

Analysis of a Honeypot Intrusion Detection System for Medical and Healthcare Services

Aastha Yadav ¹, Sarthak Raisurana ², N.Ch. Sriman Narayana Iyengar ^{3*}

Abstract: Cyber-attacks have been increasingly becoming alarming in recent years specifically for medical and healthcare systems. One of the cyber-attackers aims is to break into the medical or healthcare networks and gain access to the patient's medical records. This paper deals with the honeypot-based intrusion detection system to provide information security for medical and healthcare systems. The proposed system utilizes the Dionaea and Kippo SSH (Kippo Secure Shell) honeypots to secure the medical and healthcare network infrastructure and analyze the activities of cyber-attackers. A possible Metasploit and Brute force attacks logged by the Dionaea and Kippo SSH will be analyzed to prepare the malware analysis report of the suspicious file download.

Keywords: Honeypot, Intrusion detection system, Dionaea, Kippo SSH, Metasploit attack, Brute force attack

1. Introduction

Information security has been a prevalent challenge for information technology (IT) systems intended for medical and healthcare services and still needs extensive research and formidable solutions. IT systems for medical and healthcare services were vulnerable to a variety of exploitations from cyber-attackers compromising confidential information of patients and impeding its daily operations if not provided with proper security measures [1]. There is an increasing variety of network-related threats as medical and healthcare services become dependent on networked or online platforms for their daily operations.

Information privacy and security for medical and healthcare services are essentially important in providing for confidentiality, integrity, availability, privacy, authenticity, trustworthiness, non-repudiation, accountability, and auditability [2]. It is essentially necessary to protect personal privacy in order to secure the interests of patients and medical or healthcare personnel. Securing information in medical and healthcare services is important for they require the collection, storage, and use of large

¹ School of Computer Science & Engineering, Vellore Institute of Technology University, Vellore, Tamil Nadu, India
Email: aasthay1705@gmail.com

² School of Computer Science & Engineering, Vellore Institute of Technology University, Vellore, Tamil Nadu, India
Email: sarthak.dbz@gmail.com

^{3*} Sreenidhi Institute of Science and Technology, Yamnampet, Ghatkesar, Hyderabad, India
Email: srimannarayanach@sreenidhi.edu.in (Corresponding Author)

Received [August 6, 2021]; Revised [November 30, 2021]; Accepted [January 18, 2022]



amounts of an individual's personal health information which can be sensitive and requires privacy. Cyber-attackers might aim to access such information to use for their own benefits. In this regard, there is an increasing demand for robust and efficient intrusion detection system (IDS) that can keep track of the activities of cyber-attackers and protect the medical and healthcare services from potential threats and attacks.

The honeypot IDS aims to address the limitations of traditional systems to ensure safety and a secured computing environment. A honeypot is a computer security method used to detect and prevent unauthorized access to an information system. It uses a decoy to deceive an attacker and monitor its activities by making the honeypot act like a legitimate system. They are essentially useful in order to expose the current vulnerabilities of the IT system. The information gathered from the honeypots can be used in preventing potential cyber-attacks in IT systems [3]. The Dionaea honeypot is used for capturing malicious software (malware) which is initially developed under the HoneyNet Project's 2009 Google Summer off Code (GSoC) [4]. It aims to trap malware that exploits the vulnerabilities that were exposed by services offered over the network, and obtains a malware copy for analysis. It utilizes the Server Message Block (SMB) protocol to capture remote exploitable bugs and worms.

This paper deals with the analysis of a honeypot-based intrusion detection system for medical and healthcare services. The system utilizes the features of Dionaea and Kippo SSH honeypots as decoys to attract malware and monitor the activities of cyber-attackers and prevent its future and potential attacks. It aims to analyze the possible Metasploit and Brute force attacks logged by the Dionaea and Kippo SSH (Kippo Secure Shell) in order to prepare the malware analysis report of the suspicious file download.

The rest of this paper is organized as follows: Section 2 discusses the review of related IDS systems; Section 3 outlines the medical and healthcare services as a vulnerable sector for cyber-attacks; the network architecture of the proposed honeypot IDS is outlined in Section 4; the implementation analysis of the proposed honeypot intrusion detection system is shown in Section 5; and the concluding remarks are presented in Section 6.

