PROJECT REPORT
“Ethernet Wiretap”

Table of Contents

Introduction

Objective

The objective of this project is to create an Ethernet Wiretap that can be installed between two switches or between a switch and a router to intercept data packets passing through them. The wiretap can also be used to create a .pcap file of the captured data and send it to a command and control server.

The ethernet wiretap must remain undetected by security devices such as Network Access Control (NAC). It must avoid raising suspicious alerts from security systems, allowing stealthy monitoring of network traffic. The wiretap must be small and unobtrusive, ensuring that it can be easily concealed within the network infrastructure. The compact size of the wiretap is essential to minimize the risk of being detected by network administration or other employees.

This project caters to the needs of penetration testers, who evaluate network security and find potential vulnerabilities. The network traffic collected by the wiretap allows penetration testers to obtain invaluable insights into the protocols used for communication, information of devices in the network and data transmitted within the network. The wiretap assess the effectiveness of security controls such as firewalls, intrusion detection and prevention systems.

Goals

1) Create an Ethernet Wiretap Device that captures data that flow between devices.

2) The wiretap must be compact, unobtrusive and easy to conceal.

3) The wiretap must be undetected by network security devices like Network Access Control (NAC).

4) Generate a .pcap file to be later accessed by C2 server using SSH.

Project Requirements

Hardware:

1. 4 X RJ45 Cat- Ethernet Patch/Lan Cable
2. Any Nexus, OnePlus or Samsung phone running Android 10 or above
3. RJ45 to type C connector

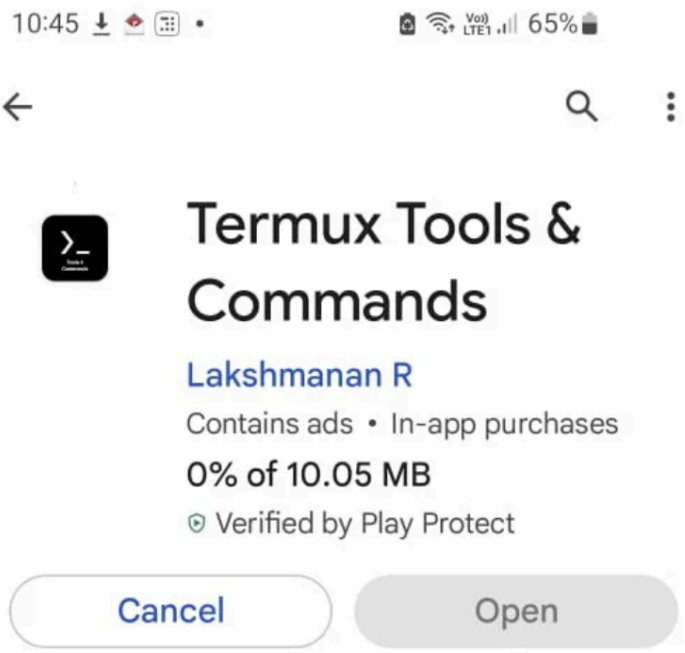
Software:

1. Termux
2. Kali Nethunter
3. Wireshark
4. Nethunter Kex

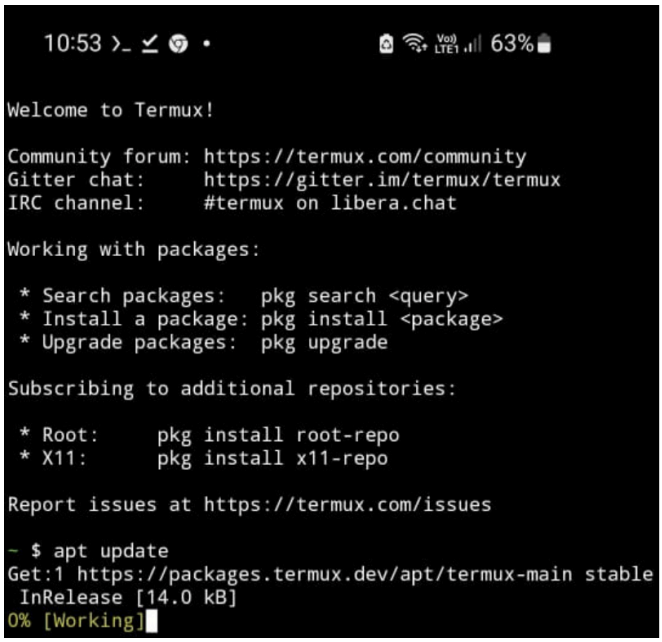
Procedure

Setting up Kali Nethunter

Step 1 : Download Termux from play store.



Step 2 : Update Repositories using command “apt update”.



