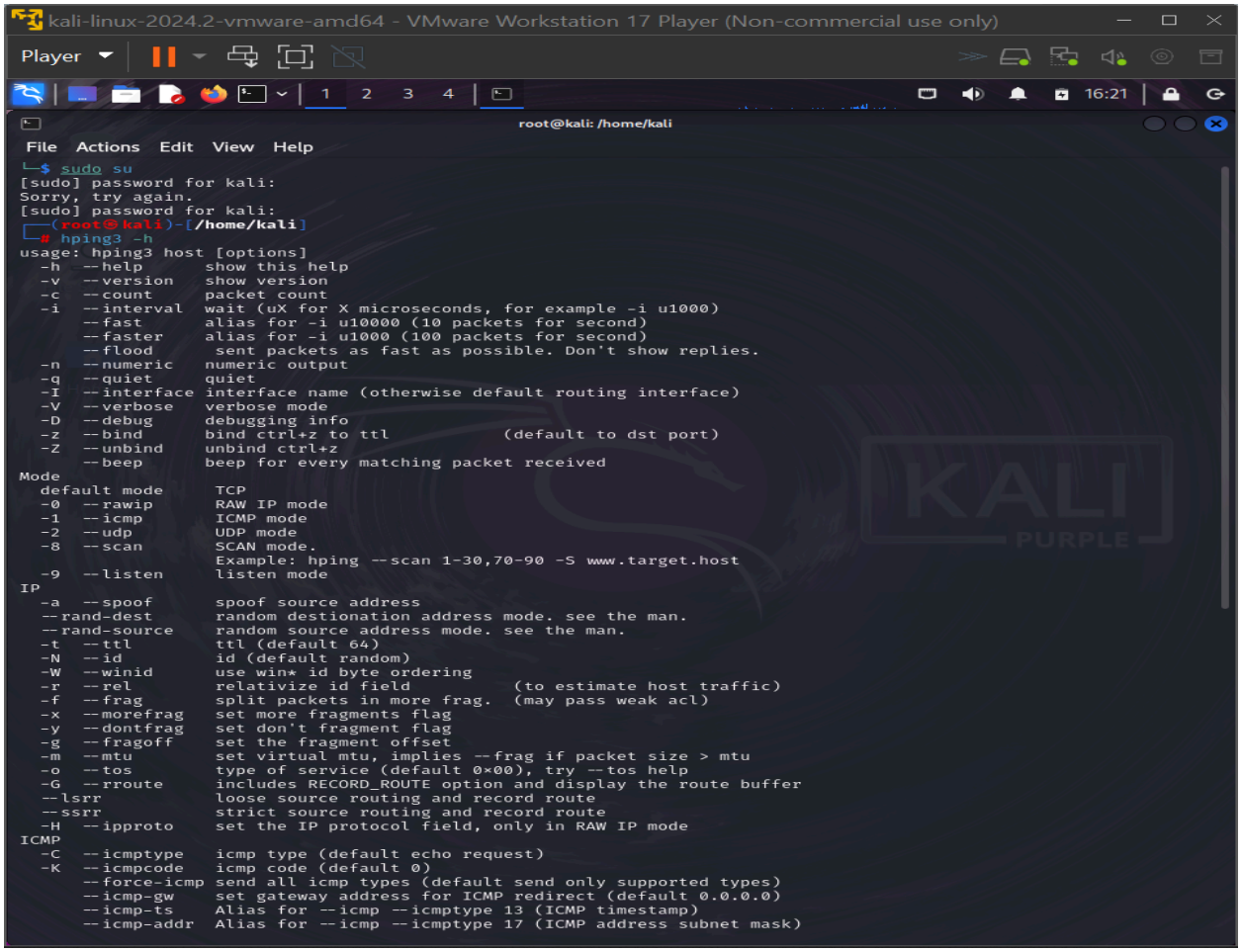
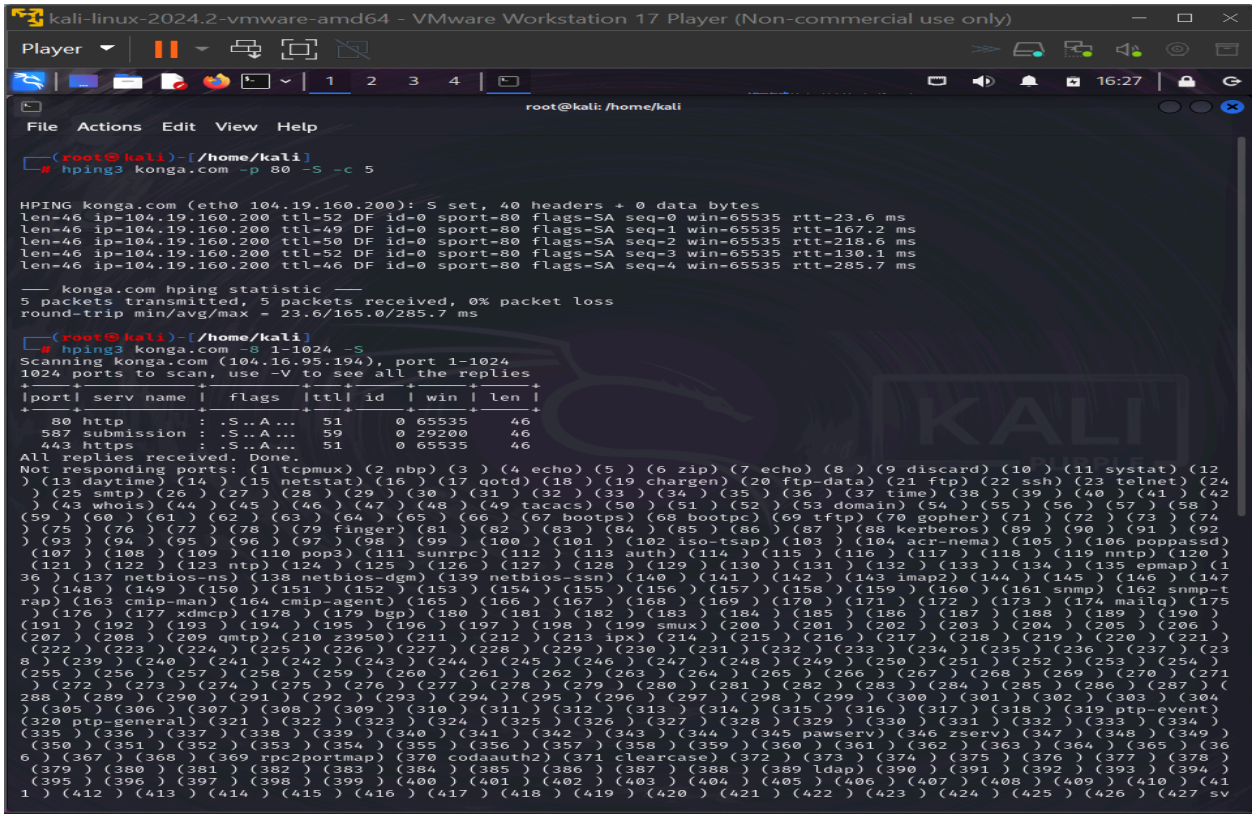
HPING FOR SECURITY AUDITING AND TESTING OF NETWORK DEVICES

