

INTRODUCTION

DNS Harvesting is technique used for getting information of the Domain Name Server by performing various sequences of steps on the target Domain/IP. DNS Harvesting comes under the Footprinting phase of Ethical Hacking. The DNS server contains various kind of information that may helps in performing an attack on that server. The information can be harvested using various tools and utilities where the information related domain registration, personal details of owner, hosting server detail, name servers, mail servers etc. can be fetched. It can also provide location details of the servers.

There are certain records that a typical DNS server maintains

Record Type	Description
A	Points to the host's IP address
MX	Points to domain's mail server
NS	Points to host's name server
CNAME	Canonical naming allows aliases to a host
SDA	Indicate authority for domain
SRV	Service records
PTR	Maps IP address to a hostname
RP	Responsible person
HINFO	Host information record includes CPU type and OS
TXT	Unstructured text records

DNS HARVESTING TOOLS

There are various tools that can be used to harvest information from a DNS server:

1. DIG
2. Host
3. Dnsenum
4. Nslookup

In this Report I used **NSLOOKUP** for performing DNS harvesting.

NSLOOKUP

The Nslookup stands for Name Server Lookup. It is a network administration tool which uses command line interface for executing nslookup commands. Nslookup tool can be found in various operating systems including windows and almost in every linux and unix distributions by default. Nslookup can perform all the required operations in order to retrieve juicy informations from DNS records.

In this Report I used a specific website to perform all the nslookup operations.

TARGET WEBSITE: www.techvertos.com

Let's try to harvest all the record types one by one....

IP ADDRESS LOOKUP

It is used for finding the IP address of the domain name.

COMMAND:

```
>> nslookup techvertos.com
```

OUTPUT:

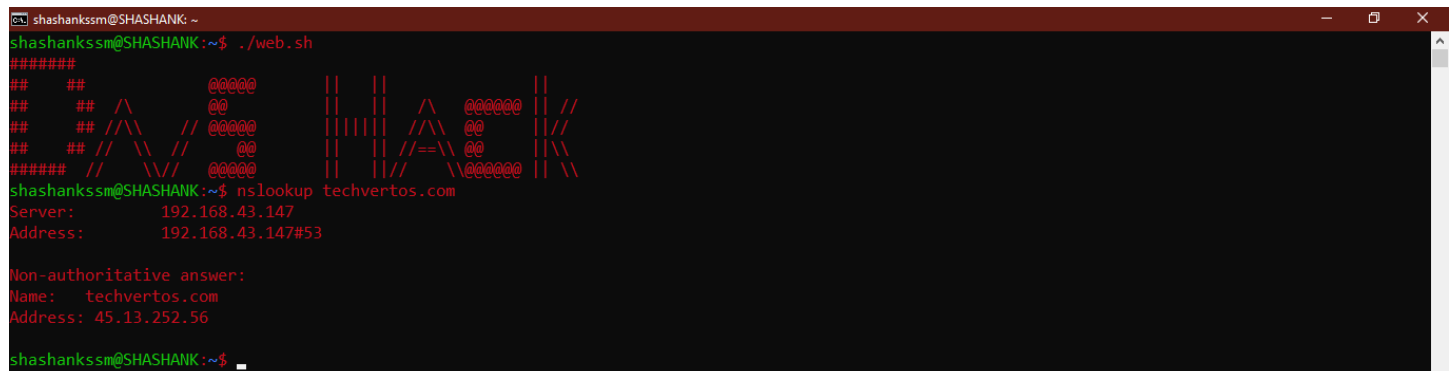
Server: 192.168.43.147

Address: 192.168.43.147#53

Non-authoritative answer:

Name: techvertos.com

Address: 45.13.252.56

A screenshot of a terminal window with a dark background and red text. The window title is 'shashankssm@SHASHANK ~'. The user has entered the command './web.sh' which outputs a large ASCII art logo. Then, the user enters 'nslookup techvertos.com'. The output shows the server IP as 192.168.43.147 and the address as 192.168.43.147#53. Below that, it shows 'Non-authoritative answer:' followed by 'Name: techvertos.com' and 'Address: 45.13.252.56'. The prompt returns to 'shashankssm@SHASHANK:~\$'.

RECORD (A)

It is also used for pointing the IP address of domain name. It is mostly used for switching from multiple records type to the default nslookup command.