2. Related Literature

This section identifies the existing intrusion detection systems (IDSs) to assess the requirements in the proposed utilization of honeypots as a form of intrusion detection in the network infrastructure of medical and healthcare services to guarantee its security.

The Network-based Intrusion Detection System (NBIDS) is simply implied by the name "network-based". The NBIDS utilizes a monitoring device that is directly connected to the network infrastructure capable of monitoring the traffic flows. The monitoring device makes use of these traffic flows as its source data in determining whether a particular traffic matches a known attack signature or pattern. The three main signatures used by NBIDS are the attack text string, port signatures, and header signatures. The NBIDS is capable of monitoring the entire network segments for malicious behaviors given the network data flows as its source [5].

The Host-based Intrusion Detection System (HBIDS) consists of loading software onto the system being monitored which is capable of analyzing the system for changes resembling an attack or potential threats. It utilizes log files, auditing agents, communication traffic, system file integrity, suspicious processes, and user privileges in determining potential threats and attacks. The HBIDS is effective in detecting isolated attacks including trusted-insider attacks since the system is monitoring individual hosts [5, 6, 8].

In addition to NBIDS and HBIDS, IDS are also classified into different models in determining a potential threat or attack. The most prevalent models used in detecting potential attacks include

algorithms for statistical-anomaly detection, rule-based detection, and a combination of both statistical and rules-based detection algorithms. The method is to employ the most effective model for a particular environment based on its features.

The statistical-anomaly detection model looks for abnormalities and runs under the assumption that an abnormal behavior indicates a potential threat or attack. It utilizes the factors such as log files, audit files, file or folder properties, and traffic patterns in order to determine the normal behavior of a system. Nonconformity with the normal behavior and activities may lead to suspicious behaviors and can be considered as a potential threat or attack [7].

In the Rule or Signature-based detection model, most cyber-attacks were characterized by a sequence of events or patterns making a signature in defining these attacks. The model analyzes the threat's data source for resemblance with the predefined signatures or pattern of activities. The system raises the alarm whenever signature or pattern matches with threat signatures [7, 8].

Table 1. Identified Gaps for Existing Intrusion Detection Systems

Model	Identified Gaps
NBIDS	NBIDS may not detect isolated potential attacks or threats since it monitors the entire network system. Targeted attacks may not be detected. The compromised machine cannot be detected if it is not passing suspicious traffic over the monitored network. In addition, it cannot detect attacks that are disguised in legitimate network traffic such as Hypertext Transfer Protocol (HTTP), File Transfer Protocol (FTP), or Simple Mail Transfer Protocol (SMTP).
HBIDS	The host-based detection program must be installed to monitor independent machines which are not practical in large-scale environments [8].
Statistical-anomaly detection model	The statistical-anomaly detection model uses the abnormalities from the identified normal activities for the detection of potential threats or attacks. The system adaptively learns the normal behavior or activities. It must be customized based on the normal profile of a particular organization or service for use to detect abnormalities in its activities.
Rule or signature-based detection model	The rule or signature-based detection model is capable only to detect potential threats or attacks where its signatures are known. Newer attacks cannot be detected.

3. Overview on the Vulnerability of Medical and Healthcare Institutions

Based on the Office of the Australian Information Commissioner (OAIC), the medical and health sector has the highest cyber-attack breaches with 23% among industrial sectors [9]. There were about 539 cyber breaches under ransomware (*i.e.*, consists of malicious software or malware that infects a device and holds it hostage to demand payments) that were notified within July–December of 2020. It

was reported that the leading source of data breaches was malicious attacks (*i.e.*, accounting for 58% of notifications).

Healthcare was seen by Experian as particularly vulnerable to cyberattacks since medical identity theft remains so profitable and seen by attackers as relatively easy to exploit [10]. Electronic health records remain to be the top target for hackers and new vulnerabilities were introduced by new mobile applications deployed by medical and healthcare institutions.

The increasing proliferation of cheap and connected Internet of Things (IoT) devices provides an easy gateway for cyber-attackers to unauthorized access critical healthcare information and personal data despite taking stronger cyber security precautions to prevent potential cyber-attacks [9].

