Cybersecurity Solutions- Pocket Tools for Cyber Well-being

Siddhi Jadhav[1], Prachit Save[2] Abhijit Vadu[3] , Anshul Jha[4], Dr. Pandharinath Ghonge[5], Shilpa Katre[6]

[1,2,3,4] Student,Department of Electronics and Telecommunication Engineering, (University of Mumbai) St. John College of Engineering and Management Palghar, India
[5] HoD, Department of Electronics and Telecommunication Engineering, (University of Mumbai) St. John College of Engineering and Management Palghar, India
[6] Assistant Professor, Department of Electronics and Telecommunication Engineering, (University of Mumbai) St. John College of Engineering and Management Palghar, India

---***---

Abstract— *In an era marked by increasing dependence on computational technologies, the security of computer based-systems and networks has became preeminent. The primary objective is to detect and prevent various breaches, ensuring the accuracy of data and privacy of data. This project leverages the stout capabilities of the Raspberry Pi 3B+ and to turn it into Mini computer which is very compact device. A customized Linux-based operating system is employed to provide a reliable and adaptable software environment for the system. A user-friendly interface is developed to allow system administrators to analyze network activity, configure reliable policies, and receive alerts in real-time. The cybersecurity solution includes active defense mechanisms to mitigate imminences, such as blocking malicious IP addresses, isolating compromised devices, and implementing firewall rules. This project's approach to cybersecurity emphasizes a provident and multi-layered strategy to safeguard virtual property. By combining the computational power of the Raspberry Pi, the safety features of Linux, and the flexibility of Node-MCU, this solution serves a scalable and cost-effective means of countering cyber perils. The proposed system is expected to contribute significantly to enhance cybersecurity and securing vital data in a variety of environments, from home networks to a small and medium-sized occupations. Furthermore, it offers as a precious learning source of supply for particular interested in cybersecurity. This project represents a step forward in the ongoing battle to secure electronic ecosystems and preserve the accuracy of data in an increasingly unified world.*

Keywords: Cybersecurity1, virus2, Vulnerabilities3, Raspberry Pi 3B+ 4, Honeypot5, USB Rubber Ducky6, Kali Linux7, prevention8

I. Introduction

Cyber Security is a operation to shield interconnected networks apparatuses from foreign danger. The world of digital safety spins around the business standard of secrecy of data, consistency of data, and accessible data, or CIA. Secrecy means data can be accessed only by licensed associations. Data consistency means data can be adjunct, mutated, or detached only by licensed users. Accessible proofs means systems, activities, and information must be available on-demand according to approved criterion. Cyber safety could be described as the mode to simplify the safety dreads aiming to keep safe repute damage [1]

By general observation we saw getting various bombards on wireless fidelity system, sometimes uncertified users get linked, numerous times we use public open wireless network so our safety can be compromised.

This project incorporates of showcasing various types of bombard and to establish explication on it to eliminate the risk and to stay inviolable in computational world

II. About the CYBERSECURITY

A. Introduction to Cybersecurity

Cyber protection is the hone of safeguarding structured, organization, and programs from progressive invasion. These cyberattacks are more often than not acute at approaching to, reforming, or pulverizing touchy data extortion customer receipts by means of ransomware; or hindering typical trade forms. Implementing viable cybersecurity procedure is especially challenging nowadays since there are more devices than individuals, and invaders are getting to be more imaginative. Cyber safety can also be determined as a procedure and tactics that are crafted to fortify cybernetics materials and electronic data against the menaces[2].

