



NSE Coursework: Network attack and defence

Project Report

Authors: Ahmed Bedair, Yukesh Shrestha, Varishdan Kumariah

April 23, 2024

Contents

1	Level 1: Build a network and test its connectivity	1
1.1	Network Topology	1
1.2	Connectivity Tests	2
2	Level 2: Generate and analyse traffic on your network	3
3	Level 3: Network attacks	4
4	Level 4: Network defence	5
5	Level 5: Critical evaluation and reflection	6

Chapter 1

Level 1: Build a network and test its connectivity

1.1 Network Topology

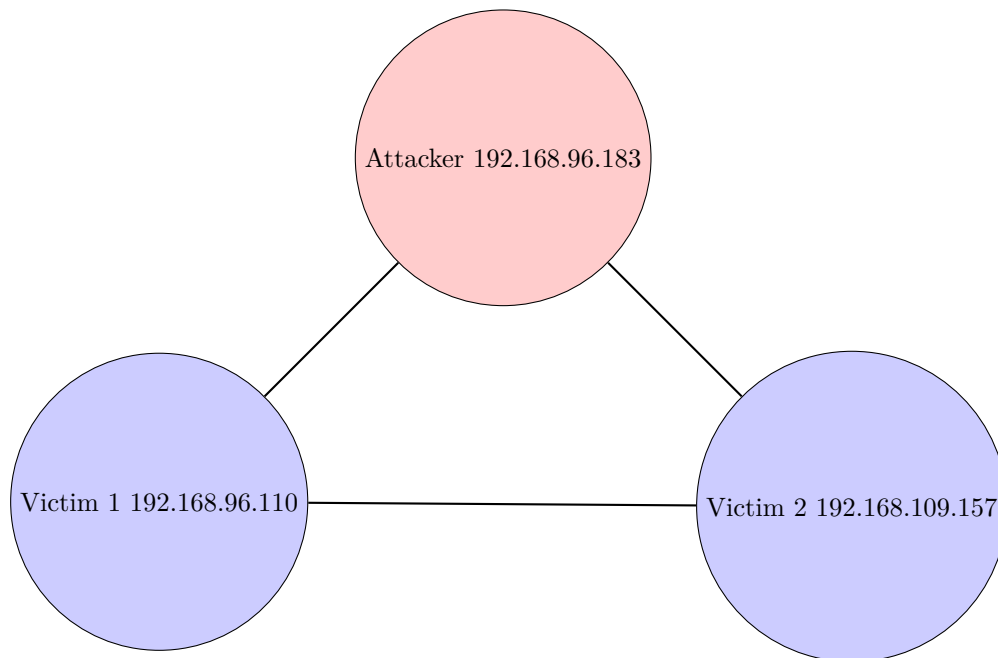
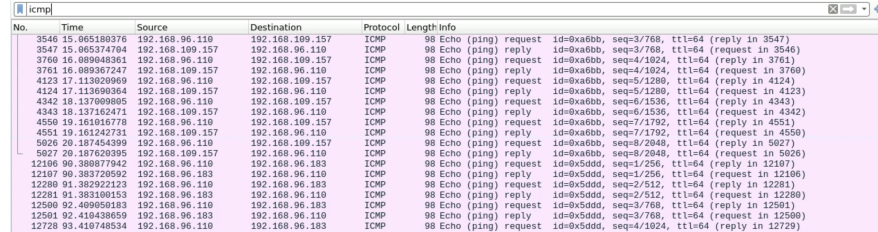


Figure 1.1: Network Topology

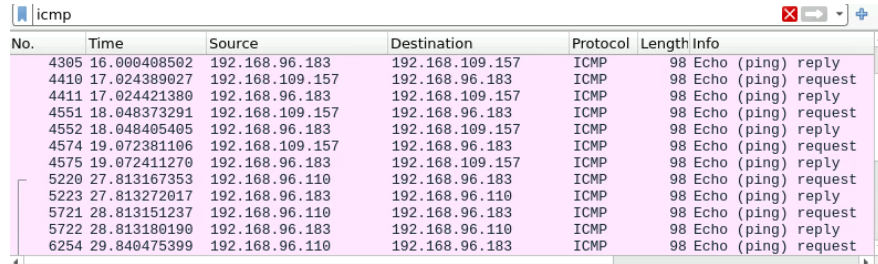
1.2 Connectivity Tests

The following screenshots demonstrate the successful ICMP ping tests between each machine, confirming that the machines are fully connected, as shown in Figure 1.1. The machines are also fully connected to the internet. We used the `iperf` tool instead of just browsing, as it reliably generates similar traffic on demand, further enhancing our ability to test the network's performance.



