EasyChair Preprint

№ 4893

Computerized Honeypot

Dhruv Gajjar

January 12, 2021

Computerized Honeypot

Author Name: -Dhruv R. Gajjar

Abstract: -

In processing phrasing, a Honeypot is a firmly observed organization bait that fills a few needs. It can give early admonition about another assault or abuse patterns, can occupy enemies from other more important assets on an organization, or permit an itemized assessment of foes during and after a honeypot has been misused.

A honeypot normally fills in as an observation and early admonition instrument. It doesn't fix a solitary issue, yet is a profoundly adaptable security device that has various applications for security, It has numerous utilizations including counteraction, discovery and data gathering.

Objective: -

A honeypot is a security component that makes a virtual snare to bait assailants. A deliberately undermined PC framework permits assailants to abuse weaknesses so you can consider them to improve your security arrangements. You can apply a honeypot to any figuring asset from programming and organizations to record workers and switches.

Introduction: -

What is Computerized?

To control, perform, cycle, or store (a framework, activity, or data) by methods for or in an electronic PC or PCs. To outfit with or robotize by PCs: to modernize a business. For instance, we have utilized site to have honeypot.

In registering, an info gadget is a fringe (bit of PC equipment hardware) used to give information and control signs to a data preparing framework, for example, a PC or other data machine. Instances of information gadgets incorporate consoles, mice, scanners, computerized cameras and joysticks.

How does computerized works?

A blueprint of interconnected PCs that share a focal amassing structure and assorted fringe contraptions, for example, a printers, scanners or switches. Every PC related with the framework can work uninhibitedly, yet can conserves with other outside gadgets and PCs.

What is Honeypot?

A honeypot is a security mechanism that creates a virtual trap to lure attackers. An intentionally compromised computer system allows attackers to exploit vulnerabilities so you can study them to improve your security policies. You can apply a honeypot to any computing resource from software and networks to file servers and routers.

Honeypots are a type of deception technology that allows you to understand attacker behaviour patterns. Security teams can use honeypots to investigate cybersecurity breaches to collect Intel on how cybercriminals operate. They also reduce the risk of false positives, when compared to

traditional cybersecurity essential, because they are unlikely to attract legitimate activity.

How does honeypot works?

On the off chance that you, for example, were accountable for IT security for a bank, you may set up a honeypot framework that, to outcasts, resembles the bank's organization. The equivalent goes for those accountable for or investigating different sort of secure web associated frameworks.

By monitoring traffic to such systems, you can better understand where cybercriminals are coming from, how they operate, are what they want. More importantly, you can determine which security essential you have in place are working and which ones may need improvement.

Honeypots vary based on design and deployment models, but they are all decoys intended to look like legitimate, vulnerable systems to attract cybercriminals.

Types of honeypot?

Honeypots can be separate based on their deployment (use/action) and based on their level of involvement. Based on deployment, honeypots may be separated as

Production honeypots are run to gather intelligence, and are used primarily by corporations. Production honeypots are placed inside the production network with other production servers by an organization to improve their overall state of security. Normally, production honeypots are low-interaction honeypots, which are easier to deploy. They give less intelligence about the attacks or attackers than research honeypots.

Research honeypots are run to gather intelligence about the motives and tactics of the black hat community targeting different networks. These honeypots do not add direct value to a specific organization; instead, they are used to research the threats that organizations face and to learn how to better protect against those threats. Research honeypots are complex to deploy and maintain, capture extensive intelligence, and are used primarily research, military, or government organizations.

Based on design criteria, honeypots can be separated as

Pure honeypots are fully-fledged production systems. The activities of the attacker are observed by utilizing a bug tap that has been installed on the honeypot's link to the network. No other software needs to be installed. Even though a pure honeypot is useful, stealthiness of the defence mechanisms can be ensured by a more controlled mechanism.

High-interaction honeypots imitate the activities of the production systems that host a variety of services and, therefore, an assailant might be permitted a great deal of administrations to waste their time. By employing virtual machines, multiple honeypots can be hosted on a single physical machine. Therefore, even if the honeypot is compromised, it can be restored more quickly. In general, high-interaction honeypots provide more security by being difficult to detect, but they are expensive to maintain. If virtual machines are not available, one physical computer must be maintained for each honeypot, which can be exorbitantly expensive. Example: Honeynet.