B. Importnce of Cybersecurity

Nowadays we live in a computerized period where all angles of our lives depend on the organize, computer and other electronic gadgets, and computer program applications. All basic foundation such as the keeping money framework, healthcare, money related terms, governments, and fabricating businesses utilize gadgets associated to the Web as a center portion of their operations. A few of their data, such as mental property, monetary information, and individual information, can be delicate for unauthorized get to or introduction that seems to have negative results. This data gives gatecrashers and danger performing artists to penetrate them for budgetary pick up, blackmail, political or social thought processes, or fair vandalism. the constituent that are binding to information security are guarded provision of illegitimate entry loss of assets changing content illegal activities databases technology hardware machines computers media and other systems that depend on information data and software.[3]

Cyber-attack is presently a global solicitude that hacks the construction, and other reliability violence seems imperil the global financial state. In this manner, it is basic to have a fabulous cybersecurity procedure to ensure touchy data from high-profile reliability breaches. Besides, as the volume of intrusion develop, association and organizations, particularly those that bargain with data related to national defense, wellbeing, or money related chronicle, got to utilize solid cybersecurity actions and forms to secure their delicate commerce and individual data.

III. CYBERSECURITY GOALS

Cyber Security's basic aim is to covenant data aplomb. The invulnerabilities community gives a triangle of three related criterions to ensure the information from cyber-attacks. This rule is called the CIA group of three. The CIA demonstrate is planned to direct proposal for businesses data security foundation. When any security breaches are found, one or more of these criterion have been damaged.

Able to break the CIA demonstrate into three parts: Let us examine each portion in detail.

A. *Confidentiality*

It is comparable to unassailability that maintains a pivotal distance from an illicit get to of data. It includes guaranteeing the data is open by those who are permitted to utilize it and blocking get to others. It anticipates basic data from coming to the off-base personalized. Data encryption is a great case of guaranteeing confidentiality.

B. *Intergrity*

This concept ensures that the data is authenticate , exact, and shielded from illicit alteration by danger performing artists or inadvertent client alteration. In case, any adjustments happen, certain measures ought to be taken to guarantee the touchy data from debasement or misfortune and rapidly recuperate from such an occasion. In addition, it shows to create the source of data veritable.

C. *Availability*

This makes the source to be attainable and main for its validate people continuously. It guarantees that these get to are not prevented by framework breakdown or cyber-attacks.

IV. METHODOLOGY

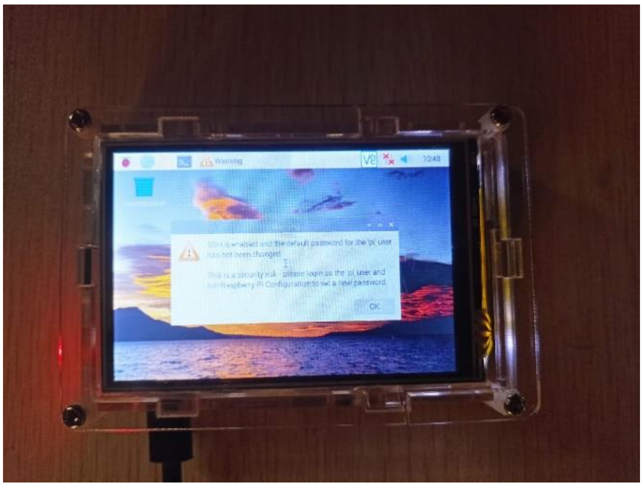
Here we have designed and developed a technological proposition for auditing privately owned portable electronic device hardware for backdoors and vulnerabilities. The solution has the capability to audit embedded as well as third-party integrated hardware. In this project we have demonstrated the attacks and developed solutions on it to eliminate the risk and to stay safe.

These are the integral parts of project paper:

A. *Mini Computer:*

With help of Raspberry Pi 3B+ board we have constructed our own mini pocket computer. Which is compact & handy & can be carried in pocket. This mini computer will be used as a portable device and functions similar like a conventional computer.

We have installed Raspbian OS in it to enable raspberry Pi 3B+ as a Mini Computer. A3.5 TFT screen is mounted on Raspberry Pi 3B+ to operate Mini Computer with an ease.



SSH is enabled and the default password for the 'pi' user has not been changed.

This is a security risk - please login as the 'pi' user and run Raspberry Pi Configuration to set a new password.