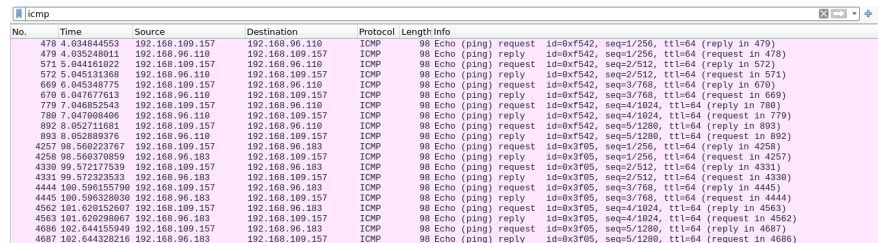
No.	Time	Source	Destination	Protocol	Length	Info
3546	15.065199376	192.168.96.110	192.168.109.157	ICMP	98	Echo (ping) request id=0xa6bb, seq=3/768, ttl=64 (reply in 3547)
3547	15.065374764	192.168.109.157	192.168.96.110	ICMP	98	Echo (ping) reply id=0xa6bb, seq=3/768, ttl=64 (request in 3546)
3760	16.009048361	192.168.96.110	192.168.109.157	ICMP	98	Echo (ping) request id=0xa6bb, seq=4/1024, ttl=64 (reply in 3761)
3761	16.009367247	192.168.109.157	192.168.96.110	ICMP	98	Echo (ping) reply id=0xa6bb, seq=4/1024, ttl=64 (request in 3760)
4123	17.113029969	192.168.96.110	192.168.109.157	ICMP	98	Echo (ping) request id=0xa6bb, seq=5/1280, ttl=64 (request in 4124)
4124	17.113690364	192.168.109.157	192.168.96.110	ICMP	98	Echo (ping) reply id=0xa6bb, seq=5/1280, ttl=64 (request in 4123)
4342	18.137099905	192.168.96.110	192.168.109.157	ICMP	98	Echo (ping) request id=0xa6bb, seq=6/1536, ttl=64 (reply in 4343)
4343	18.137162471	192.168.109.157	192.168.96.110	ICMP	98	Echo (ping) reply id=0xa6bb, seq=6/1536, ttl=64 (request in 4342)
4550	19.161016778	192.168.96.110	192.168.109.157	ICMP	98	Echo (ping) request id=0xa6bb, seq=7/1792, ttl=64 (reply in 4551)
4551	19.161242731	192.168.109.157	192.168.96.110	ICMP	98	Echo (ping) reply id=0xa6bb, seq=7/1792, ttl=64 (request in 4550)
5026	20.187454309	192.168.96.110	192.168.109.157	ICMP	98	Echo (ping) request id=0xa6bb, seq=8/2048, ttl=64 (reply in 5027)
5027	20.187620395	192.168.109.157	192.168.96.110	ICMP	98	Echo (ping) reply id=0xa6bb, seq=8/2048, ttl=64 (request in 5026)
12106	90.388877942	192.168.96.110	192.168.96.183	ICMP	98	Echo (ping) request id=0x5ddd, seq=1/256, ttl=64 (reply in 12107)
12107	90.388770502	192.168.96.183	192.168.96.110	ICMP	98	Echo (ping) reply id=0x5ddd, seq=1/256, ttl=64 (request in 12106)
12280	91.382922123	192.168.96.110	192.168.96.183	ICMP	98	Echo (ping) request id=0x5ddd, seq=2/512, ttl=64 (reply in 12281)
12281	91.383190153	192.168.96.183	192.168.96.110	ICMP	98	Echo (ping) reply id=0x5ddd, seq=2/512, ttl=64 (request in 12280)
12500	92.409050163	192.168.96.110	192.168.96.183	ICMP	98	Echo (ping) request id=0x5ddd, seq=3/768, ttl=64 (reply in 12501)
12501	92.410438659	192.168.96.183	192.168.96.110	ICMP	98	Echo (ping) reply id=0x5ddd, seq=3/768, ttl=64 (request in 12500)
12728	93.419748534	192.168.96.110	192.168.96.183	ICMP	98	Echo (ping) request id=0x5ddd, seq=4/1024, ttl=64 (reply in 12729)

