910-5911,5915,5922,5925,5950,5952,5959-5963,5987-5989,5998-6007,6009,6025,6059,6100-6101,6106,6112,6123,6129,6156,6346,6389,6502,6510,6543,6547,6565-6567,6580,6646,6666-6669,6689,6692,6699,6779,6788-6789,6792,6839,6881,6901,6969,7000-7002,7004,7007,7019,7025,7070,7100,7103,7106,7200-7201,7402,7435,7443,7496,7512,7625,7627,7676,7741,7777-7778,7800,7911,7920-7921,7937-7938,7999-8002,8007-8011,8021-8022,8031,8042,8045,8080-8090,8093,8099-8100,8180-8181,8192-8194,8200,8222,8254,8290-8292,8300,8333,8383,8400,8402,8443,8500,8600,8649,8651-8652,8654,8701,8800,8873,8888,8899,8994,9000-9003,9009-9011,9040,9050,9071,9080-9081,9090-9091,9099-9103,9110-9111,9200,9207,9220,9290,9415,9418,9485,


Kali Linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
kali@kali: ~
File Actions Edit View Help
|
|_ (Request type: HEAD)
|_http-fetch: Please enter the complete path of the directory to save data in.
|_http-date: Sat, 25 Feb 2023 16:53:41 GMT; +1h00m09s from local time.
| http-comments-displayer:
| Spidering limited to: maxdepth=3; maxpagecount=20; withinhost=gateway
|
| Path: http://gateway:80/
| Line number: 3
| Comment:
| <!--
| Modified from the Debian original for Ubuntu
| Last updated: 2022-03-22
| See: https://launchpad.net/bugs/1966004
|_ -->
Host script results:
| dns-blacklist:
| SPAM
|_ l2.apews.org - FAIL
| port-states:
| tcp:
| open: 22,80
|_ closed: 1,3-4,6-7,9,13,17,19-21,23-26,30,32-33,37,42-43,49,53,70,79,81-85,88-90,99-100,106,109-111,113,119,125,135,139,143-144,146,161,163,179,199,211-212,222,254-256,259,264,280,301,306,311,340,366,389,406-407,416-417,425,427,443-445,458,464-465,481,497,500,512-515,524,541,543-545,548,554-555,563,587,593,616-617,625,631,636,646,648,666-668,683,687,691,700,705,711,714,720,722,726,749,765,777,783,787,800-801,808,843,873,880,888,898,900-903,911-912,981,987,990,992-993,995,999-1002,1007,1009-1011,1021-1100,1102,1104-1108,1110-1114,1117,1119,1121-1124,1126,1130-1132,1137-1138,1141,1145,1147-1149,1151-1152,1154,1163-1166,1169,1174-1175,1183,1185-1187,1192,1198-1199,1201,1213,1216-1218,1233-1234,1236,1244,1247-1248,1259,1271-1272,1277,1287,1296,1300-1301,1309-1311,1322,1328,1334,1352,1417,1433-1434,1443,1455,1461,1494,1500-1501,1503,1521,1524,1533,1556,1580,1583,1594,1600,1641,1658,1666,1687-1688,1700,1717-1721,1723,1755,1761,1782-1783,1801,1805,1812,1839-1840,1862-1864,1875,1900,1914,1935,1947,1971-1972,1974,1984,1998-2010,2013,2020-2022,2030,2033-2035,2038,2040-2043,2045-2049,2065,2068,2099-2100,2103,2105-2107,2111,2119,2121,2126,2135,2144,2160-2161,2170,2179,2190-2191,2196,2200,2222,2251,2260,2288,2301,2323,2366,2381-2383,2393-2394,2399,2401,2492,2500,2522,2525,2557,2601-2602,2604-2605,2607-2608,2638,2701-2702,2710,2717-2718,2725,2800,2809,2811,2869,2875,2909-2910,2920,2967-2968,2998,3000-3001,3003,3005