Conpot: Deployment and Case Study

Priyanshu Sharma
Bachelor of Technology(CSE)
Bennett University
Greater Noida, India
priyanshusharma3377@gmail.com

Sachchit Bhasin
Bachelor of Technology(CSE)
Bennett University
Greater Noida, India
e21cseu0021@bennett.edu.in

Akshit Verma
Bachelor of Technology(CSE)
Bennett University
Greater Noida, India
e21cseu0167@bennett.edu.in

***Abstract*—Honeypots are a famous idea used for risk intelligence and have become extra everyday inside ICS environments. A standard ICS honeypot, Conpot, is famous and has been deployed on a huge scale. These deployments aren't constantly efficiently configured and feature peculiar traits as compared to a actual industrial manipulate system. We hereby has done the analysis of the conpot honeypot by deploying it in three ways from our system to other IP addresses. This paper conclude the ways we have executed in a brief manner. We came to the conclusion that right deployment of a low-interaction honeypot, consisting of Conpot, requires time and assets to absolutely obfuscate the tool and trap or confuse the attacker to a constrained level. However, small modifications to the default configuration does growth the overall performance of Conpot and results in greater returning traffic.**

Keywords- Honeypots, ICS, Conpot, Deployment, low-interaction honeypot

I. Introduction

A honeypot is a protection mechanism that creates a digital lure to trap attackers. An deliberately compromised laptop gadget lets in attackers to make the most vulnerabilities so that you can examine them to enhance your protection policies. You can follow a honeypot to any computing useful resource from software program and networks to report servers and routers.

Honeypots are a form of deception generation that lets in you to apprehend attacker conduct patterns. Security groups can use honeypots to research cybersecurity breaches to accumulate intel on how cybercriminals operate. They additionally lessen the hazard of fake positives, while as compared to standard cybersecurity measures, due to the fact they're not likely to draw valid activity.

Honeypots range primarily based totally on layout and deployment models, however they're all decoys meant to seem like valid, prone structures to draw cybercriminals.

Conpot is a open source honeypot available online on conpot.org; Conpot is a ICS/SCADA honeypot. It is a invaluable tool for guarding any infrastructure or organizations precious data against the attackers who desire for their data. Like any other honeypot conpot also works by creating a fake or fabricated file system or network before the real treasure to fool the attackers and we can actually than look out for what tools they are pursuing to make this attack happen we could be more prepared for the further attack against cyberattacks on industrial control systems.

This paper targets to delve into the sector of honeypots, with a selected attention on Conpot and its deployment strategies. We will discover the history and evolution of honeypots as a cybersecurity era and look at the specific skills and blessings that Conpot gives withinside the context of commercial manipulate systems. Furthermore, the paper will speak the numerous deployment strategies and first-class practices for Conpot honeypots, allowing businesses to efficiently put in force them as a part of their cybersecurity strategy.

II. History

The concept of honeypots commenced in 1991 with publications, "The Cuckoos Egg" and "An Evening with Breford". "The Cuckoos Egg" via way of means of Clifford Stoll became approximately his revel in catching a pc hacker that became in his organisation trying to find secrets. The different publication, "An Evening with Berferd" via way of means of Bill Chewick is ready a pc hacker's movements via traps that he and his colleagues used to seize him. In each of those writings had been the beginnings of what have become honeypots. The first kind of honeypot became launched in 1997 referred to as the Deceptive Toolkit. The point of this package became to apply deception to attack back. In 1998 the primary industrial honeypot got here out. This became referred to as Cybercop Sting. In 2002 the honeypot will be shared and used all around the world. Since then honeypot generation has stepped forward significantly and many honeypot customers sense that that is best the beginning. In the year, 2005, The Philippine Honeypot Project became commenced to promote pc protection over withinside the Philippines.