In the 2014 SANS survey, it is found that 7% of malicious traffic comes from radiology imaging software, another 7% of malicious traffic came from video conferencing systems, and 3% originated from digital video systems that were used for consultations and remote procedures. The study also shows that 8% of malicious traffic originated from web-based call center websites used by medical supply companies. In addition, 33% of the malicious traffic was transmitted from virtual private network (VPN) applications, whereas 16% was sent by firewalls, 7% was sent from routers, and 3% from enterprise network controllers (ENCs). This result indicates that security devices and applications themselves may have been compromised or such security systems were not detecting malicious traffic coming from network devices. Also, healthcare organizations must keep track of the other types of medical devices as new technologies were being developed [11].

In 2016, there are about 93 major cyber-attack hits in healthcare organizations [1]. According to the report, sophisticated attackers were responsible for the 31% of major data breaches of the Health Insurance Portability and Accountability Act (HIPAA) in the same year which is a 300% increase over the past 3 years. Examples of breached medical equipment causing severe situations include x-ray and dialysis machines.

Medical X-ray machines are used in taking images of dense tissues such as bones and teeth. Radiation emitted from X-ray machines is highly penetrating, ionizing radiation, thus, they can be very dangerous. If a cyber-attacker is able to manipulate the dose or radiation exposure of patients, they can be overexposed resulting in permanent destruction of either sweat glands or the skin. Overexposed to ionizing radiation may result in long-term effects such as carcinogenesis, life span shortening, cataract formation, and increased prevalence of leukemia and other cancers [12].

The dialysis machines are designed to mix and monitor fluids that help to filter unwanted waste products such as salt and excess fluids from the blood. It is used to supplant the kidney's important functions when damaged, dysfunctional, or missing. A single failure of a dialysis machine may not be life-threatening, however, two independent failures caused by cyber-attacks result in operations in unsafe conditions and are life-threatening. Other potential medical equipment that may be targeted by attackers includes infusion pumps, barcode scanning systems, and medical imaging systems [12].

Moreover, since the start of the Coronavirus disease (COVID-19) pandemic, cyberattacks have continued to plague medical and healthcare institutions [13]. Based on the analysis of CyberPeace Institute on the data over 235 cyberattacks against the medical and healthcare sector across 33 countries, there were over 10 million stolen records (*i.e.*, includes social security numbers, patient medical records, financial data, human immunodeficiency virus (HIV) test results, and private details of medical donors). In addition, about 155,000 records are being breached during an attack (*i.e.*, on average).

4. Network Architecture of the Honeypot based IDS

Both the low-interaction and medium-interaction virtual honeypots will be utilized in the proposed model in automatically collecting malware. The low-interaction honeypot provides cyber-attackers with limited access to the operating system. It can be used in detecting known exploits and measuring how often the network gets attacked [14]. There are smaller risks in running low-interaction honeypots as compared to honeypots that cyber-attackers can exploit and control. The medium-interaction honeypots combine the benefits of both low and high-interaction honeypots with regards to botnet detection and malware collection. They provide sufficient responses that make the known exploits wait for certain ports that will bait them to send their payloads.

