ISSN No:-2456-2165

Cybersecurity Awareness Counter Cyber Threats and Terrorism: A Case Study of Cybersecurity in MINICT

BASOMINGERA Senga Gael[1] Masters, Dr. Musoni Wilson[2] Supervisor,
[1] Information Communication and Technology (ICT), University of Kigali, Kigali, Rwanda

Abstract:- Nowadays, cybersecurity plays a bigger role in the world of technology whereby each and each of the fields now have joined a digitalization ecosystem, this implies the needs CIA triad where data availability, confidentiality and integrity must take in place.

As the technology is growing faster and wider, users or people must be aware of cybersecurity at least having basic knowledge. This may help to lessen cyber threats and terrorism whereby due to user's awareness and basic knowledge they could now be proactive rather than being reactive which this can result in as a success story. The idea of this research came after realizing and looking into Rwandan digitalization policy and growth where at each stage or level to IT infrastructure they must be also a security measure taken to prevent from any intruders to exploit the environment so due to that there are some standards, measures and policies to be taken in order to secure the entire environment.

On this research, I have been exploring trending cyber risks, how to assess them and how to detect, prevent and analyze them whereby I have been using different tools used in the world of cybersecurity. I have introduced the value and benefit of taking cybersecurity into consideration, whereby I have been providing techniques that can be implemented, policy standards and much more used to secure and harden IT infrastructure based on OSI model concept where I have been showing how to secure from the physical layer up the application layer.

To do so I have therefore need some common customized tools such as Burpsuite, nmap, nessus, Metasploit and much more as each tool has different features and capacity and I have been using a variety of tools as my research have be a qualitative research based, what I have be emphasizing on is the quality of service to be ensured in for the organization cybersecurity assurance.

I. INTRODUCTION

Cyber security in today's words plays a bigger role whereby in today's generation we have now became a digital driven world where each and every service can be requested and being provided online without moving, this to be happen there must be infrastructures and also those infrastructures must be secure in other to avoid intruders to compromise the process. To do so we involve cyber security to ensure process safety and privacy whereby we protect data from the source up to the expected destination.

Safeguarding, detection, and reply are indeed the three foundational pillars of security. It is advisable to initiate a self-assessment to identify gaps within each pillar; most enterprises evolved over time and never really updated their security tools to accommodate the new threat landscape and how attackers exploit vulnerabilities.

The majority of business operations are conducted over the internet, exposing their data and resources to a variety of cyber threats. Because data and system resources are the foundations upon which the organization operates, it follows that a threat to these individuals is unquestionably a threat to the group as a whole. A threat can be anywhere between a minor bug in a code to a complex cloud hijacking liability.

As most of the organization shifted to the cloud based solution where they store their institution data sometime they even store sensitive information and as we know how cloud computing works they gave you a place to store your information/data and it's up to you to maintain and secure your data so to do it you engage cyber security in other words while you're in a technology career (agriculture, aviation, telecommunication, IT etc.) the need of cyber security remains higher as each and every field use to share information online and as we know cyber security main goal is to secure cyber space from being threatened.

Cybersecurity and cyberwarfare have continued to be important research areas as the internet and communication technologies alter and evolve. Furthermore, for government management, internet transactions have become vital. This means that criminal networks have continue to discover ways to break security systems and target these transactions for breaches and fraudulent operations.

II. THE LOCKHEED MARTIN CYBER KILL CHAIN

The cyber kill chain methodology is part of an information defense strategy for detecting and preventing malicious intrusion activities. This methodology assists security professionals in identifying the steps adversaries take to achieve their objectives. The cyber kill chain is a framework for securing cyberspace that was inspired by military kill chains. The goal of this method is to actively improve intrusion detection and response. To mitigate and reduce cyber threats, the cyber kill chain contains a seven-phase defensive mechanism. According to Lockheed Martin, cybersecurity threats can occur in seven stages, from reconnaissance to completion of the objective.

The cyber kill chain is a quick and easy way to demonstrate how an adversary can attack the target organization. This model assists organizations in recognizing the various potential threats at each stage of an attack, as well as the countermeasures required to protect against such threats. Furthermore, this model provides security professionals with a clear understanding of the adversary's attack strategy, allowing different levels of security controls to be implemented to protect the organization's IT infrastructure.

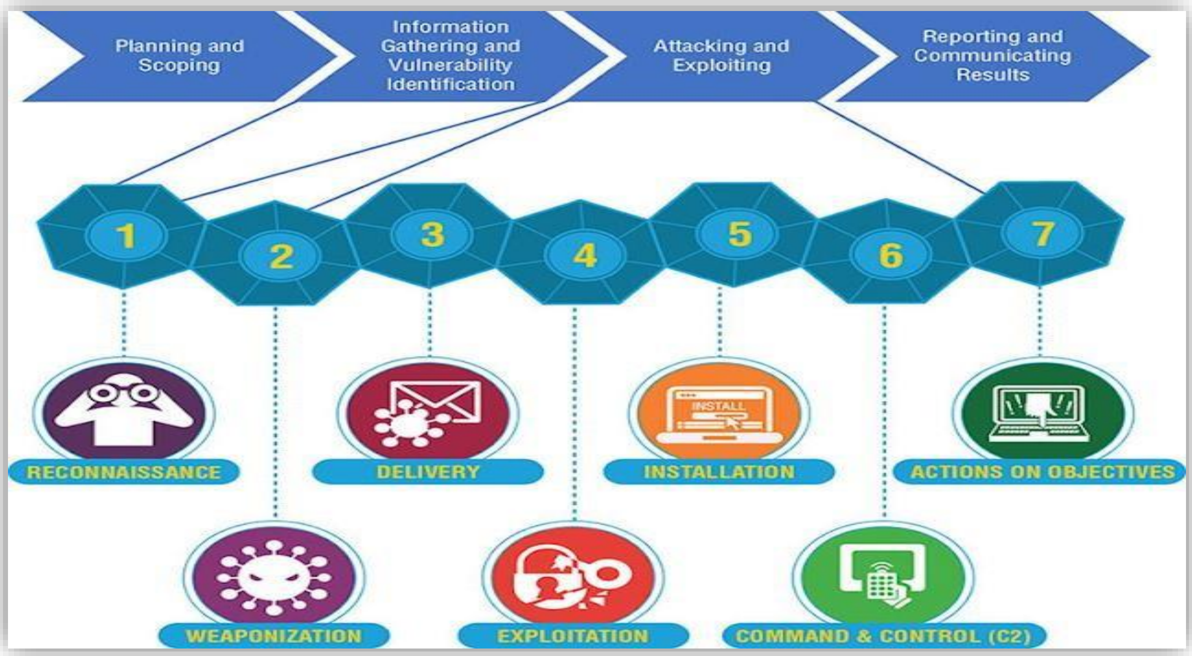


Fig. 1: Cyber Kill Chain

III. CYBERSECURITY FRAMEWORK

A cybersecurity framework provides a common language and set of standards for security leaders across countries and industries to help comprehend their own as well as their vendors' security postures. With a framework in place, defining the processes and procedures that your organization must follow to assess, monitor, and mitigate cybersecurity incidents becomes much easier.

There are seven common cybersecurity frameworks as shown below:

- NIST Cybersecurity Framework
- ISO 27001 and ISO 27002
- System and Organization Controls 2 (SOC2) Audits
- General Data Protection Regulation (GDPR)
- Federal Information Security Management Act (FISMA)

A. NIST Cybersecurity Framework

The National Institute of Standards and Technology (NIST) developed a Cybersecurity System which may be a deliberate direction, based on existing measures, rules, and hones for organizations to superior oversee and diminish cybersecurity hazard. In expansion to making a difference organizations oversee and diminish dangers, it was outlined to cultivate chance and cybersecurity administration communications among both inner and outside organizational partners.

It incorporates five functions which have been chosen since they speak to the five primary pillars for a fruitful and all-encompassing cyber security program.

The five Functions included in the Framework Core are:

- Identify: This aids in establishing a company's awareness of cybersecurity risk to systems, people, resources, information, and skills. Understanding the trade setting, the assets that back basic capacities, and the related cybersecurity dangers empowers an organization to center and prioritize its endeavors, reliable with its chance administration methodology and commerce needs.
- Protect: This function outlines appropriate safeguards to ensure critical infrastructure services are delivered. The Protect Function assists in limiting or containing the impact of a potential cybersecurity event.
- Detect: This function specifies activities required to discover the occurrence of a cybersecurity event. The Detect Function allows for the timely detection of cybersecurity events.
- Respond: This function includes activities required to respond to a detected cybersecurity incident. The Respond Function aids in mitigating the impact of a potential cybersecurity incident.
- Recover: This function identifies appropriate activities to maintain resilience plans and restore any capabilities or services that have been compromised as a result of a cybersecurity incident. The Recover Function enables

timely return to normal operations in order to mitigate the impact of a cybersecurity incident.

B. ISO 27001 and ISO 27002

ISO 27001 is the recognized standard for an organization's information security management system (ISMS). It explains how to do everything from system scoping to rule design to employee training.

ISO 27002 provides comprehensive knowledge on how to improve your ISMS. It contains the Annex A controls that must be implemented in order to receive ISO 27001 certification.

An organization's information security management system should follow the guidelines provided by the international security standard ISO 27001. (ISMS). In general, this is a list of all the things you must do to satisfy your needs. It can be adopted and implemented by organizations of all sizes and types, whether corporate or nonprofit, government or private.

The ISO 27002 standard is closely related to the ISO 27001 standard. It includes reference rules for information security, cybersecurity, data protection, and implementation assistance based on globally recognized best practices. In other words, it provides guidelines on how to build an ISO 27001 certified ISMS.

This standard does not have its own certification criteria. Alternatively, organizations can achieve ISO 27001 certification by complying with ISO 27002 information and physical security, cyber and privacy management controls. ISO 27002 addresses specific risks identified in the ISO 27001 risk assessment and provides a list of recommended controls.

C. System and Organization Controls 2 (SOC2) Audits

It is a framework designed to assist software vendors and other companies in demonstrating the security controls they use to protect customer data in the cloud. It is also known as SOC II. The Trust Services Principles are a set of controls that include security, availability, processing integrity, confidentiality, and privacy.

SOC 2 is designed specifically for service providers that store customer data in the cloud, to assist them in demonstrating the security controls they use to protect that data. As such, it applies to nearly every SaaS company and cloud vendor, as well as any company that stores customer data in the cloud.

