*International Journal of Engineering & Technology*, 7 (2.7) (2018) 820-824

International Journal of Engineering & Technology

*Website: www.sciencepubco.com/index.php/IJET*

***Research Paper***

# Securing Internet of Things(IoT) Using HoneyPots

**Sai Sudha Gadde[1*], Rama Krishna Srinivas Ganta[2], ASALG Gopala Gupta[3], Raghava Rao K[4], KRR Mohan Rao[5]**

[1]*Assistant Professor, Department of CSE, Koneru Lakshmaih Education Foundation, Vaddeswaram.*
[2]*Assistant Professor, Department of CSE, Koneru Lakshmaih Education Foundation, Vaddeswaram.*
[3]*Assistant Professor, Department of CSE, Koneru Lakshmaih Education Foundation, Vaddeswaram.*
[4]*Professor & Head, Department of ECSE, Koneru Lakshmaih Education Foundation, Vaddeswaram.*
[5]*Associate Professor, Department of ECE, Koneru Lakshmaih Education Foundation, Vaddeswaram.*
**Email: saisudhagadde@gmail.com*

**Abstract**

In today's everlasting technological world, information and data communication create more devices stay connected to the internet. This lead to achieving development for building different software and internet connection very inexpensive this affected privacy and security. Security today became of the most important issue because day-by-day new technologies are put forward for different purposes of study while these come with a lot of vulnerabilities which makes the exploitation of the data. IoT is also such kind technology which is available for exploiting. For preserving information from such type of attacks we use honeypot which serves as a decoy based technology in a network and these are cost effective and works as a deception model which entice attackers with low vulnerabilities and security. Here are how honeypots used to defend IoT devices from being attacked and gather information about the attackers' device.

***Keywords***: *Security, Internet of Things(IoT), Port Scan, HoneyPot*

## 1. Introduction

With the rapid growth of data processing and information technology in past few decades one of the biggest innovation in this century is Internet of Things termed as IoT which is the combination of two words i.e. Internet and physical things or objects where each physical object is connected to the internet using the RFID tags, sensors, actuators etc. which allows transferring information between the computing devices without the intervention of mankind. The rapid growth of the internet has been increased during this century which enabled the growth of internet of things a lot which is connected through a network with a wired or wireless technology. In-depth research for the origination of IoT in the late 1960's communication between the two computing devices is done through the computer network. Later in the early 80's TCP/IP was introduced which led the invention of WWW in early 90's which made internet more circulation with a rapid growth for people and Internet of Things started increasing from late 90's. The term IoT is originated by Kevin Ashton, executive director of the AutoID center in Massachusetts Institute of Technology (MIT) in the year 1999.

As an enormous growth of internet helped the growth of IoT applications in various fields which induced into human day-to-day life. As IoT applications are build using internet security became an important obstruct for IoT applications where data from the user/organization is breached and been vulnerable to malicious attacks performed by the attacker. There are several attacks that can be performed to make IoT system more vulnerable such as Man-In-The-Middle (MITM), Sniffing, Denial of Service (DoS), Cryptographical attacks, Botnet attacks, Denial of Service (Dos) and Distributed Denial of Service (DDoS). This paper mainly deals when an IoT device is been attacked by above attacks and in order to control such type of attacks this paper also provides a solution on IoT system/network/application by introducing honeypots which enables to mislead the attacker and capture the information about the attacker.

A honeypot is a type of systematic mechanism which is used to resemble the server system by enticing the potential hacker who pursues to achieve unauthorized access to data in a system. It is also used to examine the movements, traces left by an attacker and repairs the security of the system to prevent any attacks in the future. Mainly honeypots consist of a computer, applications, and information that replicate the behavior and makes attacker entrap. Honeypots are mainly classified into two types based on the type of deployment into the system either production or research honeypots. Production honeypots are typical honeypots with low interaction where it provides less information about the attack but research honeypots are high interaction honeypots where it provides the information about the attack and movements of the attacker such that it helps the organization/system to protect their against those attacks these are very hard to deploy and preserve the organization data. Most of the time honeypots are security measures for averting and handling attacks in web servers. In this paper, we provide a solution to verify system how KF Sensor honeypot is used to secure IoT application.

## 2. Literature Survey

Anirudh M, Arul Thileeban S and Daniel Jeswin Nallathambi proposed two models where one model illustrates how honeypots are used to detect anomalies and information of the client by storing the logs into database while the other illustrates by checking

**Copyright © 2018 Authors. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.**

information of the client logs, if data matches with the logs it sends a verification request to client while it also block client from server if verification fails and recognized as spam. Quang Duy La, Tony Q.S. Quek, Jemin Lee, Shi Jin and Hongbo Zhu illustrated four theorems for one-shot attack and defense game using Navie Bayers' rule with consistency in belief and sequential rationality of the attacker with optimal responses from a defender.

