Network Security for ARM based IoT Devices

A Seminar Report

Submitted to the yeshwantrao chavan college of engineering

in partial fulfillment of requirements for the award of degree

Bachelor of Technology

in

Computer Science and Engineering(Artificial Intelligence and Machine Learning

by

Arnab Chakraborty

21070140

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

YESHWANTRAO CHAVAN COLLEGE OF ENGINEERING

NAGPUR, MAHARASHTRA

October 2023

Abstract

The proliferation of Internet of Things (IoT) devices, largely powered by ARM(Advanced Reduced Instruction Set Computing Machines) architecture, has revolutionized connectivity and automation across various domains. However, this technological advancement has brought forth unprecedented challenges in ensuring robust network security within these devices. This research paper investigates the critical role of network security in ARM-based IoT devices, addressing the vulnerabilities, threats, and the evolving landscape of security protocols and defenses.

The paper provides an extensive overview of ARM architecture's prevalence in IoT devices and delves into the unique security concerns surrounding these systems. It explores the inherent vulnerabilities in ARM processors, emphasizing the significance of secure design principles, firmware integrity, and protection against sophisticated cyber threats. Furthermore, the study examines the impact of network security breaches on IoT devices, including data privacy risks, potential exploitation by malicious actors, and the broader implications for user safety and system reliability. This paper also aims to explore the possible measures that can be implemented to secure a shared network between IoT devices and methodologies to resist a network attack on ARM devices.

Contents

Abstract **i**

List of Figures **iv**

List of Tables **v**

1 Introduction **1**

1.1 Problems 1

1.1.1 Confidential Data 1

1.1.2 Botnet Formation 2

1.1.3 Privacy Breach 2

1.1.4 Fatal Implications 2

1.2 Prevention Methodology 3

1.2.1 DNS Sinkholes 3

1.2.2 Virtual Private Network 3

2 Literature Review **4**

2.0.1 Autonomous NAT Traversal - A. Muller, N. Evans, C. Grothoff, S. Kamkar — Year: 2010 — Conference Paper — Publisher: IEEE 4

2.0.2 Evaluating the Vulnerability of Network Traffic Using Joint Security and Routing Analysis - Patrick Tague, David Slater, Jason Rogers, Radha Poovendra 4

2.0.3 DNS Amplification and DNS Tunneling Attacks Simulation, Detection and Mitigation Approaches - Sanjay, Balaji Rajendra, Pushparaj Shetty D — Year: 2020 — Conference Paper — Publisher: IEEE 5

2.0.4 Experimental performance comparison between TCP vs UDP tunnel using OpenVPN - Irfaan Coonjah, Pierre Clarel Catherine, K.M.S Soyjaudah — Year: 2015 — Conference Paper — Publisher: IEEE 5

2.0.5 Internet of Things Security - Multilayered Method For End to End Data Communications - Craig Lee, Andrea Fumagalli — Year: 2019 — Conference Paper — Publisher: IEEE 6

2.0.6 IEE Colloquium on 'RISC Architectures and Applications' (Digest No.163) — Year: 1991 — Conference Paper — Publisher: IET 6

3 Implementation 7

3.1 Tools 7

3.2 Description 7

4 Results 10

4.0.1 Testing Results 10

5 Conclusion 15

References 16

List of Figures

3.1 VPN Classification 8
3.2 TCP vs UDP 9
3.3 DNS Sinkhole 9

4.1 tcpdump Output without defenses 11
4.2 iftop Output without defenses 12
4.3 TCP vs. UDP 12
4.4 tcpdump Output with defenses 13
4.5 iftop Output with defenses 14

List of Tables

3.1 Tools Used 7

Chapter 1

Introduction

As the Internet of Things (IoT) continues to grow, ARM-based devices have become integral components of the connected ecosystem, serving diverse applications ranging from smart homes to industrial automation. However, this proliferation of ARM devices has also exposed a widening attack surface, making network security a paramount concern. Cybercriminals can compromise a large number of IoT devices and create botnets. These botnets can be used to launch distributed denial of service (DDoS) attacks, overwhelm online services, and disrupt the internet. Smart Home devices like assistants, cameras, appliances, etc. often collect sensitive data, such as audio and video feeds, and user preferences. Unauthorized access to this data can lead to privacy breaches. Some IoT devices, like connected cars or medical devices, have physical safety implications. If these devices are compromised, they can endanger lives and property.

1.1 Problems

1.1.1 Confidential Data

Hackers have the power to launch assaults and enter thousands or millions of unprotected connected devices, destroying infrastructure, taking down networks, or accessing confidential data.

1.1.2 Botnet Formation

Cybercriminals can compromise a large number of IoT devices and create botnets. These botnets can be used to launch distributed denial of service (DDoS) attacks, overwhelm online services, and disrupt the internet. One of the worst DDoS attack was executed with thee use of the Mirai Botnet. After becoming infected with the Mirai malware, computer continuously search the web for susceptible IoT devices before infecting them with malware by logging in using well know default usernames and passwords.

1.1.3 Privacy Breach

Smart Home devices like assistants, cameras, appliances, etc. often collect sensitive data, such as audio and video feeds, and user preferences. Unauthorized access to this data can lead to privacy breaches. Verkada, a cloud-based video surveillance service, was hacked in March 2021. The attackers could access private information belonging to Verkada software clients and access live feeds of over 150,000 cameras mounted in factories, hospitals, schools, prisons, and other sites using legitimate admin account credentials found on the internet. Over 100 employees were later found to have ”super admin” privileges, enabling them access to thousands of customer cameras, revealing the risks associated with over privileged users.

1.1.4 Fatal Implications

Some IoT devices, like connected cars or medical devices, have physical safety implications. If these devices are compromised, they can endanger lives and property. This is one of the most severe implications of a network attack on IoT devices as it could ultimately lead to loss of life. In July 2015, a group of researchers tested the security of the Jeep SUV. They managed to take control of the vehicle via the Sprint cellular network by taking advantage of a firmware update vulnerability. They could then control the vehicle’s speed and even steer it off the road.

1.2 Prevention Methodology

1.2.1 DNS Sinkholes

DNS sinkhole or black hole DNS is used to spoof DNS servers to prevent resolving hostnames of specified URLs. This can be achieved by configuring the DNS forwarder to return a false IP address to a specific URL. DNS sinkholing can be used to prevent access to malicious URLs at an enterprise level. The malicious URLs can be blocked by adding a false entry in the DNS and thus there will be a second level of protection. Normally firewalls and proxies are used to block malicious traffic across the organization.

1.2.2 Virtual Private Network

A virtual private network (VPN) is a mechanism for creating a secure connection between a computing device and a computer network, or between two networks, using an insecure communication medium such as the public internet. A VPN can extend access to a private network to users who do not have direct access to it. A VPN is established by creating a virtual point to point connection through the use of tunneling protocols over existing networks.

Chapter 2

Literature Review

The objective of this review is to provide a comprehensive overview of existing research, methodologies, and best practices concerning the security implications associated with ARM-based IoT devices.

