INTERNATIONAL JOURNAL OF ADVANCE RESEARCH, IDEAS AND INNOVATIONS IN TECHNOLOGY

ISSN: 2454-132X
Impact Factor: 6.078

(Volume 7, Issue 3 - V7I3-1265)
Available online at: https://www.ijariit.com

AMUNET: Advanced multi utility network evaluation toolkit

Karthik S. K.
karthiksudeep99@gmail.com
Marian Engineering College, Trivandrum, Kerala

Nikhil Robinson
nikhilrobinson2000@gmail.com
Marian Engineering College, Trivandrum, Kerala

Asha Shaji
asha4mars@gmail.com
Marian Engineering College, Trivandrum, Kerala

Navaneeth V. H.
navaneethvijayahari10@gmail.com
Marian Engineering College, Trivandrum, Kerala

Preetha S. L.
preetha.nair.s@gmail.com
Marian Engineering College, Trivandrum, Kerala

ABSTRACT

Cybercrime is the greatest threat to every individual in the world. In the upcoming years, it might become a serious threat to every person, place and organisations around the globe. During this pandemic situation, hackers exploited the opportunity to attack vulnerable networks of many organisations and breached their data. This proves that we are also in the midst of an epidemic of cybercrime. To solve this problem, we are proposing an AI powered security device called AMUNET (Advanced Multi Utility Network Evaluation Toolkit). It uses artificial intelligence and machine learning to detect various problems in a network and protects against various vulnerabilities and exploits. It can even monitor live network packets and detect intrusions and take steps to prevent intrusion attacks.

Keywords— *AI in Cybersecurity, IDPS using Machine Learning, Auto Vulnerability Scanner, Network Security*

1. INTRODUCTION

Cybercrimes are increasing day by day. We live in a world where every devices and machines that we use in daily life are connected to the internet. With the development of IOT all the devices starting from our mobile phones and computers to televisions are linked to the internet to make our lives easier. But they have also led to the increase of cybercrimes. Things have gone to a situation where any cyber expert can access our private information and activities. Cybercrimes are also a threat to organisations as their data are no longer safe if proper security measures are not undertaken. Cyber criminals does not use one but a variety of methods to breach vulnerable networks. , it is difficult to prevent a breach with just few security measures. AMUNET provides a solution to these problems. It is a highly sophisticated device incorporating many security features such as IDS, IPS, Firewall, etc. It uses state of the art AI which adapts and learn continuously. AMUNET provides an additional layer of support for your network devices. Our aim is to bring cybersecurity awareness to the common people. The hurdle was to create a device which is advanced and can be operated by normal and experts alike. So, we contemplated a device with plug and play capability which enables the user with easy setup and configuration.

AMUNET works on a 3-D framework we designed

- DEFEND
- DETECT
- DIAGONOSIS

These are the fundamental working block of our device. AMUNET is connect to live network traffic. It creates a NAT bridge between the internet and the internal network devices so all the data flows through the AMUNET hiding the device's public IP address. Due to this all the network traffics flows through AMUNET which allows it to monitor and study the patterns and signature of data flow. So, by continuously monitoring the data flow AMUNET can defend against various intrusion attacks this forms the first 'D' of our framework which is DEFEND.

© 2021, www.IJARIIT.com All Rights Reserved

The main advantage of AMUNET is its AI engine which finds various vulnerability and exploits that are open in the network infrastructure. We used various exploits and signatures to train the model to identify the vulnerabilities very easily. AMUNET will initiate a host scan of all the connected devices and the results are stored in a database. Later on, AMUNET studies about each host and its characteristics and its packet flow. After reconnaissance AMUNET will perform vulnerability scan and DETECTS loop holes in the system. This is the second 'D' that is detect.

AMUNET not only find loopholes it also diagnoses it for available patches. If it is possible to solve, then AMUNET will initiate a patch or alert the user. This helps the network devices to be UpToDate and loophole free. We designed a prototype of AMUNET with the help of a RASPBERRY-PI 4B+ with 4GB ram and installed Debian Linux as the operating system. More technical details are available on the implementation part.

