International Journal of Innovative Technology and Exploring Engineering (IJITEE)
ISSN: 2278-3075 (Online), Volume-9 Issue-6, April 2020

Network Protection using Honeypots

D. Rajesh, M.I. Thariq Hussan, B. Sri Vastav

Abstract*: PC Networks and Internet has become acclaimed these days since it fulfills individuals with varying needs by giving assortment of perfect service. Computer Networks have reformed our utilization of PC. Debits, Purchasing from e-commerce and many other needful activities performed by a single click from our homes. In spite of the fact that it is an aid right now, likewise has its own dangers what's more, shortcomings as well. Enterprises need to tussle to give security to their systems and in reality not conceivable to offer a cent percent security because of the immaterial knowledge of hackers meddling into the network. This paper gives the idea of honeypots for securing the network of the different organizations which might not have custom intrusion detection system or firewalls. The proposed model shows the different techniques utilized by hackers and makes a log of all hackers exercises. Hence utilizing this log, the network can be kept from assailants.

Keywords* :*Honeypot, Network, Intrusion, Honeynet.

I. INTRODUCTION

The Internet is the global network communication consists of interconnected networks which uses some standard protocols. It depends on the concept of packet switching. In spite of the reality that the administrations offered via internet are extensively applied from the layman to most skilled person., it moreover has its personal defects. Many assaults on Internet are being recognized and revealed. A portion of the basic types of system attacks is eavesdropping, statistics change, spoofing, secret key based assaults and denial of service attacks. To defeat these types of attacks an association mainly introduces an intrusion detection system to protect the private statistics traded over community. The local community is then related to the internet alongside these lines profiling the personnel to be online as the fly. Information security has three objectives to be specific.

1. Information privacy
2.Data integrity
3. Information availability.

Information privacy guarantees that the safe information can be gotten to just by approved people.

Revised Manuscript Received on April 30, 2020.
***** Correspondence Author
D. Rajesh*, B.Tech Scholar, Department of Information Technology,GuruNanak Institutions Technical Campus,Ibrahimpatnam, Hyderabad, India.Email: rajeshdurganath@gmail.com
B. Srivastav, B.TechScholar, Department of Information Technology, Guru Nanak Institutions Technical Campus,Ibrahimpatnam, Hyderabad, India. Email: srivastavbanda@gmail.com
Dr. M.I. Thariq Hussan, Professor and Head, Department of Information Technology, Guru Nanak Institutions Technical Campus,Ibrahimpatnam, Hyderabad, India. Email: thariqhussain@rediffmail.com

Data integrity permits secure adjustment of information. Information availability guarantees that the information is accessible promptly to approved people.

Small-scale businesses regularly do not prefer toward intrusion detection system because of its installation and upkeep costs. Honeypots and Honeynets are a productive elective for such organizations. A Honeypot can actually be a PC, which can go about as a hotspot for attacks. It pulls in the attackers to have a go at hacking it which thus may log the techniques utilized by the attackers. This log is helpful to forestall such assaults to the legitimate network. Honeypot PC normally do no longer have any significant information or data to be made sure about. It just has fake date or fake service, which is running on its ports to attract the attackers. There are numerous kinds of honeypots based on their design and deployment. Based on deployment honeypots may classified into two types mainly.

1.Production honeypots
2.Research honeypots.

Production honeypots are effortlessly deployed in the live environments that may catch just some measure of data about the attacks. Research honeypot deployment is confounded and utilized fundamentally for investigate purposed by government organizations. Based on plan, honeypots can be separated into three types

1. Pure honeypots.
2. High-interactionhoneypots.
3. Low-interaction honeypots.

Pure honeypots are complete production frameworks. The honeypot PC is hooked up to the system and faucets the attacks. Low-interaction honeypots lets in confined conversation with attacker and thus they're now not tainted by the attacks. High-interaction honeypots are vulnerable against attacks. No imitating takes place and henceforth increasingly inclined to be tainted by way of attacks. Honeynet is an assortment of honeypots introduced to trap the attacker exercises and log them.

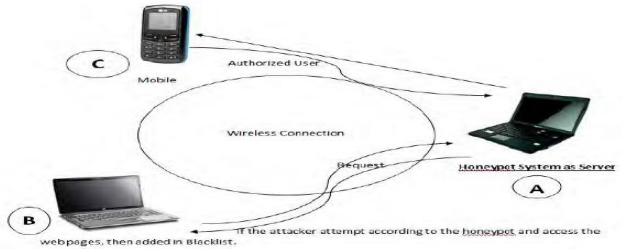


Figure 1: Network with Honeypot

II. RELATED WORK

The investigation about Honeypots has been longer than 10 years and it's one amongst the fields, which have high degree for inquire about. most vital research papers on honeypots are being talked about without delay.

A. Research applied in LAN security

This paper discusses how honeypots that combine physical and virtual honeypots can be implemented in the LAN system. It focuses on an variety of advancement such as IDS, creativity in honeypot and firewall.