COMMAND:

```
>> nslookup  
  
>> set type=a  
  
>> techvertos.com
```

OUTPUT:

```
Server:          192.168.43.147  
Address:         192.168.43.147#53
```

Non-authoritative answer:

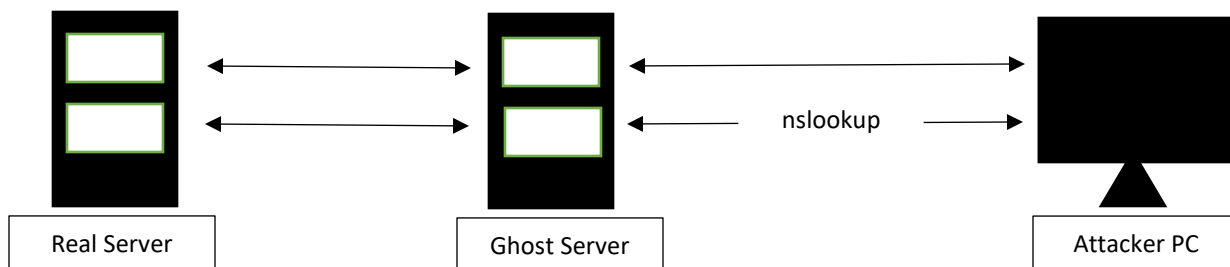
```
Name:   techvertos.com  
Address: 45.13.252.56
```



```
shashankssm@SHASHANK: ~  
shashankssm@SHASHANK:~$ ./web.sh  
#####  
##  ## @@@@@ @@@@ || ||  
##  ## /\ @ @ || || /\ @@@@@ ||  
##  ## // \ // @@@@@ @@@@ ||  
##  ## // \ // @ @ || || // \ @@@@ ||  
##### // \ // @@@@@ @@@@ ||  
shashankssm@SHASHANK:~$ nslookup  
> set type=a  
> techvertos.com  
Server:          192.168.43.147  
Address:         192.168.43.147#53  
  
Non-authoritative answer:  
Name:   techvertos.com  
Address: 45.13.252.56  
>
```

NOTE: In default nslookup and record (A) the output is **Non-authoritative answer**.

Here, **Non-authoritative answer** means that the discovered IP may or may not be the real IP pointing to that domain. It generally happens because there are some protective measures that has been used to avoid the discloser of the server's IP. The discovered IP may be the Ghost server's IP which is used before the real server that behaves as the real server.



RECORD (MX)

It is used for identifying the mail server records. It gives the information about the IP addresses and domain/subdomain names of the mail servers.

COMMAND:

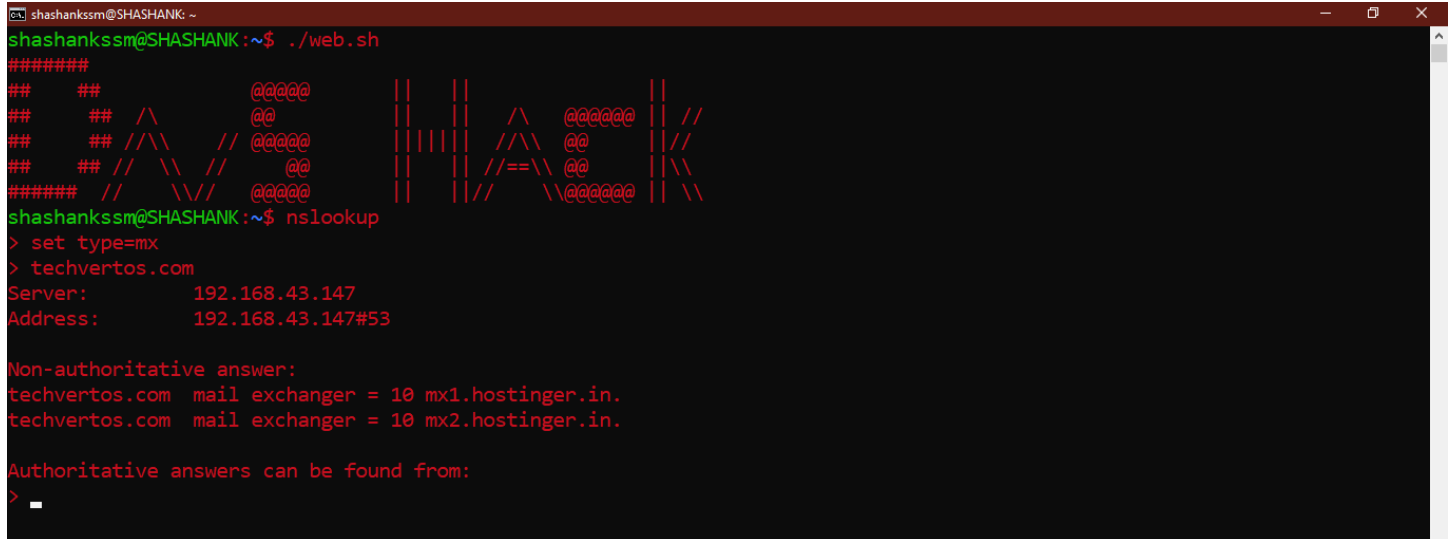
```
>> nslookup  
  
>> set type=mx  
  
>> techvertos.com
```