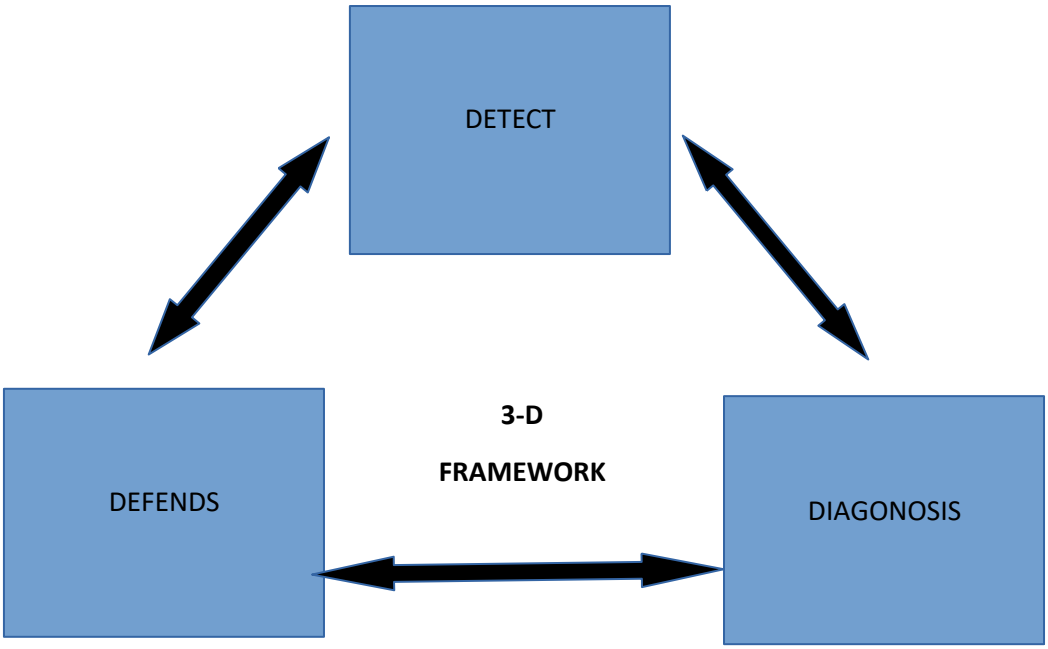

Chart-1: 3-D framework

2. IMPLEMENTATION

2.1 Hardware

We selected a raspberry pi 4b with 4gb ram as the core of our project because it's both portable and perfect for our POC. It comes with a 1.5 GHz 64-bit quad core ARM Cortex-A72 processor which gives the necessary computing power and system capabilities for our AMUNET with a clock speed of 600MHz. It has an on-board Broadcom BCM43438 wi-fi chipset which is capable of handling both 2.4GHz and 5.2Ghz with high-speed data transfer. It is also equipped with gigabit ethernet port. We also use an additional wi-fi adapter for creating access point for the client devices to connect to. For this purpose, we used a Leoxsys 150MBps USB wi-fi adapter with RALINK RT5370 chipset. We chose this chipset for enabling monitor mode.

2.2 NAT Connection

For monitoring of live packets flow the network should be set is a way that all the traffic from the client devices should pass through AMUNET. Network Address Translation helps us to achieve this. AMUNENT is connected directly to the wi-fi access point / router with ethernet cable. AMUNET then creates an access point for other clients to connect to with the help of hostapd, dnsmasq, and dhcpcd, AMUNET creates a self-hosted dhcp client and dns probes. AMUNET uses iptables for forwarding data between the 2 network interface cards wlan0 and wlan1

Fig 2.2.1: IP table rules

The above set of rules are applied to the iptables to enable IP forwarding from wlan0 to wlan1. The access point created by the AMUNET is protected by 16-bit alphanumeric characters with symbols. It also has features such as MAC filtering, Client isolation and DEAUTH detection which increases the security of the access point and prevent breaches.

© 2021, www.IJARIIT.com All Rights Reserved

2.3 IDS/IPS with Machine Learning

IDPS is a major plus point of the AMUNET. We teach our system to differentiate between normal traffic and malicious traffic. For achieving this we utilized CSE-CIC-IDS2018 dataset provided by the Canadian Institute for Cybersecurity. It was created by capturing all network traffic inside a controlled network environment on web server where realistic background traffic and different attacks were conducted. As a result, the dataset contains both normal traffics and attacks. We used various machine learning algorithms like Machine like k-nearest neighbours, random forest and SVM and deep learning models like convolutional neural networks, autoencoders and recurrent neural networks. AMUNET determines the pattern with readily trained data from the live network and gives an interrupt to block the IP address to the firewall and adds the IP address to the block list. We used python with pytorch keras NumPy and TensorFlow to build the machine learning model the data is trained outside the device with higher computational power and the trained data is stored in AMUNET's database. We also deployed a signature based IDPS using snort community rules which gives a failsafe and can verify the findings of the model by signature verification.