-3007,3011,3013,3017,3030-3031,3052,3071,3077,3128,3168,3211,3221,3260-3261,3268-3269,3283,3300-3301,3306,3322-3325,3333,3351,3367,3369-3372,3389-3390,3404,3476,3493,3517,3527,3546,3551,3580,3659,3689-3690,3703,3737,3766,3784,3800-3801,3809,3814,3826-3828,3851,3869,3871,3878,3880,3889,3905,3914,3918,3920,3945,3971,3986,3995,3998,4000-4006,4045,4111,4125-4126,4129,4224,4242,4279,4321,4343,4443-4446,4449,4550,4567,4662,4848,4899-4900,4998,5000-5004,5009,5030,5033,5050-5051,5054,5060-5061,5080,5087,5100-5102,5120,5190,5200,5214,5221-5222,5225-5226,5269,5280,5298,5357,5405,5414,5431-5432,5440,5500,5510,5544,5550,5555,5560,5566,5631,5633,5666,5678-5679,5718,5730,5800-5802,5810-5811,5815,5822,5825,5850,5859,5862,5877,5900-5904,5906-5907,5910-5911,5915,5922,5925,5950,5952,5959-5963,5987-5989,5998-6007,6009,6025,6059,6100-6101,6106,6112,6123,6129,6156,6346,6389,6502,6510,6543,6547,6565-6567,6580,6646,6666-6669,6689,6692,6699,6779,6788-6789,6792,6839,6881,6901,6969,7000-7002,7004,7007,7019,7025,7070,7100,7103,7106,7200-7201,7402,7435,7443,7496,7512,7625,7627,7676,7741,7777-7778,7800,7911,7920-7921,7937-7938,7999-8002,8007-8011,8021-8022,8031,8042,8045,8080-8090,8093,8099-8100,8180-8181,8192-8194,8200,8222,8254,8290-8292,8300,8333,8383,8400,8402,8443,8500,8600,8649,8651-8652,8654,8701,8800,8873,8888,8899,8994,9000-9003,9009-9011,9040,9050,9071,9080-9081,9090-9091,9099-9103,9110-9111,9200,9207,9220,9290,9415,9418,9485,9500,9502-9503,9535,9575,9593-9595,9618,9666,9876-9878,9898,9900,9917,9929,9943-9944,9968,9998-10004,10009-10010,10012,10024-10025,10082,10180,10215,10243,10566,10616-10617,10621,10626,10628-10629,10778,11110-11111,11967,12000,12174,12265,12345,13456,13722,13782-13783,14000,14238,14441-14442,15000,15002-15004,15660,15742,16000-16001,16012,16016,16018,16080,16113,16992-16993,17877,17988,18040,18101,18988,19101,19283,19315,19350,19780,19801,19842,20000,20005,20031,20221-20222,20828,21571,22939,23502,24444,24800,25734-25735,26214,27000,27352-27353,27355-27356,27715,28201,30000,30718,30951,31038,31337,32768-32785,33354,33899,34571-34573,35500,38292,40193,40911,41511,42510,44176,44442-44443,44501,45100,48080,49152-49161,49163,49165,49167,49175-49176,49400,49999-50003,50006,50300,50389,50500,50636,50800,51103,51493,52673,52822,52848,52869,54045,54328,55055-55056,55555,55600,56737-56738,57294,57797,58080,60020,60443,61532,61900,62078,63331,64623,64680,65000,65129,65389
| unusual-port:
|_ WARNING: this script depends on Nmap's service/version detection (-sV)
|_dns-brute: Can't guess domain of "gateway"; use dns-brute.domain script argument.
| resolveall:
| Host 'gateway' also resolves to:
| Use the 'newtargets' script-arg to add the results as targets
|_ Use the --resolve-all option to scan all resolved addresses without using this script.
