

CS-Minor project-MAY

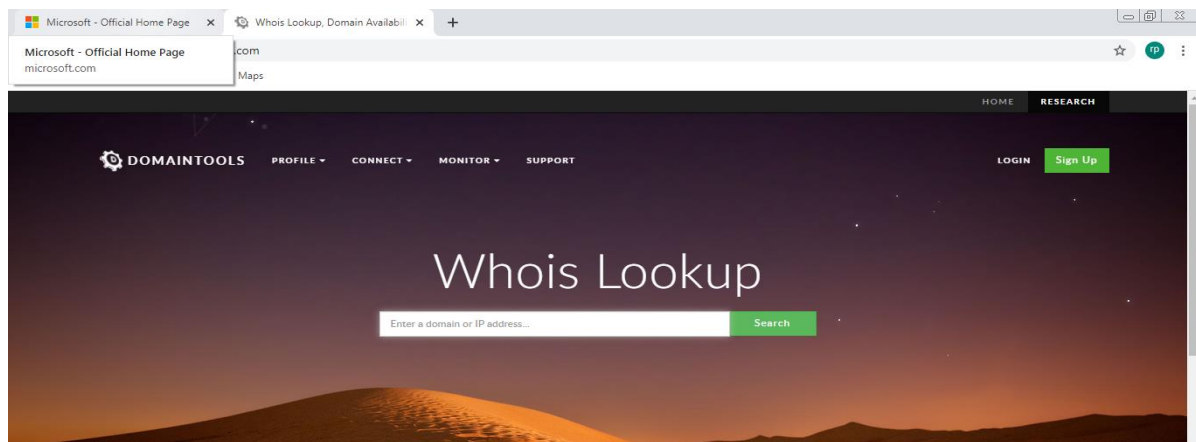
NAME: SRIBANANDA PANDA

TASK 1:

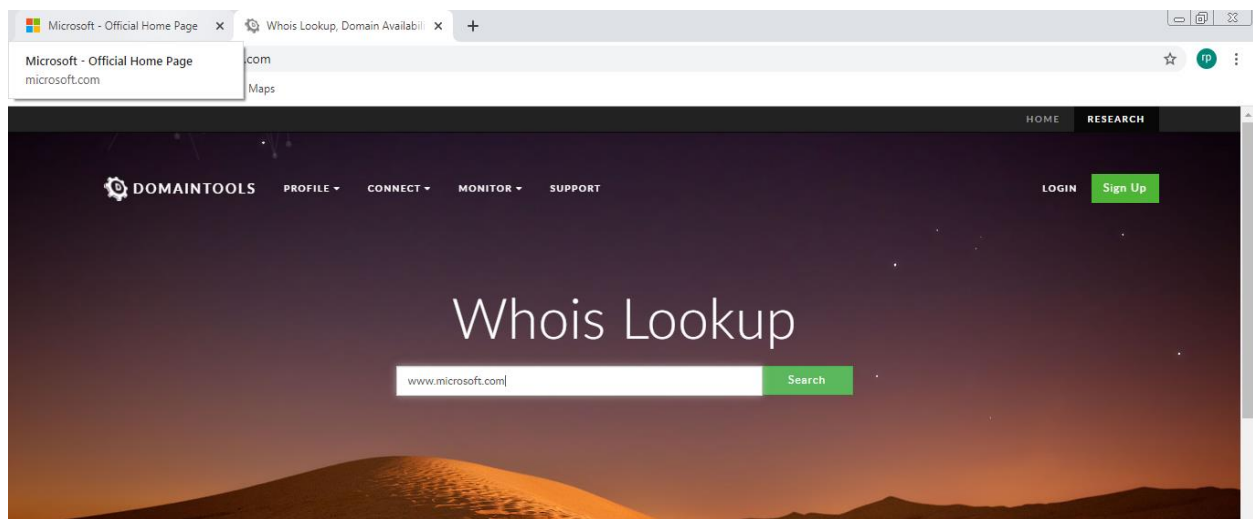
In this task we have to perform foot printing on Microsoft website i.e www.microsoft.com and gather information from that website using various online tools like whois/netcraft/shodan/dnsdumpster/advanced IP scanner etc.

So, first we gather information from whois online tool i.e www.whois.domaintools.com

1.The first step is to open the website by entering the name of the website on the search engine:



2.The second step is to enter the domain name or IP address of the website we want to search for like in this case we have to type www.microsoft.com and then enter the search button :



3. Then the third step is to gather the information present in this website:

Microsoft - Official Home Page x Microsoft.com WHOIS, DNS, & D x +

Microsoft - Official Home Page microsoft.com

com/microsoft.com Maps

DOMAINTOOLS PROFILE CONNECT MONITOR SUPPORT Whois Lookup

Whois Record for Microsoft.com

Domain Profile

Registrant	Domain Administrator	these are the information present in the website.
Registrant Org	Microsoft Corporation	
Registrant Country	us	
Registrar	MarkMonitor, Inc. MarkMonitor Inc. IANA ID: 292 URL: http://www.markmonitor.com Whois Server: whois.markmonitor.com abusecomplaints@markmonitor.com (p) 12083895770	
Registrar Status	clientDeleteProhibited, clientTransferProhibited, clientUpdateProhibited, serverDeleteProhibited, serverTransferProhibited, serverUpdateProhibited	
Dates	11,021 days old Created on 1991-05-01 Expires on 2022-05-02 Updated on 2021-04-07	
Name Servers	NS1-205.AZURE-DNS.COM (has 364,491 domains)	

The information gather from whois.com are as follows:

Registrant Org: Microsoft Corporation

Registrant Country: us

Registrar: MarkMonitor, Inc. MarkMonitor Inc.

IANA ID: 292

URL: http://www.markmonitor.com

Whois Server: whois.markmonitor.com

(p)

Dates: 11,021 days old

Created on 1991-05-01

Expires on 2022-05-02

Updated on 2021-04-07

Name Servers: NS1-205.AZURE-DNS.COM (has 364,491 domains)

NS2-205.AZURE-DNS.NET (has 668 domains)

NS3-205.AZURE-DNS.ORG (has 538 domains)

NS4-205.AZURE-DNS.INFO (has 624 domains)

Tech Contact: MSN Hostmaster

Microsoft Corporation

One Microsoft Way,,

Redmond, WA, 98052, us

msnhst@microsoft.com

(p)14258828080 (f)14259367329

IP Address: 23.54.49.182 - 16 other sites hosted on this server

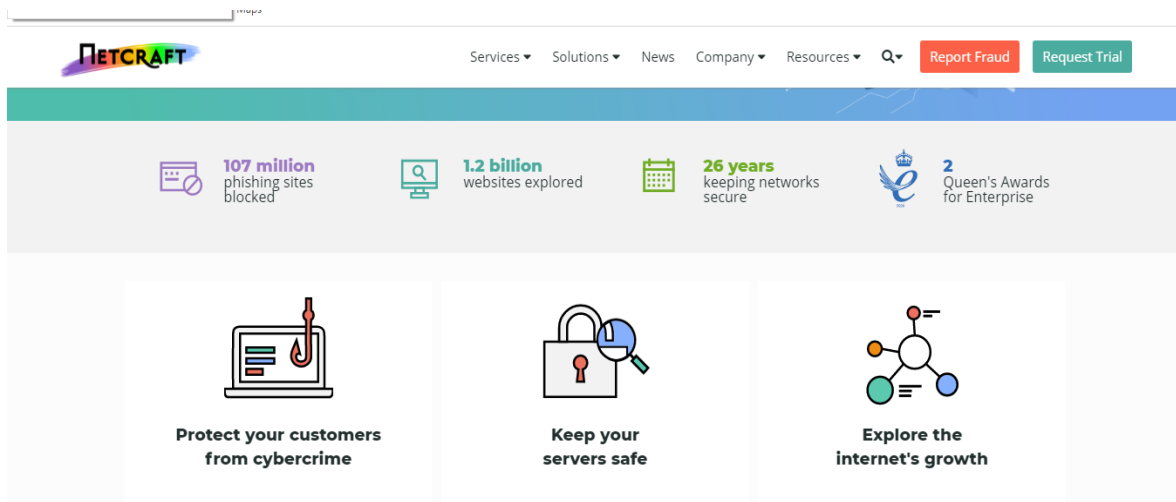
IP Location: United States - Washington - Seattle - Akamai Technologies Inc.

Domain Status: Registered And Active Website

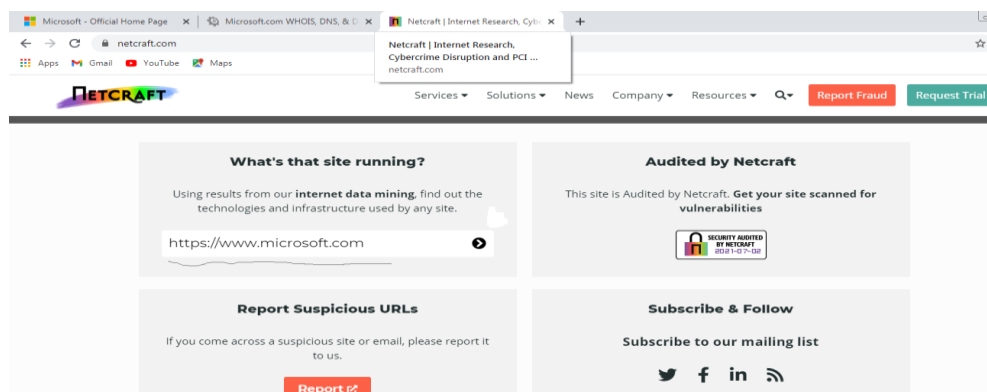
Hosting History:3 changes on 4 unique name servers over 1 year

Then we try to **gather more information from netcraft website i.e www.netcraft.com** :