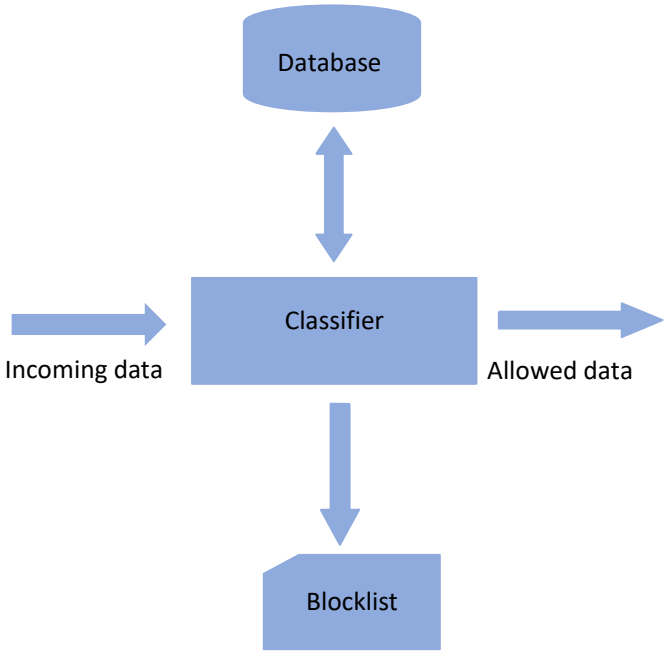

Chart-2: IDPS system

2.4 Honey pot

AMUNET is also packed with honeypot which acts as an easy target for the attackers. When an intruder tries to exploit it, the honeypot will log the user information into the database. It captures the information such as location, IP address, different methods used by the attacker and adds the IP address into the block list.