B. Honeypots to catch Network attack traffic

This paper suggested a method for unraveling the honey-looked problems that is UNIX's oprn source honeypot. It centers on unraveling the log size problem by specifically planning two modules to logging and log breaking down modules.

C. Dynamic honeypot for Intrusion Detection

This paper proposed a effective dynamic systems Honeypot Strategy. This model collaborates with virtual honeypots and dynamic and inactive tests.

D. Making sure about WMN utilizing half breed honeypot framework

This paper proposed a model of assault discovery for remote arrangement of research using honeypot process. A Honeynet is seen for trapping the assailants.

E. Banking security utilizing honeypots

This paper suggested a secure structure for the use of honeypot innovation in banking application.

F. Visual analytic approach for SSH honeypots

This paper suggested a systematic model which could be used by specialists to image knowledge from ssh honeypot. Specialists can be given the opportunity to rapidly differentiate between meetings to catch the aggressors.

G. Honeypots in network security

This paper proposed a security model for small-scale businesses using a half-and-a-half grunt, Nmap, and Xprobe framework.

III. PROPOSED WORK

We have used the honeypots concept right now to offer security from attackers. A honeypot PC is set up to go beyond real or credible structures as an easily assaulted victim. The creation of a honeypot ha two aims.

1. Finding out how the attackers test into the system from the logged data.
2. Gather proper confirmations to send law enforcement officials for lawful action for interruptions by the attackers. The honeypot frameworks should fulfill certain conditions in order to attain these objectives.

a. The honeypot PC ought to be like other creation frameworks.
b. Utilization of fascinating data about honeypots to draw in programmers.
c. Limit the traffic conveyed to the Internet by a gatecrasher.

A. Levels of Tracking

Programmers' data recovered relies upon the degree of following set during arrangement. This may include firewall logs, system logs and instrument sniffers.

a. Despite the honeypot environment, firewall logs setting up a firewall into a network are incredibly useful in any situation. It helps to distinguish the method an interloper uses to penetrate a honeypot PC. Firewall have distinguishing note features such as sms, pager etc.

b. Windows and UNIX system logs are larger work systems used on the internet which help highlight logging. Event viewer in Windows is a tool that offers protection by recording the subtleties of the event. The User Manager lets the executives run the client and caught the administrations using netsvc.exc. The application movement logs are in UNIX, utmp, wtmp, btmp, lastlog, and Syslog is a remote server log-in.

c. Sniffer Tools These devices catch the bundles that fly between the firewall and the honeypot PC. When contrasted with the framework and firewall logs, sniffer instruments collect increasingly itemized data about gatecrashers. Additionally they deliver log storage

B. Building a Honeypot

a. The tools to be used to create a honeypot fluctuate depending on the working environment.
b. Good Pre-imperatives
   1. Workstation or PC
   2. Functional application (Microsoft NT or RedHat respectively)

To be unique to Tripware, Cybercop sting ans so on, there are numerous lucrative honeypots promptly accessible in the industry. This can be bought from the store, pit into the nearby structure.

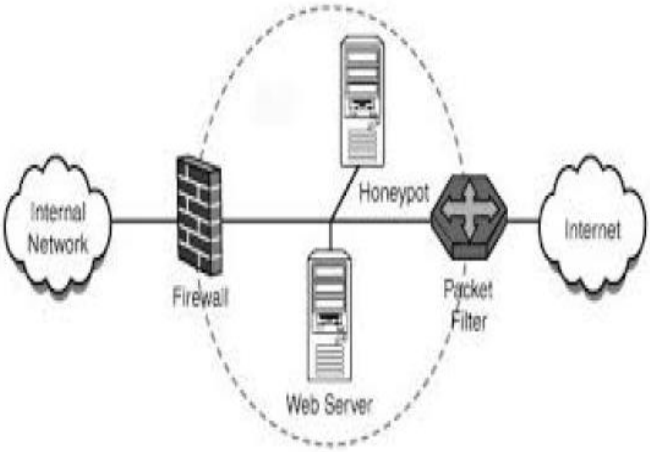
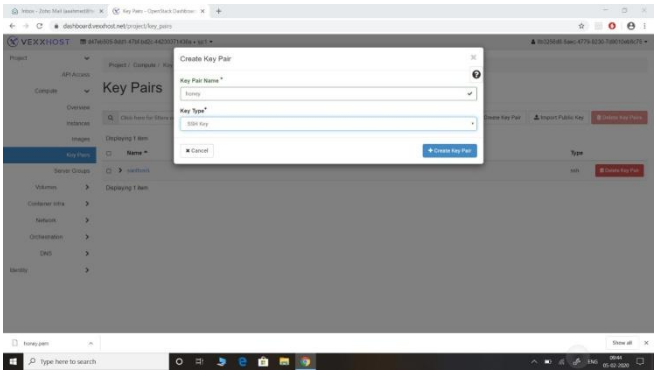
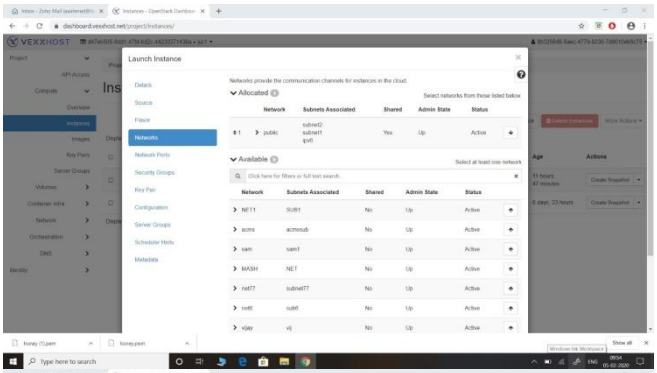


