KOCAELI UNIVERSITY

ENGINEERING FACULTY

DEPARTMENT OF COMPUTER ENGINEERING

CLOUD BASED HONEYPOT SYSTEMS

GÜRKAN GÖKDEMİR

KOCAELI 2019

CONTENTS

CONTENTS.. ii

ABSTRACT.. iv

INTRODUCTION..v

1. CLOUD COMPUTING..7

1.1. What is Cloud Computing Services?..7

1.2. Advantages of Cloud Computing Services 7

1.3. Types of Cloud Computing 9

2. SECURITY..10

2.1. Network Security 10

2.3. Types of Malware..10

3. HONEYPOTS 13

3.1. Modern Honey Network..13

3.2. Cowrie Honeypot 16

3.3. Conpot Honeypot 16

3.4. Glastopf Honeypot 17

3.5. Database Honeypots..18

3.6. Web Honeypots 18

3.7. Service Honeypots..19

3.8. SCADA Honeypots..19

3.9. VM Tools for Honeypots 19

3.10. Low Interaction Honeypots 20

3.11. Server Honeypots 20

3.12. Client Honeypots 21

3.13. SSH Honeypots 21

3.14. Honeytokens 21

3.15. Spamtrap Honeypots 22

3.16. Botnet Honeypots 22

3.17. Other 22

4. TELNET & SECURE SHELL (SSH) 24

4.1. Telnet 24

4.2. Secure Socket Shell (SSH) 24

5. SANDBOX 26

5.1. Cuckoo Sandbox 26

RESULTS 28

BIOGRAPHY 29

CLOUD-BASED HONEYPOT SYSTEMS

ABSTRACT

The purpose of this study is to examine honeypot based network security systems and theoretically usage of them to use with the cloud technologies.

First of all, cloud technologies are basically described. At the security part, various kind of threats is compared.

In the honeypot part, all types of honeypots with few detailed examples are shown. One of the Telnet/SSH honeypot (Cowrie) analyzed and summarized in this thesis.

Keywords: Cloud Technologies, Cowrie, Honeypot, Network Security, SSH.

INTRODUCTION

Today distributed systems rising, businesses change their infrastructure and adopt cloud technologies with data centers, servers, and all kinds load go-to cloud then the business does what it its best. Also, today's technology shapes our daily lives, mobile devices, tablets, laptops. We used to need heavy computers only for tiny works, now tiny devices do heavy work. A connection is everywhere, every place is part of a network.

Protecting a network is an extremely hard thing to do. We must protect our servers. There are multiple defense solutions to protect it like Firewalls etc. But the environment changes the behavior of attackers and threats also changes. As we connect our computer from every place that contains connection. Attackers also wants to connect to our data like us. It's hard to detect, what, who, whom, where, when. To solve this problem we created "Honeypots". Acts like a real device. But it's actually a trap for attackers. One another way is using this decoy systems. It makes us understand who is attacking with which tools from where. Honeypot is an effective way to see potential attacks for detecting attackers and stabilize our real system.

Before using a honeypot it's better to test it, testing it in a local device is extremely dangerous. Honeypots consist of vulnerabilities by their nature to take attacks. But if we use it on the local computer. We can give an open door to them to attacks us in multiple ways.

Therefore we use cloud technology to protect ourselves and detect attackers’ information securely. Cloud service providers are the most secure environment to protect ourselves and our important information. To stay economically efficient we used multiple cloud service vendors (AWS, Azure, and Google Cloud) and their free services and coupons.

After we look at what does cloud means to the user and what are its benefits, then we searched about what is a network security and what are potential threats also types of malware.

As a security solution, we look honeypots generally and as an easy way to use honeypots we used Modern Honey Network to use for visualizing the attacks, to detect attackers' IP and other information. With the easy interface of MHN, we used Cowrie to test the honeypot system. It’s a Telnet/SSH honeypot. We searched for other types of honeypots and what is SSH and Telnet.

Application is going to be in a Linux environment thus we will prepare Telnet SSH Honeypot. Then we will install the Modern Honey Network to visualize threats.

This thesis is generally about cloud technologies, Modern Honey Network, Cowrie honeypot. We will look at also general security threats.