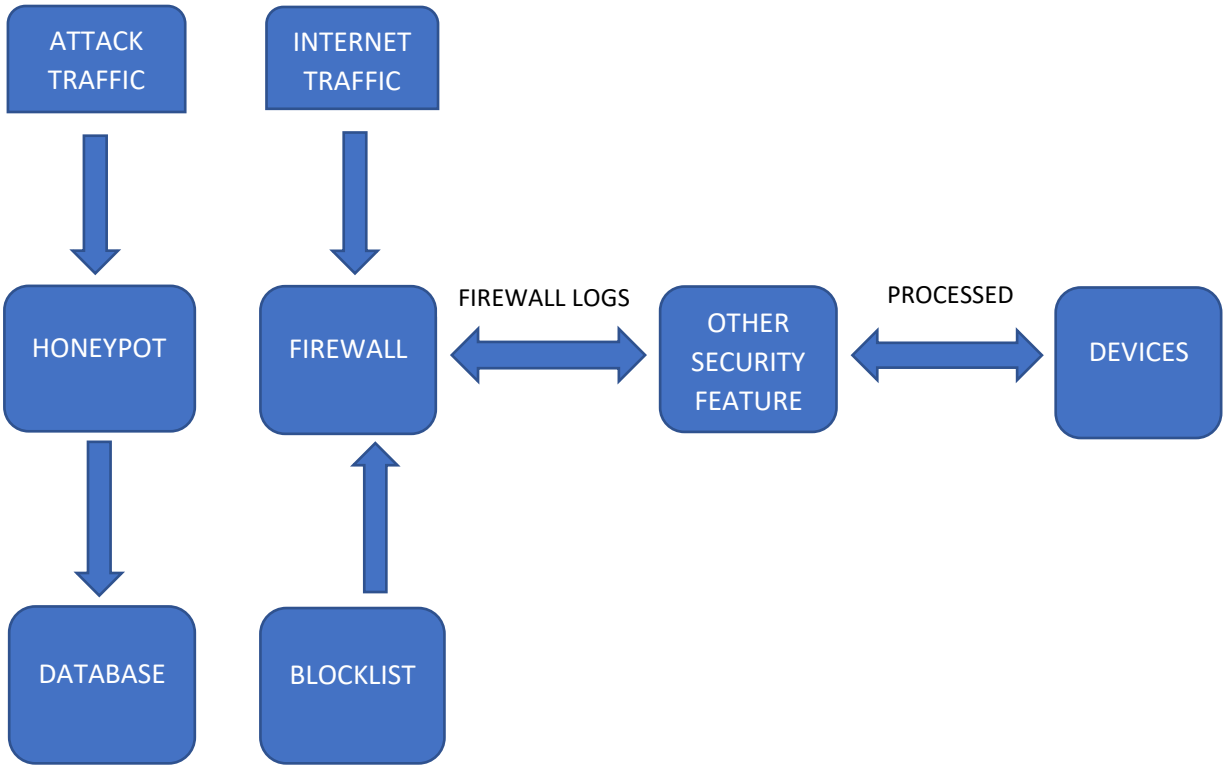

Chart-3: Honeypot block diagram

© 2021, www.IJARIIT.com All Rights Reserved

2.5 Vulnerability scanning of client devices

AMUNET learns how to exploit by itself using advanced machine learning model called A3C.The A3C consists of Multiple Neural Networks. It obtains the training server information such as the OS type, product name, product version, etc, as inputs of neural network, and outputs the Payload depending on the input information. If an optimal payload is received then the exploitation is successful.

In training, the model executes more than 10,000 exploits by altering the combination of the input information and delivers it to the training servers through Metasploit. Multithreading is used to shorten the training time. Depending on the exploitation results it revise the weights of the neural network, which will eventually optimize the neural network. Therefore, learning by using various training servers, AMUNET can execute accurate exploit according to various situations. Thus, AMUNET can accurately execute exploit in relation to different situation by learning using various servers. So, AMUNET uses training servers such as metasploitable3, metasploitable2, owaspbwa for learning. AMUNET finds the status of all opened ports on the target server and executes the exploit at pinpoint using Machine Learning. Its key features are following.

- Using Machine Learning AMUNET can perform pinpoint execution of exploits, at least in 1 attempt.
- If AMUNET is able to perform exploit to the target server, it will also execute the exploit to other internal servers.
- By using Reinforcement Learning AMUNET can learn how to exploit by itself.
- Since Reinforcement Learning takes a lot of time, AMUNET makes use of Distributed Learning by multi agents.
- For the exploitation to be successful it is important to collect the details of the software that operated on the target server. AMUNET can identify its name and version using the methods such as Intelligence gathering, Threat modelling, Vulnerability analysis, Exploitation, Post-Exploitation, Reporting, etc.