D. General Data Protection Regulation (GDPR)

It’s a regulation in EU law for data protection and privacy in the European Union (EU) and the European Economic Area is known as the General Data Protection Regulation (EU) (GDPR) (EEA). A significant part of EU privacy legislation and human rights law is the GDPR. It deals with the export of personal data from the EU and EEA.

The main goals of the GDPR are to make it easier for international businesses to operate legally and to provide individuals more control and rights over their personal data. Since the GDPR is a regulation rather than a directive, it is immediately enforceable and applicable and offers room for individual member states to modify some components of the legislation.

E. Federal Information Security Management Act (FISMA)

Agencies must have an inventory of their information systems in place according to FISMA. In accordance with

FISMA, the head of each agency is required to create and maintain a list of the major information systems (including major national security systems) that are controlled or operated by that agency.

The list of information systems under this subsection shall also include a list of the interfaces that connect each such system to any other systems or networks, including those that are not controlled or operated by the agency.

The second mandatory security standard mandated by the FISMA legislation is FIPS 200, which is a minimum security requirement for federal information and information systems, it defines the minimum security requirements for federal information systems. Organizations must meet the minimum security requirements by choosing the appropriate security controls and assurance requirements.

IV. PROACTIVE VS REACTIVE CYBERSECURITY APPROACH

Reactive cybersecurity approach, it is when an assault happens, and your cybersecurity team reacts or responds, to the breach. The assault is found, the assailant repulsed, the harm is evaluated, and the clean-up starts. This is often frequently the standard way we think around cybersecurity teams and controls. There's nothing inalienably off-base with receptive security, usually portion of the reason you’ve contributed in cybersecurity controls, but when your whole security culture is receptive, that can be an issue.

When your cybersecurity culture is proactive, your team is committed to anticipation instead of essentially to reacting to threats. This implies contributing in a solid defensive position, educating your workers almost great cyber cleanliness, and arranging for risks your organization hasn’t yet encountered. Penetration testing, contracting ethical hackers to evaluate your framework, is additionally portion of a proactive cybersecurity strategy. Basically, a proactive cybersecurity team acknowledges that there are strategies of attacks they may not know around. Then they commit to learning almost and planning for as many attack scenarios as they can.

V. RESPONSE RATE FOR THE QUESTIONNAIRE AND INTERVIEW GUIDE

Typically, the result of the respondents working together to communicate their contemplations on a particular address, which is communicated in a few themes. 154 participants were sought for the study. 154 surveys and interviews were effectively assembled by the researcher. A return rate of more than 50% is respected as suitable for consider. This recommended that the information that had been assembled was satisfactory to carry out the examination.

Information on respondent's experience was also collected. The researcher's intention was to measure how work experience can help in collecting information concerning Cybersecurity awareness counter cyber threats and terrorism.

VI. METHODOLOGY

The results of this research study achieved through qualitative and descriptive methods. To achieve the best results, I used both quantitative and descriptive data collection methods. When I combined the two, we get deeper insights.

VII. DATA ANALYSIS

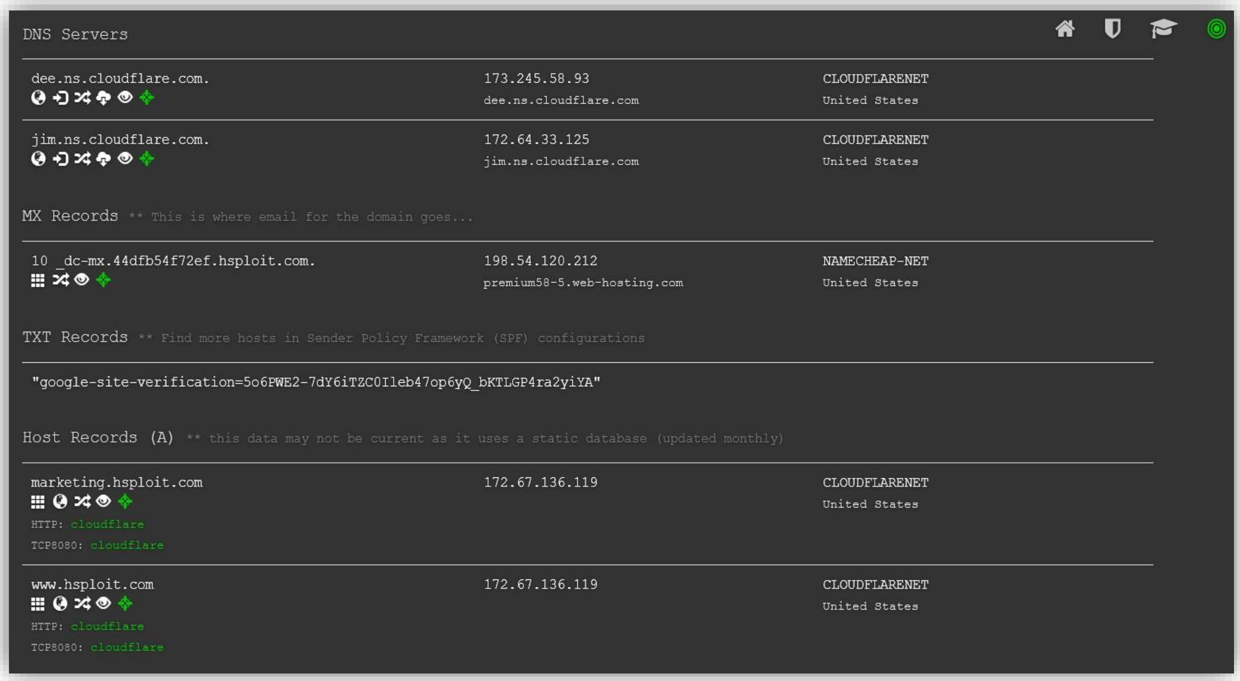
Data analysis is the process of cleaning, transforming, and processing raw data in order to extract actionable, relevant information that assists businesses in making informed decisions. The procedure reduces the risks associated with decision-making by providing useful insights and statistics, which are frequently presented in charts, images, tables, and graphs.

Kenton, (2019), said that, descriptive statistics are brief descriptive coefficients that summarize a given data set, which can be either a representation of the entire or a sample of a population. Descriptive statistics are divided into measures of central tendency and measures of variability (spread). The mean, median, and mode are examples of measures of central tendency, whereas the standard deviation, variance, minimum and maximum variables, and kurtosis and skewness are examples of measures of variability.

Descriptive statistics or frequencies used to summarize the data. The researcher evaluated the mean by using these equivalences which are found in the table illustrated below. These equivalences of mean help to know the perception of each group about the sub-variables.

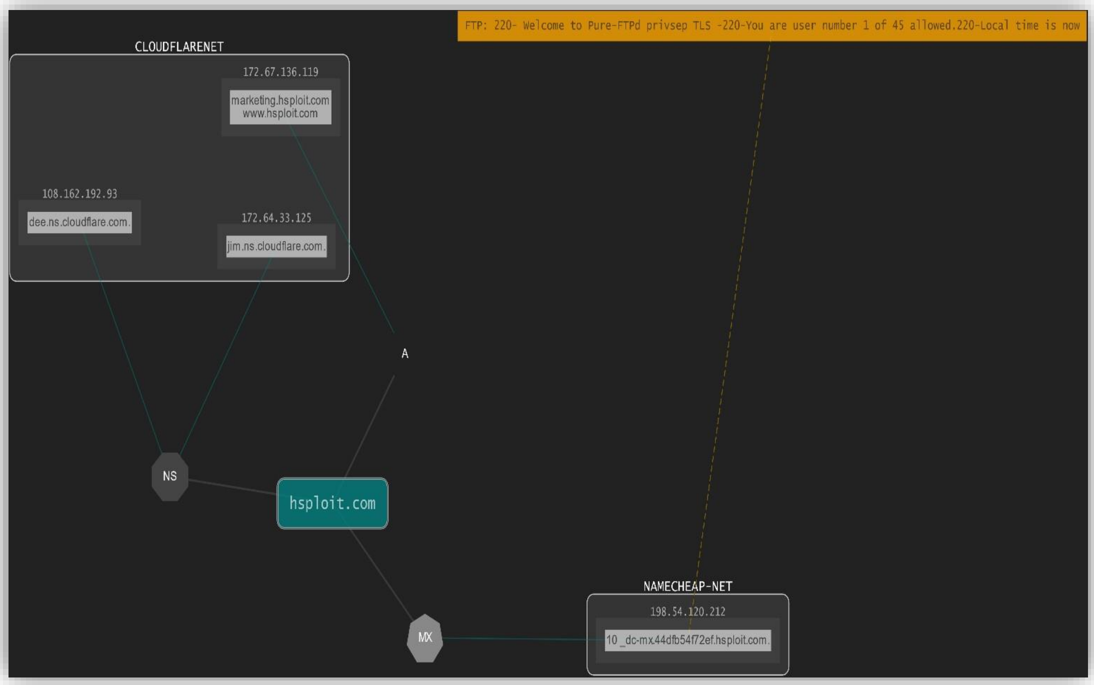
A. Domain Name System(DNS) Enumeration

Domain Name System(DNS) is a program that converts or translates a domain name into an IP address vice versa.DNS enumeration is one of the most important steps during the Information Gathering phase. When we talk about DNS enumeration, we're referring to all of the strategies we utilize to accumulate as much data as conceivable by questioning a website's or host's DNS server.



```
DNS Servers

dee.ns.cloudflare.com.          173.245.58.93              CLOUDFLARENET
                                dee.ns.cloudflare.com      United States

jim.ns.cloudflare.com.          172.64.33.125              CLOUDFLARENET
                                jim.ns.cloudflare.com      United States

MX Records ** This is where email for the domain goes...

10 _dc-mx.44dfb54f72ef.hsploit.com.   198.54.120.212               NAMECHEAP-NET
                                      premium58-5.web-hosting.com  United States

TXT Records ** Find more hosts in Sender Policy Framework (SPF) configurations

"google-site-verification=5o6PWE2-7dY6iTZC0Ileb47op6yQ_bKTLGP4ra2yiYA"

Host Records (A) ** this data may not be current as it uses a static database (updated monthly)

marketing.hsploit.com           172.67.136.119             CLOUDFLARENET
                                                           United States
HTTP: cloudflare
TCP8080: cloudflare

www.hsploit.com                 172.67.136.119             CLOUDFLARENET
                                                           United States
HTTP: cloudflare
TCP8080: cloudflare
```

Fig. 2: Dns Server Detailed Info



FTP: 220- Welcome to Pure-FTPd privsep TLS -220-You are user number 1 of 45 allowed.220-Local time is now

Fig. 3: Hsploit Dns Map

DNS enumeration is the process of locating all of an organization's DNS servers and their corresponding records. DNS enumeration will yield potential target systems' usernames, computer names, and IP addresses. The DNS record list provides an overview of the various types of resource records (database records) stored in the Domain Name System zone files (DNS). The DNS is a distributed, hierarchical, and redundant database that stores information about Internet domain names and addresses.