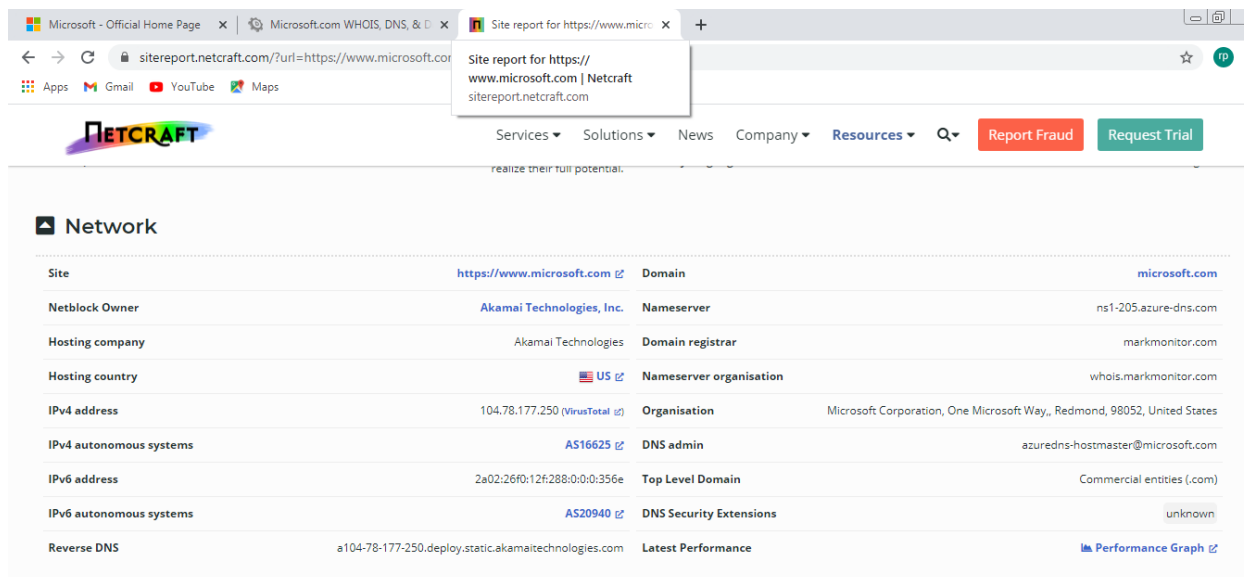
1. The first step is to enter the website name i.e www.netcraft.com in the search engine and then opens the website:



- Then we have to enter the domain name or IP address of the website to extract more information from the website:



- Then the third step to extract information from this website:



The information **extracted from this websites are:**

Site rank 70

IPv4 address: 104.78.177.250

IPv4 autonomous systems AS16625

IPv6 address: 2a02:26f0:12f:288:0:0:0:356e

IPv6 autonomous systems AS20940

Reverse DNS: a104-78-177-250.deploy.static.akamaitechnologies.com

DNS admin azuredns-hostmaster@microsoft.com

SSL/TLS

Supported TLS Extensions RFC8446 supported versions,

RFC8446 key share, RFC4366 server name, RFC4492 elliptic curves,

RFC7301 application-layer protocol negotiation, RFC4366 status request

Subject Alternative Name wwwqa.microsoft.com, www.microsoft.com, staticview.microsoft.com,
i.s-microsoft.com, microsoft.com, c.s-microsoft.com,
privacy.microsoft.com

Validity period: From Aug 28 2020 to Aug 28 2021 (12 months)

Public key algorithm rsaEncryption

Protocol version TLSv1.3

Public key length 2048

Signature algorithm sha256WithRSAEncryption

Serial number 0x6b000003f4e3a67a2348550c330000000003f4

OCSP data generated Jul 2 08:26:17 2021 GMT

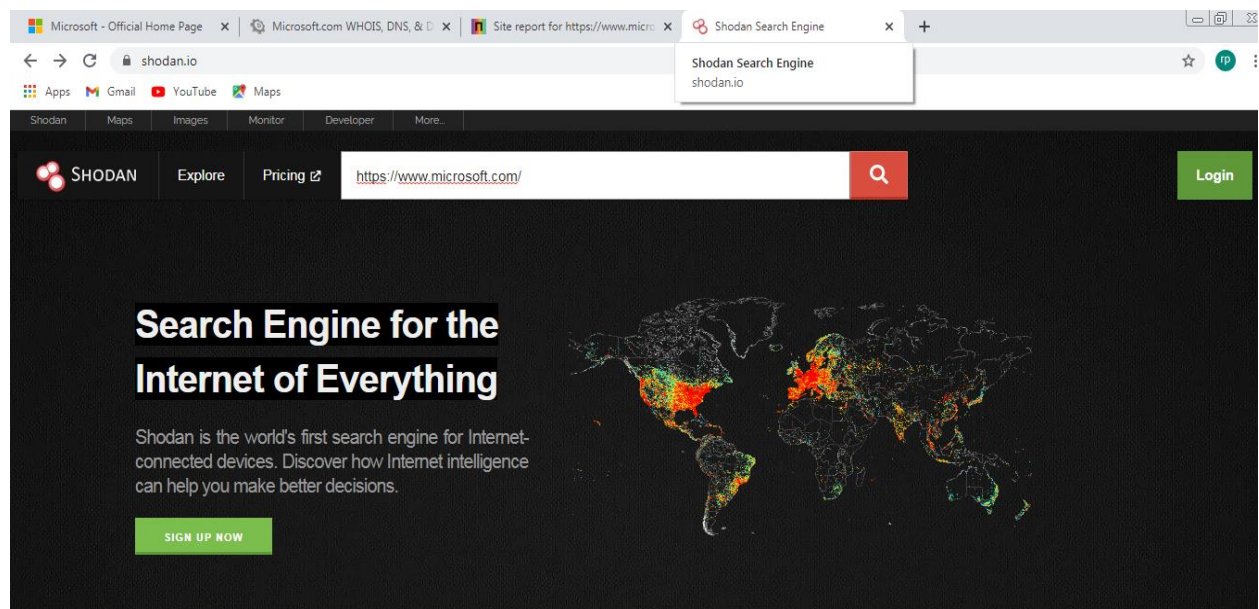
OCSP data expires Jul 6 08:26:17 2021 GMT

We can also check **the hosting history from this website:**

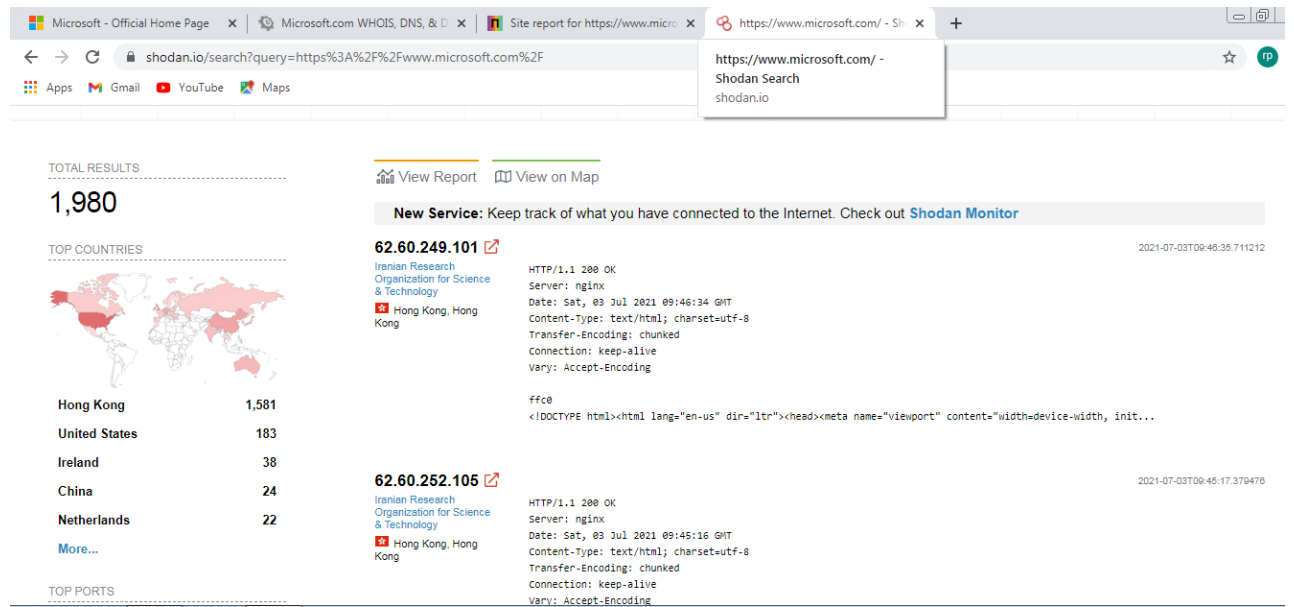
Netblock owner	IP address	OS	Web server	Last seen
Akamai Technologies, Inc. 145 Broadway Cambridge MA US 02142	104.110.245.246	Linux	unknown	29-Jun-2021
Akamai Technologies, Inc. 145 Broadway Cambridge MA US 02142	104.95.181.163	Linux	unknown	27-Jun-2021
Akamai Technologies, Inc. 145 Broadway Cambridge MA US 02142	104.110.245.246	Linux	unknown	20-Jun-2021
Akamai Technologies, Inc. 145 Broadway Cambridge MA US 02142	104.95.181.163	Linux	unknown	12-Jun-2021
Akamai Technologies	92.122.165.100	Linux	unknown	5-Jun-2021
Akamai Technologies, Inc. 145 Broadway Cambridge MA US 02142	104.95.181.163	Linux	unknown	29-May-2021
Akamai Technologies	92.122.165.100	Linux	unknown	22-May-2021
Akamai	88.221.16.244	Linux	unknown	19-Mar-2021
Akamai Technologies, Inc. 145 Broadway Cambridge MA US 02142	104.85.57.244	Linux	unknown	12-Mar-2021
Akamai Technologies	92.122.165.100	Linux	unknown	5-Mar-2021

Now we explore another website name shodan to extract information about a particular server:

1. First step is to enter the name of the website i.e. www.shodan.io on the search engine and enter the domain name of the website we want to search for:



2. Then the second step is to extract the information about the server present in the website:



The information about the servers we gather from this websites are:

Server in TOP COUNTRIES

Hong Kong 1,581

United States 183

Ireland 38

China 24

Netherlands 22

India 7

France 3

Germany 1

TOP PORTS

443 256

8081 158

8089 155

8083 145

8834 144

8140 139

8139 138

8443 138

8880 137

8181 130

8500 127

8889 127

TOP ORGANIZATIONS

Iranian Research Organization for Science & Technology 1,562

Microsoft Corporation 156

IT7 Networks Inc 35

Amazon Data Services Ireland Limited 15

Aliyun Computing Co., LTD 12

Microsoft Limited UK 11

Microsoft Corp 10

Clayer Limited 8

Amazon Technologies Inc. 7

Google LLC 5

Virtual Machine Solutions LLC 5

Vultr Holdings, LLC 5

Defense.Net, Inc 4

DigitalOcean, LLC 4

Oracle Corporation 4

Oracle Public Cloud 4

BAcloud 3

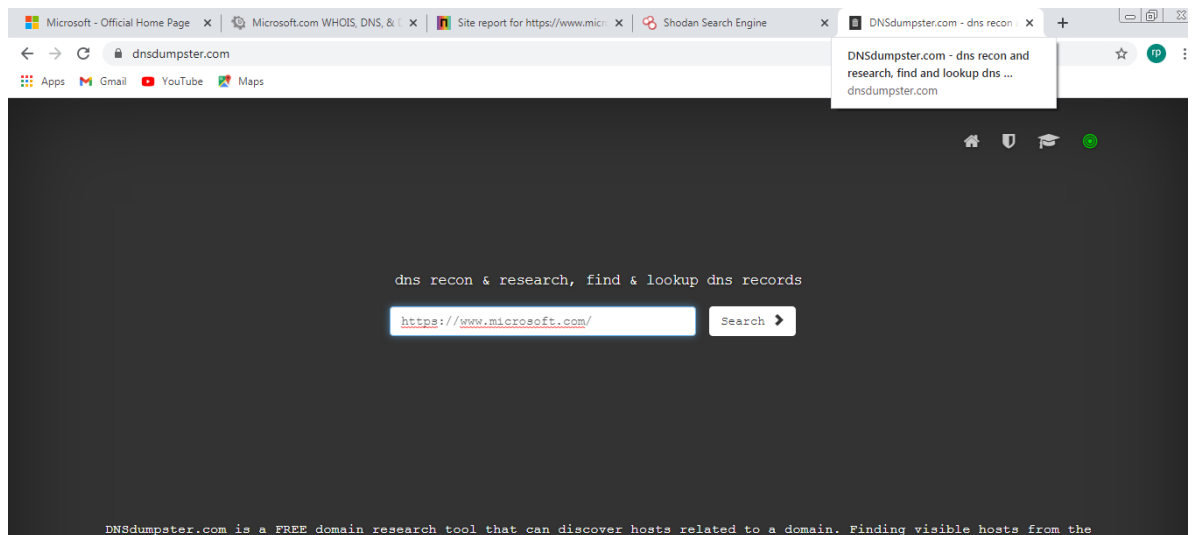
TOP PRODUCTS

nginx	805
Apache httpd	40
Microsoft IIS httpd	23

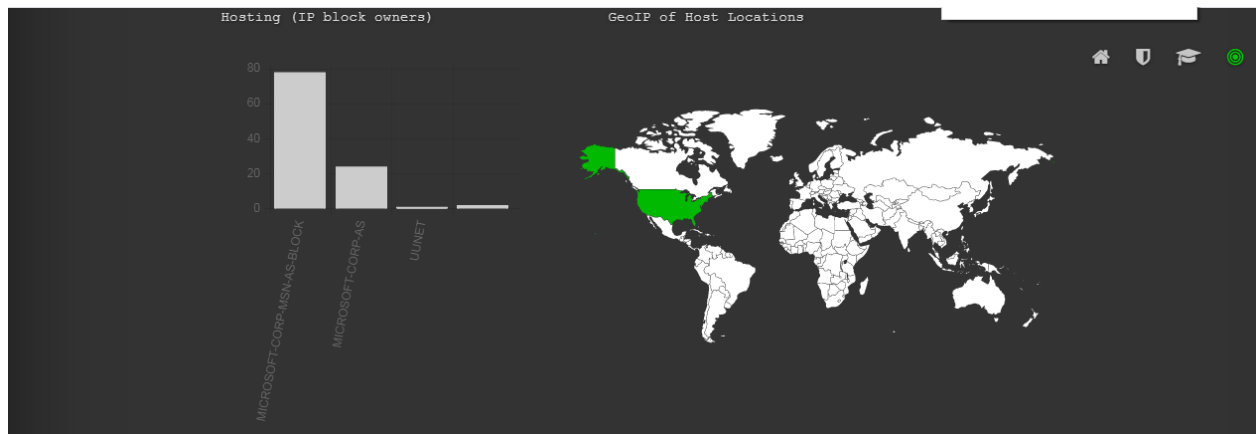
We can also gather information about particular **server IP address on shodan.io**

Now we can use another website named dnsdumpster to extract more information about a particular server:

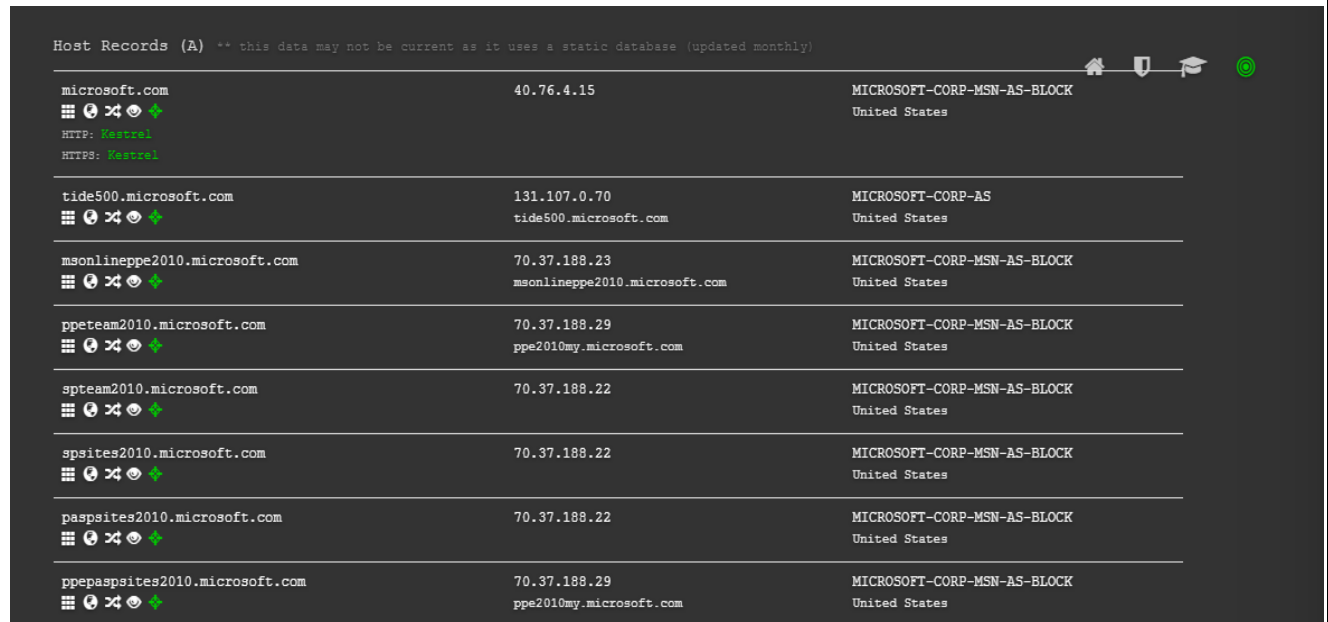
1. The first step is to open the website i.e. <https://dnsdumpster.com> on search engine and enter the domain name of the website want to search for:



2. Then collect the information present in the website:



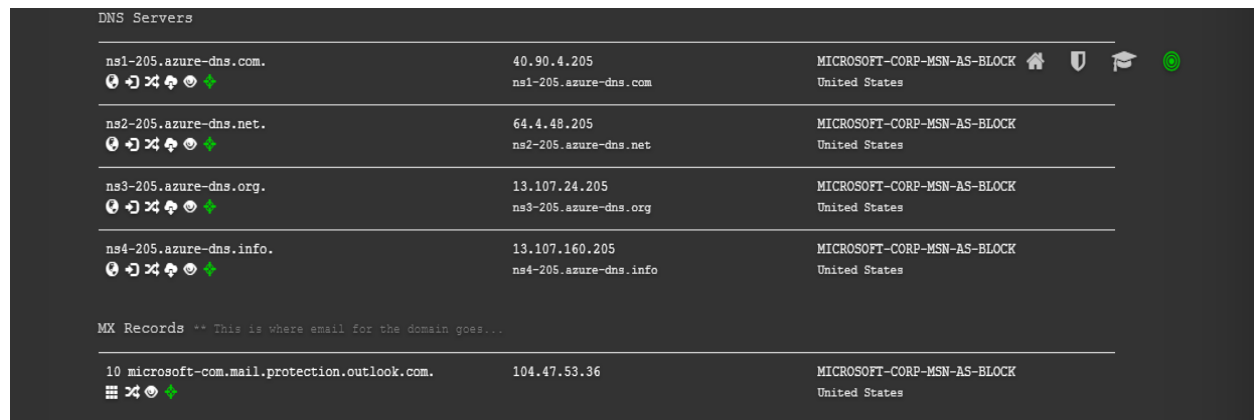
The above picture shows number of hosts located in the geolocation like in this case united states of America has 10 hosts.



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

microsoft.com 🏠 🛡️ 🎓 🟢 HTTP: Kestrel HTTPS: Kestrel	40.76.4.15	MICROSOFT-CORP-MSN-AS-BLOCK United States
tide500.microsoft.com 🏠 🛡️ 🎓 🟢 tide500.microsoft.com	131.107.0.70	MICROSOFT-CORP-AS United States
msonlineppe2010.microsoft.com 🏠 🛡️ 🎓 🟢 msonlineppe2010.microsoft.com	70.37.188.23	MICROSOFT-CORP-MSN-AS-BLOCK United States
ppeteam2010.microsoft.com 🏠 🛡️ 🎓 🟢 ppe2010my.microsoft.com	70.37.188.29	MICROSOFT-CORP-MSN-AS-BLOCK United States
spteam2010.microsoft.com 🏠 🛡️ 🎓 🟢	70.37.188.22	MICROSOFT-CORP-MSN-AS-BLOCK United States
spsites2010.microsoft.com 🏠 🛡️ 🎓 🟢	70.37.188.22	MICROSOFT-CORP-MSN-AS-BLOCK United States
paspsites2010.microsoft.com 🏠 🛡️ 🎓 🟢	70.37.188.22	MICROSOFT-CORP-MSN-AS-BLOCK United States
ppepaspsites2010.microsoft.com 🏠 🛡️ 🎓 🟢 ppe2010my.microsoft.com	70.37.188.29	MICROSOFT-CORP-MSN-AS-BLOCK United States

The above picture show the number of hosting,IP addresses and their locations present in the website.