Step 3 : Install wget using command “apt install wget”.

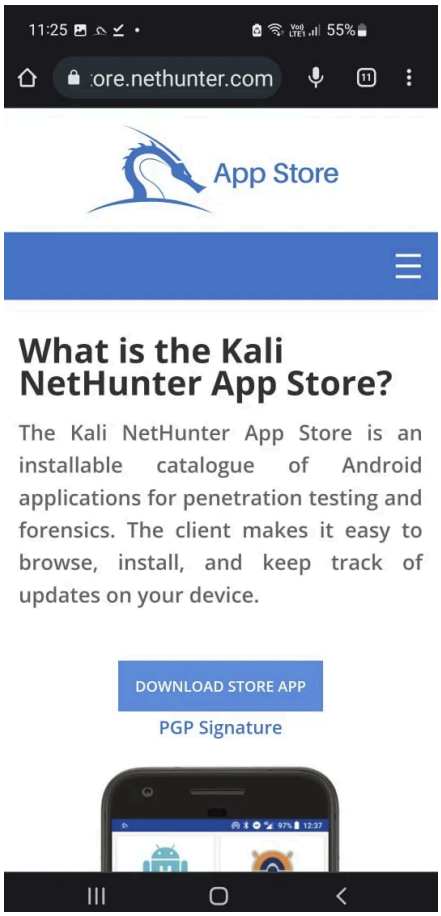
```
~ $ apt install wget
Reading package lists... Done
Building dependency tree... Done
The following additional packages will be installed:
  libuuid
The following NEW packages will be installed:
  libuuid wget
0 upgraded, 2 newly installed, 0 to remove and 63 not up
graded.
Need to get 293 kB of archives.
After this operation, 877 kB of additional disk space wi
ll be used.
Do you want to continue? [Y/n] Y
Get:1 https://packages.termux.dev/apt/termux-main stable
/main aarch64 libuuid aarch64 2.39.2 [14.6 kB]
Get:2 https://packages.termux.dev/apt/termux-main stable
/main aarch64 wget aarch64 1.21.4-1 [278 kB]
Fetched 293 kB in 3s (116 kB/s)
Selecting previously unselected package libuuid.
(Reading database ... 4112 files and directories current
ly installed.)
Preparing to unpack .../libuuid_2.39.2_aarch64.deb ...
Unpacking libuuid (2.39.2) ...
Selecting previously unselected package wget.
Preparing to unpack .../wget_1.21.4-1_aarch64.deb ...
Unpacking wget (1.21.4-1) ...
Setting up libuuid (2.39.2) ...
Setting up wget (1.21.4-1) ...
```

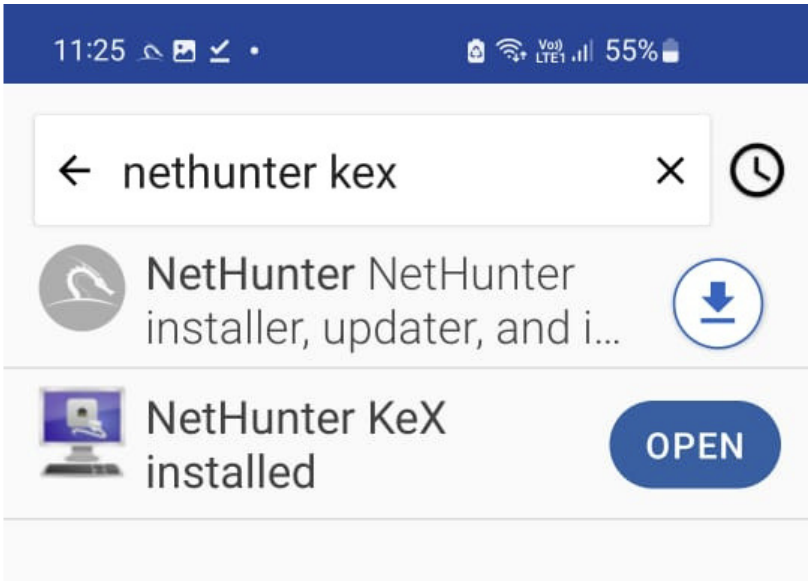
Step 4 : Download Kali Nethunter using command “wget -O install-nethunter-termux https://offs.ec/2MceZWr”.