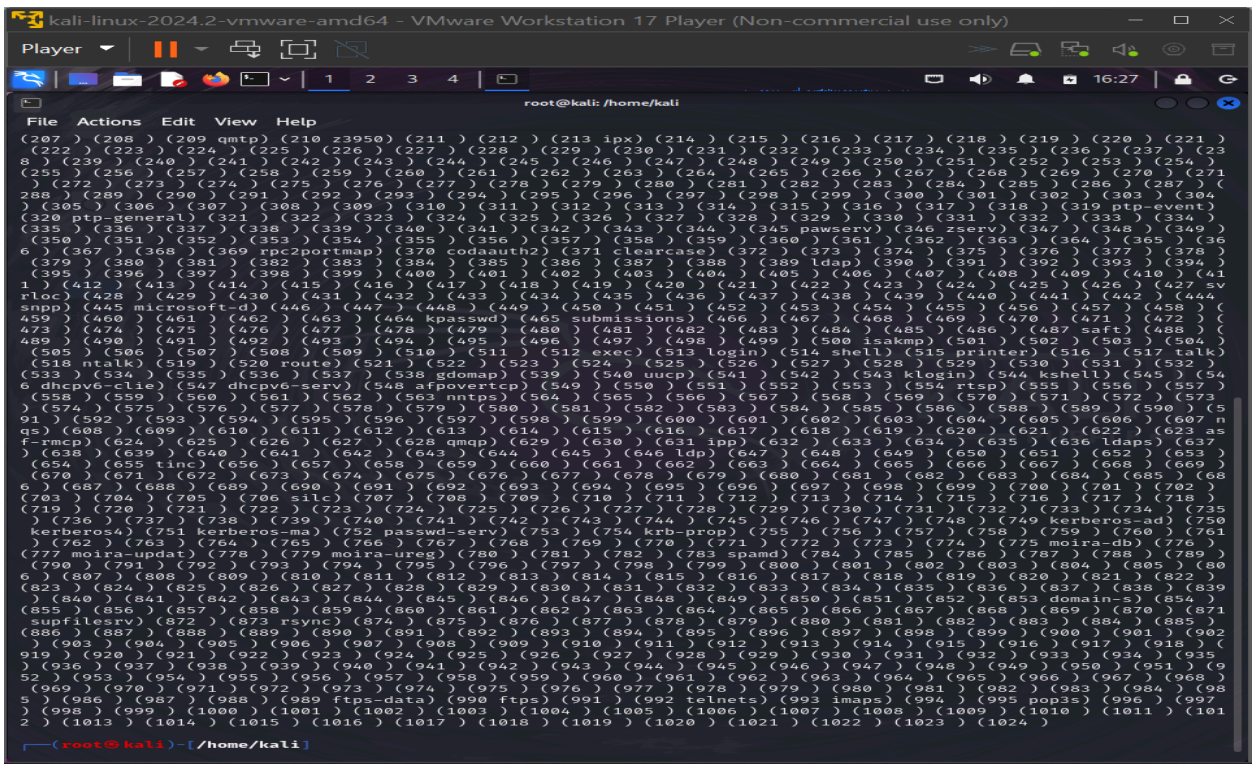
Tools : HPING3 on KALI
Site : konga.com, google.com, scanme.nmap.org

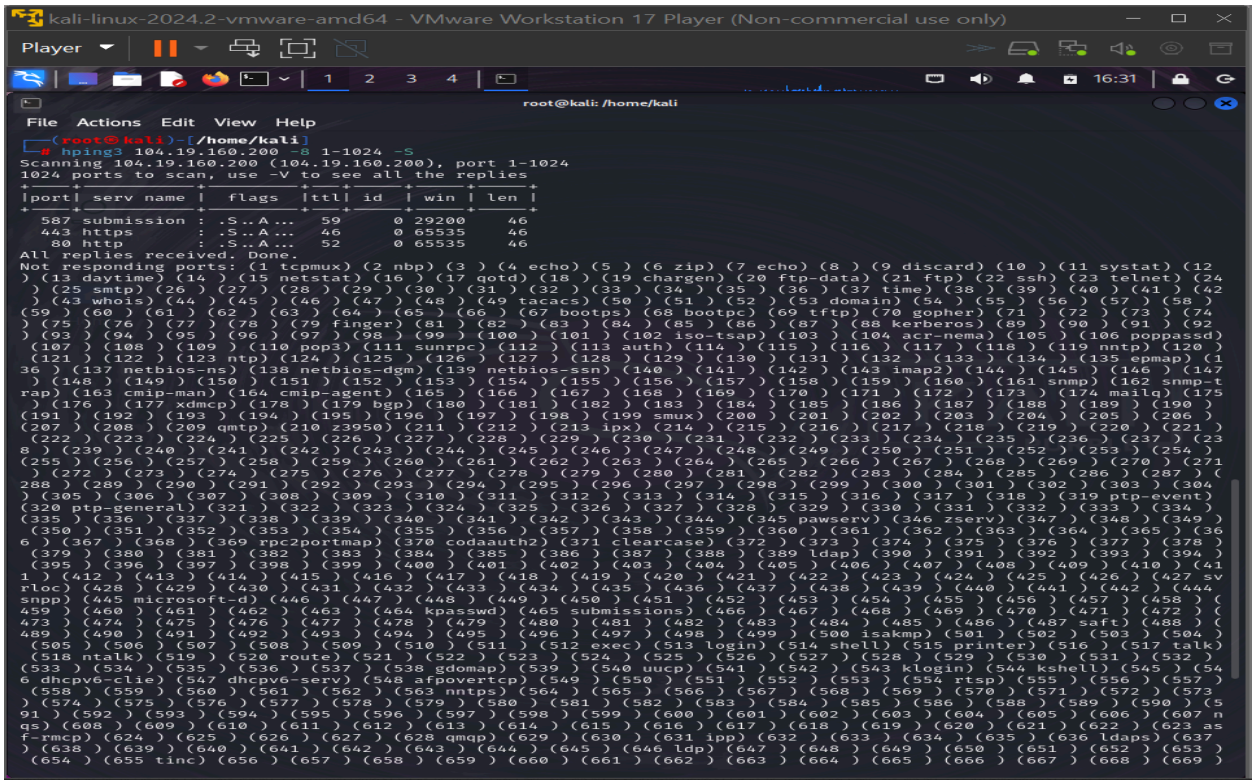
`hping3` is a versatile command-line tool primarily used for network security and testing. It allows you to send customized packets to a target machine and is often used for tasks like network diagnostics, firewall testing, and penetration testing.