## 3. Types of Attacks

### 3.1. Port scan

Typically, a port scan is a passive attack where it can't harm any system or server, but it is a simple probe which retrieves the complete details of victim machine or severs and vulnerabilities to the attacker. Port scan is a procedure that sends requests to a client that are in a range of server port addresses on a host with an aim of finding any active port. There are different types of port scans among them TCP Connect, SYN scan, UDP scan, XMAS scan, ACK scan and FIN scan are the majority of scans used by an attacker.

### 3.2. Man-In-The-Middle

Also knew as MITM attack is a typical type of attack in which attacker tries to intercept communication between two parties. In other words, we can say this attack as a Janus attack (or) active eavesdropping because the attacker frames a reliable connection between the two parties and relays messages on either side such that to make a belief they are in a private conversation, but the entire communication is managed by the attacker.

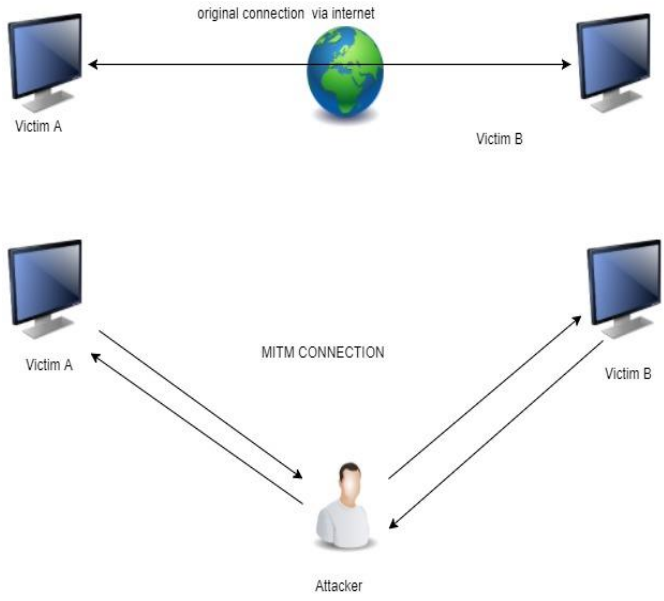



**Fig.1.** MITM Attack to Intercept Communication

### 3.3. Denial of Service attack

It is one of a type of attack which is used to shut down machine (or) network (or) application for a period such that it user can't use the system/network. It is done through pinging the network/system with heavy spam requests such that system/network can't able to handle those many requests which will lead the system to crash because it has a limited capability. Mostly attacker tries to attack using botnet and buffer overflow vulnerability and common victims of this attacks are high profile organizations like banking and government sectors which lead them the loss of important data and time to fix back the system/network.

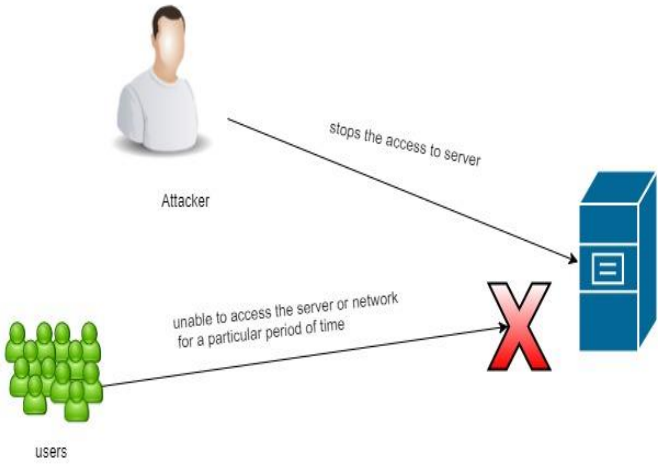



Fig.2. Denial of Service Attack

### 3.4. Distributed Denial of Service attack

Is like Denial of service attack but here attacker doesn't involve directly rather than he uses several systems to take down the machine/network such that it causes a temporary denial of service for users in the organization. A typical DDoS attack consists of master and zombie where master is referred to the attacker who initially start the attack by exploiting a vulnerability in the system and identifies other vulnerable systems and attain command over them either by infecting systems through malware or bypassing the general authentication access which are used commonly while the zombie is the list of systems or network components that are under the control of master. It is also called as Bot.

