Communication and Computer Engineering Research Magazine, Vol (1), No (1), 2024.

Hacker Traps

AlHasan Sameh*, Reem Ezzat, Alaa Abdelmohsen, Ahmed O.Khalil , Khaled k.Elkodosy , Abdelrahman G.Taher , Ahmed I.Elsanet , Youssef Hesham , Ahmed S.Ahmed , Hanaa Y. Zain Eldin

Communication and Computer Engineering Program, Faculty of Engineering, Mansoura University, Egypt

*: Corresponding Author

Research Paper Data:

- *Paper ID:*
- *Submitted:*
- *Revised:*
- *Accepted:*

Abstract

Virtual vortex project is a security measure that sets up a digital trap to catch unauthorized attempts to enter a computer system that is installed in various locations throughout the network. In order to gather data on attackers and how hackers operate, we employed honeypots to look into cybersecurity breaches and provide early warning of an ongoing attack. This project presents a technique of hacking traps known as "honeypots" for fully simulating SSH, FTP, HTTP, Telnet, and other services and interacting with the attacker in order to help consume the attacker's resources and extract as much important information about the attacker, his techniques, and the software tools used to distract him away from the actual systems. We will use Modern honey Network (MHN), which is a centralserver that uses to deploy and manage honeypots, GNS3 software and Wireshark eavesdropping software and analyze packages and the VMware program using a set of virtual machines to simulate attacks on SSH, Amun (Honeypots) servers, Linux-Kali and direct connection with other services.

Keywords: *Cybersecurity Encryption Authenticatio Firewall Malware Phishing*

1. Introduction

Honeypots are an extra layer of security that can be used in conjunction with firewalls and other security solutions to protect networks from hackers. They appear to be an easy entry point into a network and can distract attackers from other parts of the system. They are deliberate holes in system security that can be exploited without causing damage. They allow IT teams to gather valuable information about hackers trying to gain access to their networks. A honeypot is designed as a deployable resource designed to perform various attacks, compromise, and collect data over the Internet. Unlike IDSs, honeypots provide malicious actors access to a restricted environment with the goal of monitoring their behavior to determine their motives and ultimate goals. This allows companies or security professionals to learn from attacks and modify, update and improve existing security infrastructure.

The main functions of honeypot can be summarized into:

- Distract the attacker from the real network and into hack traps in order to conserve physical resources of the system.
- Exhausting the resources of the attacker and slowing down his work, which calls for running out of time by exploiting fake resources.
- Capturing new viruses or suspicious movements for future use.
- Monitoring the attacker's behavior to know his methods, the mechanisms of his depletion, and the techniques used.

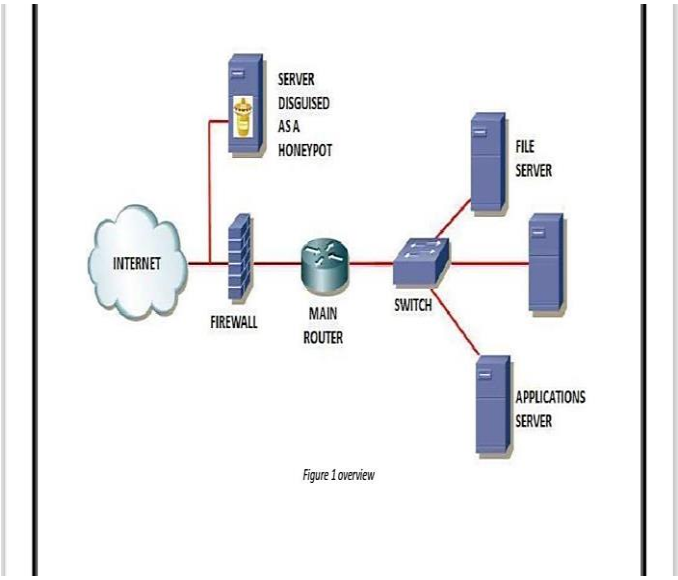

Figure 1 overview

With the continuous development of modern technology, optical fiber transmission has been adopted in the process of information engineering applications, as shown in Figure (1)

services and raspberry pi imitating what is within the system and that to interact with them and to extract as much valuable information as possible about the attacker and his techniques and the software tools used.