Fig. 1. Mini Computer

The device is so super-convenient that it analyzes a variety of various networks [4]

B. USB Rubber Ducky:

USB rubber ducky is for social awareness to make users aware about USB port attacks. We often use USB ports of Computers to connect USB devices to share the data. We use Public Power Bank Stations sometimes which are nowadays available on Railway Stations, Airports, Hospitals etc. to charge our devices by using USB port enabled chargers. We do these things without any awareness and slight idea that our devices can be hacked by malicious attackers with help of tools like USB Rubber ducky, Bad USB etc. Here with help of ATTiny 85 Board we have developed USB rubber ducky. We have generated a C language script and then we have generated Payloads for USB rubber ducky. Then by connecting such USB rubber ducky we have demonstrated how attackers can attack the system

It is a USB device that is exploited by an intruder so that when detected by the aimed computer this end-device will be identified as an ordinary USB connection end-device [7]

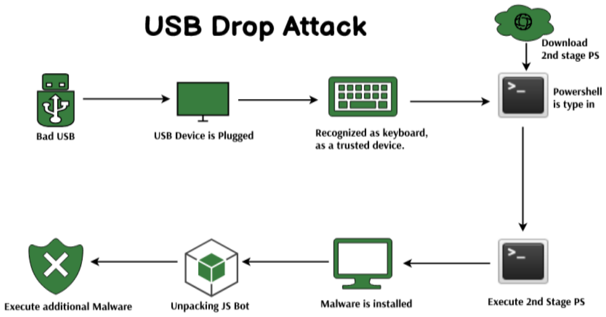


Fig. 2 . Block diagram of USB Rubber ducky

C. Wi-Fi Repeater:

It is used to elongate the area of your network. It works by obtaining your active signal, intensifying it and then sending the amplified signal. With a Wi-Fi repeater you can suitably dual the service area of your wireless network - reaching far of your workplace.

As of today, the internet is very essential as it can be the source for limitless amount of information. For some places that has low coverage area, cut-off communication can be happened during certain happenings such as when natural hazards occurs which affecting communication structure. To ensure a uninterrupted communication, signal's coverage should be extended [8]

D. Honeypot:

In cybersecurity a honeypot is a tool build to analyze divert or otherwise mitigate illicit access to information systems essentially a honeypot simulates genuine data or resources within a network or website enticing potential intruders while appearing legitimate these honeypots are actually segregated environments meticulously examine and equipped to either block or analyze any malicious activity from intruders these concept draws parallels to police sting operations or undercover operations aimed at apprehending criminals where bait is used to lure suspects into revealing their intentions or committing unlawful acts . We have used Kali Linux OS to setup a honeypot with the help of Linux Commands and Shell Scripting.

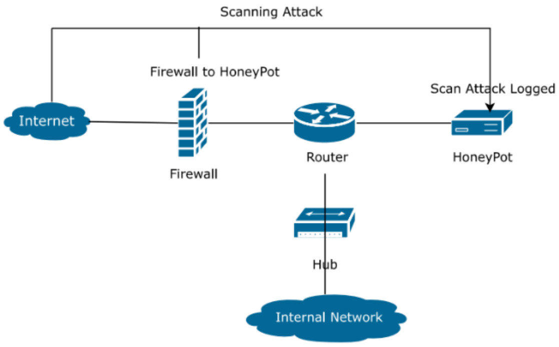


Fig. 3.1. Block diagram of Honeypot

Honeypots industrial networks do the job of attracting invaders[11]

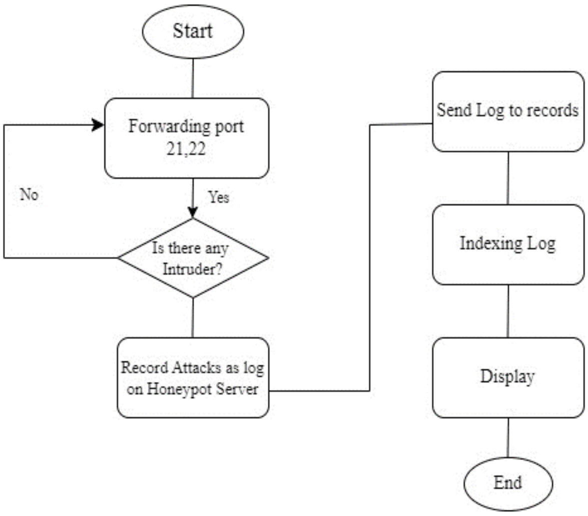


Fig. 3.2. Flowchart of Honeypot

Installing Kali Linux to Set up Honeypot

It is divided into three parts
1. Setting up Environment for Running Kali Linux
2. Installing and Running Kali Linux on it
3. Setting up Honeypot on Kali Linux