III. Background

Honeypots constitute a proactive technique to cybersecurity via way of means of developing deceptive, inclined objectives that divert the eye of capability attackers from crucial structures and actual assets. They may be classified into diverse types, consisting of low-interplay honeypots, high-interplay honeypots, and hybrid honeypots, every presenting extraordinary ranges of engagement with malicious actors.

Honeypots have an extended and wealthy history, with early iterations serving in general as studies equipment and getting to know aids to recognize attacker behavior. Over time, their programs have accelerated to consist of community defense, hazard intelligence, and incident response. Researchers and

safety experts have diagnosed the price of honeypots in improving situational attention and expertise the ever-evolving hazard landscape.

One of the important thing demanding situations in deploying honeypots is making sure their authenticity and believability. Conpot addresses this undertaking via way of means of specializing in commercial manipulate structures and SCADA devices, making it an appealing alternative for agencies searching for to guard crucial infrastructure. The deployment of Conpot in a community surroundings can considerably beautify the detection, analysis, and mitigation of cyber threats focused on commercial structures.

A. Cloud Models

The adoption of cloud computing has delivered new dimensions to the deployment of honeypots. Cloud transport fashions for honeypots leverage the scalability, accessibility, and cost-performance of cloud offerings to beautify the effectiveness of those cybersecurity tools. Organizations can install honeypots withinside the cloud, taking gain of Infrastructure as a Service (IaaS), Platform as a Service (PaaS), or maybe Software as a Service (SaaS) fashions. Cloud-primarily based totally honeypots may be effortlessly provisioned, managed, and scaled in line with the organization's needs. They permit the deployment of disbursed honeypot networks throughout geographically dispersed records centers, presenting a broader assault floor for tracking and records collection. Furthermore, cloud-primarily based totally honeypots are perfect for agencies with constrained on-premises resources, as they could harness the computing electricity and garage skills of the cloud provider.

Cloud-primarily based totally honeypots additionally provide the advantage of improved records evaluation and centralized management. The records accrued via way of means of honeypots throughout diverse cloud times may be consolidated and analyzed in a centralized manner, presenting a holistic view of the chance landscape. Additionally, the scalability of cloud transport fashions lets in agencies to speedy adapt to converting chance eventualities via way of means of spinning up extra honeypot times as needed. Furthermore, cloud carriers regularly provide superior protection features, inclusive of DDoS safety and intrusion detection, which could supplement the honeypot deployment. However, agencies should be diligent in securing the cloud-primarily based totally honeypot infrastructure itself to save you attackers from compromising the honeypots or the use of them as a springboard for similarly attacks. In summary, cloud transport fashions for honeypots introduce new tiers of agility and performance, making them a compelling choice for agencies looking for to strengthen their cybersecurity efforts.

B. ICS (Industrial Control System)

Industrial Control Honeypots, often abbreviated as ICS honeypots, are specialized cybersecurity tools tailored to safeguard industrial control systems (ICS). These systems are the foundation of critical infrastructure and are prone to cyber threats that can have dire real-world consequences. ICS honeypots emulate ICS components and protocols, drawing potential attackers away from actual systems. By capturing and analyzing these adversaries' behaviors, ICS honeypots offer invaluable insights into ICS-specific threats, enabling organizations to strengthen their defenses. Deploying ICS honeypots is a proactive measure in the ongoing effort to enhance the resilience and security of critical infrastructure and industrial control systems.

C. Other Honeypots

This section lists the ICS honeypots used previously other than conpot

1) Honeyd-SCADA: An extension of the famous Honeyd honeypot, Honeyd-SCADA focuses on emulating SCADA protocols and services, making it a precious device for tracking and studying threats towards SCADA systems.

2) DShield: Focused on emulating the Modbus protocol, that's extensively utilized in ICS environments. DShield is devoted to tracking and accumulating data on capability threats to the Modbus protocol, helping withinside the detection of assaults concentrated on unique ICS gadgets.

3) GasPot: A deception honeypot that emulates fueloline potentiometers and regulators utilized in herbal fueloline infrastructure. GasPot draws attackers trying to compromise vital additives in fueloline distribution systems, imparting insights into threats towards fueloline-associated ICS.