2.0.1 Autonomous NAT Traversal - A. Muller, N. Evans, C. Grothoff, S. Kamkar — Year: 2010 — Conference Paper — Publisher: IEEE

Traditional NAT traversal methods require the help of a third party for signalling. This paper investigates a new autonomous method for establishing connections to peers behind NAT. The proposed method for autonomous NAT traversal uses fake ICMP messages to initially contact the NATed peer. This paper presents how the method is supposed to work in theory, discusses some possible variations, introduces various concrete implementations of the proposed approach and evaluates empirical results of a measurement study designed to evaluate the efficacy of the idea in practice.

2.0.2 Evaluating the Vulnerability of Network Traffic Using Joint Security and Routing Analysis - Patrick Tague, David Slater, Jason Rogers, Radha Poovendra

Joint analysis of security and routing protocols in wireless networks reveals vulnerabilities of secure network traffic that remain undetected when security and routing protocols are analyzed independently. This paper formulates a class of continuous metrics to evaluate the vulnerability of network traffic as a function of security and routing protocols used in wireless networks.

2.0.3 DNS Amplification and DNS Tunneling Attacks Simulation, Detection and Mitigation Approaches - Sanjay, Balaji Rajendra, Pushparaj Shetty D — Year: 2020 — Conference Paper — Publisher: IEEE

DNS is a critical infrastructure service of the Internet that translates hostnames to network IP addresses and vice versa. The criticality of DNS can be evidenced by the fact that all most all organizations and enterprises do not block DNS traffic, as it would eventually stop access to the Internet. As a result, attackers have been exploiting the DNS infrastructure and using it as a launchpad for carrying out various attacks e.g. DoS /DDoS , DNS reflection and amplification, DNS tunneling, NXDOMAIN attack, and DNS hijacking, etc. During the historic implementation of DNS protocol, its security was not considered which lead to the exploitation of various vulnerabilities in the DNS infrastructure. This paper brings out the technicalities behind DNS amplification and DNS tunneling attacks and presents a number of countermeasures and mitigation techniques to protect against these attacks and the DNS Infrastructure.

2.0.4 Experimental performance comparison between TCP vs UDP tunnel using OpenVPN - Irfaan Coonjah, Pierre Clarel Catherine, K.M.S Soyjaudah — Year: 2015 — Conference Paper — Publisher: IEEE

The comparison between TCP and UDP tunnels have not been sufficiently reported in the scientific literature. In this work, they use OpenVPN as a platform to demonstrate the performance between TCP/UDP. The de facto belief has been that TCP tunnel provides a permanent tunnel and therefore ensures a reliable transfer of data between two end points. However the effects of transmitting TCP within a UDP tunnel has been explored and could provide a valuable attempt. The results provided in this paper demonstrates that indeed TCP in UDP tunnel provides better latency. Throughout this paper, a series of tests have been performed, UDP traffic was sent inside UDP tunnel and TCP tunnel successively. The same tests was performed using TCP traffic.

2.0.5 Internet of Things Security - Multilayered Method For End to End Data Communications - Craig Lee, Andrea Fumagalli — Year: 2019 — Conference Paper — Publisher: IEEE

The aim of this paper is to put forth a multilayered method for securing data transport from a cellular connected Internet of Things device to a host through a cellular network. This method employs many interlocking security elements – described in this paper – that when implemented in their totality provide a highly secure connectivity solution.

2.0.6 IEE Colloquium on ’RISC Architectures and Applications’ (Digest No.163) — Year: 1991 — Conference Paper — Publisher: IET

Chapter 3

Implementation

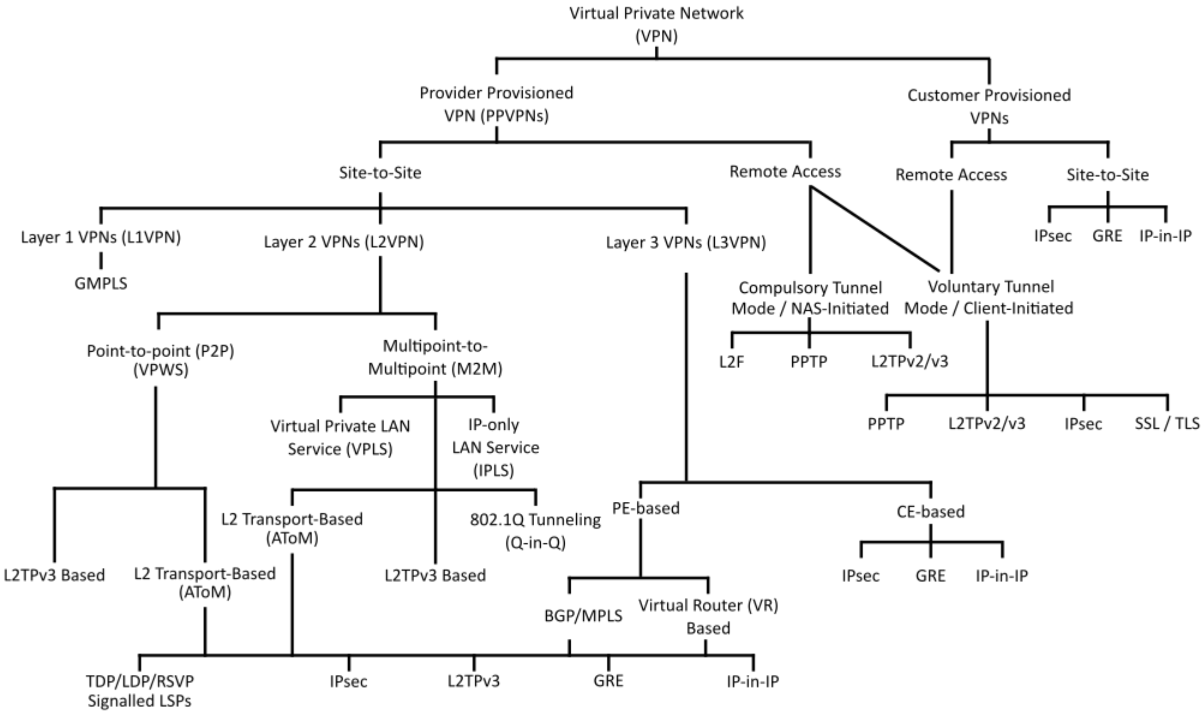
3.1 Tools

Table 3.1: Tools Used

Sl. No	Item	Description
1	Laptop	Laptop running an x86-64 Operating System
2	Arch Linux	Linux Distro used for the laptop
3	Raspberry Pi 0-2	Single Board Computer used for implementing defensive measures
4	Raspberry Pi OS	Debian Based Linux Distro used for Raspberry Pi 0-2
5	CLi Network Tools	Tools like dnsmasq, iftop, nmap, tcpdump, etc.
6	Pi-Hole	DNS Sinkhole for network wide network defense
7	ProtonVPN	VPN Service Provider
8	Browser Extensions	Extensions for always use HTTPs and disabling Javascript