- Classify, categorize and compare the types of penetration detection systems.
- Trick the attacker and distract his attention away.
- Software or solid system vulnerabilities identified that have not yet been discovered.
- Anchor the techniques and methods used by the attacker and prevent him from implementing them on the actual network.

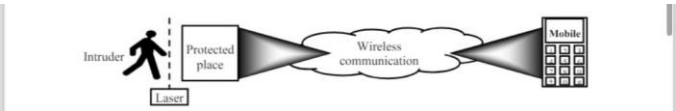

Figure (2) General block diagram of wireless security system.

2. Background

honeypot is a program, machine, or system placed on a network as bait for an attacker.

The idea is to trick an attacker into making the honeypot look like a legitimate system. Honeypots are usually virtual machines that mimic real machines by simulating running services and open ports that one might find on a typical machine on the network Ubuntu Server: is a server operating system that can be used with almost any hardware or virtualization platform. It can serve websites, files and shares.

Graphical Network Simulator (shortened to GNS3) a network software simulator, first released in 2008.

It allows combining virtual and real devices for simulating complex networks.

Wireshark. Is a free and open source packet analyzer. It is used for network troubleshooting, analysis, development of A4 software and communication protocols, and training.. VMware: helps users create a virtual machine on their computer easily.

The top use cases of VMware are

- Improved resource management.
- Improved flexibility of computing environment.
- Reduced IT costs.
- Quick and safe software installation

3. Related Work

in the field of honeypot security systems encompasses a rich array of approaches aimed at comprehensively understanding and proactively mitigating cybersecurity threats. Extensive research has delved into the intricacies of honeypot design, deployment, and operation, exploring various methodologies to effectively detect, analyze, and respond to malicious activities. This includes the development of diverse types of honeypots, ranging from traditional network-based variants that emulate vulnerable services to sophisticated high-interaction systems that replicate entire computing environments. Moreover, studies have investigated innovative techniques such as data mining, anomaly detection, and machine learning to augment honeypot capabilities, enabling more accurate threat detection and response mechanisms. Furthermore, research efforts have extended beyond conventional network settings to explore the applicability and effectiveness of honeypots in emerging environments such as cloud computing infrastructures and Internet of Things (IoT) ecosystems. By examining the efficacy of honeypot deployments in these diverse contexts, researchers aim to advance our collective understanding of cybersecurity threats and bolster defensive strategies against evolving attack vectors.

4. Project Details

Design And Implementation

Overview of the project

I am familiar with GNS3 but i didn't know the configuration of connectivity between devices in correct way so i studied CCNA and fundamentals of CCNP, after that i knew the routing protocols and switching protocols and that helped me to make the project. In this section, we will implement the proposed framework using GNS3 software and Virtual Box software, using a set of virtual machines to simulate attacks on Honeypots servers. The network is programmed so that the Attacker can access the Honeypots network but cannot reach the Honeypots Intranet via Firewall and ACL, even if Honeypots and other servers are hacked. The real Serv Art will not be able to access the internal networks because the DMZ network is completely isolated from the network interior. The internal network can reach the DMZ network, but the DMZ network cannot reach the network interior and then, Raspberry Pi four Model B is the state-of-the-art product in the famous Raspberry Pi vary of computers. It affords ground-breaking will increase in processor speed, multimedia performance, memory, and connectivity in contrast to the prior-generation Raspberry Pi three Model B+, whilst keeping backwards compatibility and comparable electricity consumption. For the cease user, Raspberry Pi four Model B offers laptop overall performance related to entrylevel x86 PC systems. This product’s key aspects consist of a high-performance 64-bit quad-core processor, dual-display assist at resolutions up to 4K by a pair of micro-HDMI ports, hardware video decode at up to 4Kp60, up to 4GB of RAM, dual-band 2.4/5.0 GHz wi-fi LAN, Bluetooth 5.0, Gigabit Ethernet, USB 3.0, and PoE functionality (via a separate PoE HAT

add-on). The dualband wi-fi LAN and Bluetooth have modular compliance certification, permitting the board to be designed into give up merchandise with notably decreased compliance testing, enhancing each price and time to market.