DNS Servers

ns1-205.azure-dns.com. 🏠 🛡️ 🎓 🟢 ns1-205.azure-dns.com	40.90.4.205	MICROSOFT-CORP-MSN-AS-BLOCK United States
ns2-205.azure-dns.net. 🏠 🛡️ 🎓 🟢 ns2-205.azure-dns.net	64.4.48.205	MICROSOFT-CORP-MSN-AS-BLOCK United States
ns3-205.azure-dns.org. 🏠 🛡️ 🎓 🟢 ns3-205.azure-dns.org	13.107.24.205	MICROSOFT-CORP-MSN-AS-BLOCK United States
ns4-205.azure-dns.info. 🏠 🛡️ 🎓 🟢 ns4-205.azure-dns.info	13.107.160.205	MICROSOFT-CORP-MSN-AS-BLOCK United States

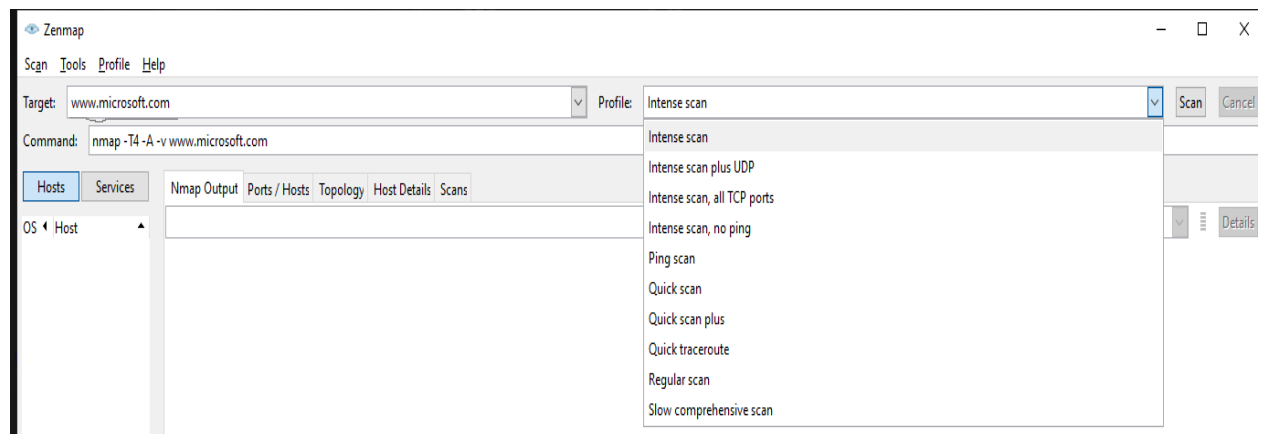
MX Records ** This is where email for the domain goes...

10 microsoft-com.mail.protection.outlook.com. 🏠 🛡️ 🎓 🟢	104.47.53.36	MICROSOFT-CORP-MSN-AS-BLOCK United States
---	--------------	--

The above picture shows the DNS servers, their IP addresses and the geolocation of the servers.

Then we use another tool called **NMAP to scan a particular network:**

1.write the name of the target and select the type of the scan and then click on scan button to start scanning of a network. The picture is attached as below:



Then collect the information from the given tool:

```
Starting Nmap 7.91 ( https://nmap.org ) at 2021-07-03 23:41 India Standard Time
NSE: Loaded 153 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 23:41
Completed NSE at 23:41, 0.05s elapsed
Initiating NSE at 23:41
Completed NSE at 23:41, 0.00s elapsed
Initiating NSE at 23:41
Completed NSE at 23:41, 0.00s elapsed
Initiating Ping Scan at 23:41
Scanning www.microsoft.com (23.45.186.3) [4 ports]
Completed Ping Scan at 23:41, 0.87s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 23:41
Completed Parallel DNS resolution of 1 host. at 23:41, 0.06s elapsed
Initiating SYN Stealth Scan at 23:41
Scanning www.microsoft.com (23.45.186.3) [1000 ports]
Discovered open port 1723/tcp on 23.45.186.3
Discovered open port 80/tcp on 23.45.186.3
Discovered open port 554/tcp on 23.45.186.3
Discovered open port 21/tcp on 23.45.186.3
Discovered open port 443/tcp on 23.45.186.3
Completed SYN Stealth Scan at 23:42, 7.31s elapsed (1000 total ports)
Initiating Service scan at 23:42
Scanning 5 services on www.microsoft.com (23.45.186.3)
Service scan Timing: About 60.00% done; ETC: 23:45 (0:01:21 remaining)
Service scan Timing: About 80.00% done; ETC: 23:45 (0:00:40 remaining)
Completed Service scan at 23:44, 159.15s elapsed (5 services on 1 host)
Initiating OS detection (try #1) against www.microsoft.com (23.45.186.3)
Retrying OS detection (try #2) against www.microsoft.com (23.45.186.3)
Initiating Traceroute at 23:44
Completed Traceroute at 23:44, 3.03s elapsed
Initiating Parallel DNS resolution of 4 hosts. at 23:44
Completed Parallel DNS resolution of 4 hosts. at 23:44, 0.43s elapsed
NSE: Script scanning 23.45.186.3.
Initiating NSE at 23:44
Completed NSE at 23:45, 37.89s elapsed
Initiating NSE at 23:45
Completed NSE at 23:45, 19.88s elapsed
Initiating NSE at 23:45
```

```

Initiating Parallel DNS resolution of 4 hosts. at 23:44
Completed Parallel DNS resolution of 4 hosts. at 23:44, 0.43s elapsed
NSE: Script scanning 23.45.186.3.
Initiating NSE at 23:44
Completed NSE at 23:45, 37.89s elapsed
Initiating NSE at 23:45
Completed NSE at 23:45, 19.88s elapsed
Initiating NSE at 23:45
Completed NSE at 23:45, 0.00s elapsed
Nmap scan report for www.microsoft.com (23.45.186.3)
Host is up (0.084s latency).
Other addresses for www.microsoft.com (not scanned): 2405:200:1630:8b6::356e 2405:200:1630:8a2::356e
rDNS record for 23.45.186.3: a23-45-186-3.deploy.static.akamaitechnologies.com
Not shown: 995 filtered ports
PORT      STATE SERVICE VERSION
21/tcp    open  ftp?
80/tcp    open  http    AkamaiGHost (Akamai's HTTP Acceleration/Mirror service)
|_ http-methods:
|_ Supported Methods: GET HEAD POST OPTIONS
|_ http-title: Your request has been blocked. This could be ...
443/tcp   open  ssl/http AkamaiGHost (Akamai's HTTP Acceleration/Mirror service)
|_ http-methods:
|_ Supported Methods: GET HEAD POST OPTIONS
|_ http-title: Your request has been blocked. This could be ...
|_ ssl-cert: Subject: commonName=www.microsoft.com/organizationName=Microsoft Corporation/stateOrProvinceName=WA/countryName=US
|_ Subject Alternative Name: DNS:wwwqa.microsoft.com, DNS:www.microsoft.com, DNS:staticview.microsoft.com, DNS:i.s-microsoft.com, DNS:microsoft.com, DNS:c.s-microsoft.com, DNS:privacy.microsoft.com
|_ Issuer: commonName=Microsoft RSA TLS CA 01/organizationName=Microsoft Corporation/countryName=US
|_ Public Key type: rsa
|_ Public Key bits: 2048
|_ Signature Algorithm: sha256WithRSAEncryption
|_ Not valid before: 2020-08-28T22:17:02
|_ Not valid after: 2021-08-28T22:17:02
|_ MD5: 5c3f abd1 133a 0a77 0e52 e9ef 56ae f0bb
|_ SHA-1: 9b2b 8ae6 5169 aa47 7c57 83d6 480f 296e f48c f14d
|_ ssl-date: TLS randomness does not represent time
|_ tls-alpn:
|_ http/1.1
|_ http/1.0

|_ http/1.0
|_ tls-nextprotoneg:
|_ http/1.1
|_ http/1.0
554/tcp   open  rtsp?
1723/tcp  open  pptp?
|_ pptp-version: ERROR: Script execution failed (use -d to debug)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: load balancer
Running (JUST GUESSING): F5 Networks TMOS 11.6.X (85%)
OS CPE: cpe:/o:f5:tmos:11.6
Aggressive OS guesses: F5 BIG-IP Local Traffic Manager load balancer (TMOS 11.6) (85%)
No exact OS matches for host (test conditions non-ideal).
Uptime guess: 21.279 days (since Sat Jun 12 17:03:56 2021)
Network Distance: 6 hops
TCP Sequence Prediction: Difficulty=257 (Good luck!)
IP ID Sequence Generation: Busy server or unknown class

TRACEROUTE (using port 80/tcp)
HOP RTT ADDRESS
1 58.00 ms 192.168.43.252
2 ...
3 129.00 ms 10.72.69.10
4 130.00 ms 172.25.29.9
5 131.00 ms 172.25.17.36
6 131.00 ms a23-45-186-3.deploy.static.akamaitechnologies.com (23.45.186.3)

NSE: Script Post-scanning.
Initiating NSE at 23:45
Completed NSE at 23:45, 0.00s elapsed
Initiating NSE at 23:45
Completed NSE at 23:45, 0.00s elapsed
Initiating NSE at 23:45
Completed NSE at 23:45, 0.00s elapsed
Read data files from: C:\Program Files (x86)\Nmap
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 284.26 seconds
Raw packets sent: 2098 (96.004KB) | Rcvd: 73 (4.116KB)

```

These are the information collected from NMAP tool

This tool gives the IP address of the target and the number of ports open in the target. Like in the case the IP address is 23.45.186.3 and 4 ports are open for this IP address.

These many information we can collect from foot printing.

-----END OF TASK 1-----

TASK 7:

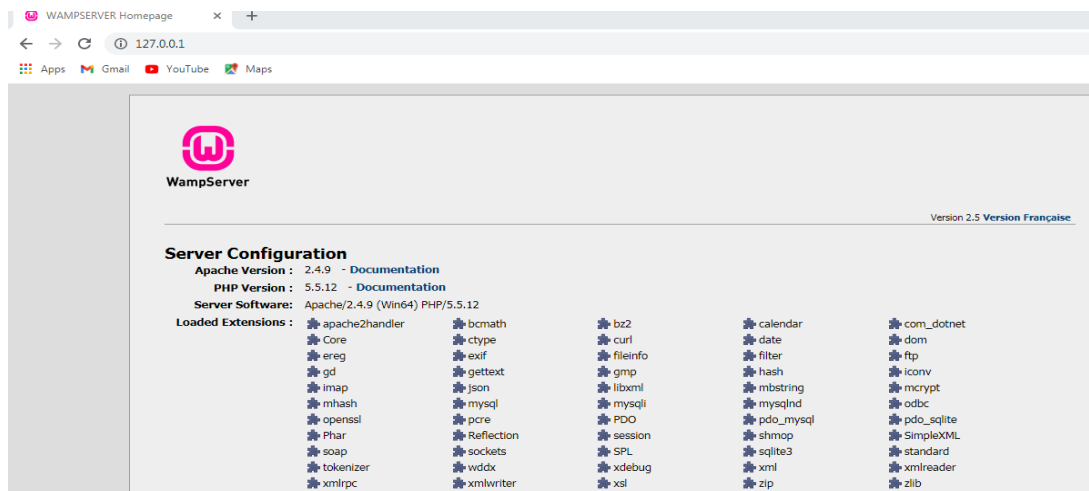
In this task we have to clone a facebook page and perform desktop phishing and capture the credentials:

Desktop phishing is another type of phishing attack in which an attacker make his own machine as a server and clone a page in his server and send the link to the victim to perform phishing attack.

1.first we need to install wamp server in our machine and wait for the icon color to turn into green.