4) Laconia: A Python-primarily based totally ICS honeypot framework designed for simulating diverse ICS protocols and services. It permits groups to create custom designed ICS honeypots primarily based totally on their unique desires and objectives.

5) Mnemosyne: An open-supply ICS honeypot designed for tracking and studying assaults towards ICS and SCADA systems. Mnemosyne gives a number emulated ICS gadgets and protocols.

6) Sophia: An ICS honeypot targeted at the Modbus protocol. Sophia gives a bendy and extensible platform for tracking and analyzing assaults concentrated on Modbus-primarily based totally ICS gadgets.

7) S4 Insecure Suite: Developed with the aid of using digitalbond.com, this honeypot suite consists of numerous ICS honeypots and equipment for taking pictures and studying assaults towards SCADA and ICS systems.

8) ECSimHoneypot: An ICS honeypot designed to emulate the Emerson Process Management DeltaV dispensed manage system (DCS). It gives insights into capability threats concentrated on DeltaV systems.

9) SHIVA: The "SCADA Honeypot with Intelligent Virtual Analyzer" emulates SCADA protocols to draw and examine assaults towards SCADA systems, specializing in hazard detection and response.

IV. Types of Honeypots

A. Production Honeypot

They are used in performing an advanced detection function. They prove whether the security function of Honeypot is

inadequate in case of an attack which becomes hard to lock. However measures should be taken to avoid a real attack. With the knowledge of the attack on the Honeypot it is easier to determine and close security holes. Honeypot allows justifying the investment of a firewall. With a Honeypot there is recorded evidence of attacks. The system can provide information for statistics of monthly happened attacks. A person with legal access to the internal network can pose an unidentifiable threat. Activities on Honeypots can be used to proof if that person has malicious intentions. Another benefit and the most important one is that a Honeypot detects attacks which are not caught by other security systems.

B. Research Honeypot

A research Honeypot is used in a different scenario. A research Honeypot is used to learn about the tactics and techniques of the Blackhat community (In the computer security community, a Blackhat is a skilled hacker who uses his or her ability to pursue his interest illegally).

The Honeypot operator gains knowledge about the Blackhats tools and tactics. When a system was compromised the administrators usually find the tools used by the attacker but there is no information about how they were used. A Honeypot gives a real-live insight on how the attack happened.

Honeyed Research: Honeypots against spam: Honeyd can be used effectively to battle spam. Since June 2003, Honeyd has been deployed to instrument several networks with spam traps. We observe how spammers detect open mail relays and so forth. The diagram on the right shows the overall architecture of the system. The networks are instrumented with open relays and open proxies. We intercept all spam email and analyze why we received it. A single Honeyd machine is capable of simultaneously instrumenting several C- class networks. It simulates machines running mail servers, proxies and web servers. Captured email is sent to a collaborative spam filter that allows other users to avoid reading known spam. Curiously, this setup has also been very successful in identifying hosts infected with worms. Our findings are going to be made available as research paper in the near future.

C. OTHERS

There are also other types of honeypots:

1) Looking for trouble: Client honeypots: Instead of passively waiting for an attack, client honeypots will actively search out malicious servers; typically this has centered on web servers that deliver client- side browser exploits, but is certainly not limited to such. Recently, client honeypots have expanded to investigate attacks on office applications.

Capture HPC is now in version 2.0 and allows the use of different clients, such as Firefox, RealPlayer, Microsoft Word, etc, as well as an option to collect pushed malware and log tcpdump captures of the interactions between client and webserver. Client honeypots need to interact with servers in order to determine whether they are malicious or not. With high interaction client honeypots, this is quite expensive, and therefore selection of what servers to interact with can greatly increase the success rate of finding malicious servers on a network.

