Raspberry Pi Based Intrusion Detection System

Ranjeethapriya K, Susila N, Granty Regina Elwin, Balakrishnan S

1Department of Information Technology, Sri Krishna College of Engineering and Technology, Coimbatore, Tamilnadu, India

Abstract

Industrial control networks and smart grid infrastructure which are having large number of connected networks are facing many security issues like intruders passing and traffic in the network. Network administrators are ensuring the regularly huge number of associated resources for which they are mindful. The gadgets might be firmly combined with Raspberry pi which persistently screens the system movement. Ettercap, Wireshark are compelling devices for watching and drawing in network intruder activity. It displays an outline and execution for self-designing honeypots that latently inspect control framework organize movement and effectively adjust to the watched condition. Using Ettercap XML yield, intruder action is checked. A calculation was created for refreshing the equipment and relegating the limit esteem. This calculation was tried on a current little grounds lattice and sensor arrange by execution of a synergistic use situation. Virtual hosts were consequently arranged and intruders are diverted to that host to recognize the correct intruders. Ettercap copied arrange stack practices for 92% of the focused on gadgets. Raspberry pi identifies 98% of intruders action in the system.

Keywords: Intruder, raspberry pi, Ettercap etc.
1. Introduction

Network security deals with various techniques to identify real members taking part in communication systems. Industrial control networks have many secret information that to be preserved from unauthorized users. Many industries and small grid infrastructure are taking prevention techniques to detect the intruders passing through the network. Raspberry pi hardware is connected to the physical devices in the industries and monitored through the PC. A single PI can scan large number of host and network entities connected through the network. To overcome the security issues faced by industrial networks Ettercap is installed in raspberry pi and hosts were scanned. Ethernet cable is used for connecting PC, raspberry pi and network. Access point can be used to connect large number of raspberry pi in the industries. In this mechanism network entities (i.e) source, destination and port activity which is helpful for creating virtual networks using raspberry pi. This virtual host is created in the raspberry pi to divert the intruders’ activity. Hardware is already assigned with list of IP addresses that to be blocked or be diverted.

The fig 1 shows the common industrial control system which is connected with hardware to obtain the information and for the creation of virtual host.

![Diagram](image)

**Fig 1**: A Common ICS system connected with Raspberry pi

2. Related Works

The Autonomic Intelligent Cyber Sensor to Support Industrial Control Network Awareness were discussed in [1]. When there comes the purpose of honeypots, information can be gathered using active and passive scanning tools. Lightweight
intrusion detection for networks is carried out using snort tool [2]. In which snort resembles the rule based intrusion detection system but only limited amount of information can cleaned by passive scanning tool was restricted in collecting the information from captured stream. The suitable tool that identify passive information is Ettercap[3]. Nmap is one of the active scanning tool that gives successful result in interrogating hosts on a network [4]. Active scanning tool suffers from the problem of service request interruption on hosts especially in most of the industrial network control systems that may leads to damages. Dynamic host configuration and virtual honeypots for detecting intruders [5]. DHP solutions were discussed in [6] [7]. In the literature review the identification tools are used for providing network host identification are P0f [8], Tshark [9], Tcpdump [10], SinFP [11] and Ntop [12]. The architecture of CPS’s, security and safety framework of CPS and challenges and negative impact of CPS are presented in the paper [13].

Proposed system [14] consists of four steps: grouping state changes into clusters, distinguishing between benign and malicious clusters, committing benign clusters, and recovering from malicious state.

2.1 Existing System

Automatic configuration in honeyd has a great advantage in solving the security issues. It differs from honeypot and honeynet which connects number of networks. These honeypots or honeynet is implemented in system to connect large number of hosts in a network. But low interaction honeypots can only gather basic information. Ettercap is an effective tool for gathering network entities. A four step process is carried out for creating XML output, using this output honeyd is created automatically and updated. This honeyd enables one to connect large number of host on a network, so that attackers can be identified easily.

\[
\begin{array}{cccc}
\text{Attacker} & \text{Honeyd} \\
\end{array}
\]

Virtual honeypots

Fig 2: Honeyd configuration

The fig 2 shows the honeyd configuration which monitors unused ip addresses in the network. If an attacker uses it which is identified by virtual host with the help of ip spoofing.