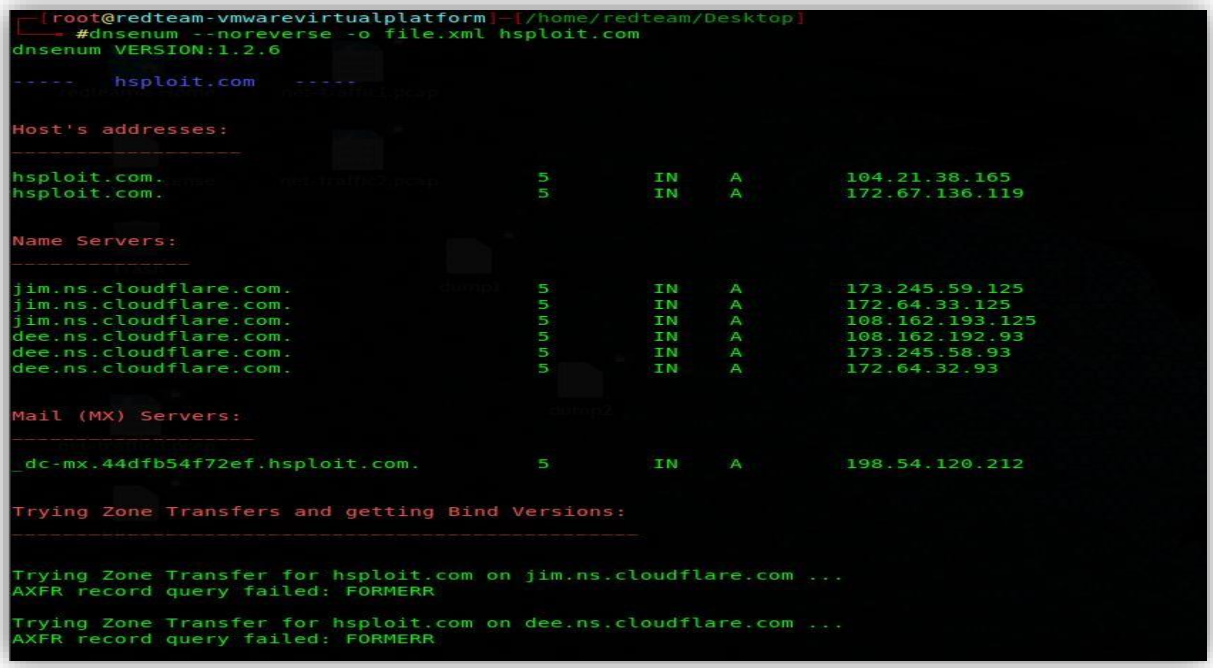
Once DNS enumeration is complete, unauthenticated users can use this information to inspect internal network records, grabbing useful DNS information that provides the intruder access to the entire DNS map. This allows him to explore any company's attack surface area in order to later scan it, collect data, and exploit it if there is an open opportunity. DNS Enumeration is used to collect as many potential details as possible about your target before initiating an exploit.

DNS provides a variety of information about public and sometimes private organization servers, such as IP addresses, server names, and server functionality.

B. Domain Name System(DNS) Enumeration using DnsEnum script

Dnsenum can be used to enumerate available DNS records for a domain and find non-contiguous IP blocks.

Dnsenum's main objective is to acquire as much information as possible on a domain.



```
┌─[root@redteam-vmwarevirtualplatform]─[/home/redteam/Desktop]
└──╼ #dnsenum --noreverse -o file.xml hsploit.com
dnsenum VERSION:1.2.6

-----   hsploit.com   -----


Host's addresses:
__________________

hsploit.com.                             5        IN    A        104.21.38.165
hsploit.com.                             5        IN    A        172.67.136.119


Name Servers:
______________

jim.ns.cloudflare.com.                   5        IN    A        173.245.59.125
jim.ns.cloudflare.com.                   5        IN    A        172.64.33.125
jim.ns.cloudflare.com.                   5        IN    A        108.162.193.125
dee.ns.cloudflare.com.                   5        IN    A        108.162.192.93
dee.ns.cloudflare.com.                   5        IN    A        173.245.58.93
dee.ns.cloudflare.com.                   5        IN    A        172.64.32.93


Mail (MX) Servers:
___________________

_dc-mx.44dfb54f72ef.hsploit.com.         5        IN    A        198.54.120.212


Trying Zone Transfers and getting Bind Versions:
_________________________________________________


Trying Zone Transfer for hsploit.com on jim.ns.cloudflare.com ...
AXFR record query failed: FORMERR

Trying Zone Transfer for hsploit.com on dee.ns.cloudflare.com ...
AXFR record query failed: FORMERR
```

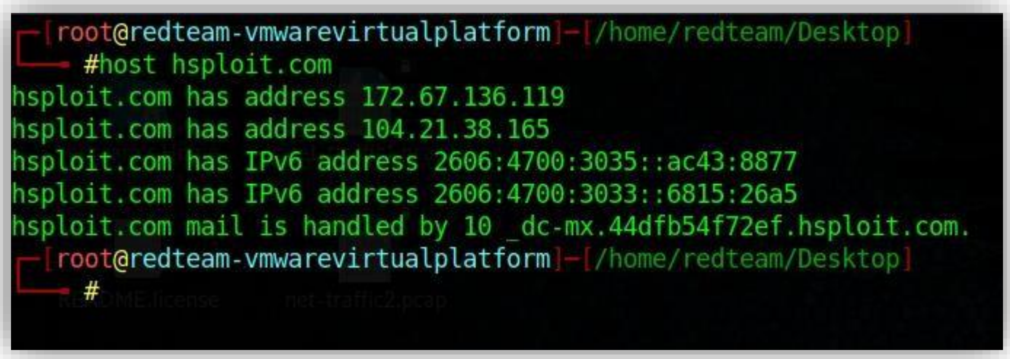
Fig. 4: Dnsenum enumeration output

DNSEnum is one of the best script used specifically designed for DNS recon activities. It is written in Perl and it can help to create a full DNS map of any domain name available on the Internet. DNS Zone Transfer is a method of replicating DNS data across multiple DNS servers or backing up DNS files. A specific zone transfer request from a name server will be performed by a user or server. If the name server allows anonymous zone transfers, all DNS names and IP addresses hosted by the name server will be returned in human-readable ASCII text. DNS enumeration is a popular reconnaissance task for developing a profile of your target.

C. Domain Name System(DNS) Enumeration using host script

For DNS (Domain Name System) lookup activities, the host command is used in the Linux operating system.

Clearly explained, the host command comes in handy if you want to discover the domain name linked to a particular IP address or if you want to find the IP address associated with a specific domain name. By adding the corresponding option to the domain name, you can also get additional specific information about a domain.

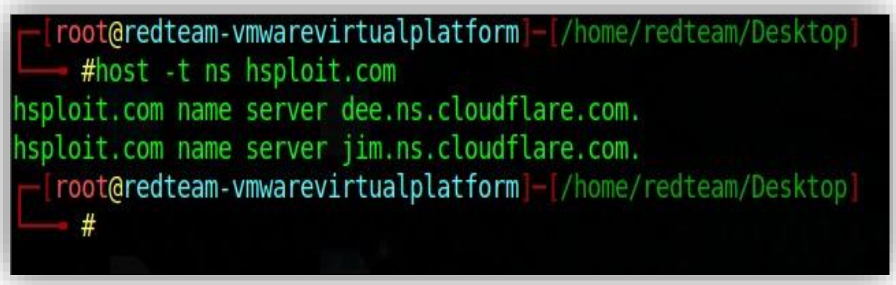


```
┌─[root@redteam-vmwarevirtualplatform]─[/home/redteam/Desktop]
└──╼ #host hsploit.com
hsploit.com has address 172.67.136.119
hsploit.com has address 104.21.38.165
hsploit.com has IPv6 address 2606:4700:3035::ac43:8877
hsploit.com has IPv6 address 2606:4700:3033::6815:26a5
hsploit.com mail is handled by 10 _dc-mx.44dfb54f72ef.hsploit.com.
┌─[root@redteam-vmwarevirtualplatform]─[/home/redteam/Desktop]
└──╼ #
```

Fig. 5: host enumeration output

With the above script you're able to identify the public internet protocol associate to your domain name, as shown above the hsploit.com domain is associated to 2 public internet protocol addresses which are **172.67.136.119** and **104.21.38.165**.

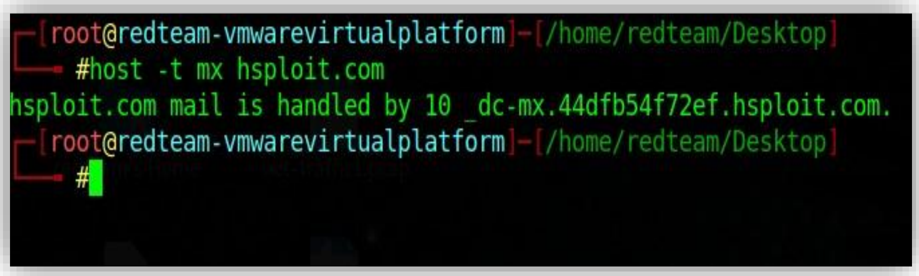
A public IP address is one that can be accessed directly via the internet and is assigned by your internet service provider (ISP) to your network router.



```
┌─[root@redteam-vmwarevirtualplatform]─[/home/redteam/Desktop]
└──╼ #host -t ns hsploit.com
hsploit.com name server dee.ns.cloudflare.com.
hsploit.com name server jim.ns.cloudflare.com.
┌─[root@redteam-vmwarevirtualplatform]─[/home/redteam/Desktop]
└──╼ #
```

Fig. 6: host name server enumeration filtered output

With the above script an intruder is able to gather and identify name servers associated to your domain, as for the above scenario I've been able to gather 2 name servers for the hsploit.com domain, the 2 name servers identified are **dee.ns.cloudflare.com** and **jim.ns.cloudflare.com**. after this we definitely identify also where the application is hosted as of now it's hosted at cloudflare.