Components

GNS3 is categorized asit is one of the open-source software program (GPL GNU), which is a application well-known simulator that simulates actual Internet networks, and permits you to make a digital community comparable inits work to the community in fact.GNS3 affords an intuitive graphical interface for designing and configuring digital networks, and it works on private computer systems and can additionally be used on a couple of working systems VMWare VMware is a virtualization and cloud computing software program supplier primarily based in Palo Alto, California. Founded in 1998, VMware is now a subsidiary of Dell Technologies. VMware bases its virtualization applied sciences on its bare-metal hypervisor ESX/ESXi in x86 architecture. Bare-metal embedded hypervisors can run at once on a server's hardware besides the want of a important working system. With VMware server virtualization, a hypervisor is mounted on the bodily server to permit for a couple of digital machines (VMs) to run on the identical bodily server. Each VM can run its personal working system, permitting a couple of to run on one bodily server. All of the VMs on the equal physical server share resources, such as networking and RAM. Brute-Force Attack The time period Brute -Force Attack refers to assault operations the usage of a (guessing) technique to attempt to getsure data such as username and password by way of guessing a crew of Possibly, Force-Brute assaults are used via cybercriminals to damage the safety of encrypted records as properly as via safety analysts to take a look at the safety of the networks of applicable establishments and organizations, the approach is one of the oldest methods, however it is nonetheless famous and superb and used with the aid of many pirates.

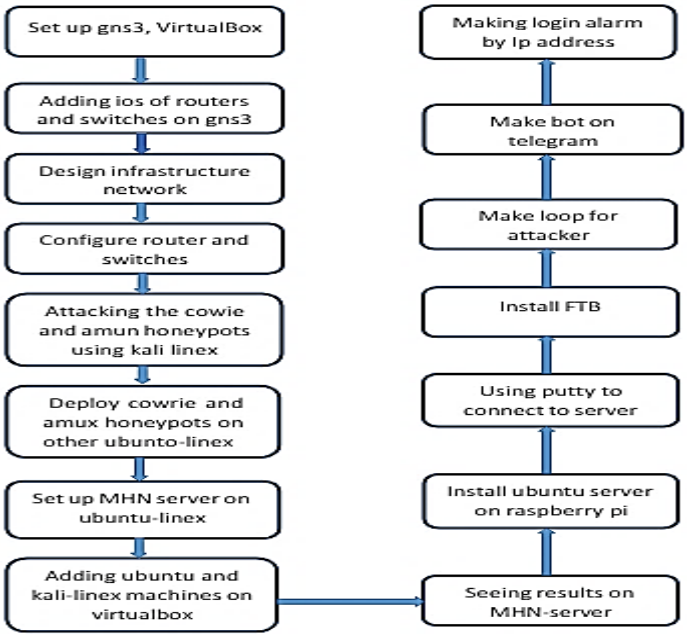

Figure (3)

4.1 We use the device for its small size and low price to suit all users, and ease of use

Advanced tracking can also be utilized. All you need to do is use the other canary tokens, upload them to the SPIFFS of the ESP board. From there, the hacker can download and trigger the tokens. Even though it looks as if anyone can upload and rename files on the FTP server, it's simply not the case. Those modifications are flushed away when the files are reloaded. They aren't actually on the ESP in the first place. When configuring the FTP server, you can specify a username and/or password that connects to the server. Connecting to the ESP over FTP is pretty straight forward. Get the IP from the serial monitor and connect with the username and password with port 21. Allowing

insecure connections can be enabled by ticking a box as well. The ESP canary is prompted when a hacker connects to the FTP server and sends an email that warns you they're spying on your network. The email contains the source IP, which is the FTP server's IP. It also shows user-agent, the IP address of the hacker connecting to the server. You can even specify any web-hook URL if you don't want to use canarytokens.org. This lets you append the hacker's IP to the query string as an additional parameter.