2) Niche players: Application-specific honeypots: This is application or protocol specific honeypots. These honeypots are designed to catch spam by masquerading as open email relays or open proxies. Jackpot is written in Java and pretends to be a misconfigured SMTP server which allows relaying. Instead however, it presents a list of messages to the user, who can then pass the spammer's test message and hold the rest of the spam run. (Usually, spammers will attempt to deliver a test email to verify the host in question is actually an open relay.).

The protocol which has been given attention recently is HTTP, specifically web application honeypots. The Google Hack Honeypot is designed to provide reconaissance against attackers that use search engines as a hacking tool against your resources.

V. METHODOLOGY AND DESIGN

This section concludes different methodologies and techniques to run a conpot.

A. Docker

Docker packing containers are lightweight, stand-alone, and transportable software program applications that encapsulate an utility and its dependencies, which includes libraries and runtime environments. They offer consistency in development, testing, and deployment, making sure that programs run reliably throughout distinctive environments. Docker's containerization era gives a streamlined and green manner to isolate and control programs, making it a famous preference for microservices architectures and cloud-local development.

Follow the steps given to run conpot docker container

1) via pre-built image:

- Install Docker
- Run *docker pull honeynet/conpot*
- Run *docker run -it -p 80:80 -p 102:102 -p 502:502 -p 161:161/udp –network=bridge honeynet/conpot:latest /bin/sh*

2) building image from source:

- Install Docker
- Clone this *git clone https://github.com/mushorg/conpot.git* and *cd conpot/docker*
- Run *docker build -t conpot*
- Run *docker run -it -p 80:8800 -p 102:10201 -p 502:5020 -p 161:16100/udp -p 47808:47808/udp -p 623:6230/udp -p 21:2121 -p 69:6969/udp -p 44818:44818 –network=bridge conpot*

3) building image from source via docker-compose:

- Install Docker-Compose
- Clone this *git clone https://github.com/mushorg/conpot.git* and *cd conpot/docker*
- Build the image with *docker-compose build*
- Check if the Docker Compose is intalled properly *docker-compose up*

- Permanently run as a daemon with *docker-compose up -d*

To confirm the setup search for the ports assigned

B. Raw Conpot Installation

This method installs and deploy the conpot from your linux system for local implementation by building a virtualized enviroment.

1) Installing conpot on linux:

- Ensure your Ubuntu Installation is up to date: *sudo apt update*
- Install dependencies: *sudo apt-get install git libsmi2ldbl smistrip libxslt1-dev python3.6-dev libevent-dev default-libmysqlclient-dev*
- Install virtualenv: *sudo apt-get install python3-pip sudo pip3 install virtualenv*
- Create a Virtual Environment (conpot is environment name in this case): *virtualenv –python=python3.6 conpot*
- Activate the environment ('conpot' is the environment name in this case): *source conpot/bin/activate*
- Upgrade and install basic tools dependencies within the environment: *pip install –upgrade pip pip install –upgrade setup tools pip install cffi*
- Install base (table) version of Conpot from PYPI: *pip install conpot*
- Test Conpot using the testing configuration- You are will verify that the conpot boots without issues in the testing configuration. Remember that the default and testing templates use inaccurate port numbers (i.e. 8800 for http instead of 80): *conpot -f –template default*
- Verify Conpot is up: - Open browser and go to "*127.0.0.1:8800*" - You should see a minimal Web page with the word "Technodrome" at the top - Ensure you can see this before moving on - Use CTR+C to shut down the conpot

2) Building a Config File:

- Find the file "testing.cfg" (Should be at /home/conpot/lib/python3.6/site- packages/conpot)
- Make a copy of "testing.cfg" and change name to "config.cfg"
- Place your new "config.cfg" in a new location (I placed mine at /home/conpot/)
- Open "config.cfg" for editing: *cd /conpot/ nano config.cfg*
- Make the following changes under [Virtual file system] change to: - data fs url = /tmp/ - fs url = tar:///home/conpot/conpot/lib/python3.6/site- packages/conpot/data.tar - Ensure a data.tar file is in the above location
- Test config.cfg file using default template- You will verify that the conpot boots without issues in the default configuration. Remember that the default and testing templates use inaccurate port numbers (i.e. 8800 for http instead of 80). NOTE: Installation and use directions for a terminal-based browser called "lynx" is in section 4.5 of this guide: *conpot –c /conpot/config.cfg –template default*
- Verify Conpot is up: - Open browser and go to "127.0.0.1:8800" - You should see a minimal Web page with the word "Technodrome" at the top - Ensure you can see this before moving on - Use CTR+C to shut down the conpot

3) Install and Configure Authbind:

- Install Authbind: *sudo apt-get install authbind*
- Conduct the following steps for the following ports: 21, 69, 80, 102, 161, 502, 623- NOTE: in step 'b.' below our username was conpot, therefore substitute in your username: *sudo touch /etc/authbind/byport/(port) (I.e. /byport/80) sudo chown conpot:conpot /etc/authbind/byport/(port) sudo chmod 755 /etc/authbind/byport/(port)* NOTE: For port numbers greater than 512, additional verification is needed by the system to bind. You must add '!' in front of port 623 in byport folder (IPMI will NOT work w/o this step). You will need 'root' access to make this change. (i.e. /etc/authbind/byport/!623)

4) Correct Port Numbers Within Default Template:

- On terminal: *cd "/home/conpot/lib/python3.6/site- packages/conpot/templates/default*

5) Boot Conpot Using the Default Template and Authbind:

- Clone this *authbind conpot -c /conpot/config.cfg –template default*
- Open the browser and go to *127.0.0.1*

6) Verify Conpot Visibility Outside Your Home/ Local Network:

- Ensure your network is bridged on your Virtual Machine - For VirtualBox: Shut down your Ubuntu VM and go to Virtualbox - Right click on your VM and select 'Settings' - In 'Network' under 'Adapter 1', select 'Bridged Adapter' in 'Attached to:' - Click 'OK' to save changes and reboot your VM
- Run *source conpot/bin/activate* (conpot was the name of my virtual environment)
- Run *authbind conpot -c /conpot/config.cfg –template default*

VI. Deploying on a University Network: A Case Study

Universities, as reservoirs of highbrow capital and crucibles of information dissemination, discover themselves uniquely susceptible to cyber threats. The efficiency of touchy studies data, the economic property beneathneath their custodianship, and the various expanse in their consumer base converge to create a fascinating panorama for malicious actors. Recognizing this, the strategic deployment of a honeypot stands as a sentinel poised to intercept malevolent endeavors, supplying a useful vantage factor to scrutinize, evaluate, and reply to the myriad diversifications of cyberattacks that threaten the sanctity of the college network. In this paper, we embark on an highbrow odyssey, delving into the deployment strategies,

the demanding situations and rewards, and the profound implications for shielding the citadels of getting to know withinside the virtual age.

A. The Honeypot Trilogy:

1) LIHP: Low-Interaction Honeypots are cybersecurity equipment designed to imitate handiest the superficial conduct of actual structures and services. They provide confined interplay capabilities, making them much less resource-extensive and simpler to set up and maintain. LIHPs normally characteristic via way of means of emulating open ports and services, attractive ability attackers to interact with the decoy system. While they lack the intensity of records furnished via way of means of higher-interplay honeypots, LIHPs are powerful for figuring out scanning and reconnaissance activities, and that they assist shield actual structures via way of means of diverting attackers farfar from real assets. Their low threat of compromise and ease lead them to appropriate for agencies searching out a cost-powerful and low-renovation method to honeypot deployment.

2) MIHP: Medium-Interaction Honeypots strike a stability among the realism of high-interplay honeypots and the simplicity of low-interplay honeypots. They simulate the conduct of actual structures and offerings to a slight extent, providing extra distinct interplay with capacity attackers. MIHPs can seize precious statistics approximately attacker techniques and intentions with out the complexity and threat related to high-interplay honeypots. They are regularly hired for danger detection and analysis, supplying corporations with insights into capacity threats even as minimizing the protection burden.