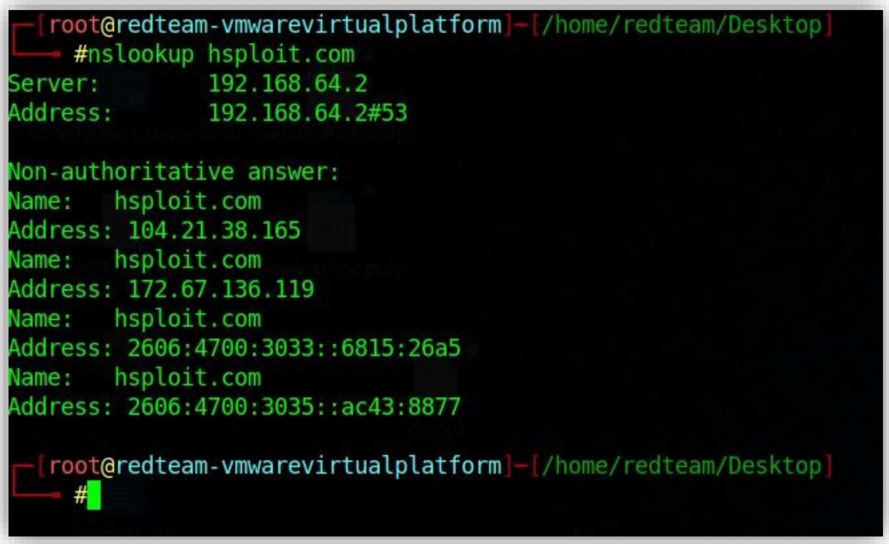
```
┌─[root@redteam-vmwarevirtualplatform]─[/home/redteam/Desktop]
└──╼ #host -t mx hsploit.com
hsploit.com mail is handled by 10 _dc-mx.44dfb54f72ef.hsploit.com.
┌─[root@redteam-vmwarevirtualplatform]─[/home/redteam/Desktop]
└──╼ #
```

Fig. 7: host mail server enumeration filtered output

With the above script an intruder is able to gather information concerning the mail server used by the hsploit domain as for the above scenario, the mail server is **_dx-mx.44df54f72ef.hsploit.com.**

D. Domain Name System(DNS) Enumeration using nslookup scripts

In Linux, a tool called nslookup (name server lookup) is used to perform DNS lookups. It is used to display DNS information, such as a domain's NS servers, MX records, or the IP address of a specific computer.

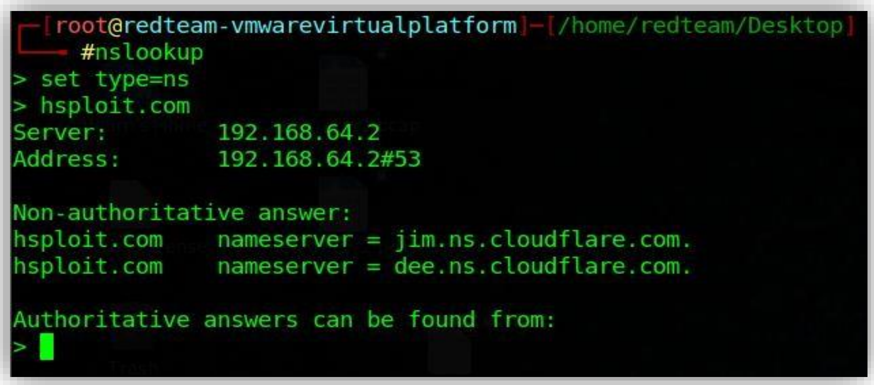


```
┌─[root@redteam-vmwarevirtualplatform]─[/home/redteam/Desktop]
└──╼ #nslookup hsploit.com
Server:         192.168.64.2
Address:        192.168.64.2#53

Non-authoritative answer:
Name:   hsploit.com
Address: 104.21.38.165
Name:   hsploit.com
Address: 172.67.136.119
Name:   hsploit.com
Address: 2606:4700:3033::6815:26a5
Name:   hsploit.com
Address: 2606:4700:3035::ac43:8877

┌─[root@redteam-vmwarevirtualplatform]─[/home/redteam/Desktop]
└──╼ #
```

Fig. 8: nslookup enumeration result

Nslookup can scan Internet domain name servers. The two modes of Nslookup are interactive and non-interactive. The user can print a list of hosts in a domain or query name servers for details about different hosts and domains while in interactive mode. For a host or domain, non-interactive mode is used to output only the name and the requested details.

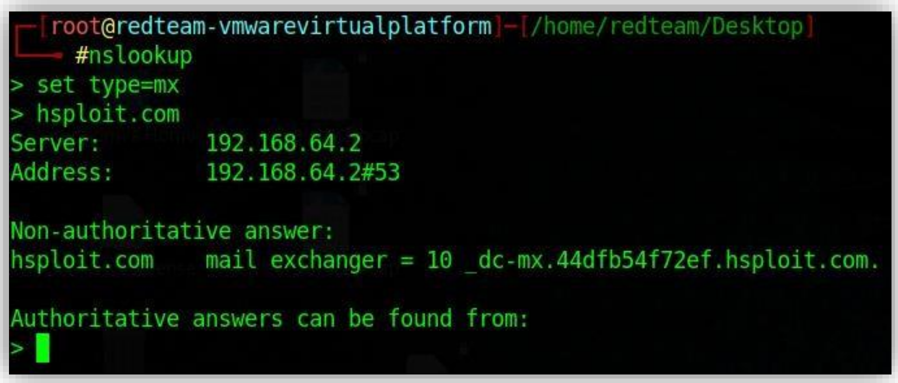
While executing the above script an intruder is able to collect ipv4 and ipv6 public internet protocol used by the target.



```
┌─[root@redteam-vmwarevirtualplatform]─[/home/redteam/Desktop]
└──╼ #nslookup
> set type=ns
> hsploit.com
Server:         192.168.64.2
Address:        192.168.64.2#53

Non-authoritative answer:
hsploit.com     nameserver = jim.ns.cloudflare.com.
hsploit.com     nameserver = dee.ns.cloudflare.com.

Authoritative answers can be found from:
> 
```

Fig. 9: nslookup name server enumeration result

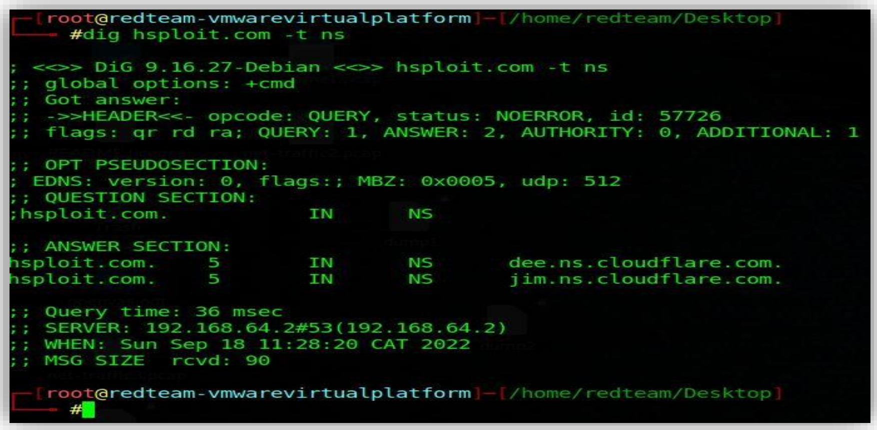
Using the above script an intruder will be able to gather name server associated to the target.



```
┌─[root@redteam-vmwarevirtualplatform]─[/home/redteam/Desktop]
└──╼ #nslookup
> set type=mx
> hsploit.com
Server:         192.168.64.2
Address:        192.168.64.2#53

Non-authoritative answer:
hsploit.com     mail exchanger = 10 _dc-mx.44dfb54f72ef.hsploit.com.

Authoritative answers can be found from:
> 
```

Fig. 10: nslookup mail server enumeration result

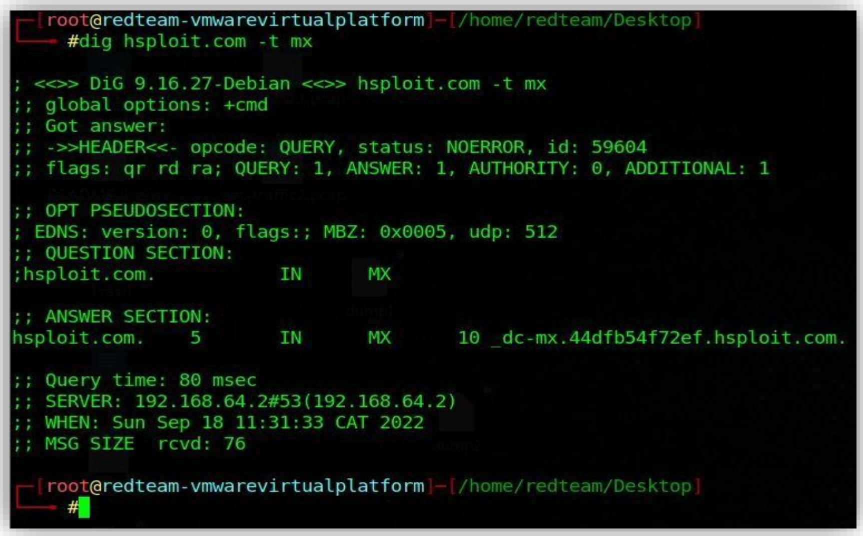
Using the above script, an intruder is capable of collecting mail server used by the target. **Domain Name System(DNS) Enumeration using dig script** dig command stands for Domain Information Groper. It is used to gather information regarding DNS name servers. Basically, network administrators use it. It is used to carry out DNS lookups as well as to check and debug DNS issues.



```
┌─[root@redteam-vmwarevirtualplatform]─[/home/redteam/Desktop]
└──╼ #dig hsploit.com -t ns

; <<>> DiG 9.16.27-Debian <<>> hsploit.com -t ns
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 57726
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; MBZ: 0x0005, udp: 512
;; QUESTION SECTION:
;hsploit.com.                   IN      NS

;; ANSWER SECTION:
hsploit.com.    5       IN      NS      dee.ns.cloudflare.com.
hsploit.com.    5       IN      NS      jim.ns.cloudflare.com.

;; Query time: 36 msec
;; SERVER: 192.168.64.2#53(192.168.64.2)
;; WHEN: Sun Sep 18 11:28:20 CAT 2022
;; MSG SIZE  rcvd: 90

┌─[root@redteam-vmwarevirtualplatform]─[/home/redteam/Desktop]
└──╼ #
```