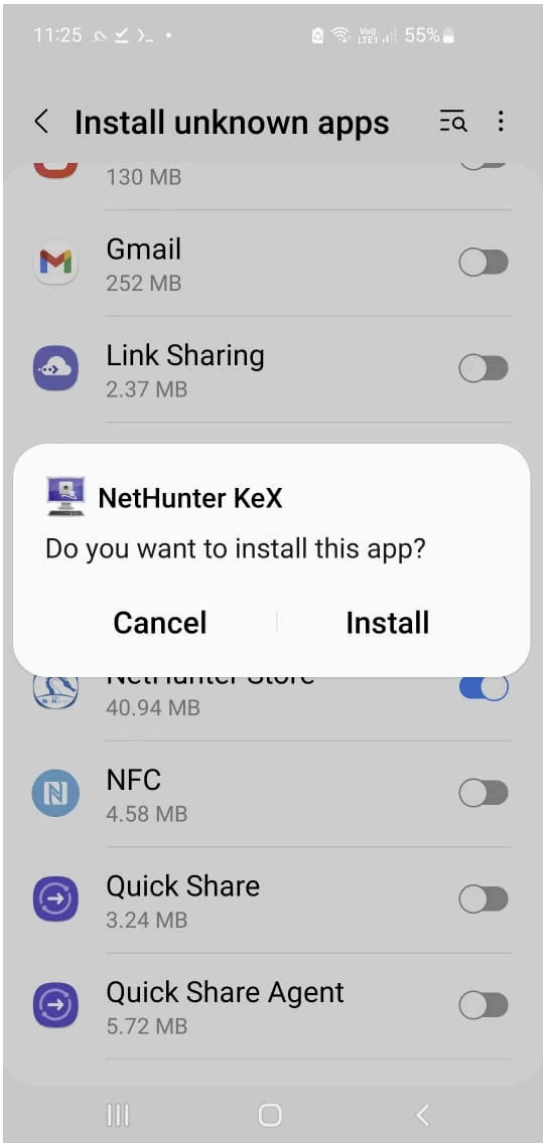
```
~ $ wget -O install-nethunter-termux https://offs.ec/2Mc
eZWr
--2023-08-22 23:04:58--  https://offs.ec/2MceZWr
Resolving offs.ec (offs.ec)... 67.199.248.12, 67.199.248
.13
Connecting to offs.ec (offs.ec)|67.199.248.12|:443... co
nnected.
HTTP request sent, awaiting response... 301 Moved Perman
ently
Location: https://gitlab.com/kalilinux/nethunter/build-s
cripts/kali-nethunter-project/raw/master/nethunter-rootl
ess/install-nethunter-termux [following]
--2023-08-22 23:05:00--  https://gitlab.com/kalilinux/ne
thunter/build-scripts/kali-nethunter-project/raw/master/
nethunter-rootless/install-nethunter-termux
Resolving gitlab.com (gitlab.com)... 2606:4700:90:0:f22e
:fbec:5bed:a9b9, 172.65.251.78
Connecting to gitlab.com (gitlab.com)|2606:4700:90:0:f22
e:fbec:5bed:a9b9|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 11782 (12K) [text/plain]
Saving to: ‘install-nethunter-termux’

install-nethu 100%  11.51K  --.-KB/s    in 0s
```

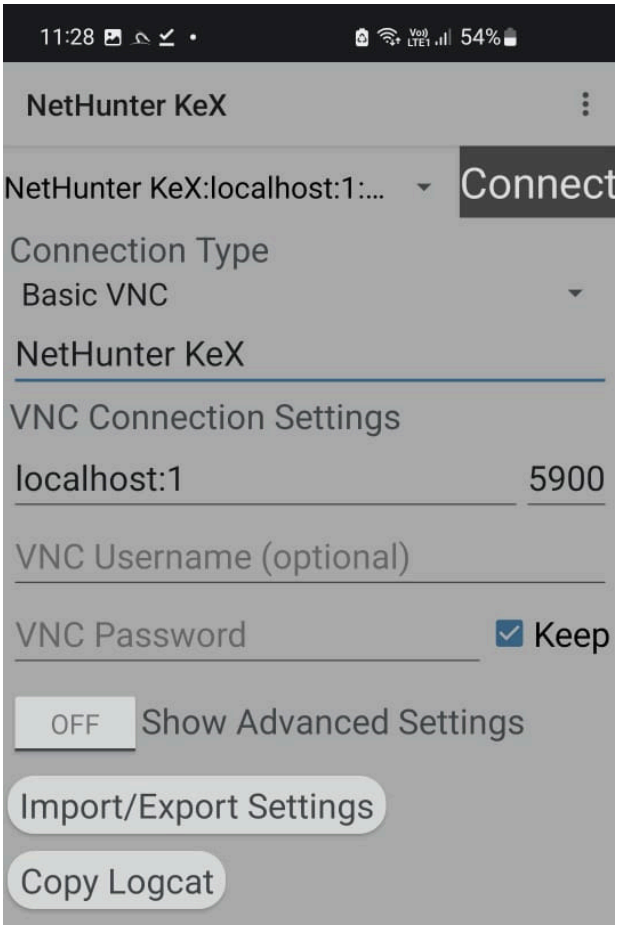
Step 5 : Run Kali Nethunter install script.