Part 1.
Setting up Environment for Running Kali Linux
Step 1
Open the browser and Search for Virtual Box

Step 2
Click on www.virtualbox.org
And install it

Part 2.
Installing and Running Kali Linux on Virtual Box
Step 1
Search for www.kali.org on browser and Click on it

Step 2
Under Prebuilt Virtual Machines
Select bit file(32 bit or 64 bit) as per OS of the PC (Here it's 64 bit)

Step 3
Open the extracted Kali Linux folder

Step 4
Two files with extension
i. .vbox
ii. .vdI
Can be seen

Step 5
Open the Virtual Box which was installed previously

Step 6
Open extracted Kali Linux folder again

Step 7
Double click on .vbox file

Step 8
Open Virtual Box again

Step 9
A Kali Linux file can be seen on Left Hand Side Window on Virtual Box

Step 10
Click on Kali Linux file in Virtual Box

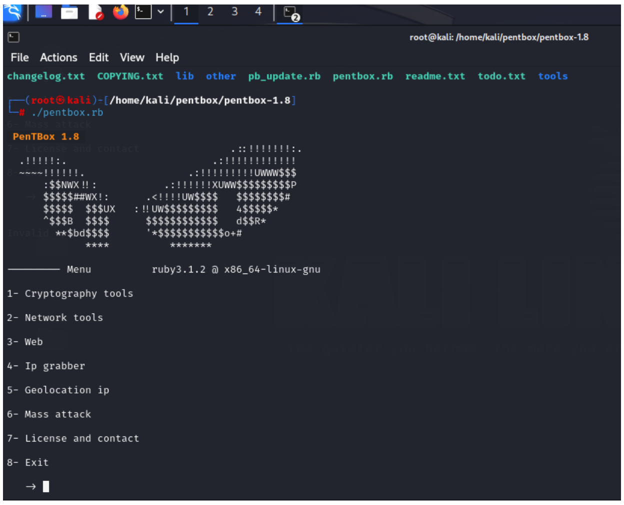
Step 11
Click on Start button
Now Kali Linux can be used

Part 3.
Setting up Honeypot on Kali Linux
Step 1
Open Virtual Box and Start Kali Linux on it

Step 2
The pentbox has been installed now in Kali Linux

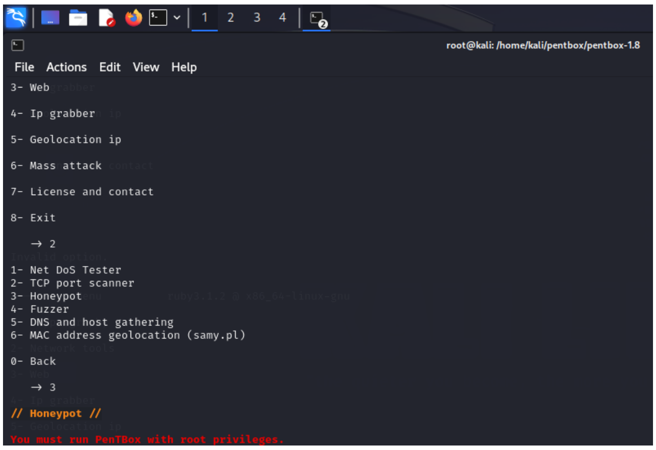
Step 3
Now a Honeypot can be set in Kali Linux using Pentbox tool