Fig. 11: dig enumeration result

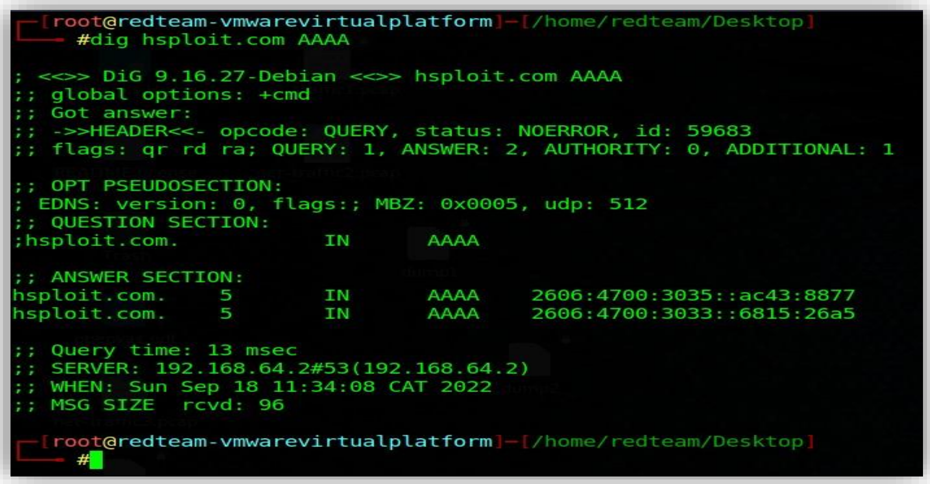
Using the above script, an intruder is able to gather name server information about the target.



```
┌─[root@redteam-vmwarevirtualplatform]─[/home/redteam/Desktop]
└──╼ #dig hsploit.com -t mx

; <<>> DiG 9.16.27-Debian <<>> hsploit.com -t mx
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 59604
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; MBZ: 0x0005, udp: 512
;; QUESTION SECTION:
;hsploit.com.                   IN      MX

;; ANSWER SECTION:
hsploit.com.    5       IN      MX      10 _dc-mx.44dfb54f72ef.hsploit.com.

;; Query time: 80 msec
;; SERVER: 192.168.64.2#53(192.168.64.2)
;; WHEN: Sun Sep 18 11:31:33 CAT 2022
;; MSG SIZE  rcvd: 76

┌─[root@redteam-vmwarevirtualplatform]─[/home/redteam/Desktop]
└──╼ #
```

Fig. 12: dig mail server enumeration result

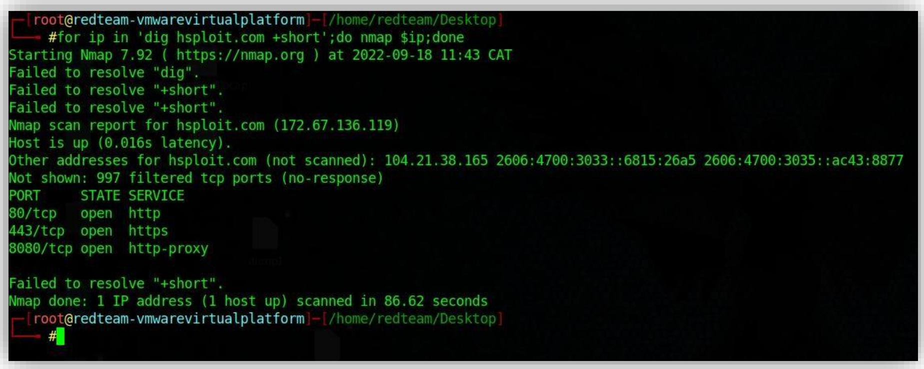
Using the above script, an intruder is able to collect mail server information about the target.



```
┌─[root@redteam-vmwarevirtualplatform]─[/home/redteam/Desktop]
└──╼ #dig hsploit.com AAAA

; <<>> DiG 9.16.27-Debian <<>> hsploit.com AAAA
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 59683
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; MBZ: 0x0005, udp: 512
;; QUESTION SECTION:
;hsploit.com.                   IN      AAAA

;; ANSWER SECTION:
hsploit.com.    5       IN      AAAA    2606:4700:3035::ac43:8877
hsploit.com.    5       IN      AAAA    2606:4700:3033::6815:26a5

;; Query time: 13 msec
;; SERVER: 192.168.64.2#53(192.168.64.2)
;; WHEN: Sun Sep 18 11:34:08 CAT 2022
;; MSG SIZE  rcvd: 96

┌─[root@redteam-vmwarevirtualplatform]─[/home/redteam/Desktop]
└──╼ #
```

Fig. 13: dig Authentication, Authorization Accounting and Auditing enumeration result

Using the above script, an intruder is able to collect dns server ip address, authentication, authorization, accounting and auditing (AAAA) info and ipv6 address used by the target if any available.



```
┌─[root@redteam-vmwarevirtualplatform]─[/home/redteam/Desktop]
└──╼ #for ip in 'dig hsploit.com +short';do nmap $ip;done
Starting Nmap 7.92 ( https://nmap.org ) at 2022-09-18 11:43 CAT
Failed to resolve "dig".
Failed to resolve "+short".
Failed to resolve "+short".
Nmap scan report for hsploit.com (172.67.136.119)
Host is up (0.016s latency).
Other addresses for hsploit.com (not scanned): 104.21.38.165 2606:4700:3033::6815:26a5 2606:4700:3035::ac43:8877
Not shown: 997 filtered tcp ports (no-response)
PORT     STATE SERVICE
80/tcp   open  http
443/tcp  open  https
8080/tcp open  http-proxy

Failed to resolve "+short".
Nmap done: 1 IP address (1 host up) scanned in 86.62 seconds
┌─[root@redteam-vmwarevirtualplatform]─[/home/redteam/Desktop]
└──╼ #
```

Fig. 14: dig combined with nmap schedule with python script output

Using the above script, an intruder is able to gather detailed info about the target such as the public ip address (ipv4 and ipv6), the open port of the target and it's running service.

VIII. FOOTPRINTING

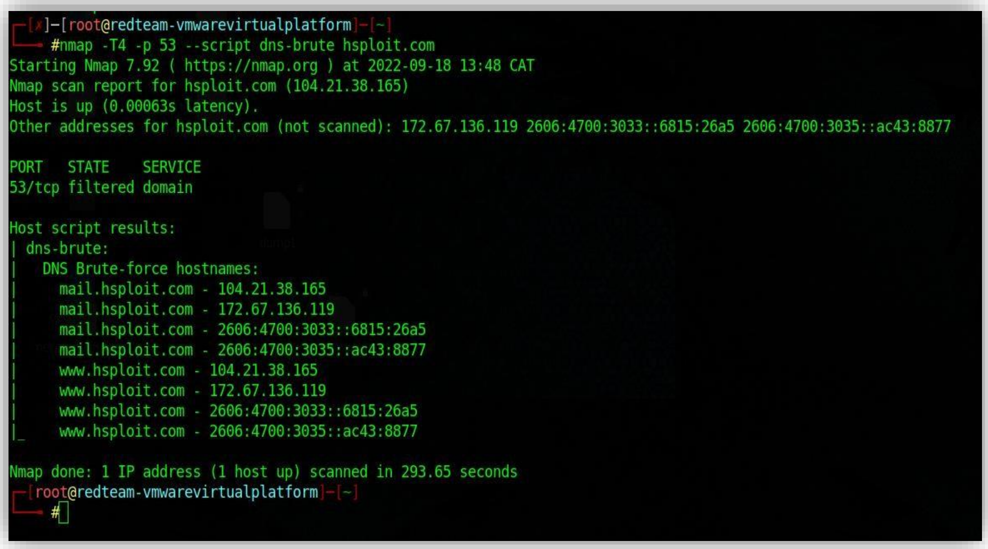
Footprinting is the process of obtaining data on a target system that can be utilized to carry out an effective cyberattack. An intruder might employ multiple techniques and a variety of tools to obtain this information. This data is the intruder's initial step toward breaking a system. Footprinting comes in two varieties, which are listed below.

- Active Footprinting: To perform active footprinting, you must physically interact with the target machine.
- Passive Footprinting: Gathering data on a system that is far away from the attacker is referred to as passive footprinting.

A. *Footprinting using Nmap*

Nmap (short for "Network Mapper") is an open source tool for network exploration and security audits. Although it functions perfectly against a single host, it was created to quickly scan huge networks. To distinguish which has been display 5 on the arrange, what services application title and form that are advertised, what working systems and OS forms they are running, what sorts of bundle filters/firewalls are in utilize, and handfuls of other characteristics, Nmap utilizes novel procedures that utilize crude IP parcels.