OUTPUT:

```
Server:          192.168.43.147  
Address:         192.168.43.147#53
```

Non-authoritative answer:

```
techvertos.com  mail exchanger = 10 mx1.hostinger.in.  
techvertos.com  mail exchanger = 10 mx2.hostinger.in.
```



```
shashankssm@SHASHANK: ~$ ./web.sh  
#####  
##      ##      @@@@      ||  ||      ||  
##      ##  /\      @      ||  ||  /\  @@@@@@  ||  
##      ## // \      @@@@@  || || || // \  @      ||  
##      ## //  \      @      ||  ||  // = \  @      ||  
#####  //  \      @@@@@  ||  ||  //  \  @@@@@  ||  
shashankssm@SHASHANK: ~$ nslookup  
> set type=mx  
> techvertos.com  
Server:          192.168.43.147  
Address:         192.168.43.147#53  
  
Non-authoritative answer:  
techvertos.com  mail exchanger = 10 mx1.hostinger.in.  
techvertos.com  mail exchanger = 10 mx2.hostinger.in.  
  
Authoritative answers can be found from:  
> _
```

The respective mail server can be found after performing the above command.

NOTE: Let's assume if we have to affect the mail services of the respective domain then we have to perform the DOS attack on the mail server address instead of the actual domain that can be found using below commands.