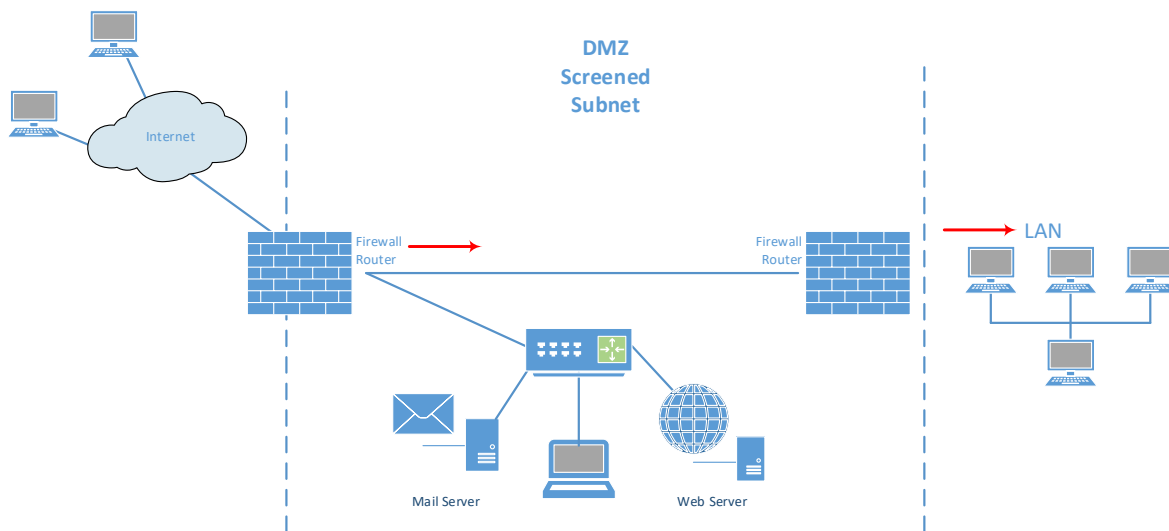


Figure 1. Architecture of Proposed Network Design

This proposed model aims to collect malware using honeypots in order to monitor the activities of cyber-attackers on the shell of a decoy system. The honeypot-based IDS can prevent malware in the form of botnets that can bring down servers using Distributed Denial of Service (DDoS) attacks. Honeypots installed within the demilitarized zone (DMZ) exposed into external traffic will be detecting external attacks and analyses [15]. In addition, honeypots installed on the internal network will be detecting the internal potential threats or attacks. In Figure 1, honeypots will be installed inside the local area network (LAN) to maximize the detection of any malware or malicious activities for in most cases, cyber-attacks in medical and healthcare services are done by insiders.

The proposed system utilizes Dionaea and Kippo SSH honeypots in collecting malware in medical and healthcare services. The Dionaea honeypot is intended to trap malware that exploits the vulnerabilities exposed by medical or healthcare services offered to a network aiming to download a copy of such malware. It uses libev (*i.e.*, a full-featured and high-performance event loop) to get notified once it can act on a socket or perform read or write. If required, the Dionaea offers services via Transmission Control Protocol/User Datagram Protocol (TCP/UDP) and Transport Layer Security (TLS) both for Internet Protocol version 4 (IPv4) and Internet Protocol version 6 (IPv6). It can also offer rate-limiting and accounting limits per connection to both TCP and TLS connections. The Dionaea honeypot detects and evaluates the payload sent by malware with the use of LibEmu in order to obtain its copy. The shellcode measurement and profiling were performed by executing the shellcode in LibEmu virtual machine (VM) and recording application programming interface (API) calls and arguments [4, 16].

Kippo is classified as a medium-interaction SSH honeypot that is designed to log brute force attacks and monitor the entire shell interaction activities performed by the attacker. The SSH protocol can be

utilized to perform a secure remote login over an insecure network to access a remote shell. The Kippo SSH honeypot can be used to monitor and study the activities performed by the attackers after they have compromised a particular system. It allows the attacker to believe that it is accessing a legitimate SSH session with the server, thus, trying to login into the system by guessing the password. The attacker can then interact with the fake system as soon as it successfully guessed the system password, enabling the recording and monitoring of its activities [17, 18].