Step 4
Open pentbox and run it using following commands


1 2 3 4
root@kali: /home/kali/pentbox/pentbox-1.8
File Actions Edit View Help

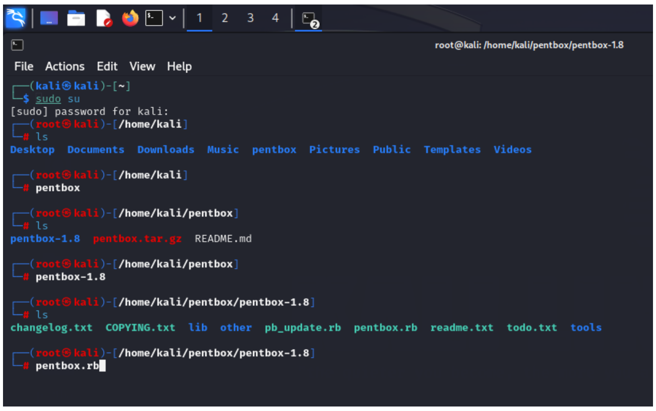
```
changelog.txt  COPYING.txt  lib  other  pb_update.rb  pentbox.rb  readme.txt  todo.txt  tools

┌──(root㉿kali)-[/home/kali/pentbox/pentbox-1.8]
└─# ./pentbox.rb

 PenTBox 1.8
                                              .:: !!!!!!!:.
  .!!!!!:.                                 .:!!!!!!!!!!!!
  ~~~~!!!!!!.                          .:!!!!!!!!!UWWW$$$
      :$$NWX!!:                    .:!!!!!!XUWW$$$$$$$$$P
      $$$$$##WX!:              .<!!!!UW$$$$    $$$$$$$$#
      $$$$$  $$$UX        :!!UW$$$$$$$$$$    4$$$$$*
      ^$$$B  $$$$          $$$$$$$$$$$$    d$$R*
        **$bd$$$$          '*$$$$$$$$$$$o+#
             ****              *******

──────── Menu          ruby3.1.2 @ x86_64-linux-gnu

1- Cryptography tools

2- Network tools

3- Web

4- Ip grabber

5- Geolocation ip

6- Mass attack

7- License and contact

8- Exit

   → █
```

Step 5
Select Network Tools

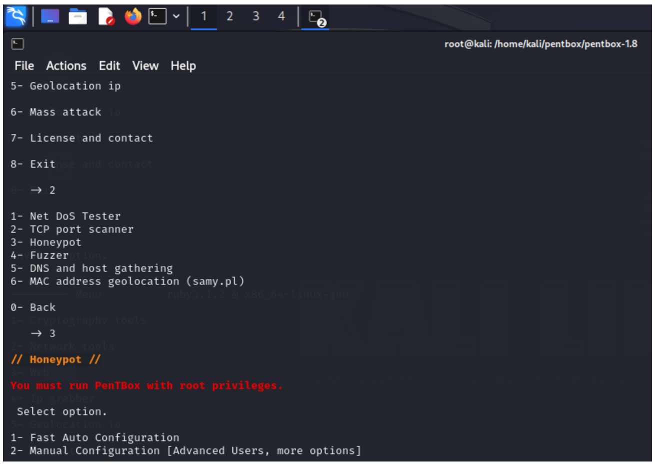

1 2 3 4
root@kali: /home/kali/pentbox/pentbox-1.8
File Actions Edit View Help

```
3- Web

4- Ip grabber

5- Geolocation ip

6- Mass attack

7- License and contact

8- Exit

   → 2

1- Net DoS Tester
2- TCP port scanner
3- Honeypot
4- Fuzzer
5- DNS and host gathering
6- MAC address geolocation (samy.pl)