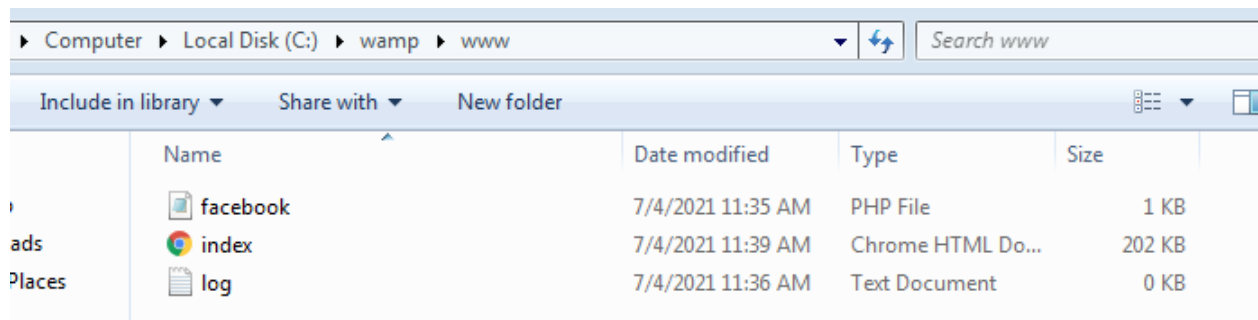
2. Then check in the browser whether the wamp server is loaded in the browser or not by writing the **IP address of the machine** or type **localhost** or type loopback IP address i.e **127.0.0.1**



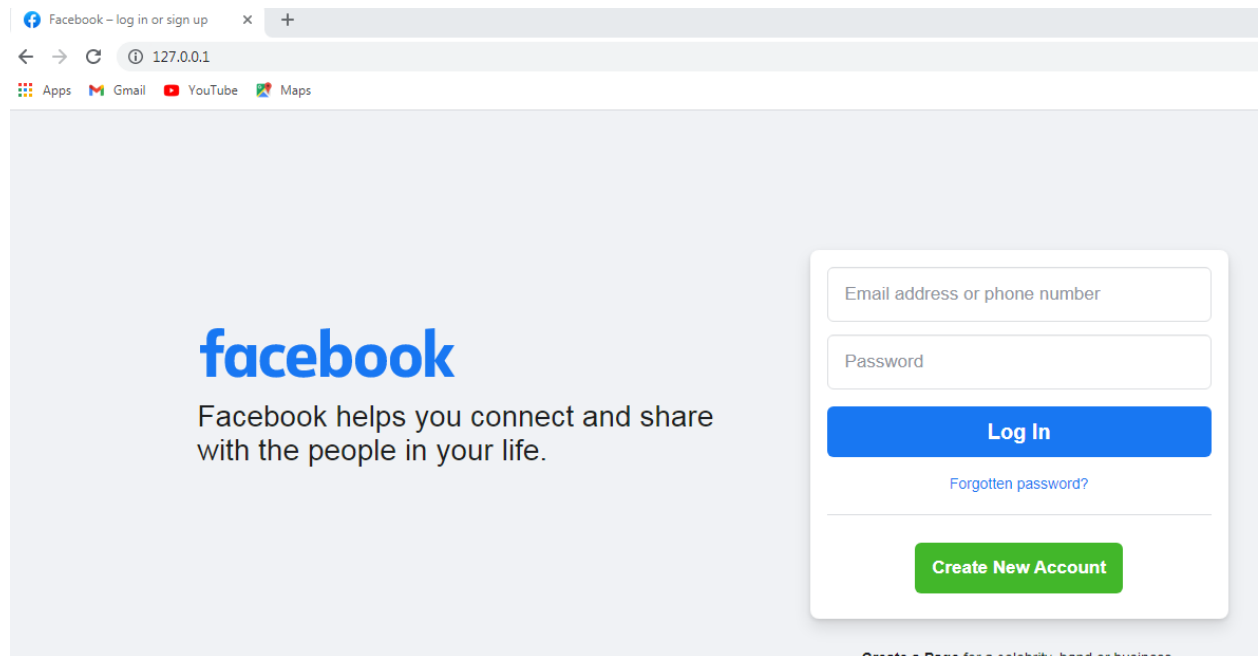
3. download a facebook clone page and save it as **.html extension** only, download a phishing script and save it as a **.php** extension and then a **notepad file** to save user name and password.

4. then open the HTML page with notepad and search for action=,remove the original link from there and paste your own phishing script link there.

5. Copy all the three files and paste it in the www folder of the wamp server file. The path is: **c: /wamp/www.**



6. Check in the browser whether the facebook page is loaded in the server or not.



7. Send this link to **someone (this will work for the people in the same network only)** for the attack when the victim enters the login credentials it will save in the log file in the wampserver files.

```
log - Notepad
File Edit Format View Help
jazoest=21051
1sd=AvpTaTuxNao
email=someone@gmail.com
login_source=comet_headerless_login
next=
encpass=#PWD_BROWSER:5:1625446279:AQ9QAfRVKHwo284wEqrw/xj405+0jPcfHIobyv3/3Q39d1CT21CuqFQ5K62Ljm7EaRxcfIH6pmdNQ85V
```

If the attacker want to send this to other victim present in the other network then the attacker have to create a tunnel name vortex (downloaded from internet) and send the link generated from it to the victim.

Some solutions to keep safe from phishing are:

1. Check the link twice before opening any link.
2. Check the link in the website called phish tank whether it is a phishing website or not.
3. Don't click on any link from untrustable source.
4. Always verify the website security before opening it.
5. Install an antiphishing toolbar.

-----END OF TASK 7-----

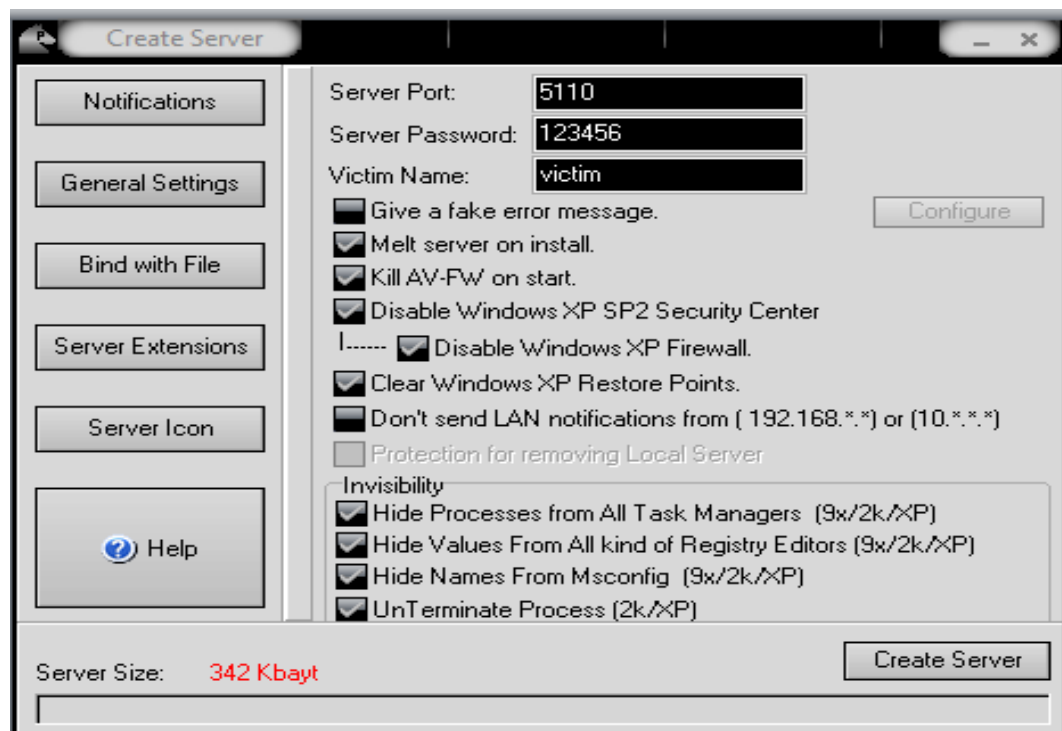
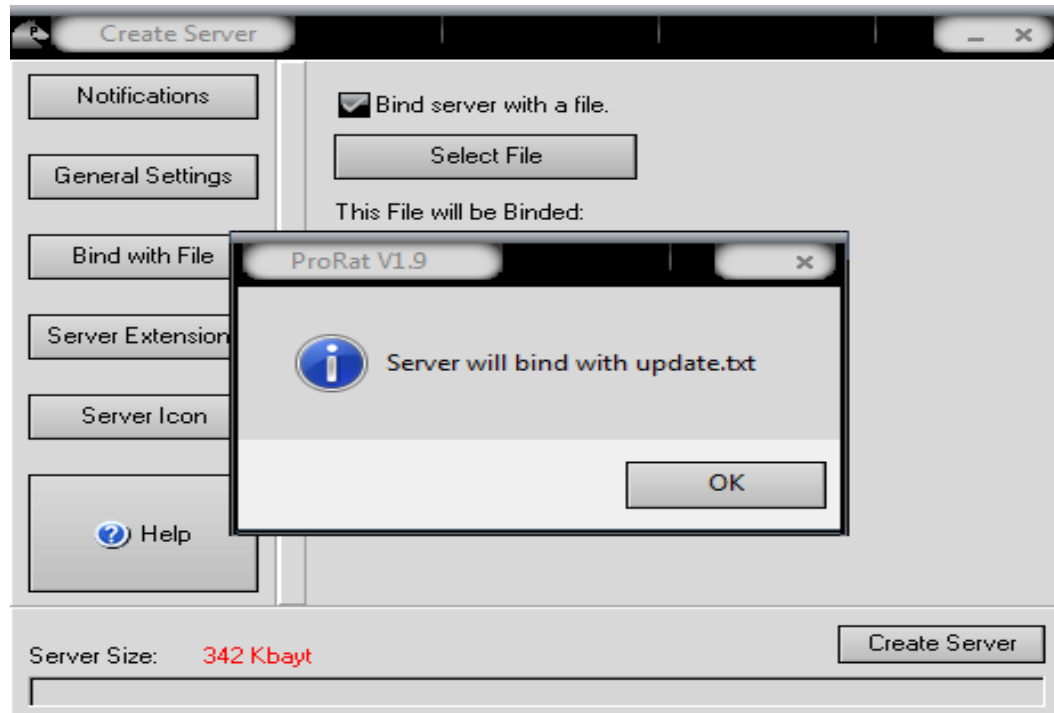
Task 2

In this task first download prorot(an app used to create virus and help to hack the victim machine) from internet and install it on the machine.

Step1: the first step is to open the prorot in the machine and select create option to create a server.



Step 2: Then select bind with file option and select the file in which you want to inject virus. And then click on create server and then the app will create a file.



Step 3: send the created file into victim machine and execute the file in victim machine.