3.2 Description

User friendly sinkholes like Pi-Hole that can run off of a cheap Raspberry Pi 0 running the ARMhf architecture can be used to block access to malicious websites and IPs. Tools used to evaluate this hyopthesis were a laptop computer running a barebones Linux Distro based on Arch Linux and CLi tools such as nmap, iftop, dnsmasq and tcpdump among many others as well as a single board computer Raspberry Pi 0-2 running a Debian based Raspberry Pi OS. Connections from the computer to the internet were routed through the SBC which was configured to block malicious IP addresses and websites. The SBC also acted as a VPN that would mask the orignal IP address of the computer. Another VPN connection was also used to mask user IP address using a public VPN service provider. Other implementations were also put into place like force usage of TCP(Transmission Control Protocol) instead of UDP(User Datagram Protocol) to check whether or not the data packets received during data transfer were mangled or not as one of the most common Denial-Of-Service attacks on an ARM device is achieved by rapidly sending malformed data packets to the target computers which can be as simple as just sending data packets with incorrect headers which can lead to an ARM device crashing because it cannot process such large amount of malformed data as it can only process a reduced instruction set and doesn't support CPU parallelism i.e. it cannot pipeline tasks. Usage of browser extensions were also present to force websites to use an HTTPs(Hypertext Transfer Protocol Secure) connection instead of HTTP and force disable the use of javascript while using some suspicious websites. Testing was done on both private and public networks.



Virtual Private Network (VPN)
Provider Provisioned VPN (PPVPNs)
Customer Provisioned VPNs
Site-to-Site
Remote Access
Remote Access
Site-to-Site
IPsec
GRE
IP-in-IP
Layer 1 VPNs (L1VPN)
Layer 2 VPNs (L2VPN)
Layer 3 VPNs (L3VPN)
GMPLS
Compulsory Tunnel Mode / NAS-Initiated
Voluntary Tunnel Mode / Client-Initiated
L2F
PPTP
L2TPv2/v3
Point-to-point (P2P) (VPWS)
Multipoint-to-Multipoint (M2M)
PPTP
L2TPv2/v3
IPsec
SSL / TLS
Virtual Private LAN Service (VPLS)
IP-only LAN Service (IPLS)
L2 Transport-Based (AToM)
802.1Q Tunneling (Q-in-Q)
PE-based
CE-based
L2TPv3 Based
L2 Transport-Based (AToM)
L2TPv3 Based
IPsec
GRE
IP-in-IP
BGP/MPLS
Virtual Router (VR) Based
TDP/LDP/RSVP Signalled LSPs
IPsec
L2TPv3
GRE
IP-in-IP