0- Back

   → 3

// Honeypot //

You must run PenTBox with root privileges.
```

Step 6
Select Honeypot & then Select fast Auto Configuration

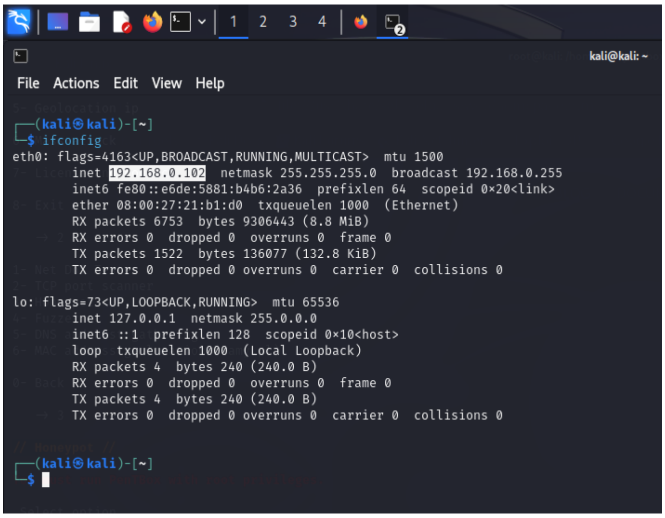

1 2 3 4
root@kali: /home/kali/pentbox/pentbox-1.8
File Actions Edit View Help

```
┌──(kali㉿kali)-[~]
└─$ sudo su
[sudo] password for kali:
┌──(root㉿kali)-[/home/kali]
└─# ls
Desktop  Documents  Downloads  Music  pentbox  Pictures  Public  Templates  Videos

┌──(root㉿kali)-[/home/kali]
└─# pentbox

┌──(root㉿kali)-[/home/kali/pentbox]
└─# ls
pentbox-1.8  pentbox.tar.gz  README.md

┌──(root㉿kali)-[/home/kali/pentbox]
└─# pentbox-1.8

┌──(root㉿kali)-[/home/kali/pentbox/pentbox-1.8]
└─# ls
changelog.txt  COPYING.txt  lib  other  pb_update.rb  pentbox.rb  readme.txt  todo.txt  tools

┌──(root㉿kali)-[/home/kali/pentbox/pentbox-1.8]
└─# pentbox.rb█
```


root@kali: /home/kali/pentbox/pentbox-1.8
File Actions Edit View Help

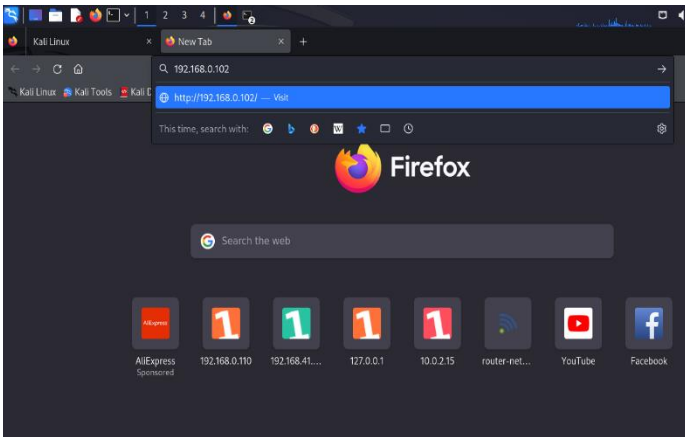
```
5- Geolocation ip

6- Mass attack

7- License and contact

8- Exit

   → 2

1- Net DoS Tester
2- TCP port scanner
3- Honeypot
4- Fuzzer
5- DNS and host gathering
6- MAC address geolocation (samy.pl)

0- Back

   → 3

// Honeypot //

You must run PenTBox with root privileges.

 Select option.

1- Fast Auto Configuration
2- Manual Configuration [Advanced Users, more options]
```

Step 7
Locate IP Address of Device using “ifconfig” command & copy the IP Address

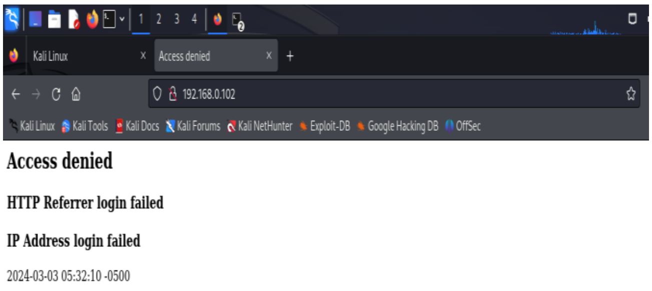


