VERZIO MINOR PROJECT

CYBER SECURITY MINOR PROJECT OCTOBER

SUBMITTED BY

AKASH M

Q1)Perform Foot printing on Amazon Website and gather information about website by using onlineWebsites (Whois / netcraft / Shodan / dnsdumpster., etc.) as much as possible and write report ongathered info along with screenshots

ANS) The footprinting on given website using online information's gathering websites and noted some necessary information that would be useful to find vulnerability in websites

The foot printing are performed by following website
1) Whois:
2) Netcraft
3) Shodan
4) Dnsdumpster

`1) Whois lookup:

Domain Profile

Registrant	Hostmaster, Amazon Legal Dept.
Registrant Org	Amazon Technologies, Inc
Registrant Country	us
Registrar	MarkMonitor, Inc. MarkMonitor Inc. IANA ID: 292 URL: http://www.markmonitor.com
Dates	9,878 days old Created on 1994-10-31 Expires on 2024-10-30 Updated on 2019-08-26

Name Servers	NS1.P31.DYNECT.NET (has 225,126 domains) NS2.P31.DYNECT.NET (has 225,126 domains) NS3.P31.DYNECT.NET (has 225,126 domains) NS4.P31.DYNECT.NET (has 225,126 domains) PDNS1.ULTRADNS.NET (has 93,366 domains) PDNS6.ULTRADNS.CO.UK (has 2,579 domains)
Tech Contact	Hostmaster, Amazon Legal Dept. Amazon Technologies, Inc. P.O. Box 8102, Reno, NV, 89507, us
IP Address	13.224.31.152 - 6 other sites hosted on this server
IP Location	United States - Washington - Seattle - Amazon.com Inc
ASN	United States AS16509 AMAZON-02, US (registered May 04, 2000)
Domain Status	Registered And Active Website
IP History	459 changes on 459 unique IP addresses over 17 years
Registrar History	2 registrars with 1 drop
Hosting History	4 changes on 4 unique name servers over 17 years

Whois Record

(last updated on 2021-11-16)

Domain Name:	amazon.com
Registry Domain ID:	281209_DOMAIN_COM-VRSN
Registrar WHOIS Server:	whois.markmonitor.com
Registrar URL:	http://www.markmonitor.com
Updated Date:	2019-08-26T19:19:56+0000
Creation Date:	1994-11-01T05:00:00+0000
Registrar Expiration Date:	2024-10-30T07:00:00+0000
Registrar:	MarkMonitor, Inc.
Registrar IANA ID:	292
Registrar Contact Phone:	+1.2083895770
Registrant Name:	Hostmaster, Amazon Legal Dept.
Registrant Organization:	Amazon Technologies, Inc.
Registrant Street:	P.O. Box 8102
Registrant City:	Reno
Registrant State:	NV
Registrant Postal Code:	89507
Registrant Country:	US
Name Server:	ns1.p31.dynect.net
Name Server:	ns3.p31.dynect.net
Name Server:	ns2.p31.dynect.net
Name Server:	pdns6.ultradns.co.uk
Name Server:	pdns1.ultradns.net
Name Server:	ns4.p31.dynect.net

SCREENSHOTS

Whois Record for Amazon.com

– Domain Profile

Registrant	Hostmaster, Amazon Legal Dept.
Registrant Org	Amazon Technologies, Inc.
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	9,878 days old Created on 1994-10-31 Expires on 2024-10-30 Updated on 2019-08-26
Name Servers	NS1.P31.DYNECT.NET (has 225,126 domains) NS2.P31.DYNECT.NET (has 225,126 domains) NS3.P31.DYNECT.NET (has 225,126 domains) NS4.P31.DYNECT.NET (has 225,126 domains) PDNS1.ULTRADNS.NET (has 93,366 domains) PDNS6.ULTRADNS.CO.UK (has 2,579 domains)
Tech Contact	Hostmaster, Amazon Legal Dept. Amazon Technologies, Inc. P.O. Box 8102, Reno, NV, 89507, us hostmaster@amazon.com (p) 12062664064 (f) 12062667010
IP Address	13.224.31.152 - 6 other sites hosted on this server
IP Location	- Washington - Seattle - Amazon.com Inc.
ASN	AS16509 AMAZON-02, US (registered May 04, 2000)
Domain Status	Registered And Active Website
IP History	459 changes on 459 unique IP addresses over 17 years
Registrar History	2 registrars with 1 drop

Hosting History	4 changes on 4 unique name servers over 17 years

– Website

Website Title	None given.
Server Type	Server
Response Code	200
Terms	385 (Unique: 239, Linked: 210)
Images	31 (Alt tags missing: 3)
Links	82 (Internal: 80, Outbound: 0)

```
Domain Name: amazon.com
Registry Domain ID: 281209_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.markmonitor.com
Registrar URL: http://www.markmonitor.com
Updated Date: 2019-08-26T19:19:56+0000
Creation Date: 1994-11-01T05:00:00+0000
Registrar Registration Expiration Date: 2024-10-30T07:00:00+0000
Registrar: MarkMonitor, Inc.
Registrar IANA ID: 292
Registrar Abuse Contact Email: abusecomplaints@markmonitor.com
Registrar Abuse Contact Phone: +1.2083895770
Domain Status: clientUpdateProhibited (https://www.icann.org/epp#clientUpdateProhibited)
Domain Status: clientTransferProhibited (https://www.icann.org/epp#clientTransferProhibited)
Domain Status: clientDeleteProhibited (https://www.icann.org/epp#clientDeleteProhibited)
Domain Status: serverUpdateProhibited (https://www.icann.org/epp#serverUpdateProhibited)
Domain Status: serverTransferProhibited (https://www.icann.org/epp#serverTransferProhibited)
Domain Status: serverDeleteProhibited (https://www.icann.org/epp#serverDeleteProhibited)
Registry Registrant ID:
Registrant Name: Hostmaster, Amazon Legal Dept.
Registrant Organization: Amazon Technologies, Inc.
Registrant Street: P.O. Box 8102
Registrant City: Reno
Registrant State/Province: NV
Registrant Postal Code: 89507
Registrant Country: US
Registrant Phone: +1.2062664064
Registrant Phone Ext:
Registrant Fax: +1.2062667010
Registrant Fax Ext:
Registrant Email: hostmaster@amazon.com
Registry Admin ID:
Admin Name: Hostmaster, Amazon Legal Dept.
Admin Organization: Amazon Technologies, Inc.
Admin Street: P.O. Box 8102
Admin City: Reno
Admin State/Province: NV
Admin Postal Code: 89507
Admin Country: US
Admin Phone: +1.2062664064
Admin Phone Ext:
Admin Fax: +1.2062667010
Admin Fax Ext:
Admin Email: hostmaster@amazon.com
Registry Tech ID:
Tech Name: Hostmaster, Amazon Legal Dept.
Tech Organization: Amazon Technologies, Inc.
Tech Street: P.O. Box 8102
Tech City: Reno
Tech State/Province: NV
Tech Postal Code: 89507
Tech Country: US
Tech Phone: +1.2062664064
Tech Phone Ext:
Tech Fax: +1.2062667010
Tech Fax Ext:
Tech Email: hostmaster@amazon.com
```

```
Name Name Server: ns1.p31.dynect.net
Name Name Server: ns3.p31.dynect.net
Name Name Server: ns2.p31.dynect.net
Name Name Server: pdns6.ultradns.co.uk
Name Name Server: pdns1.ultradns.net
Name Name Server: ns4.p31.dynect.net
DNSS DNSSEC: unsigned
URL  URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/

For  For more information on WHOIS status codes, please visit:
  ht   https://www.icann.org/resources/pages/epp-status-codes

Mark MarkMonitor Domain Management(TM)
Prot Protecting companies and consumers in a digital world.

Visi Visit MarkMonitor at https://www.markmonitor.com
Cont Contact us at +1.8007459229
In E In Europe, at +44.02032062220
---- ----
```

NETCRAFT

Use our tools to find out what infrastructure and technologies any site is using, which sites are the most popular, how reliable common hosting / OCSP providers are, and to stay safe on the internet

Hosting History

Netblock owner	IP address	OS	Web server	Last seen
PROD IAD	176.32.103.205	unknown	Server	8-Nov-2021
Amazon Technologies Inc. 410 Terry Ave N. Seattle WA US 98109	54.239.28.85	unknown	Server	21-Oct-2021
Amazon.com, Inc. 1918 8th Ave SEATTLE WA US 98101-1244	205.251.242.103	unknown	Server	13-Oct-2021
PROD IAD	176.32.103.205	unknown	Server	3-Oct-2021
Amazon.com, Inc. 1918 8th Ave SEATTLE WA US 98101-1244	205.251.242.103	unknown	Server	21-Sep-2021
PROD IAD	176.32.103.205	unknown	Server	10-Sep-2021
Amazon.com, Inc. 1918 8th Ave SEATTLE WA US 98101-1244	205.251.242.103	unknown	Server	1-Sep-2021
Amazon Technologies Inc. 410 Terry Ave N. Seattle WA US 98109	54.239.28.85	unknown	Server	23-Aug-2021
Amazon.com, Inc. 1918 8th Ave SEATTLE WA US 98101-1244	205.251.242.103	unknown	Server	16-Aug-2021
PROD IAD	176.32.103.205	unknown	Server	4-Aug-2021

Sender Policy Framework

A host's Sender Policy Framework (SPF) describes who can send mail on its behalf. This is done by publishing an SPF record containing a series of **rules**. Each rule consists of a qualifier followed by a specification of which domains to apply this qualifier to. For more information please see **open-spf.org**.

Qualifier	Mechanism	Argument
+ (Pass)	include	spf1.amazon.com
+ (Pass)	include	spf2.amazon.com
+ (Pass)	include	amazonses.com
- (Fail)	all	

Certificate Transparency

Signed Certificate Timestamps (SCTs)

Source	Log	Timestamp	Signature Verification
Certificate	Google Argon 2022 KXm+8J45OSHwVnOfY6V35b5XfZxgCvj5TV0mXCVdx4Q=	2021-10-06 02:59:08	Success
Certificate	DigiCert Nessie 2022 UaOw9f0BeZxWbbg3eI8MpHrMGyfL956IQpoN/tSLBeU=	2021-10-06 02:59:08	Success
Certificate	Cloudflare Nimbus 2022 QcjKsd8iRkoQxqE6CUKHXk4xixsD6+tLx2jwkGKWBvY=	2021-10-06 02:59:08	Success

SSLv3/POODLE

This site does not support the SSL version 3 protocol.

More information about SSL version 3 and the POODLE vulnerability.

Heartbleed

The site did not offer the Heartbeat TLS extension prior to the Heartbleed disclosure, and so was not exploitable.

This test does not exploit the Heartbleed vulnerability but uses information from conventional HTTPS requests. More information about Heartbleed detection.

SSL Certificate Chain

Common name	DigiCert Global Root G2
Organisational unit	www.digicert.com
Organisation	DigiCert Inc
Validity period	From 2013-08-01 to 2038-01-15

↓

Common name	DigiCert Global CA G2
Organisational unit	Not Present
Organisation	DigiCert Inc
Validity period	From 2013-08-01 to 2028-08-01

Site Technology (fetched 16 days ago)

Server-Side

Includes all the main technologies that Netcraft detects as running on the server such as PHP.

Technology	Description	Popular sites using this technology
SSL	A cryptographic protocol providing communication security over the Internet	

Client-Side

Includes all the main technologies that run on the browser (such as JavaScript and Adobe Flash).

Technology	Description	Popular sites using this technology
Local Storage	*No description*	www.roblox.com, www.ebay.co.uk, www.w3schools.com
JavaScript	Widely-supported programming language commonly used to power client-side dynamic content on websites	

Client-Side Scripting Frameworks

Frameworks or libraries allow for easier development of applications by providing an Application Program Interface (API) or a methodology to follow whilst developing.

Technology	Description	Popular sites using this technology
AJAX	*No description*	www.twitch.tv, www.microsoft.com, www.paypal.com
jQuery	A JavaScript library used to simplify the client-side scripting of HTML	www.geeksforgeeks.org, www.xvideos.com, www.amazon.de

E-Commerce

Electronic commerce, commonly known as e-commerce, is the buying and selling of product or service over electronic systems such as the Internet and other computer networks.

Technology	Description	Popular sites using this technology
General Domain Holding	Loading temporary content under a domain name	www.sciencedirect.com, www.dell.com, www.tutorialspoint.com

DMARC

DMARC (Domain-based Message Authentication, Reporting and Conformance) is a mechanism for domain owners to indicate how mail purporting to originate from their domain should be authenticated. It builds on SPF and DKIM, providing a method to set policy and to give reporting of failures. For more information please see dmarc.org.

Raw DMARC record:

```
v=DMARC1;p=quarantine;pct=100;rua=mailto:report@dmarc.amazon.com;ruf=mailto:report@dmarc.amazon.com
```

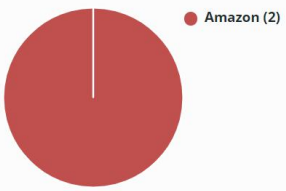
Tag	Field	Value
p=quarantine	Requested handling policy	Quarantine: emails that fail the DMARC mechanism check should be treated by Mail Receivers as suspicious. Depending on the capabilities of the Mail Receiver, this can mean "place into spam folder", "scrutinize with additional intensity", and/or "flag as suspicious".
pct=100	Sampling rate	100% of messages from the Domain Owner's mail stream should have DMARC applied.
rua=mailto:report@dmarc.amazon.com	Reporting URI(s) for aggregate data	report@dmarc.amazon.com
ruf=mailto:report@dmarc.amazon.com	Reporting URI(s) for failure data	report@dmarc.amazon.com

Web Trackers

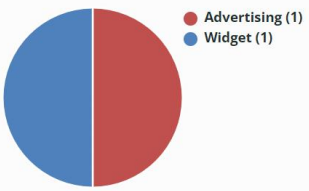
Web Trackers are third-party resources loaded onto a webpage. Trackable resources include social sharing widgets, javascript files, and images. These trackers can be used to monitor individual user behaviour across the web. Data derived from these trackers are primarily used for advertising or analytics purposes.

2 known trackers were identified.