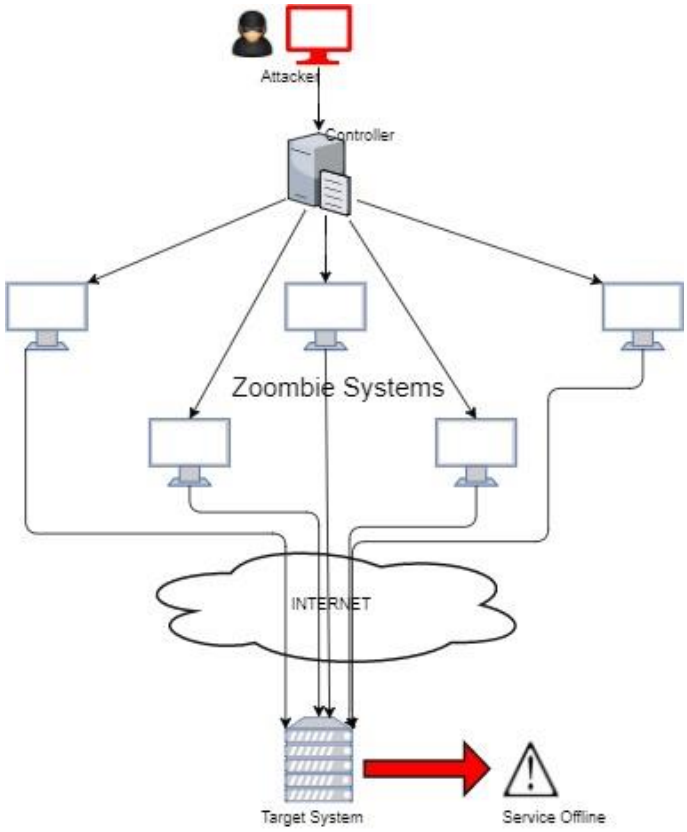



**Fig.3.** Distributed Denial of Service Attack

### 3.5. Sniffing attack

It is a common type of attack that can be performed over the wired and wireless networks which will help the attacker to get

access over the device such that attacker can obtain, collect and modify information from the device (or) machine. The main purpose of using sniffing attack is to obtain access over a particular network and then later attacker access the internet without any restriction. There are two most important methods that are used by the attacker during sniffing that includes ARP poisoning and TCP session stealing methods. ARP poisoning is a method in sniffing attack where it is used to attack the network with packet-spoofing attacks and router based vulnerabilities while TCP session stealing method is used to catch the source and destination IP address packets in promiscuous mode.

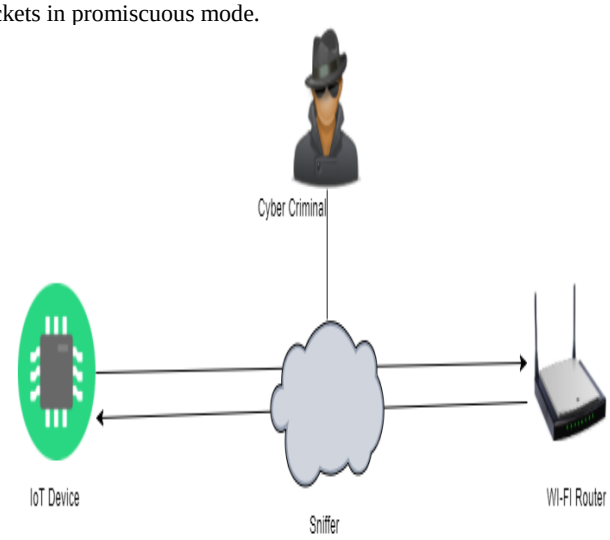



**Fig.4.** Sniffing Attack to gain Network Access

The most common widely used and successful Cryptographical attacks are Social engineering for key discovery, Dictionary attack, Reverse engineering, Brute-force attack and Implementation attacks where social engineering for key discovery depends upon humans to implement and operate the intellectual property illegal while dictionary attack is used for retrieving password files when the user chooses a common detectable password by using simple and natural words. There is a software which encrypts all the words in the dictionary and checks the hash result that matches the encrypted password which is stored in the password file. Implementation attacks are also called as the algorithmic attack because these are implemented by the elements outside the system. There are three main implementation types of attacks which comprise of side-channel attack, probing attack and fault analysis.

## 4. Attack Detection using HoneyPots

KF Sensor honeypot is Windows-based honeypot Intrusion Detection System commonly known as IDS which acts a decoy server to divert attacks and to identify hackers (or) attackers (or) unauthorized users and viruses by duplicating virtual vulnerable system services and trojans. The design of KF Sensor is widely in use for windows environment with its unique GUI management console which provides a cost-effective way to improve security in the network and includes many innovative and unique features. KF Sensor allows an easy combination of SIM/SOC, Syslog systems, and Databases. KF sensor alerts administrator when an intrusion event occurs, it also protects and responds to real-time intrusions in the network and is recorded in its log. There are six different alert types validated by KF Sensor. They are system Tray alerts, Audio alerts, Email alerts, Syslog alerts, Event Log alerts and External alerts. The main advantage of using KF Sensor over other honeypots is it gives attention and alerts to its author if any unusual event occurs. It has the capacity to deal with multiple remote KF Sensor Installation from a single machine which enables an author to view the logs from different sensors together and reconfigure honeypot remotely. Apart from advantages it also has few disadvantages, because of the application level honeypot it doesn't work at IP stack level. It can also run only one emulated honeypot for every machine and there is no way to tell KF Sensor will automatically acknowledge all open port requests. Below diagram shows the KF Sensor which is opened when installing on a host operating system.