Step 6 : Setup nethunter kex.




11:25
55%
nethunter kex
NetHunter NetHunter installer, updater, and i...
NetHunter KeX installed
OPEN

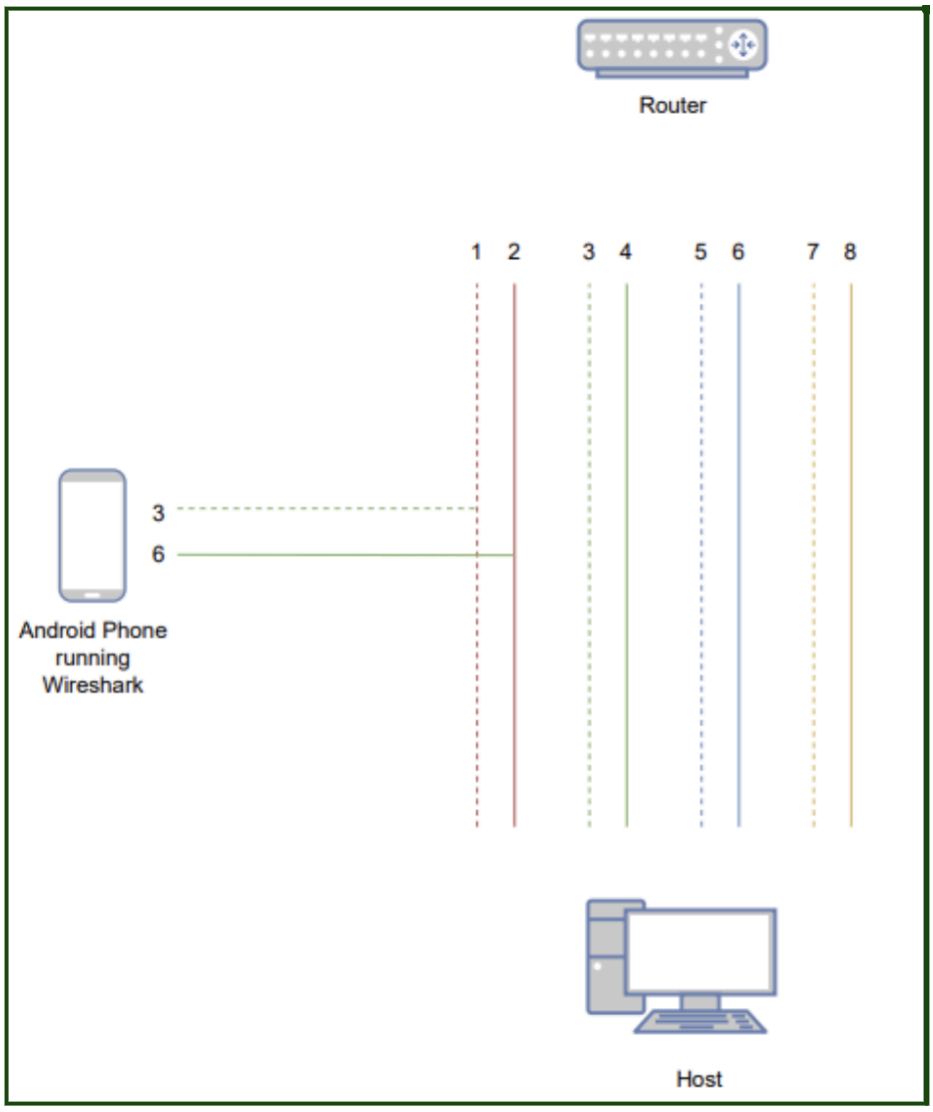

11:25
55%
Install unknown apps
130 MB
Gmail
252 MB
Link Sharing
2.37 MB
NetHunter KeX
Do you want to install this app?
Cancel
Install
40.94 MB
NFC
4.58 MB
Quick Share
3.24 MB
Quick Share Agent
5.72 MB