|_fcrdns: FAIL (No PTR record)
|_clock-skew: 1h00m08s
Post-scan script results:
| reverse-index:
| 22/tcp: 192.168.123.1
|_ 80/tcp: 192.168.123.1
Nmap done: 1 IP address (1 host up) scanned in 1904.11 seconds
┌──(kali㉿kali)-[~]
└─$

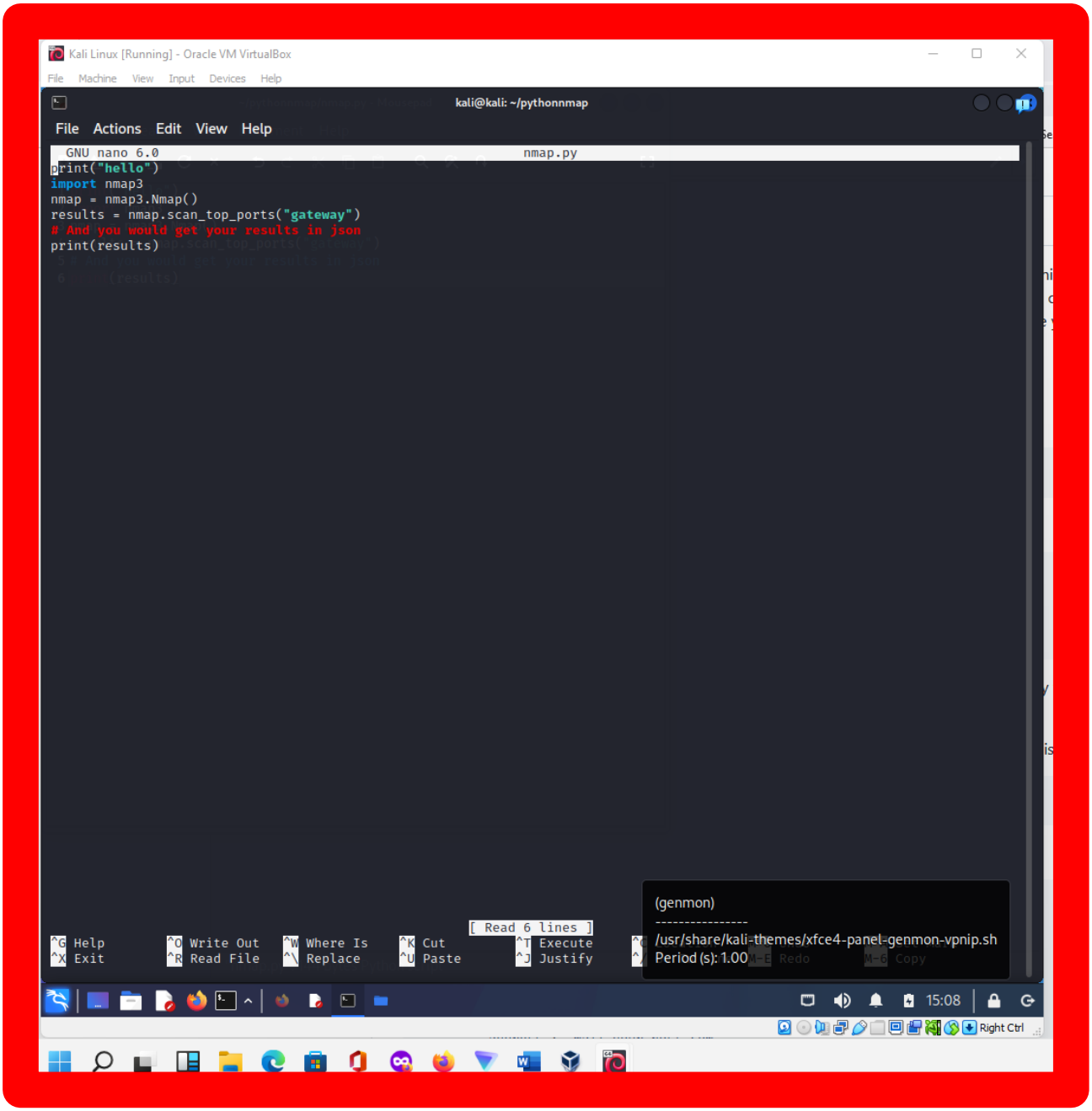

Kali Linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
kali@kali: ~
File Actions Edit View Help
┌──(kali㉿kali)-[~]
└─$ nmap --script discovery gateway
Starting Nmap 7.92 (https://nmap.org) at 2023-02-25 17:00 GMT
┌──(kali㉿kali)-[~]
└─$ nmap --script safe,default gateway
Starting Nmap 7.92 (https://nmap.org) at 2023-02-25 17:00 GMT
┌──(kali㉿kali)-[~]
└─$ nmap -A -T4 gateway
Starting Nmap 7.92 (https://nmap.org) at 2023-02-25 17:01 GMT
Nmap scan report for gateway (192.168.123.1)
Host is up (0.0043s latency).