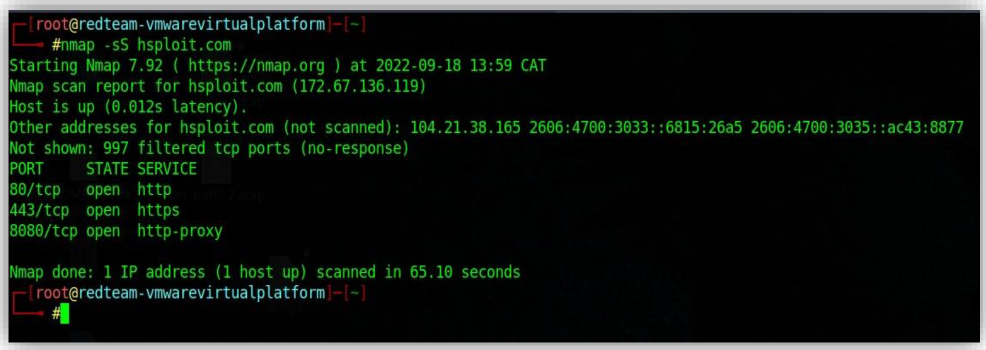
Nmap is frequently employed for security assessments, but many system and network administrators also find it useful for daily chores like network inventory, scheduling service upgrades, and keeping track of host or service uptime.



```
┌─[✗]─[root@redteam-vmwarevirtualplatform]─[~]
└──╼ #nmap -T4 -p 53 --script dns-brute hsploit.com
Starting Nmap 7.92 ( https://nmap.org ) at 2022-09-18 13:48 CAT
Nmap scan report for hsploit.com (104.21.38.165)
Host is up (0.00063s latency).
Other addresses for hsploit.com (not scanned): 172.67.136.119 2606:4700:3033::6815:26a5 2606:4700:3035::ac43:8877

PORT   STATE    SERVICE
53/tcp filtered domain

Host script results:
| dns-brute:
|   DNS Brute-force hostnames:
|     mail.hsploit.com - 104.21.38.165
|     mail.hsploit.com - 172.67.136.119
|     mail.hsploit.com - 2606:4700:3033::6815:26a5
|     mail.hsploit.com - 2606:4700:3035::ac43:8877
|     www.hsploit.com - 104.21.38.165
|     www.hsploit.com - 172.67.136.119
|     www.hsploit.com - 2606:4700:3033::6815:26a5
|_    www.hsploit.com - 2606:4700:3035::ac43:8877

Nmap done: 1 IP address (1 host up) scanned in 293.65 seconds
┌─[root@redteam-vmwarevirtualplatform]─[~]
└──╼ #
```

Fig. 15: Nmap dns-brute forcing script output result

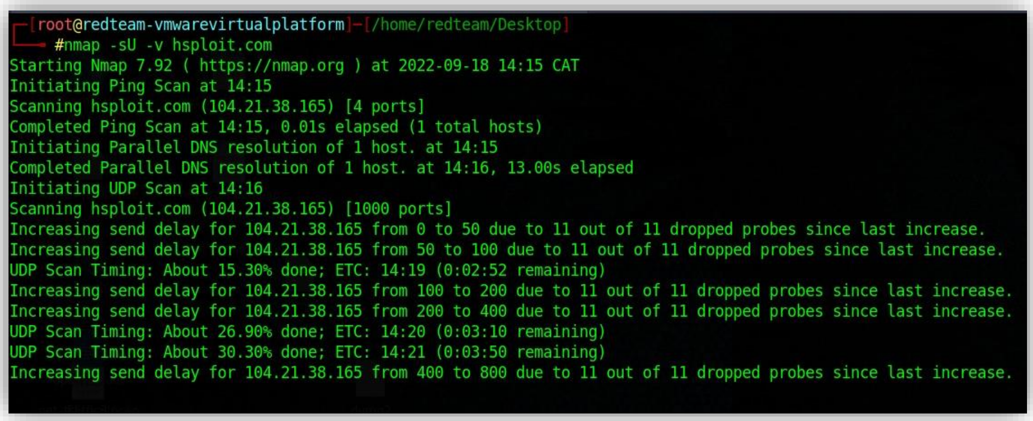
Using the above dns brute forcing script, an intruder is capable of capturing detailed info about the target such as mail server and its public ip address and also the domain name and its associated public ip address either ipv4 or ipv6.



```
┌─[root@redteam-vmwarevirtualplatform]─[~]
└──╼ #nmap -sS hsploit.com
Starting Nmap 7.92 ( https://nmap.org ) at 2022-09-18 13:59 CAT
Nmap scan report for hsploit.com (172.67.136.119)
Host is up (0.012s latency).
Other addresses for hsploit.com (not scanned): 104.21.38.165 2606:4700:3033::6815:26a5 2606:4700:3035::ac43:8877
Not shown: 997 filtered tcp ports (no-response)
PORT     STATE SERVICE
80/tcp   open  http
443/tcp  open  https
8080/tcp open  http-proxy

Nmap done: 1 IP address (1 host up) scanned in 65.10 seconds
┌─[root@redteam-vmwarevirtualplatform]─[~]
└──╼ #
```

Fig. 16: Nmap open port capturing output

Using the above script command, an intruder is capable of gathering some info about the target such as open ports and its running service, public ip addresses assigned to the targeted domain either ipv4 or ipv6.

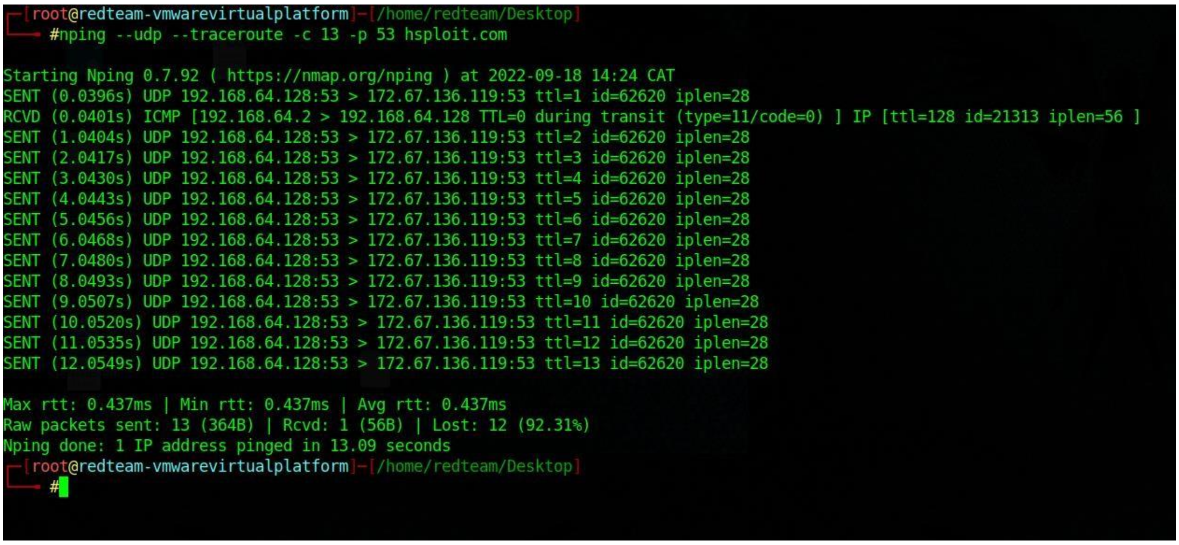


```
┌─[root@redteam-vmwarevirtualplatform]─[/home/redteam/Desktop]
└──╼ #nmap -sU -v hsploit.com
Starting Nmap 7.92 ( https://nmap.org ) at 2022-09-18 14:15 CAT
Initiating Ping Scan at 14:15
Scanning hsploit.com (104.21.38.165) [4 ports]
Completed Ping Scan at 14:15, 0.01s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 14:15
Completed Parallel DNS resolution of 1 host. at 14:16, 13.00s elapsed
Initiating UDP Scan at 14:16
Scanning hsploit.com (104.21.38.165) [1000 ports]
Increasing send delay for 104.21.38.165 from 0 to 50 due to 11 out of 11 dropped probes since last increase.
Increasing send delay for 104.21.38.165 from 50 to 100 due to 11 out of 11 dropped probes since last increase.
UDP Scan Timing: About 15.30% done; ETC: 14:19 (0:02:52 remaining)
Increasing send delay for 104.21.38.165 from 100 to 200 due to 11 out of 11 dropped probes since last increase.
Increasing send delay for 104.21.38.165 from 200 to 400 due to 11 out of 11 dropped probes since last increase.
UDP Scan Timing: About 26.90% done; ETC: 14:20 (0:03:10 remaining)
UDP Scan Timing: About 30.30% done; ETC: 14:21 (0:03:50 remaining)
Increasing send delay for 104.21.38.165 from 400 to 800 due to 11 out of 11 dropped probes since last increase.
```

Fig. 17: Nmap UDP deep scanning result

Using the above script command, the intruder is able to scan and gather all user datagram protocol (UDP) information about the target.Depending on the options used, Nmap display a list of scanned targets with additional information for each. The "interesting ports table" is essential among that data. The port number, protocol, service name, and state are listed in that table. The status can be unfiltered, closed, filtered, or open.