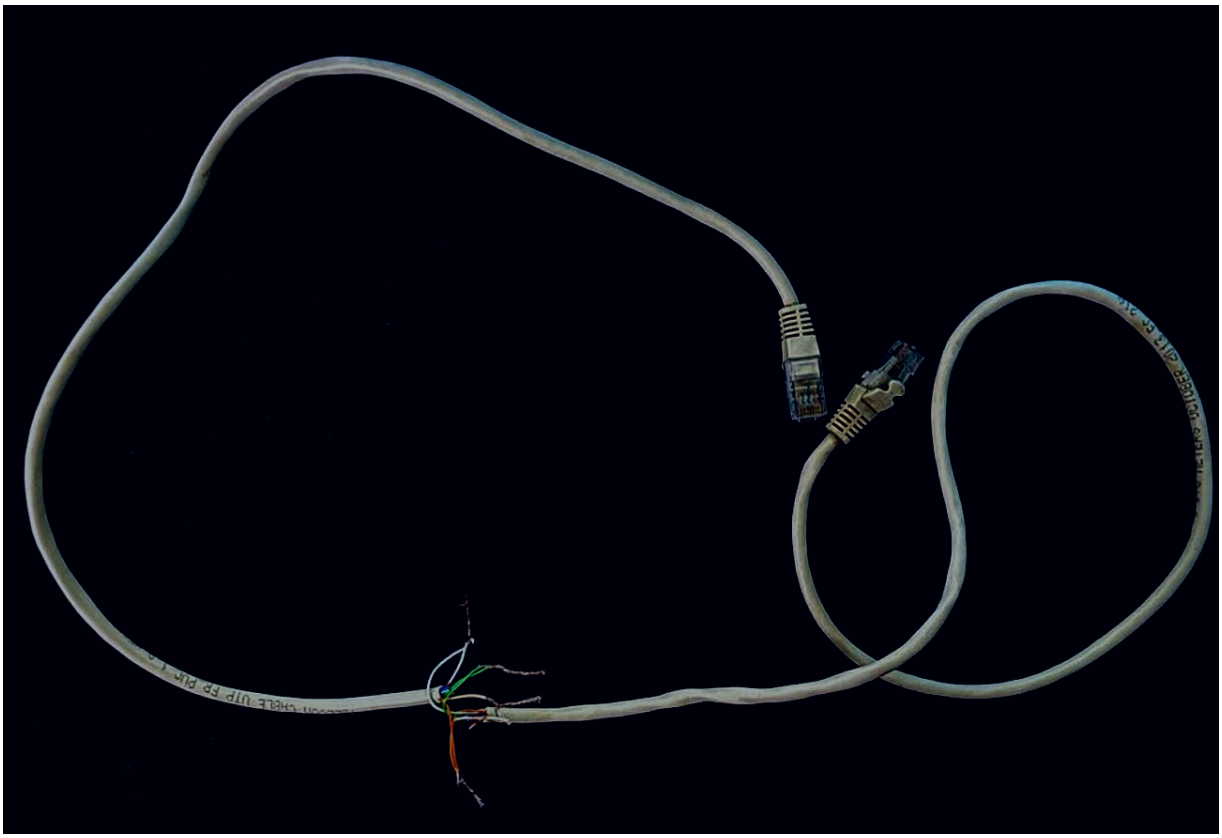
Step 7 : Access Kali Linux GUI using Nethunter Kex.

