INDONESIAN JOURNAL OF ENGINEERING RESEARCH
2021, Vol. 2, No. 2, 53 – 60
http://dx.doi.org/10.11594/ijer.02.02.04

Research Article

Network Security Using Honeypot and Attack Detection with Android Application

Farizqi Panduardi[1]*, Herman Yuliandoko[1], Agus Priyo Utomo[1]

[1]Informatic Department, State Polytechnic of Banyuwangi

Article history:
Submission November 2021
Revised November 2021
Accepted November 2021

**Corresponding author:*
E-mail:
akufarisqi@poliwangi.ac.id

ABSTRACT

Network security is now increasingly needed in the era of the industrial revolution 4.0. As technology grows, cybercrimes are becoming more and more common, including attacks on a resource. At this time, honeypots are also widely used by large industries for network security, besides that honeypots are also useful for them in developing intrusion and preventing systems. Honeypots are usually used in a virtual environment, they will stimulate a fake system to capture data packets on the network and be analysed offline later for all threats and attacks.

This propose of this paper is to detect and prevent building attacks from computer network attackers using an android application. This application can monitor an attack on the server by installing a honeypot tool into the server as an attack detector, then the honeypot log is used as a Rest API using Django framework with MongoDB database. this application can find out if there is an attack on the server, and can block the attacker's IP address.

Keywords: honeypot, intrusion, DDOS, brute force.

Introduction

Computer network technology continues to grow, in terms of security, speed, and efficiency. As the development of computer networks continues to grow, hackers are also getting smarter to attack or control a resource. One tool that is quite often used for detection and prevention of attacks is using a honeypot. A honeypot is a program, machine, or system put on a network as bait for attackers (Kumar Jain & Surabi, 2012). Honeypot is a system created with the main purpose of attacked, accessed, or taken over in an unauthorized manner by the attacker. Honeypot is made similar to the actual system. With a honey pot, an administrator can analyse the methods used, along with information about the paths used by attackers to penetrate the server. From that information the administrator can fix gaps in the system that cause computer network security vulnerabilities. Attacks on servers usually use DDOS (Distributed Denial of Service) an attack used to flooding internet, server or web network traffic.

In this paper, we use a combination of the Dionaea honeypot and Kippo honeypot to detect various types of attacks. Dionaea honeypot is a low interaction honeypot, Dioanea created a fake service emulation that would serve as the main target of attack, Kippo is a medium interaction honeypot that designed using the

How to cite:
Panduardi, F., Yuliandoko, H., & Utomo, A. P. (2021). Network Security Using Honeypot and Attack Detection with Android Application. *Indonesian Journal of EngineeringResearch*. *2*(2), 53 – 60. doi: 10.11594/ijer.02.02.04

python programming language to store brute force information and save intruder information. Every time there is an attack from outside, there will be a notification in the android application. so that the server administrator can find out if there is an attack on the server in real time. The server administrator can also block the attacker's IP address through the android application

Literature Review

Honeypot

A honeypot is a resource that appears as legitimate systems. It has long been proven to be effective at catching malware, helping to fight spam and provide early warning signals about emerging threats.

Low Interaction Honeypot

This low interaction honeypot provides little opportunity to interact with attackers. This type of honeypot is relatively easy to implement and has a low risk to the network and system. low interaction honeypot collects a limited amount of information such as low-level connection logs and network flow level information.

Medium Interaction Honeypot

Compared to low interaction honeypot, this type of honeypot provides more opportunities for interact with attackers to gather more information detail.

High Interaction Honeypot

This type of honeypot allows the attacker to have the highest level of interaction with a real system and allows us to collect. Disadvantages of high interaction honeypot is too risky, because attackers can use high interaction honeypot to attack other systems to use, maintain, configure and analyze, they require highly skilled network administrator.

Dionaea

Dionaea is a low-interaction honeypot was created as a replacement for Nepenthes. Dionaea is used to trap attackers exploit malware vulnerabilities against service on the network. Dionaea using python programming language as a scripting language and libemu to detect shellcodes. Dionaea also supports IPv6 and TPS (Transport Layer Security). as much information as possible will come First, confirm that you have the correct template for your paper size. This template has been tailored for output on the A4 paper size. If you are using US letter-sized paper, please close this file and download the Microsoft Word, Letter file. The first scenario commonly used by attackers is to use the port scanning method. port scanning is used to get information from server services to be used in the intrusion process. Dionaea honeypot will respond with fake services as if the attacker managed to get information from the legimate server. Next, the attacker will use the DDOS attack method, Dionaea will record the attack in a log so that the administrator can analyze it later.