Figure 3.1: VPN Classification

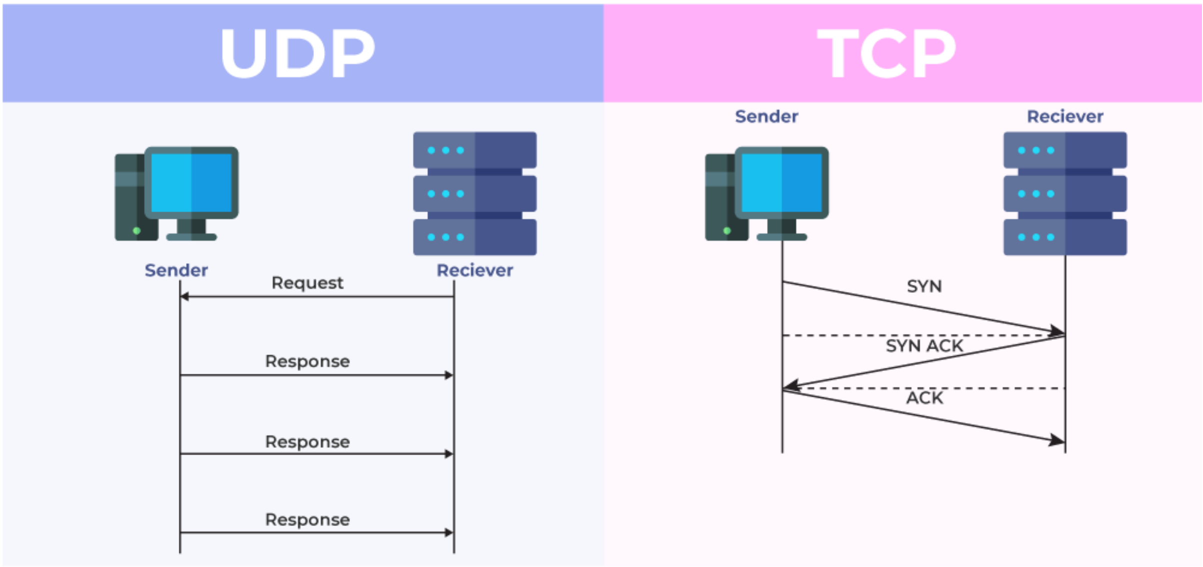


Figure 3.2: TCP vs UDP

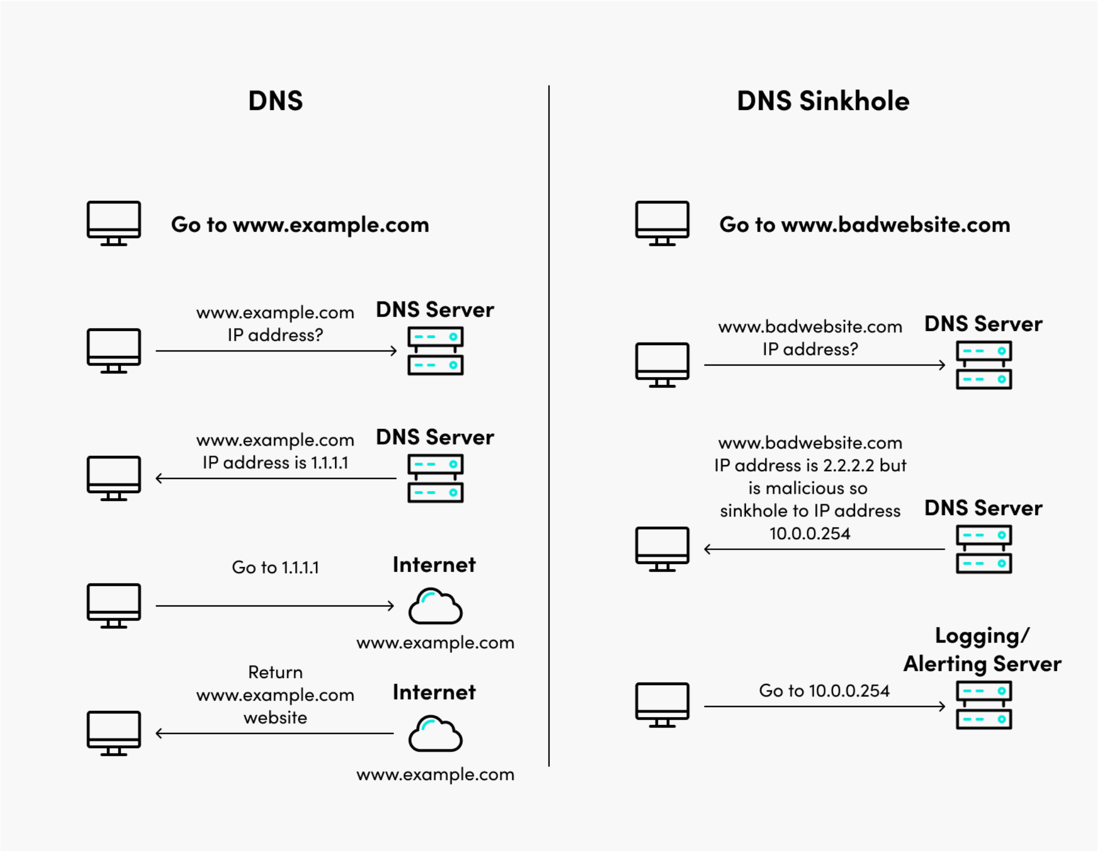


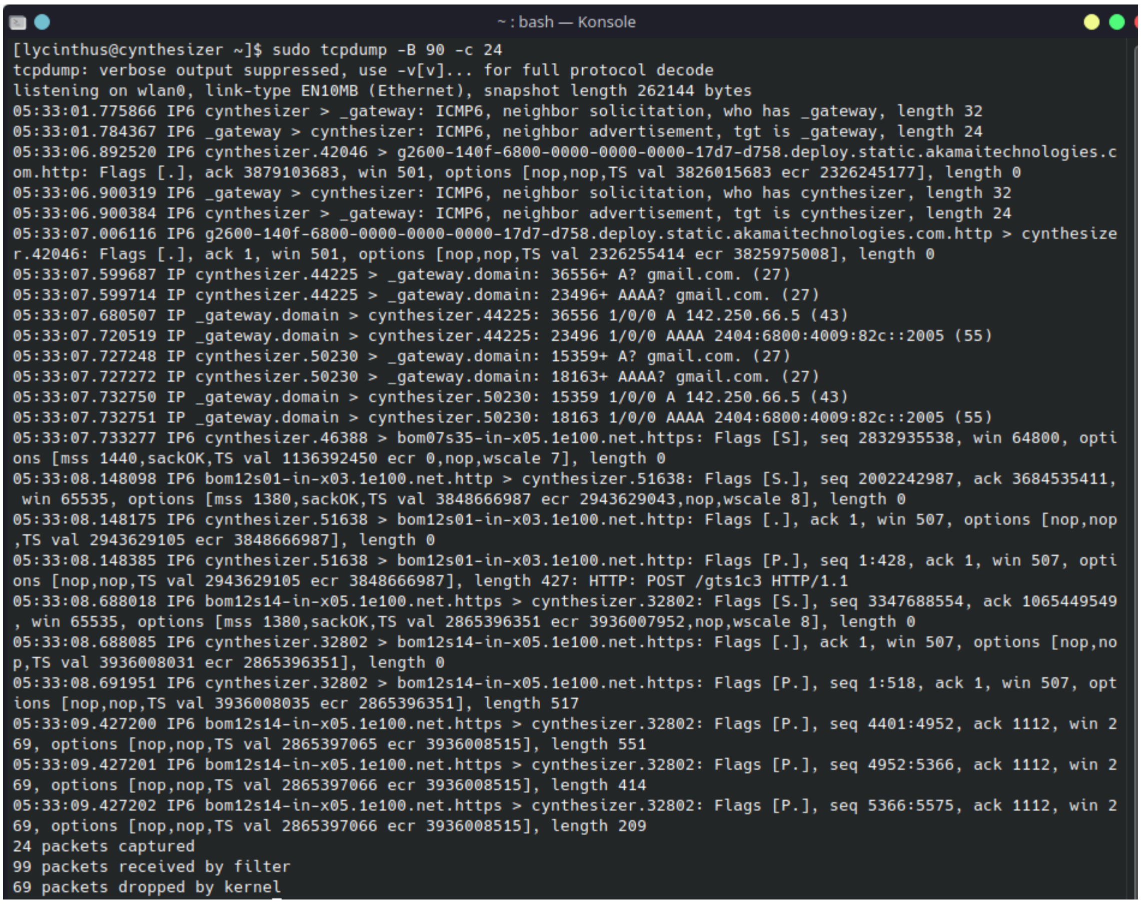
Figure 3.3: DNS Sinkhole

Chapter 4

Results

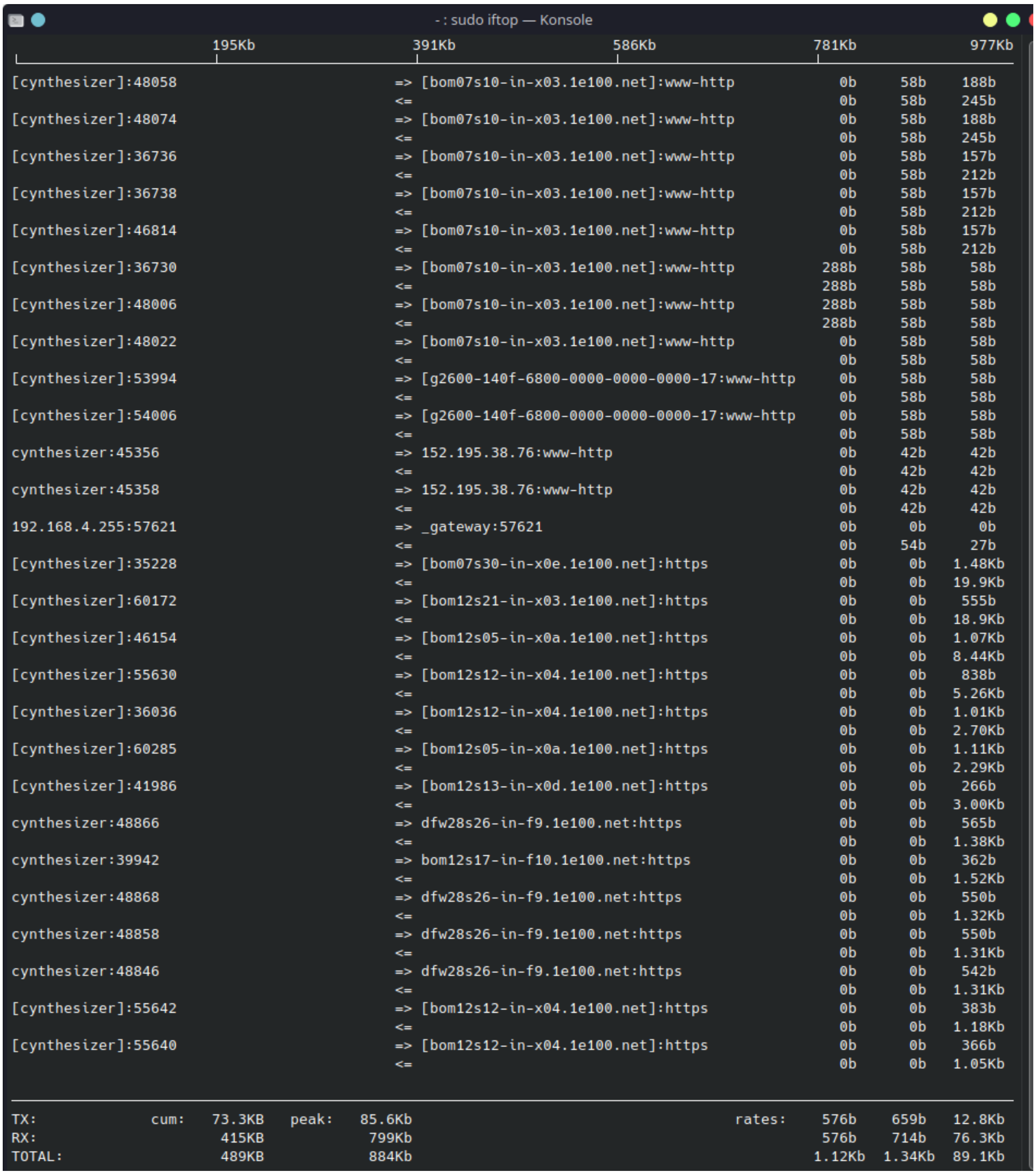
Intensive testing by trial and error of network security implementations with different software applications working individually or in tandem shows positive results which means that the defenses put into place were successful at resisting network attacks up to a certain extent.