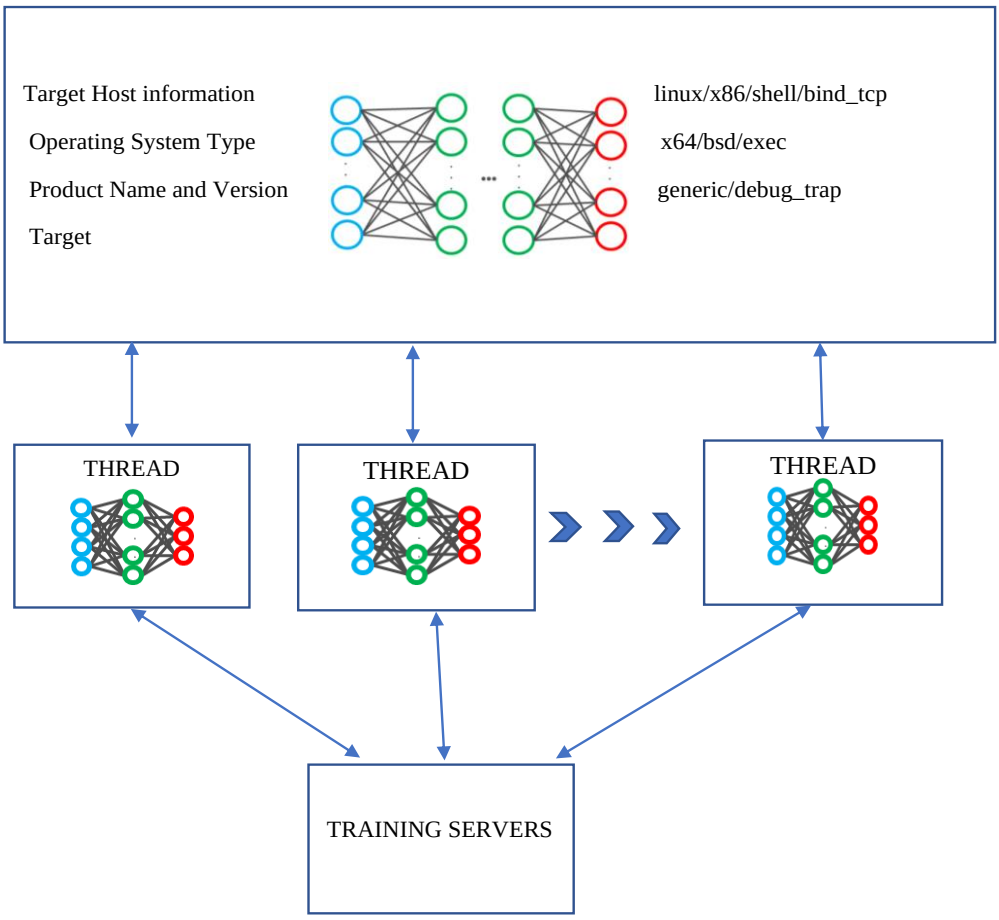

Chart-4: Vulnerability scanning framework

2.6 Generating Reports

All the logs generated by the IDS, IPS, Honey Pot, Vulnerability scan and other features are converted into a readable format that could be accessed by a user. These logs can be used to gain information like top denied hosts, pattern of the intrusions, top security events generated, etc.

2.7 User interface

AMUNET has a predefined user interface for accessing the internal core features and troubleshooting the errors the interface is designed as a CLI which can be accessed by SSHing into the AMUNET. A user can completely change the working of the current system and modify the various configuration files that are used by AMUNET. With additional root privileges the user can directly access the root of the Linux system and its file AMUNET comes with a failsafe which save all your config in a backup which user can restore if the file system was accidentally corrupted. There are several options available within the UI like configuring the IDPS, manual network scanning, add a VPN client, enable tor, change configuration of honeypot, view all the logs, and manual restart of services.

© 2021, www.IJARIIT.com All Rights Reserved

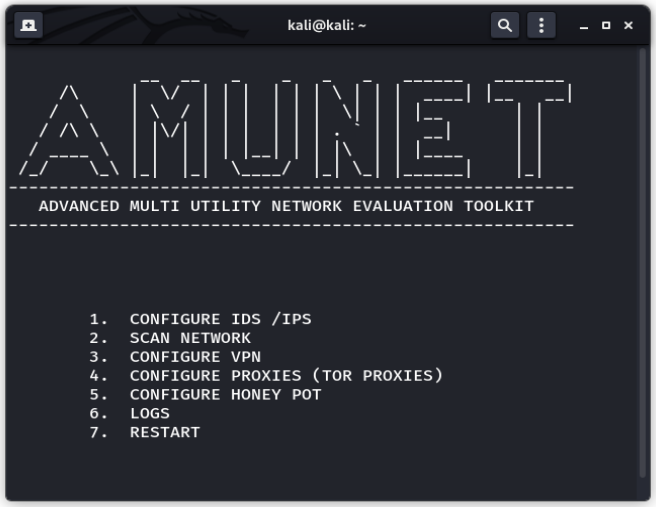

Fig 2.7.1: User Interface

3. RESULTS

3.1 Blocking the ping

AMUNET's IDPS system detects the flow of packets for the attackers IP and compare it with the trained model if an attack match is found the attackers IP is added into the block list and prevent future attacks all this is done automatically with the help of deep learning feature the below figure shows a ping flood from an attacker.