4.2 Digital Video Recorder (DVR) System

A Digital Video Recorder is a security system device that records video from surveillance cameras on a hard disk. In this work DVR system operates and starts recording from a connected camera when it receives a signal from the controlling system. Surveillance camera is set to monitoring and covering an important zone for the owner. DVR system can records video from 8 surveillance cameras on a hard disk capacity of 500GB. DVR and cameras

operate at 220V AC, while the operating signal voltage from controlling system is about 5V DC so it needs to use a driver circuit to operate DVR and camera system.

4.3 Calling Circuit

One of the control circuit's output signals is used to activate the calling circuit. This circuit is responsible for making the calling process by activate speed dial function in mobile phone. The activation of speed dials function done.

4.4 Controlling Circuit

The microcontroller PIC18F452 is the main component in the controlling circuit. This microcontroller is considered as one of the best High Performance, Enhanced FLASH Microcontrollers with 10-Bit A/D. Where some of PIC18F452 features could be seen. The main objective of controlling circuit is to give the sensing system and the calling system more accuracy and more stability. This objective is done by the way of programming the microcontroller PIC18F452.

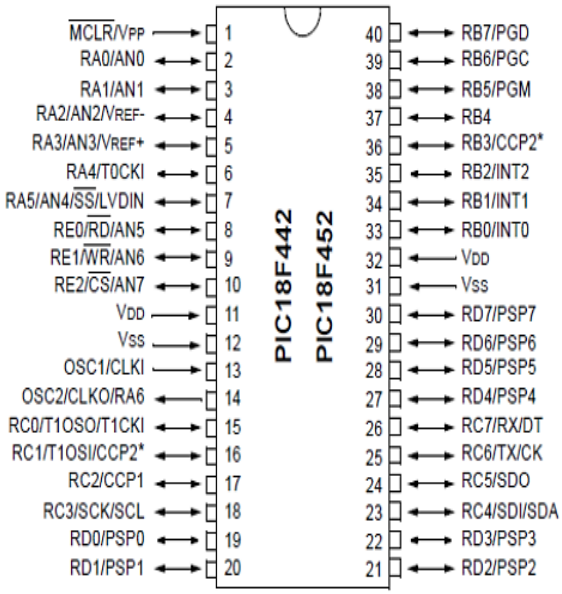

Figure (4) PIC18F452 pin configuration.

4.5 Delay and Make Ignition Circuit

The delay and ignition circuit is designed to make delay time about (120 second) to complete the tons of calling in remote (mobile owner). After that, the output signal from the ignition circuit is used to make ignition repeatedly to the calling circuit through motivating the Triac1 of its circuit. The operations of Relay2 are: Group1: Connection 1 and 2 are used to make charging time (120sec.) which is the required time to delay another calling with the remote mobile. Connection 2 and 3 are used to make discharging time (1sec.) which is the required time to make ignition to the first Triac. Group2: 1 and 2 connecting Vref1 to the OP. Amp. at the charging period. 2 and 3 connecting Vref2 to

the OP. Amp. at the discharging period. Where: T1=5t. t= must be 120 second. Assume that C1=470 µf, therefore (Rd1+Rdv1) =545kΩ. We used Rd1=400kΩ & Rdv2=150kΩ to make facility to change in the charging time (T1). Where: T2=5t. t= must be 2 second. C1=470 µf, therefore (Rd2+Rdv2) =25kΩ. We used R1=5kΩ & Rv2=20kΩ to make facility to change in the discharging time (T2).

4.6 Reset Circuit for The System The reset circuit is used to avoid the continuous repeatedly calling for the remote mobile. This mechanism is achieving by calling the fixed mobile from remote mobile to makes cut off the voltage in call circuit. Fig. (12) shows the reset circuit. The operations of Relay 3: In this circuit: Group1: Connection 1 and 2 are used to make the Triac 1 (circuit 1) and Triac 2 (circuit 2) with voltage (12 volt). Connection 2 and 3 are used to cut off the voltage for Triac 1 and Triac 2.

4.7 Group2

Connection 1 and 2 are used to activate the op-amp at the charging period.