COMMAND:

```
>> set type=a
```

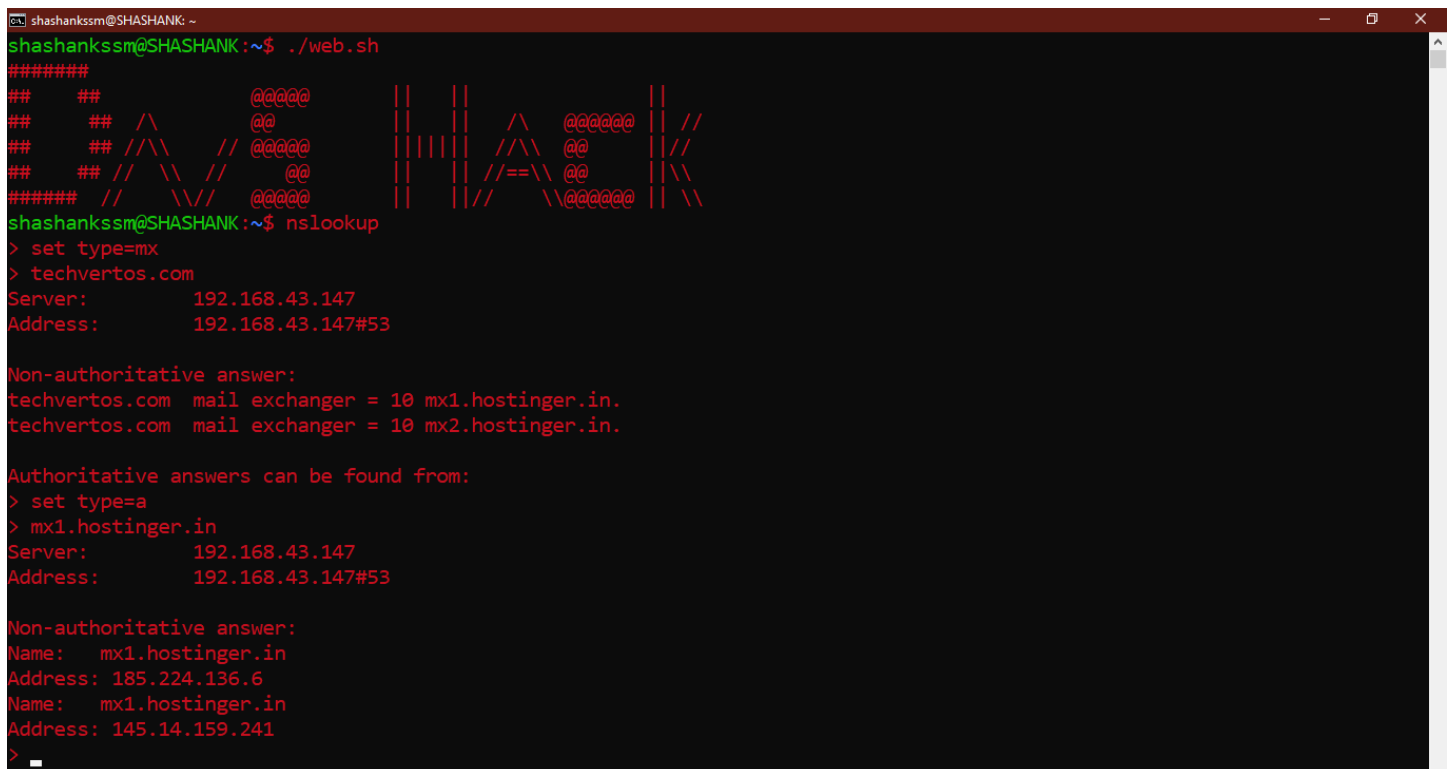
```
>> mx1.hostinger.in
```

OUTPUT:

```
Server:          192.168.43.147
Address:         192.168.43.147#53
```

Non-authoritative answer:

```
Name:   mx1.hostinger.in
Address: 185.224.136.6
Name:   mx1.hostinger.in
Address: 145.14.159.241
```

A screenshot of a terminal window with a dark background and red text. The window title is 'shashankssm@SHASHANK ~'. The user has run './web.sh', which displays a large ASCII art logo for 'SHASHANK' made of '@' and '/' characters. Below the logo, the user runs 'nslookup'. The output shows the results of an nslookup for 'techvertos.com', identifying the mail exchanger as 'mx1.hostinger.in' with IP '192.168.43.147'. Then, the user sets the type to 'a' and looks up 'mx1.hostinger.in', showing its IP address as '192.168.43.147#53'. Finally, the user sets the type to 'ns' and looks up 'mx1.hostinger.in', showing its IP address as '185.224.136.6' and '145.14.159.241'.

```
shashankssm@SHASHANK:~$ ./web.sh
#####
##      ##      @@@@      ||  ||      ||  ||
##      ##  /\      @@      ||  ||  /\  @@@@@@  ||  ||
##      ## // \      // @@@@@  || || || // \  @@  ||  ||
##      ## //  \      //  @@  ||  || //  \  @@  ||  ||
#####  //   \      @@@@@  ||  || //   \  @@@@@  ||  ||
shashankssm@SHASHANK:~$ nslookup
> set type=mx
> techvertos.com
Server:          192.168.43.147
Address:         192.168.43.147#53

Non-authoritative answer:
techvertos.com  mail exchanger = 10 mx1.hostinger.in.
techvertos.com  mail exchanger = 10 mx2.hostinger.in.

Authoritative answers can be found from:
> set type=a
> mx1.hostinger.in
Server:          192.168.43.147
Address:         192.168.43.147#53

Non-authoritative answer:
Name:   mx1.hostinger.in
Address: 185.224.136.6
Name:   mx1.hostinger.in
Address: 145.14.159.241
>
```

RECORD (NS)

It is used for finding the host's name server. These name servers are responsible for handling the website data and name servers are the one which are responsible for mapping the host server with the domain name or the IP address.