4.0.1 Testing Results



```
[lycinthus@cynthesizer ~]$ sudo tcpdump -B 90 -c 24
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on wlan0, link-type EN10MB (Ethernet), snapshot length 262144 bytes
05:33:01.775866 IP6 cynthesizer > _gateway: ICMP6, neighbor solicitation, who has _gateway, length 32
05:33:01.784367 IP6 _gateway > cynthesizer: ICMP6, neighbor advertisement, tgt is _gateway, length 24
05:33:06.892520 IP6 cynthesizer.42046 > g2600-140f-6800-0000-0000-0000-17d7-d758.deploy.static.akamaitechnologies.c
om.http: Flags [.], ack 3879103683, win 501, options [nop,nop,TS val 3826015683 ecr 2326245177], length 0
05:33:06.900319 IP6 _gateway > cynthesizer: ICMP6, neighbor solicitation, who has cynthesizer, length 32
05:33:06.900384 IP6 cynthesizer > _gateway: ICMP6, neighbor advertisement, tgt is cynthesizer, length 24
05:33:07.006116 IP6 g2600-140f-6800-0000-0000-0000-17d7-d758.deploy.static.akamaitechnologies.com.http > cynthesize
r.42046: Flags [.], ack 1, win 501, options [nop,nop,TS val 2326255414 ecr 3825975008], length 0
05:33:07.599687 IP cynthesizer.44225 > _gateway.domain: 36556+ A? gmail.com. (27)
05:33:07.599714 IP cynthesizer.44225 > _gateway.domain: 23496+ AAAA? gmail.com. (27)
05:33:07.680507 IP _gateway.domain > cynthesizer.44225: 36556 1/0/0 A 142.250.66.5 (43)
05:33:07.720519 IP _gateway.domain > cynthesizer.44225: 23496 1/0/0 AAAA 2404:6800:4009:82c::2005 (55)
05:33:07.727248 IP cynthesizer.50230 > _gateway.domain: 15359+ A? gmail.com. (27)
05:33:07.727272 IP cynthesizer.50230 > _gateway.domain: 18163+ AAAA? gmail.com. (27)
05:33:07.732750 IP _gateway.domain > cynthesizer.50230: 15359 1/0/0 A 142.250.66.5 (43)
05:33:07.732751 IP _gateway.domain > cynthesizer.50230: 18163 1/0/0 AAAA 2404:6800:4009:82c::2005 (55)
05:33:07.733277 IP6 cynthesizer.46388 > bom07s35-in-x05.1e100.net.https: Flags [S], seq 2832935538, win 64800, opti
ons [mss 1440,sackOK,TS val 1136392450 ecr 0,nop,wscale 7], length 0
05:33:08.148098 IP6 bom12s01-in-x03.1e100.net.http > cynthesizer.51638: Flags [S.], seq 2002242987, ack 3684535411,
 win 65535, options [mss 1380,sackOK,TS val 3848666987 ecr 2943629043,nop,wscale 8], length 0
05:33:08.148175 IP6 cynthesizer.51638 > bom12s01-in-x03.1e100.net.http: Flags [.], ack 1, win 507, options [nop,nop
,TS val 2943629105 ecr 3848666987], length 0
05:33:08.148385 IP6 cynthesizer.51638 > bom12s01-in-x03.1e100.net.http: Flags [P.], seq 1:428, ack 1, win 507, opti
ons [nop,nop,TS val 2943629105 ecr 3848666987], length 427: HTTP: POST /gts1c3 HTTP/1.1
05:33:08.688018 IP6 bom12s14-in-x05.1e100.net.https > cynthesizer.32802: Flags [S.], seq 3347688554, ack 1065449549
, win 65535, options [mss 1380,sackOK,TS val 2865396351 ecr 3936007952,nop,wscale 8], length 0
05:33:08.688085 IP6 cynthesizer.32802 > bom12s14-in-x05.1e100.net.https: Flags [.], ack 1, win 507, options [nop,no
p,TS val 3936008031 ecr 2865396351], length 0
05:33:08.691951 IP6 cynthesizer.32802 > bom12s14-in-x05.1e100.net.https: Flags [P.], seq 1:518, ack 1, win 507, opt
ions [nop,nop,TS val 3936008035 ecr 2865396351], length 517
05:33:09.427200 IP6 bom12s14-in-x05.1e100.net.https > cynthesizer.32802: Flags [P.], seq 4401:4952, ack 1112, win 2
69, options [nop,nop,TS val 2865397065 ecr 3936008515], length 551
05:33:09.427201 IP6 bom12s14-in-x05.1e100.net.https > cynthesizer.32802: Flags [P.], seq 4952:5366, ack 1112, win 2
69, options [nop,nop,TS val 2865397066 ecr 3936008515], length 414
05:33:09.427202 IP6 bom12s14-in-x05.1e100.net.https > cynthesizer.32802: Flags [P.], seq 5366:5575, ack 1112, win 2
69, options [nop,nop,TS val 2865397066 ecr 3936008515], length 209
24 packets captured
99 packets received by filter
69 packets dropped by kernel
```