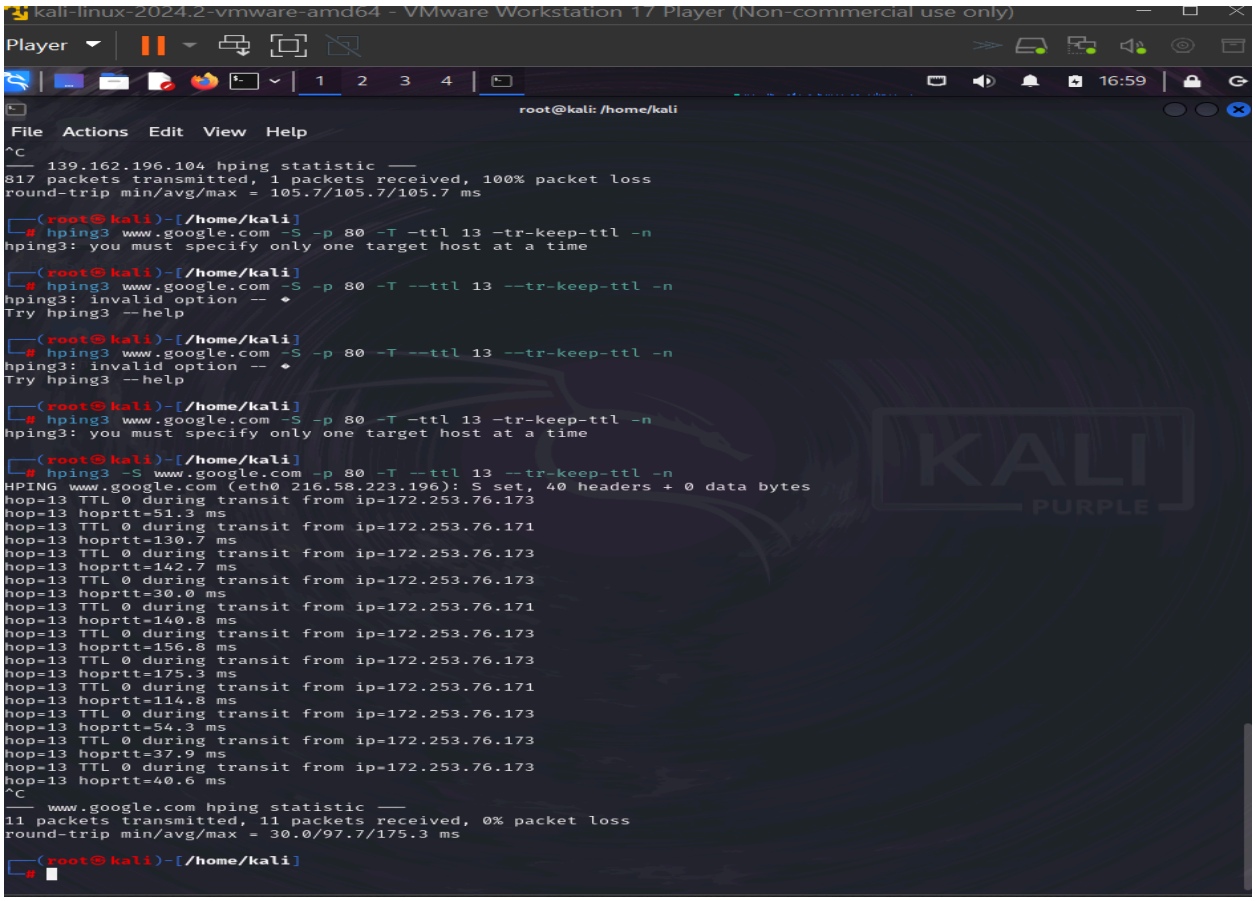
Input from hping3:

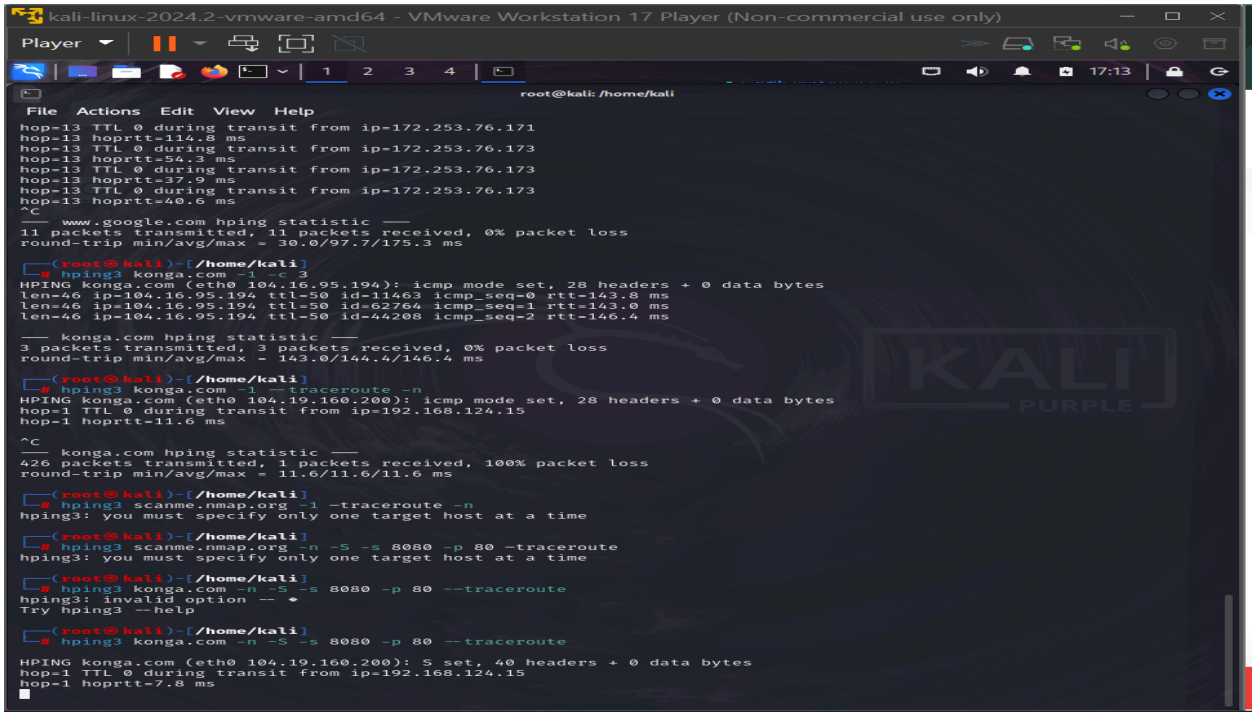


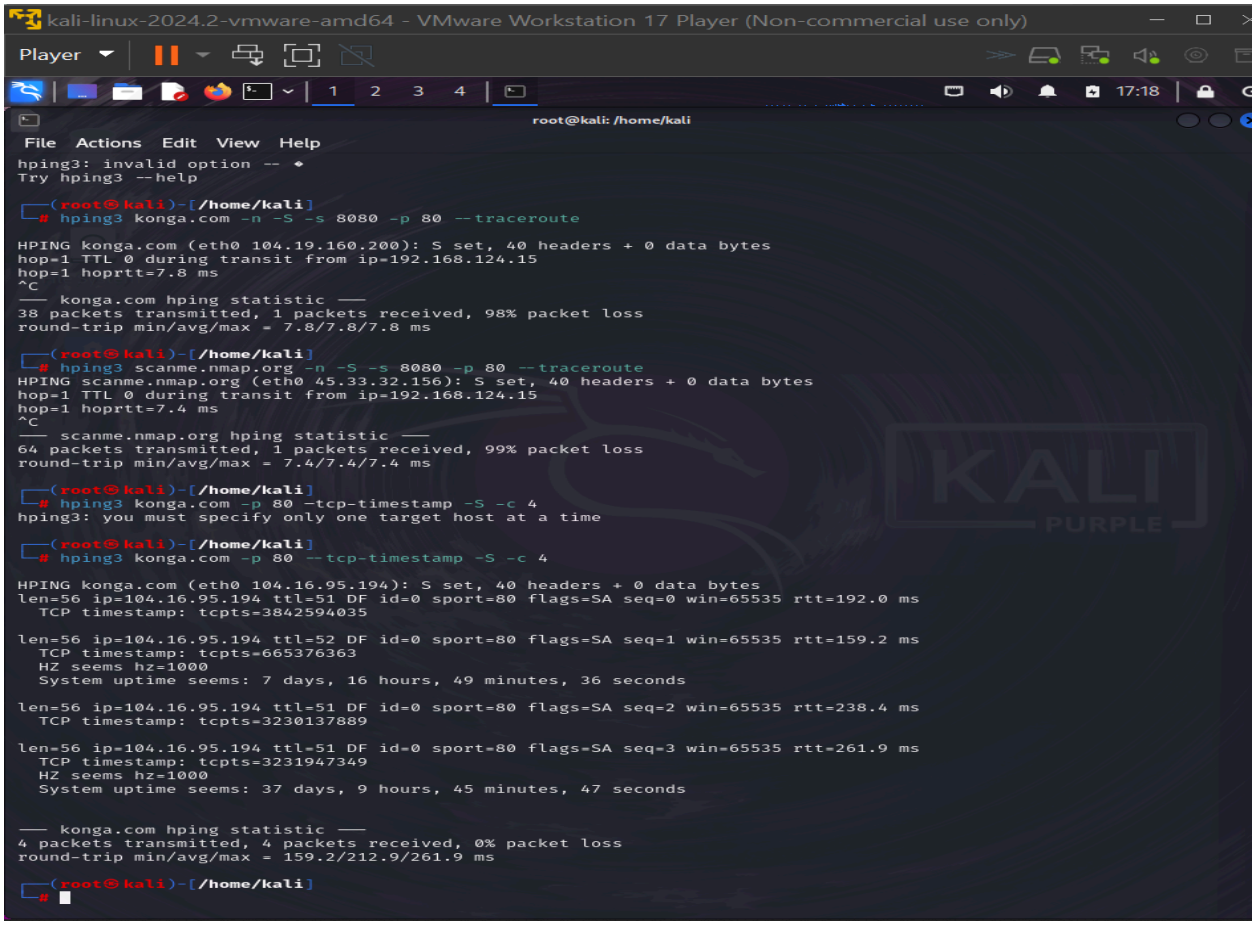

kali-linux-2024.2-vmware-amd64 - VMware Workstation 17 Player (Non-commercial use only)
Player
16:27
root@kali: /home/kali
File Actions Edit View Help
┌──(root㉿kali)-[/home/kali]
└─# hping3 konga.com -p 80 -S -c 5
HPING konga.com (eth0 104.19.160.200): S set, 40 headers + 0 data bytes
len=46 ip=104.19.160.200 ttl=52 DF id=0 sport=80 flags=SA seq=0 win=65535 rtt=23.6 ms
len=46 ip=104.19.160.200 ttl=49 DF id=0 sport=80 flags=SA seq=1 win=65535 rtt=167.2 ms
len=46 ip=104.19.160.200 ttl=50 DF id=0 sport=80 flags=SA seq=2 win=65535 rtt=218.6 ms
len=46 ip=104.19.160.200 ttl=52 DF id=0 sport=80 flags=SA seq=3 win=65535 rtt=130.1 ms
len=46 ip=104.19.160.200 ttl=46 DF id=0 sport=80 flags=SA seq=4 win=65535 rtt=285.7 ms
--- konga.com hping statistic ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 23.6/165.0/285.7 ms
┌──(root㉿kali)-[/home/kali]
└─# hping3 konga.com -8 1-1024 -S
Scanning konga.com (104.16.95.194), port 1-1024
1024 ports to scan, use -V to see all the replies
+----+----------+---------+---+-----+-----+----+
|port| serv name | flags |ttl| id | win | len |
+----+----------+---------+---+-----+-----+----+
80 http : .S..A... 51 0 65535 46
587 submission : .S..A... 59 0 29200 46
443 https : .S..A... 51 0 65535 46
All replies received. Done.
Not responding ports: (1 tcpmux) (2 nbp) (3) (4 echo) (5) (6 zip) (7 echo) (8) (9 discard) (10) (11 systat) (12) (13 daytime) (14) (15 netstat) (16) (17 qotd) (18) (19 chargen) (20 ftp-data) (21 ftp) (22 ssh) (23 telnet) (24) (25 smtp) (26) (27) (28) (29) (30) (31) (32) (33) (34) (35) (36) (37 time) (38) (39) (40) (41) (42) (43 whois) (44) (45) (46) (47) (48) (49 tacacs) (50) (51) (52) (53 domain) (54) (55) (56) (57) (58) (59) (60) (61) (62) (63) (64) (65) (66) (67 bootps) (68 bootpc) (69 tftp) (70 gopher) (71) (72) (73) (74) (75) (76) (77) (78) (79 finger) (81) (82) (83) (84) (85) (86) (87) (88 kerberos) (89) (90) (91) (92) (93) (94) (95) (96) (97) (98) (99) (100) (101) (102 iso-tsap) (103) (104 acr-nema) (105) (106 poppassd) (107) (108) (109) (110 pop3) (111 sunrpc) (112) (113 auth) (114) (115) (116) (117) (118) (119 nntp) (120) (121) (122) (123 ntp) (124) (125) (126) (127) (128) (129) (130) (131) (132) (133) (134) (135 epmap) (136) (137 netbios-ns) (138 netbios-dgm) (139 netbios-ssn) (140) (141) (142) (143 imap2) (144) (145) (146) (147) (148) (149) (150) (151) (152) (153) (154) (155) (156) (157) (158) (159) (160) (161 snmp) (162 snmp-trap) (163 cmip-man) (164 cmip-agent) (165) (166) (167) (168) (169) (170) (171) (172) (173) (174 mailq) (175) (176) (177 xdmcp) (178) (179 bgp) (180) (181) (182) (183) (184) (185) (186) (187) (188) (189) (190) (191) (192) (193) (194) (195) (196) (197) (198) (199 smux) (200) (201) (202) (203) (204) (205) (206) (207) (208) (209 qmtp) (210 z3950) (211) (212) (213 ipx) (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 ptp-event) (320 