3) HIHP: High-Interaction Honeypots constitute the maximum immersive form of honeypot, carefully emulating actual systems, applications, and services. HIHPs provide considerable interplay with capacity attackers, letting them carry out a huge variety of sports as though they had been compromising authentic assets. This complete emulation gives in-intensity insights into attacker behavior, tactics, and intentions. However, HIHPs require greater resources, expertise, and cautious control because of the heightened hazard of compromise. Organizations frequently use HIHPs for superior risk research, incident response, and gaining a profound expertise of state-of-the-art assault techniques.

B. Usage of Deploying to UNI Networks

Deploying honeypots in the confines of a college community is a prudent preference withinside the relentless struggle in opposition to cyber threats. In an generation in which highbrow capital and studies statistics are an increasing number of digitized, universities locate themselves perched upon a significant repository of precious information, making them engaging goals for cybercriminals. Honeypots function virtual decoys that imitate valid systems, applications, or services, attracting capacity attackers and luring them farfar from the real college community. By diverting malicious actors to those misleading systems, universities can proactively locate and screen nefarious sports whilst safeguarding their important highbrow property, studies findings, and economic assets. Moreover, honeypots provide a completely unique vantage factor for cybersecurity specialists to study and examine rising assault techniques, for this reason empowering establishments to beef up their defenses and reply unexpectedly to threats that can compromise the integrity in their virtual ecosystems.

In addition to their defensive role, honeypots can extensively decorate the cybersecurity posture of universities with the aid of using presenting real-time chance intelligence. By shooting and studying the tactics, techniques, and methods hired with the aid of using capacity adversaries, universities can live in advance of evolving cyber threats. This precious statistics now no longer simplest aids withinside the identity of vulnerabilities in the community however additionally informs protection specialists approximately the motivations and intentions of malicious actors. It equips universities with the understanding required to fine-track protection policies, replace defenses, and domesticate a protection-conscious lifestyle amongst personnel and students. The deployment of honeypots inside a college community is a proactive step closer to mitigating risks, fortifying defenses, and making sure the uninterrupted pursuit of educational excellence in an an increasing number of virtual and interconnected world.

C. Honeypots Deployment

Honeypots were deployed using Docker which is an open-source platform for running, developing and distributing applications. Docker offers the possibility of grouping all the necessary dependencies inside one package, named container, which is offering isolation, abstraction and security . Therefore, the honey- pots were deployed into individual containers to ensure isolation and also to avoid any errors to escalate. In Figure the honeypots relation with Docker is demonstrated, and the approach is presented horizontally. For bringing more value to the architecture, the honeypots were integrated with University's existing network, and the following subsection will present a general overview of how the integration was made.

D. Integration with Honeypot

Docker was hosted on a Virtual Private Server (VPS) provided by University. Figure gives an overview of the architecture. The VPS was configured on a small subnet (X.X.X.113/29) that was sitting outside main firewall, and a firewall (see the figure) was setup by us to control the trac to and from the VPS. For this reason, the VPS had a principal network interface used exclusively for administration purposes, the connection was established over SSH, and a number of secondary network interfaces were created in software for the honeypots.

Considering the design from a security perspective, traffic originated from the VPS was not allowed to go back to main network. As a consequence all traffic to the Internet was freely allowed, since it was also important to keep the appearances and to not raise any suspicions for the attackers. In addition, four secondary network interfaces were created and the IPs