Kippo

Kippo (Solomon & Avadhani, 2016) is a medium interaction SSH honeypot designed to log brute force attacks and, most importantly, the entire shell interaction performed by the attacker. how the Kippo honeypot works is create an interactable fake SSH service. The attacker will use the brute force method to get the username and password that will be used to enter the SSH service. kippo will record all these brute force attacks by storing them in a log. The attacker will get the real user and password provided by kippo to enter the kippo's own SSH honeypot service. when the attacker is logged in, kippo will emulate the SSH features like on a legitimate server. Under these conditions, Kippo's honeypot can interact directly by attacking. when interacting, kippo will record all shell command interactions performed by the attacker and stored in a log that can be analyzed by the administrator later.

Python

Python is a high-level programming language based on interpreted, object-oriented, with dynamic semantics. built in data structures and combined with dynamic typing and dynamic binding, making it very attractive for RAD (Rapid Application Development), and is used as a scripting language for connecting existing components together. Syntax in python programming language simple and very easy to

learn emphasizes readability and reduce program maintenance costs. Python supports modules and packages, which encourages program modularity and code reuse.

Django Framework

Django is a high-level python web framework that supports fast app development and clean pragmatic design. Django built by experienced developers, to reduce complexity in web development, so users can focus on making applications. The jango framework is open source and free.

Port Scanning

Port Scanning is an activity to check the status of TCP and UDP ports on a machine. Or the process of finding andview and examine possible system weaknesses attached to a computer or equipment. through the destination port. The attacker will do reconnaissance by doing ports canning, to find out what services are available on the target server and can be a serious threat to the server.

Brute Force

A brute force attack is an algorithm that solves a problem in a very simple, direct, and clear way. Solving password cracking problems using brute force algorithm, will locate and search all possible password with character input and password length. A brute-force attack with a wordlist or dictionary is an attack to get a username and password with try all possible usernames and passwords in the file wordlist. Attackers will try different usernames and passwords to enter into the SSH service, in this attack it is possible to get the user/password if in the wordlist there is combination of username and password that is logged on the SSH server service certain. Of course, with lots of password combinations.

DDOS Attack

This type of DDoS attack sends junk data messages mass to cause overload, which also resulted in reduced available network bandwidth or reduced network device resources. Often routers, servers and firewall that is attacked, has limited resources. This attack causes network device failure to handle normal access. so, there is a decrease significant quality of service or complete paralysis system (DoS). in both cases it means the user cannot access the systems they need. The most common form of a DDOS attack is a flood network traffic. This attack is carried out by sending a large number of TCP packets, UDP packets, ICMP packets which appears to be legitimate to the target host/server. Some attacks on this basis, can also avoid scanning the system with the origin address camouflage. Legitimate requests are ultimately not served due to so many attack packets circulating on the network. This attack can also do more damage if combined with other illegal activities, such as exploitation using malware that causes leaks sensitive information/data theft on the target computer.

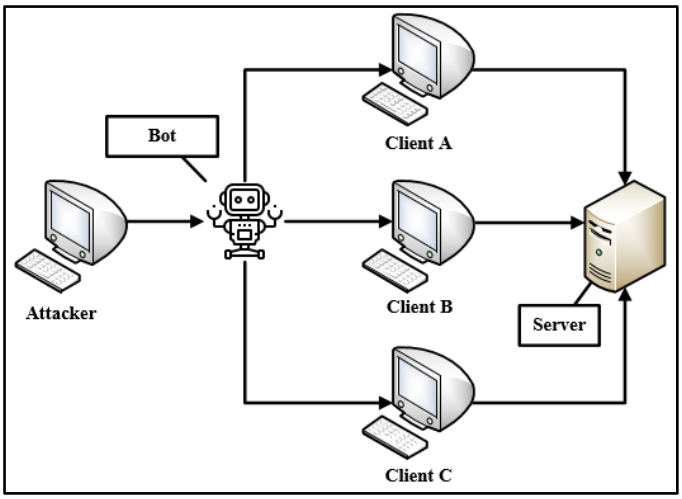

Figure 1. DDOS Attack

In the picture above, the attacker uses bots to disguise himself as several clients. In this case the client requests service from the server. In a DDoS attack, the attacker is able to create hundreds or even thousands of clients which can cause server services to be hampered because they are unable to handle too many requests and at worst can make the server hang.