1. CLOUD COMPUTING

1.1. What is Cloud Computing Services?

Cloud services make us easily connect to servers or storage or database and many more application services over the network. A cloud computing service provider like AWS (Amazon Web Services), Microsoft Azure or Google Cloud owns all hardware needed for these services and maintains them, and we use it with a web application.

1.2. Advantages of Cloud Computing Services

Cost

With cloud computing, there is an efficient solution for costs. It’s not necessary to buy software, hardware and hire extra IT professionals to set it up to data centers then take care of it. There is also electricity costs like power and cooling. Cloud is cheaper because of the larger economies of scale so it’s economical than doing by yourself.

Speed

Almost all cloud services are provided on-demand and self-service, most of them can be ready with some clicks in few minutes, it gives much flexibility to the businesses and takes the pressure off capacity to from them.

Productivity

Cloud services remove most of the IT tasks in the on-site datacenters. They need a lot of hardware setup, racking, and stacking, software patching, etc. Cloud computing services removes them all. The team can spend time gaining achievements on business goals.

Global scale

With cloud services, businesses can able to scale elastically. It is the right amount of IT resources by delivering when needed. It means more or less storage, computing power, bandwidth, etc. In the best global location.

Performance

Cloud service providers have secure data centers all around the world. They periodically upgrade these data centers with the best hardware and reduces latency for applications. Single corporate datacenter includes bigger economies of scale.

Security

Almost all cloud service providers use a set of policies and technologies that control security and strengths. This helps to protect our apps, data, and infrastructure against threats.

Reliability

Cloud service copies your data at many redundant locations on the provider's network. This makes any recovery and backup cheaper and efficient. Business continues easily.

1.3. Types of Cloud Computing

Public

Owned by third-party cloud computing service providers who deliver their resources over the internet like storage or servers. Cloud service providers own and manage all hardware and software, also supporting infrastructures. Businesses access their services to manage the account with a web browser.

Private

Cloud resources used by a single business exclusively. It could be located physically on the businesses on-site datacenter or third-party service providers could host their private cloud. In one sentence, a private cloud is a service infrastructure that maintains on a private network.

Hybrid

It mixes public cloud and private clouds together with technology to allow data and apps to share between. This gives the company to bigger flexibility and more options. It helps the optimization of our existing security and compliance infrastructure.

2. SECURITY

Internet is a subject for attacks from malicious sources. Attacks can be in two categories “Passive” or “Active”. With “Passive” attacks intruder intercepts data traveling via the network and in “Active” attacks intruder uses commands to disrupt the normal operation of the network. The attacker conducts lateral movements to find and gain access to assets on the network.

2.1. Network Security

Network security is an activity designed to protect the integrity of the usability of data and networks.

- This includes software and hardware technologies.
- This targets various threats.
- This stops threats from spreading or entering our network.
- Efficient security manages access to the network.

2.3. Types of Malware

Malware is a short version of malicious software. It is software or code that is used to steal, damage, disrupt, or other illegitimate actions in data, hosts, or networks specifically. There are three types of malware. Viruses, Worms and Trojan horses.

Viruses

The virus spreads by inserting a copy of itself into a program, then it became a part of it and spreads one computer to another one. It can be in severity from causing to damage software or data and causes a denial of service condition. All viruses are tied to an executable file and that means the virus can be found on a system but won’t be active until a user runs or opens the infected file. When the file runs, the virus runs as well. Generally, the main program keeps functions after it infected. Despite that, some of them overwrite the main program. Viruses extend when the file they are part of it one to another via disks, network, emails or file sharing.

Worms

Worms are like viruses in that they copy of them and creates a similar type of harm. Viruses need an infected host file to spread. A worm doesn’t need a program to attach themselves to infect a computer or host. Worms use system characteristics to move through the network.

Trojan Horses

Trojan horse is a different kind of malicious software. It’s a damaging slice of software that looks normal. Users are generally tricked to executing that file on their system. It can create so many attacks on the host, from annoying the user with changing desktops to damage the host with stealing data or deleting files or spreading other malware. They also leave backdoors to give access to systems by malicious users. Trojan horses don’t reproduce themselves unlike worms or viruses, Trojan horses spread with user interaction like with an email attachment or running or downloading a file from the internet.

3. HONEYPOTS

A honeypot is a bait computer system to snare hackers and tracks unusual and new hacking methods. They designed with a purpose to deceive and engage hackers and detect malicious activities happened on the Internet.