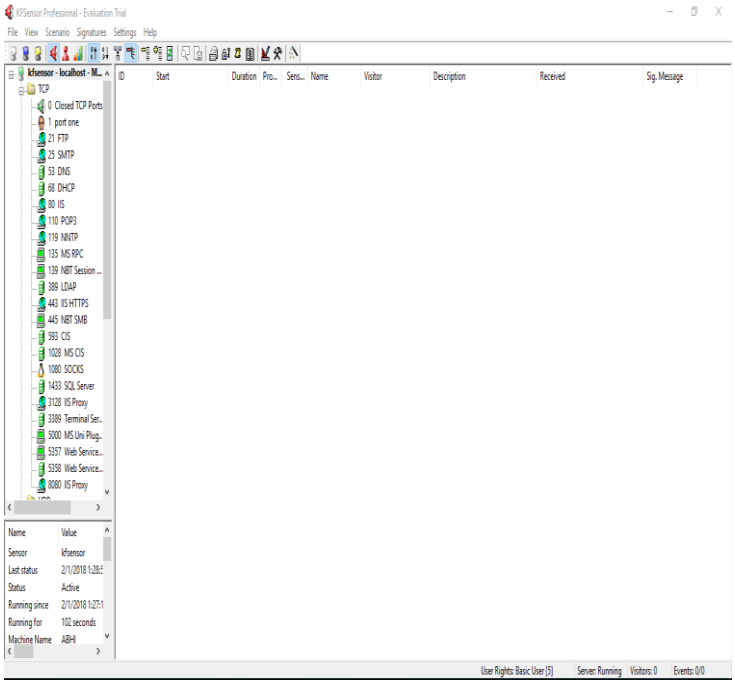


**Fig.5.** Environment for Port Scanning

For detecting different types of attacks that are executed by attacker

### 4.1. Port Scanning

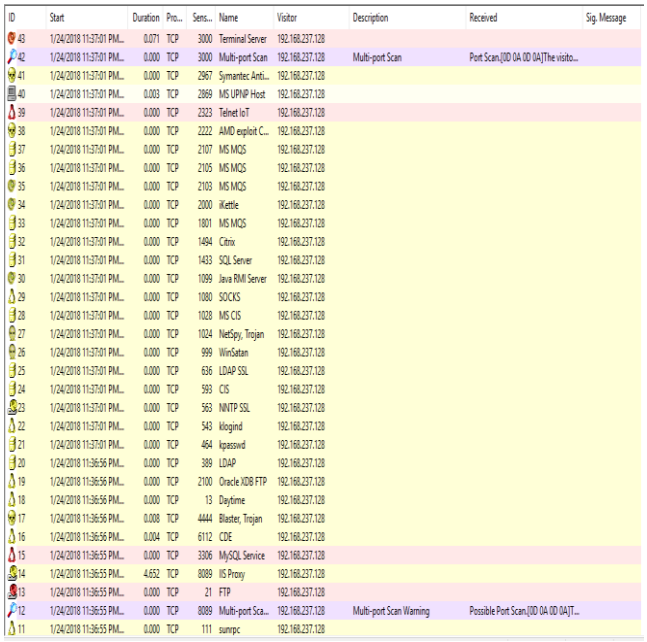
As mentioned above the major port scan when an attacker tries to retrieve information of which port is in open on the target can be determined with the following codes by the attacker and the below picture represents the detection of a port scan by the KF Sensor Honeypot.

When an attacker tries to retrieve information of which port is in open on the target

*nmap -sT 192.168.237.1 <option>--- TCP Connect Scan*
*nmap -sS 192.168.237.1 <option>--- SYN Stealth scan*
*nmap -sA 192.168.237.1 <option>---ACK Scan*
*nmap -sX 192.168.237.1 <option> ---XMAS Scan*
*nmap -sF 192.168.237.1 <option>--- FIN Scan*
*nmap -sN 192.168.237.1 <option>---NULL Scan*