5. Honeypot Intrusion Detection System Implementation Analysis

This section presents the analysis of the implementation of Dionaea and Kippo SSH honeypots to capture malware. The statistics in collecting binaries to study the types of malware by analyzing activities and behaviors of malware using dockers were presented. The VMWare workstation was utilized in creating a virtual system and installed with Ubuntu 14.04 operating system (OS). The computer running the instance of the Ubuntu OS and executing the VMWare refers to the host machine. The 64-bit Ubuntu was used as the guest OS to run Linux-based honeypots. Each VMWare workstation was allotted a minimum of 256MB of memory. The Dionaea honeypot locates the file wherein the cyber-attacker targets to download from the shellcode and gets the copy of the file. The protocols in downloading the files via Trivial File Transfer Protocol (TFTP) and FTP were implemented using Python (*i.e.*, ftp.py and tftp.py) as part of Dionaea. Dionaea can then post the file to several services such as CWSandbox, Norman Sandbox, or VirusTotal.

```

Terminal
aasthay1705@ubuntu: ~
Trace/breakpoint trap (core dumped)
aasthay1705@ubuntu:~$ dionaea -l all,-debug -L 'con*,py*'
Dionaea Version 0.1.0
Compiled on Linux/x86_64 at Aug 20 2014 17:08:40 with gcc 4.8.2
Started on ubuntu running Linux/x86_64 release 3.13.0-113-generic
Trace/breakpoint trap (core dumped)
aasthay1705@ubuntu:~$ dionaea -u nobody -g nogroup -r /opt/dionaea/ -w /opt/dio
naea -p /opt/dionaea/var/dionaea.pid
Dionaea Version 0.1.0
Compiled on Linux/x86_64 at Aug 20 2014 17:08:40 with gcc 4.8.2
Started on ubuntu running Linux/x86_64 release 3.13.0-113-generic
[03042017 04:14:34] dionaea dionaea.c:245: User nobody has uid 65534
[03042017 04:14:34] dionaea dionaea.c:264: Group nogroup has gid 65534
[03042017 04:14:34] dionaea dionaea.c:273: chroot root has to match workingdir,
try -r /opt/dionaea
Trace/breakpoint trap (core dumped)
aasthay1705@ubuntu:~$
    
```

Figure 2. Dionaea Setup in Creating a User and Group

The Dionaea setup depicted in Figure 2 was used to perform a Metasploit attack and the dionaea.log was used to check if it logs the information. Cyber-attackers do not seek the service, but, they will be asking the service for some packet when they wanted to exploit them, and then Dionaea must detect the sent payload by the attackers in order to gain a copy of the malware. Dionaea utilizes libemu (*i.e.*, the library used for shellcode detection) to perform such a process.

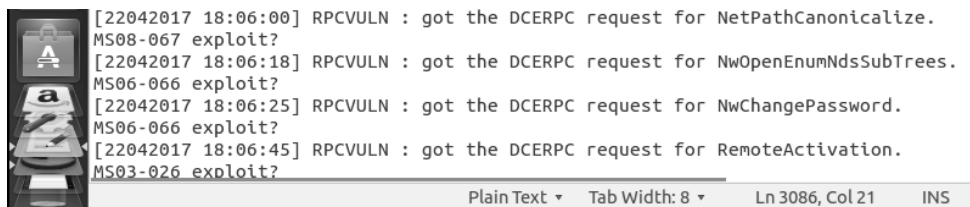
```

[*] Started reverse handler on 192.168.22.128:4444
[*] Using URL: http://0.0.0.0:8080/8yaE0zDnBvrI
[*] Local IP: http://192.168.22.128:8080/8yaE0zDnBvrI
[*] Server started.
[*] Run the following command on the target machine:
python -c "import urllib2; r = urllib2.urlopen('http://192.168.22.128:8080/8yaE0zDnBvrI'); exec(r.read());"
msf exploit(web_delivery) > [*] 192.168.22.129  web_delivery - Delivering Payload
[*] Sending stage (18558 bytes) to 192.168.22.129
[*] Meterpreter session 1 opened (192.168.22.128:4444 -> 192.168.22.129:39843) at 2017-04-24 13:32:33 +0530
sessions -l

Active sessions
=====
  Id  Type
  ---  ---
  1   meterpreter python/python root @ ubuntu 192.168.22.128:4444 -> 192.168.22.129:39843 (192.168.22.129)
msf exploit(web_delivery) > sessions -il

```

Figure 3. The Performed Metasploit Analysis



```

[22042017 18:06:00] RPCVULN : got the DCERPC request for NetPathCanonicalize.
MS08-067 exploit?
[22042017 18:06:18] RPCVULN : got the DCERPC request for NwOpenEnumNdsSubTrees.
MS06-066 exploit?
[22042017 18:06:25] RPCVULN : got the DCERPC request for NwChangePassword.
MS06-066 exploit?
[22042017 18:06:45] RPCVULN : got the DCERPC request for RemoteActivation.
MS03-026 exploit?