Companies



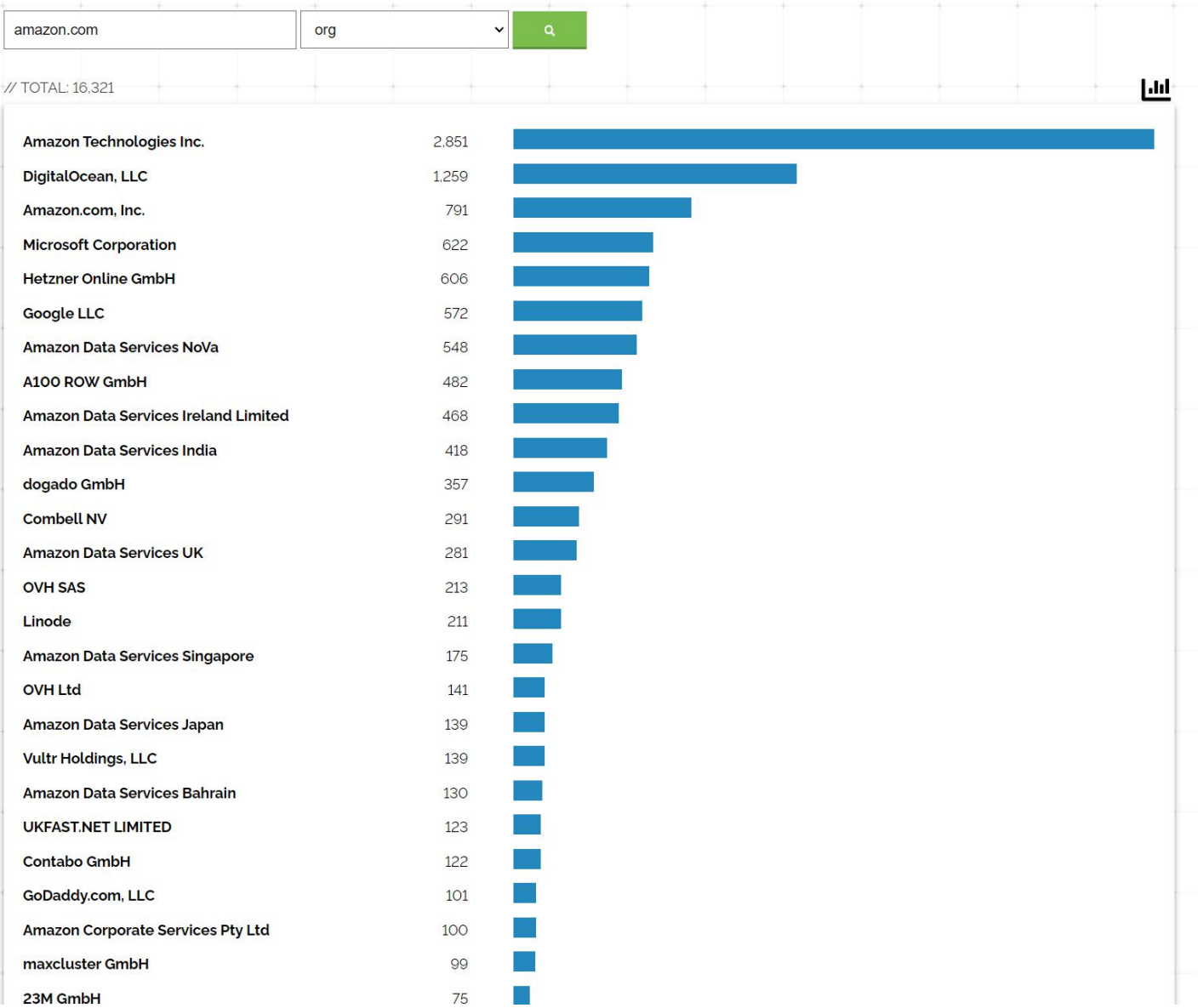
Categories



Company	Primary Category	Tracker	Popular Sites with this Tracker
Amazon	Advertising	Amazon Associate	www.aljazeera.com, www.wunderground.com, www.leparisien.fr
	Widget	Amazonwidget	www.amazon.co.jp, www.amazon.in, www.primevideo.com

SHODAN

Shodan works by requesting connections to every imaginable internet protocol (IP) address on the internet and indexing the information that it gets back from those connection requests. Shodan crawls the web for devices using a global network of computers and servers that are running 24/7



New Service: Keep track of what you have connected to the Internet. Check out **Shodan Monitor**

Startseite

2021-11-16T13:59:53.919727

89.22.118.38
dogado GmbH
Germany, Leipzig

SSL Certificate

Issued By:
|- Common Name:
R3

|- Organization:
Let's Encrypt

Issued To:
|- Common Name:
schoepe-display-v6-kv92f.your-printq.com

Supported SSL Versions:
TLSv1.2, TLSv1.3

Diffie-Hellman Fingerprint:
RFC3526/Oakley Group 14

```
HTTP/1.1 200 OK
Date: Tue, 16 Nov 2021 13:59:53 GMT
Server: Apache/2.4.37 (centos) OpenSSL/1.1.1g
X-Powered-By: PHP/7.4.14
X-Magento-Cache-Control: max-age=86400, public, s-maxage=86400
X-Magento-Tags: store,cms_b,cms_p_7,cms_b_porto_homeslider_1,cms_b_porto_custom_block_for_header,cms_b_por...
```

185.170.104.199

2021-11-16T13:58:07.775857

host-185-170-104-199.dataspace.pl
IPv4 address space for Data Space Sp. z o.o.
Poland, Warsaw

```
HTTP/1.1 302 Found
Date: Tue, 16 Nov 2021 13:58:06 GMT
Content-Type: text/html; charset=UTF-8
Set-Cookie: PHPSESSID=ic2f8teqea4r3hpprdc0msut9v; expires=Fri, 26-Nov-2021 13:58:06 GMT; Max-Age=864000; path=/; domain=185.170.104.199; HttpOnly; SameSite=Lax
Location: https://swederm.com/
Report-...
```

Modern Contempo - Modern Contemporary furniture for homes, offices, and everything else

2021-11-16T13:57:31.811634

107.22.155.41
ec2-107-22-155-41.compute-1.amazonaws.com
Amazon.com, Inc.
United States, Ashburn

cloud

```
HTTP/1.1 200 OK
Date: Tue, 16 Nov 2021 13:57:30 GMT
Server: Apache/2.4.41 (Ubuntu)
Set-Cookie: PHPSESSID=85r8u0434bkhno8a5qg2nb7rdl; expires=Tue, 16-Nov-2021 14:57:30 GMT; Max-Age=3600; path=/; domain=107.22.155.41; HttpOnly; SameSite=Lax
Expires: Mon, 16 Nov 2020 13:57:30 GMT
Cache-Control:...
```

Template Account

2021-11-16T13:57:08.870161

18.210.223.13
ec2-18-210-223-13.compute-1.amazonaws.com
Amazon Technologies Inc.
United States, Ashburn

cloud

```
HTTP/1.1 200 OK
Cache-Control: private
Content-Type: text/html; charset=utf-8
Server: Microsoft-IIS/10.0
Set-Cookie: ASP.NET_SessionId=lrfeyczjg3ky0cxckwonly2x; path=/; HttpOnly; SameSite=Lax
Content-Security-Policy: object-src 'none'; script-src 'self' 'unsafe-inline' 'unsafe-eval'        ...
```

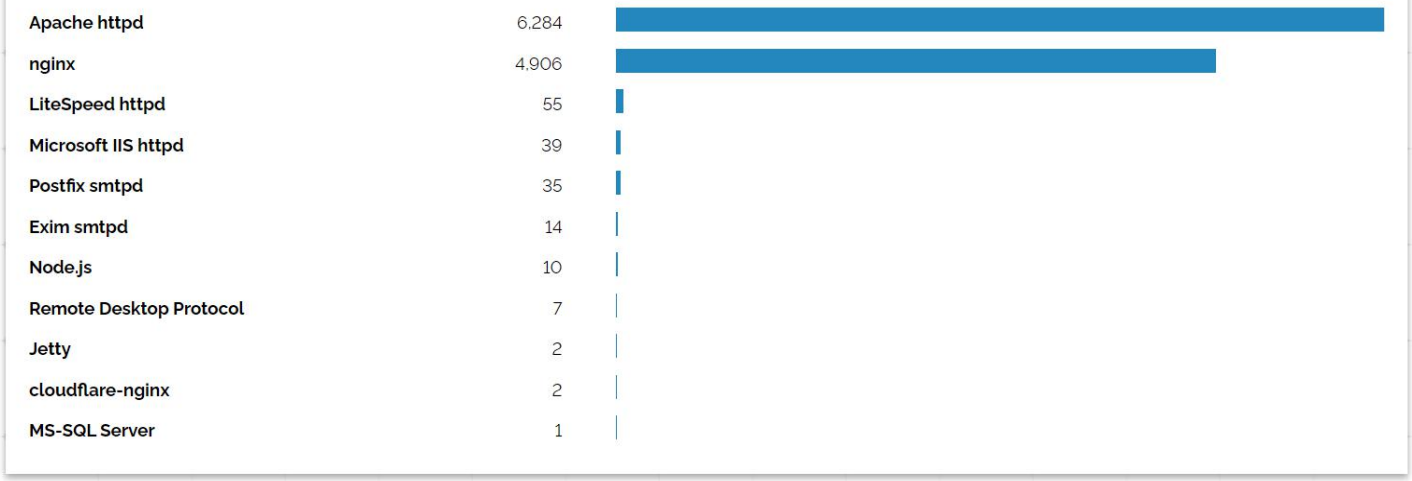
amazon.com | port

// TOTAL: 16,320

443	9,796
80	5,160
8080	409
8181	212
8443	130
9001	128
25	77
8081	55
81	35
8888	27
8000	26
9000	23
10554	16
10443	15
53	14
8880	14
20000	12
444	10

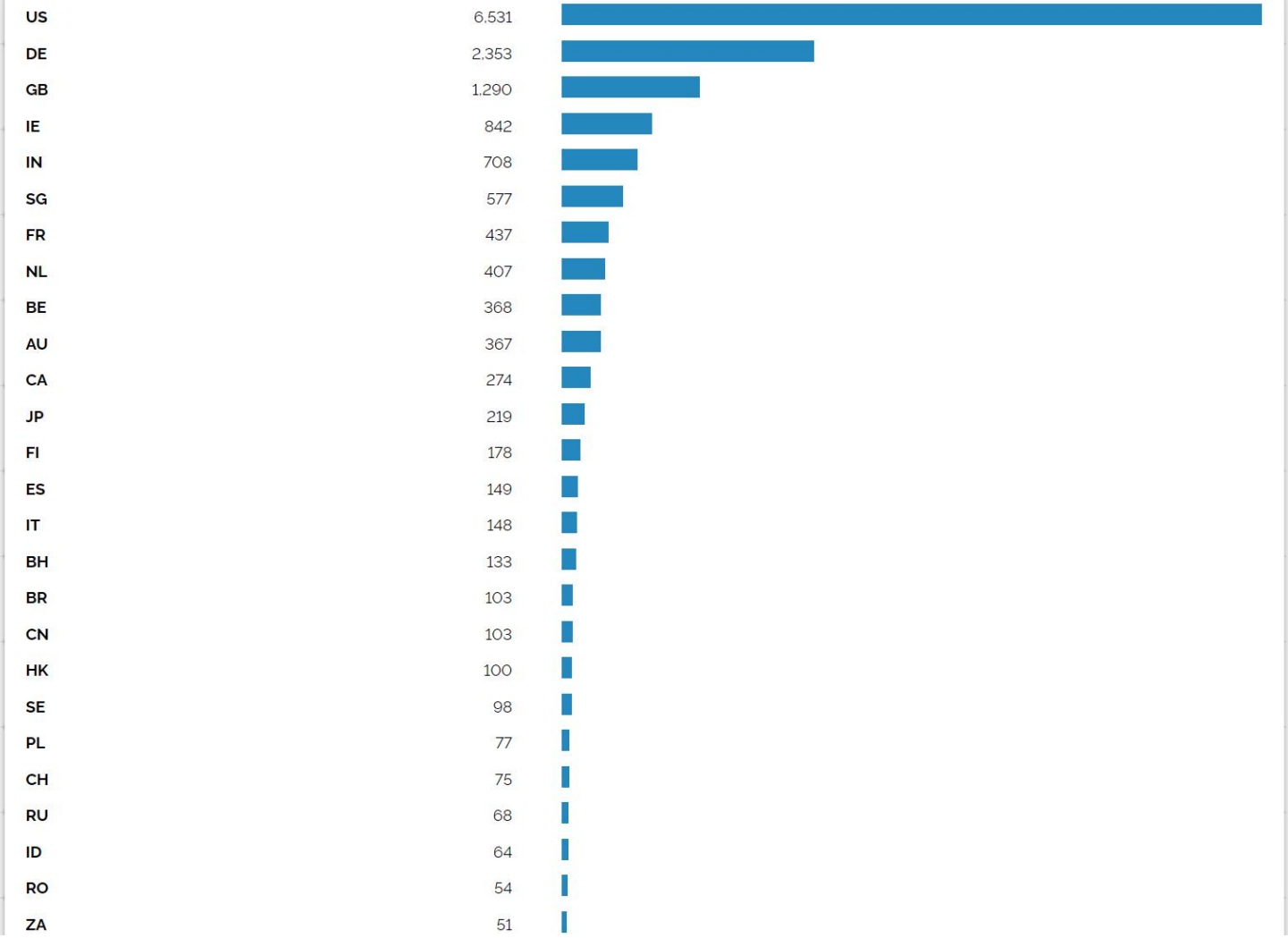
amazon.com | product

// TOTAL: 16,314



amazon.com | country

// TOTAL: 16,315



Information Gathered from dnsdumpster.com

DNS Servers

ns4.p31.dynect.net.	204.13.251.31 ns4.p31.dynect.net	DYNDNS United States
ns2.p31.dynect.net.	204.13.250.31 ns2.p31.dynect.net	DYNDNS United States
pdns6.ultradns.co.uk.	204.74.115.1 pdns6.ultradns.co.uk	ULTRADNS United States
ns1.p31.dynect.net.	208.78.70.31 ns1.p31.dynect.net	DYNDNS United States
ns3.p31.dynect.net.	208.78.71.31 ns3.p31.dynect.net	DYNDNS United States
pdns1.ultradns.net.	204.74.108.1 pdns1.ultradns.net	NEUSTAR-AS6 United States

MX Records

amazon-smtp.amazon.com	52.94.124.8 smtp-fw-7003.amazon.com	AMAZON-02 United States