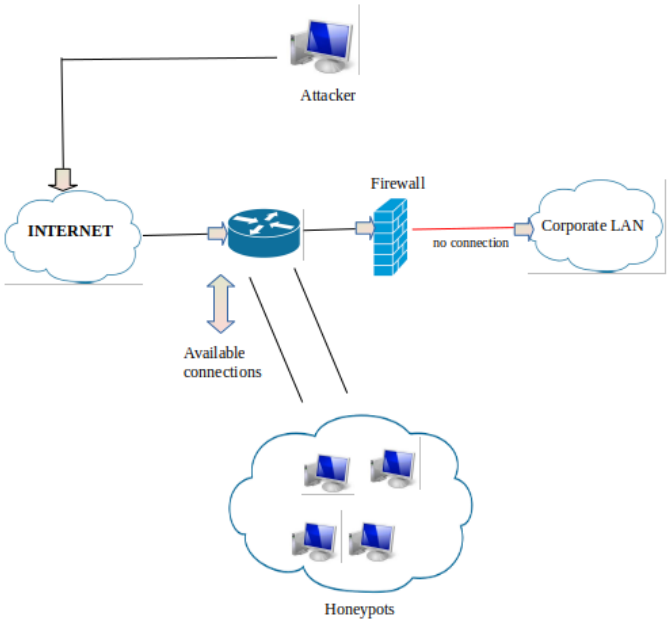

Fig. 1 An overview on how Honeypots work

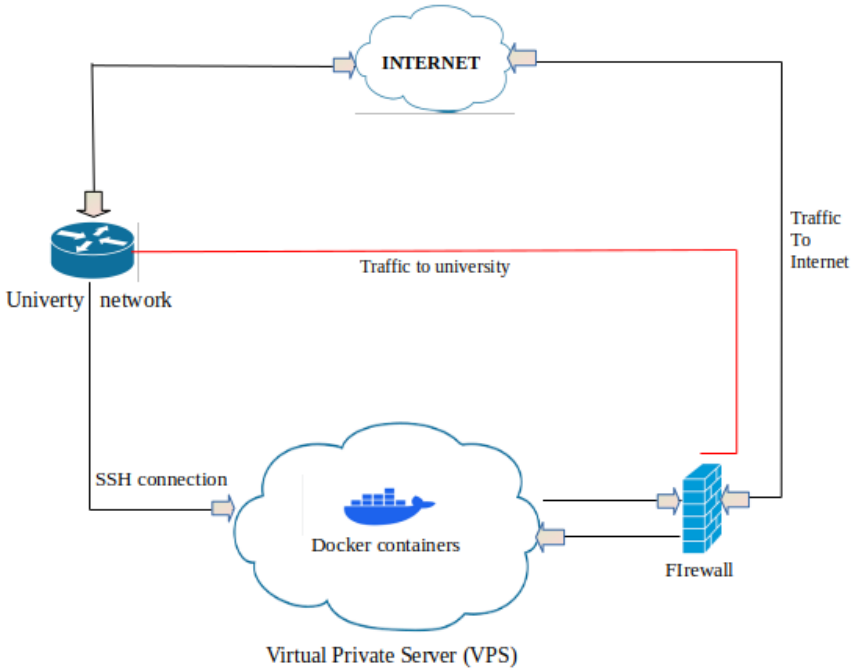

Fig. 3 Honeypot integration with University's network (Case study)