Not shown: 998 closed tcp ports (conn-refused)
PORT STATE SERVICE VERSION
22/tcp open ssh OpenSSH 8.9p1 Ubuntu 3ubuntu0.1 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
| 256 14:b2:17:81:f5:d1:ed:ab:17:7d:6a:47:07:08:bb:d0 (ECDSA)
|_ 256 04:eb:f3:1f:ea:ef:b3:1a:15:b7:49:45:39:22:d4:d2 (ED25519)
80/tcp open http Apache httpd 2.4.52 ((Ubuntu))
|_http-title: Apache2 Ubuntu Default Page: It works
|_http-server-header: Apache/2.4.52 (Ubuntu)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 7.35 seconds
┌──(kali㉿kali)-[~]
└─$ nmap -p 22 --script ssh-brute.nse gateway
Starting Nmap 7.92 (https://nmap.org) at 2023-02-25 17:03 GMT
NSE: [ssh-brute] Trying username/password pair: root:root
NSE: [ssh-brute] Trying username/password pair: admin:admin
NSE: [ssh-brute] Trying username/password pair: administrator:administrator
NSE: [ssh-brute] Trying username/password pair: webadmin:webadmin
NSE: [ssh-brute] Trying username/password pair: sysadmin:sysadmin
NSE: [ssh-brute] Trying username/password pair: netadmin:netadmin
NSE: [ssh-brute] Trying username/password pair: guest:guest
NSE: [ssh-brute] Trying username/password pair: user:user
NSE: [ssh-brute] Trying username/password pair: web:web
NSE: [ssh-brute] Trying username/password pair: test:test
NSE: [ssh-brute] Trying username/password pair: root:
NSE: [ssh-brute] Trying username/password pair: admin:
NSE: [ssh-brute] Trying username/password pair: administrator:
NSE: [ssh-brute] Trying username/password pair: webadmin:
NSE: [ssh-brute] Trying username/password pair: sysadmin:
NSE: [ssh-brute] Trying username/password pair: netadmin:
NSE: [ssh-brute] Trying username/password pair: guest:
NSE: [ssh-brute] Trying username/password pair: user:
NSE: [ssh-brute] Trying username/password pair: web:
NSE: [ssh-brute] Trying username/password pair: test:
NSE: [ssh-brute] Trying username/password pair: root:123456
NSE: [ssh-brute] Trying username/password pair: admin:123456
NSE: [ssh-brute] Trying username/password pair: administrator:123456
NSE: [ssh-brute] Trying username/password pair: webadmin:123456
NSE: [ssh-brute] Trying username/password pair: sysadmin:123456
NSE: [ssh-brute] Trying username/password pair: netadmin:123456
NSE: [ssh-brute] Trying username/password pair: guest:123456
NSE: [ssh-brute] Trying username/password pair: user:123456
NSE: [ssh-brute] Trying username/password pair: web:123456
NSE: [ssh-brute] Trying username/password pair: test:123456
NSE: [ssh-brute] Trying username/password pair: root:12345