TXT Records

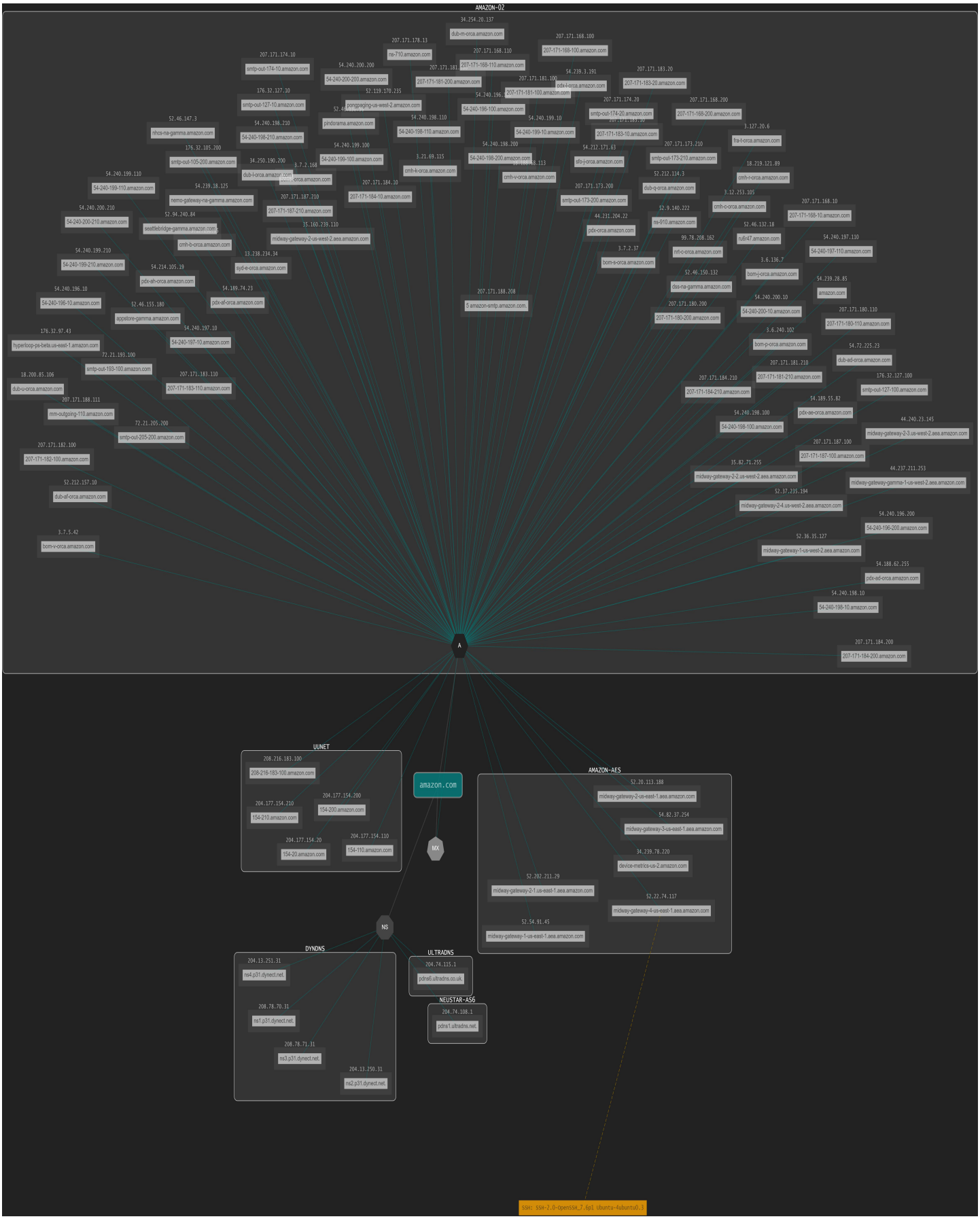
"google-site-verification=14WGW2MdNMxchG8PlinF7LgqqE0OwwHqOq0HKhb7rDQ"
"apple-domain-verification=dVkKZnu17XS0EN2X"
"MS=4B600B22799EB2CAC0D8FF0A3A3CAECA5EE2BF3A"
"facebook-domain-verification=d9u57u52gylohx845ogo1axzpywpmq
"wrikeverification=MzI3NzM2ODo2NDk5MjE4NjQ2MWJmOTEwMGMxM 2MzNzJmNWJlY2U5ZDU4MmVlNzQ2NWU4MTY5OWJjMjlmYjQ4Mjc5M2JiMzky"
"cisco-ci-domain-verification=4d609172fa2701a94410a4d6a857713b7d0931a92e9761d2428b37432d89eda"
"spf2.0/pra include:spf1.amazon.com include:spf2.amazon.com include:amazonses.com -all"
"v=spf1 include:spf1.amazon.com include:spf2.amazon.com include:amazonses.com -all"
"pardot326621=b26a7b44d7c73d119ef9dfd1a24d93c77d583ac50ba4ecedd899a9134734403b"

DNS Servers

ns1.p31.dynect.net.	208.78.70.31 ns1.p31.dynect.net	DYNDNS United States
ns2.p31.dynect.net.	204.13.250.31 ns2.p31.dynect.net	DYNDNS United States
ns3.p31.dynect.net.	208.78.71.31 ns3.p31.dynect.net	DYNDNS United States
ns4.p31.dynect.net.	204.13.251.31 ns4.p31.dynect.net	DYNDNS United States
pdns1.ultradns.net.	204.74.108.1 pdns1.ultradns.net	NEUSTAR-AS6 United States
pdns6.ultradns.co.uk.	204.74.115.1 pdns6.ultradns.co.uk	ULTRADNS United States

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

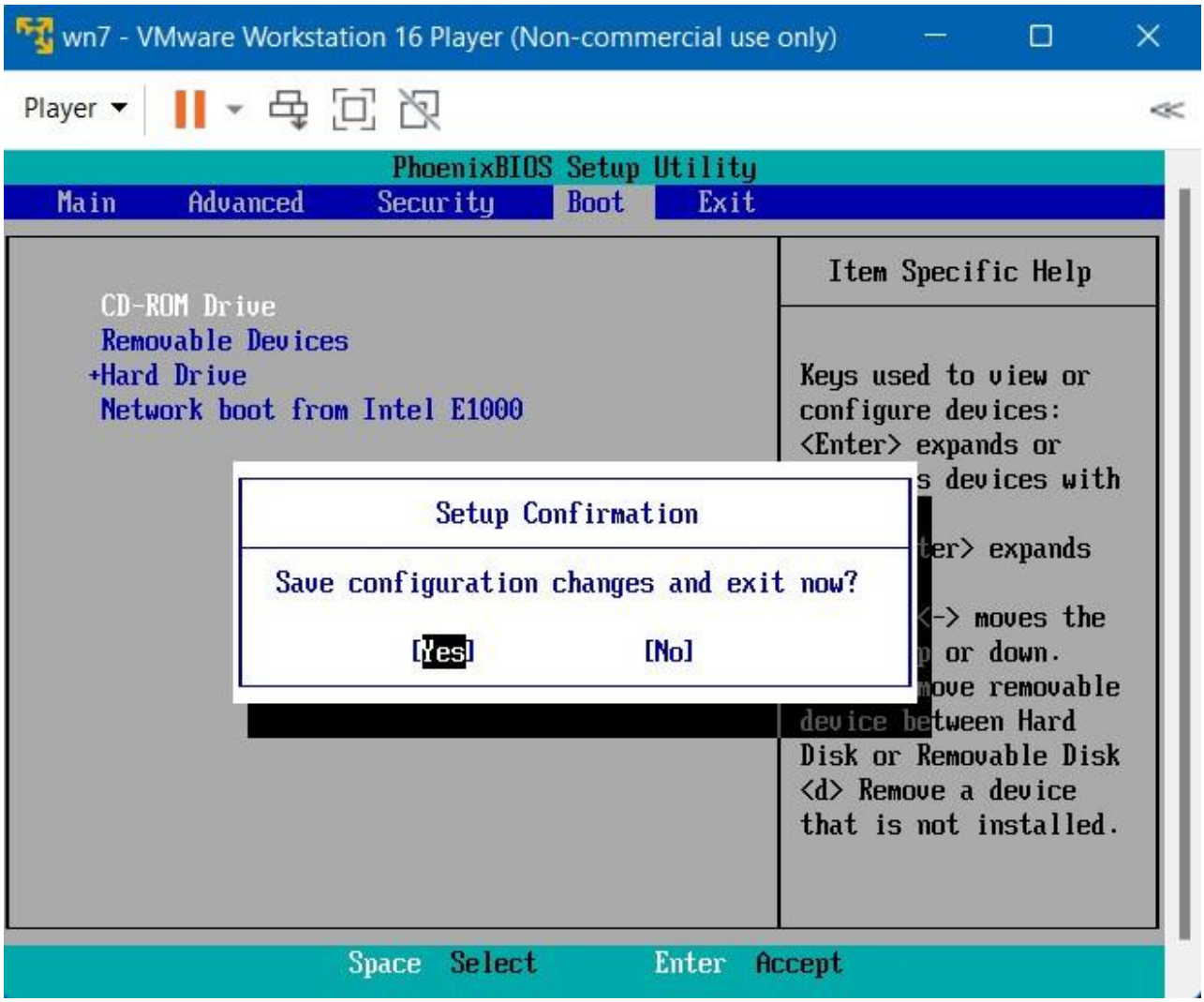
amazon.com	54.239.28.85	AMAZON-02 United States
midway-gateway-2-us-east-1.ana.amazon.com smtp: [illegible] smtps: [illegible]	52.20.113.188 ec2-52-20-113-188.compute-1.amazonaws.com	AMAZON-AES United States
54-240-196-188.amazon.com	54.240.196.188 54-240-196-188.amazon.com	AMAZON-02 United States
cmh-b-orca.amazon.com	3.12.190.15 ec2-3-12-190-15.us-east-2.compute.amazonaws.com	AMAZON-02 United States
154-33.amazon.com	204.177.154.33	UUNET United States
smtp-out-205-200.amazon.com	72.21.205.200 smtp-out-205-200.amazon.com	AMAZON-02 United States
dub-ed-orca.amazon.com	54.72.225.23 ec2-54-72-225-23.eu-west-1.compute.amazonaws.com	AMAZON-02 Ireland
cmh-b-orca.amazon.com	3.21.69.115 ec2-3-21-69-115.us-east-2.compute.amazonaws.com	AMAZON-02 United States
midway-gateway-3-us-east-1.ana.amazon.com smtp: [illegible] smtps: [illegible]	54.82.37.254 ec2-54-82-37-254.compute-1.amazonaws.com	AMAZON-AES United States
207-171-180-200.amazon.com	207.171.180.200 207-171-180-200.amazon.com	AMAZON-02 United States
54-240-196-10.amazon.com	54.240.196.10 54-240-196-10.amazon.com	AMAZON-02 United States
midway-gateway-2-3.us-west-2.ana.amazon.com	44.240.23.165 ec2-44-240-23-165.us-west-2.compute.amazonaws.com	AMAZON-02 United States


AMAZON-02
34.254.20.137
dub-m-orca.amazon.com
207.171.178.13
ns-710.amazon.com
207.171.168.100
207-171-168-100.amazon.com
207.171.168.110
207-171-168-110.amazon.com
207.171.174.10
smtp-out-174-10.amazon.com
54.240.200.200
54-240-200-200.amazon.com
207.171.181.200
207-171-181-200.amazon.com
54.239.3.191
pdx-l-orca.amazon.com
207.171.183.20
207-171-183-20.amazon.com
207.171.181.100
207-171-181-100.amazon.com
176.32.127.10
smtp-out-127-10.amazon.com
52.119.170.235
pongpaging-us-west-2.amazon.com
54.240.196.100
54-240-196-100.amazon.com
207.171.174.20
smtp-out-174-20.amazon.com
207.171.168.200
207-171-168-200.amazon.com
52.46.147.3
nhcs-na-gamma.amazon.com
pindorama.amazon.com
54.240.198.110
54-240-198-110.amazon.com
54.240.199.10
54-240-199-10.amazon.com
207.171.183.10
207-171-183-10.amazon.com
3.127.20.6
fra-t-orca.amazon.com
54.240.198.210
54-240-198-210.amazon.com
54.240.199.100
54-240-199-100.amazon.com
54.240.198.200
54-240-198-200.amazon.com
54.212.171.63
sfo-j-orca.amazon.com
207.171.173.210
smtp-out-173-210.amazon.com
176.32.105.200
smtp-out-105-200.amazon.com
34.250.190.200
3.7.2.168
dub-l-orca.amazon.com
3.21.69.115
cmh-k-orca.amazon.com
cmh-v-orca.amazon.com
18.219.121.89
cmh-r-orca.amazon.com
54.240.199.110
54-240-199-110.amazon.com
54.239.18.125
nemo-gateway-na-gamma.amazon.com
207.171.184.10
207-171-184-10.amazon.com
52.212.114.3
dub-q-orca.amazon.com
207.171.173.200
smtp-out-173-200.amazon.com
3.12.253.105
cmh-o-orca.amazon.com
207.171.168.10
207-171-168-10.amazon.com
54.240.200.210
54-240-200-210.amazon.com
52.94.240.84
seattlebridge-gamma.amazon.com
207.171.187.210
207-171-187-210.amazon.com
52.9.140.222
ns-910.amazon.com
44.231.204.22
pdx-orca.amazon.com
35.160.239.110
midway-gateway-2-us-west-2.aea.amazon.com
52.46.132.18
ru6r47.amazon.com
99.78.208.162
nrt-c-orca.amazon.com
54.240.197.110
54-240-197-110.amazon.com
3.7.2.37
bom-s-orca.amazon.com
3.6.136.7
bom-j-orca.amazon.com
54.240.199.210
54-240-199-210.amazon.com
13.238.234.34
syd-e-orca.amazon.com
52.46.150.132
dss-na-gamma.amazon.com
54.239.28.85
amazon.com
54.214.105.19
pdx-ah-orca.amazon.com
54.240.200.10
54-240-200-10.amazon.com
54.240.196.10
54-240-196-10.amazon.com
54.189.74.23
pdx-af-orca.amazon.com
207.171.188.208
5.amazon-smtp.amazon.com.
207.171.180.200
207-171-180-200.amazon.com
207.171.180.110
207-171-180-110.amazon.com
52.46.155.180
appstore-gamma.amazon.com
176.32.97.43
hyperloop-ps-beta.us-east-1.amazon.com
54.240.197.10
54-240-197-10.amazon.com
3.6.240.102
bom-p-orca.amazon.com
54.72.225.23
dub-ad-orca.amazon.com
72.21.193.100
smtp-out-193-100.amazon.com
207.171.181.210
207-171-181-210.amazon.com
18.200.85.106
dub-u-orca.amazon.com
207.171.183.110
207-171-183-110.amazon.com
207.171.184.210
207-171-184-210.amazon.com
176.32.127.100
smtp-out-127-100.amazon.com
207.171.188.111
mm-outgoing-110.amazon.com
54.189.55.82
pdx-ae-orca.amazon.com
54.240.198.100
54-240-198-100.amazon.com
44.240.23.145
midway-gateway-2-3.us-west-2.aea.amazon.com
72.21.205.200
smtp-out-205-200.amazon.com
207.171.187.100
207-171-187-100.amazon.com
207.171.182.100
207-171-182-100.amazon.com
35.82.71.255
midway-gateway-2-2.us-west-2.aea.amazon.com
44.237.211.253
midway-gateway-gamma-1-us-west-2.aea.amazon.com
52.212.157.10
dub-af-orca.amazon.com
52.37.235.194
midway-gateway-2-4.us-west-2.aea.amazon.com
54.240.196.200
54-240-196-200.amazon.com
3.7.5.42
bom-v-orca.amazon.com
52.36.35.127
midway-gateway-1-us-west-2.aea.amazon.com
54.188.62.255
pdx-ad-orca.amazon.com
54.240.198.10
54-240-198-10.amazon.com
A
207.171.184.200
207-171-184-200.amazon.com
UUNET
208.216.183.100
208-216-183-100.amazon.com
204.177.154.210
154-210.amazon.com
204.177.154.200
154-200.amazon.com
204.177.154.20
154-20.amazon.com
204.177.154.110
154-110.amazon.com
amazon.com
MX
AMAZON-AES
52.20.113.188
midway-gateway-2-us-east-1.aea.amazon.com
54.82.37.254
midway-gateway-3-us-east-1.aea.amazon.com
34.239.78.220
device-metrics-us-2.amazon.com
52.202.211.29
midway-gateway-2-1.us-east-1.aea.amazon.com
52.22.74.117
midway-gateway-4-us-east-1.aea.amazon.com
52.54.91.45
midway-gateway-1-us-east-1.aea.amazon.com
NS
DYNDNS
204.13.251.31
ns4.p31.dynect.net.
208.78.70.31
ns1.p31.dynect.net.
208.78.71.31
ns3.p31.dynect.net.
204.13.250.31
ns2.p31.dynect.net.
ULTRADNS
204.74.115.1
pdns6.ultradns.co.uk.
NEUSTAR-AS6
204.74.108.1
pdns1.ultradns.net.
SSH: SSH-2.0-OpenSSH_7.6p1 Ubuntu-4ubuntu0.3