Figure 4.1: tcpdump Output without defenses

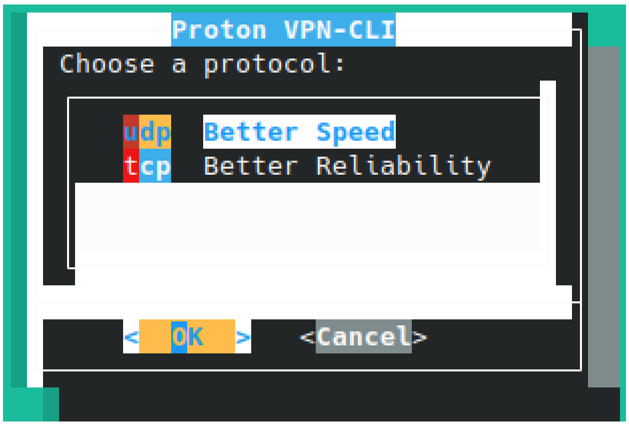


- : sudo iftop — Konsole

```
                      195Kb                  391Kb                  586Kb                  781Kb              977Kb
[cynthesizer]:48058                            => [bom07s10-in-x03.1e100.net]:www-http          0b     58b    188b
                                               <=                                                0b     58b    245b
[cynthesizer]:48074                            => [bom07s10-in-x03.1e100.net]:www-http          0b     58b    188b
                                               <=                                                0b     58b    245b
[cynthesizer]:36736                            => [bom07s10-in-x03.1e100.net]:www-http          0b     58b    157b
                                               <=                                                0b     58b    212b
[cynthesizer]:36738                            => [bom07s10-in-x03.1e100.net]:www-http          0b     58b    157b
                                               <=                                                0b     58b    212b
[cynthesizer]:46814                            => [bom07s10-in-x03.1e100.net]:www-http          0b     58b    157b
                                               <=                                                0b     58b    212b
[cynthesizer]:36730                            => [bom07s10-in-x03.1e100.net]:www-http        288b     58b     58b
                                               <=                                              288b     58b     58b
[cynthesizer]:48006                            => [bom07s10-in-x03.1e100.net]:www-http        288b     58b     58b
                                               <=                                              288b     58b     58b
[cynthesizer]:48022                            => [bom07s10-in-x03.1e100.net]:www-http          0b     58b     58b
                                               <=                                                0b     58b     58b
[cynthesizer]:53994                            => [g2600-140f-6800-0000-0000-0000-17:www-http   0b     58b     58b
                                               <=                                                0b     58b     58b
[cynthesizer]:54006                            => [g2600-140f-6800-0000-0000-0000-17:www-http   0b     58b     58b
                                               <=                                                0b     58b     58b
cynthesizer:45356                              => 152.195.38.76:www-http                        0b     42b     42b
                                               <=                                                0b     42b     42b
cynthesizer:45358                              => 152.195.38.76:www-http                        0b     42b     42b
                                               <=                                                0b     42b     42b
192.168.4.255:57621                            => _gateway:57621                                0b      0b      0b
                                               <=                                                0b     54b     27b
[cynthesizer]:35228                            => [bom07s30-in-x0e.1e100.net]:https             0b      0b   1.48Kb
                                               <=                                                0b      0b   19.9Kb
[cynthesizer]:60172                            => [bom12s21-in-x03.1e100.net]:https             0b      0b    555b
                                               <=                                                0b      0b   18.9Kb
[cynthesizer]:46154                            => [bom12s05-in-x0a.1e100.net]:https             0b      0b   1.07Kb
                                               <=                                                0b      0b   8.44Kb
[cynthesizer]:55630                            => [bom12s12-in-x04.1e100.net]:https             0b      0b    838b
                                               <=                                                0b      0b   5.26Kb
[cynthesizer]:36036                            => [bom12s12-in-x04.1e100.net]:https             0b      0b   1.01Kb
                                               <=                                                0b      0b   2.70Kb
[cynthesizer]:60285                            => [bom12s05-in-x0a.1e100.net]:https             0b      0b   1.11Kb
                                               <=                                                0b      0b   2.29Kb
[cynthesizer]:41986                            => [bom12s13-in-x0d.1e100.net]:https             0b      0b    266b
                                               <=                                                0b      0b   3.00Kb
cynthesizer:48866                              => dfw28s26-in-f9.1e100.net:https                0b      0b    565b
                                               <=                                                0b      0b   1.38Kb
cynthesizer:39942                              => bom12s17-in-f10.1e100.net:https               0b      0b    362b
                                               <=                                                0b      0b   1.52Kb
cynthesizer:48868                              => dfw28s26-in-f9.1e100.net:https                0b      0b    550b
                                               <=                                                0b      0b   1.32Kb
cynthesizer:48858                              => dfw28s26-in-f9.1e100.net:https                0b      0b    550b
                                               <=                                                0b      0b   1.31Kb
cynthesizer:48846                              => dfw28s26-in-f9.1e100.net:https                0b      0b    542b
                                               <=                                                0b      0b   1.31Kb
[cynthesizer]:55642                            => [bom12s12-in-x04.1e100.net]:https             0b      0b    383b
                                               <=                                                0b      0b   1.18Kb
[cynthesizer]:55640                            => [bom12s12-in-x04.1e100.net]:https             0b      0b    366b
                                               <=                                                0b      0b   1.05Kb

TX:            cum:   73.3KB   peak:   85.6Kb                                   rates:    576b    659b   12.8Kb
RX:                    415KB           799Kb                                              576b    714b   76.3Kb
TOTAL:                 489KB           884Kb                                            1.12Kb  1.34Kb   89.1Kb
```