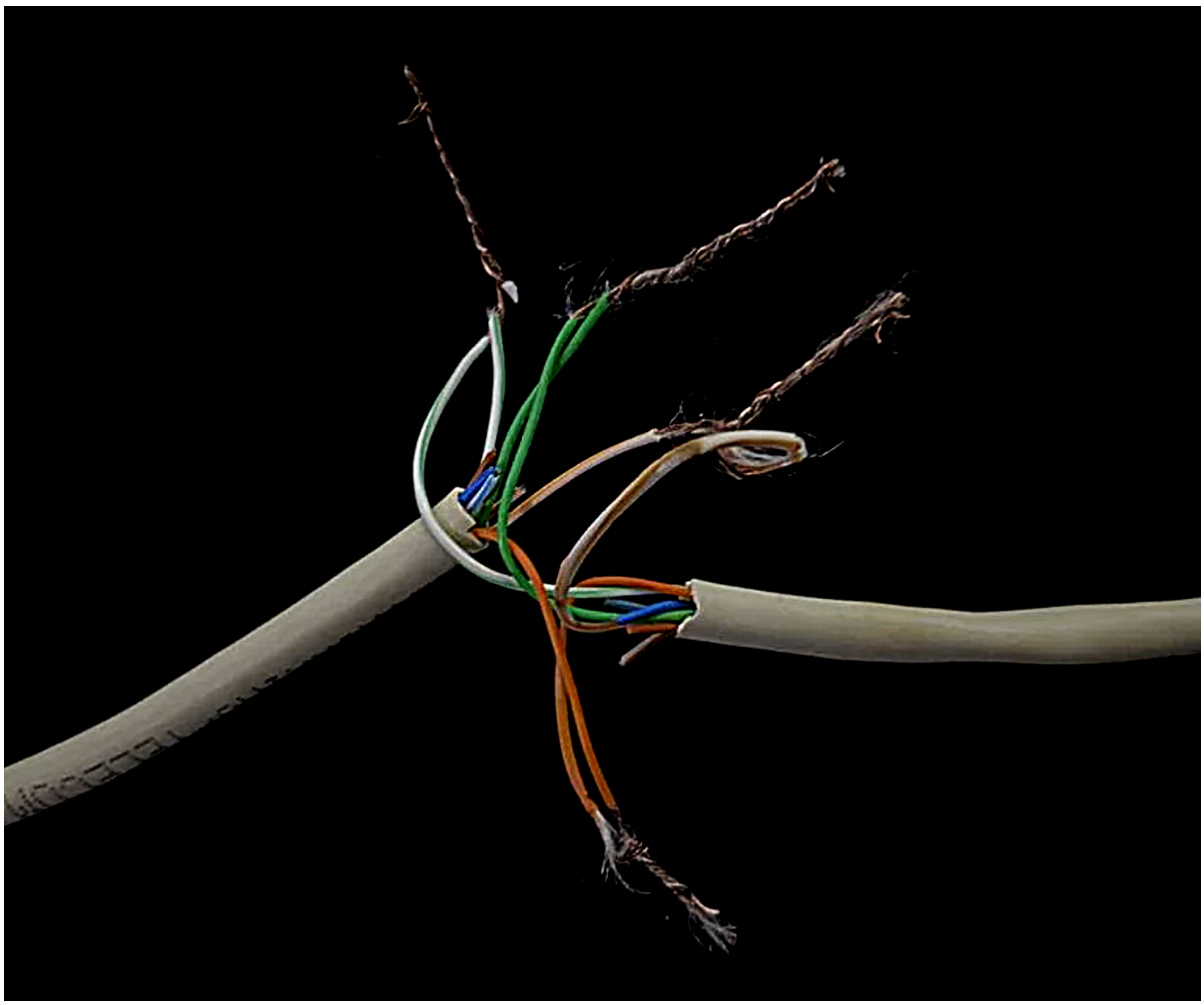
```
~ $ nethunter kex passwd
Password:
Verify:
Would you like to enter a view-only password (y/n)?
A view-only password is not used
~ $ nethunter kex
vncserver: No matching VNC server running for this user!
vncserver: No matching VNC server running for this user!


NetHunter KeX server sessions:

X DISPLAY #     RFB PORT #      RFB UNIX PATH   PROCESS ID # S
ERVER
1               5901                            19528        X
tigervnc

You can use the KeX client to connect to any of these displays
.
```

Creating tap using RJ45 Cables

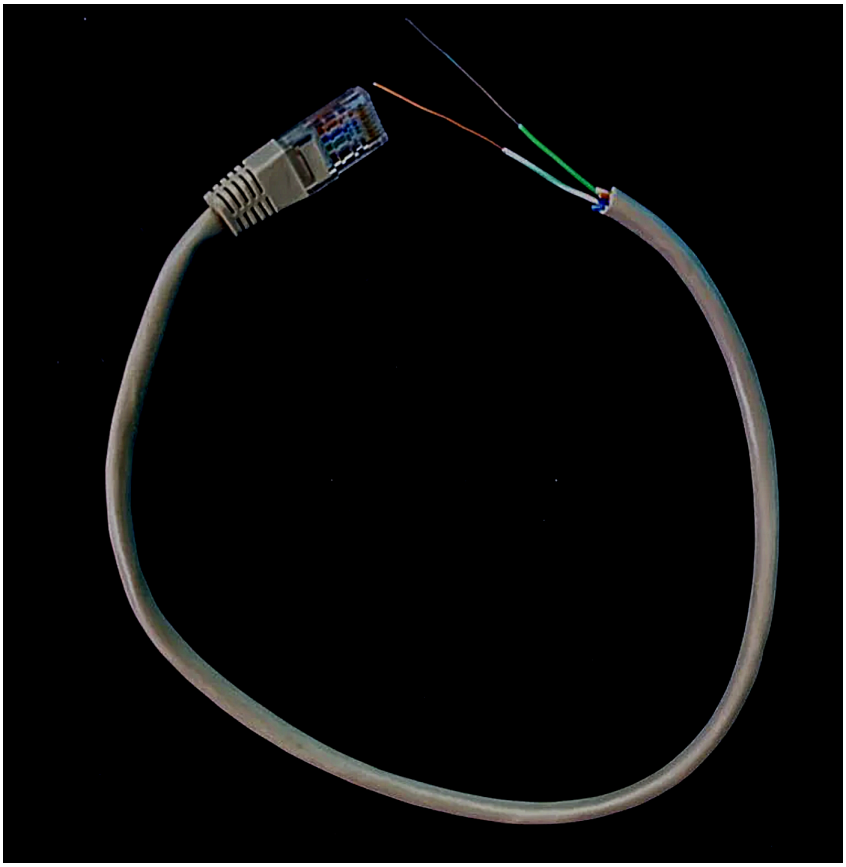


Step 1 : Splicing and connecting two RJ45 cables to facilitate data transmission between a host and router.