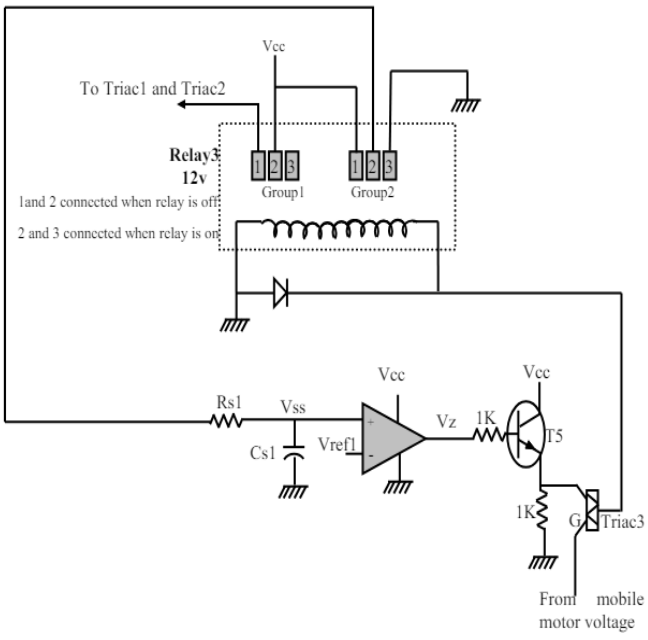

Figure (5) Circuit 3 (Reset circuit for the system).

4.8 Implementation of The Security System

System's hardware is built according to the designed circuits in which all of these circuits are connected together in addition to the mobile phone and the DC power supplies to complete the desired system. The integral system is tested in different situations depending on the mechanism of laser grids in sensing system. Therefore, there was no dialing between the fixed and remote mobile phone and (DVR - camera) switches off when no event occur in sensing system illustrates the dialing between the fixed mobile and the remote mobile phone after the barrier cut off the laser beams grid in sensing system and the DVR began to records the events with through the digital camera and display it on monitor.

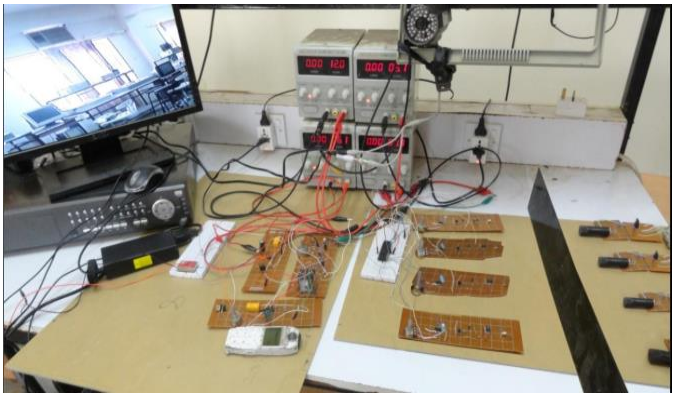

Figure (6) Overall system at secure state without interrupted.

4.9 Putty

is a free and open-source terminal emulator, serial console and community file switch application. It helps various community protocols, consisting of SCP, SSH, Telnet, rlogin, and uncooked socket connection. It can additionally join to a serial port. The title "PuTTY" has no respectable meaning. PuTTY used to be at the start written for Microsoft Windows, however it has been ported to a variety of different running systems. Official ports are accessible for some Unix-like platforms, with work-in-progress ports to Classic Mac OS and macOS, and unofficial ports have been contributed to systems such as Symbian,[6][7] Windows

Mobile and Windows Phone. PuTTY was once written and is maintained in particular with the aid of Simon Tatham, a British programmer.

4.10 What is Ubuntu Server?

Ubuntu Server is a server running system, developed through Canonical and open-source programmers round the world, that works with almost any hardware or virtualization platform. It can serve up websites, file shares, and containers, as nicely as make bigger your enterprise choices with an superb cloud presence.

4.11 Why does Ubuntu Server matter?

Back in 2015, it used to be pronounced that Ubuntu used to be twice as widely wide-spread on Amazon Cloud offerings as all different working structures combined. Ubuntu Server doesn't simply work nicely in the cloud; it policies the cloud. For small- to mid-size companies searching for a
not pricey server solution, Ubuntu have to be your first end.