```

Figure 4. Dionaea.log Indicates the Malware Information

The Dionaea honeypot also supports shell emulation and downloads through FTP, HTTP, and TFTP for malware. In Figure 3, the script command generated by the Metasploit attack on the target enables complete control of the system including keystroke logging, turning the microphone on, and reading or deleting any files on the system. The SMB protocol used by Dionaea is a very popular target for worms and remotely exploitable bugs. Figure 4 is a Dionaea log file that logs a possible MS08-067 exploit.




SHA256:	127d1cd82f4c6697eb371dcf5619481606cdef43139b07692f4beb2b59b3ea8c	
File name:	Qarawify	
Detection ratio:	3 / 55	
Analysis date:	2017-04-24 11:43:17 UTC (0 minutes ago)	
Analysis Additional information Comments Votes		
Antivirus	Result	Update
Avast	JS.Downloader-EQA [Trj]	20170424
ClamAV	Legacy.Trojan.Agent-37025	20170424
Qihoo-360	Script/Trojan.Downloader.4e1	20170424

Figure 5. VirusTotal scan of the file

Dionaea honeypot also includes a VirusTotal module that automatically submits the suspicious files and prepares a malware analysis report. The file downloaded in Figure 3 undergoes a VirusTotal scan for malware behavior as shown in Figure 5.

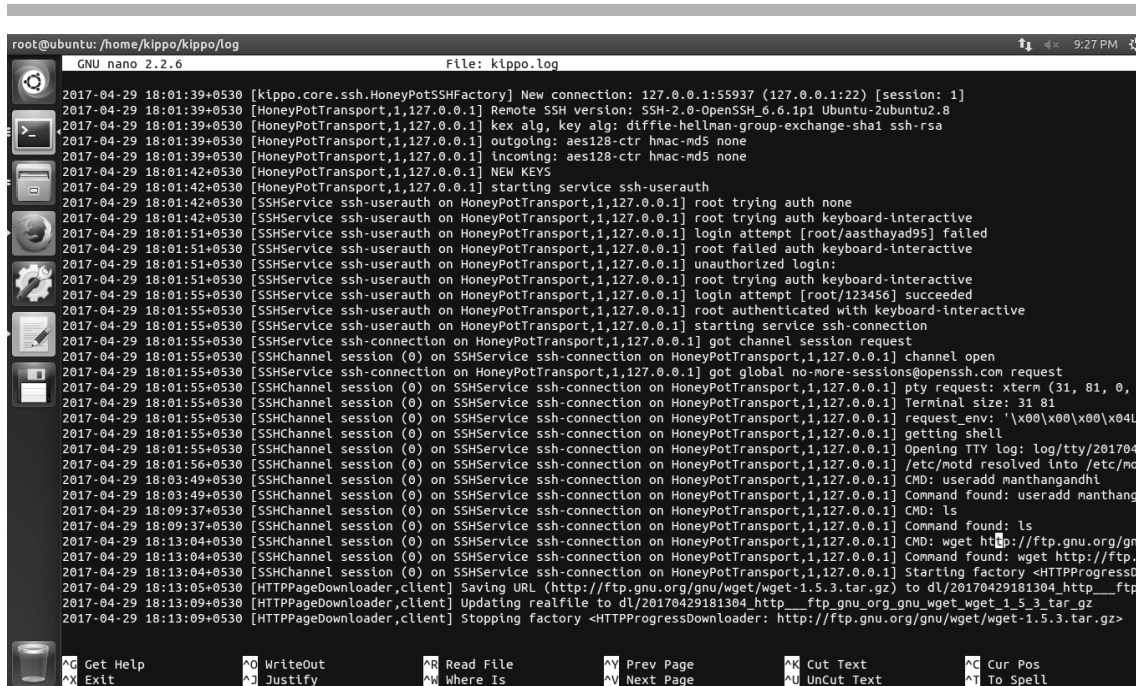


Figure 6. Intruder’s activity on Kippo on the fake file system

The next process would be to track the potentially malicious activity of the attacker using the Kippo SSH setup on port 22. Figure 6 depicts the attacker’s activity logged on kippo.log. It includes the username and passwords that were entered including the add, modify, and delete commands run by the attacker on the files of the fake file system. The system also allows the use of wget (*i.e.*, retrieves content from web servers) and other commands that were commonly used in fetching or downloading files. The files downloaded with the wget command will be saved for later analysis in the download (dl) folder of logs.