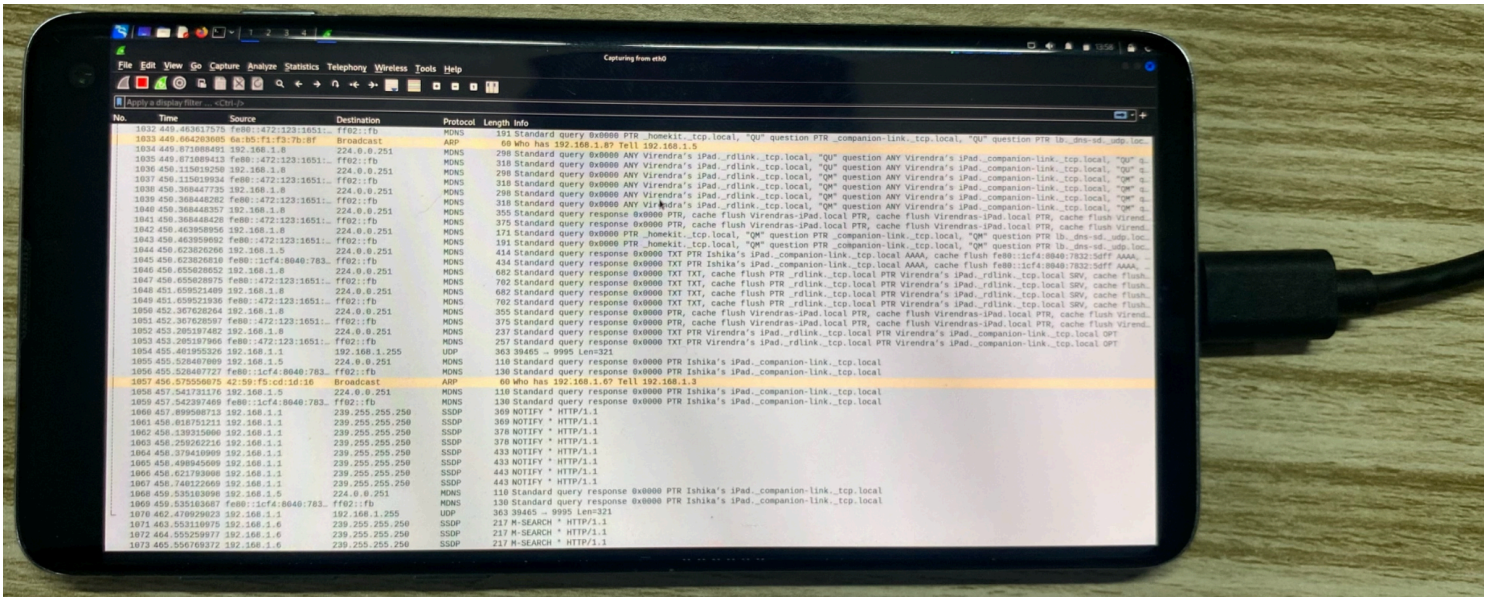
Step 2 : Connect the tap wire, which is linked to an Android phone running Kali Nethunter, to the wire carrying data from the router to the host.