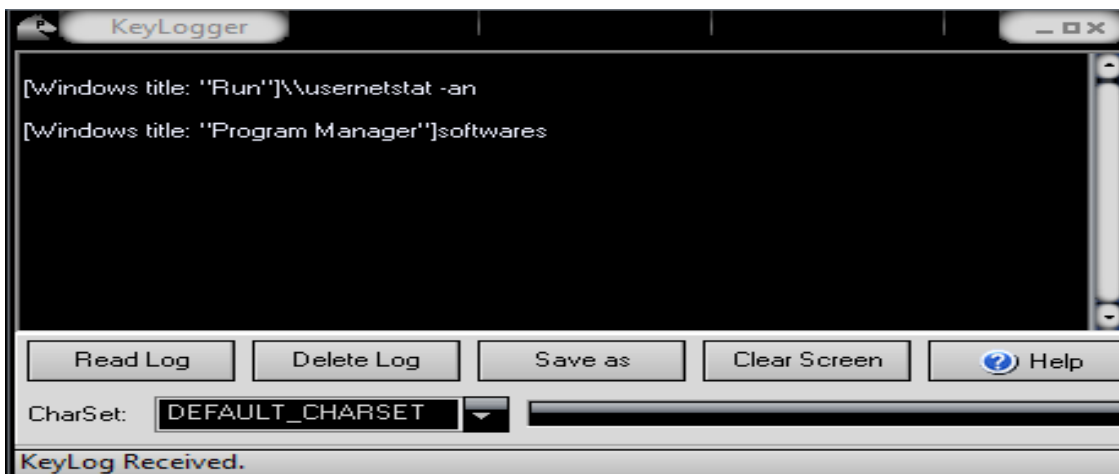


Step 4: then enter the IP address of the victim machine and click on connect, then the attacker will connect to victim.

The screenshot of the victim machine is attached below:



The screenshot of the keystroke is attached below:



Security patch to avoid system hacking:

1. Check the properties of the file before opening it.
2. Never click on links from untrusted source.
3. Install an antivirus on the system.

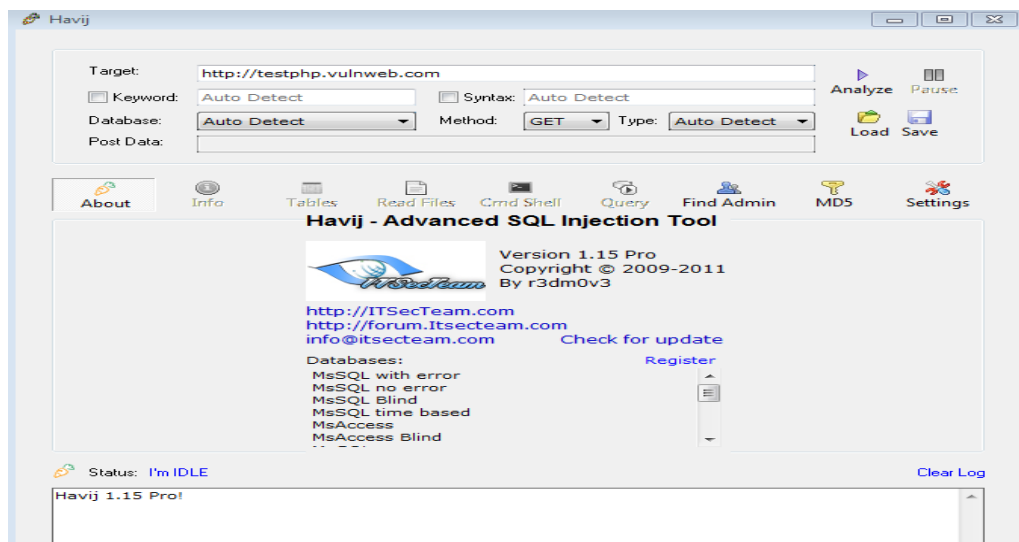
----- **END OF TASK 2**-----

TASK 5:

In this task we have to perform sql injection attack using havij tool to extract information from a website.

Havij tool is a advanced sql injection tool used to extract data such as login id and passwords, tables, columns, emails etc. from websites.

Step1: The first step is to download havij tool from the internet and run it as a administrator mode.

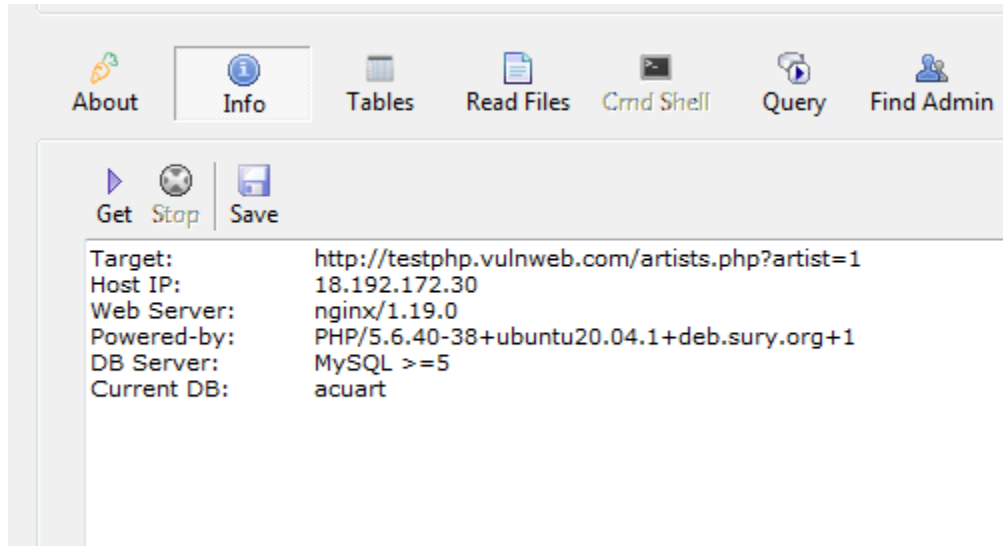


Step 2: then enter the name of the website in the target bar and click on analyze button to fetch the details of the website.

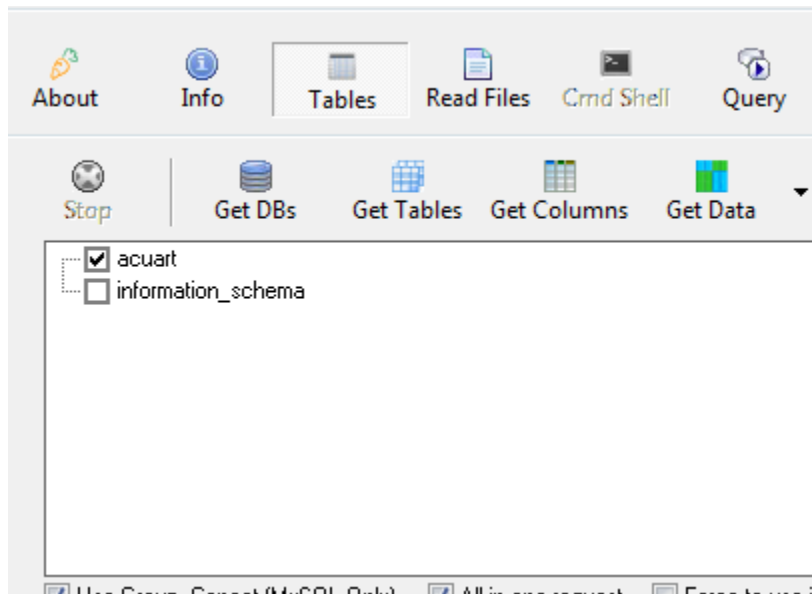
Host IP: 18.192.172.30
Web Server: nginx/1.19.0
Powered-by: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Keyword Found: ipsum
Injection type is Integer

In this case we got HOST IP as 18.192.172.30, web server as nginx/1.19.0.

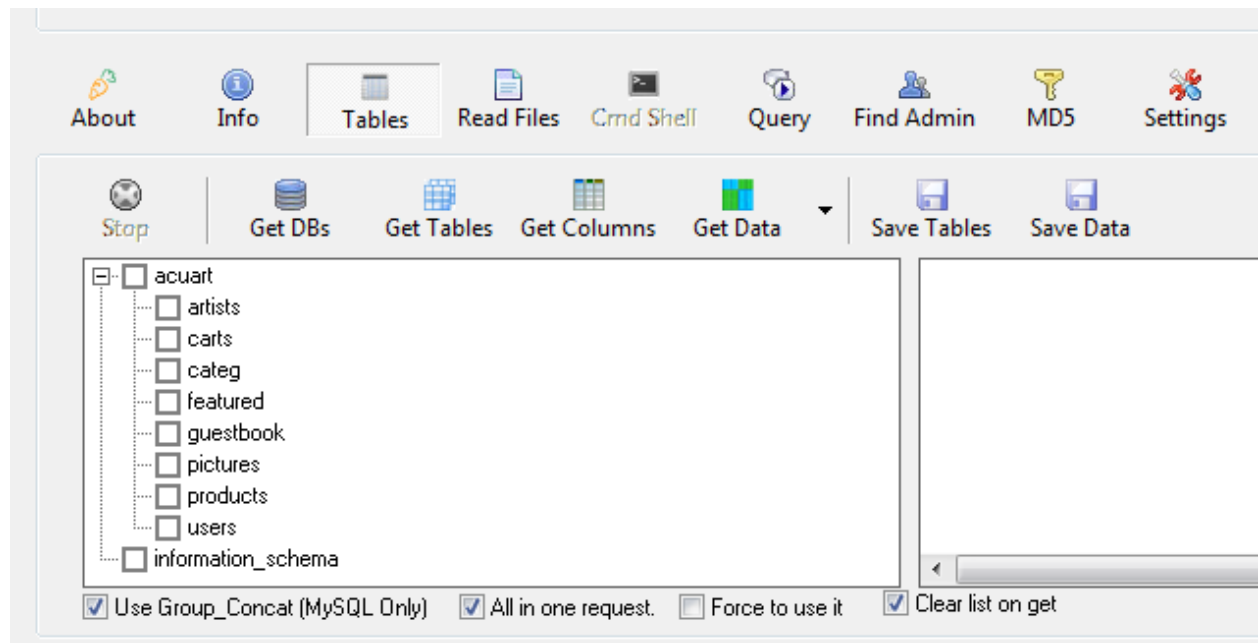
Step 3: then click on info to get information about the target.