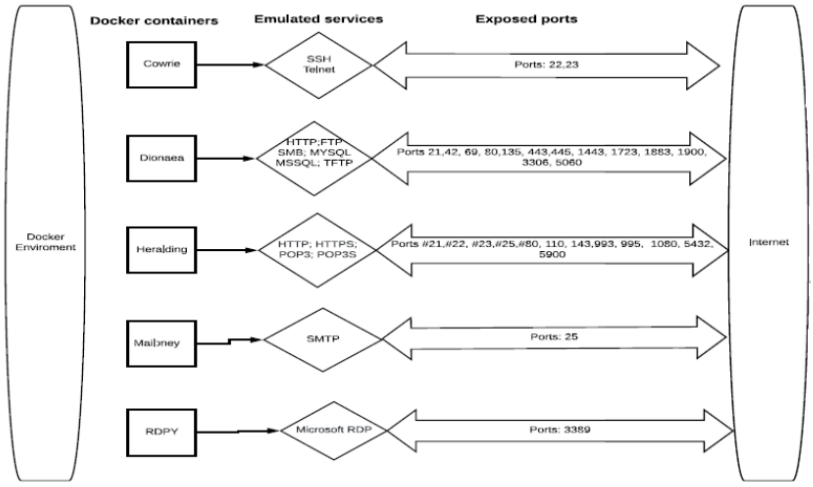

Fig. 2 Honeypots integration with Docker conatiners

TABLE I
THIS TABLE INCLUDES THE PRINCIPAL CHARACTERISTICS OF LIHP,MIHP AND HIHP.

	LIHP	MIHP	HIHP
real operating system	no	no	yes
risk of compromise	low	mid	high
wish of compromise	no	no	yes
information gathering	low	mid	high
knowledge to deploy	low	mid	high
knowledge to develop	low	high	high
maintenance time	low	low	very high

were distributed across the docker containers. The primary containers behaviour was modified by as- signing a public static IP address to every container in order to integrate them with the existing University network. All the interactions with the honeypots are stored individually in log files and therefore a method to structure and analyze the files is presented in the following subsection.

VII. CONCLUSION

In this research paper, we launched into an exploratory adventure into the arena of honeypots, losing mild on their importance in current cybersecurity and offering a compelling case take a look at that exemplifies their realistic utility. Honeypots, as our take a look at has shown, are flexible equipment that function each a proactive protection mechanism and a fount of helpful chance intelligence. The complete evaluation of honeypot technology, deployment strategies, and real-global case research underscores their essential function in improving the safety posture of groups and networks.

Our case take a look at, targeted on a real-global scenario, illuminated the strength of honeypots in detecting and mitigating cyber threats. The insights gleaned from this realistic utility furnished a tangible demonstration of honeypots' efficacy in safeguarding essential assets, augmenting chance detection, and assisting in incident response. Furthermore, the take a look at showcased the adaptability of honeypots to numerous environments, reinforcing their relevance throughout various sectors, from instructional establishments to commercial manage systems.

As we finish our exploration, it's far obtrusive that honeypots are integral additives of a sturdy cybersecurity strategy. Their capacity to entice, divert, and dissect malicious activities, coupled with their function in producing chance intelligence, positions them as crucial equipment withinside the arsenal of cybersecurity professionals. By constantly evolving honeypot technology, embracing nice practices, and staying vigilant towards the ever-evolving chance landscape, groups can harness the whole capacity of honeypots to reinforce their defenses and navigate the virtual realm with extra resilience and confidence. In an technology wherein cyber threats loom large, honeypots stand as beacons of safety and knowledge, guiding groups closer to a more secure and extra knowledgeable future.

REFERENCES

[1] Noah - a european network of aned honeypots (2018), https://cordis.europa.eu/docs/publications/1201/120142541-6en.pdf, [Online; accessed 18-August- 2019]

[2] for Cyber Security (CFCS), D.D.I.S.C.: Foreign hackers threaten danish pub- lic research (2017), https://feddis.dk/cfcs/publikationer/Documents/TV20forskning

[3] Fraunholz, D., Zimmermann, M., Hafner, A., Schotten, H.D.: Data mining in long- term honeypot data. In: 2017 IEEE International Conference on Data Mining Workshops (ICDMW). pp. 649–656. IEEE (2017)

[4] Nawrocki, M., W¨ahlisch, M., Schmidt, T.C., Keil, C., Sch¨onfelder, J.: A survey on honeypot software and data analysis. arXiv preprint arXiv:1608.06249 (2016)

[5] Deploying a University Honeypot: A case study; Aalborg University;September 2019;Authors:Rasmi Vlad Mahmoud, Jens Myrup Pedersen.

[6] Spitzner, L.: The honeynet project: trapping the hackers. IEEE Security Privacy 1(2), 15–23 (March 2003). https://doi.org/10.1109/MSECP.2003.1193207