ptp-general) (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 pawserv) (346 zserv) (347) (348) (349) (350) (351) (352) (353) (354) (355) (356) (357) (358) (359) (360) (361) (362) (363) (364) (365) (366) (367) (368) (369 rpc2portmap) (370 codaauth2) (371 clearcase) (372) (373) (374) (375) (376) (377) (378) (379) (380) (381) (382) (383) (384) (385) (386) (387) (388) (389 ldap) (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 svrloc) (428) (429) (430) (431) (432) (433) (434) (435) (436) (437) (438) (439) (440) (441) (442) (443 snpp) (445 microsoft-d) (446) (447) (448) (449) (450) (451) (452) (453) (454) (455) (456) (457) (458) (459) (460) (461) (462) (463) (464 kpasswd) (465 submissions) (466) (467) (468) (469) (470) (471) (472) (473) (474) (475) (476) (477) (478) (479) (480) (481) (482) (483) (484) (485) (486) (487 saft) (488) (489) (490) (491) (492) (493) (494) (495) (496) (497) (498) (499) (500 isakmp) (501) (502) (503) (504) (505) (506) (507) (508) (509) (510) (511) (512 exec) (513 login) (514 shell) (515 printer) (516) (517 talk) (518 ntalk) (519) (520 route) (521) (522) (523) (524) (525) (526) (527) (528) (529) (530) (531) (532) (533) (534) (535) (536) (537) (538 gdomap) (539) (540 uucp) (541) (542) (543 klogin) (544 kshell) (545) (546 dhcpv6-clie) (547 dhcpv6-serv) (548 afpovertcp) (549) (550) (551) (552) (553) (554 rtsp) (555) (556) (557) (558) (559) (560) (561) (562) (563 nntps) (564) (565) (566) (567) (568) (569) (570) (571) (572) (573) (574) (575) (576) (577) (578) (579) (580) (581) (582) (583) (584) (585) (586) (588) (589) (590) (591) (592) (593) (594) (595) (596) (597) (598) (599) (600) (601) (602) (603) (604) (605) (606) (607 nqs) (608) (609) (610) (611) (612) (613) (614) (615) (616) (617) (618) (619) (620) (621) (622) (623 asf-rmcp) (624) (625) (626) (627) (628 qmqp) (629) (630) (631 ipp) (632) (633) (634) (635) (636 ldaps) (637) (638) (639) (640) (641) (642) (643) (644) (645) (646 ldp) (647) (648) (649) (650) (651) (652) (653) (654) (655 tinc) (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 silc) (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 kerberos-adm) (750 kerberos4) (751 kerberos-ma) (752 passwd-serv) (753) (754 krb-prop) (755) (756) (757) (758) (759) (760) (761) (762) (763) (764) (765) (766) (767) (768) (769) (770) (771) (772) (773) (774) (775 moira-db) (776) (777 moira-updat) (778) (779 moira-ureg) (780) (781) (782) (783 spamd) (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 domain-s) (854) (855) (856) (857) (858) (859) (860) (861) (862) (863) (864) (865) (866) (867) (868) (869) (870) (871 supfilesrv) (872) (873 rsync) (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 ftps-data) (990 ftps) (991) (992 telnets) (993 imaps) (994) (995 pop3s) (996) (997) (998) (999) (1000) (1001) (1002) (1003) (1004) (1005) (1006) (1007) (1008) (1009) (1010) (1011) (1012) (1013) (1014) (1015) (1016) (1017) (1018) (1019) (1020) (1021) (1022) (1023) (1024)
┌──(root㉿kali)-[/home/kali]