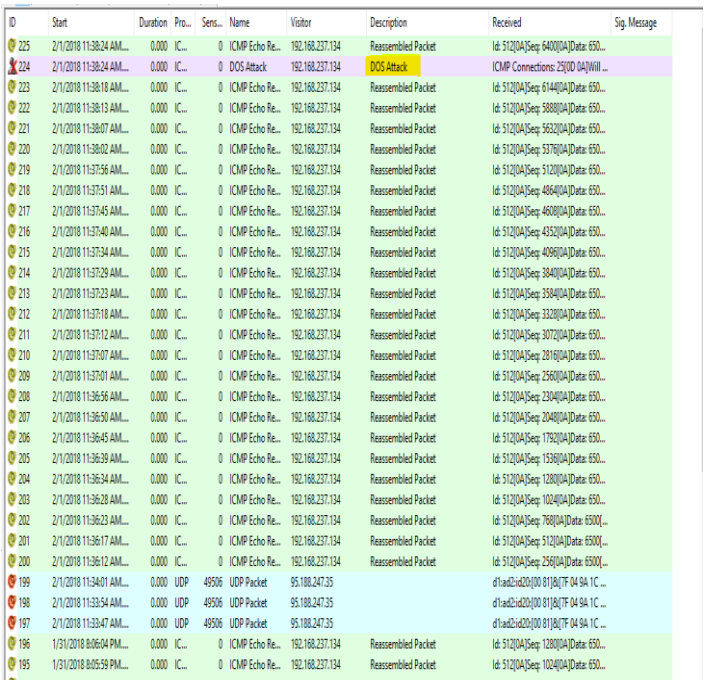
Here different <option> are used to retrieve the information from the target by attacker. Where

- -O for operating system detection details
- -sV for version detection details
- -p for custom port scan
- -sU for any UDP port open
- -Sn for ping scan
- --open for showing open port if any



| ID | Start | Duration | Pro... | Sens... | Name | Visitor | Description | Received | Sig. Message |
|---|---|---|---|---|---|---|---|---|---|
| 43 | 1/24/2018 11:37:01 PM... | 0.071 | TCP | 3000 | Terminal Server | 192.168.237.128 | | | |
| 42 | 1/24/2018 11:37:01 PM... | 0.000 | TCP | 3000 | Multi-port Scan | 192.168.237.128 | Multi-port Scan | Port Scan,[0D 0A 0D 0A]The visito... | |
| 41 | 1/24/2018 11:37:01 PM... | 0.000 | TCP | 2967 | Symantec Anti... | 192.168.237.128 | | | |
| 40 | 1/24/2018 11:37:01 PM... | 0.003 | TCP | 2869 | MS UPNP Host | 192.168.237.128 | | | |
| 39 | 1/24/2018 11:37:01 PM... | 0.000 | TCP | 2323 | Telnet IoT | 192.168.237.128 | | | |
| 38 | 1/24/2018 11:37:01 PM... | 0.000 | TCP | 2222 | AMD exploit C... | 192.168.237.128 | | | |
| 37 | 1/24/2018 11:37:01 PM... | 0.000 | TCP | 2107 | MS MQS | 192.168.237.128 | | | |
| 36 | 1/24/2018 11:37:01 PM... | 0.000 | TCP | 2105 | MS MQS | 192.168.237.128 | | | |
| 35 | 1/24/2018 11:37:01 PM... | 0.000 | TCP | 2103 | MS MQS | 192.168.237.128 | | | |
| 34 | 1/24/2018 11:37:01 PM... | 0.000 | TCP | 2000 | iKettle | 192.168.237.128 | | | |
| 33 | 1/24/2018 11:37:01 PM... | 0.000 | TCP | 1801 | MS MQS | 192.168.237.128 | | | |
| 32 | 1/24/2018 11:37:01 PM... | 0.000 | TCP | 1494 | Citrix | 192.168.237.128 | | | |
| 31 | 1/24/2018 11:37:01 PM... | 0.000 | TCP | 1433 | SQL Server | 192.168.237.128 | | | |
| 30 | 1/24/2018 11:37:01 PM... | 0.000 | TCP | 1099 | Java RMI Server | 192.168.237.128 | | | |
| 29 | 1/24/2018 11:37:01 PM... | 0.000 | TCP | 1080 | SOCKS | 192.168.237.128 | | | |
| 28 | 1/24/2018 11:37:01 PM... | 0.000 | TCP | 1028 | MS CIS | 192.168.237.128 | | | |
| 27 | 1/24/2018 11:37:01 PM... | 0.000 | TCP | 1024 | NetSpy, Trojan | 192.168.237.128 | | | |
| 26 | 1/24/2018 11:37:01 PM... | 0.000 | TCP | 999 | WinSatan | 192.168.237.128 | | | |
| 25 | 1/24/2018 11:37:01 PM... | 0.000 | TCP | 636 | LDAP SSL | 192.168.237.128 | | | |
| 24 | 1/24/2018 11:37:01 PM... | 0.000 | TCP | 593 | CIS | 192.168.237.128 | | | |
| 23 | 1/24/2018 11:37:01 PM... | 0.000 | TCP | 563 | NNTP SSL | 192.168.237.128 | | | |
| 22 | 1/24/2018 11:37:01 PM... | 0.000 | TCP | 543 | klogind | 192.168.237.128 | | | |
| 21 | 1/24/2018 11:37:01 PM... | 0.000 | TCP | 464 | kpasswd | 192.168.237.128 | | | |
| 20 | 1/24/2018 11:36:56 PM... | 0.000 | TCP | 389 | LDAP | 192.168.237.128 | | | |
| 19 | 1/24/2018 11:36:56 PM... | 0.000 | TCP | 2100 | Oracle XDB FTP | 192.168.237.128 | | | |
| 18 | 1/24/2018 11:36:56 PM... | 0.000 | TCP | 13 | Daytime | 192.168.237.128 | | | |
| 17 | 1/24/2018 11:36:56 PM... | 0.008 | TCP | 4444 | Blaster, Trojan | 192.168.237.128 | | | |
| 16 | 1/24/2018 11:36:56 PM... | 0.004 | TCP | 6112 | CDE | 192.168.237.128 | | | |
| 15 | 1/24/2018 11:36:55 PM... | 0.000 | TCP | 3306 | MySQL Service | 192.168.237.128 | | | |
| 14 | 1/24/2018 11:36:55 PM... | 4.652 | TCP | 8089 | IIS Proxy | 192.168.237.128 | | | |
| 13 | 1/24/2018 11:36:55 PM... | 0.000 | TCP | 21 | FTP | 192.168.237.128 | | | |
| 12 | 1/24/2018 11:36:55 PM... | 0.000 | TCP | 8089 | Multi-port Sca... | 192.168.237.128 | Multi-port Scan Warning | Possible Port Scan,[0D 0A 0D 0A]T... | |
| 11 | 1/24/2018 11:36:55 PM... | 0.000 | TCP | 111 | sunrpc | 192.168.237.128 | | | |