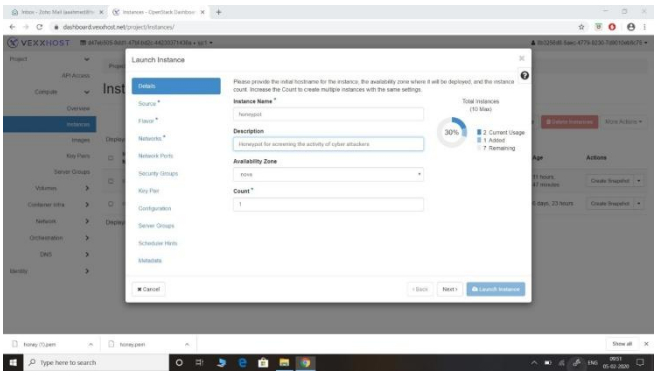
Figure 2: Architecture of a Honeypot

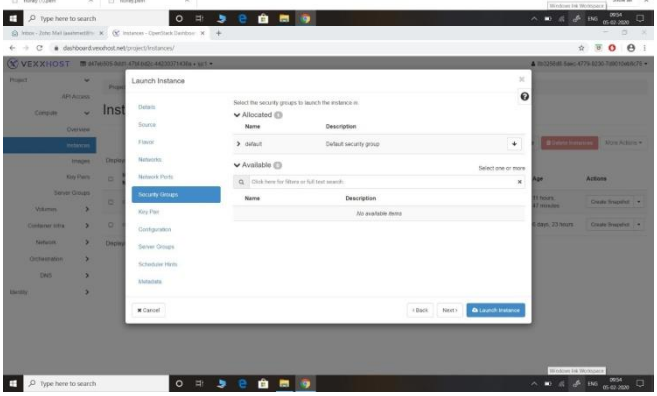
In this document, we've executed the honeypot to capture attackers data such as savings number and IP address controlled by government. A phony financial site is made available on a honeypot PC. A login page that includes the login I'd as the uniform savings number and a hidden word to access the banking arrangement is shown. Assume a programmer attempts to meddle into the bank organize by giving incorrectly data or use sql infusion strategies a log is caught for the given subtleties. The honeypot permits the programmers to go into the login page as though his login subtleties were approved and shows the page for doing reserve move, which is at last a phony page, and accordingly no mischief should be possible to the bank. By along these lines, a honeypot can be utilized to catch programmer data encroaching into a nearby system utilized by little scope enterprises.