NSE: [ssh-brute] Trying username/password pair: admin:12345
NSE: [ssh-brute] Trying username/password pair: administrator:12345
┌──(kali㉿kali)-[~]
└─$

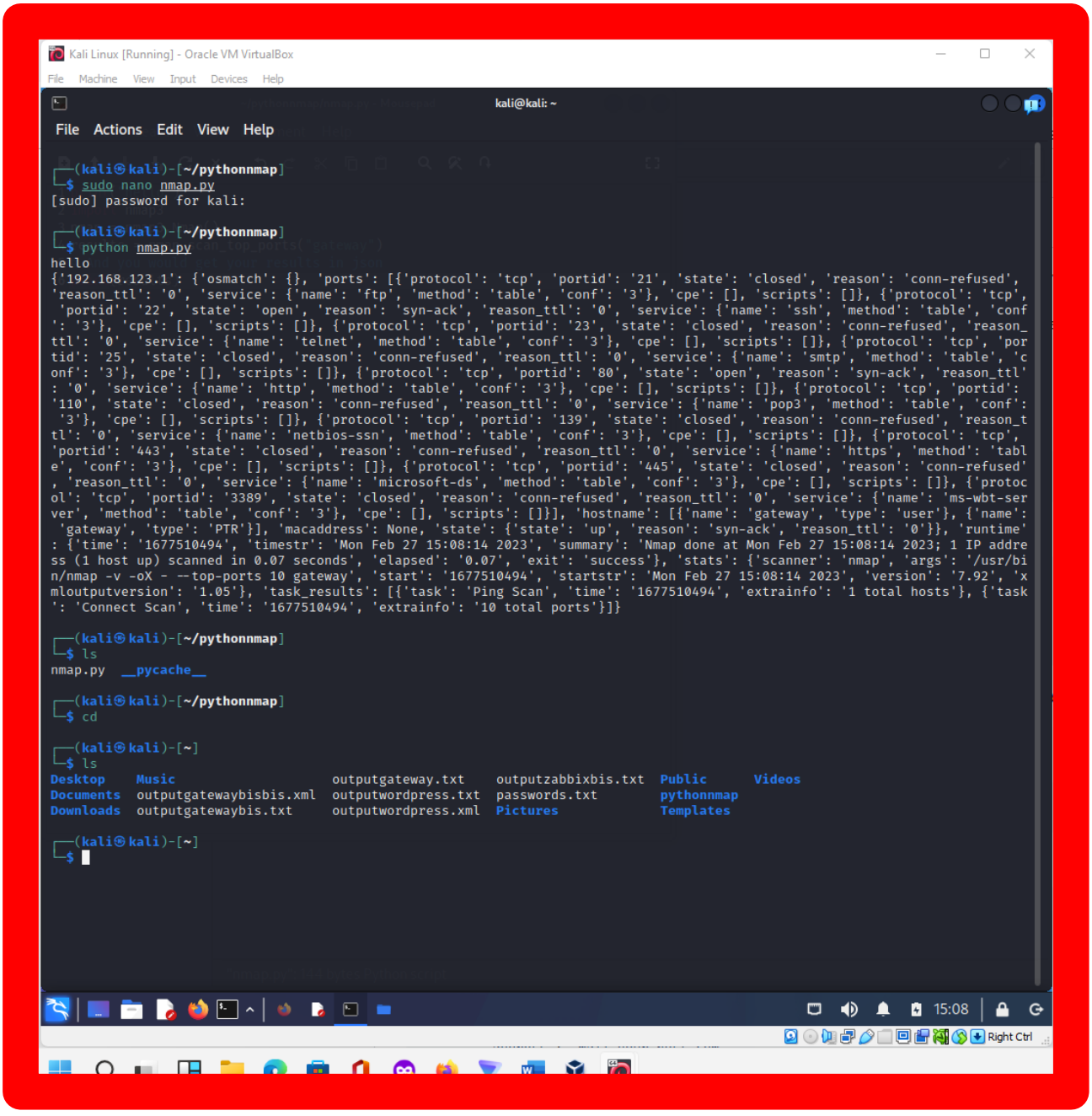

Kali Linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
kali@kali: ~
File Actions Edit View Help
┌──(kali㉿kali)-[~]
└─$ nmap -p 22 --script=ssh-run gateway
Starting Nmap 7.92 (https://nmap.org) at 2023-02-25 17:06 GMT
NSE: [ssh-run] Failed to specify credentials and command to run.
Nmap scan report for gateway (192.168.123.1)
Host is up (0.0018s latency).
PORT STATE SERVICE
22/tcp open ssh
|_ssh-run: Failed to specify credentials and command to run.
Nmap done: 1 IP address (1 host up) scanned in 0.29 seconds
┌──(kali㉿kali)-[~]
└─$ nmap -p 22 --script ssh-auth-methods --script-args="ssh.user=student" gateway
Starting Nmap 7.92 (https://nmap.org) at 2023-02-25 17:08 GMT
Nmap scan report for gateway (192.168.123.1)
Host is up (0.0011s latency).
PORT STATE SERVICE
22/tcp open ssh
| ssh-auth-methods:
| Supported authentication methods:
| publickey
|_ password
Nmap done: 1 IP address (1 host up) scanned in 0.30 seconds
┌──(kali㉿kali)-[~]
└─$ nmap -p 22 --script ssh-auth-methods --script-args="ssh.user=student" wordpress
Starting Nmap 7.92 (https://nmap.org) at 2023-02-25 17:08 GMT
Nmap scan report for wordpress (192.168.123.10)
Host is up (0.0022s latency).
PORT STATE SERVICE
22/tcp closed ssh
Nmap done: 1 IP address (1 host up) scanned in 0.30 seconds
┌──(kali㉿kali)-[~]
└─$ nmap -p 22 --script ssh-auth-methods --script-args="ssh.user=student" analytics
Starting Nmap 7.92 (https://nmap.org) at 2023-02-25 17:08 GMT
Nmap scan report for analytics (10.10.123.30)
Host is up (0.0030s latency).
PORT STATE SERVICE
22/tcp closed ssh
Nmap done: 1 IP address (1 host up) scanned in 0.28 seconds
┌──(kali㉿kali)-[~]
└─$ nmap -p 22 --script ssh-auth-methods --script-args="ssh.user=student" zabbix
Starting Nmap 7.92 (https://nmap.org) at 2023-02-25 17:08 GMT
Nmap scan report for zabbix (172.31.123.30)
Host is up (0.0025s latency).
PORT STATE SERVICE
22/tcp open ssh
| ssh-auth-methods:
| Supported authentication methods:
| publickey
|_ password
Nmap done: 1 IP address (1 host up) scanned in 0.32 seconds
┌──(kali㉿kali)-[~]
└─$


Kali Linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
File Actions Edit View Help
┌──(kali㉿kali)-[~]
└─$ nmap --script ssh2-enum-algos gateway
Starting Nmap 7.92 (https://nmap.org) at 2023-02-25 17:09 GMT
Nmap scan report for gateway (192.168.123.1)
Host is up (0.0011s latency).