**Fig. 6.** Result after Port Scanning



| ID | Start | Duration | Pro... | Sens... | Name | Visitor | Description | Received | Sig. Message |
|---|---|---|---|---|---|---|---|---|---|
| 225 | 2/1/2018 11:38:24 AM... | 0.000 | IC... | 0 | ICMP Echo Re... | 192.168.237.134 | Reassembled Packet | Id: 512[0A]Seq: 6400[0A]Data: 650... | |
| 224 | 2/1/2018 11:38:24 AM... | 0.000 | IC... | 0 | DOS Attack | 192.168.237.134 | DOS Attack | ICMP Connections: 25[0D 0A]Will ... | |
| 223 | 2/1/2018 11:38:18 AM... | 0.000 | IC... | 0 | ICMP Echo Re... | 192.168.237.134 | Reassembled Packet | Id: 512[0A]Seq: 6144[0A]Data: 650... | |
| 222 | 2/1/2018 11:38:13 AM... | 0.000 | IC... | 0 | ICMP Echo Re... | 192.168.237.134 | Reassembled Packet | Id: 512[0A]Seq: 5888[0A]Data: 650... | |
| 221 | 2/1/2018 11:38:07 AM... | 0.000 | IC... | 0 | ICMP Echo Re... | 192.168.237.134 | Reassembled Packet | Id: 512[0A]Seq: 5632[0A]Data: 650... | |
| 220 | 2/1/2018 11:38:02 AM... | 0.000 | IC... | 0 | ICMP Echo Re... | 192.168.237.134 | Reassembled Packet | Id: 512[0A]Seq: 5376[0A]Data: 650... | |
| 219 | 2/1/2018 11:37:56 AM... | 0.000 | IC... | 0 | ICMP Echo Re... | 192.168.237.134 | Reassembled Packet | Id: 512[0A]Seq: 5120[0A]Data: 650... | |
| 218 | 2/1/2018 11:37:51 AM... | 0.000 | IC... | 0 | ICMP Echo Re... | 192.168.237.134 | Reassembled Packet | Id: 512[0A]Seq: 4864[0A]Data: 650... | |
| 217 | 2/1/2018 11:37:45 AM... | 0.000 | IC... | 0 | ICMP Echo Re... | 192.168.237.134 | Reassembled Packet | Id: 512[0A]Seq: 4608[0A]Data: 650... | |
| 216 | 2/1/2018 11:37:40 AM... | 0.000 | IC... | 0 | ICMP Echo Re... | 192.168.237.134 | Reassembled Packet | Id: 512[0A]Seq: 4352[0A]Data: 650... | |
| 215 | 2/1/2018 11:37:34 AM... | 0.000 | IC... | 0 | ICMP Echo Re... | 192.168.237.134 | Reassembled Packet | Id: 512[0A]Seq: 4096[0A]Data: 650... | |
| 214 | 2/1/2018 11:37:29 AM... | 0.000 | IC... | 0 | ICMP Echo Re... | 192.168.237.134 | Reassembled Packet | Id: 512[0A]Seq: 3840[0A]Data: 650... | |
| 213 | 2/1/2018 11:37:23 AM... | 0.000 | IC... | 0 | ICMP Echo Re... | 192.168.237.134 | Reassembled Packet | Id: 512[0A]Seq: 3584[0A]Data: 650... | |
| 212 | 2/1/2018 11:37:18 AM... | 0.000 | IC... | 0 | ICMP Echo Re... | 192.168.237.134 | Reassembled Packet | Id: 512[0A]Seq: 3328[0A]Data: 650... | |
| 211 | 2/1/2018 11:37:12 AM... | 0.000 | IC... | 0 | ICMP Echo Re... | 192.168.237.134 | Reassembled Packet | Id: 512[0A]Seq: 3072[0A]Data: 650... | |
| 210 | 2/1/2018 11:37:07 AM... | 0.000 | IC... | 0 | ICMP Echo Re... | 192.168.237.134 | Reassembled Packet | Id: 512[0A]Seq: 2816[0A]Data: 650... | |