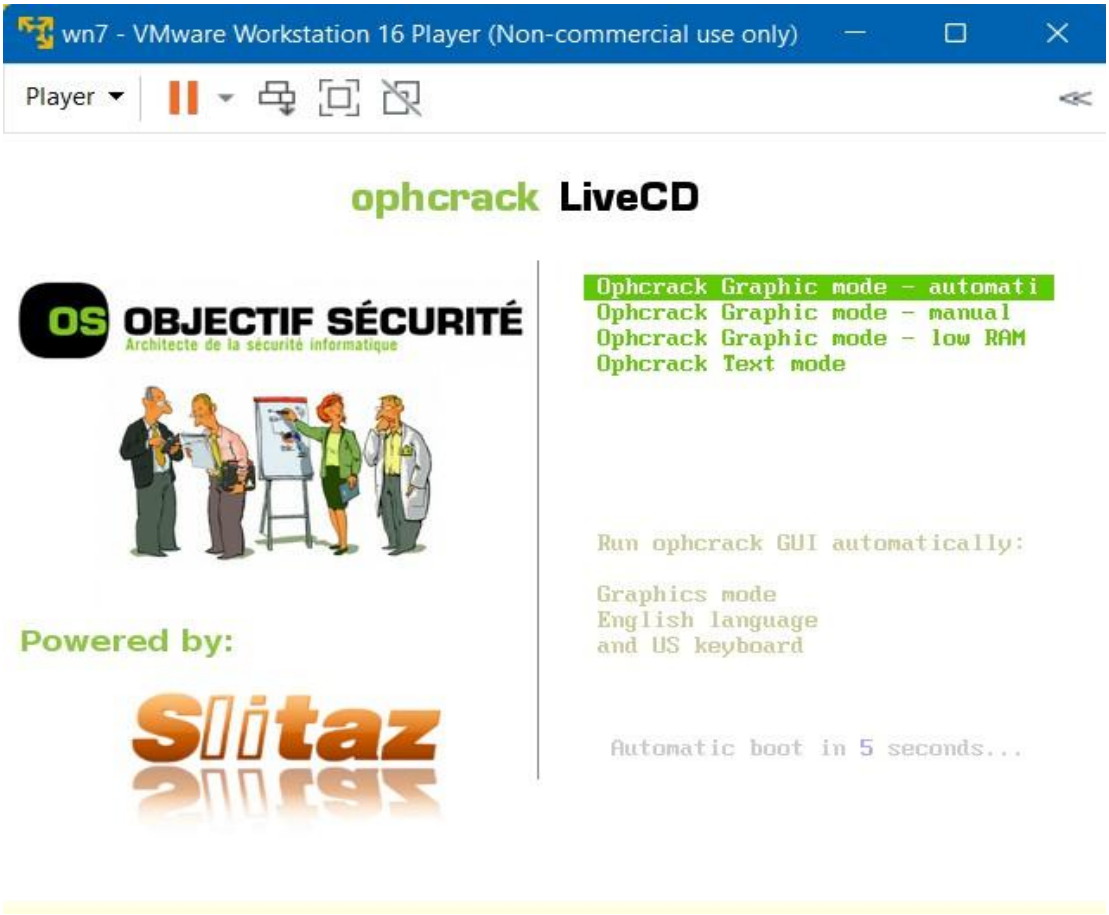
Q2. Try to bypass the Windows 7 machine password by using ophcrack tool and change the password from command prompt without knowing old password.

ANSWER

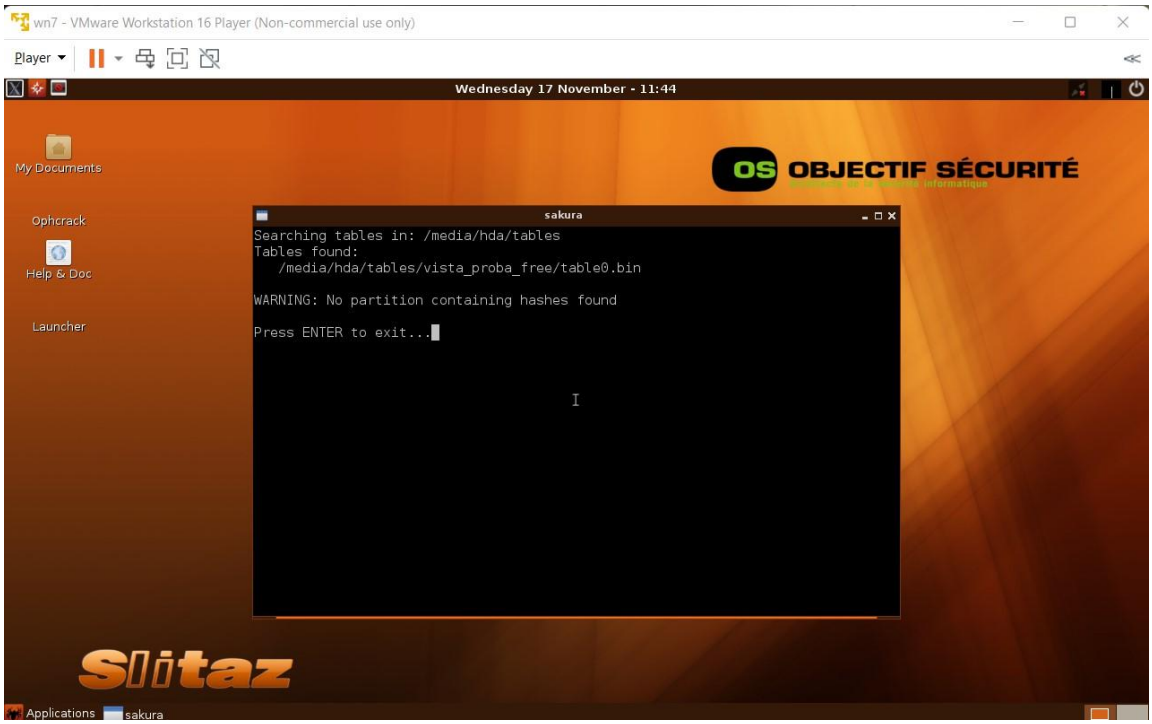
Step 1- Download ophcrack from official website extract move the files to the CD-ROM and Take CD-Rom Drive to first priority in boot option save and run.



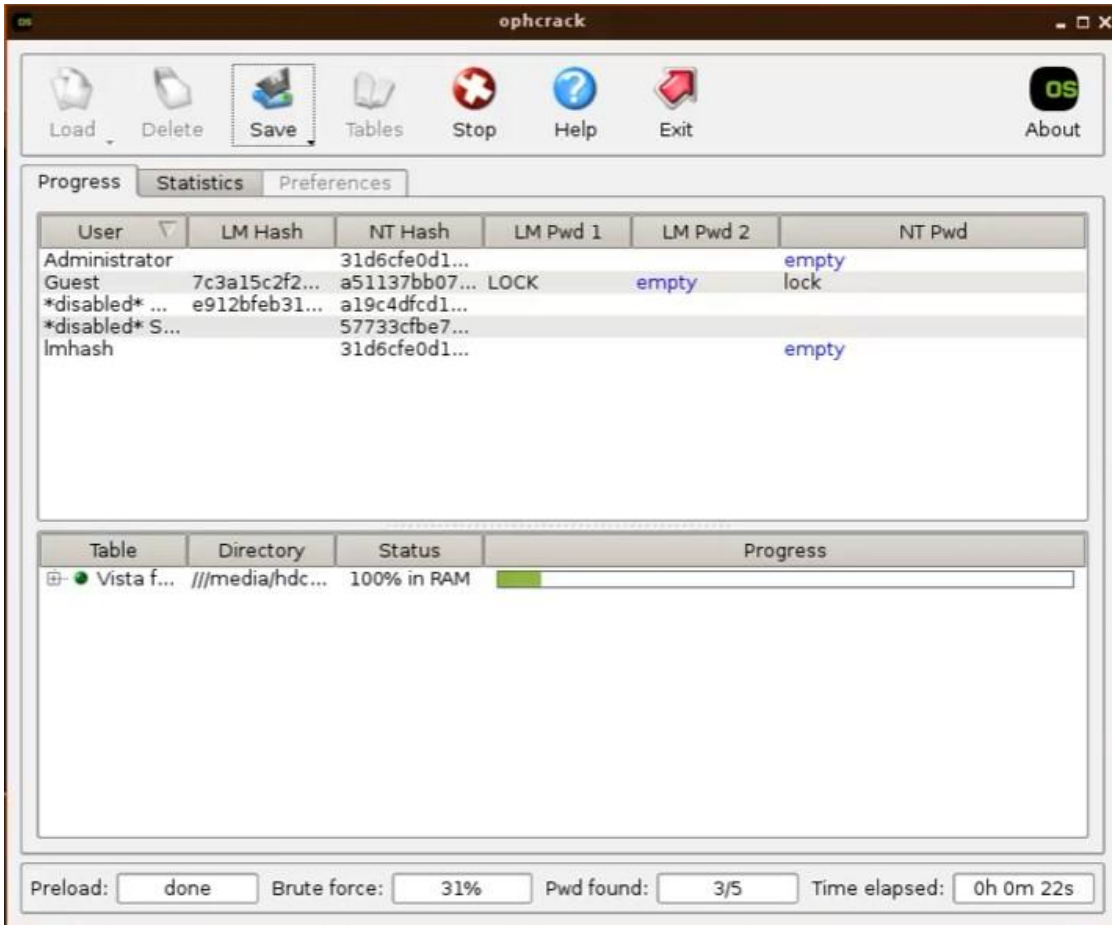
STEP 2 - Select automatic and leave it to boot and load automatically