Not shown: 998 closed tcp ports (conn-refused)
PORT STATE SERVICE
22/tcp open ssh
| ssh2-enum-algos:
| kex_algorithms: (10)
| curve25519-sha256
| curve25519-sha256@libssh.org
| ecdh-sha2-nistp256
| ecdh-sha2-nistp384
| ecdh-sha2-nistp521
| sntrup761x25519-sha512@openssh.com
| diffie-hellman-group-exchange-sha256
| diffie-hellman-group16-sha512
| diffie-hellman-group18-sha512
| diffie-hellman-group14-sha256
| server_host_key_algorithms: (4)
| rsa-sha2-512
| rsa-sha2-256
| ecdsa-sha2-nistp256
| ssh-ed25519
| encryption_algorithms: (6)
| chacha20-poly1305@openssh.com
| aes128-ctr
| aes192-ctr
| aes256-ctr
| aes128-gcm@openssh.com
| aes256-gcm@openssh.com
| mac_algorithms: (10)
| umac-64-etm@openssh.com
| umac-128-etm@openssh.com
| hmac-sha2-256-etm@openssh.com
| hmac-sha2-512-etm@openssh.com
| hmac-sha1-etm@openssh.com
| umac-64@openssh.com
| umac-128@openssh.com
| hmac-sha2-256
| hmac-sha2-512
| hmac-sha1
| compression_algorithms: (2)
| none
|_ zlib@openssh.com
80/tcp open http
Nmap done: 1 IP address (1 host up) scanned in 0.40 seconds
┌──(kali㉿kali)-[~]
└─$


Kali Linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
File Actions Edit View Help
80/tcp open http
Nmap done: 1 IP address (1 host up) scanned in 0.40 seconds
┌──(kali㉿kali)-[~]
└─$ nmap --script ssh2-enum-algos zabbix wordpress analytics
Starting Nmap 7.92 (https://nmap.org) at 2023-02-25 17:10 GMT
Nmap scan report for zabbix (172.31.123.30)
Host is up (0.0096s latency).
Not shown: 998 closed tcp ports (conn-refused)
PORT STATE SERVICE
22/tcp open ssh
| ssh2-enum-algos:
| kex_algorithms: (10)
| curve25519-sha256
| curve25519-sha256@libssh.org
| ecdh-sha2-nistp256
| ecdh-sha2-nistp384
| ecdh-sha2-nistp521
| sntrup761x25519-sha512@openssh.com
| diffie-hellman-group-exchange-sha256
| diffie-hellman-group16-sha512
| diffie-hellman-group18-sha512
| diffie-hellman-group14-sha256
| server_host_key_algorithms: (4)
| rsa-sha2-512
| rsa-sha2-256
| ecdsa-sha2-nistp256
| ssh-ed25519
| encryption_algorithms: (6)
| chacha20-poly1305@openssh.com
| aes128-ctr
| aes192-ctr
| aes256-ctr
| aes128-gcm@openssh.com
| aes256-gcm@openssh.com
| mac_algorithms: (10)
| umac-64-etm@openssh.com
| umac-128-etm@openssh.com
| hmac-sha2-256-etm@openssh.com
| hmac-sha2-512-etm@openssh.com
| hmac-sha1-etm@openssh.com
| umac-64@openssh.com
| umac-128@openssh.com
| hmac-sha2-256
| hmac-sha2-512
| hmac-sha1
| compression_algorithms: (2)
| none
|_ zlib@openssh.com
80/tcp open http
Nmap scan report for wordpress (192.168.123.10)
Host is up (0.0014s latency).
Not shown: 998 closed tcp ports (conn-refused)
PORT STATE SERVICE
21/tcp open ftp
80/tcp open http
Nmap scan report for analytics (10.10.123.30)
Host is up (0.0066s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT STATE SERVICE
22/tcp closed ssh
80/tcp closed http
443/tcp closed https
Nmap done: 3 IP addresses (3 hosts up) scanned in 5.35 seconds
┌──(kali㉿kali)-[~]
└─$

```
┌──(kali㉿kali)-[~]
└─$ nmap host --script ssh-hostkey --script-args ssh_hostkey=full gateway
Starting Nmap 7.92 ( https://nmap.org ) at 2023-02-25 17:12 GMT
Failed to resolve "host".