COMMAND:

```
>> nslookup
>> set type=ns
```

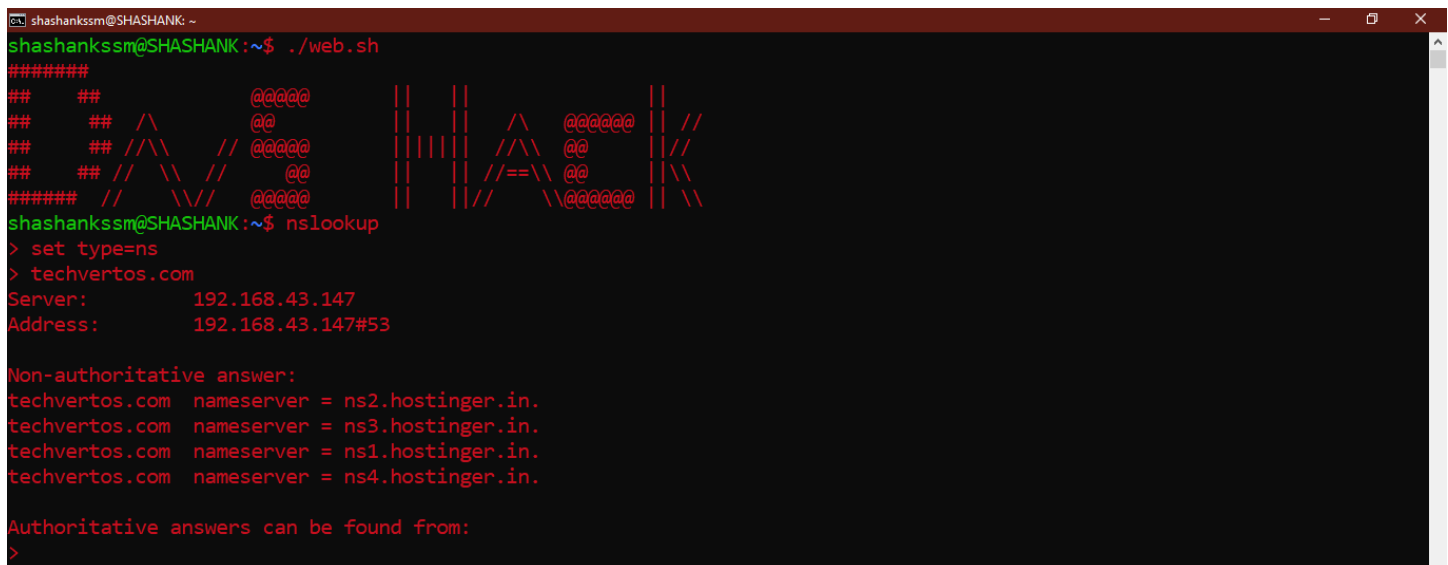
>> techvertos.com

OUTPUT:

Server: 192.168.43.147
Address: 192.168.43.147#53

Non-authoritative answer:

techvertos.com nameserver = ns2.hostinger.in.
techvertos.com nameserver = ns3.hostinger.in.
techvertos.com nameserver = ns1.hostinger.in.
techvertos.com nameserver = ns4.hostinger.in.

A screenshot of a terminal window with a dark background and red text. The window title is 'shashankssm@SHASHANK ~'. The user has run a script './web.sh' which outputs a large ASCII art logo for 'SHASHANK' made of '@' and '/' characters. Below the logo, the user runs 'nslookup'. The output shows the server IP as 192.168.43.147 and the address as 192.168.43.147#53. It also lists non-authoritative nameservers: ns2.hostinger.in, ns3.hostinger.in, ns1.hostinger.in, and ns4.hostinger.in. The prompt '>' is visible at the bottom.

```
shashankssm@SHASHANK:~$ ./web.sh
#####
##      ##      @@@@      ||  ||      ||
##      ##  /\      @@      ||  ||  /\  @@@@@@  ||  //
##      ## // \      // @@@@@  || ||  // \  @@  ||  //
##      ## //  \      //  @      ||  ||  //  = \  @  ||  \
#####  //   \      // @@@@@  ||  ||  //   \  @@@@@  ||  \
shashankssm@SHASHANK:~$ nslookup
> set type=ns
> techvertos.com
Server:      192.168.43.147
Address:     192.168.43.147#53

Non-authoritative answer:
techvertos.com nameserver = ns2.hostinger.in.
techvertos.com nameserver = ns3.hostinger.in.
techvertos.com nameserver = ns1.hostinger.in.
techvertos.com nameserver = ns4.hostinger.in.

Authoritative answers can be found from:
>
```

Let's try to find out some interesting information that can be required to perform an attack on the hosting servers.