3.1. Modern Honey Network

Modern Honey Network is a centralized server to manage and to collect data of honeypots. Modern Honey Network allows us to deploy honeypots fast and to collect data just in time and view. Honeypot scripts include several common honeypots to deploy.

Features

- Connect and register.
- Download a deploy script and snort rules.
- List new attacks.
- Send intrusion detection logs.
- Manage snort rules (enable download, disable download).

Installing

- The Modern Honey Network server is supported on Ubuntu and Centos.
- Other versions of Linux should work but are usually not tested.

Deploying Honeypots

Modern Honey Network was designed to make easy and scalable deployment of honeypots. There are the steps to deploy with Modern Honey Network:

1. Login to your Modern Honey Network server via a web browser.
2. Select a honeypot type from the menu.
3. Copy the deployment command.
4. Log in to a honeypot server and run that command.

Modern Honey Network uses MongoDB as a database to store data. MongoDB is a NoSQL database that stores data in a similar way to JSON documents. JSON supports nested objects as values and arrays.

It uses HoneyMap to show a real-time visualization of attacks and allows dynamic and flexible schemas. HoneyMap is a web application that visualizes a live stream of locations on a world map.

Supported Honeypots by Manage-Deploy Page of Modern Honey Network.

With the Manage-Deploy page, users can easily deploy a few most used honeypot as a sensor. These are officially supported honeypots.

- Conpot
- Wordpot
- Shockpot
- Suricata
- Glastopf

- ElasticHoney
- Amun
- Dionaea
- Cowrie

3.2. Cowrie Honeypot

Cowrie is a medium interaction SSH/Telnet honeypot. It designed to log brute force attacks and shell interaction of the attack. It also functions as a Telnet/SSH proxy to observe the behavior of attackers on another system.

Features

- Stores session logs in a UML format to easy replay with the bin/playlog utility.
- Supports SCP and SFTP to file upload.
- Support for SSH exec commands.
- Logs direct-TCP connection attempts (ssh proxying).
- Forwards SMTP connections to SMTP Honeypot like Mailoney.
- Logs as JSON to process easily in log management.

3.3. Conpot Honeypot

Conpot is a low interactive server-side ICS honeypot (Industrial Control Systems) designed to easily deploy, extend and modify. It provides many industrial control protocols to build in the system. It’s capable to imitate complex infrastructure to persuade an opponent that it found a large industrial complex. Conpot improves the deceptive capability with a possible server a custom human-machine interface to grow the honeypots attack surface. The response times of the services can be artificially delayed to mimic the real system behavior under constant load. It provides total stacks of the protocols. Conpot also can be extended with real hardware or accessed with a human-machine interface.

3.4. Glastopf Honeypot

Features

- When exposure type is emulated, Glastopf can handle the same type of unknown attacks. While implementation can be slower and more complicated, we remain in front of the attackers until they come up with a new type of attack or discover a new defect in our implementation.
- It has a modular design for adding attack type handlers or new logging abilities. Many database abilities are in it.
- Remote File Inclusion with a build-in PHP sandbox, Local File Inclusion that provides files from a virtual file system and HTML injection with POST requests. JSON logging for easy processing in log management solutions.
- It has popular attack type emulation: Local File Inclusion provides files from a virtual file system, Remote File Inclusion with a build-in PHP sandbox and HTML injection with POST requests. Also JSON logging as processing in log management solution.
- Opponents generally use specially crafted search requests and search engines to find victims. To attract them, Glastopf provides keywords and also extracts them form requests and extends its attack surface automatically. As a result, the honeypot gets more and more attractive with each new attack attempted on it.

3.5. Database Honeypots

- Elastichoney - It is an elasticsearch honeypot designed for catching attackers that exploiting Remote Code Evaluation vulnerabilities in elasticsearch.
- NoSQLpot - It is an open-source honeypot for NoSQL databases to automate the process for detecting attackers and logging attack incidents.
- MongoDB-HoneyProxy - MongoDB honeypot proxy.