Nmap scan report for gateway (192.168.123.1)
Host is up (0.0035s latency).
Not shown: 998 closed tcp ports (conn-refused)
PORT   STATE SERVICE
22/tcp open  ssh
| ssh-hostkey:
|   ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBPpx1TBHqs2yUJgo6YZIfyuZp8u6LMc7EduKctXNG2Ds0/yoQYQimRt8xPu3vExighqAjKQmqxS7CQ7FU7NTHIE=
|_  ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAICg668t5RY27qAFi3KVR27322uuCbj1N54TTeJfXP/z2
80/tcp open  http

Nmap done: 1 IP address (1 host up) scanned in 1.01 seconds

┌──(kali㉿kali)-[~]
└─$ nmap gateway --script ssh-hostkey --script-args ssh_hostkey=full
Starting Nmap 7.92 ( https://nmap.org ) at 2023-02-25 17:12 GMT
Nmap scan report for gateway (192.168.123.1)
Host is up (0.0049s latency).
Not shown: 998 closed tcp ports (conn-refused)
PORT   STATE SERVICE
22/tcp open  ssh
| ssh-hostkey:
|   ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBPpx1TBHqs2yUJgo6YZIfyuZp8u6LMc7EduKctXNG2Ds0/yoQYQimRt8xPu3vExighqAjKQmqxS7CQ7FU7NTHIE=
|_  ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAICg668t5RY27qAFi3KVR27322uuCbj1N54TTeJfXP/z2
80/tcp open  http

Nmap done: 1 IP address (1 host up) scanned in 1.03 seconds

┌──(kali㉿kali)-[~]
└─$ nmap zabbix --script ssh-hostkey --script-args ssh_hostkey=full
Starting Nmap 7.92 ( https://nmap.org ) at 2023-02-25 17:13 GMT
Nmap scan report for zabbix (172.31.123.30)
Host is up (0.0036s latency).
Not shown: 998 closed tcp ports (conn-refused)
PORT   STATE SERVICE
22/tcp open  ssh
| ssh-hostkey:
|   ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBPpx1TBHqs2yUJgo6YZIfyuZp8u6LMc7EduKctXNG2Ds0/yoQYQimRt8xPu3vExighqAjKQmqxS7CQ7FU7NTHIE=
|_  ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAICg668t5RY27qAFi3KVR27322uuCbj1N54TTeJfXP/z2
80/tcp open  http

Nmap done: 1 IP address (1 host up) scanned in 0.70 seconds

┌──(kali㉿kali)-[~]
└─$ nmap wordpress --script ssh-hostkey --script-args ssh_hostkey=full
Starting Nmap 7.92 ( https://nmap.org ) at 2023-02-25 17:13 GMT
Nmap scan report for wordpress (192.168.123.10)
Host is up (0.0011s latency).
Not shown: 998 closed tcp ports (conn-refused)
PORT   STATE SERVICE
21/tcp open  ftp
80/tcp open  http

Nmap done: 1 IP address (1 host up) scanned in 0.39 seconds

┌──(kali㉿kali)-[~]
└─$ nmap analytics --script ssh-hostkey --script-args ssh_hostkey=full
Starting Nmap 7.92 ( https://nmap.org ) at 2023-02-25 17:13 GMT
Nmap scan report for analytics (10.10.123.30)
Host is up (0.0027s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT    STATE  SERVICE
22/tcp  closed ssh
80/tcp  closed http
443/tcp closed https

Nmap done: 1 IP address (1 host up) scanned in 5.04 seconds
```


Kali Linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
kali@kali: ~/pythonnmap
File Actions Edit View Help
GNU nano 6.0 nmap.py
print("hello")
import nmap3
nmap = nmap3.Nmap()
results = nmap.scan_top_ports("gateway")
# And you would get your results in json
print(results)
[Read 6 lines]
^G Help ^O Write Out ^W Where Is ^K Cut ^T Execute
^X Exit ^R Read File ^\ Replace ^U Paste ^J Justify
(genmon)
/usr/share/kali-themes/xfce4-panel-genmon-vpnip.sh
Period (s): 1.00
15:08
Right Ctrl


Kali Linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
kali@kali: ~
File Actions Edit View Help
(kali㉿kali)-[~/pythonnmap]
$ sudo nano nmap.py
[sudo] password for kali:
(kali㉿kali)-[~/pythonnmap]
$ python nmap.py
hello