Figure 1.2: Pings from Attacker to Other Machines



No.	Time	Source	Destination	Protocol	Length	Info
4305	16.000408502	192.168.96.183	192.168.109.157	ICMP	98	Echo (ping) reply
4410	17.024389027	192.168.109.157	192.168.96.183	ICMP	98	Echo (ping) request
4411	17.024421380	192.168.96.183	192.168.109.157	ICMP	98	Echo (ping) reply
4551	18.048373291	192.168.109.157	192.168.96.183	ICMP	98	Echo (ping) request
4552	18.048405405	192.168.96.183	192.168.109.157	ICMP	98	Echo (ping) reply
4574	19.072381106	192.168.109.157	192.168.96.183	ICMP	98	Echo (ping) request
4575	19.072411270	192.168.96.183	192.168.109.157	ICMP	98	Echo (ping) reply
5220	27.813167353	192.168.96.110	192.168.96.183	ICMP	98	Echo (ping) request
5223	27.813272017	192.168.96.183	192.168.96.110	ICMP	98	Echo (ping) reply
5721	28.813151237	192.168.96.110	192.168.96.183	ICMP	98	Echo (ping) request
5722	28.813180190	192.168.96.183	192.168.96.110	ICMP	98	Echo (ping) reply
6254	29.840475399	192.168.96.110	192.168.96.183	ICMP	98	Echo (ping) request

Figure 1.3: Pings from Victim 1 to Other Machines



No.	Time	Source	Destination	Protocol	Length	Info
478	4.034844553	192.168.109.157	192.168.96.110	ICMP	98	Echo (ping) request id=0xf542, seq=1/256, ttl=64 (reply in 479)
479	4.035248911	192.168.96.110	192.168.109.157	ICMP	98	Echo (ping) reply id=0xf542, seq=1/256, ttl=64 (request in 478)
571	5.044161022	192.168.109.157	192.168.96.110	ICMP	98	Echo (ping) request id=0xf542, seq=2/512, ttl=64 (reply in 572)
572	5.045131398	192.168.96.110	192.168.109.157	ICMP	98	Echo (ping) reply id=0xf542, seq=2/512, ttl=64 (request in 571)
668	6.045348775	192.168.109.157	192.168.96.110	ICMP	98	Echo (ping) request id=0xf542, seq=3/768, ttl=64 (reply in 669)
670	6.047677613	192.168.96.110	192.168.109.157	ICMP	98	Echo (ping) reply id=0xf542, seq=3/768, ttl=64 (request in 668)
779	7.040825243	192.168.109.157	192.168.96.110	ICMP	98	Echo (ping) request id=0xf542, seq=4/1024, ttl=64 (reply in 780)
780	7.047080406	192.168.96.110	192.168.109.157	ICMP	98	Echo (ping) reply id=0xf542, seq=4/1024, ttl=64 (request in 779)
892	8.052711681	192.168.109.157	192.168.96.110	ICMP	98	Echo (ping) request id=0xf542, seq=5/1280, ttl=64 (reply in 893)
893	8.052890376	192.168.96.110	192.168.109.157	ICMP	98	Echo (ping) reply id=0xf542, seq=5/1280, ttl=64 (request in 892)
4257	98.560223767	192.168.109.157	192.168.96.183	ICMP	98	Echo (ping) request id=0x3f05, seq=1/256, ttl=64 (reply in 4258)
4258	98.560370859	192.168.96.183	192.168.109.157	ICMP	98	Echo (ping) reply id=0x3f05, seq=1/256, ttl=64 (request in 4257)
4330	99.572177539	192.168.109.157	192.168.96.183	ICMP	98	Echo (ping) request id=0x3f05, seq=2/512, ttl=64 (reply in 4331)
4331	99.572323533	192.168.96.183	192.168.109.157	ICMP	98	Echo (ping) reply id=0x3f05, seq=2/512, ttl=64 (request in 4330)
4444	100.596155790	192.168.109.157	192.168.96.183	ICMP	98	Echo (ping) request id=0x3f05, seq=3/768, ttl=64 (reply in 4445)
4445	100.596320830	192.168.96.183	192.168.109.157	ICMP	98	Echo (ping) reply id=0x3f05, seq=3/768, ttl=64 (request in 4444)
4562	101.620152607	192.168.109.157	192.168.96.183	ICMP	98	Echo (ping) request id=0x3f05, seq=4/1024, ttl=64 (reply in 4563)
4563	101.620290867	192.168.96.183	192.168.109.157	ICMP	98	Echo (ping) reply id=0x3f05, seq=4/1024, ttl=64 (request in 4562)
4686	102.644155040	192.168.109.157	192.168.96.183	ICMP	98	Echo (ping) request id=0x3f05, seq=5/1280, ttl=64 (reply in 4687)
4687	102.644328216	192.168.96.183	192.168.109.157	ICMP	98	Echo (ping) reply id=0x3f05, seq=5/1280, ttl=64 (request in 4686)

Figure 1.4: Pings from Victim 2 to Other Machines

Chapter 2

Level 2: Generate and analyse traffic on your network

Chapter 3

Level 3: Network attacks

Chapter 4

Level 4: Network defence

Chapter 5

Level 5: Critical evaluation and reflection