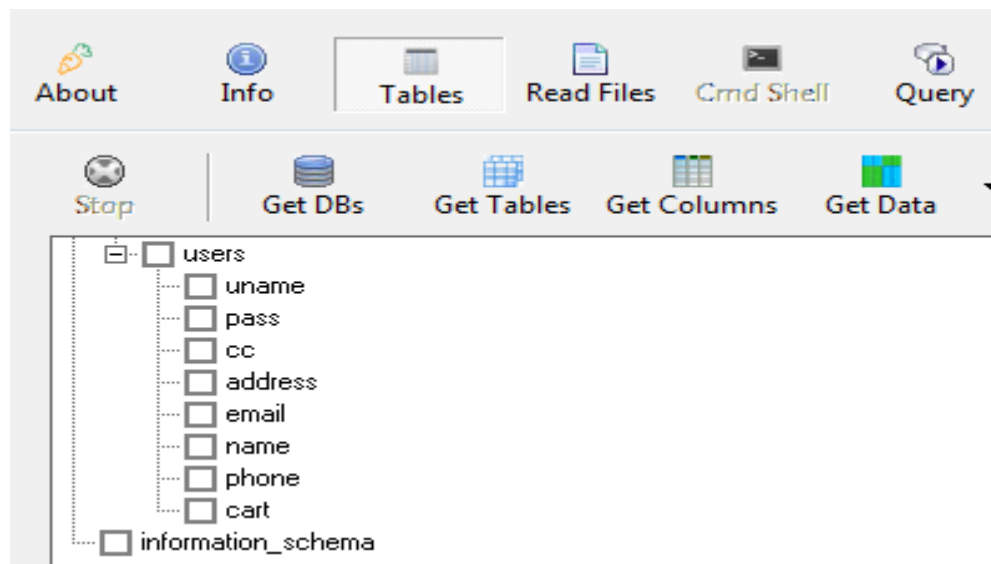
Step 4: then click on tables to fetch tables in the database.



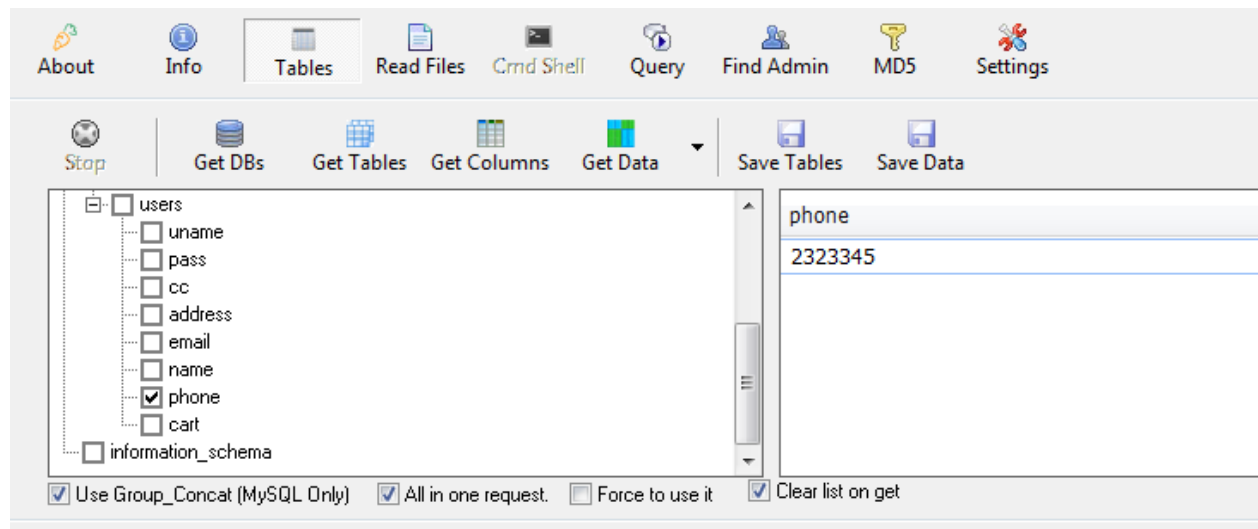
Step 5: then click on tables to get tables of the selected database.



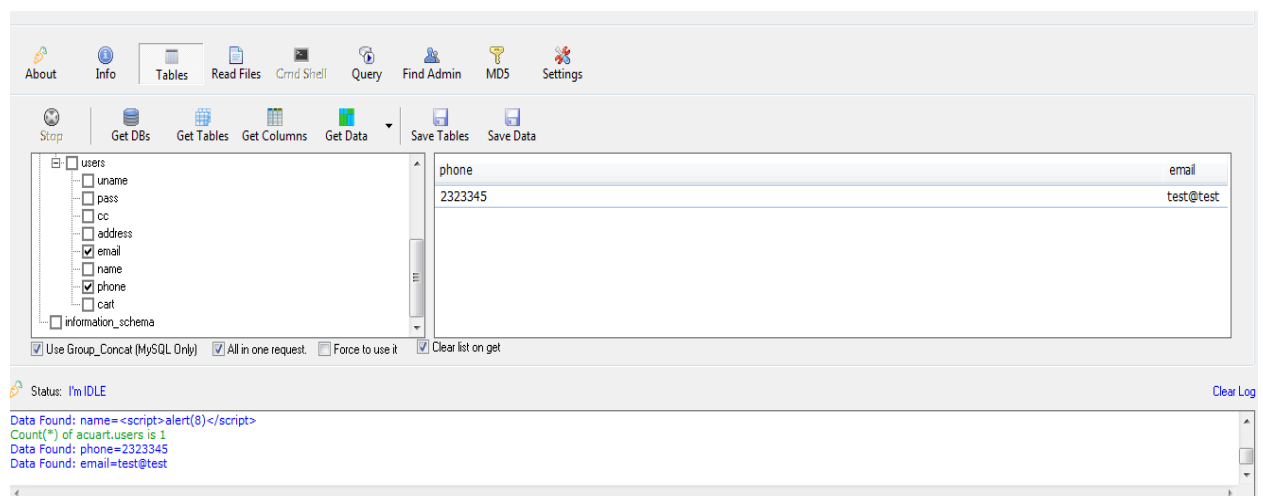
Step 6: suppose the attacker want to fetch the columns of the user table, select users and click on get columns.



Step 7: suppose the attacker wants to extract phones of the users, select phone and click on get data.



Step 8: suppose the user wants to fetch phone and email both then select email and phone and click on get data to extract the data.



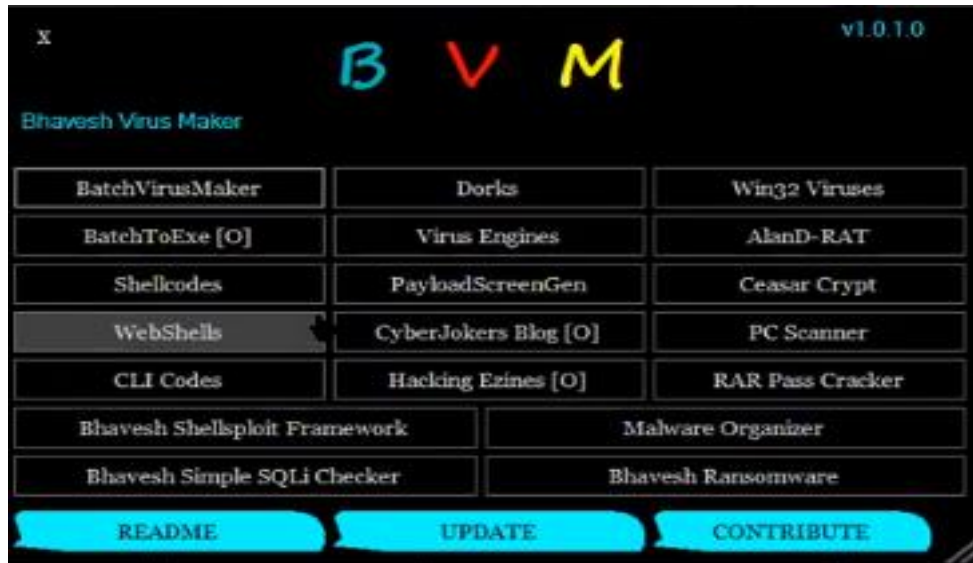
Preventive steps to avoid sql injections are:

1. Raise virtual or physical firewalls.
2. Actively manage patches and updates.
3. Use stored procedures in the database.
4. Validate user inputs.
5. Continuous monitoring of sql statements.
6. Perform regular auditing and penetration testing.

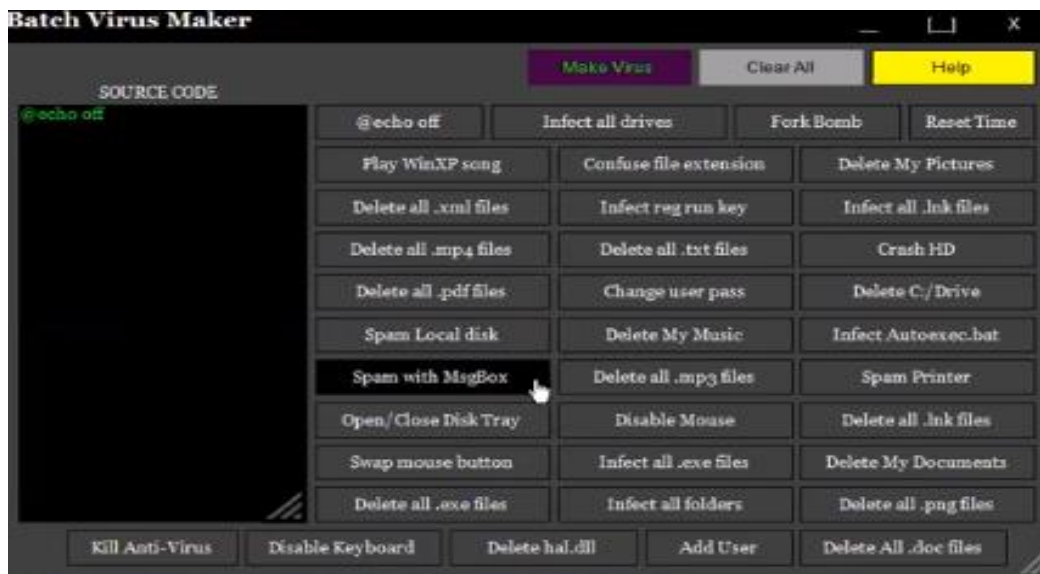
-----END OF TASK 5-----

TASK 3: In this task we have to create virus in the machine and send it to victim machine. We will BVM(bhavesh virus maker) tool to create virus.