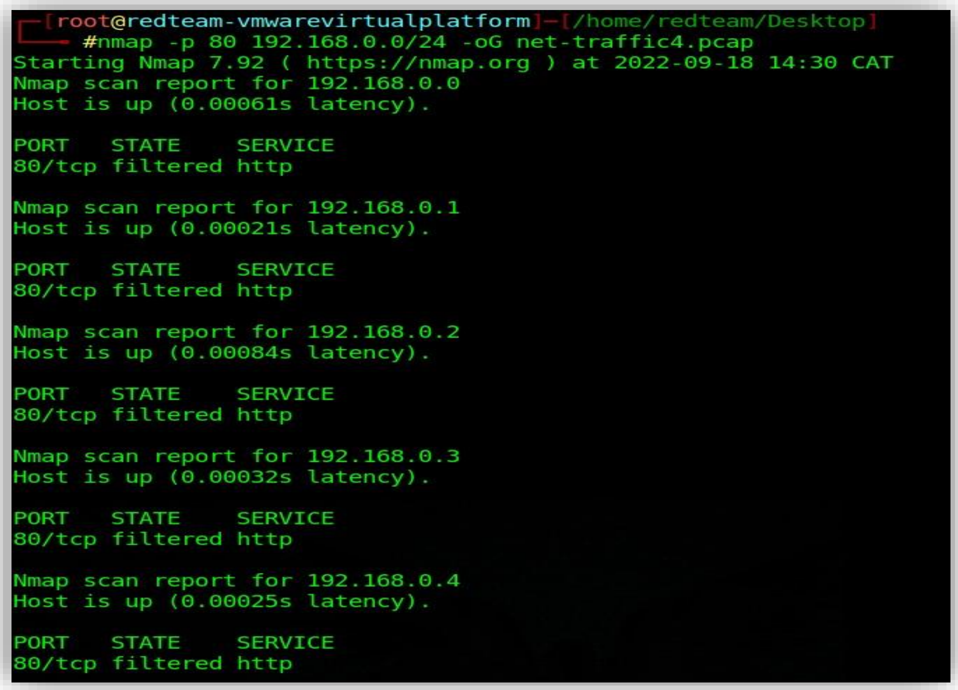
Open denotes the presence of a target computer application that is monitoring that port for connections or packets. Filtered describes a port that is being blocked by a firewall, filter, or other network barrier, making it impossible for Nmap to determine whether it is open or closed. Closed ports are not currently being used by any applications, but they might do so in the future. Unfiltered ports are categorized.



```
┌─[root@redteam-vmwarevirtualplatform]─[/home/redteam/Desktop]
└──╼ #nping --udp --traceroute -c 13 -p 53 hsploit.com

Starting Nping 0.7.92 ( https://nmap.org/nping ) at 2022-09-18 14:24 CAT
SENT (0.0396s) UDP 192.168.64.128:53 > 172.67.136.119:53 ttl=1 id=62620 iplen=28
RCVD (0.0401s) ICMP [192.168.64.2 > 192.168.64.128 TTL=0 during transit (type=11/code=0) ] IP [ttl=128 id=21313 iplen=56 ]
SENT (1.0404s) UDP 192.168.64.128:53 > 172.67.136.119:53 ttl=2 id=62620 iplen=28
SENT (2.0417s) UDP 192.168.64.128:53 > 172.67.136.119:53 ttl=3 id=62620 iplen=28
SENT (3.0430s) UDP 192.168.64.128:53 > 172.67.136.119:53 ttl=4 id=62620 iplen=28
SENT (4.0443s) UDP 192.168.64.128:53 > 172.67.136.119:53 ttl=5 id=62620 iplen=28
SENT (5.0456s) UDP 192.168.64.128:53 > 172.67.136.119:53 ttl=6 id=62620 iplen=28
SENT (6.0468s) UDP 192.168.64.128:53 > 172.67.136.119:53 ttl=7 id=62620 iplen=28
SENT (7.0480s) UDP 192.168.64.128:53 > 172.67.136.119:53 ttl=8 id=62620 iplen=28
SENT (8.0493s) UDP 192.168.64.128:53 > 172.67.136.119:53 ttl=9 id=62620 iplen=28
SENT (9.0507s) UDP 192.168.64.128:53 > 172.67.136.119:53 ttl=10 id=62620 iplen=28
SENT (10.0520s) UDP 192.168.64.128:53 > 172.67.136.119:53 ttl=11 id=62620 iplen=28
SENT (11.0535s) UDP 192.168.64.128:53 > 172.67.136.119:53 ttl=12 id=62620 iplen=28
SENT (12.0549s) UDP 192.168.64.128:53 > 172.67.136.119:53 ttl=13 id=62620 iplen=28

Max rtt: 0.437ms | Min rtt: 0.437ms | Avg rtt: 0.437ms
Raw packets sent: 13 (364B) | Rcvd: 1 (56B) | Lost: 12 (92.31%)
Nping done: 1 IP address pinged in 13.09 seconds
┌─[root@redteam-vmwarevirtualplatform]─[/home/redteam/Desktop]
└──╼ #
```

Fig. 18: Nmap UDP TTL result

Using the above script command, an intruder is able to scan a collect other related user datagram time to live (ttl) info about the target that can help while performing an intrusion.



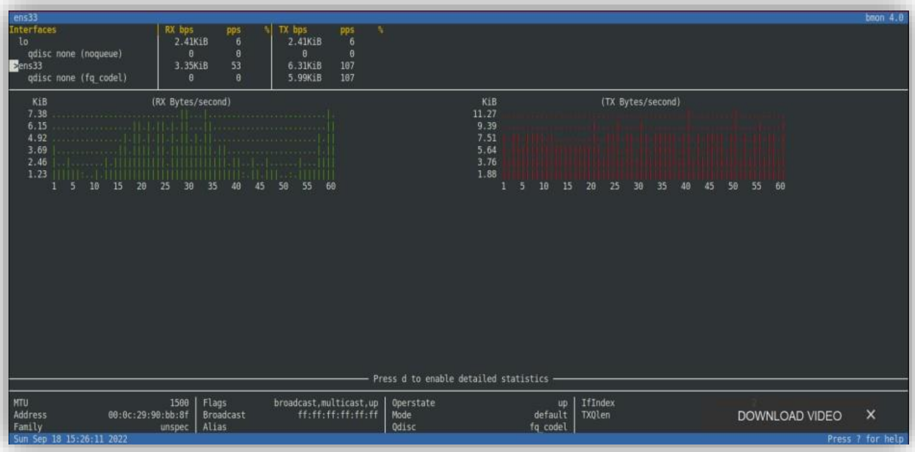
```
┌─[root@redteam-vmwarevirtualplatform]─[/home/redteam/Desktop]
└──╼ #nmap -p 80 192.168.0.0/24 -oG net-traffic4.pcap
Starting Nmap 7.92 ( https://nmap.org ) at 2022-09-18 14:30 CAT
Nmap scan report for 192.168.0.0
Host is up (0.00061s latency).

PORT   STATE    SERVICE
80/tcp filtered http

Nmap scan report for 192.168.0.1
Host is up (0.00021s latency).

PORT   STATE    SERVICE
80/tcp filtered http

Nmap scan report for 192.168.0.2
Host is up (0.00084s latency).

PORT   STATE    SERVICE
80/tcp filtered http

Nmap scan report for 192.168.0.3
Host is up (0.00032s latency).

PORT   STATE    SERVICE
80/tcp filtered http

Nmap scan report for 192.168.0.4
Host is up (0.00025s latency).

PORT   STATE    SERVICE
80/tcp filtered http
```

Fig. 19: Nmap port 80 scanning result

Using the above script, an intruder aims to gather information to insure it the hypertext transfer protocol is up as it is one of vulnerable protocol if it is up an intruder can be using it to perform an exploit such as sql injection, cross site scripting and much more attacks due to the vulnerable port opened.

B. *Network traffic monitoring using bmon*

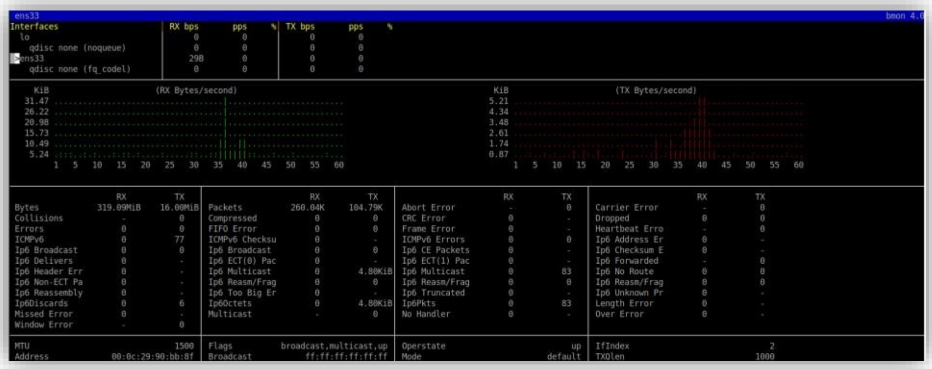
With bmon command, an intruder can be able to capture traffic statistics by the chosen/used interface either incoming or outgoing traffic (upload or downloads) as shown below:



```
ens33                                                                  bmon 4.0
Interfaces                 │ RX bps      pps    %│ TX bps      pps    %
  lo                       │   2.41KiB     6     │   2.41KiB     6
    qdisc none (noqueue)   │      0        0     │      0        0
>ens33                     │   3.35KiB    53     │   6.31KiB   107
    qdisc none (fq_codel)  │      0        0     │   5.99KiB   107
```

```
──────────────── Press d to enable detailed statistics ────────────────
MTU                  1500 │ Flags       broadcast,multicast,up │ Operstate          up │ IfIndex
Address 00:0c:29:90:bb:8f │ Broadcast    ff:ff:ff:ff:ff:ff     │ Mode          default │ TXQlen
Family             unspec │ Alias                              │ Qdisc        fq_codel │
Sun Sep 18 15:26:11 2022                                                  Press ? for help
```

Fig. 20: Bmon network monitoring result1



```
ens33                                                                          bmon 4.0
Interfaces                 RX bps       pps     %  TX bps       pps     %
  lo                            0         0             0         0
    qdisc none (noqueue)        0         0             0         0
>ens33                        29B         0             0         0
    qdisc none (fq_codel)       0         0             0         0

     KiB                   (RX Bytes/second)                               KiB                   (TX Bytes/second)
   31.47                                                                   5.21
   26.22                                                                   4.34
   20.98                                                                   3.48
   15.73                                                                   2.61
   10.49                                                                   1.74
    5.24                                                                   0.87
         1   5   10   15   20   25   30   35   40   45   50   55   60             1   5   10   15   20   25   30   35   40   45   50   55   60

                      RX          TX                       RX          TX                          RX          TX                          RX          TX
Bytes          319.09MiB    16.00MiB | Packets        260.04K     104.79K | Abort Error            -           0 | Carrier Error          -           0
Collisions             -           0 | Compressed           0           0 | CRC Error              0           - | Dropped                0           0
Errors                 0           0 | FIFO Error           0           0 | Frame Error            0           - | Heartbeat Erro         -           0
ICMPv6                 0          77 | ICMPv6 Checksu       0           - | ICMPv6 Errors          0           0 | Ip6 Address Er         0           -
Ip6 Broadcast          0           0 | Ip6 Broadcast        0           0 | Ip6 CE Packets         0           - | Ip6 Checksum E         0           -
Ip6 Delivers           0           - | Ip6 ECT(0) Pac       0           - | Ip6 ECT(1) Pac         0           - | Ip6 Forwarded          -           0
Ip6 Header Err         0           - | Ip6 Multicast        0     4.80KiB | Ip6 Multicast          0          83 | Ip6 No Route           0           0
Ip6 Non-ECT Pa         0           - | Ip6 Reasm/Frag       0           0 | Ip6 Reasm/Frag         0           0 | Ip6 Reasm/Frag         0           0
Ip6 Reassembly         0           - | Ip6 Too Big Er       0           - | Ip6 Truncated          0           - | Ip6 Unknown Pr         0           -
Ip6Discards            0           6 | Ip6Octets            0     4.80KiB | Ip6Pkts                0          83 | Length Error           0           -
Missed Error           0           - | Multicast            -           0 | No Handler             0           - | Over Error             0           -
Window Error           -           0 |                                    |                                     |

MTU                             1500 | Flags     broadcast,multicast,up | Operstate                       up | IfIndex                         2
Address            00:0c:29:90:bb:8f | Broadcast      ff:ff:ff:ff:ff:ff | Mode                       default | TXQlen                       1000
```

Fig. 21: Bmon network monitoring result2

IX. NETWORK FINGERPRINTING WITH MATLEGO

Fingerprinting is a penetration testing technique used to collect as much configuration information about a system as possible. A fingerprint may contain information such as application software technology, network topology, cluster architecture, host OS platform, and database version. Fingerprinting entails scanning network traffic and outgoing packets from target systems, as well as sending custom packets to the target network. The goal of such malicious actions is typically to obtain the target system's response in the form of a digital signature.