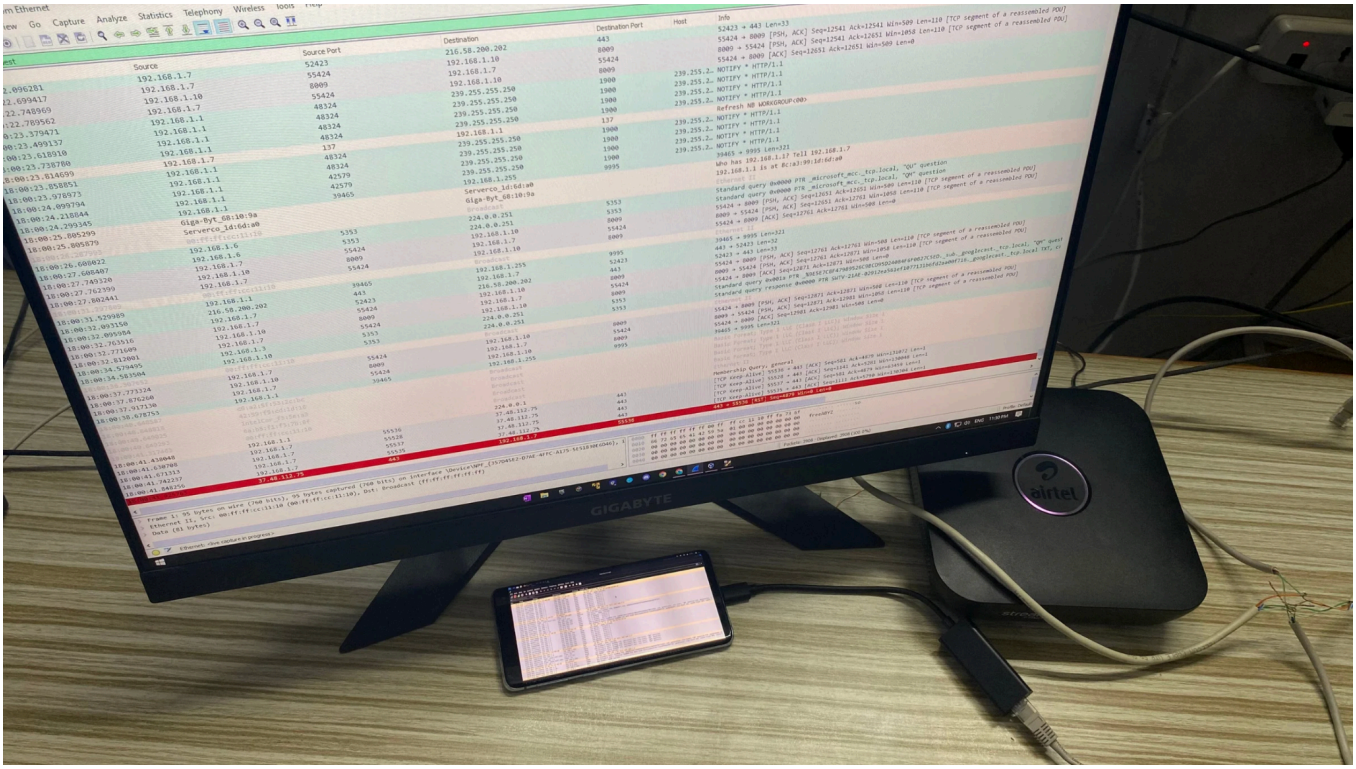


Starting the Capture

Step 1 : Connect the phone to wiretap by a Type-C to Ethernet dongle.

Step 2: Open Wireshark and start capturing.





Conclusion

In conclusion, the Ethernet Wiretap was successful in the objective of discreetly intercepting data packets within the network while remaining undetected by security measures like Network Access Control (NAC). By addressing the challenges of compactness and discretion, the wiretap ensures undetected integration into the network infrastructure without raising any suspicion.

The .pcap file generated by wireshark can be later accessed and analyzed to footprint and identify the endpoint devices within the network. This solution not only provides penetration testers with critical insights into communication protocol and device information but also test the efficacy of various network security solutions put in place such as firewalls and intrusion detection system.

In a rapid evolving digital landscape, where the security of interconnected systems is paramount, the Ethernet Wiretap can enhance the process of proactive security assessments by delivering a tool that can go undetected while capturing all the data flowing through the network that can be used by a bad actor to launch a sophisticated attack. This project provides a vital tool to security professionals and organization striving to fortify their network against unforeseen threat.

References

[1] Patel, Nimisha & Patel, Rajan & Patel, Dhiren. (2009). Packet Sniffing: Network Wiretapping. IEEE International Advance Computing Conference (IACC 2009) Patiala, India, 6–7 March 2009. 2691-2696.

[2] Shang, Zhihui & Zhang, Tao & Cai, Yueming & Yang, Weiwei & Wu, Hao & Yu, Zhang & Tao, Liwei. (2020). Secure Transmission in Cognitive Wiretap Networks with Full-Duplex Receivers. Applied Sciences. 10. 1840. 10.3390/app10051840.

[3] Branch, Philip & Pavlicic, A. & Armitage, G.. (2004). Using MAC Addresses in the Lawful Interception of IP Traffic.

[4] Carnut, Marco & Gondim, Joao. (2003). ARP SPOOFING DETECTION ON SWITCHED ETHERNET NETWORKS: A FEASIBILITY STUDY.

[5] Jason Rollette (2008). PASSIVE NETWORK TAP. https://hackaday.com/2008/09/14/passive-networking-tap/

[6] Alex Hoyland (2007). A Standalone Ethernet Packet Sniffer. http://ee.bradley.edu/projects/proj2007/dsniff/proposal.pdf