Experiment Setup

In a computer network, the side that is directly connected to the internet has a higher risk in terms of network security. The

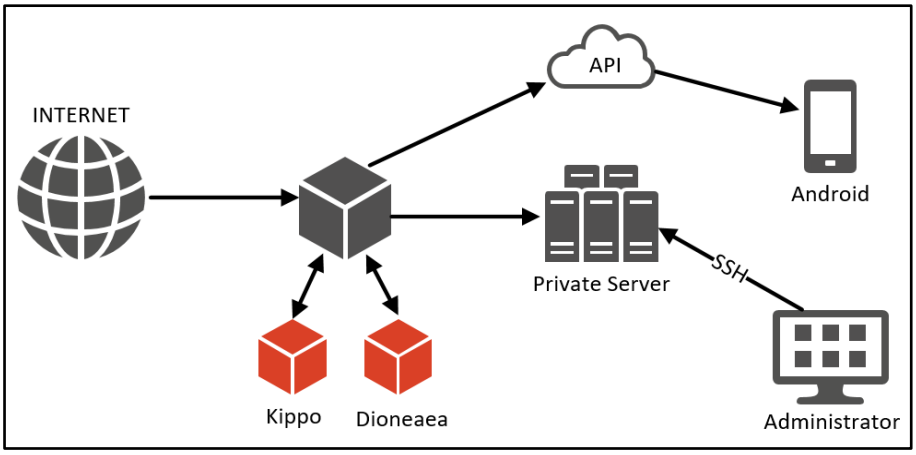

Figure 2. Experiment Setup

Honeypot will be placed between the server and the internet, so it can prevent attacks directly from entering the server. In this experiment, we use a virtual private server (VPS). The

Dionaea honeypot and Kippo honeypot will be placed gateway of the server. This area is also known as the demilitary zone (DMZ). In practice, both honeypots use the SSH feature provided by the VPS. the function of the honeypot Dionaea emulates a fake service that is used to trap attacks from Internet. The function of the Kippo honeypot is to detect an attack intended for SSH services, then the results of the attack are integrated with Android, making it easier for administrators to monitor computer network attacks.

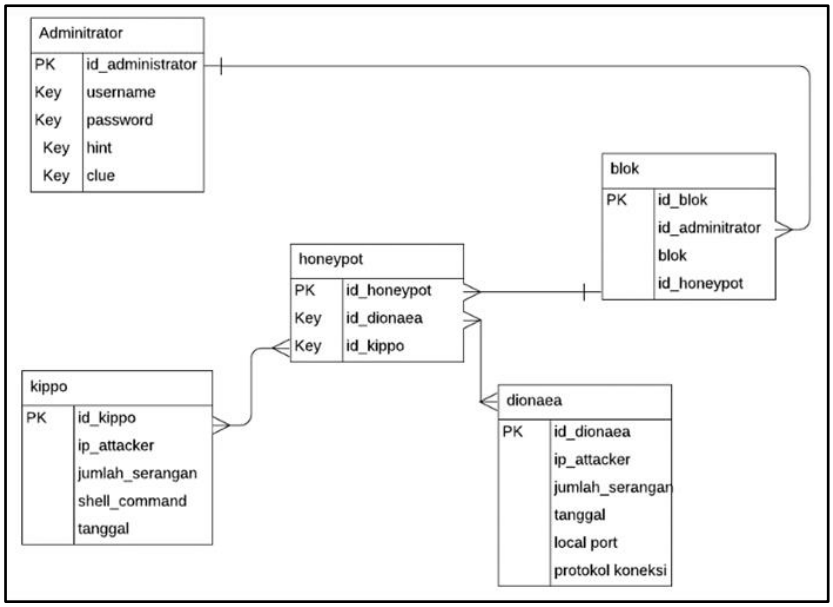

Figure 3. ERD Experiment Setup

Figure 3 is the design of the ERD database on the honeypot Kippo. This database is used to store all logs and shell command information of intrusion activities that occur on the SSH port. Honeypot Kippo has a log store that can be integrated with the database.

All activity and attack data will be stored in the database. the data will be analyzed, and the results will be reported through the android application in real time. Attack activities include, the time of attack, the type of attack, the attacker's IP address, and the number of times the same IP address penetrates the server. With real time reports, administrators can immediately find out if there is an attack on the server, and the administrator can execute the attack.

Result and Discussion

The honeypot that has been implemented has succeeded in preventing external attacks. DDoS attacks can be detected by the Dionaea honeypot, the Kippo honeypot has also succeeded in overcoming the brute force attacks that occurred. all data about attack activity, both DDoS and brute force can be stored in the database and reported through the android application to the administrator.