Low-interaction honeypots simulate only the service frequently requested by attackers. Since they consume relatively few resources, multiple virtual machines can easily be hosted on one physical system, the virtual

systems have a short response time, and less code is required, reducing the complexity of the virtual system's security. Example: Honeyd.

Recently, a new market segment called deception technology has emerged using basic honeypot technology with the addition of advanced automation for scale. Deception technology addresses the automates deployment of honeypot resources over a large commercial enterprise or government institution.

Malware honeypots are used to detect malware by exploiting the know replica and attack vectors of malware. Imitation vectors, for example, USB streak drives can undoubtedly be checked for proof of changes, either through manual or using specific reason honeypots that copy drives. Malware progressively is utilized to look for and take digital forms of money.

Simulation: -

Tools: -

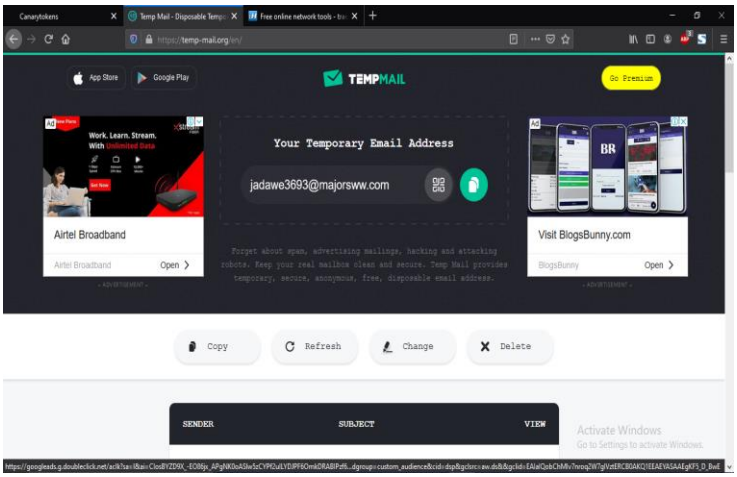
https://nmap.org/ :- nmap

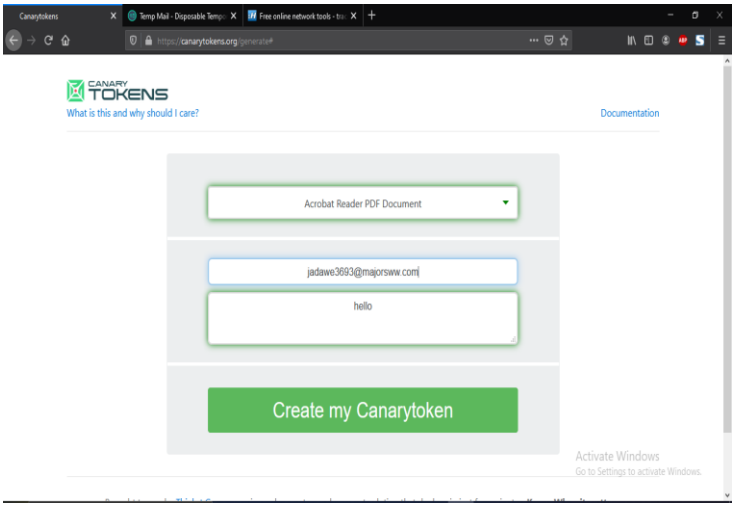
Websites: -

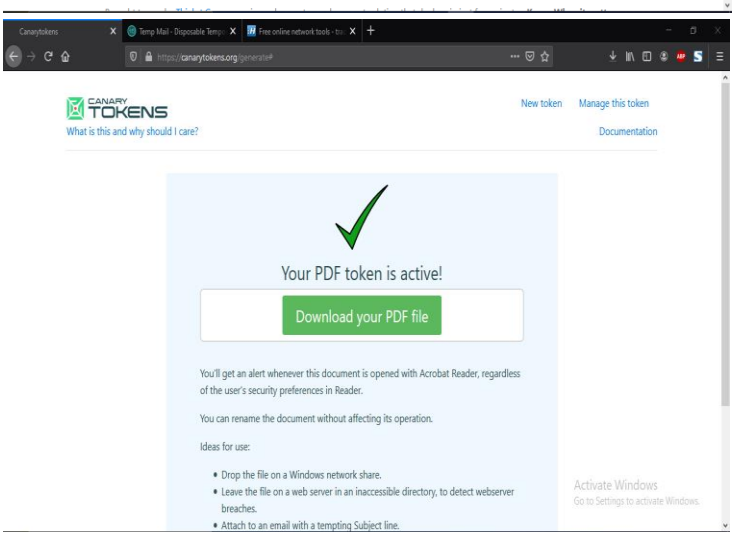
https://temp-mail.org/en/ : - temp mail

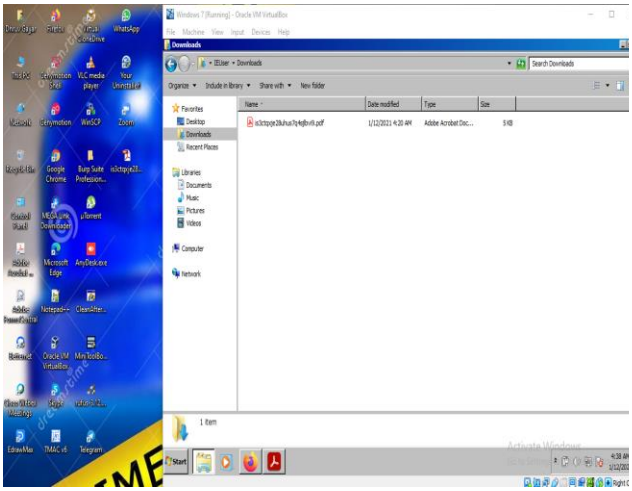
https://canarytokens.org/ : - canary token