```
┌──(kali㉿kali)-[~]
└─$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.0.102  netmask 255.255.255.0  broadcast 192.168.0.255
        inet6 fe80::e6de:5881:b4b6:2a36  prefixlen 64  scopeid 0×20<link>
        ether 08:00:27:21:b1:d0  txqueuelen 1000  (Ethernet)
        RX packets 6753  bytes 9306443 (8.8 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 1522  bytes 136077 (132.8 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0×10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 4  bytes 240 (240.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 4  bytes 240 (240.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

┌──(kali㉿kali)-[~]
└─$ 
```

Step 8
Open the browser and paste selected IP address and press Enter



Step 9
Honeypot is activated now and because of it Intruder can’t access browser where Honeypot is set



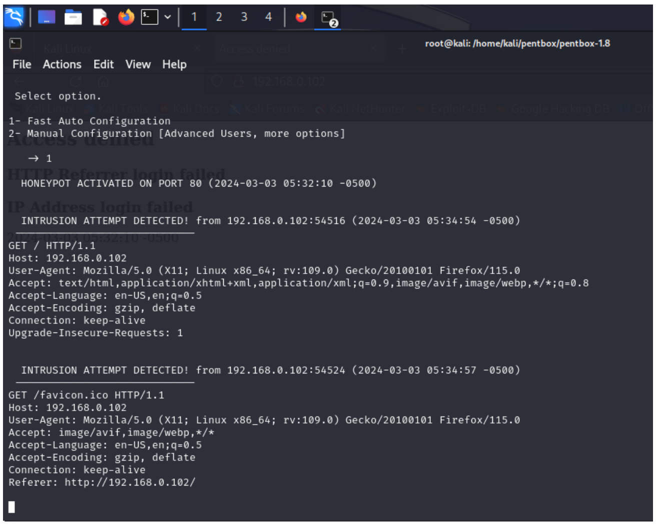
Access denied

HTTP Referrer login failed

IP Address login failed

2024-03-03 05:32:10 -0500

Step 10
Open terminal again and one can see all the information regarding intruder who tried to access where HoneyPot was set


root@kali: /home/kali/pentbox/pentbox-1.8
File Actions Edit View Help

```
 Select option.

1- Fast Auto Configuration
2- Manual Configuration [Advanced Users, more options]

   → 1

  HONEYPOT ACTIVATED ON PORT 80 (2024-03-03 05:32:10 -0500)

  INTRUSION ATTEMPT DETECTED! from 192.168.0.102:54516 (2024-03-03 05:34:54 -0500)
 ─────────────────────────────
GET / HTTP/1.1
Host: 192.168.0.102
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: keep-alive
Upgrade-Insecure-Requests: 1


  INTRUSION ATTEMPT DETECTED! from 192.168.0.102:54524 (2024-03-03 05:34:57 -0500)
 ─────────────────────────────
GET /favicon.ico HTTP/1.1
Host: 192.168.0.102
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: image/avif,image/webp,*/*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: keep-alive
Referer: http://192.168.0.102/