| 209 | 2/1/2018 11:37:01 AM... | 0.000 | IC... | 0 | ICMP Echo Re... | 192.168.237.134 | Reassembled Packet | Id: 512[0A]Seq: 2560[0A]Data: 650... | |
| 208 | 2/1/2018 11:36:56 AM... | 0.000 | IC... | 0 | ICMP Echo Re... | 192.168.237.134 | Reassembled Packet | Id: 512[0A]Seq: 2304[0A]Data: 650... | |
| 207 | 2/1/2018 11:36:50 AM... | 0.000 | IC... | 0 | ICMP Echo Re... | 192.168.237.134 | Reassembled Packet | Id: 512[0A]Seq: 2048[0A]Data: 650... | |
| 206 | 2/1/2018 11:36:45 AM... | 0.000 | IC... | 0 | ICMP Echo Re... | 192.168.237.134 | Reassembled Packet | Id: 512[0A]Seq: 1792[0A]Data: 650... | |
| 205 | 2/1/2018 11:36:39 AM... | 0.000 | IC... | 0 | ICMP Echo Re... | 192.168.237.134 | Reassembled Packet | Id: 512[0A]Seq: 1536[0A]Data: 650... | |
| 204 | 2/1/2018 11:36:34 AM... | 0.000 | IC... | 0 | ICMP Echo Re... | 192.168.237.134 | Reassembled Packet | Id: 512[0A]Seq: 1280[0A]Data: 650... | |
| 203 | 2/1/2018 11:36:28 AM... | 0.000 | IC... | 0 | ICMP Echo Re... | 192.168.237.134 | Reassembled Packet | Id: 512[0A]Seq: 1024[0A]Data: 650... | |
| 202 | 2/1/2018 11:36:23 AM... | 0.000 | IC... | 0 | ICMP Echo Re... | 192.168.237.134 | Reassembled Packet | Id: 512[0A]Seq: 768[0A]Data: 6500[... | |
| 201 | 2/1/2018 11:36:17 AM... | 0.000 | IC... | 0 | ICMP Echo Re... | 192.168.237.134 | Reassembled Packet | Id: 512[0A]Seq: 512[0A]Data: 6500[... | |
| 200 | 2/1/2018 11:36:12 AM... | 0.000 | IC... | 0 | ICMP Echo Re... | 192.168.237.134 | Reassembled Packet | Id: 512[0A]Seq: 256[0A]Data: 6500[... | |
| 199 | 2/1/2018 11:34:01 AM... | 0.000 | UDP | 49506 | UDP Packet | 95.188.247.35 | | d1ad2cd20:[00 81]8c[TF 04 9A 1C ... | |
| 198 | 2/1/2018 11:33:54 AM... | 0.000 | UDP | 49506 | UDP Packet | 95.188.247.35 | | d1ad2cd20:[00 81]8c[TF 04 9A 1C ... | |
| 197 | 2/1/2018 11:33:47 AM... | 0.000 | UDP | 49506 | UDP Packet | 95.188.247.35 | | d1ad2cd20:[00 81]8c[TF 04 9A 1C ... | |
| 196 | 1/31/2018 8:06:04 PM... | 0.000 | IC... | 0 | ICMP Echo Re... | 192.168.237.134 | Reassembled Packet | Id: 512[0A]Seq: 1280[0A]Data: 650... | |
| 195 | 1/31/2018 8:05:59 PM... | 0.000 | IC... | 0 | ICMP Echo Re... | 192.168.237.134 | Reassembled Packet | Id: 512[0A]Seq: 1024[0A]Data: 650... | |

**Fig.7.** Dos Attack Detection

### 4.2. Dos Attack

Dos attack can be performed by using the below codes and a GUI tool called Low Orbit Ion Cannon(LOIC) where DOS attacks can be implemented even from a windows machine. Dos attacks are performed on different platforms such as machine to machine, machine to a web server, machine to a cloud, machine to a IoT devices and to many things.