https://centralops.net/ :- centralops

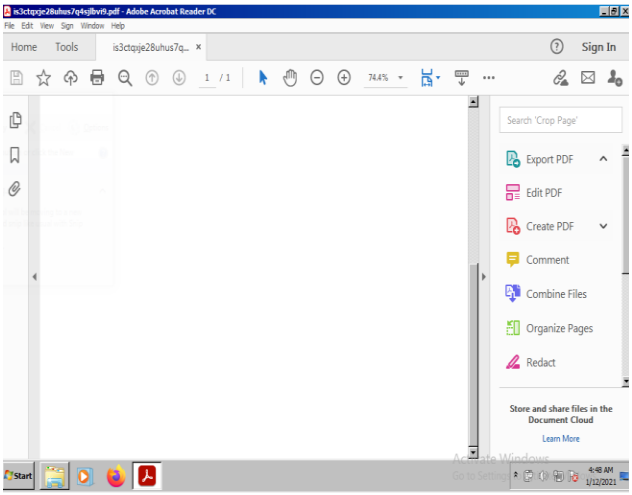


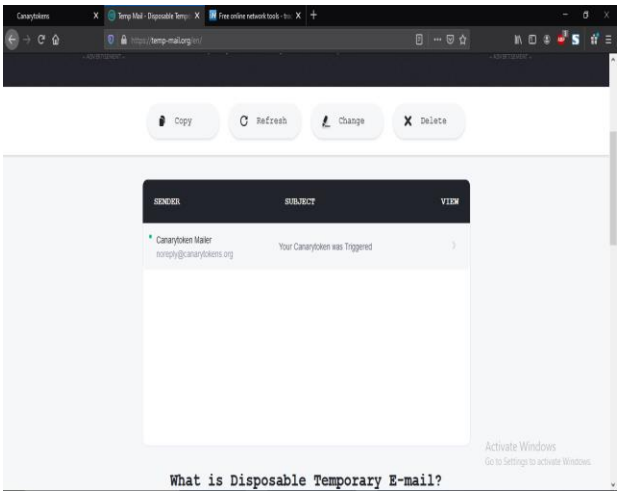




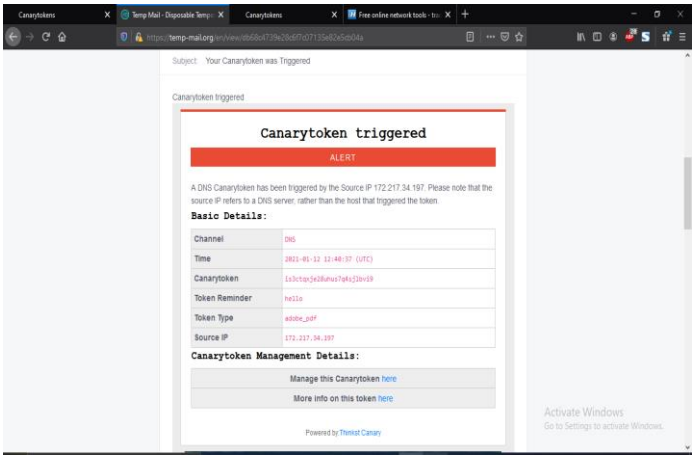


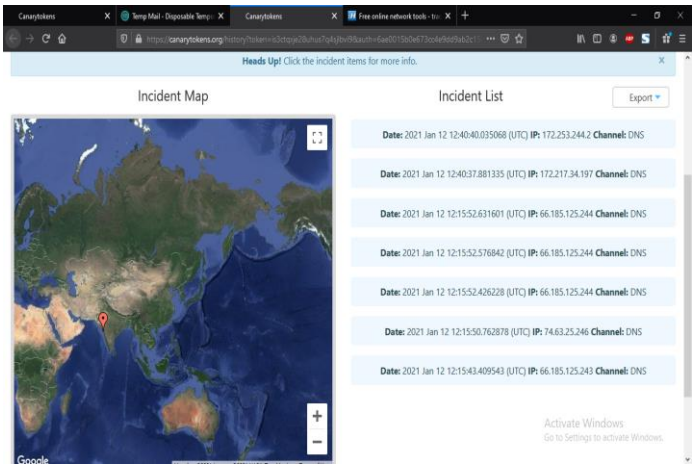
Transfer of files to the other window



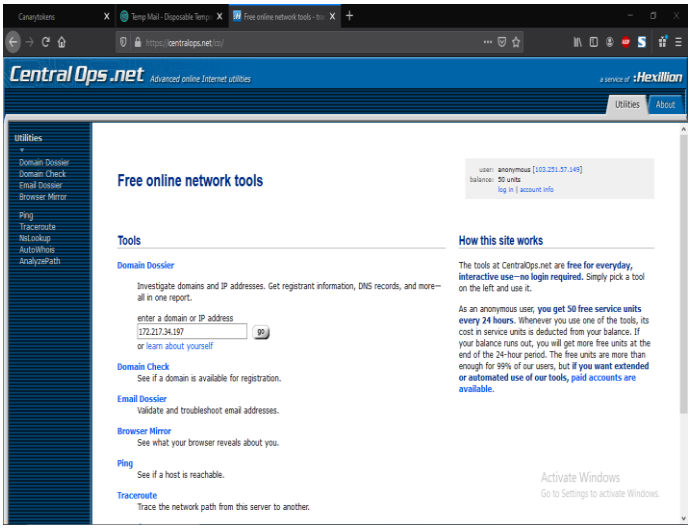


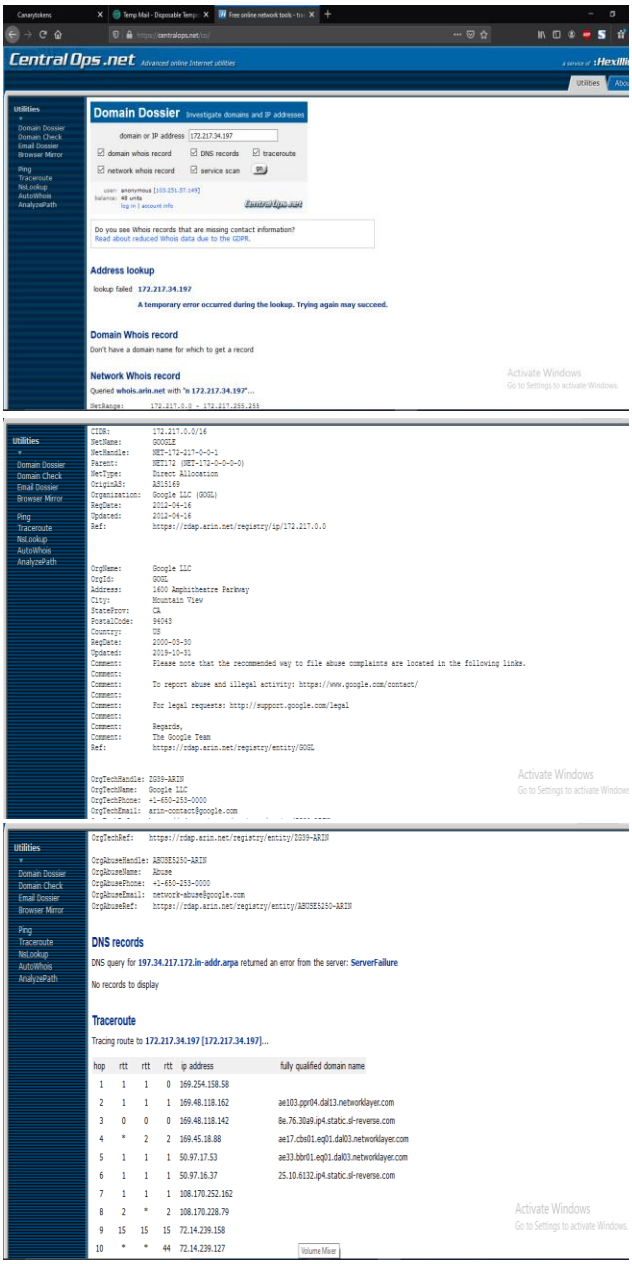
Mail Alert





Geolocation



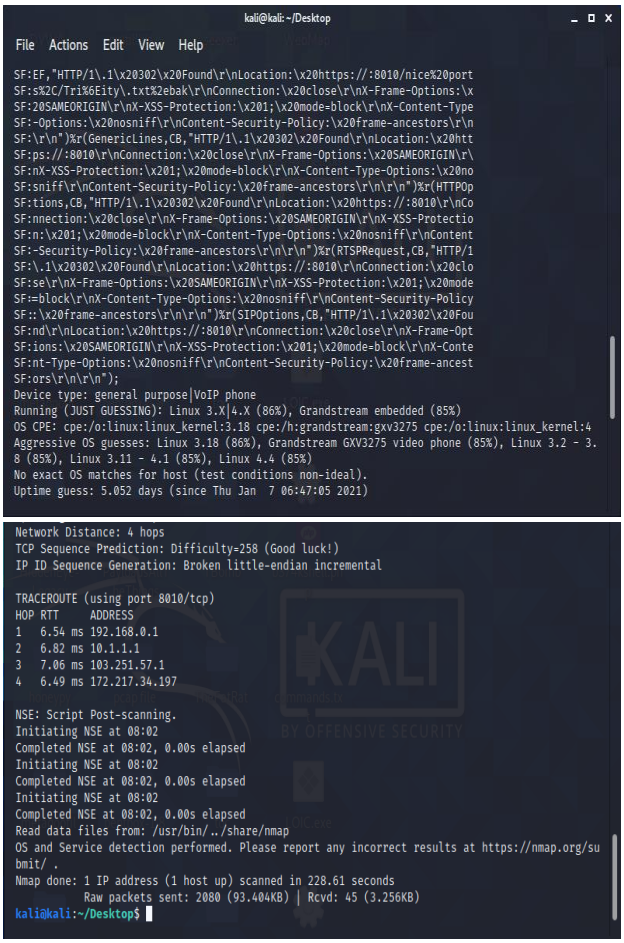


DNS Report

```
kali@kali: ~/Desktop
File  Actions  Edit  View  Help

kali@kali:~/Desktop$ sudo nmap -O -A -T4 -v 172.217.34.197
[sudo] password for kali:
Starting Nmap 7.91 ( https://nmap.org ) at 2021-01-12 07:58 EST
NSE: Loaded 153 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 07:59
Completed NSE at 07:59, 0.00s elapsed
Initiating NSE at 07:59
Completed NSE at 07:59, 0.00s elapsed
Initiating NSE at 07:59
Completed NSE at 07:59, 0.00s elapsed
Initiating Ping Scan at 07:59
Scanning 172.217.34.197 [4 ports]
Completed Ping Scan at 07:59, 0.37s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 07:59
Completed Parallel DNS resolution of 1 host. at 07:59, 2.92s elapsed
Initiating SYN Stealth Scan at 07:59