STEP 3 - It will boot into ophcrack and start to crack hash outomatically

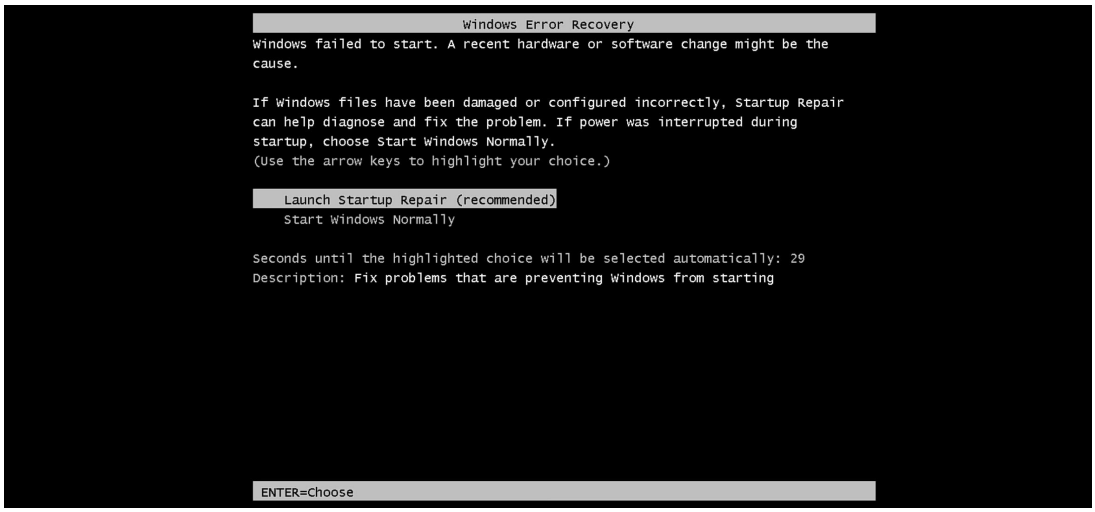


`**STEP 4 -** After Cracking the hash it will displays the password

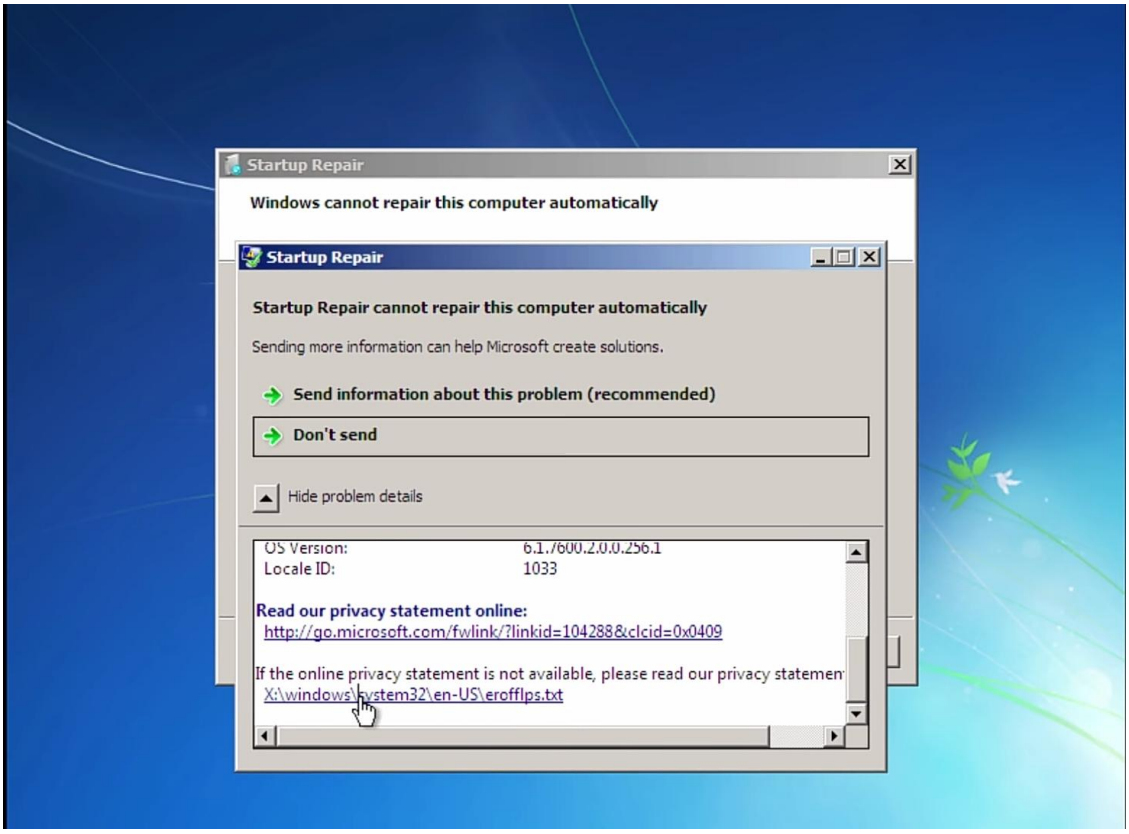


Another method to reset password without knowing

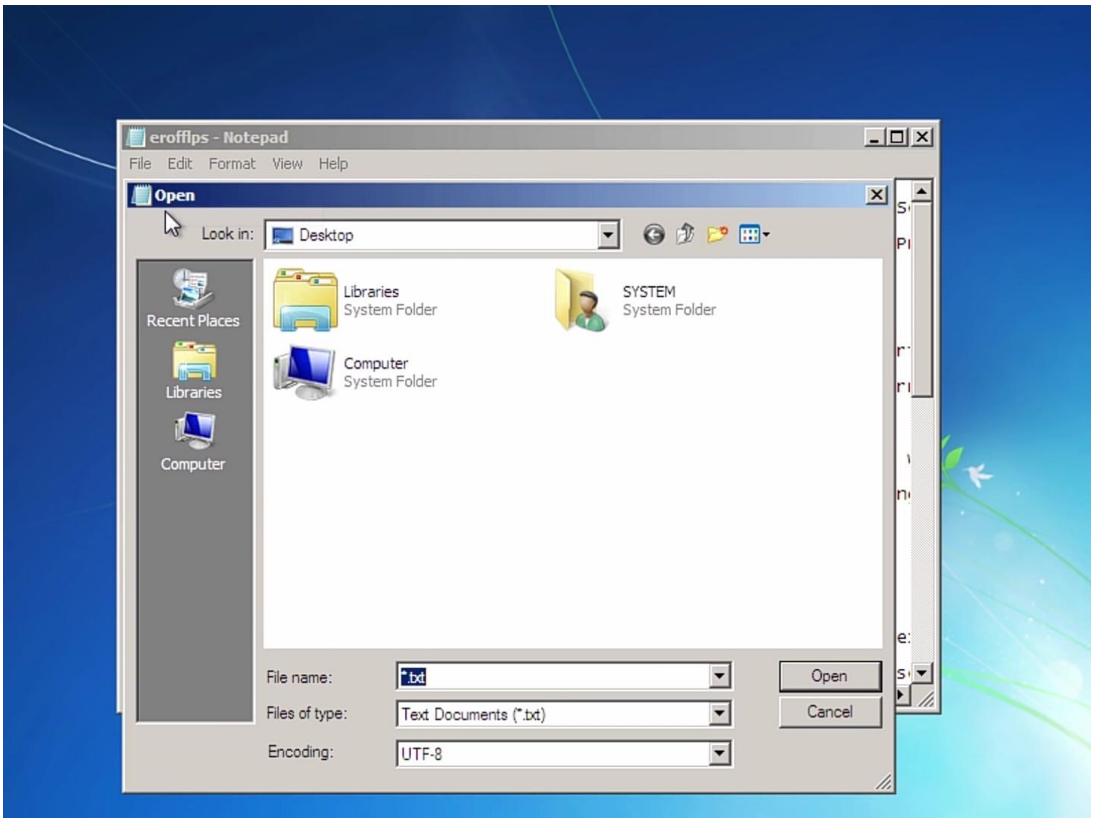
Step 1:-



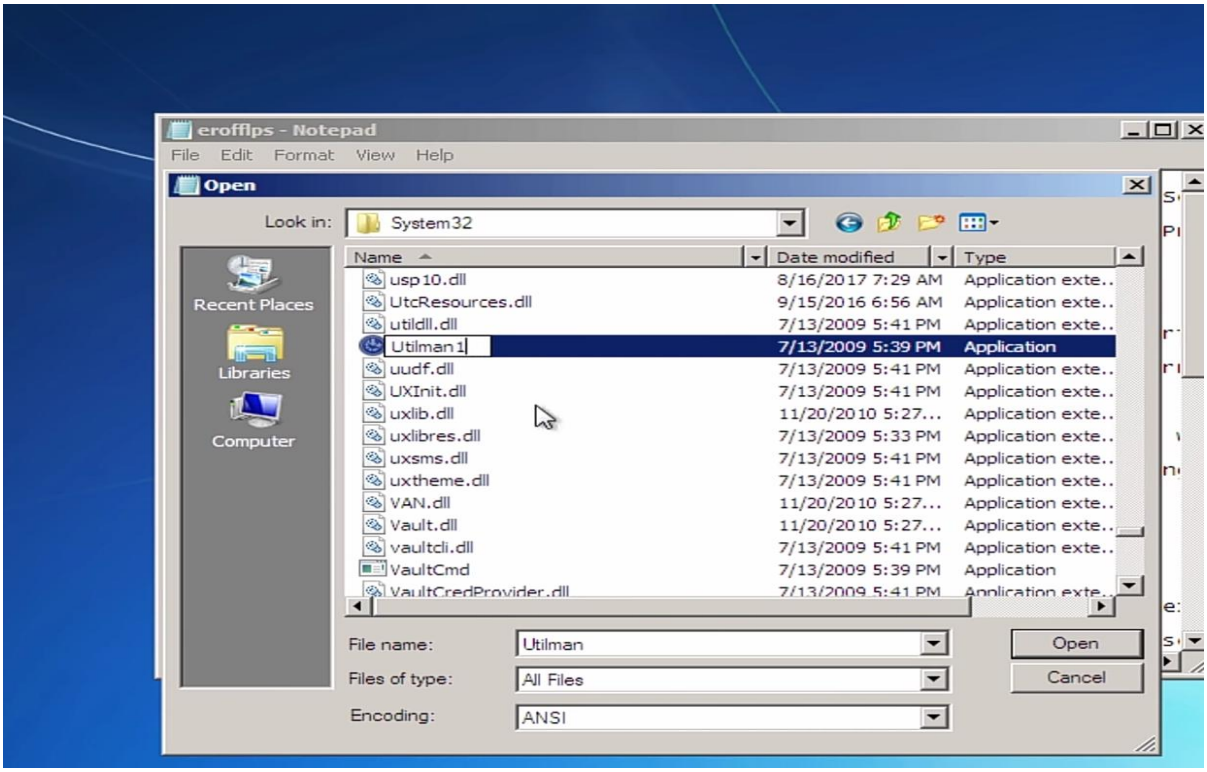
Step2:-


Startup Repair
Windows cannot repair this computer automatically
Startup Repair
Startup Repair cannot repair this computer automatically
Sending more information can help Microsoft create solutions.
Send information about this problem (recommended)
Don't send
Hide problem details
OS Version: 6.1.7600.2.0.0.256.1
Locale ID: 1033
Read our privacy statement online:
http://go.microsoft.com/fwlink/?linkid=104288&clcid=0x0409
If the online privacy statement is not available, please read our privacy statemen
X:\windows\system32\en-US\erofflps.txt

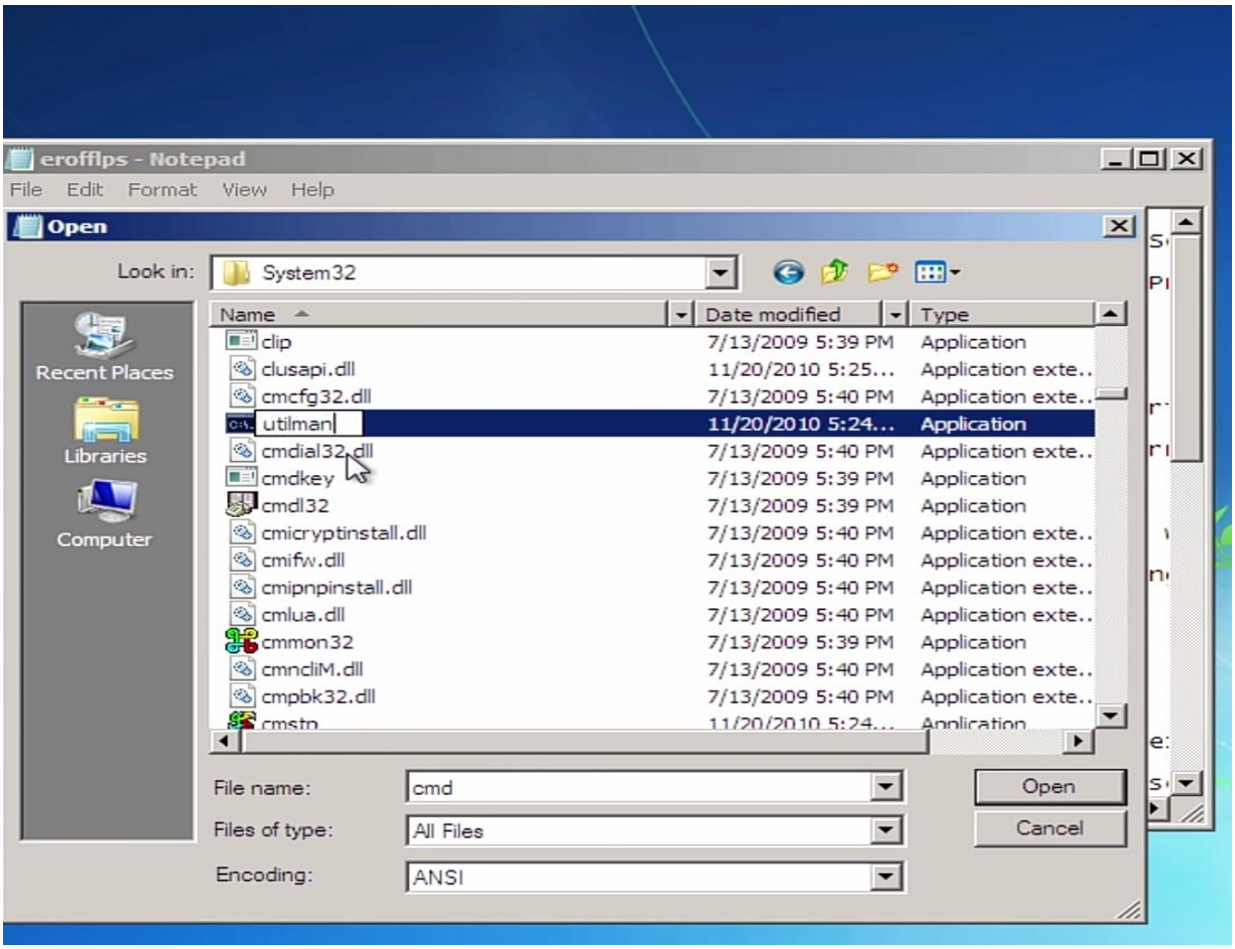
Step 3:-


erofflps - Notepad
File Edit Format View Help
Open
Look in: Desktop
Recent Places
Libraries
Computer
Libraries
System Folder
SYSTEM
System Folder
Computer
System Folder
File name: *.txt
Files of type: Text Documents (*.txt)
Encoding: UTF-8
Open
Cancel