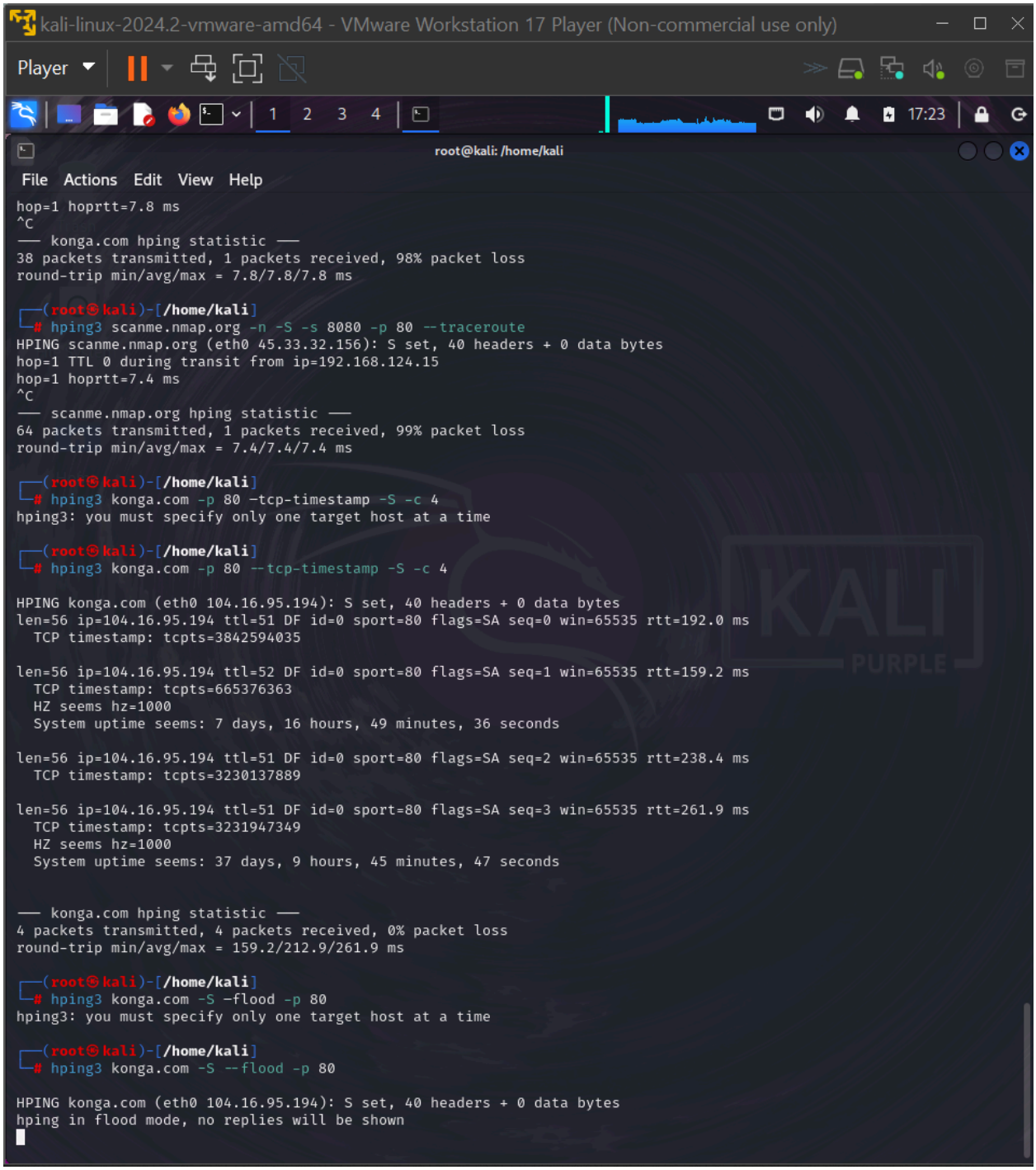

kali-linux-2024.2-vmware-amd64 - VMware Workstation 17 Player (Non-commercial use only)
Player
16:27
root@kali: /home/kali
File Actions Edit View Help
(207) (208) (209 qmtp) (210 z3950) (211) (212) (213 ipx) (214) (215) (216) (217) (218) (219) (220) (221) (222) (223) (224) (225) (226) (227) (228) (229) (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 ptp-event) (320 ptp-general) (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 pawserv) (346 zserv) (347) (348) (349) (350) (351) (352) (353) (354) (355) (356) (357) (358) (359) (360) (361) (362) (363) (364) (365) (366) (367) (368) (369 rpc2portmap) (370 codaauth2) (371 clearcase) (372) (373) (374) (375) (376) (377) (378) (379) (380) (381) (382) (383) (384) (385) (386) (387) (388) (389 ldap) (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 svrloc) (428) (429) (430) (431) (432) (433) (434) (435) (436) (437) (438) (439) (440) (441) (442) (443 snpp) (445 microsoft-d) (446) (447) (448) (449) (450) (451) (452) (453) (454) (455) (456) (457) (458) (459) (460) (461) (462) (463) (464 kpasswd) (465 submissions) (466) (467) (468) (469) (470) (471) (472) (473) (474) (475) (476) (477) (478) (479) (480) (481) (482) (483) (484) (485) (486) (487 saft) (488) (489) (490) (491) (492) (493) (494) (495) (496) (497) (498) (499) (500 isakmp) (501) (502) (503) (504) (505) (506) (507) (508) (509) (510) (511) (512 exec) (513 login) (514 shell) (515 printer) (516) (517 talk) (518 ntalk) (519) (520 route) (521) (522) (523) (524) (525) (526) (527) (528) (529) (530) (531) (532) (533) (534) (535) (536) (537) (538 gdomap) (539) (540 uucp) (541) (542) (543 klogin) (544 kshell) (545) (546 dhcpv6-clie) (547 dhcpv6-serv) (548 afpovertcp) (549) (550) (551) (552) (553) (554 rtsp) (555) (556) (557) (558) (559) (560) (561) (562) (563 nntps) (564) (565) (566) (567) (568) (569) (570) (571) (572) (573) (574) (575) (576) (577) (578) (579) (580) (581) (582) (583) (584) (585) (586) (588) (589) (590) (591) (592) (593) (594) (595) (596) (597) (598) (599) (600) (601) (602) (603) (604) (605) (606) (607 nqs) (608) (609) (610) (611) (612) (613) (614) (615) (616) (617) (618) (619) (620) (621) (622) (623 asf-rmcp) (624) (625) (626) (627) (628 qmqp) (629) (630) (631 ipp) (632) (633) (634) (635) (636 ldaps) (637) (638) (639) (640) (641) (642) (643) (644) (645) (646 ldp) (647) (648) (649) (650) (651) (652) (653) (654) (655 tinc) (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 silc) (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 kerberos-adm) (750 kerberos4) (751 kerberos-ma) (752 passwd-serv) (753) (754 krb-prop) (755) (756) (757) (758) (759) (760) (761) (762) (763) (764) (765) (766) (767) (768) (769) (770) (771) (772) (773) (774) (775 moira-db) (776) (777 moira-updat) (778) (779 moira-ureg) (780) (781) (782) (783 spamd) (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 domain-s) (854) (855) (856) (857) (858) (859) (860) (861) (862) (863) (864) (865) (866) (867) (868) (869) (870) (871 supfilesrv) (872) (873 rsync) (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 ftps-data) (990 ftps) (991) (992 telnets) (993 imaps) (994) (995 pop3s) (996) (997) (998) (999) (1000) (1001) (1002) (1003) (1004) (1005) (1006) (1007) (1008) (1009) (1010) (1011) (1012) (1013) (1014) (1015) (1016) (1017) (1018) (1019) (1020) (1021) (1022) (1023) (1024)
┌──(root㉿kali)-[/home/kali]


kali-linux-2024.2-vmware-amd64 - VMware Workstation 17 Player (Non-commercial use only)
Player
16:31
root@kali: /home/kali
File Actions Edit View Help
┌──(root㉿kali)-[/home/kali]
└─# hping3 104.19.160.200 -8 1-1024 -S
Scanning 104.19.160.200 (104.19.160.200), port 1-1024
1024 ports to scan, use -V to see all the replies
+----+------------+-------+---+-----+-----+-----+
|port| serv name | flags |ttl| id | win | len |
+----+------------+-------+---+-----+-----+-----+
  587 submission : .S..A ... 59   0 29200   46
  443 https   : .S..A ... 46   0 65535   46
   80 http   : .S..A ... 52   0 65535   46
All replies received. Done.
Not responding ports: (1 tcpmux) (2 nbp) (3) (4 echo) (5) (6 zip) (7 echo) (8) (9 discard) (10) (11 systat) (12) (13 daytime) (14) (15 netstat) (16) (17 qotd) (18) (19 chargen) (20 ftp-data) (21 ftp) (22 ssh) (23 telnet) (24) (25 smtp) (26) (27) (28) (29) (30) (31) (32) (33) (34) (35) (36) (37 time) (38) (39) (40) (41) (42) (43 whois) (44) (45) (46) (47) (48) (49 tacacs) (50) (51) (52) (53 domain) (54) (55) (56) (57) (58) (59) (60) (61) (62) (63) (64) (65) (66) (67 bootps) (68 bootpc) (69 tftp) (70 gopher) (71) (72) (73) (74) (75) (76) (77) (78) (79 finger) (81) (82) (83) (84) (85) (86) (87) (88 kerberos) (89) (90) (91) (92) (93) (94) (95) (96) (97) (98) (99) (100) (101) (102 iso-tsap) (103) (104 acr-nema) (105) (106 poppassd) (107) (108) (109) (110 pop3) (111 sunrpc) (112) (113 auth) (114) (115) (116) (117) (118) (119 nntp) (120) (121) (122) (123 ntp) (124) (125) (126) (127) (128) (129) (130) (131) (132) (133) (134) (135 epmap) (136) (137 netbios-ns) (138 netbios-dgm) (139 netbios-ssn) (140) (141) (142) (143 imap2) (144) (145) (146) (147) (148) (149) (150) (151) (152) (153) (154) (155) (156) (157) (158) (159) (160) (161 snmp) (162 snmp-trap) (163 cmip-man) (164 cmip-agent) (165) (166) (167) (168) (169) (170) (171) (172) (173) (174 mailq) (175) (176) (177 xdmcp) (178) (179 bgp) (180) (181) (182) (183) (184) (185) (186) (187) (188) (189) (190) (191) (192) (193) (194) (195) (196) (197) (198) (199 smux) (200) (201) (202) (203) (204) (205) (206) (207) (208) (209 qmtp) (210 z3950) (211) (212) (213 ipx) (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 ptp-event) (320 ptp-general) (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 pawserv) (346 zserv) (347) (348) (349) (350) (351) (352) (353) (354) (355) (356) (357) (358) (359) (360) (361) (362) (363) (364) (365) (366) (367) (368) (369 rpc2portmap) (370 codaauth2) (371 clearcase) (372) (373) (374) (375) (376) (377) (378) (379) (380) (381) (382) (383) (384) (385) (386) (387) (388) (389 ldap) (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 svrloc) (428) (429) (430) (431) (432) (433) (434) (435) (436) (437) (438) (439) (440) (441) (442) (443 snpp) (445 microsoft-d) (446) (447) (448) (449) (450) (451) (452) (453) (454) (455) (456) (457) (458) (459) (460) (461) (462) (463) (464 kpasswd) (465 submissions) (466) (467) (468) (469) (470) (471) (472) (473) (474) (475) (476) (477) (478) (479) (480) (481) (482) (483) (484) (485) (486) (487 saft) (488) (489) (490) (491) (492) (493) (494) (495) (496) (497) (498) (499) (500 isakmp) (501) (502) (503) (504) (505) (506) (507) (508) (509) (510) (511) (512 exec) (513 login) (514 shell) (515 printer) (516) (517 talk) (518 ntalk) (519) (520 route) (521) (522) (523) (524) (525) (526) (527) (528) (529) (530) (531) (532) (533) (534) (535) (536) (537) (538 gdomap) (539) (540 uucp) (541) (542) (543 klogin) (544 kshell) (545) (546 dhcpv6-clie) (547 dhcpv6-serv) (548 afpovertcp) (549) (550) (551) (552) (553) (554 rtsp) (555) (556) (557) (558) (559) (560) (561) (562) (563 nntps) (564) (565) (566) (567) (568) (569) (570) (571) (572) (573) (574) (575) (576) (577) (578) (579) (580) (581) (582) (583) (584) (585) (586) (588) (589) (590) (591) (592) (593) (594) (595) (596) (597) (598) (599) (600) (601) (602) (603) (604) (605) (606) (607 nqs) (608) (609) (610) (611) (612) (613) (614) (615) (616) (617) (618) (619) (620) (621) (622) (623 asf-rmcp) (624) (625) (626) (627) (628 qmqp) (629) (630) (631 ipp) (632) (633) (634) (635) (636 ldaps) (637) (638) (639) (640) (641) (642) (643) (644) (645) (646 ldp) (647) (648) (649) (650) (651) (652) (653) (654) (655 tinc) (656) (657) (658) (659) (660) (661) (662) (663) (664) (665) (666) (667) (668) (669)