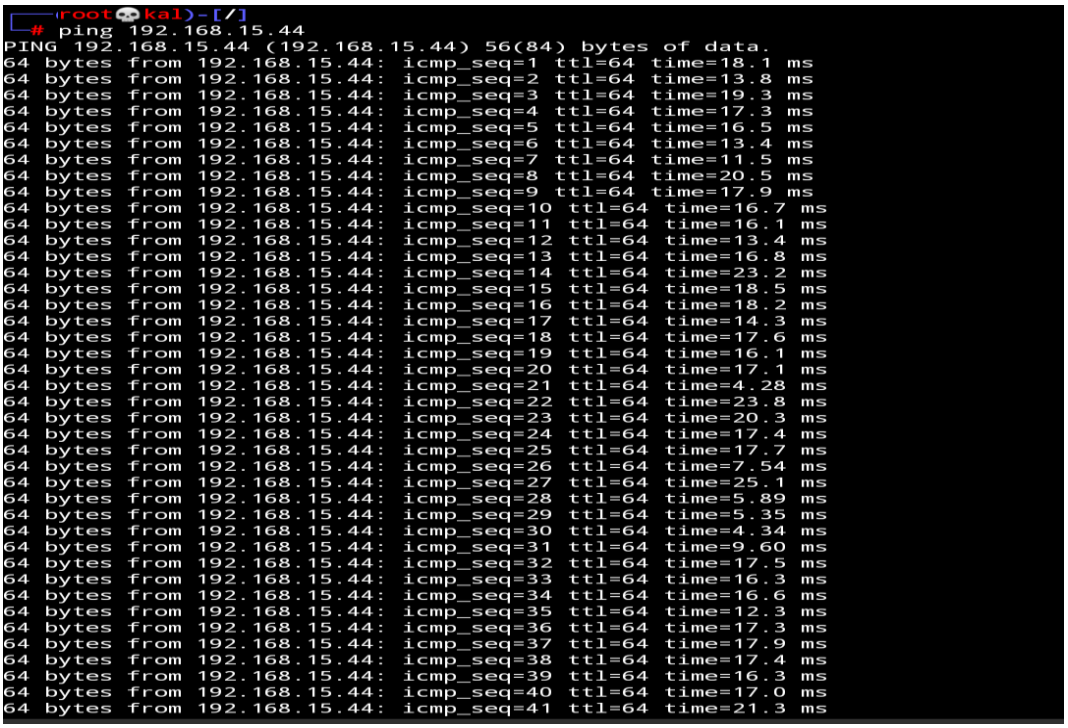

Fig 3.1.1: Ping scan

At first the data was passed and AMUNET's deep learning engine detects the packet flow which is shown in the figure below

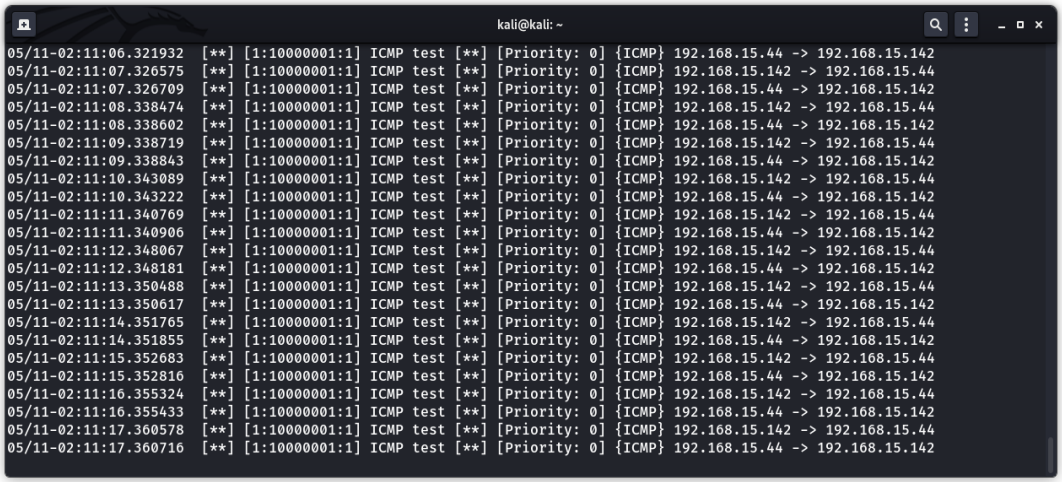

Fig 3.1.2: Detecting the ping request

© 2021, www.IJARIIT.com All Rights Reserved

We can see the source IP and destination IP and the type of packet flow within the same scope all this information are logged and passed to the internal deep learning engine which take action regarding the type of attack. If any attack flag is raised by the deep learning engine the IP address of the attacker is added to the firewall rules to block future attacks.

Fig 3.1.3: IP address blocked

After adding the IP address to block list we can see that the ping service stopped and the packets is 100% lost.

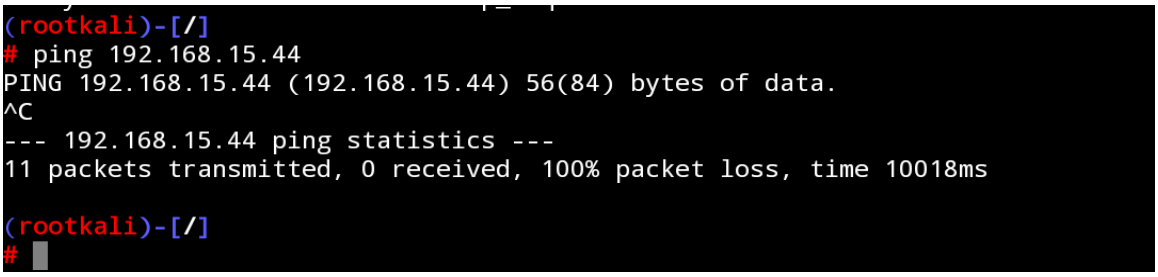

Fig 3.1.4: Ping request failure

3.2 Nmap scan

AMUNET protects from Nmap scan by filtering out all the open ports so the Nmap client cannot identify which all services are running on the system.