3. Proposed System

In this paper honeyd configuration is done using raspberry pi so that this device acts as an virtual honeypot. Ettercap tool is also implemented in raspberry pi to gather the network entity information and list of IP address to be restricted is
marked. A log file is created using ettercap and list of IP address to be restricted is written in that hardware. This is the base for the creation of virtual host. A session is created in the system which is already connected with raspberry pi. Administrator can control the hardware manually using this session. Virtual host Apache is installed using python, mysql etc. This virtual host monitors the intruders activity and that particular IP can be redirected to this virtual host. This virtual host can then provide access or deny them based on their performance.

3.1 Algorithm
Initialize and identify the Rip
Identify the ‘n’ connected Sip to Rip
Check the log of Sip, if (sys_time>=50ms) then
Assign Rlog with Slog
For all Sip ∈ Rlog
    If(hits_Sip>th_hits) then
        Assign VSip with Sip
        VSip monitors the intruder activity.
        VSip is involved in supervised learning
    If (VSip_PASS != db_pass) then
        C++
        If(C>5) then
            Assign Blog with Sip
        END FOR

4. Implementation and Design
The above proposed system is implemented by means of python and essential software’s to obtain the required result. The steps are as follows:
- The hardware is connected to the control system with preinstalled ipscanner, putty and xming software.
- Using ettercap monitor the intruders activity using sniffing process and create a log file.
Virtual host is created in the hardware to divert the intruders process.

IP classification and IP extraction is done based on the log file.

All the intruders is redirected to virtual host created and their activity is monitored.

Initially the system should be installed with software like putty, xming and ipscanner. Raspberry pi to be connected with the system is installed with ettercap software for running in Linux platform and wireshark for windows operating system. This software provides the network entities like source, port and MAC address. Using DNS server one end of LAN cable is connected to the laptop and other end to the hardware. Now, the IP address of hardware is identified through system using IP scanner and Putty software is used for creating new session and ssh forwarding that is done using x11 forwarding.

### 4.1 Ettercap Tool

The session is created in the system for controlling the hardware directly. Ettercap is made to run using terminal and number of host in the network is scanned. Network entities like source, port and MAC address is also displayed by this tool. Since there is large number of hosts target is fixed for any two host. Sniffing process is started to monitor the activity of that particular host. If any intruder continuously tries to steal the information from the organizations that intruders IP is displayed using Ettercap. ARP poisoning is also achieved through this tool. Finally a log file is created and given to the hardware. Using this file each host operating system is displayed using raspberry pi terminal.

Intruders tries to attack the system is identified and their activity is monitored simultaneously. Finally a virtual host is created in that hardware using terminal. Here apache is chosen as a virtual host or server to monitor the intruder’s activity. Once the intruder is fixed its IP is diverted the virtual host which is similar to the real host. Intruder will think the emulated host as real host and request the services from that server, so that their activity is monitored. Once the intruder is fixed their access is restricted in the network.

A threshold value (t=5) is maintained and fixed to identify the intruders activity. Whenever a particular user crosses this level their activity is closely monitored and identified as intruder. The intruder is assigned to virtual host automatically for restricting the access to that particular network.

This virtual host is updated manually using the hardware terminal.

### 5. Results and Discussion
Fig 3: IP Detection

Fig 4: Virtual host
6. Conclusion

In this paper we discussed some of the drawbacks faced by the existing system regarding virtual host configuration and updating process. This is effectively handled by our proposed system which updates the virtual system and usage of hardware for connecting large number of networks and host.

References