kali-linux-2024.2-vmware-amd64 - VMware Workstation 17 Player (Non-commercial use only)
Player
16:59
root@kali: /home/kali
File Actions Edit View Help
^C
--- 139.162.196.104 hping statistic ---
817 packets transmitted, 1 packets received, 100% packet loss
round-trip min/avg/max = 105.7/105.7/105.7 ms
┌──(root㉿kali)-[/home/kali]
└─# hping3 www.google.com -S -p 80 -T -ttl 13 -tr-keep-ttl -n
hping3: you must specify only one target host at a time
┌──(root㉿kali)-[/home/kali]
└─# hping3 www.google.com -S -p 80 -T --ttl 13 --tr-keep-ttl -n
hping3: invalid option -- -
Try hping3 --help
┌──(root㉿kali)-[/home/kali]
└─# hping3 www.google.com -S -p 80 -T --ttl 13 --tr-keep-ttl -n
hping3: invalid option -- -
Try hping3 --help
┌──(root㉿kali)-[/home/kali]
└─# hping3 www.google.com -S -p 80 -T -ttl 13 -tr-keep-ttl -n
hping3: you must specify only one target host at a time
┌──(root㉿kali)-[/home/kali]
└─# hping3 -S www.google.com -p 80 -T --ttl 13 --tr-keep-ttl -n
HPING www.google.com (eth0 216.58.223.196): S set, 40 headers + 0 data bytes
hop=13 TTL 0 during transit from ip=172.253.76.173
hop=13 hoprtt=51.3 ms
hop=13 TTL 0 during transit from ip=172.253.76.171
hop=13 hoprtt=130.7 ms
hop=13 TTL 0 during transit from ip=172.253.76.173
hop=13 hoprtt=142.7 ms
hop=13 TTL 0 during transit from ip=172.253.76.173
hop=13 hoprtt=30.0 ms
hop=13 TTL 0 during transit from ip=172.253.76.171
hop=13 hoprtt=140.8 ms
hop=13 TTL 0 during transit from ip=172.253.76.173
hop=13 hoprtt=156.8 ms
hop=13 TTL 0 during transit from ip=172.253.76.173
hop=13 hoprtt=175.3 ms
hop=13 TTL 0 during transit from ip=172.253.76.171
hop=13 hoprtt=114.8 ms
hop=13 TTL 0 during transit from ip=172.253.76.173
hop=13 hoprtt=54.3 ms
hop=13 TTL 0 during transit from ip=172.253.76.173
hop=13 hoprtt=37.9 ms
hop=13 TTL 0 during transit from ip=172.253.76.173
hop=13 hoprtt=40.6 ms
^C
--- www.google.com hping statistic ---
11 packets transmitted, 11 packets received, 0% packet loss
round-trip min/avg/max = 30.0/97.7/175.3 ms
┌──(root㉿kali)-[/home/kali]
└─#


kali-linux-2024.2-vmware-amd64 - VMware Workstation 17 Player (Non-commercial use only)
Player
17:13
root@kali: /home/kali
File Actions Edit View Help
hop=13 TTL 0 during transit from ip=172.253.76.171
hop=13 hoprtt=114.8 ms
hop=13 TTL 0 during transit from ip=172.253.76.173
hop=13 hoprtt=54.3 ms
hop=13 TTL 0 during transit from ip=172.253.76.173
hop=13 hoprtt=37.9 ms
hop=13 TTL 0 during transit from ip=172.253.76.173
hop=13 hoprtt=40.6 ms
^C
--- www.google.com hping statistic ---
11 packets transmitted, 11 packets received, 0% packet loss
round-trip min/avg/max = 30.0/97.7/175.3 ms
┌──(root㉿kali)-[/home/kali]
└─# hping3 konga.com -1 -c 3
HPING konga.com (eth0 104.16.95.194): icmp mode set, 28 headers + 0 data bytes
len=46 ip=104.16.95.194 ttl=50 id=11463 icmp_seq=0 rtt=143.8 ms
len=46 ip=104.16.95.194 ttl=50 id=62764 icmp_seq=1 rtt=143.0 ms
len=46 ip=104.16.95.194 ttl=50 id=44208 icmp_seq=2 rtt=146.4 ms
--- konga.com hping statistic ---
3 packets transmitted, 3 packets received, 0% packet loss
round-trip min/avg/max = 143.0/144.4/146.4 ms
┌──(root㉿kali)-[/home/kali]
└─# hping3 konga.com -1 --traceroute -n
HPING konga.com (eth0 104.19.160.200): icmp mode set, 28 headers + 0 data bytes
hop=1 TTL 0 during transit from ip=192.168.124.15
hop=1 hoprtt=11.6 ms
^C
--- konga.com hping statistic ---
426 packets transmitted, 1 packets received, 100% packet loss
round-trip min/avg/max = 11.6/11.6/11.6 ms
┌──(root㉿kali)-[/home/kali]
└─# hping3 scanme.nmap.org -1 -traceroute -n
hping3: you must specify only one target host at a time
┌──(root㉿kali)-[/home/kali]
└─# hping3 scanme.nmap.org -n -S -s 8080 -p 80 -traceroute
hping3: you must specify only one target host at a time
┌──(root㉿kali)-[/home/kali]
└─# hping3 konga.com -n -S -s 8080 -p 80 --traceroute
hping3: invalid option -- -
Try hping3 --help
┌──(root㉿kali)-[/home/kali]
└─# hping3 konga.com -n -S -s 8080 -p 80 --traceroute
HPING konga.com (eth0 104.19.160.200): S set, 40 headers + 0 data bytes
hop=1 TTL 0 during transit from ip=192.168.124.15
hop=1 hoprtt=7.8 ms


kali-linux-2024.2-vmware-amd64 - VMware Workstation 17 Player (Non-commercial use only)
Player
17:18
root@kali: /home/kali
File Actions Edit View Help
hping3: invalid option -- -
Try hping3 --help
┌──(root㉿kali)-[/home/kali]
└─# hping3 konga.com -n -S -s 8080 -p 80 --traceroute
HPING konga.com (eth0 104.19.160.200): S set, 40 headers + 0 data bytes
hop=1 TTL 0 during transit from ip=192.168.124.15
hop=1 hoprtt=7.8 ms
^C
--- konga.com hping statistic ---
38 packets transmitted, 1 packets received, 98% packet loss
round-trip min/avg/max = 7.8/7.8/7.8 ms
┌──(root㉿kali)-[/home/kali]
└─# hping3 scanme.nmap.org -n -S -s 8080 -p 80 --traceroute
HPING scanme.nmap.org (eth0 45.33.32.156): S set, 40 headers + 0 data bytes
hop=1 TTL 0 during transit from ip=192.168.124.15
hop=1 hoprtt=7.4 ms
^C
--- scanme.nmap.org hping statistic ---
64 packets transmitted, 1 packets received, 99% packet loss
round-trip min/avg/max = 7.4/7.4/7.4 ms
┌──(root㉿kali)-[/home/kali]
└─# hping3 konga.com -p 80 -tcp-timestamp -S -c 4
hping3: you must specify only one target host at a time
┌──(root㉿kali)-[/home/kali]
└─# hping3 konga.com -p 80 --tcp-timestamp -S -c 4
HPING konga.com (eth0 104.16.95.194): S set, 40 headers + 0 data bytes
len=56 ip=104.16.95.194 ttl=51 DF id=0 sport=80 flags=SA seq=0 win=65535 rtt=192.0 ms
TCP timestamp: tcpts=3842594035
len=56 ip=104.16.95.194 ttl=52 DF id=0 sport=80 flags=SA seq=1 win=65535 rtt=159.2 ms
TCP timestamp: tcpts=665376363
HZ seems hz=1000
System uptime seems: 7 days, 16 hours, 49 minutes, 36 seconds
len=56 ip=104.16.95.194 ttl=51 DF id=0 sport=80 flags=SA seq=2 win=65535 rtt=238.4 ms
TCP timestamp: tcpts=3230137889
len=56 ip=104.16.95.194 ttl=51 DF id=0 sport=80 flags=SA seq=3 win=65535 rtt=261.9 ms
TCP timestamp: tcpts=3231947349
HZ seems hz=1000
System uptime seems: 37 days, 9 hours, 45 minutes, 47 seconds
--- konga.com hping statistic ---
4 packets transmitted, 4 packets received, 0% packet loss
round-trip min/avg/max = 159.2/212.9/261.9 ms
┌──(root㉿kali)-[/home/kali]
└─#