Android Application

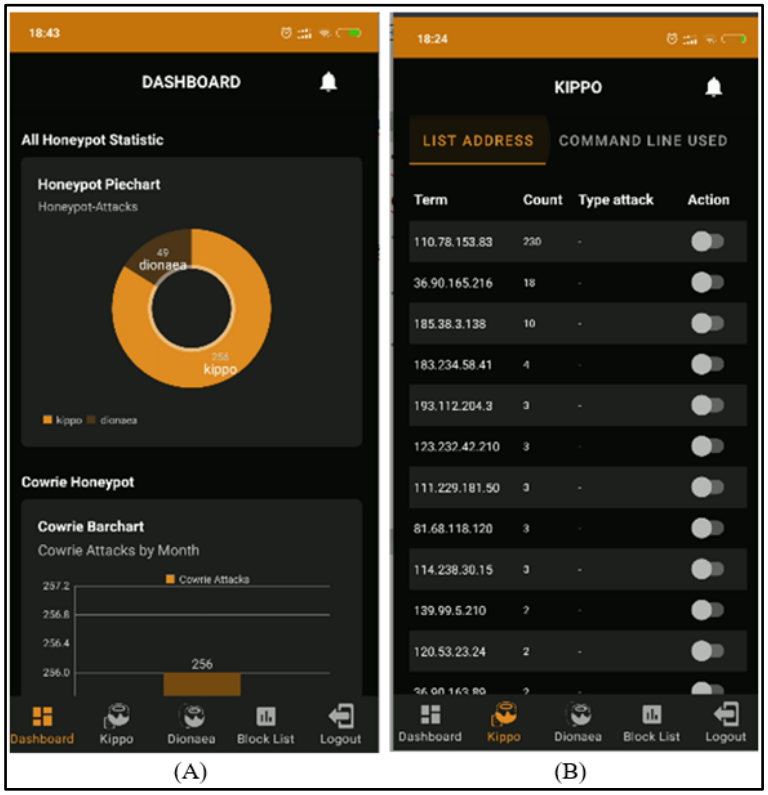

Figure 4. (A) Dashboard, (B) Kippo Page Display

Figure 4 (A) shows the dashboard view of the Android application. in the dashboard displays all attacks that occur on the VPS. Pie chart honeypot is a graph containing data on all attacks on VPS with Honeypot Kippo and honeypot Dionaea, used as a comparison for attacks on both honeypots.

On this dashboard has the facility to display the attacks prevented by honeypot Dionaea and Kippo in one day, and in one month. This application can also display the top 10 IP addresses that are most frequently attacked.

Figure 4 (B) shows some IP addresses that are trying to perform a brute force attack against the server. in addition to displaying the IP address, it also displays the number of attempted attacks by the attacker.

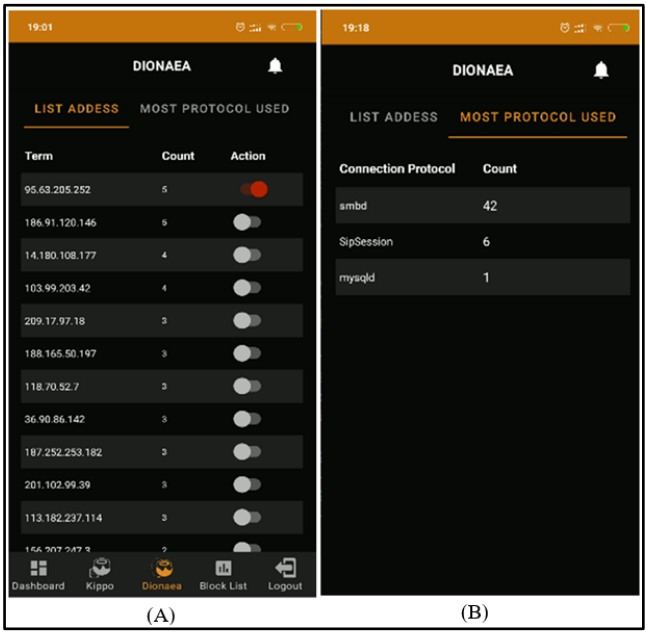

Figure 5. (A) Dionaea Page Display, (B) Most Protocol Used

Figure 6 shows the Dionaea honeypot page display. This page shows the IP address of the attempted attack, and the number of times that IP address was attacked. given a choice of actions to block or leave certain IP addresses Equipped with a choice of actions, whether to block or not.