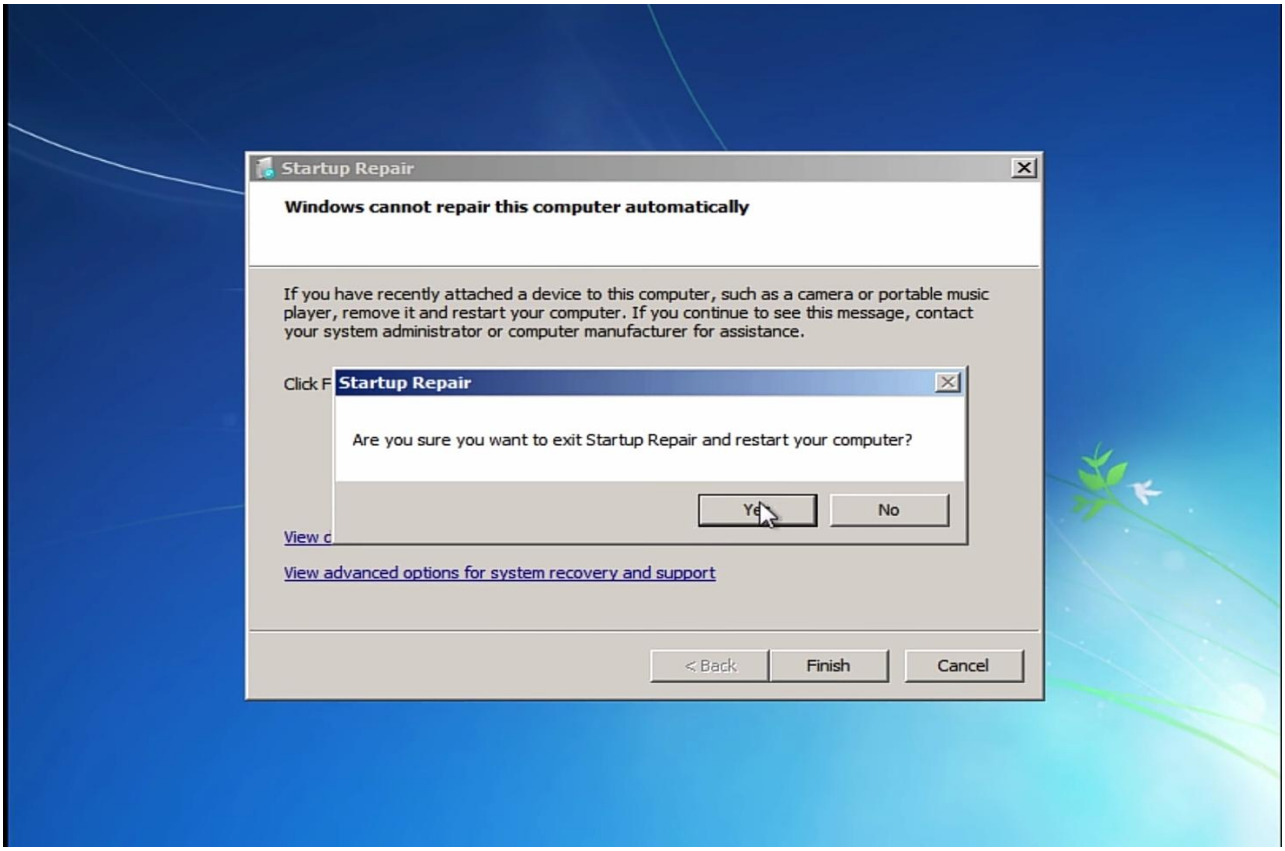
Step 4:-


erofflps - Notepad
File Edit Format View Help
Open
Look in: System32
Recent Places
Libraries
Computer
Name
Date modified
Type
usp10.dll 8/16/2017 7:29 AM Application exte..
UtcResources.dll 9/15/2016 6:56 AM Application exte..
utildll.dll 7/13/2009 5:41 PM Application exte..
Utilman1 7/13/2009 5:39 PM Application
uudf.dll 7/13/2009 5:41 PM Application exte..
UXInit.dll 7/13/2009 5:41 PM Application exte..
uxlib.dll 11/20/2010 5:27... Application exte..
uxlibres.dll 7/13/2009 5:33 PM Application exte..
uxsms.dll 7/13/2009 5:41 PM Application exte..
uxtheme.dll 7/13/2009 5:41 PM Application exte..
VAN.dll 11/20/2010 5:27... Application exte..
Vault.dll 11/20/2010 5:27... Application exte..
vaultcli.dll 7/13/2009 5:41 PM Application exte..
VaultCmd 7/13/2009 5:39 PM Application
File name: Utilman
Files of type: All Files
Encoding: ANSI
Open
Cancel

Step 5:-

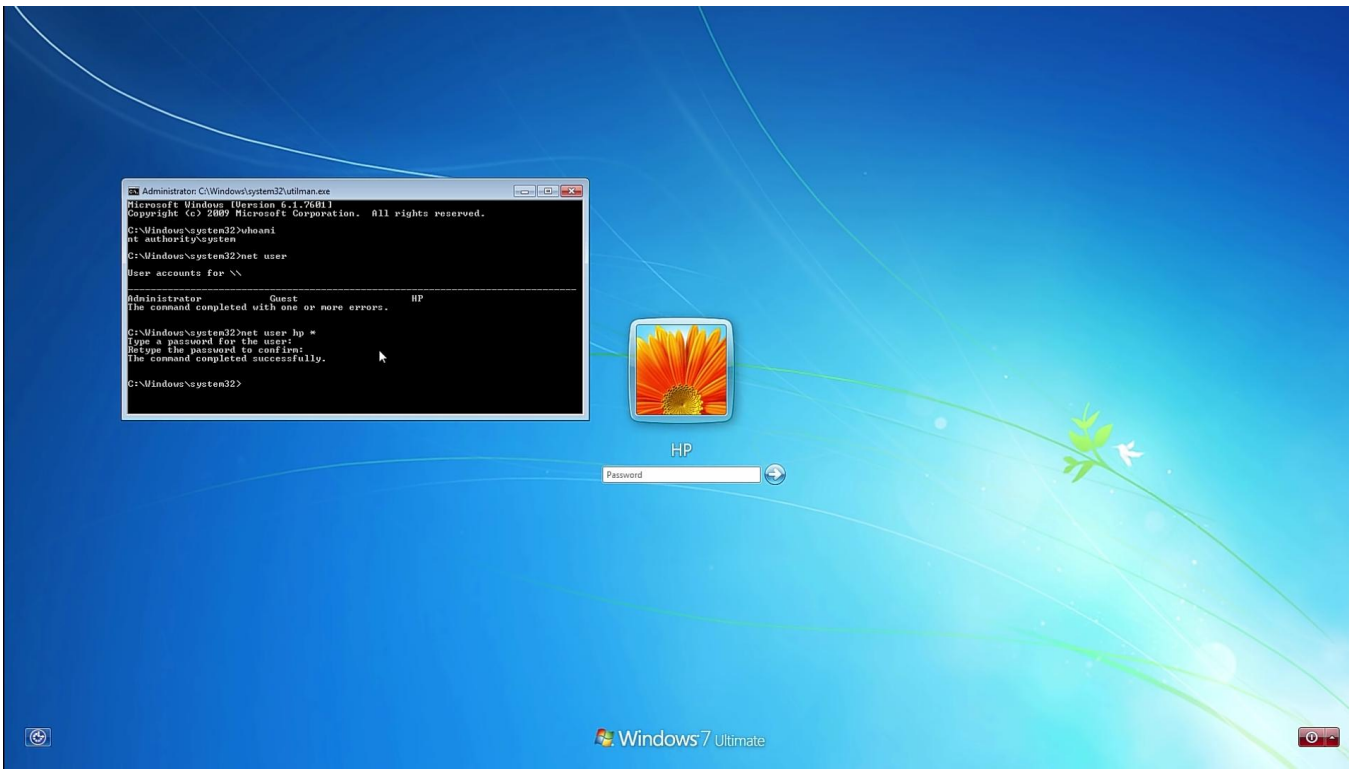

erofflps - Notepad
File Edit Format View Help
Open
Look in: System32
Recent Places
Libraries
Computer
Name
Date modified
Type
clip 7/13/2009 5:39 PM Application
clusapi.dll 11/20/2010 5:25... Application exte..
cmcfg32.dll 7/13/2009 5:40 PM Application exte..
utilman 11/20/2010 5:24... Application
cmdial32.dll 7/13/2009 5:40 PM Application exte..
cmdkey 7/13/2009 5:39 PM Application
cmdl32 7/13/2009 5:39 PM Application
cmicryptinstall.dll 7/13/2009 5:40 PM Application exte..
cmifw.dll 7/13/2009 5:40 PM Application exte..
cmipnpinstall.dll 7/13/2009 5:40 PM Application exte..
cmlua.dll 7/13/2009 5:40 PM Application exte..
cmmon32 7/13/2009 5:39 PM Application
cmncliM.dll 7/13/2009 5:40 PM Application exte..
cmpbk32.dll 7/13/2009 5:40 PM Application exte..
File name: cmd
Files of type: All Files
Encoding: ANSI
Open
Cancel

Step 6:-


Startup Repair
Windows cannot repair this computer automatically
If you have recently attached a device to this computer, such as a camera or portable music player, remove it and restart your computer. If you continue to see this message, contact your system administrator or computer manufacturer for assistance.
Click F
Startup Repair
Are you sure you want to exit Startup Repair and restart your computer?
Ye
No
View d
View advanced options for system recovery and support
< Back
Finish
Cancel

Step 7:-


HP
Password
Windows 7 Ultimate


Administrator: C:\Windows\system32\utilman.exe
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.
C:\Windows\system32>whoami
nt authority\system
C:\Windows\system32>net user
User accounts for \\
Administrator Guest HP
The command completed with one or more errors.
C:\Windows\system32>net user hp *
Type a password for the user:
Retype the password to confirm:
The command completed successfully.
C:\Windows\system32>
HP
Password
Windows 7 Ultimate

Step 8:-

Q3) Use Tetrabit virus maker Tool (Download from Internet) to create a virus and inject in to Virtual systemand perform destruction program as per your wish and write a document along with screenshots andsuggest the preventive measures to avoid this malware affect.

Hacker Machine : Windows 7 / Windows 10
Victim machine : Windows XP / Windows 7

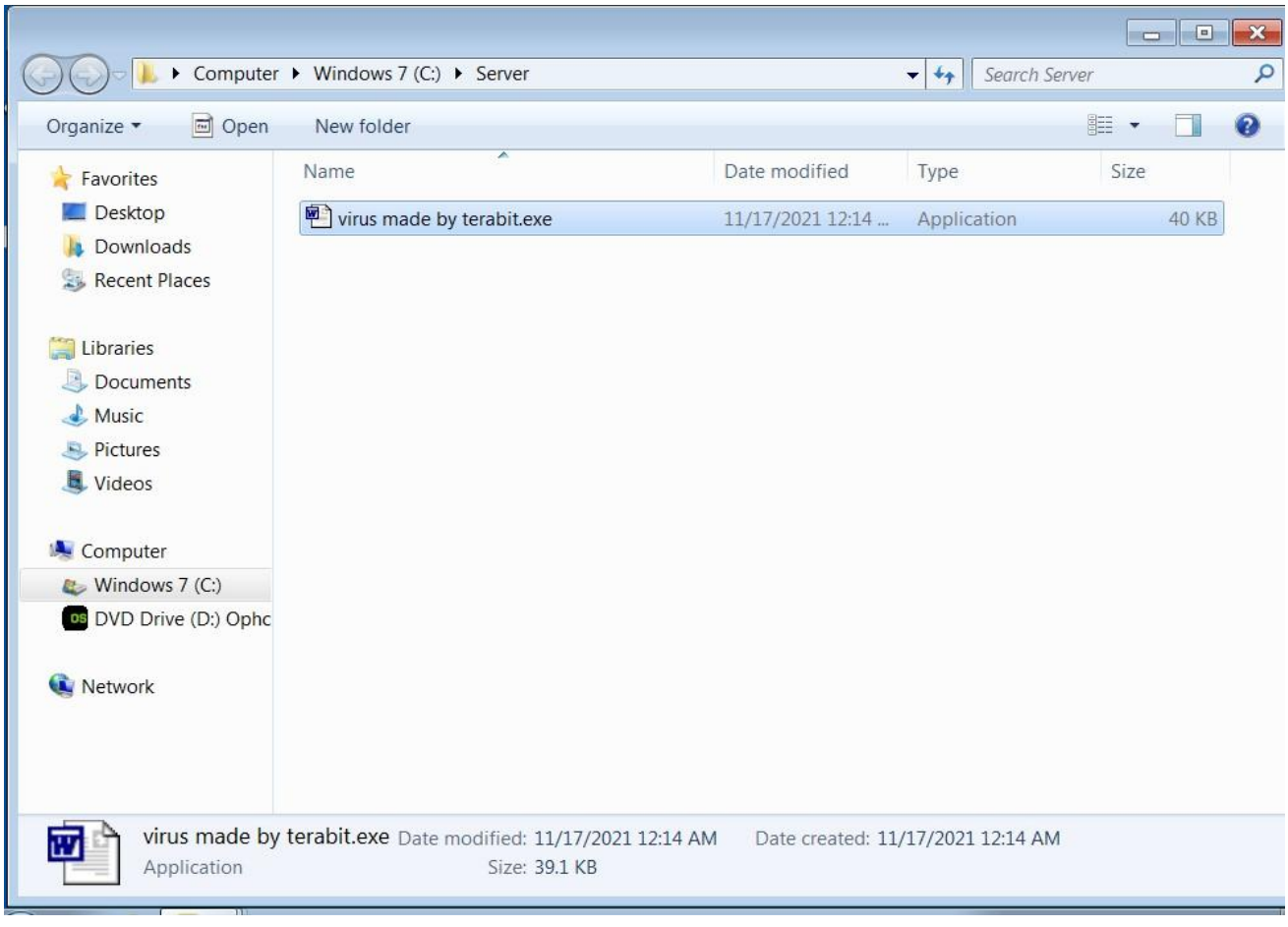
TERABIT VIRUS MAKER

STEP 1:

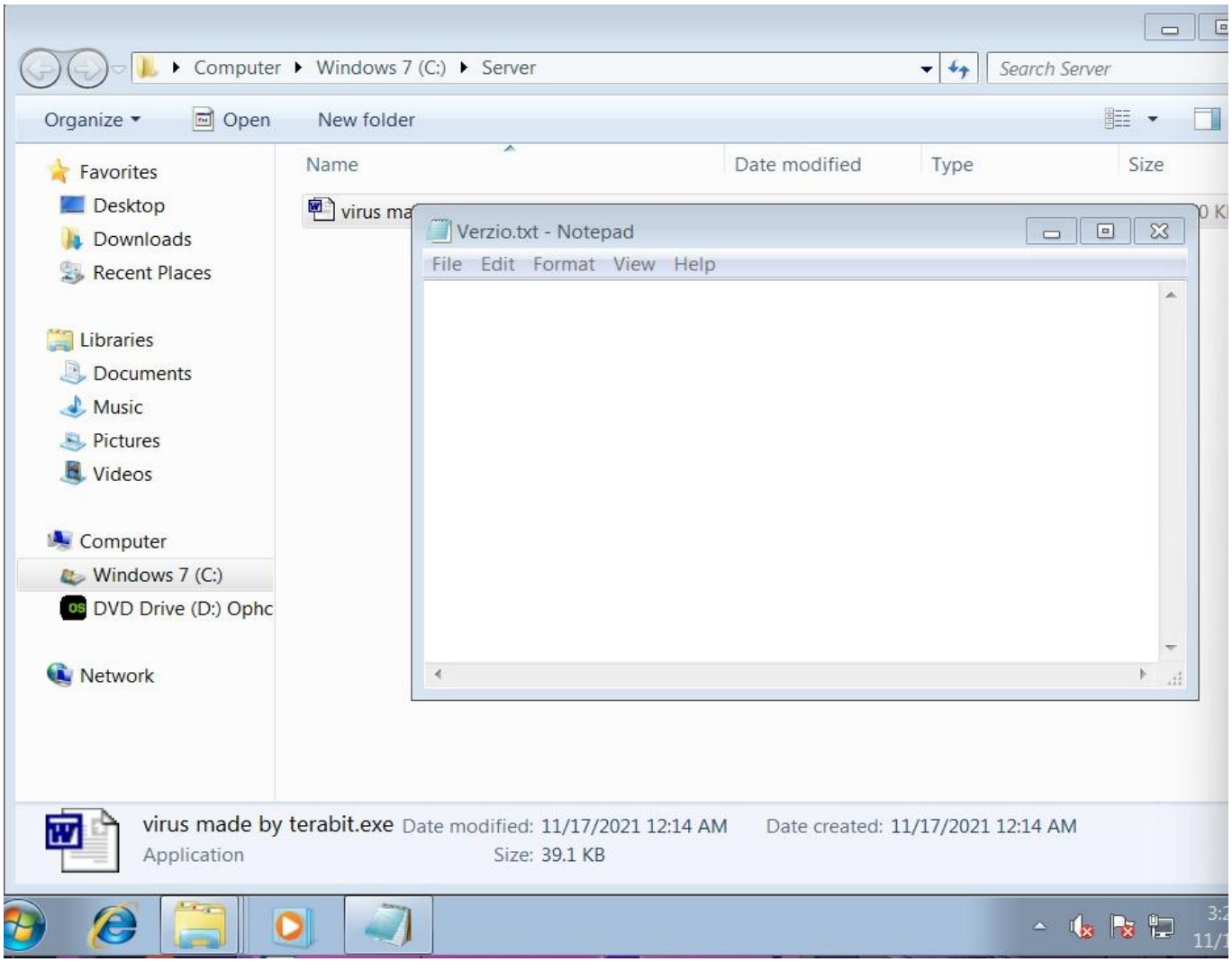
Select the options and click Create Virus , It will create exe file.