kali-linux-2024.2-vmware-amd64 - VMware Workstation 17 Player (Non-commercial use only)
Player
1 2 3 4
17:23
root@kali: /home/kali
File Actions Edit View Help
hop=1 hoprtt=7.8 ms
^C
── konga.com hping statistic ──
38 packets transmitted, 1 packets received, 98% packet loss
round-trip min/avg/max = 7.8/7.8/7.8 ms
┌──(root㉿kali)-[/home/kali]
└─# hping3 scanme.nmap.org -n -S -s 8080 -p 80 --traceroute
HPING scanme.nmap.org (eth0 45.33.32.156): S set, 40 headers + 0 data bytes
hop=1 TTL 0 during transit from ip=192.168.124.15
hop=1 hoprtt=7.4 ms
^C
── scanme.nmap.org hping statistic ──
64 packets transmitted, 1 packets received, 99% packet loss
round-trip min/avg/max = 7.4/7.4/7.4 ms
┌──(root㉿kali)-[/home/kali]
└─# hping3 konga.com -p 80 -tcp-timestamp -S -c 4
hping3: you must specify only one target host at a time
┌──(root㉿kali)-[/home/kali]
└─# hping3 konga.com -p 80 --tcp-timestamp -S -c 4
HPING konga.com (eth0 104.16.95.194): S set, 40 headers + 0 data bytes
len=56 ip=104.16.95.194 ttl=51 DF id=0 sport=80 flags=SA seq=0 win=65535 rtt=192.0 ms
TCP timestamp: tcpts=3842594035
len=56 ip=104.16.95.194 ttl=52 DF id=0 sport=80 flags=SA seq=1 win=65535 rtt=159.2 ms
TCP timestamp: tcpts=665376363
HZ seems hz=1000
System uptime seems: 7 days, 16 hours, 49 minutes, 36 seconds
len=56 ip=104.16.95.194 ttl=51 DF id=0 sport=80 flags=SA seq=2 win=65535 rtt=238.4 ms
TCP timestamp: tcpts=3230137889
len=56 ip=104.16.95.194 ttl=51 DF id=0 sport=80 flags=SA seq=3 win=65535 rtt=261.9 ms
TCP timestamp: tcpts=3231947349
HZ seems hz=1000
System uptime seems: 37 days, 9 hours, 45 minutes, 47 seconds
── konga.com hping statistic ──
4 packets transmitted, 4 packets received, 0% packet loss
round-trip min/avg/max = 159.2/212.9/261.9 ms
┌──(root㉿kali)-[/home/kali]
└─# hping3 konga.com -S -flood -p 80
hping3: you must specify only one target host at a time
┌──(root㉿kali)-[/home/kali]
└─# hping3 konga.com -S --flood -p 80
HPING konga.com (eth0 104.16.95.194): S set, 40 headers + 0 data bytes
hping in flood mode, no replies will be shown

Here we used hping to perform security auditing and the testing of networking devices.

First we need to enter **ROOT** user using the terminal : sudo su.
for this session we need another “victim” machine to make connections through. We can use **scanme.nmap.org** as a target host on the internet. Do not scan a site without permission from the owner. Incase you have no internet connection during hping testing, you may consider installing a Kali or Ubuntu VM on your own working PC.

We will begin by viewing the help information screen by executing the following command: **hping3 -h** as we can see the result in pic 1.

The default packet which hping will create is a TCP packet. This means that even if a device such as a router or firewall is blocking ping requests, we can still perform host discovery and reconnaissance with hping. We will perform our first scan using the SYN flag. This will send out the same packets as nmap would when performing a -sS scan. We will also check if port 80 is open. “-c 5” parameter tells us that this scan will only be repeated 5 times. Type the following command: **hping3 scanme.nmap.org -p 80 -S -c 5** Note that, in my scan, the packets came back with the flags “SA” set. This indicates that the port is open. If the flag were set to “RA”, the port would be closed.

Create a SYN package and use scan mode to scan port 1 through 1000 on these targets. “-8” puts hping command to sweep-scan mode**. hping3 scanme.nmap.org -8 1-1024 -S** then **hping3 192.168.1.123 -8 1-1024 -S**

In these two examples, we scanned two different machines. As a result of both scans, the ports that are detected as open give us some information about the operating systems of the machines. We can roughly say that the first is Linux OS and the second is Windows.

If we want to perform a more detailed scan, we can scan all the ports beginning with 1. We can do this by adding the increment switch (++1) after the port switch and the port number where we want the scan to begin. **hping3 -S 139.162.196.104 -p ++1**

Nowadays, many websites which are heavily accessible use multiple servers to meet incoming requests. For example, a web request to www.google.com is handled by more than one server. In order to learn the IP addresses of these servers that are behind the DNS, type this command:**hping3 www.google.com -S -p 80 -T –ttl 13 –tr-keep-ttl -n**

In this case, we used the TTL in traceroute to obtain some of the load-balancing devices' IP addresses.
We can use hping command as an ordinary ping tool. "-1" parameter indicates that this is an ICMP package. **Hping3 scanme.nmap.org -1 -c 3**
Traceroute to a target using ICMP mode and show verbose**. Hping scanme.nmap.org -1 –traceroute -n**
Hping also improves on the traceroute ability. Traceroute uses ping to determine the location of servers, firewalls, routers etc. This can be very useful for hackers looking to create a network map of their target. For this reason, many firewalls do not respond to ping packets. Hping does the same thing but can also use TCP packets instead of ICMP, which all firewalls will allow (otherwise, it would not allow internet traffic). Let's try this now**: hping3 scanme.nmap.org -n -S -s 8080 -p 80 –traceroute** Traceroute to determine if port 80 is open, set local traffic to be generated from source port 8080.

Hping can be used to tell us how long a server has been up. This is useful information for a hacker as each time a server is patched or updated, it must also be rebooted. If we see that a server is up for 5 years, we can be sure that the server has not been patched or updated in that time, and that it therefore will be vulnerable to all vulnerabilities discovered during that time frame. We can do this using the following command: **hping3 scanme.nmap.org -p 80 –tcp-timestamp -S -c 4**

To start a SYN flood attack, run the command below. **hping3 scanme.nmap.org -S –flood -p 80** When running the commands, hping3 will not show any output; it is working in the background as seen in the last pic.