Scanning 172.217.34.197 [1000 ports]
Discovered open port 8008/tcp on 172.217.34.197
Discovered open port 2000/tcp on 172.217.34.197
Completed SYN Stealth Scan at 07:59, 4.64s elapsed (1000 total ports)
Initiating Service scan at 07:59
Scanning 2 services on 172.217.34.197
Service scan Timing: About 50.00% done; ETC: 08:03 (0:02:19 remaining)
Completed Service scan at 08:01, 161.47s elapsed (2 services on 1 host)
Initiating OS detection (try #1) against 172.217.34.197
Retrying OS detection (try #2) against 172.217.34.197
```

```
kali@kali: ~/Desktop
File  Actions  Edit  View  Help

Initiating Traceroute at 08:02
Completed Traceroute at 08:02, 0.02s elapsed
Initiating Parallel DNS resolution of 4 hosts. at 08:02
Completed Parallel DNS resolution of 4 hosts. at 08:02, 2.90s elapsed
NSE: Script scanning 172.217.34.197.
Initiating NSE at 08:02
Completed NSE at 08:02, 28.20s elapsed
Initiating NSE at 08:02
Completed NSE at 08:02, 1.12s elapsed
Initiating NSE at 08:02
Completed NSE at 08:02, 0.00s elapsed
Nmap scan report for 172.217.34.197
Host is up (0.0081s latency).
Not shown: 996 filtered ports