The digital signature contains critical information that can be used to map out the ecosystem's infrastructure, services, and network components, allowing the intruder to better assess the system's security posture.Maltego is an open-source intelligence and forensics software.

Maltego is an open source intelligence and graphical link analysis tool for gathering and connecting information for investigative tasks. Maltego is used by a broad range of users, ranging from security professionals to forensic investigators and researchers. Open source intelligence (OSINT) is the act of gathering and analyzing publicly available data for intelligence purposes. Below here are the findings obtained from maltego:

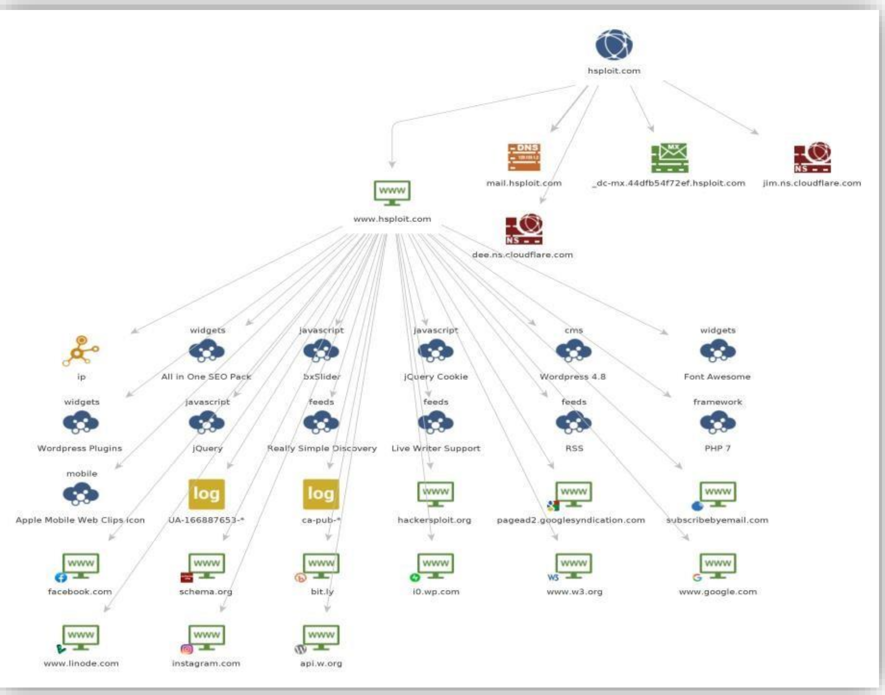


Fig. 22: hsploit network fingerprinting with maltego output

Maltego is an example which uses Open Source Intelligence (OSINT) to gather information. Maltego, is an open source insights and forensics application and appears how data is associated to each other. Another advantage of this device is that the relationship between different sorts of data can provide distant much better higher picture on how they are interlinked and can moreover offer assistance in recognizing obscure relationship.

X. CONCLUSION

Though cybersecurity and its prerequisite risk is a technical challenge, there's a need of knowledge transfer from expert to beginners and also awareness policy matters as it boosts and build enough capacity to users and when users are trained they can't commit harms to their organization's infrastructure as they will be aware of the risk behind or the impact that can be caused by that action.

Technology or internet can't work alone as there's a need of institution's or people's data privacy and security due to that it involves the need of cybersecurity in order to ensure data protection and privacy. As in today's world, the use of internet increased it automatically increased cybersecurity needs in organizations which also impact on the need of expert in cybersecurity, so due to that empowering people with knowledge yes is necessary but also even introducing end users at least with a basic of cybersecurity and how it can be used to fight against cyber threats and terrorism. Knowledge transfer is the key and can be a better solution to deliver.

MINICT and its affiliated agencies implemented laws, policies and regulations regarding cybersecurity whereby they have tried to secure their infrastructure in a way that all their open system interconnection model network layer is secured and they have also 24/7 implemented system security monitoring solutions as it alerts whenever any harmful packet captured so that system security personnel can respond accordingly.

MINICT has a cybersecurity team whereby they daily monitor, evaluate and pentest their entire IT infrastructure in order to fix any loopholes that may be available before being used by the intruder while exploiting their organization's infrastructure or systems.

Even though MINICT did their best to secure their IT infrastructure and ensure data privacy and protection, it's not enough as they need improvement for them to be so sure that they are safe and secure they need to empower their end users with cybersecurity basic needs as they're the one to whom intruders can use in order to penetrate and exploit your organization through several used attacks such as phishing, social engineering and much more due to that there's a need to have end users awareness concerning cybersecurity basic need, this result in having a safer infrastructure environment.

XI. RECOMMENDATION

No matter the size, kind, or industry of the organization, cyber security must be given top priority because it has been on the rise recently. The COVID-19 epidemic, which made people and businesses more vulnerable, was also used by malicious actors. Businesses had to stretch the limits of their corporate networks during the epidemic because employees were compelled to use remote working options, which was bad for information security. Because the way we utilize technology in our daily lives is constantly evolving, cyber threats become more critical. Our ability to safeguard ourselves from cyber threats will get harder as networks get much more complicated.

Cybercriminals will continue to compromise people through hacking techniques while also implementing new technologies to increase the effectiveness and efficiency of their attacks. To prevent cyberattacks and terrorism organizations needs to empower their staff in a way that they could be up to date on the trending cybersecurity technologies therefore, organizations can implement secure infrastructure that will be managed by experts as they will be having enough knowledge to fight against cybercriminals and hacktivist. Implementing this will result in reducing business risk and loss caused by cyber threats, will then increase faith between client or customer and the concerned institution or organization.

REFERENCES

[1.] Aaron Guzman, A. G. (2017). IoT Penetration Testing Cookbook. BIRMINGHAM - MUMBAI: Packt Publishing.

[2.] Bernardita, C. (2022, March 09). Your Modern Business Guide To Data Analysis Methods And Techniques. Retrieved from The datapine Blog: https://www.datapine.com/blog/data-analysis-methods-andtechniques/

[3.] Calzon, B. (2022, March 09). Your Modern Business Guide To Data Analysis Methods And Techniques. Retrieved from datapine: https://www.datapine.com/blog/data-analysis-methods-and-techniques/#dataanalysis-definition

[4.] Charlesworth. (2022, February 25). Conceptual framework vs. Theoretical framework – and constructing each. Retrieved from Charlesworth Author Services: https://www.cwauthors.com/article/conceptualframework-versus-theoretical-framework-in-research

[5.] Dr.Yusuf Perwej. (2022, January 20). A Systematic Literature Review on the Cyber Security. Retrieved from HAL Open Science: https://hal.archives-ouvertes.fr/hal-03509116

[6.] Dudovskiy, J. (2022, January). Observation. Retrieved from Business Research Methodology: https://researchmethodology.net/research-methods/qualitative-research/observation/

[7.] Haupt, H.-G. (2001). Comparative Method : Comparative History. Retrieved from ScienceDirect: https://www.sciencedirect.com/topics/computer-science/comparative-method

[8.] HBS Online. (2022). Business Insights. Retrieved from Business Insights: https://online.hbs.edu/blog/post/datacollection-methods

[9.] IBM. (2022). What is cybersecurity? Retrieved from IBM: https://www.ibm.com/topics/cybersecurity

[10.] Ishaani Priyadarshini, R. S. (2022). Cybersecurity in IoT Infrastructure. In R. S. Ishaani Priyadarshini, Artificial Intelligence and Cybersecurity: Advances and Innovations (p. 223). CRC Press.

[11.] John W. Satzinger, Robert B. Jackson, Stephen D. Burd. (2012). Generalization/Specialization Relationships. In R. B. John W. Satzinger, Systems

Analysis and Design in a Changing World, Sixth Edition (p. 132). Boston, MA 02210: Joe Sabatino.

[12.] Kelley Dempsey, N. S. (2011). Information Security Continuous Monitoring(ISCM) for Federal Information Systems and Organizations. Gaithersburg, MD 20899-893: National Institute of Standards and Technolog.

[13.] Klein, D. (2019, November 07). Using Zero Trust Security to Ease Compliance. Retrieved from Guardicore: https://www.guardicore.com/blog/using-zero-trust-security-model-to-ease-compliance/

[14.] Kothari, C. (2004). Research Mathodology : Objectives of Research. In C. Kothari, Research Mathodology : Methods and Techniques. New Delhi: New Age International Publishers.

[15.] Matthew K. Sharp, K. L. (2022). The CISO Evolution: Business Knowledge for Cybersecurity Executives. Wiley.

[16.] Mrs. Ashwini Sheth, M. S. (2021). RESEARCH PAPER ON CYBER SECURITY. 2-7.

[17.] Nmap. (2022). Nmap: Discover your network. Retrieved from https://nmap.org/

[18.] OWASP Foundation, I. (2022). OWASP Application Security Verification Standard. Retrieved from OWASP: https://owasp.org/www-project-application-security-verification-standard/

[19.] Pagel, M. (2001). Comparative Method, in Evolutionary Studies. Retrieved from ScienceDirect:

[20.] https://www.sciencedirect.com/topics/computer-science/comparative-method

[21.] Paola Velasco. (2021, March 29). Retrieved from NCSI: https://ncsi.ega.ee/country/rw/518/#details RISA. (2015). National Cyber Security Policy. 10-17.

[22.] RW-CSIRT. (2015). THE NATIONAL CYBER SECURITY POLICY. In National Cyber Security Policy. Rwanda Information Society Authority - RISA.

[23.] Turner, D. D. (2020, 01 08). HEADACHE : The jounal of Head and Face Pain. Retrieved from Sampling Methods in Research Design: 3.2 Government of Rwanda

[24.] What Is the MITRE ATT&CK Framework? (2022). Retrieved from Trellix : https://www.trellix.com/en-us/securityawareness/cybersecurity/what-is-mitre-attack-framework.htm