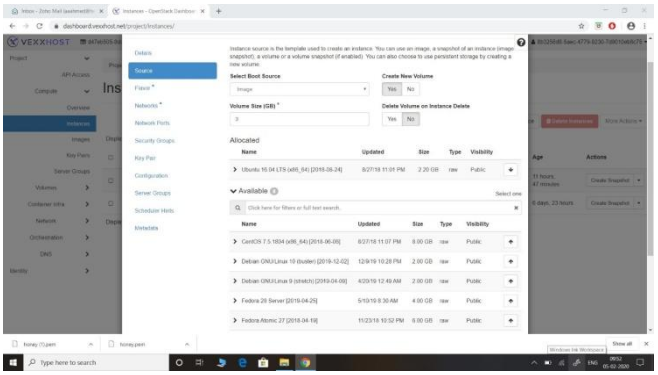
IV. RESULT

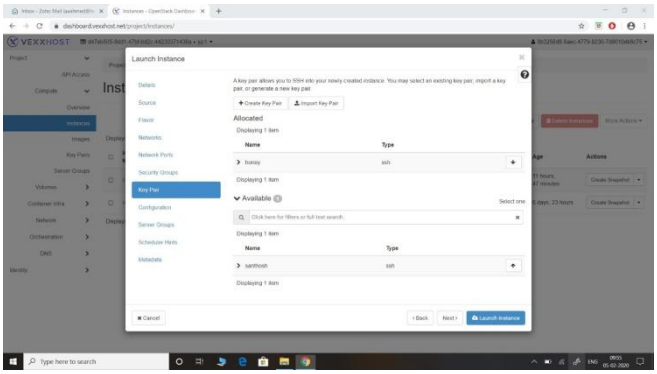

Create Key Pair
Key Pairs

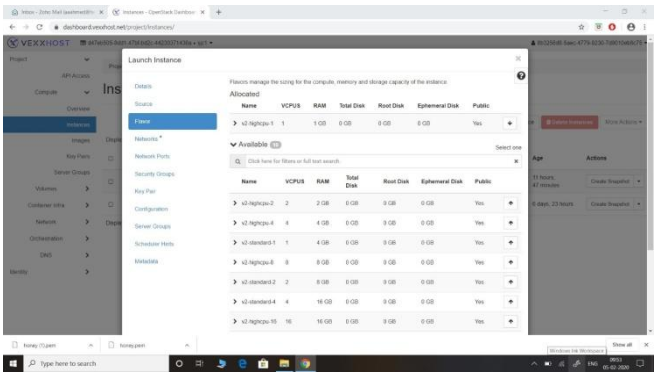

Launch Instance

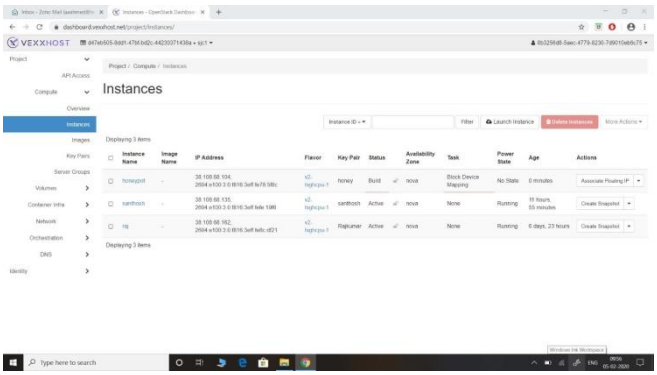

Launch Instance

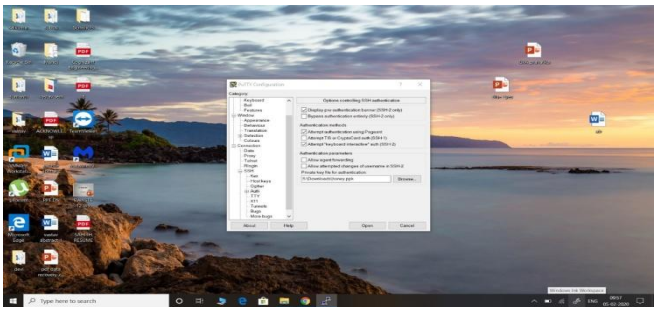

Launch Instance

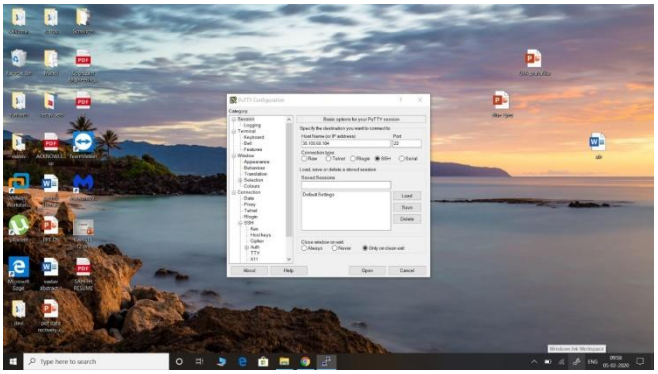

Launch Instance

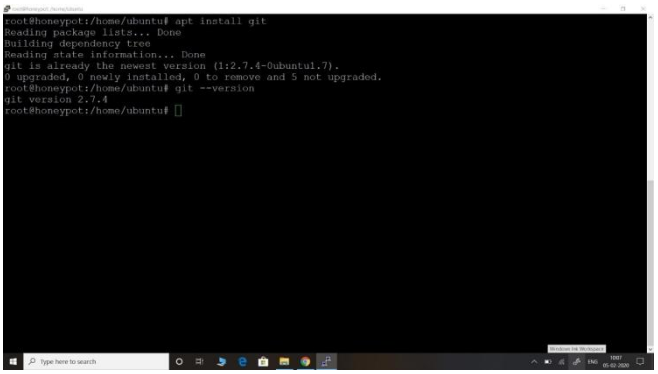

Launch Instance

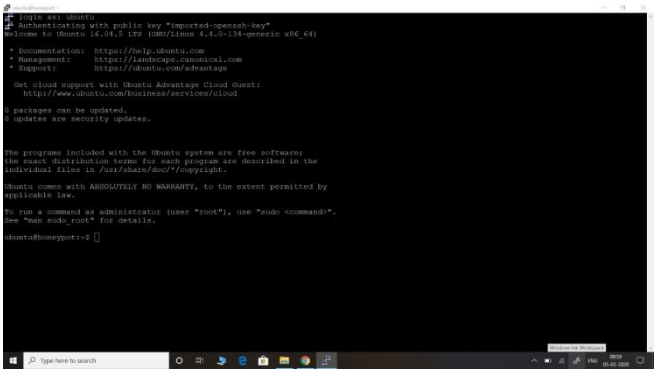

Launch Instance

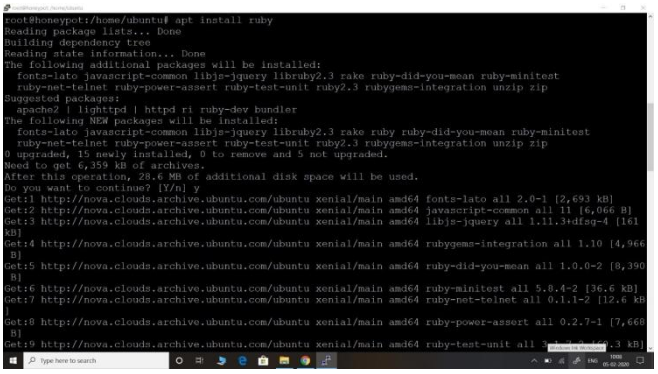

Instances

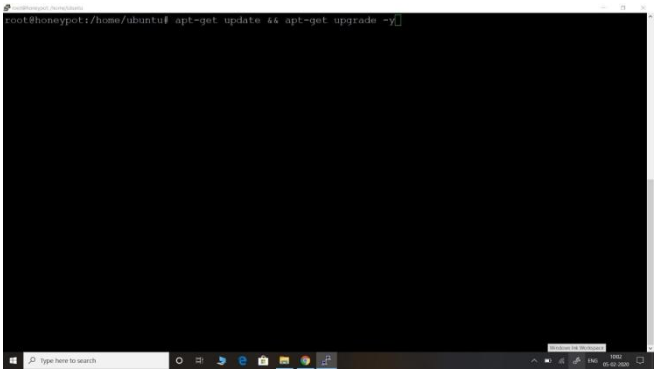


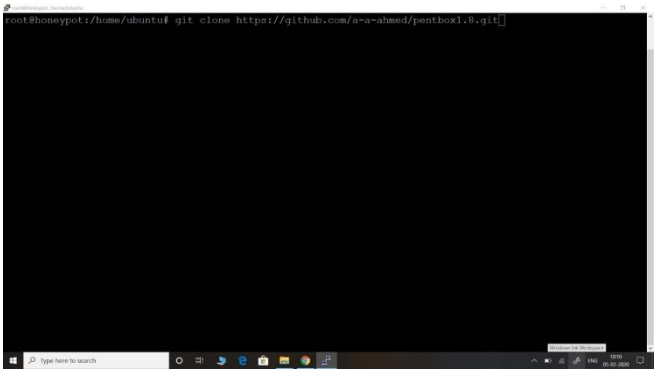