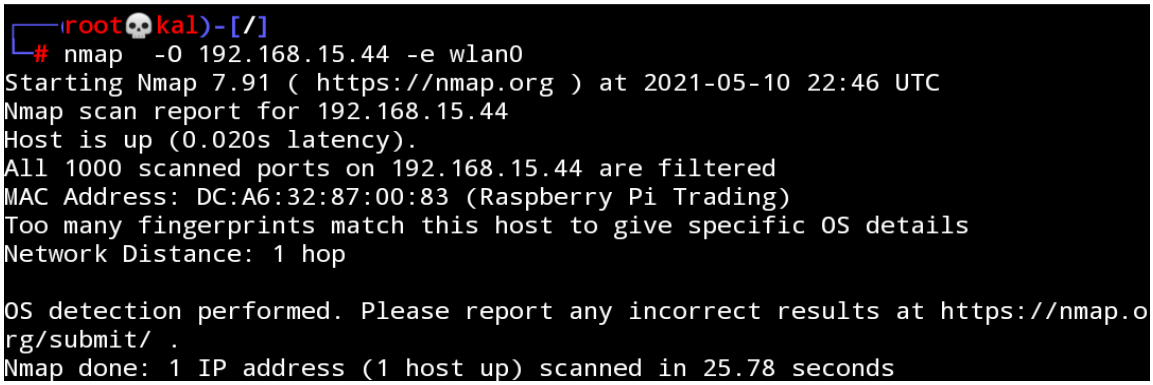

Fig 3.2.1: Nmap scan result showing filtered ports

The deep learning engine detects the port knocking and prevents sending acknowledgment thus filtering out ports from the Nmap scan.

3.3 Reverse_tcp payload attack Metasploit

One off the most dangerous attack is running a reverse_tcp payload attacks. To prevent this attack AMUNET allows only known host within the network itself to connect via reverse tcp and the deep learning engine scans for the IP that our device is connecting to and its data flow patterns is checked with already trained data preventing the attacker from getting a meterpreter shell on the target.

3.4 Vulnerability scan

AMUNET scan for devices using ARP tables with the command arp -a and finds all the devices connected to the interface.

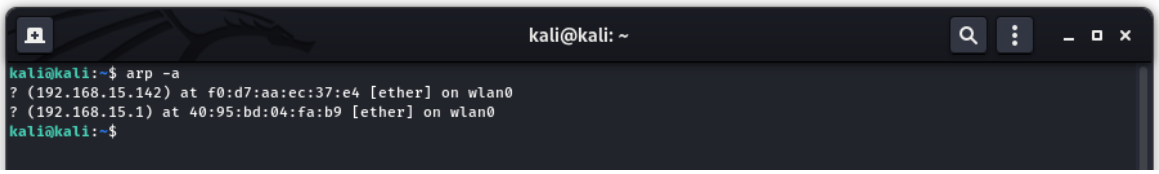

Fig 3.4.1: Host scan

The discovered host are saved to a file named host.txt

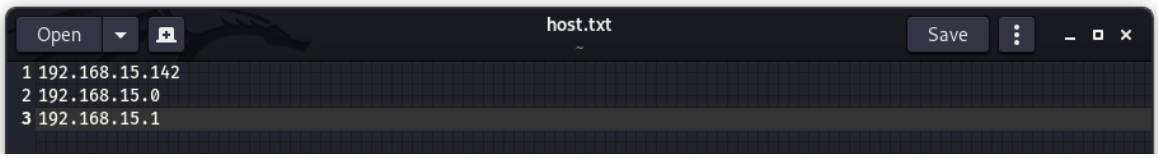

Fig 3.4.2: Gathered host

© 2021, www.IJARIIT.com All Rights Reserved

This host file is then used to detect and scan for vulnerability using our AMUNET engine and A3C algorithms are used to find various vulnerability in the host**.**

Fig 3.4.3: Vulnerability scan

All the above scan results are saved in a log file this log files are manipulated and edited by our reporting engine to create a user-friendly report, which will be uploaded to AMUNET localhost server.

3.5 Honeypot

For implementing Honeypot, we used opencannary, which we downloaded and compiled to work with our AMUNETS deep learning features and created custom config. we implemented a bridge between the honeypot and the firewall all the iptables captured by the honeypot will be blacklisted on the firewall the deep learning engine will learning about the new attacks from the honeypot.