3.6. Web Honeypots

- Glastopf - Web App Honeypot.
- Google Hack Honeypot – It designed for providing inspection in opposition to attackers that use search engines as a hacking instrument opposed to our resources.
- Shadow Daemon - Modular High-Interaction Honeypot / Web Application Firewall for Perl, PHP, and Python applications. Shadow Daemon is a tool collection for recording, detection, and blocking attacks on web apps.
- StrutsHoneypot - StrutsHoneypot is an Apache 2 based honeypot that includes a separate detection module for Apache 2 servers.
- WebTrap - Designed to create misleading webpages to redirect attackers away from real websites.
- django-admin-honeypot - Fake Django login screen to notify of unauthorized access attempts.
- Snare - Super Next-generation Advanced Reactive honeypot. It is a web application honeypot that attracts all sorts of harmfulness from the Web.

- Tanner - TANNER is a remote classification and data analysis service, evaluating SNARE events and HTTP requests and composing the response.
- wordpot - Wordpot is a WordPress honeypot that detects probes for themes, timthumb, plugins and other files used to fingerprint.

3.7. Service Honeypots

- ADBHoney - Low interaction honeypot that simulates an Android device running Android Debug Bridge (ADB) server process.
- HoneyPy - A low interaction honeypot with the capacity of a medium interaction honeypot.
- RDPy - RDPY is a Python implementation of the Microsoft Remote Desktop Protocol of the client and server-side.
- honeytrap - Advanced Honeypot framework is written in Go that can connect with other honeypot software.

3.8. SCADA Honeypots

- Conpot - SCADA honeypot.
- SCADA honeynet - Building Honeypots for Industrial Networks to understand the risks of the exposure control system potential.

3.9. VM Tools for Honeypots

- Antivmdetect - Script that creates templates for using Virtual Box to make VM detect harder.

- VMCloak - VMCloak is a tool to fully create and prepare Virtual Machines that can be used by Cuckoo Sandbox. In order to create a new Virtual Machine one should prepare a few configuration values that will be used later on by the tool.

3.10. Low Interaction Honeypots

- Honeyperl - Honeypot software based in Perl with plugins with many functions. (Telnet, squid, SMTP, etc.)
- T-Pot - All in one honeypot appliance like Modern Honey Network.

3.11. Server Honeypots

- Amun – Honeypot that emulates vulnerability. (Amun was the first python-based low-interaction honeypot.)
- Artillery - Open-source tool designed to protect OS through multiple attack methods.
- Heralding – Honeypot to catch credentials.
- Hontel - Telnet Honeypot.
- KFSensor - Windows-based Intrusion Detection System.
- LaBrea - Takes over unused IP addresses, and creates virtual servers that are attractive to hackers, worms, etc.
- glutton - All eating honeypot.
- mwcollectd - Flexible malware collection daemon, unites the best features of honeytrap and nepenthes.
- telnet-IoT-honeypot - Python Telnet honeypot to catch botnet binaries.

3.12. Client Honeypots

- HoneyWeb – It’s a web interface created for managing and sharing remotely Honeyclients resources.
- jsunpack-n - jsunpack-n emulates browser when visiting a URL. It detects exploits that target browser and plug-in vulnerabilities.
- Shelia - Client-side honeypot to detect attacks.
- Thug - Python-based low-interaction honey client.

3.13. SSH Honeypots

- Cowrie/Kippo - Cowrie SSH Honeypot (based on kippo).
- HonSSH - Logs all communication between a client and a server.
- Kojoney - Python-based low interaction honeypot to emulate an SSH server.
- MockSSH - Mock an SSH server and define all commands it supports.
- ssh-honeypot - Fake sshd that logs usernames, passwords, and IP addresses.
- sshesame - Fake SSH server that logs their activity who is in.

3.14. Honeytokens

- CanaryTokens - Self-hostable honeytoken generator with a reporting dashboard.
- Honeybits - Simple tool designed to increase the effectiveness of our traps with spreading breadcrumbs and honeytokens across our production servers and workstations to bait the attacker toward our honeypots.
- HoneyLambda - Serverless application designed to create and monitor URL honeytokens on top of AWS Lambda.

- dcept - Tool to deploy and detect the use of Microsoft's Active Directory honeytokens.

3.15. Spamtrap Honeypots

- Mail::SMTP::Honeypot - Perl module that provides the functionality of a standard SMTP server.
- Mailoney - SMTP honeypot that is written in python.
- Shiva - Spam Honeypot with Intelligent Virtual Analyzer.

3.16. Botnet Honeypots

- Hale - Hale is a botnet command and control monitor with a modular design to easily develop modules to monitoring protocols used by command and control servers.
- dnsMole - Analyses DNS traffic and detects botnet commands and controls server activities, along with infected hosts.