█
```

ACKNOWLEDGEMENT

It is a great pleasure to acknowledge that those who have extended their support and contributed time for completion for their dissertation work.

We are thankful to Dr. Pandharinath Ghonge, HoD, Electronics and Telecommunication Engineering Department, SJCEM, Palghar, and Mrs. Shilpa Katre, Asst.Professor, Electronics and Telecommunication Engineering Department, SJCEM, Palghar, for timely guidance and inspiration without which our work would not have been completed.

Also, we would like to thank all members of Electronics and Telecommunication, EXTC Dept,librarian, our college and friends who have helped us directly or indirectly to complete this project.

CONCLUSION

In conclusion, our project to build a mini computer with help of Raspberry Pi 3B+ to make it as a compact device. Cybersecurity is an ever-evolving field, and with the increasing sophistication of threats, it is crucial to develop innovative solutions to protect digital infrastructure. It empowers users with an efficient and cost-effective means of protecting their digital assets.

As we continue to innovate and adapt to emerging threats, we are contributing to a safer and more secure digital environment for all. With dedication, collaboration, and ongoing commitment to cybersecurity, we can stay one step ahead of the cyber threats that we face in our increasingly interconnected world.

RESULT

The developed mini computer is capable of delivering normal tasks like a normal computer. The Raspbian OS can be used for similar functions like other operating systems.

The AT-Tiny 85 board is used to make USB Rubber Ducky so to make people aware about USB vulnerabilities.

The Wi-Fi Repeater which is made with help of Node MCU is capable of delivering similar functions like Wi-Fi extenders but with cheaper rate and more compactness.

The Honeypot which has been set is capable of catching and blocking the malicious attacker who is trying to intrude the system.

FUTURE SCOPE

The mini-computer which is developed can further be modified by installing in-built battery in it which will make system more mobile and user need not carry any power bank for external power supply.

With help of higher versions of Raspberry pi a more refined mechanism for more refined assignments can be developed

A small vent fan or a heat-sink can be installed which will deduct overall heat level of the system.

A software system can be developed which can detect the bad USB which will alert users from potential rubber ducky attack.

REFERENCES

[1] A. Sheth, S. Bhosale, F. Kurupkar, “Research paper on cyber security”, April 2021.

[2] S. Komakula, M. Jagadeeshwar, “Recognition of identity theft in cyber security by using Confidentiality tools”, August 2021.

[3] M. Tisma, J. Andric, “Importance of cyber security awareness and e-learning motivation for cyber security in reshaping the education”, December 2021.

[4] A. Unda, A. Vera, L. Haz, V. Pinos, R. Zurita, S. Medina, “The Raspberry Pi as a Computer Substitute at Elementary Schools in Developing Countries: A Pilot Experiment in Ecuador”, *Raspberry Pi nano computer is a very good choice to build computer labs with a low cost and efficient approach(1), the device needs a heat sink and a fan(2)* , 2018.

[5] E. Neyadi, S. Shehhi, A. Shehhi, N. Hashimi, M. Qbea'H, S. Alrabaee, “Discovering Public Wi-Fi Vulnerabilities Using Raspberry pi and Kali Linux”, *public Wi-Fi is vulnerabilities(1), why public Wi-Fi is vulnerable and the possible attacks that are made possible due to such lack of security(2),* 2020.

[6] I. Astaburuaga, A. Lombardi, B. Torre, C. Hughes, S. Sengupta, “Vulnerability Analysis of AR.Drone 2.0, an Embedded Linux System”, *analyze vulnerabilities and flaws in the system(1), data verification mechanisms(2),* 2019.

[7] A. Muslim, A. Budiono, A. Almaarif, “Implementation and Analysis of USB based Password Stealer using PowerShell in Google Chrome and Mozilla Firefox”, *Rubber Ducky using Bad USB(1), USB Password Stealer device(2),* June 2020.

[8] N. S. Ismail, NE Abd Rashid, N. A. Zakaria, Z Ismail Khan, A.R. Mahmud, “Low Cost Extended Wireless Network Using xRaspberry Pi 3B+”, *Raspberry Pi can be used to act as the access point and extend the distance of an existing network signal by bridging the network using the Ethernet cable*(1), 2020.

[9] T. Adame, m. Carrascosa, b. Bellalta, i. Pretel, i. Etxebarria, “Channel Load Aware AP / Extender Selection in Home WiFi Networks Using IEEE 802.11k/v” *‘Smart scanning for mobile devices(1),*Feb 2021.

[10] A. Pashaei,M. E. Akbari “IDS Performance through Early Detection Approach” , *Honeypot IDS systems vulnerabilities are used as a trap and weakness in terms of protocol security structure to deceive and attract attackers to collect intruders*(1), *installing honeypots on systems to encourage attackers to work on these systems without the knowledge of the traps*(2), August 2022.

B. Park, S. Dang, S. Noh, J. Yi, M. Park, “Dynamic Virtual Network Honeypot”, *trapping hackers, track and analyze new hacking methods(1), system dynamic manages virtual honeypot and provides honeypot when Network IDS detects a new attack(2),* 2019.