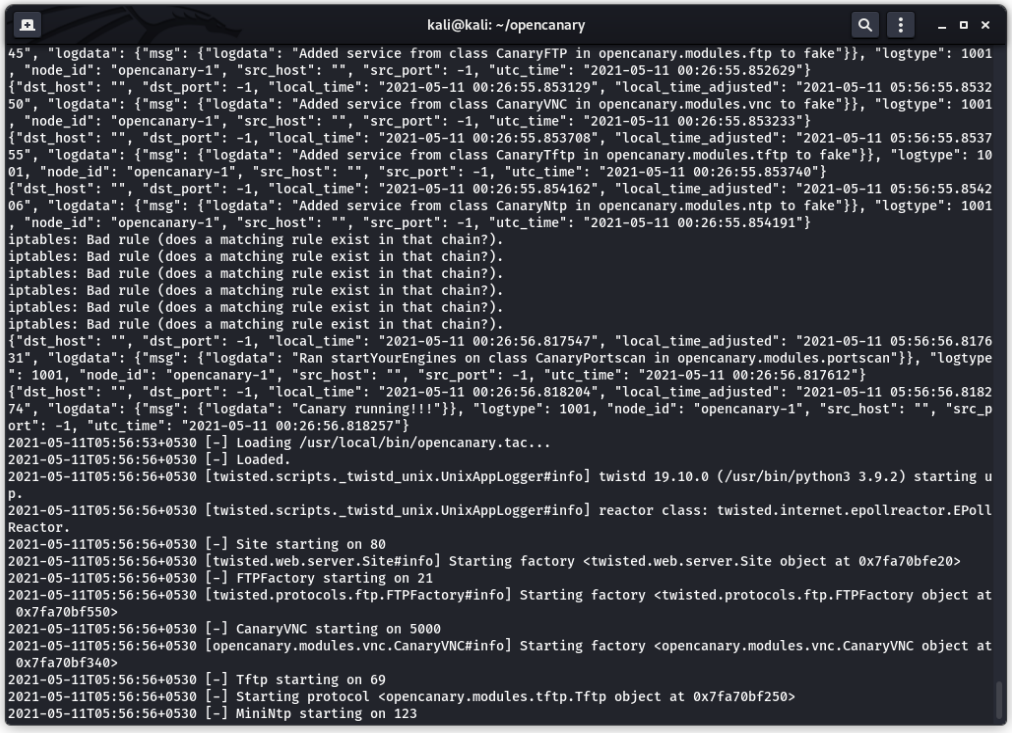

Fig 3.5.1: Configured honeypot

4. CONCLUSION

We are designing AMUNET with only one thing in mind deliver a layer of protection to every device that are connected to the internet with cost effect and plug and play capabilities. We know that no system is 100% hack proof and it never will be. The attackers are getting smarter and dangerous so it's our time to change the game and make it difficult for them to pawn our system. Our aim is to create an interconnected AMUNET network where each device learns from one another and keep on getting smarter day by day. If we could prevent 3 out of 5 attacks its a complete win for AMUNET. In future we may increase the effectiveness of

© 2021, www.IJARIIT.com All Rights Reserved

deep learning by crawlers to find and investigate about new types of attack present now. AMUNET is only strong as the data we provide one day AMUNET will collect all the necessary data to learn by itself, making it a fully self-sustained protection device. Attackers are getting smarter and so are we.

5. REFERENCES

[1] https://www.raspberrypi.org/
[2] https://pimylifeup.com/raspberry-pi-wifi-extender/
[3] https://owasp.org/
[4] https://www.exploit-db.com/
[5] https://www.rapid7.com/
[6] https://www.kali.org/
[7] https://nmap.org/
[8] https://github.com/13o-bbr-bbq/machine_learning_security/tree/master/DeepExploit
[9] https://simpaul.com/open-canary-on-a-pi/
[10] https://www.securityroundtable.org/the-growing-role-of-machine-learning-in-cybersecurity/
[11] https://medium.com/cuelogic-technologies/evaluation-of-machine-learning-algorithms-for- intrusion-detection- system-6854645f9211
[12] https://www.python.org/
[13] https://www.tensorflow.org/
[14] https://pytorch.org/
[15] https://www.snort.org/
[16] https://github.com/shirkdog/pulledpork
[17] https://www.torproject.org/

© 2021, www.IJARIIT.com All Rights Reserved