STEP 2:

Now you can send this file to the victim and make him to execute the file



STEP 3:-
Here I bind the verzio.txt with the virus. When victim tries to execute the virus , the verzio.txt will open by this we can trick the users.



PREVENTIVE MEASURES:

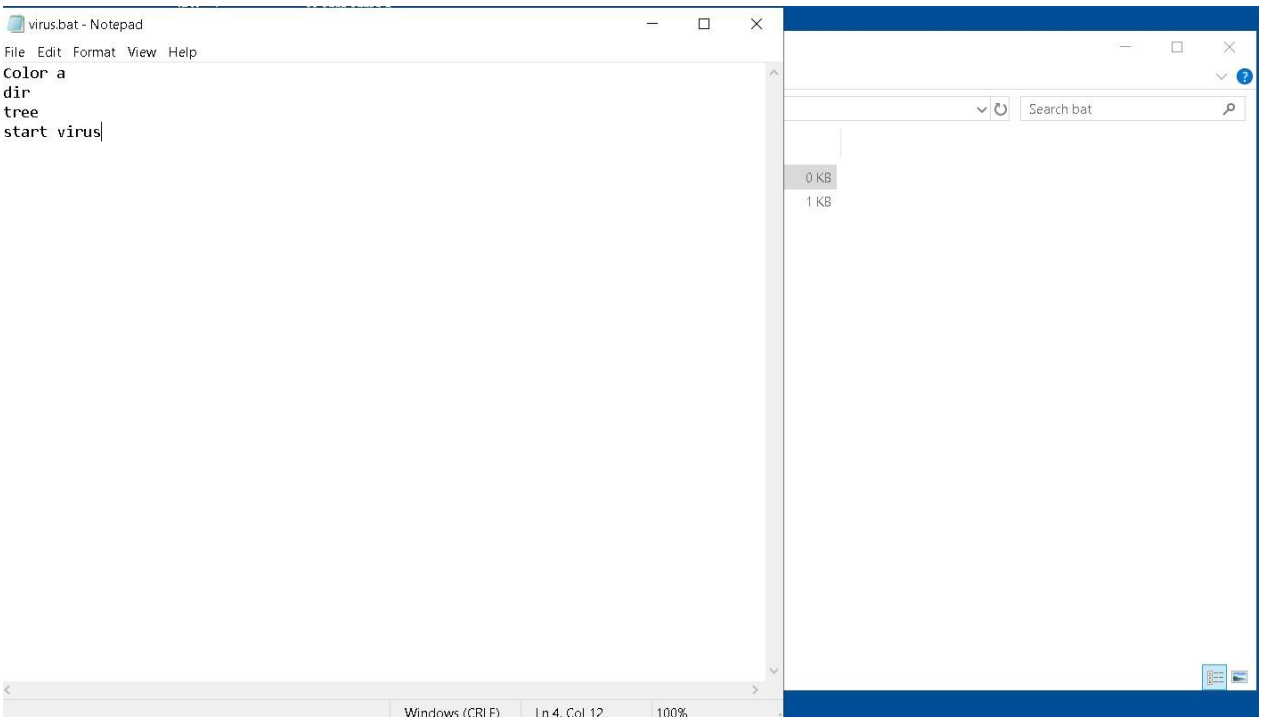
- Install antivirus software.
- Be careful with email attachments.
- Keep Everything up to Date.
- Use a Firewall.
- Run a full virus scan every week to detect any threats.
- Don’t be tricked into downloading malware

Q4) Write a small batch program and save as .bat extension and execute in victim machine (Windows 7 /
Windows 10 / Windows XP)

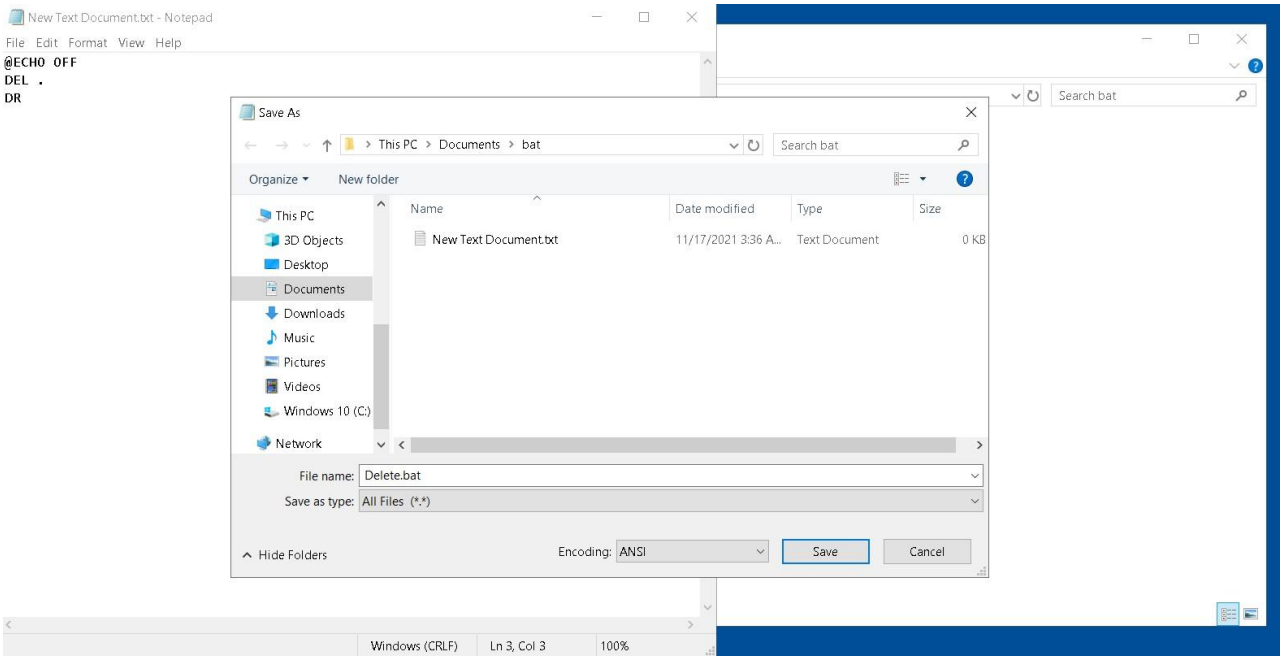
ANSWER

Created a simple bat file using notepad, Which execute Itself till the system crashes. I tried in my virtual box with safety measures. And also created a bat file which delete the files in the same directory

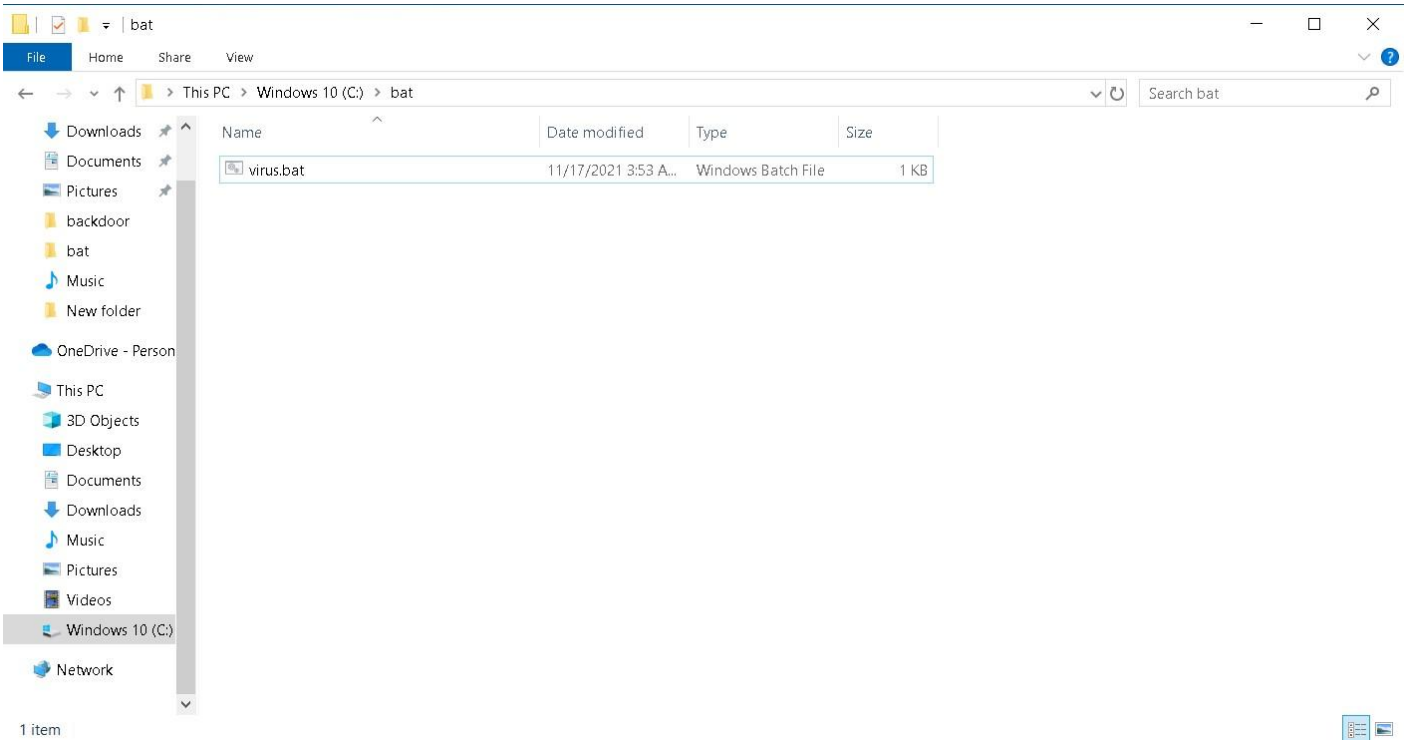
1) Batch file which execute itself for infinite times.



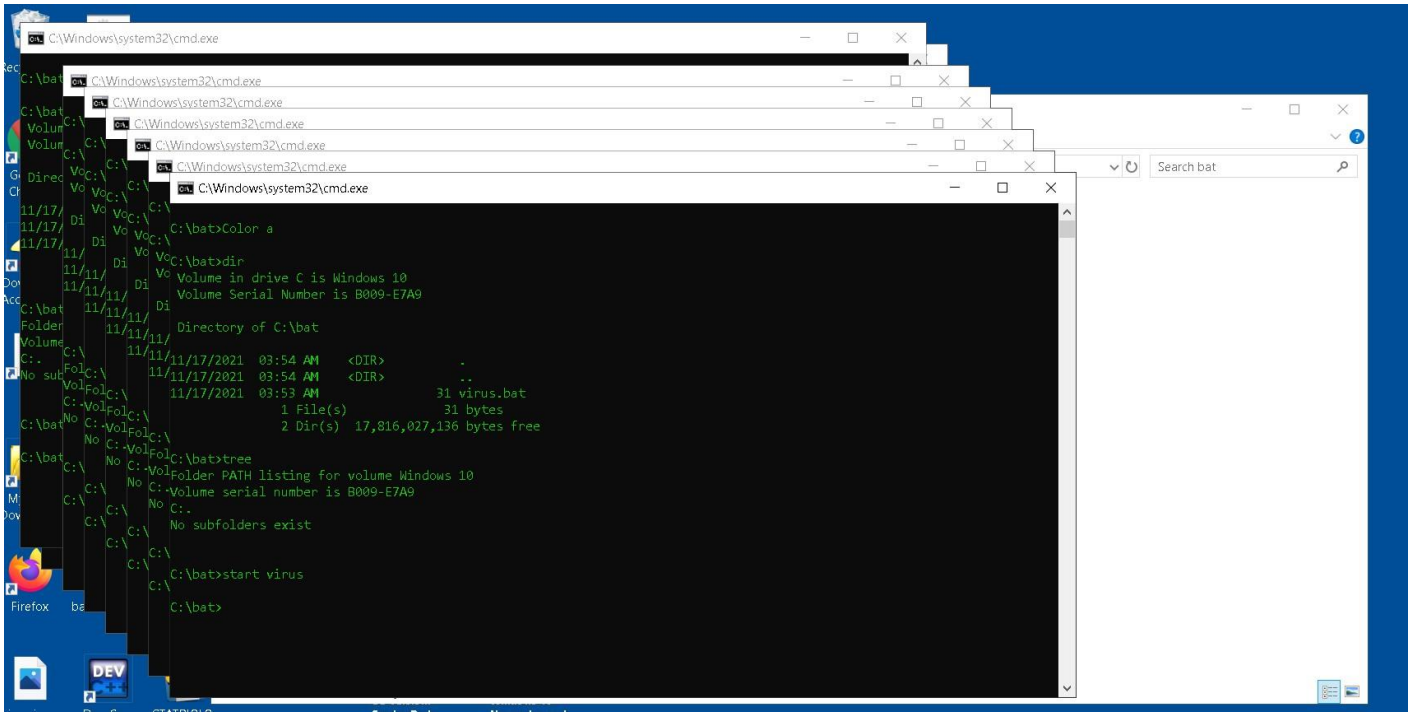
2) Batch file which delete the files on the same directory