Table 2. Kippo’s Logged Contents

Essential Information	Log File
wget commands	dl/
Username attempt	mysql.sql
Password attempt	mysql.sql
Session ID	log/tty/
Session Timestamp	log/tty/
Fake file system contents	honeys/

Table 2 includes the location of all essential information logged about the cyber-attacker’s activity on the fake file system.

In Figure 7, the message digest 5 (md5) hash value downloaded over 2 months by the Dionaea honeypot can be accessed up and running through the binaries folder. Dionaea honeypot successfully logs all the payloads and shell bindings and saves a copy of the malware for further analysis.

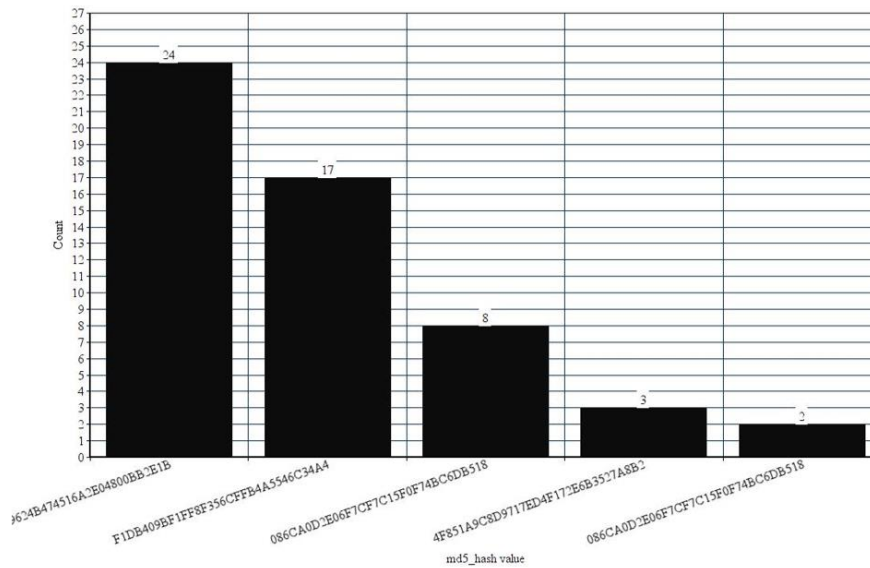


Figure 7. The md5 hash value of the Downloaded Malware

Table 3. Honeypot Systems as Security Mechanism

Honeypot System	Attacker's Activity	Potential Vulnerability	Honeypot Solution
Dionaea	Send an email with a payload using Metasploit activity that runs on the medical device	Exposed networking equipment and admin computers of Medical and Healthcare services to exploit critical medical devices	Logs the downloaded payloads and performs the analysis on malware detected using VirusTotal, CWSandbox, etc.
Kippo SSH	Successful SSH and web logins on critical medical or healthcare devices	Medical and Healthcare Secure Server	Logs the activities of the attacker including Internet Protocol (IP) addresses, geographical location, inputs, passwords, and usernames tried on the fake file system.

Table 3 explains how honeypots respond to attackers' activities attempting to gain access to medical devices and equipment to control, modify, or copy patients' critical information on medical or healthcare services.

6. Conclusion

This paper has analyzed honeypot-based intrusion detection systems for medical and healthcare services. It utilizes the full advantages of Dionaea and Kippo SSH honeypots to act as an effective security mechanism placed in the DMZ in order to trap malware and to provide reports of malware analysis on logged binaries. The honeypots can also be used to monitor and log all the activities of an attacker on the shell. This honeypot-based IDS system can also be used to send emails to network administrators of medical and healthcare systems notifying the attacker's activities. Cybersecurity for medical and healthcare services is essentially important to protect the privacy of patients as well as safeguard human lives.