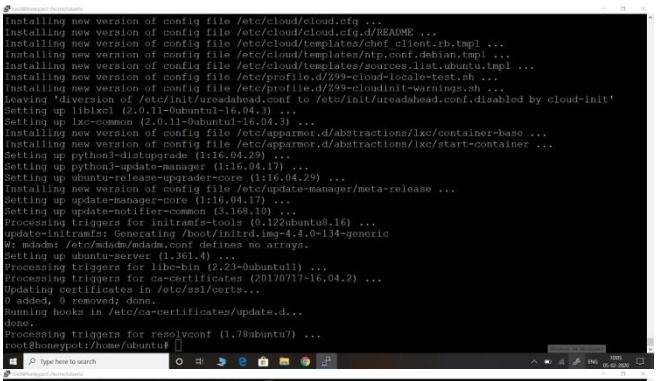

root@honeypot:/home/ubuntu# apt install git
Reading package lists... Done
Building dependency tree
Reading state information... Done
git is already the newest version (1:2.7.4-0ubuntu1.7).
0 upgraded, 0 newly installed, 0 to remove and 5 not upgraded.
root@honeypot:/home/ubuntu# git --version
git version 2.7.4
root@honeypot:/home/ubuntu#


* Documentation: https://help.ubuntu.com
* Management: https://landscape.canonical.com
* Support: https://ubuntu.com/advantage
0 packages can be updated.
0 updates are security updates.
ubuntu@honeypot:~$