PORT     STATE  SERVICE     VERSION
113/tcp  closed ident
2000/tcp open   cisco-sccp?
8008/tcp open   http
| fingerprint-strings:
|   FourOhFourRequest:
|     HTTP/1.1 302 Found
|     Location: https://:8010/nice%20ports%2C/Tri%6Eity.txt%2ebak
|     Connection: close
|     X-Frame-Options: SAMEORIGIN
|     X-XSS-Protection: 1; mode=block
|     X-Content-Type-Options: nosniff
|     Content-Security-Policy: frame-ancestors
```

```
kali@kali: ~/Desktop
File  Actions  Edit  View  Help

|   GenericLines, HTTPOptions, RTSPRequest, SIPOptions:
|     HTTP/1.1 302 Found
|     Location: https://:8010
|     Connection: close
|     X-Frame-Options: SAMEORIGIN
|     X-XSS-Protection: 1; mode=block
|     X-Content-Type-Options: nosniff
|     Content-Security-Policy: frame-ancestors
|   GetRequest:
|     HTTP/1.1 302 Found
|     Location: https://:8010/
|     Connection: close
|     X-Frame-Options: SAMEORIGIN
|     X-XSS-Protection: 1; mode=block
|     X-Content-Type-Options: nosniff
|_    Content-Security-Policy: frame-ancestors
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-title: Did not follow redirect to https://172.217.34.197:8010/