COMMAND:

>> set type=a
>> ns2.hostinger.in

OUTPUT:

Server: 192.168.43.147
Address: 192.168.43.147#53

Non-authoritative answer:

Name: ns2.hostinger.in

Address: 31.220.23.1

```
shashankssm@SHASHANK: ~  
shashankssm@SHASHANK:~$ ./web.sh  
#####  
##      ##      @@@@      ||  ||      @@@@      ||  
##      ##  /\      @      ||  ||  /\  @@@@@@  ||  //  
##      ## // \      @@@@      ||  ||  // \  @      ||  //  
##      ## //  \      @      ||  ||  //  = \  @      ||  //  
##### //  \ \  @@@@      ||  ||  //  \ \  @@@@@@  ||  //  
shashankssm@SHASHANK:~$ nslookup  
> set type=ns  
> techvertos.com  
Server:          192.168.43.147  
Address:         192.168.43.147#53  
  
Non-authoritative answer:  
techvertos.com  nameserver = ns2.hostinger.in.  
techvertos.com  nameserver = ns3.hostinger.in.  
techvertos.com  nameserver = ns1.hostinger.in.  
techvertos.com  nameserver = ns4.hostinger.in.  
  
Authoritative answers can be found from:  
> set type=a  
> ns2.hostinger.in  
Server:          192.168.43.147  
Address:         192.168.43.147#53  
  
Non-authoritative answer:  
Name:   ns2.hostinger.in  
Address: 31.220.23.1  
>
```

RECORD (CNAME)

It is used for getting the aliases to the host. CNAME is responsible for getting **Authoritative answer**.

COMMAND:

```
>> nslookup  
>> set type=cname  
>> ns2.hostinger.in
```

OUTPUT:

```
Server:          192.168.43.147  
Address:         192.168.43.147#53
```

Non-authoritative answer:

*** Can't find techvertos.com: No answer

Authoritative answers can be found from:

techvertos.com

origin = ns1.hostinger.in

```
mail addr = dns.hostinger.com

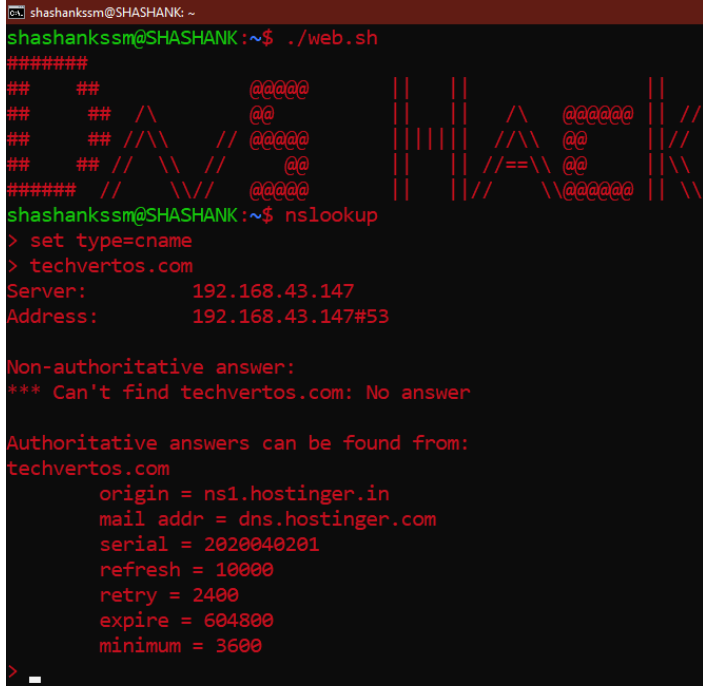
serial = 2020040201

refresh = 10000

retry = 2400

expire = 604800

minimum = 3600
```