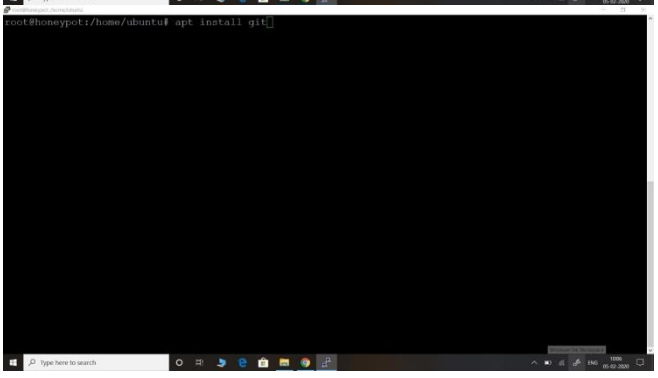

root@honeypot:/home/ubuntu# apt install ruby
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following additional packages will be installed:
fonts-lato javascript-common libjs-jquery libruby2.3 rake ruby-did-you-mean ruby-minitest
ruby-net-telnet ruby-power-assert ruby-test-unit ruby2.3 rubygems-integration unzip zip
Suggested packages:
apache2 | lighttpd | httpd ri ruby-dev bundler
The following NEW packages will be installed:
fonts-lato javascript-common libjs-jquery libruby2.3 rake ruby ruby-did-you-mean ruby-minitest
ruby-net-telnet ruby-power-assert ruby-test-unit ruby2.3 rubygems-integration unzip zip
0 upgraded, 15 newly installed, 0 to remove and 5 not upgraded.
Need to get 6,359 kB of archives.
After this operation, 28.6 MB of additional disk space will be used.
Do you want to continue? [Y/n] y

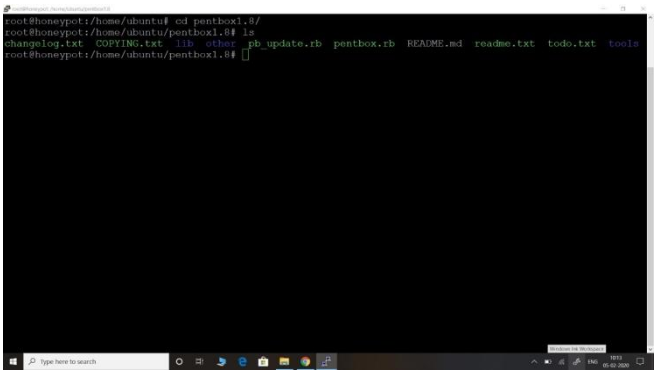

root@honeypot:/home/ubuntu# apt-get update && apt-get upgrade -y

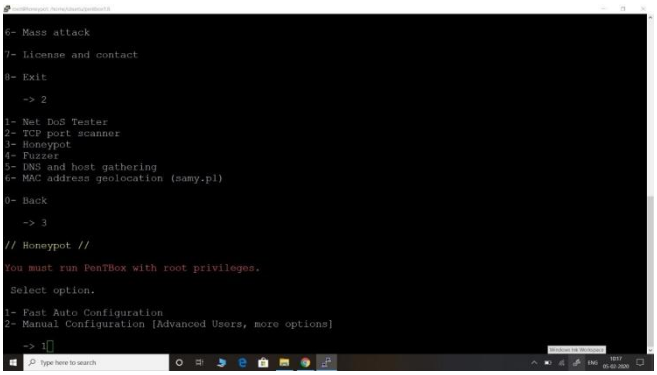

root@honeypot:/home/ubuntu# git clone https://github.com/a-a-ahmed/pentbox1.8.git

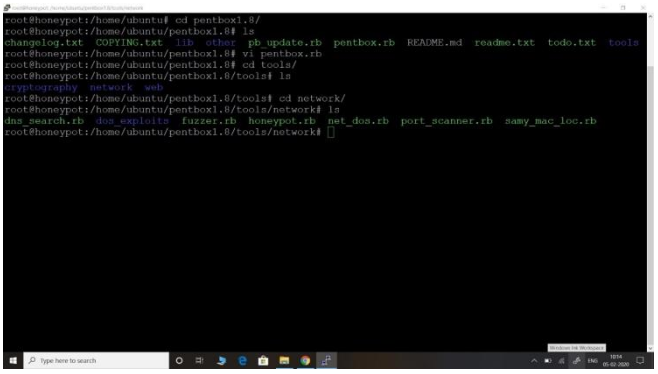

Installing new version of config file /etc/cloud/cloud.cfg ...
Installing new version of config file /etc/cloud/templates/chef_client.rb.tmpl ...
Installing new version of config file /etc/cloud/templates/ntp.conf.debian.tmpl ...
Installing new version of config file /etc/cloud/templates/sources.list.ubuntu.tmpl ...
Installing new version of config file /etc/profile.d/Z99-cloud-locale-test.sh ...
Installing new version of config file /etc/profile.d/Z99-cloudinit-warnings.sh ...
Setting up lxc-common (2.0.11-0ubuntu1~16.04.3) ...
Installing new version of config file /etc/apparmor.d/abstractions/lxc/container-base ...
Installing new version of config file /etc/apparmor.d/abstractions/lxc/start-container ...
Setting up python3-distupgrade (1:16.04.29) ...
Setting up python3-update-manager (1:16.04.17) ...
Setting up ubuntu-release-upgrader-core (1:16.04.29) ...
Installing new version of config file /etc/update-manager/meta-release ...
Setting up update-manager-core (1:16.04.17) ...
Setting up update-notifier-common (3.168.10) ...
Processing triggers for initramfs-tools (0.122ubuntu8.16) ...
update-initramfs: Generating /boot/initrd.img-4.4.0-134-generic
W: mdadm: /etc/mdadm/mdadm.conf defines no arrays.
Setting up ubuntu-server (1.361.4) ...
Processing triggers for libc-bin (2.23-0ubuntu11) ...
Processing triggers for ca-certificates (20170717~16.04.2) ...
Updating certificates in /etc/ssl/certs...
0 added, 0 removed; done.
Running hooks in /etc/ca-certificates/update.d...
done.
Processing triggers for resolvconf (1.78ubuntu7) ...
root@honeypot:/home/ubuntu#