8010/tcp closed xmpp
1 service unrecognized despite returning data. If you know the service/version, please submit
the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port8008-TCP:V=7.91%I=7%D=1/12%Time=5FFD9D29%P=x86_64-pc-linux-gnu%r(Ge
SF:tRequest,CC,"HTTP/1\.1\x20302\x20Found\r\nLocation:\x20https://:8010/\r
SF:\nConnection:\x20close\r\nX-Frame-Options:\x20SAMEORIGIN\r\nX-XSS-Prote
SF:ction:\x201;\x20mode=block\r\nX-Content-Type-Options:\x20nosniff\r\nCon
SF:tent-Security-Policy:\x20frame-ancestors\r\n\r\n")%r(FourOhFourRequest,
```



Nmap Report

Conclusion: -

Honeypot and its types are used for multiple purpose which includes used for counteraction, discovery and data gathering.

Reference: -

Linux Basics for Hackers: Getting Started with Networking, Scripting, and Security in Kali By: - OccupyThe Web

Cyber Forensics By: - Dejey, Murugan

Computer Forensics and Cyber Crime: An Introduction, 2e By: - Britz

https://www.wikipedia.org :- Wikipedia

https://nmap.org/ :- nmap

https://temp-mail.org/en/ : - temp mail

https://canarytokens.org/ : - canary token

https://centralops.net/ :- centralops