4.12 Loop For Attack In Raspberry Pi

When the hacker does not have the username and password, but he has an IP, he can use the IP to scan the open port and try to access using the open IP and port, then he will enter the loop and will not know how to make any commands.

Figure (7) Alarm Login On Raspberry Pi

4.13 Alarm Login On Raspberry Pi

We create a bot on Telegram, and it connects to a server, and in case that the hacker has a username or password, he sends an alert when he enters the server, and his IP is shown to us

We've given an overview of the plan and structure of a honeypot and proven how a honeypot can be used in Shift attackers from the live server. If attackers spend sizable time on the honeypot server, they will no longer have time to purpose troubles to stay servers. Understand the attacker's methodologies, to higher guard the actual manufacturing systems. Honeypot can additionally assist safety gurus to analyze greater about recognized and unknown attacks. Helps IT groups become aware of loops holes and vulnerabilities in the stay servers Thus, making honeypots a very beneficialsection of the protection system. You can have a look at hackers in motion and study about their behavior. Gather brain on assault vectors, malware, and exploits and use that intel to instruct IT staff. Create profiles of hackers who are making an attempt to achieve get entry to to your systems. Waste hackers' time and resources. Improve yoursafety posture by means of the use of the intel and facts to gain greater budgets for will increase for security. Any hacker who tries to hack will enter a loop and will no longer be in a position to take any information.

5. Results &Conclusion

We've given an overview of the plan and structure of a honeypot and proven how a honeypot can be used in Shift attackers from the live server. If attackers spend sizable time on the honeypot server, they will no longer have time to purpose troubles to stay servers. Understand the attacker's methodologies, to higher guard the actual manufacturing systems. Honeypot can additionally

assist safety gurus to analyze greater about recognized and unknown attacks. Helps IT groups become aware of loops holes and vulnerabilities in the stay servers Thus, making honeypots a very beneficialsection of the protection system. You can have a look at hackers in motion and study about their behavior. Gather brain on assault vectors, malware, and exploits and use that intel to instruct IT staff. Create profiles of hackers who are making an attempt to achieve get entry to to your systems. Waste hackers' time and resources. Improve yoursafety posture by means of the use of the intel and facts to gain greater budgets for will increase for security. Any hacker who tries to hack will enter a loop and will no longer be in a position to take any information.

6. Future Work

In the future, we would like to discover a variety of honeypot implementation on raspberry pi, subsequently using more than one raspberry pi for a couple of honeypot sensors, emulating large vary of community services, on a single site. With this arrangement, one website online can be designed to ship more than one assault facts to the storage server, via more than one honeypot sensors at the identical time.

References

1] CCNA and Cyberops Associate Official Cert Guide.

[2] CCNP and CCIE Security Core SCOR 350-701 Official Cert Guide

[3] W. R. Stevens, TCP/IP Illustrated Vol. 1 – The Protocols, Addison-Wesley, 1994.

[4] S. M. Bellovin, "Security Problemsin the TCP/IP Protocol Suite", Computer Communications Review, Vol. 19, No. 2, pp. 32-48, April 1989.

[5] C. Cobb and S. Cobb, "Denial of Service", Secure Computing, pp.58-60, July 1997.

[6] CERT, "TCP SYN Flooding and IP Spoofing Attacks", Carnegie Mellon University, Sept. 1996. [7] D. E. Comer, Internetworking with TCP/IP: Vol. I – Principles, Protocols and Architecture, Third Edition, Prentice Hall, 1995.

[7] Wiley & Sons.e 1995 IEEE Symposium on Security and Privacy, Oakland, CA, May 1995

[8] http://www.cisco.com/

[9] https://www.gns3.com/

[10] https://github.com/pwnlandia/mhn/

[11] https://nmap.org/

[12] https://www.osboxes.org/ubuntu-server

[13] https://www.wireshark.org

[14] https://cloudbytes.dev/snippets/upgrade-python-to- latest-version-on-ubuntu-linux

[15] https://www.ssh.com/academy/ssh/sshd