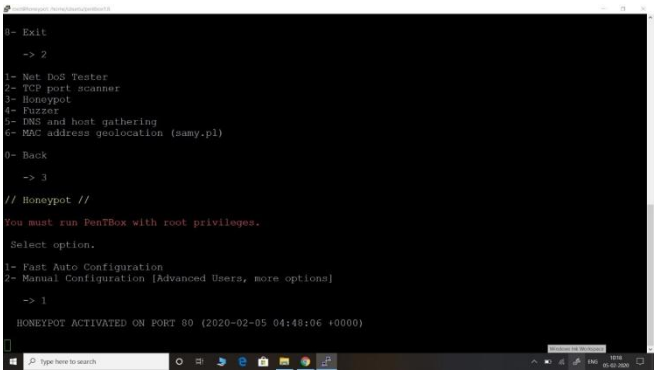

root@honeypot:/home/ubuntu# git clone https://github.com/a-a-ahmed/pentbox1.8.git
Cloning into 'pentbox1.8'...
remote: Enumerating objects: 309, done.
remote: Counting objects: 100% (309/309), done.
remote: Compressing objects: 100% (178/178), done.
remote: Total 309 (delta 114), reused 309 (delta 114), pack-reused 0
Receiving objects: 100% (309/309), 808.29 KiB | 0 bytes/s, done.
Resolving deltas: 100% (114/114), done.
Checking connectivity... done.
root@honeypot:/home/ubuntu# ls
pentbox1.8
root@honeypot:/home/ubuntu#