{'192.168.123.1': {'osmatch': {}, 'ports': [{'protocol': 'tcp', 'portid': '21', 'state': 'closed', 'reason': 'conn-refused', 'reason_ttl': '0', 'service': {'name': 'ftp', 'method': 'table', 'conf': '3'}, 'cpe': [], 'scripts': []}, {'protocol': 'tcp', 'portid': '22', 'state': 'open', 'reason': 'syn-ack', 'reason_ttl': '0', 'service': {'name': 'ssh', 'method': 'table', 'conf': '3'}, 'cpe': [], 'scripts': []}, {'protocol': 'tcp', 'portid': '23', 'state': 'closed', 'reason': 'conn-refused', 'reason_ttl': '0', 'service': {'name': 'telnet', 'method': 'table', 'conf': '3'}, 'cpe': [], 'scripts': []}, {'protocol': 'tcp', 'portid': '25', 'state': 'closed', 'reason': 'conn-refused', 'reason_ttl': '0', 'service': {'name': 'smtp', 'method': 'table', 'conf': '3'}, 'cpe': [], 'scripts': []}, {'protocol': 'tcp', 'portid': '80', 'state': 'open', 'reason': 'syn-ack', 'reason_ttl': '0', 'service': {'name': 'http', 'method': 'table', 'conf': '3'}, 'cpe': [], 'scripts': []}, {'protocol': 'tcp', 'portid': '110', 'state': 'closed', 'reason': 'conn-refused', 'reason_ttl': '0', 'service': {'name': 'pop3', 'method': 'table', 'conf': '3'}, 'cpe': [], 'scripts': []}, {'protocol': 'tcp', 'portid': '139', 'state': 'closed', 'reason': 'conn-refused', 'reason_ttl': '0', 'service': {'name': 'netbios-ssn', 'method': 'table', 'conf': '3'}, 'cpe': [], 'scripts': []}, {'protocol': 'tcp', 'portid': '443', 'state': 'closed', 'reason': 'conn-refused', 'reason_ttl': '0', 'service': {'name': 'https', 'method': 'table', 'conf': '3'}, 'cpe': [], 'scripts': []}, {'protocol': 'tcp', 'portid': '445', 'state': 'closed', 'reason': 'conn-refused', 'reason_ttl': '0', 'service': {'name': 'microsoft-ds', 'method': 'table', 'conf': '3'}, 'cpe': [], 'scripts': []}, {'protocol': 'tcp', 'portid': '3389', 'state': 'closed', 'reason': 'conn-refused', 'reason_ttl': '0', 'service': {'name': 'ms-wbt-server', 'method': 'table', 'conf': '3'}, 'cpe': [], 'scripts': []}], 'hostname': [{'name': 'gateway', 'type': 'user'}, {'name': 'gateway', 'type': 'PTR'}], 'macaddress': None, 'state': {'state': 'up', 'reason': 'syn-ack', 'reason_ttl': '0'}}, 'runtime': {'time': '1677510494', 'timestr': 'Mon Feb 27 15:08:14 2023', 'summary': 'Nmap done at Mon Feb 27 15:08:14 2023; 1 IP address (1 host up) scanned in 0.07 seconds', 'elapsed': '0.07', 'exit': 'success'}, 'stats': {'scanner': 'nmap', 'args': '/usr/bin/nmap -v -oX - --top-ports 10 gateway', 'start': '1677510494', 'startstr': 'Mon Feb 27 15:08:14 2023', 'version': '7.92', 'xmloutputversion': '1.05'}, 'task_results': [{'task': 'Ping Scan', 'time': '1677510494', 'extrainfo': '1 total hosts'}, {'task': 'Connect Scan', 'time': '1677510494', 'extrainfo': '10 total ports'}]}
(kali㉿kali)-[~/pythonnmap]
$ ls
nmap.py __pycache__
(kali㉿kali)-[~/pythonnmap]
$ cd
(kali㉿kali)-[~]
$ ls
Desktop Music outputgateway.txt outputzabbixbis.txt Public Videos
Documents outputgatewaybisbis.xml outputwordpress.txt passwords.txt pythonnmap
Downloads outputgatewaybis.txt outputwordpress.xml Pictures Templates
(kali㉿kali)-[~]
$
15:08
Right Ctrl

Please complete the following table and upload this document to Moodle.

Declaration	I certify that the work for this portfolio lab is my own work.
Brief WOW Factor Description (if completed)	Req. A and Req. B has wow factor included in screenshots. Participation in Moodle discussions. Python on Kali with nmap.
Student Name:	Tony
Student ID:	YIT19488399

####################END####################