Shown by figure 7, on the Dionaea honeypot page there is also a facility to find out what Services are most often used by attackers when conducting attack attempts. this can be a consideration for administrators to further secure which services to use and not to use.

System Testing

The testing method used is black box testing. This system testing is carried out to ensure the quality and functionality of the system so that it can work as expected. The IP address used as the attacker is 36.90.162.248, while the IP address of the server is 34.66.225.217. to test the Kippo honeypot, an attacker will try to enter the Kippo SSH. if the user and password entered are correct, it will automatically enter the Kippo honeypot command shell. if the user and password are wrong 5 times, it will be categorized as a brute force attack. To test the detection of brute force attacks, a tool called hydra is used as shown in figure 6.

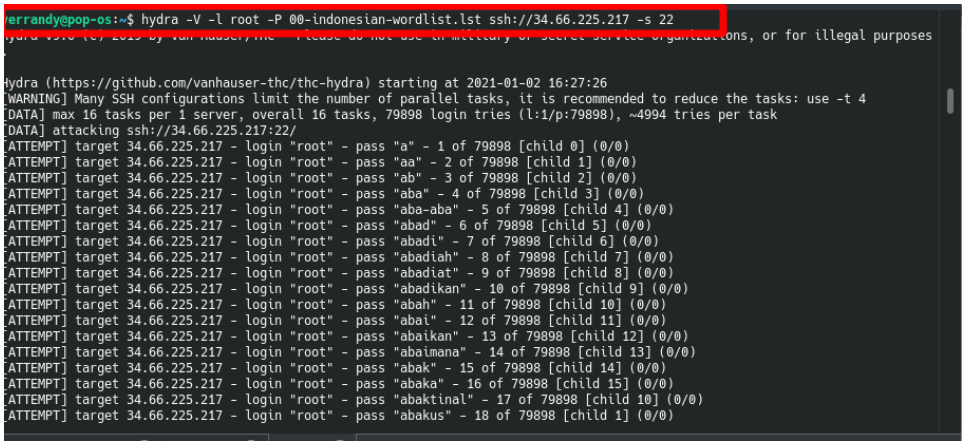

Figure 6. Tools Hydra

For testing the Dionaea honeypot, the attacker will make a request to the Dionaea honeypot service port. If the request exceeds 1000 within 60 seconds, it will be categorized as a DDOS attack. this test uses a tool called hping3 to attack with the DDOS method.

```
└─$ sudo hping3 -i u1 -S -p 445 34.66.225.217
[sudo] password for kali:
HPING 34.66.225.217 (eth0 34.66.225.217): S set, 40 headers + 0 data bytes
len=46 ip=34.66.225.217 ttl=64 id=14247 sport=445 flags=SA seq=0 win=65535
rtt=0.0 ms
len=46 ip=34.66.225.217 ttl=64 id=14248 sport=445 flags=SA seq=0 win=65535
rtt=0.0 ms
len=46 ip=34.66.225.217 ttl=64 id=14249 sport=445 flags=SA seq=0 win=65535
rtt=0.0 ms
len=46 ip=34.66.225.217 ttl=64 id=14250 sport=445 flags=SA seq=0 win=65535
rtt=0.0 ms
```

Figure 7. Hping3 Tools

Figure 7 shows when the hping3 tool works, this tool works by sending as many packets or requests to the server as possible and continuously. So that the traffic on the server will be flooded, this has an effect on server performance will decrease drastically. Other users who will request services from the server cannot be served properly because the data traffic on the server is full.

The picture above shows the top 5 IP addresses that attempted a brute force attack on the server. can be seen from the graph above, the attacker with the IP address 96.63.205.252 has carried out a brute force attack by trying the possible user password as much as 230 times. It can be concluded, the attacker with the IP address 96.63.205.252 really intends to attack the server. while the other attackers only tried the possible user password no more than 20 times. It can be concluded that, this attacker is not really trying to penetrate the server. Maybe they are just learning about network security.