References

- [1] K. Sheridan, “Major Cyberattacks on Healthcare Grew 63% in 2016”, www.darkreading.com/attacks-breaches/major-cyberattacks-on-healthcare-grew-63--in-2016/d/d-id/1327779 (Accessed April 28, 2021).
- [2] S. J. Nass, L. A. Levit, L. O. Gostin, “Beyond the HIPAA Privacy Rule: Enhancing Privacy, Improving Health Through Research”, www.ncbi.nlm.nih.gov/books/NBK9581/ (Accessed April 28, 2021).
- [3] B. Hancock and J. W. Rittinghouse, “Cybersecurity Operations Handbook: The Definitive Reference on Operational Cybersecurity”, 1st Edition, New York, USA, Elsevier Science Inc., 2003, ISBN: 9780080530185.
- [4] E. Tan, “Dionaea – A Malware Capturing Honeygot”, www.div0.sg/post/dionaea (Accessed April 28, 2021).
- [5] J.S. Sherif and R. Ayers, “Intrusion detection: methods and systems, Part II”, Information Management & Computer Security, vol. 11, no. 5, 2003, pp. 222-229, doi: 10.1108/09685220310500135.
- [6] Lata and I. Kashyap, “Study and Analysis of Network based Intrusion Detection System”, International Journal of Advanced Research in Computer and Communication Engineering, vol. 2, no. 5, May 2013, pp. 2032-2038.
- [7] C. Herringshaw, “Detecting Attacks on Networks”, Computer, vol. 30, no. 12, December 1997, pp. 16-17, doi: 10.1109/2.642762.
- [8] J. Barnes, “Intrusion Detection Systems in Hospitals: What, Why, and Where”, www.infosecwriters.com/text_resources/pdf/IDS_JBarnes.pdf (Accessed April 28, 2021).
- [9] Data & Security, “Why cyber-attacks are on the rise in healthcare”, www.medicaldirector.com/news/data-security/2021/04/why-cyber-attacks-are-on-the-rise-in-healthcare (Accessed April 28, 2021).
- [10] B. Monegain, “Healthcare top target for cyberattacks in 2017, Experian predicts”, www.healthcareitnews.com/news/healthcare-top-target-cyberattacks-2017-experian-predicts (Accessed May 12, 2021).
- [11] P. Ouellette, “SANS survey analyzes health endpoint vulnerabilities”, <https://healthitsecurity.com/news/sans-survey-analyzes-health-endpoint-vulnerabilities> (Accessed May 12, 2021).
- [12] L. Ayala “Active Medical Device Cyber-Attacks”, in Cybersecurity for Hospitals and Healthcare Facilities: A Guide to Detection and Prevention, Chapter 3, USA, Apress, 2016, pp.19-29, doi: 10.1007/978-1-4842-2155-6.
- [13] S. Duguin, “If healthcare doesn't strengthen its cybersecurity, it could soon be in critical condition”, www.weforum.org/agenda/2021/11/healthcare-cybersecurity/ (Accessed May 12, 2021).
- [14] N. Provos and T. Holz, “Virtual honeypots: from botnet tracking to intrusion detection”, USA, Addison-Wesley Professional, 2007, ISBN: 978-0-321-33632-3.
- [15] D. P. Conde, “Deploying Honeygot and the Security Architecture of a Fictitious Company”, www.giac.org/paper/gppa/548/deploying-honeygot-security-architecture-fictitious-company/105318 (Accessed May 12, 2021).
- [16] I. Koniaris, G. Papadimitriou, P. Nicopolitidis, M. Obaidat, “Honeygot Deployment for the Analysis and Visualization of Malware Activity and Malicious Connections”, In Proceedings of the 2014 IEEE International Conference on Communications (ICC), Sydney, NSW, Australia, June 10-14, 2014, pp. 1819-1824, doi: 10.1109/ICC.2014.6883587.
- [17] M. Rawat, “Tracking Attackers with a Honeygot – Part 2 (Kippo)”, www.resources.infosecinstitute.com/tracking-attackers-honeygot-part-2-kippo/#gref (Accessed May 12, 2021).
- [18] Unixmen, “Kippo – A SSH Honeygot to Monitor Brute Force Attacks on Debian 7/Ubuntu 13.10”, www.unixmen.com/kippo-ssh-honeygot-monitor-brute-force-attacks-debian-7-ubuntu-13-10/ (Accessed May 12, 2021).