Figure 4.2: iftop Output without defenses

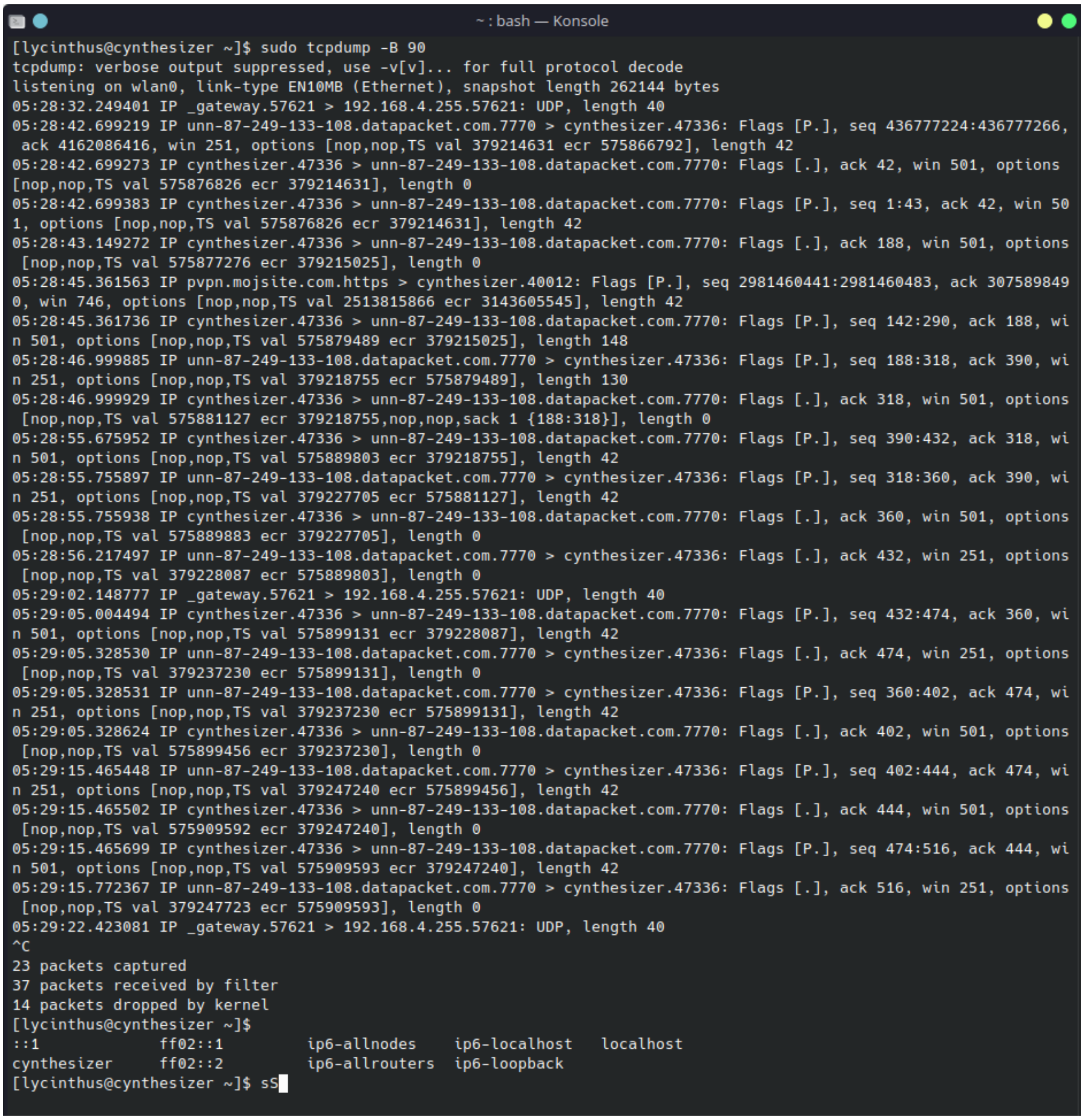


Proton VPN-CLI

Choose a protocol:

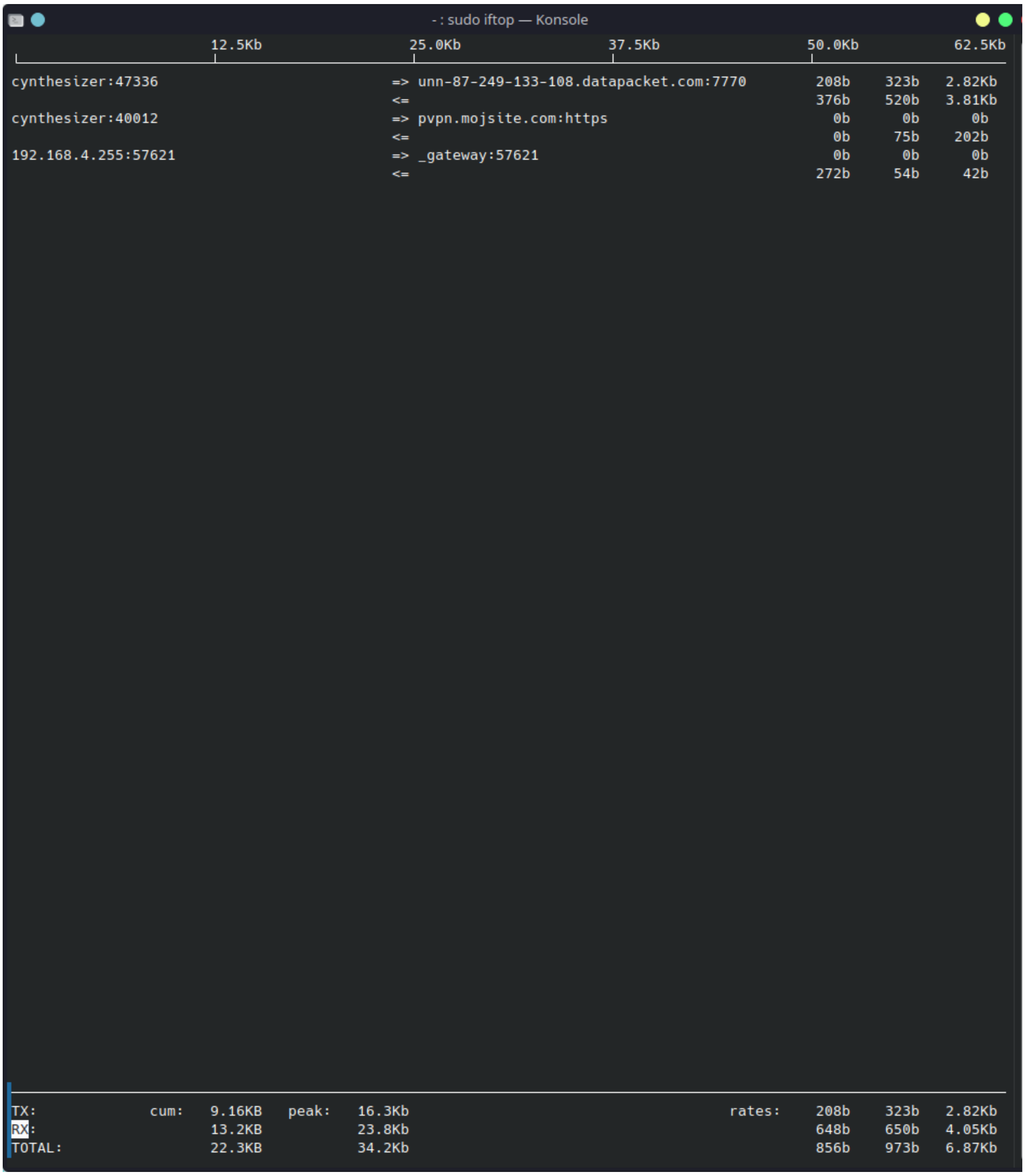
udp Better Speed
tcp Better Reliability

Figure 4.3: TCP vs. UDP



```
[lycinthus@cynthesizer ~]$ sudo tcpdump -B 90
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on wlan0, link-type EN10MB (Ethernet), snapshot length 262144 bytes
05:28:32.249401 IP _gateway.57621 > 192.168.4.255.57621: UDP, length 40
05:28:42.699219 IP unn-87-249-133-108.datapacket.com.7770 > cynthesizer.47336: Flags [P.], seq 436777224:436777266,
 ack 4162086416, win 251, options [nop,nop,TS val 379214631 ecr 575866792], length 42
05:28:42.699273 IP cynthesizer.47336 > unn-87-249-133-108.datapacket.com.7770: Flags [.], ack 42, win 501, options
[nop,nop,TS val 575876826 ecr 379214631], length 0
05:28:42.699383 IP cynthesizer.47336 > unn-87-249-133-108.datapacket.com.7770: Flags [P.], seq 1:43, ack 42, win 50
1, options [nop,nop,TS val 575876826 ecr 379214631], length 42
05:28:43.149272 IP cynthesizer.47336 > unn-87-249-133-108.datapacket.com.7770: Flags [.], ack 188, win 501, options
 [nop,nop,TS val 575877276 ecr 379215025], length 0
05:28:45.361563 IP pvpn.mojsite.com.https > cynthesizer.40012: Flags [P.], seq 2981460441:2981460483, ack 307589849
0, win 746, options [nop,nop,TS val 2513815866 ecr 3143605545], length 42
05:28:45.361736 IP cynthesizer.47336 > unn-87-249-133-108.datapacket.com.7770: Flags [P.], seq 142:290, ack 188, wi
n 501, options [nop,nop,TS val 575879489 ecr 379215025], length 148
05:28:46.999885 IP unn-87-249-133-108.datapacket.com.7770 > cynthesizer.47336: Flags [P.], seq 188:318, ack 390, wi
n 251, options [nop,nop,TS val 379218755 ecr 575879489], length 130
05:28:46.999929 IP cynthesizer.47336 > unn-87-249-133-108.datapacket.com.7770: Flags [.], ack 318, win 501, options
 [nop,nop,TS val 575881127 ecr 379218755,nop,nop,sack 1 {188:318}], length 0
05:28:55.675952 IP cynthesizer.47336 > unn-87-249-133-108.datapacket.com.7770: Flags [P.], seq 390:432, ack 318, wi
n 501, options [nop,nop,TS val 575889803 ecr 379218755], length 42
05:28:55.755897 IP unn-87-249-133-108.datapacket.com.7770 > cynthesizer.47336: Flags [P.], seq 318:360, ack 390, wi
n 251, options [nop,nop,TS val 379227705 ecr 575881127], length 42
05:28:55.755938 IP cynthesizer.47336 > unn-87-249-133-108.datapacket.com.7770: Flags [.], ack 360, win 501, options
 [nop,nop,TS val 575889883 ecr 379227705], length 0
05:28:56.217497 IP unn-87-249-133-108.datapacket.com.7770 > cynthesizer.47336: Flags [.], ack 432, win 251, options
 [nop,nop,TS val 379228087 ecr 575889803], length 0
05:29:02.148777 IP _gateway.57621 > 192.168.4.255.57621: UDP, length 40
05:29:05.004494 IP cynthesizer.47336 > unn-87-249-133-108.datapacket.com.7770: Flags [P.], seq 432:474, ack 360, wi
n 501, options [nop,nop,TS val 575899131 ecr 379228087], length 42
05:29:05.328530 IP unn-87-249-133-108.datapacket.com.7770 > cynthesizer.47336: Flags [.], ack 474, win 251, options
 [nop,nop,TS val 379237230 ecr 575899131], length 0
05:29:05.328531 IP unn-87-249-133-108.datapacket.com.7770 > cynthesizer.47336: Flags [P.], seq 360:402, ack 474, wi
n 251, options [nop,nop,TS val 379237230 ecr 575899131], length 42
05:29:05.328624 IP cynthesizer.47336 > unn-87-249-133-108.datapacket.com.7770: Flags [.], ack 402, win 501, options
 [nop,nop,TS val 575899456 ecr 379237230], length 0
05:29:15.465448 IP unn-87-249-133-108.datapacket.com.7770 > cynthesizer.47336: Flags [P.], seq 402:444, ack 474, wi
n 251, options [nop,nop,TS val 379247240 ecr 575899456], length 42
05:29:15.465502 IP cynthesizer.47336 > unn-87-249-133-108.datapacket.com.7770: Flags [.], ack 444, win 501, options
 [nop,nop,TS val 575909592 ecr 379247240], length 0
05:29:15.465699 IP cynthesizer.47336 > unn-87-249-133-108.datapacket.com.7770: Flags [P.], seq 474:516, ack 444, wi
n 501, options [nop,nop,TS val 575909593 ecr 379247240], length 42
05:29:15.772367 IP unn-87-249-133-108.datapacket.com.7770 > cynthesizer.47336: Flags [.], ack 516, win 251, options
 [nop,nop,TS val 379247723 ecr 575909593], length 0
05:29:22.423081 IP _gateway.57621 > 192.168.4.255.57621: UDP, length 40
^C
23 packets captured
37 packets received by filter
14 packets dropped by kernel
[lycinthus@cynthesizer ~]$
::1             ff02::1         ip6-allnodes    ip6-localhost   localhost
cynthesizer     ff02::2         ip6-allrouters  ip6-loopback
[lycinthus@cynthesizer ~]$ sS
```

Figure 4.4: tcpdump Output with defenses



```
                    12.5Kb              25.0Kb              37.5Kb              50.0Kb         62.5Kb
└───────────────────┴───────────────────┴───────────────────┴───────────────────┴──────────────────
cynthesizer:47336                     => unn-87-249-133-108.datapacket.com:7770     208b    323b  2.82Kb
                                      <=                                            376b    520b  3.81Kb
cynthesizer:40012                     => pvpn.mojsite.com:https                       0b      0b      0b
                                      <=                                              0b     75b    202b
192.168.4.255:57621                   => _gateway:57621                               0b      0b      0b
                                      <=                                            272b     54b     42b




────────────────────────────────────────────────────────────────────────────────────────────────────
TX:             cum:   9.16KB   peak:   16.3Kb                          rates:      208b    323b  2.82Kb
RX:                    13.2KB           23.8Kb                                      648b    650b  4.05Kb
TOTAL:                 22.3KB           34.2Kb                                      856b    973b  6.87Kb
```

Figure 4.5: iftop Output with defenses

Chapter 5

Conclusion

In conclusion, this paper has explored the crucial nexus of network security and Arm-based Internet of Things (IoT) devices. The challenges of securing resource-constrained Arm devices in the dynamic IoT landscape were examined, emphasizing the need for innovative security measures. The conclusion underscores the importance of collaborative efforts, continuous monitoring, and proactive security strategies to mitigate emerging threats. Looking forward, a commitment to security, information sharing, and adaptive technologies will be essential for fortifying the resilience of our interconnected world amidst the evolving landscape of Arm-based IoT devices.

References

[1] A. Muller, N. Evans, C. Grothoff, S. Kamkar, et al., *Autonomous NAT Traversal*, 2010 *IEEE Conference Paper*

[2] *IEE Colloquium on 'RISC Architectures and Applications'*, 1991 *IET Conference Paper)*,(Digest No.163)

[3] Patrick Tague, David Slater, Jason Rogers, Radha Poovendra, et al *Evaluating the Vulnerability of Network Traffic Using Joint Security and Routing Analysis*

[4] Sanjay, Balaji Rajendra, Pushparaj Shetty D, et al., *DNS Amplification and DNS Tunneling Attacks Simulation, Detection and Mitigation Approaches* , 2020 *IEEE Conference Paper*

[5] Craig Lee, Andrea Fumagalli, et al., *Internet of Things Security - Multilayered Method For End to End Data Communications*, 2020 *IEEE Conference Paper*

[6] Irfaan Coonjah, Pierre Clarel, Catherine, K.M.S Soyjaudah, *Experimental performance comparison between TCP vs UDP tunnel using OpenVPN*, 2015 *IEEE Conference Paper*,

[7] @online Mirai Malware, https://en.wikipedia.org/wiki/Mirai(malware) Online; accessed 28-October-2023

[8] @online DNS Sinkhole, https://en.wikipedia.org/wiki/DNSsinkhole Online; accessed 20-October-2023

[9] @online Virtual Private Network, https://en.wikipedia.org/wiki/Virtualprivatenetwork Online; accessed 29-October-2023

[10] @online Pi-Hole, https://docs.pi-hole.net/ Online; accessed 13-October-2023

[11] @online PoisonTap, https://github.com/samyk/poisontap Online; accessed 13-October-2023

[12] @online RISC Machines, https://en.wikipedia.org/wiki/ARMarchitecturefamily Online; accessed 25-October-2023