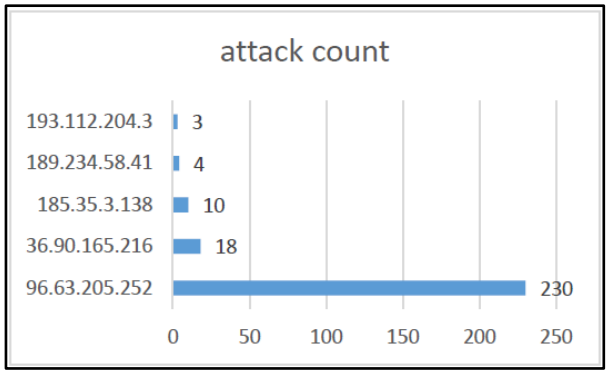

Figure 8. Top 5 Brute Force Attacker

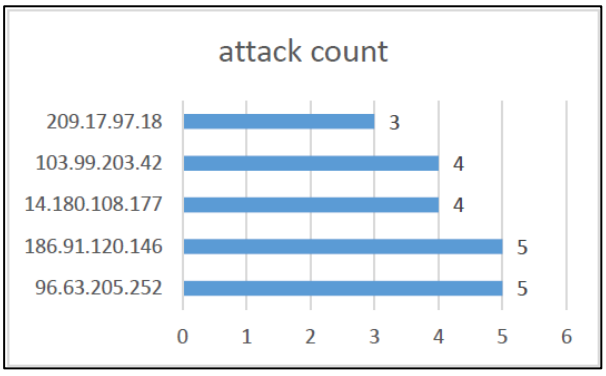

Figure 9. Top 5 DDOS Attacker

Figure 9 shows the top 5 IP addresses attacking the server using the DDoS method. For this type of attack, the number of attempted attacks is not a measure of whether the attacker intends to attack or is just having fun. But when the attacker has sent request data to the server with a large size and continuously for more than 60 seconds. Then that attack is already considered a serious attack.

Conclusions

Of the experiments that have been carried out. honeypots are relatively good at detecting and preventing attacks. Honeypot works by providing bait to attackers so that attackers think they are attacking a legitimate server. honeypot also logs and stores all activity from attackers after they successfully enter the system into a log. with the help of mongoDB and

using the jango framework, the attacker's activity log can be stored properly. With the data that has been stored properly in the database, it will make it easier to process and analyze the data. the data is also easier to convey to the administrator in real time using the android application. In this android application, administrators can monitor attacks that occur, and also execute attackers. Administrators can immediately block IP addresses suspected of attacking servers. Both brute force and DDoS attacks.

References

A. Jain, Dr. BalaBush (2015) "Advaces Trend in Network Security With Honeypot and its Compare Study With Othe Techniques", R.N. Modi Engineering College, Kota, Rajasthan, India, (IJETT), Vol. 29, No. 26, Nov

B. Adam, A. Todd (2016) "What's in Your Honeypot", International Conferrence on Cyber Warfare and Security, 355-IX

J. Kumar Jain, S. Surabi (2012) "Honeypot Base Secure Network System", Computer Science & Engineering Samrat Ashok Technological Institute Vidisha, MP, India, (IJCSE),-Volume 3 – no 2, Feb

K. Rutu (2011) "Honeypot With Honeypot Management System for Web Application", California State University, Long Beach, Proquest Dissertation Publishing

K. Shubham, (2019) "Securing Network Trough Honeypot and its Implementation", International Journal of Advanced Research in Computer Sience, Vol 10, No. 5, Sept-Okt DOI:http://dx.doi.org/10.26483/ijarcs.v10i5.6478

Lakhsmi S. Deepa, G. Arunkumar, V. Madhu (2015) "Network Security Enhancement through Honeypot based Systems", International Journal of Engineering and Technology (IJET), Vol 7, No 1, Mar, ISSN: 0975-4024

M. Solomon Z, P.S. Avadhani (2016) "Honeypot System for Attacks on SSH Protocol", I.J. Computer Network and Information Security, Sept

P. Sheilly, G. Sonali, Apoorva, Lotfy, K. Amandeep, (2016) "Honeypot : A Security Tool in Intrution Detection", International Journal of Advanced Engineering, Management and Science (IJAEMS), Vol 2, Issue 5, May , ISSN: 2454-1311.

R. Rajbhar (2018) "Intrusion Detection & Prevention Using Honeypot", International Journal of Advanced Research in Computer Sience, vol 9, No. 4, July DOI: http://dx.doi.org/10.26483/ijarcs.v9i4.6176

S. Pavol, M. Jakub, H. Martin (2017) "Honeypots and Honeynets : Issues of Privacy", EURASIP Journal on Information Security, April , DOI 10.1186/s13635-017-0057-4

Vladimir B. Oliviera, A. Zair, L. Denivaldo, Mario H. Santos, Valeria P. Fernandes (2013) "HONEYPOTLABSAC: A Virtual Honeypot Framework For Android", International Journal of Computer Network and Communication (IJCNC), vol.5, No.5, July .