3.17. Other

- OpenCanary – OpenCanary is a decentralized and modular honeypot that alerts when a service is abused.
- miniprint - A medium interaction printer honeypot.
- mitmproxy - Allows traffic to be flow for, inspected, intercepted, replayed, and modified.
- peepdf - Python tool for analyzing PDF documents.

- Droidbox - Dynamic analysis of Android apps.
- Dionaea - Honeypot designed to trap malware. Dionaea embeds Python as the scripting language with using libemu to detect shellcodes supports tls and ipv6.
- Honeyd - Honeyd is a small honeypot to create virtual hosts on a network to be configured to run random services, and their personalities can be adapted so that they seem to be running certain OS.
- Dockerpot - Docker-based honeypot.
- Shockpot - Shockpot is a web app honeypot using to find attackers who attempt to exploit the Bash remote code exposure to detect Shell Shock exploit attempts.
- Suricata - Suricata is an open-source, mature, fast network threat detection engine.

4. TELNET & SECURE SHELL (SSH)

4.1. Telnet

Telnet is a network protocol that uses the command line to communicate with the device. It is a commonly used way to manage devices remotely. To use Telnet computers requires a keyboard only. Because it used on the terminal. All information is shown as text on the screen. The terminal enables one to log on to another device.

There is various kind of telnet clients to connect a remote device. Like PuTTY, Tera Term, SecureCRT or OSX Terminal and Command Prompt on Windows can use for Telnet connection. Telnet connects you to the device as a user and grants you the direct control and with the same right user has for files and applications.

Telnet is not secure when compared to SSH. Because Telnet doesn’t contain encryption.

4.2. Secure Socket Shell (SSH)

Secure Socket Shell is a protocol that gives an encrypted connection between devices. It replaces telnet for management connections. Telnet was an older protocol that uses a plaintext username and password for authentication. Also, it used to transmit data insecurely between computers. Therefore SSH is using for remote connections with securely providing encryption transmission between the communicating computers. It assigned to port TCP 22. Telnet was assigned to TCP 23.

SSH gives a secure way to access a computer over an unsecured network to the users, especially system administrators. With strong authentication and encrypted communication over the network between two computers. It also provides users to run commands and move files between computers.

Capabilities of Secure Shell

Functions that SSH enables:

- Secure remote access to SSH-enabled network devices or systems, it’s an automated process for users.
- File transfer sessions securely and interactively.
- File transfers are secure and automated.
- Issuance commands securely on remote systems or devices.
- Manage network infrastructure components securely.

5. SANDBOX

Sandbox is a software testing environment to enable an isolated running for software or programs to separate assessment, monitoring or testing.

5.1. Cuckoo Sandbox

Cuckoo Sandbox is a free automated malicious software analysis system. It enables us to put any questionable file at it and in a few seconds, it gives us detailed results outlining what we run inside an isolated environment. Its open-source software for automation any task to analyze any malware under all popular operating systems.

Features

Cuckoo Sandbox is a modular, advanced and open-source malicious software analysis system with a lot of applications. Its features are:

- Analyze many different malicious files (executables, emails, office documents, pdf files, etc.) also malicious websites under virtualized environments.
- The behavior of the file and trace API calls and extract this into comprehensible signatures and high-level information.
- Performs advanced memory analysis of the infected virtualized system.

- Dump and analyze network traffic, also encrypted with SSL/TLS. With native network routing support to drop all traffic or route it through a VPN or a network interface.

RESULTS

Our research shows the theoretical fundamentals of honeypots and also makes us know how to test the honeypot systems in a local environment, learn to install and use it. With a similar cloud environment with the same operating system, it won't be going to be a problem to use. Also, it shows the basics of cloud services, network threats, honeypot systems as potential solutions and types of it, and with which tools to install locally.

BIOGRAPHY

After he met the computers in 1999, he found the toy that he was curious to learn. In the 2010s, he decided to start software development. When he realized the importance of entrepreneurial thought to build, he joined one of the most innovative teams in the country.

He has experience as a Data Engineer at Factories and he is always a student at the university, which has one of the most challenging faculty of engineering.

Also, he uses open source technologies. So as a part of the open-source he decided to use the Linux environment.

Currently at the Kocaeli University Computer Engineering Faculty.