A terminal window with a dark background and red text. The window title is 'shashankssm@SHASHANK: ~'. The user runs './web.sh', which displays a ASCII art logo for 'shashankssm@SHASHANK'. Then, the user runs 'nslookup', which shows the default server as 192.168.43.147. The user then sets the type to 'cname' and queries 'techvertos.com'. The output shows a non-authoritative answer from ns1.hostinger.in with the same DNS record details as shown in the first block.

```
shashankssm@SHASHANK: ~$ ./web.sh
#####
##      ##          @@@@          ||  ||
##      ##  /\      @@          ||  ||  /\  @@@@@  ||  //
##      ## //\\    // @@@@@    ||||| //\\  @@      ||  //
##      ## //  \\  //  @@      ||  ||  //==\\  @@      ||  \\
#####  //    \\//  @@@@@    ||  ||//    \\@@@@@  ||  \\

shashankssm@SHASHANK: ~$ nslookup
> set type=cname
> techvertos.com
Server:          192.168.43.147
Address:         192.168.43.147#53

Non-authoritative answer:
*** Can't find techvertos.com: No answer

Authoritative answers can be found from:
techvertos.com
    origin = ns1.hostinger.in
    mail addr = dns.hostinger.com
    serial = 2020040201
    refresh = 10000
    retry = 2400
    expire = 604800
    minimum = 3600
> _
```

Let's find the actual IP of the name server

COMMAND:

```
>> set type=a
>> ns1.hostinger.in
```

OUTPUT:

```
Server:          192.168.43.147
Address:         192.168.43.147#53
```

Non-authoritative answer:

```
Name:    ns1.hostinger.in
Address: 31.170.163.241
```



```
shashankssm@SHASHANK: ~$ nslookup
> set type=cname
> techvertos.com
Server:          192.168.43.147
Address:         192.168.43.147#53

Non-authoritative answer:
*** Can't find techvertos.com: No answer

Authoritative answers can be found from:
techvertos.com
    origin = ns1.hostinger.in
    mail addr = dns.hostinger.com
    serial = 2020040201
    refresh = 10000
    retry = 2400
    expire = 604800
    minimum = 3600
> set type=a
> ns1.hostinger.in
Server:          192.168.43.147
Address:         192.168.43.147#53

Non-authoritative answer:
Name:   ns1.hostinger.in
Address: 31.170.163.241
>
```

RECORD (TXT)

It contains the text records that may or may not be in the human readable form. It contains the record which is kept outside of direct traffic of that domain to the internet.

COMMAND:

```
>> nslookup
>> set type=txt
>> techvertos.com
```

OUTPUT:

```
Server:          192.168.43.147
Address:         192.168.43.147#53
```

Non-authoritative answer:

```
techvertos.com text = "v=spf1 include:spf.mx.hostinger.com
include:relay.mailchannels.net ~all"
```

```

shashankssm@SHASHANK: ~$ ./web.sh
#####
##  ##          @@@@@@  ||  ||          ||
##  ##  /\      @@      ||  ||  /\  @@@@@@  ||  //
##  ##  // \ \  // @@@@@@  || || ||  // \ \  @@  ||  //
##  ##  //  \ \  //  @@      ||  ||  // = \ \  @@  ||  \ \
#####  //   \ \  // @@@@@@  ||  ||  //   \ \ @@@@@@  ||  \ \

shashankssm@SHASHANK:~$ nslookup
> set type=txt
> techvertos.com
Server:         192.168.43.147
Address:        192.168.43.147#53

Non-authoritative answer:
techvertos.com  text = "v=spf1 include:spf.mx.hostinger.com include:relay.mailchannels.net ~all"

Authoritative answers can be found from:
>

```

SUMMARY

After performing all the commands, we have some juicy information about the target www.techvertos.com.

- IP **45.13.252.56**
- Mail servers : **mx1.hostinger.in ; mx2.hostinger.in**
- Name servers : **ns1.hostinger.in ; ns1.hostinger.in ; ns1.hostinger.in ; ns1.hostinger.in**
- Text : **"v=spf1 include:spf.mx.hostinger.com include:relay.mailchannels.net ~all"**

Now we can perform port and vulnerability scanning in order to exploit the web application.

We can also initiate DOS attack on the mail and name servers in order to affect the services running.

The text from TXT records can result in some vital information about any hidden functionality/services of the web application.

REFERENCE

- CEH V9 Book
- Class Notes

```

shashankssm@SHASHANK: ~$ ./web.sh
#####
##  ##          @@@@@@  ||  ||          ||
##  ##  /\      @@      ||  ||  /\  @@@@@@  ||  //
##  ##  // \ \  // @@@@@@  || || ||  // \ \  @@  ||  //
##  ##  //  \ \  //  @@      ||  ||  // = \ \  @@  ||  \ \
#####  //   \ \  // @@@@@@  ||  ||  //   \ \ @@@@@@  ||  \ \

```

THANK YOU !!