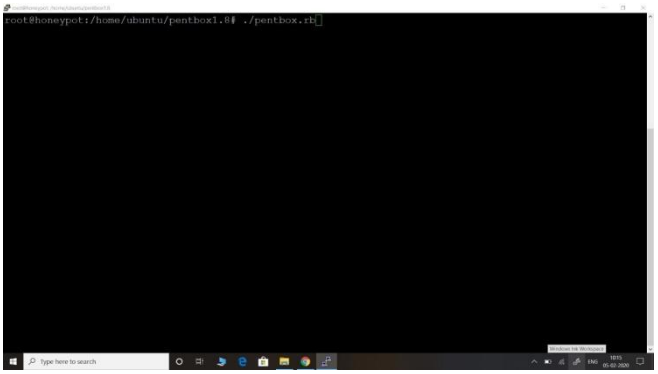

root@honeypot:/home/ubuntu# apt install git

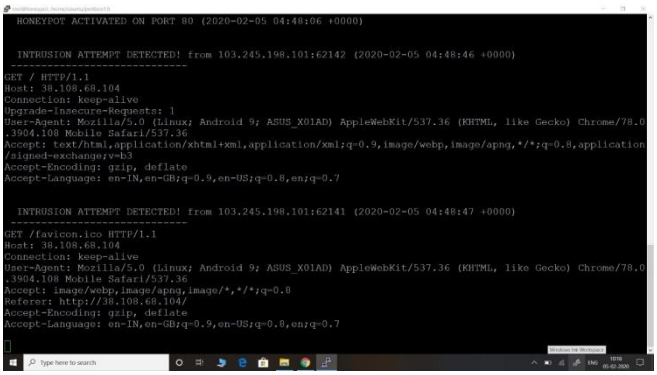


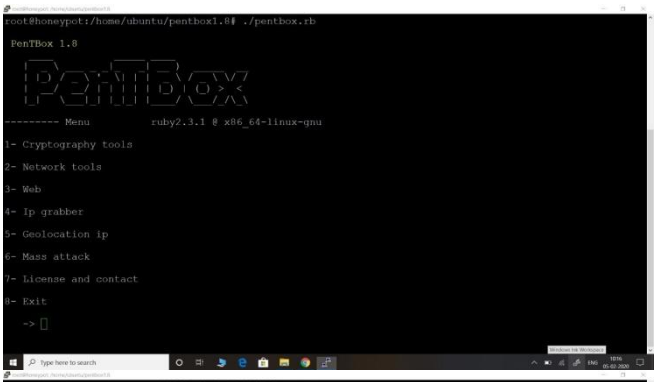


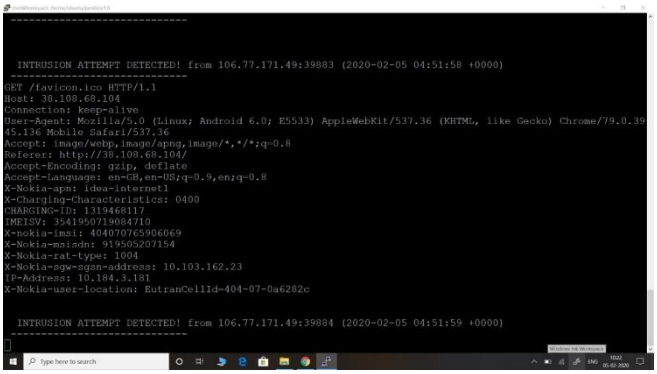


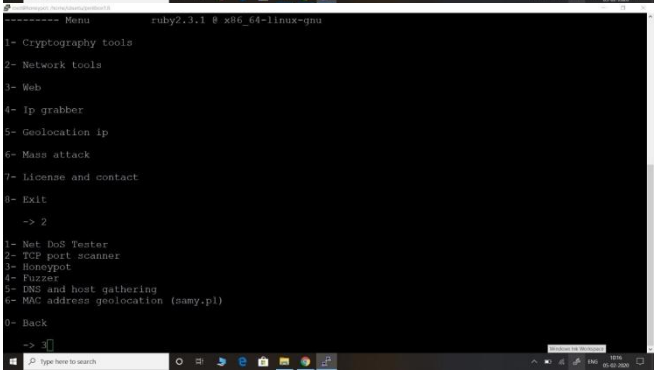












V. CONCLUSION

The proposed structure can block specific IP locations of programmers and furthermore give confirmations like SSN to the legitimate experts for making lawful move. As a future, upgrade realities that are more fascinating can be added to draw in the programmers. Because of the fast improvement in honeypot use, programmers began to concentrate on the techniques to sidestep the honeypots and encroach into the arrangement.

System head ought to limit these issues by utilizing solid doors. Log size is additionally a significant limitation to be taken care of. Developing logs are constantly an exhibition bottleneck what's more; reasonable advances ought to be taken for cleansing them in customary interims.

REFERENCES

1. Li Li et al, "The Design and Research of Honeypot System Applied in the Security of LAN", IEEE-2011
2. R.C.Joshi et al, "A Honeypot System for Efficient Capture and Analysis of Network Traffic", IEEE-2008
3. Iyad Kuwatly et al, "A Dynamic Honeypot Design for Intrusion Detection", IEEE-2010
4. Paramjeet Rawat, Sakshi Goel, Megha Agarwal and Ruby Singh, "SECURING WMN USING HYBRID HONEYPOT SYSTEM ",International Journal of Distributed and Parallel Systems (IJDPS) Vol.3, No.3, May 2011
5. Pushpa Rani, Yashpal Singh, S Niranjan," A Review in Honeypot as IDS for Wireless Network", IJERD 2012
6. Sandeep Chaware, "Banking Security using Honeypot ", International Journal of Security and Its Applications Vol. 5 No. 1, January, 2011
7. Jop van der Lelie, Rory Breuk, "A visual analytic approach for analysing SSH Honeypots", IEEE2012
8. Abhishek Sharma, "HONEYPOTS IN NETWORK SECURITY", International Journal of Technical Research and Applications 2013.
9. Collin Mulliner et al, "Poster: HoneyDroid - Creating a Smartphone Honeypot", IEEE2013
10. Radhika Goel, Anjali Sardana, and R. C. Joshi, "Wireless Honeypot: Framework, Architectures and Tools" International Journal of Network Security 2013
11. Matthias Wählisch, Sebastian Trapp, Christian Keil†, Jochen Schönfelder, "First Insights from a Mobile Honeypot", ACM 978-14503-1419-0/12/08

AUTHORS PROFILE

Mr. D.Rajesh Durganath pursuing Bachelors of Technology (Information Technology) from Guru Nanak Institutions Technical Campus. He is specialized in Hardware and Networking, Server Configuration and Maintenance, Cyber Security and Cloud Computing. He is certified as information security auditor by hackers school and Microsoft Certified Technology Specialist. His research work focuses on the security challenges in network and servers.

Mr. B. Sri Vastav pursuing Bachelors of Technology (Information Technology) from Guru Nanak Institutions Technical Campus.He is specialized in cloud computing (red hat open stack and amazon web services), server configuration maintenance and Networking.

Dr. M. I. Thariq Hussan is working as a Professor and Head, Department of Information Technology in Guru Nanak Institutions Technical Campus, Hyderabad, India. He was awarded his Doctoral Degree in the Faculty of Information and Communication Engineering from Anna University, Chennai, Tamil Nadu.