There are three different types of Dos attacks which gives sensitive information about the system to attacker are discussed in this paper"

#### 4.2.1. SMB Dos

When an attacker tries to run an SMB Dos attack on the target and by setting the target machine IP address in the above script an SMB Dos Attack is performed.

*nmap -p 338g --scrip=rdp-vuln-ms12-020.nse 192.168.237.1*

#### 4.2.2. WIFI Dos

To disconnect target connecting to Wireless network and sending heavy packets to the target IP address we use following code.

*aireplay -ng -o o -a 192.168.1.1 -c <MAC Address> -e <router name> wlan0mon*
The mac address and router name represent the network interface card mac address.

#### 4.2.3. Ping of Death

The ping of death is a simple and basic Dos attack where the attacker sends an enormous number of packets to the target such that it will consume larger bandwidth and sometimes it may lead to a crash of the system. The below code shows a pinging of a system by sending a larger number of unwanted packets such that the network to a particular user will be disclosed to use internet over a small period.

*ping 192.168.237.1 -L 65000 –t*

### 4.3. Sniffing and MITM

For detecting Network Sniffing and Man-In-The-Middle attacks in a network we must scan the complete network to find out the sniffer and both the attacks are very similar where an attacker tries to intrude in a network and steals the sensitive information of the users in that network. To identify these types of attacks and unauthorized users in the network the below code illustrates whether any sniffer is present in our network.

*nmap -sn --script=sniffer-detect 192.168.237.1/255*

***If any sniffing or MITM attack is detected on the network the test result shows all ones "11111111". If there is no sniffing attack during detected the test result will display all "_ _ _ _ _ _ _ _"***

```
Starting Nmap 7.25BETA1 ( https://nmap.org ) at 2018-02-03 08:25 IST
Nmap scan report for 192.168.0.151
Host is up (0.022s latency).

Nmap scan report for www.routerlogin.com (192.168.1.1)
Host is up (0.0028s latency).
MAC Address: 20:E5:2A:E5:0E:AC (Netgear)

Host script results:
|_sniffer-detect: Likely in promiscuous mode (tests: "11111111")

Nmap scan report for 192.168.1.4
Host is up (0.00024s latency).
MAC Address: EC:55:F9:4E:0D:04 (Hon Hai Precision Ind.)

Host script results:
|_sniffer-detect: Likely in promiscuous mode (tests: "11111111")
```

**Fig. 8.** Sniffer Attack Detection

## 5. Conclusion and Future Work

Earlier from recent years the realm of network security attained a huge development since no one wants his system to be attacked by attackers. Honeypot technology is helpful and utmost important part of security strategies in a network. This paper illustrates a precise study of how different types of attacks in iot systems are prevented using honeypots.

## References

[1] Quang Duy La, Tony Q. S. Quek, Jemin Lee, Shi Jin and Hongbo Zhu "Deceptive Attack and Defense Game in Honeypot-Enabled Networks for the Internet of Things" in IEEE Internet of Things Journal, Dec 2016.

[2] Anirudh M, Arul Thileeban S and Daniel Jeswin Nallathambi "Use of Honeypots for Mitigating DoS Attacks targeted on IoT Networks" in IEEE International Conference on Computer, Communication, and Signal Processing (ICCCSP-2017)

[3] Seamus Dowling, Michael Schukat, Hugh Melvin "A ZigBee Honeypot to assess IoT Cyberattack Behaviour" in IEEE Signals and Systems conference(ISCC-2017)

[4] Theodor Richardson "Preventing Attacks on Back-End Servers using Masquerading/Honeypots" in Seventh ACIS International Conference on Software Engineering, Artificial Intelligence, Networking, and Parallel/Distributed Computing, Jun. 2006, pp. 381–388.

[5] Aaditya Jain, Bhuwnesh Sharma, Pawan Gupta "Honeypot: An External layer of Security Against Advanced attacks on Network" in International Conference on Recent Trends in Engineering Science and Management, Apr.2016.

[6] Surendra Mahajan, Akshay Mhasku Adagale, Chetna Sahare "Intrusion Detection System Using Raspberry PI Honeypot in Network Security" in International Journal of Engineering Science and Computing, Mar.2016.

[7] S. Hausman "Navigating security threats posed by Internet of Things technology" [online]. Available: http://www.securityinfowatch.com/article/11714106/navigating-security-threats-posed-by-internet-of-things-technology

[8] http://searchsecurity.techtarget.com/tip/The-ABCs-of-ciphertext-exploits-and-other-cryptography-attacks

[9] http://www.keyfocus.net/kfsensor/help/Concepts/con_Alerts.php