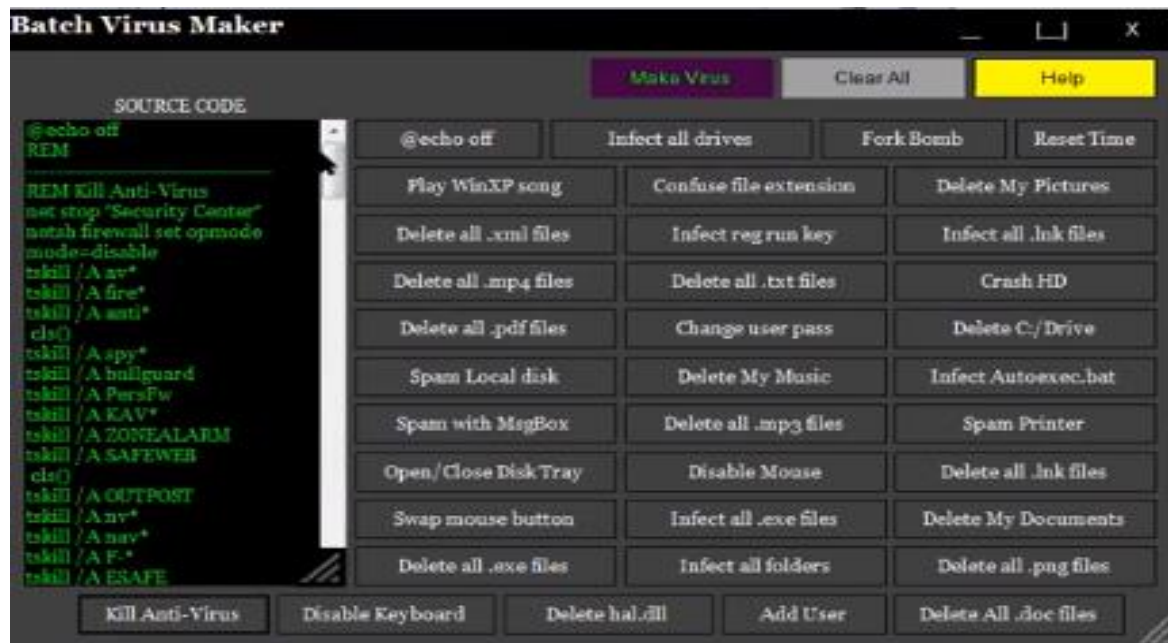
Step 1: the first step is to install the BVM tool in the machine and execute it.



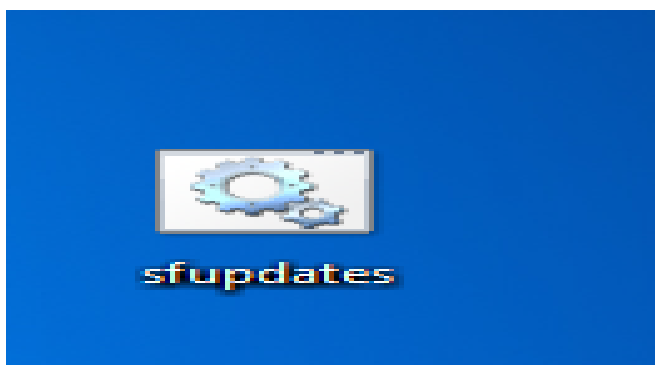
Step 2: select one of the icon to create virus for e.g click on BatchVirusMaker.



Step 3: select one of the option to create the virus code. for example the attacker wants to kill the antivirus present in the victim machine click on the kill antivirus button and the code will display automatically.



Step 4: execute this file in the victim machine :



When victim click on the file It automatically disabled all the antivirus present in the system.

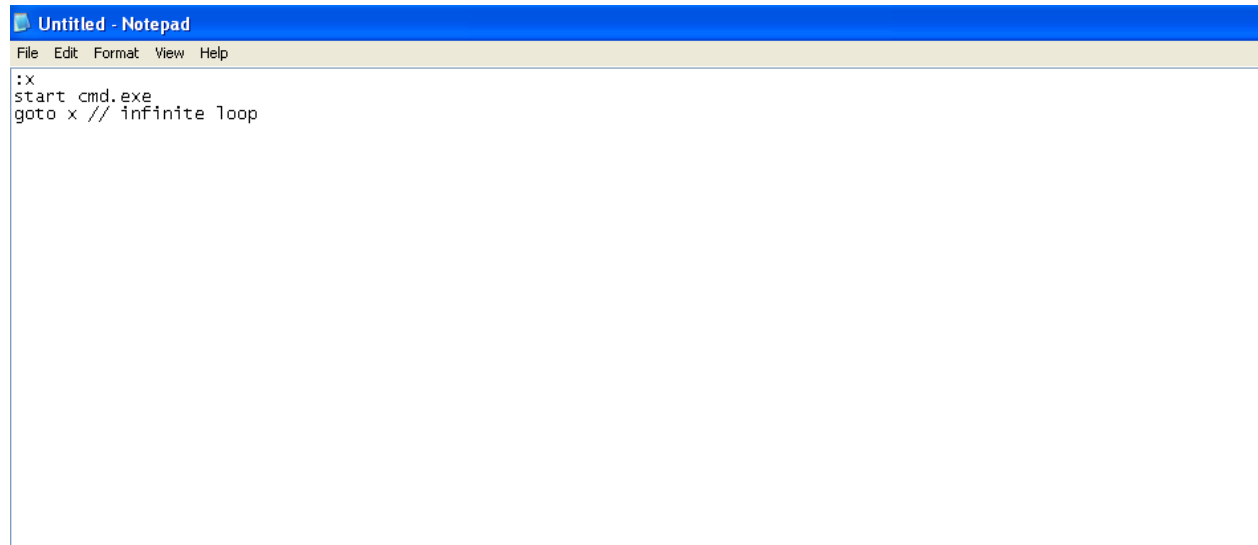
Preventive measures to avoid malware affect:

1. Update operating systems, browsers and plug-ins regularly.
2. Always use virus detection tools to scan a file.
3. Make sure of a secure connection.

-----END OF TASK 3-----

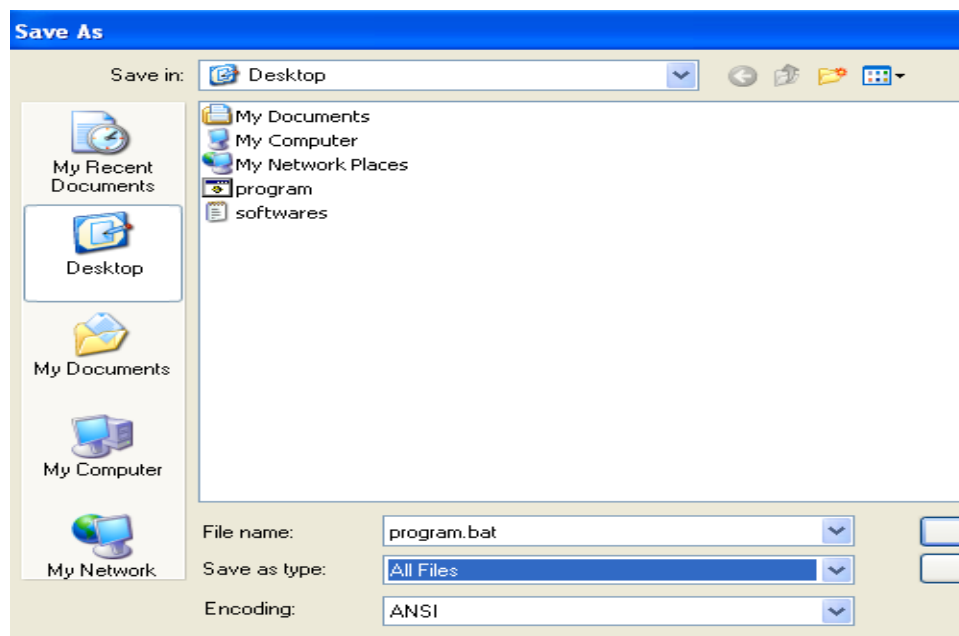
TASK 4: In this program we have to write a batch program and save it as .bat extension and execute in the victim machine.

Step 1: first open a notepad and write the program

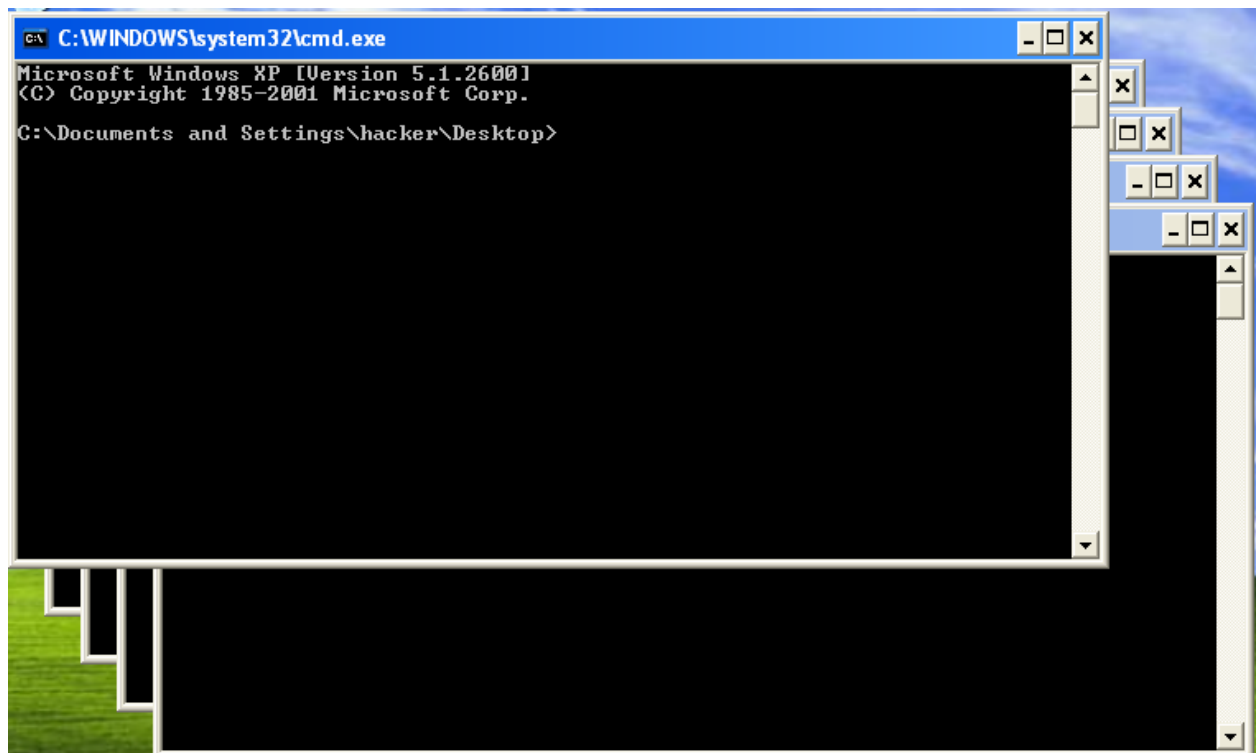


This is the program to open command prompt infinitely in the machine.

Step 2: then save it as .bat extension and select all files in file type.



Step 3: last step is to execute it by double click on the victim machine. The result is attached below. Command prompt opens infinite times in the machine.



-----END OF TASK 4-----