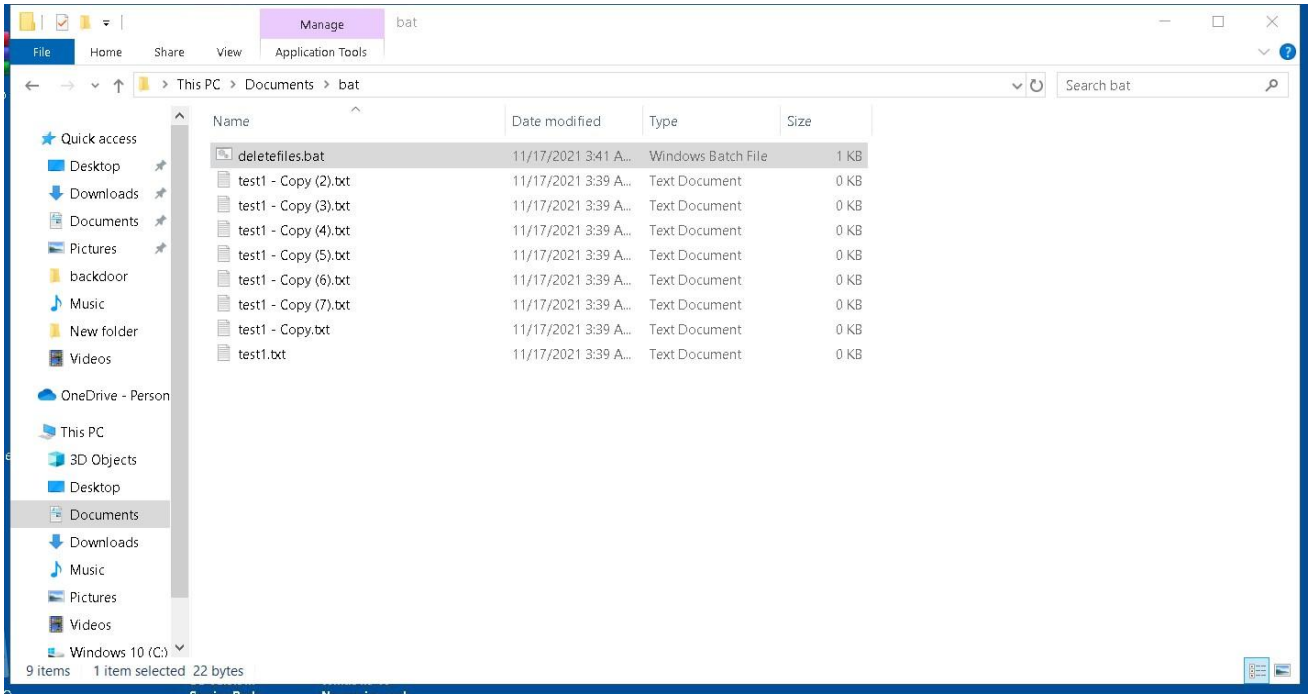
Before Execution



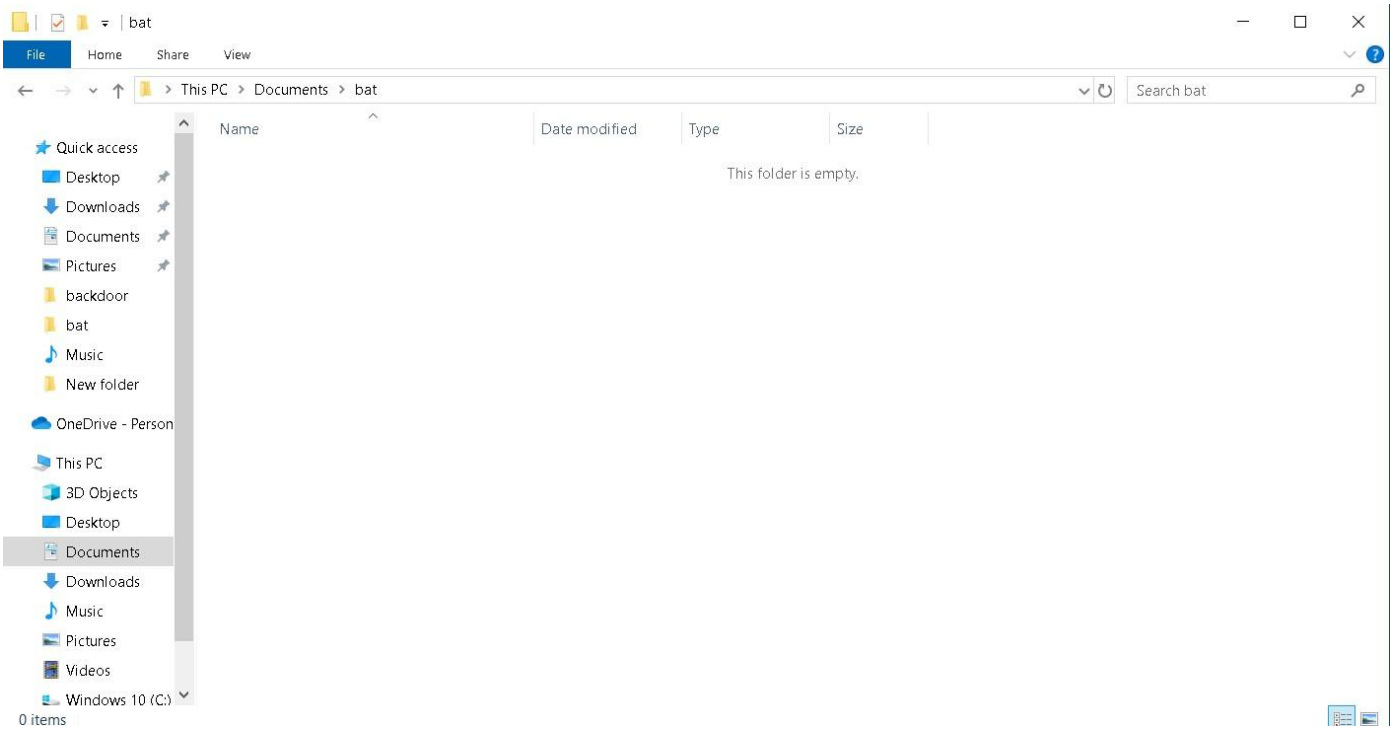
After Execution



Before Execution



After Execution



Q5)Perform SQL injection on by using Havij Tool(Download it from Internet) on http://testphp.vulnweb.com Write a report along with screenshots and mention preventive steps toavoid SQL injections

SQL INJECTION:-

- SQL injection is a code injection technique that might destroy your database.
- SQL injection is one of the most common web hacking techniques.
- SQL injection is the placement of malicious code in SQL statements, via web page input.

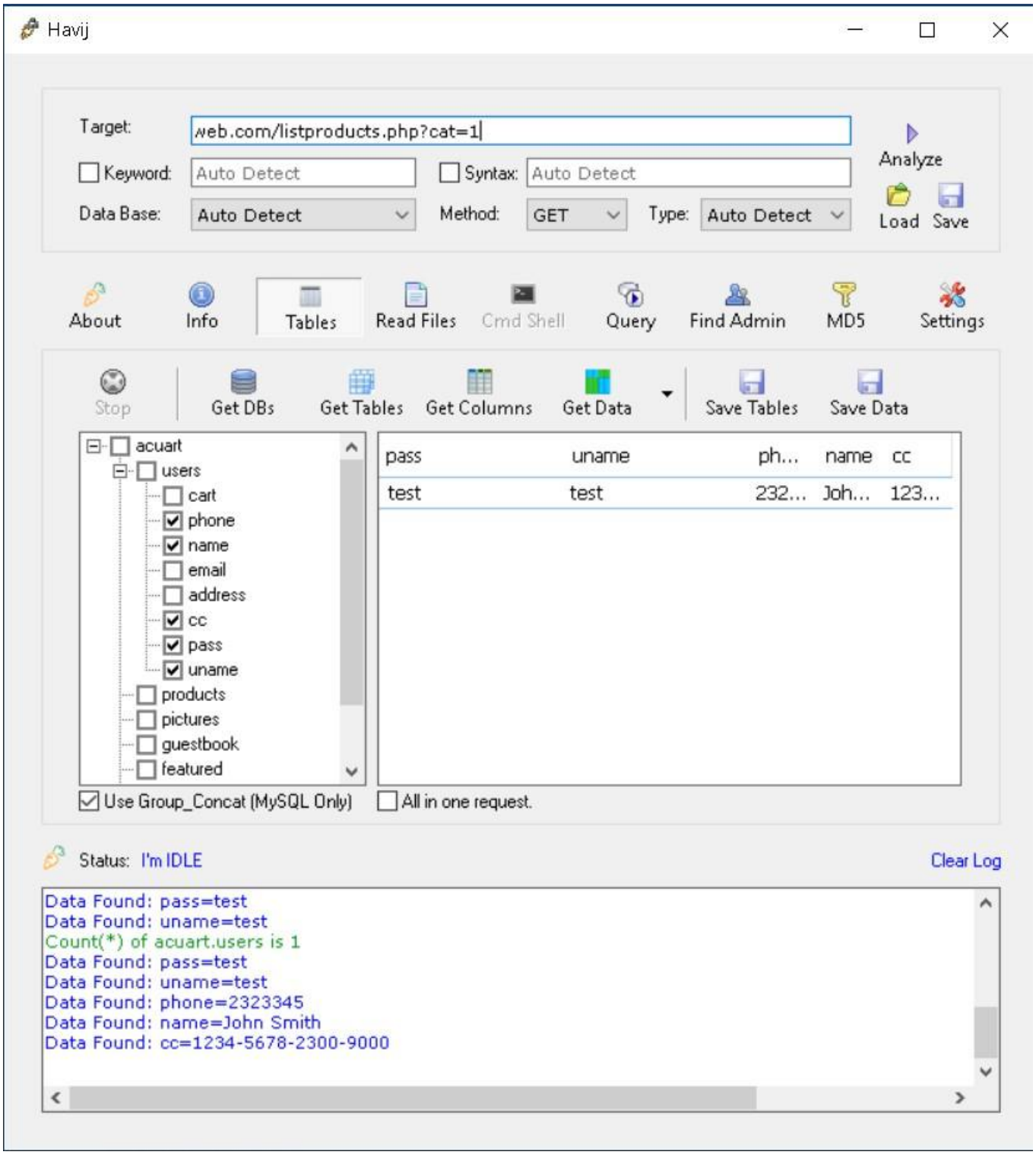
Havij Tool:-

- Havij is an automated SQL Injection tool
- It helps penetration testers to find and exploit SQL Injection vulnerabilities on a web page.
- By using this software user can perform back-end database fingerprint,
- Retrieve DBMS users and password hashes, dump tables and columns, fetching data from the database

Preventive Measures:-

- Code Development & Buying Better Software.
- Use Stored Procedures In The Database.
- Actively Manage Patches And Updates.
- Raise Virtual Or Physical Firewalls.
- Harden Your OS And Applications.
- Establish Appropriate Privileges And Strict Access.
- Limit Read-Access.
- Encryption: Keep Your Secrets Secret.
- Don’t Divulge More Than Necessary In Error Messages.

Havij Tool Implementation screenshot



Q6) Clone a Facebook page and try to perform Desktop Phishing in your local machine and capture thecre dentials and write the document along with screenshots and suggest the solution to avoid from phishing

Answer

Phishing :-

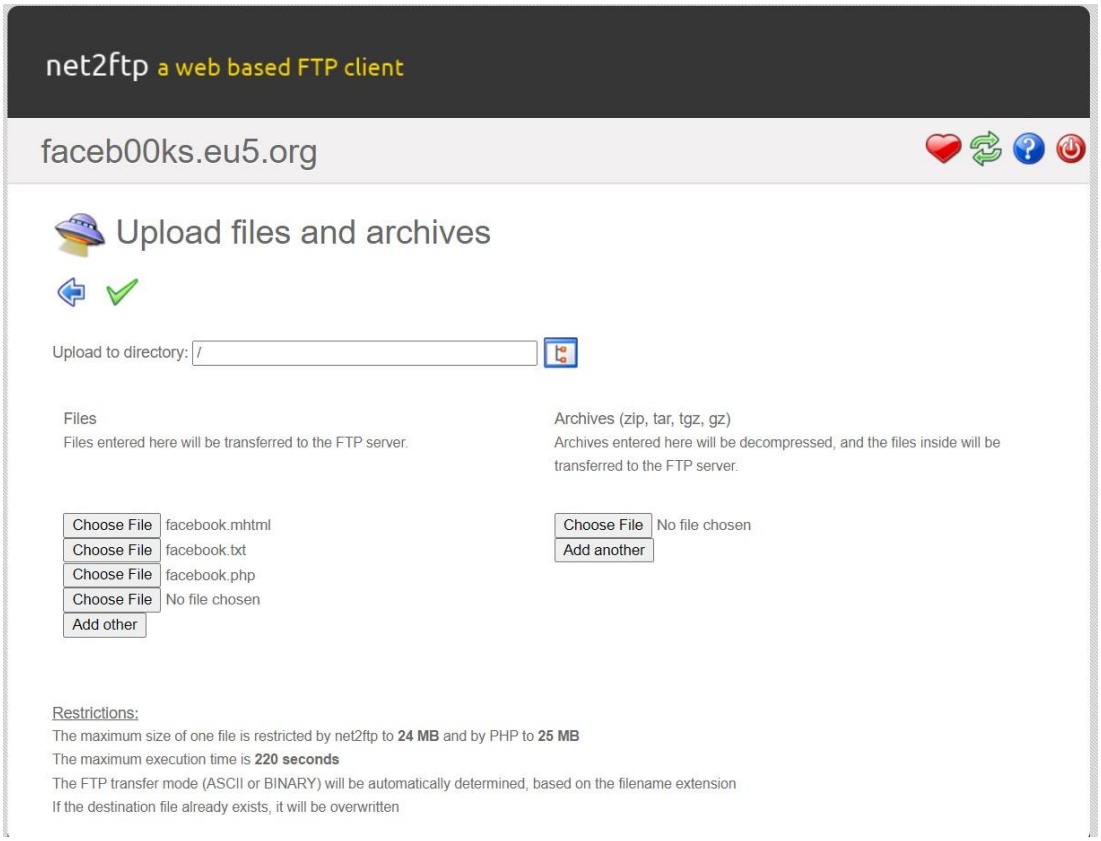
Phishing is a type of social engineering attack in which cyber criminals trick victims into handing over sensitive information or installing malware.

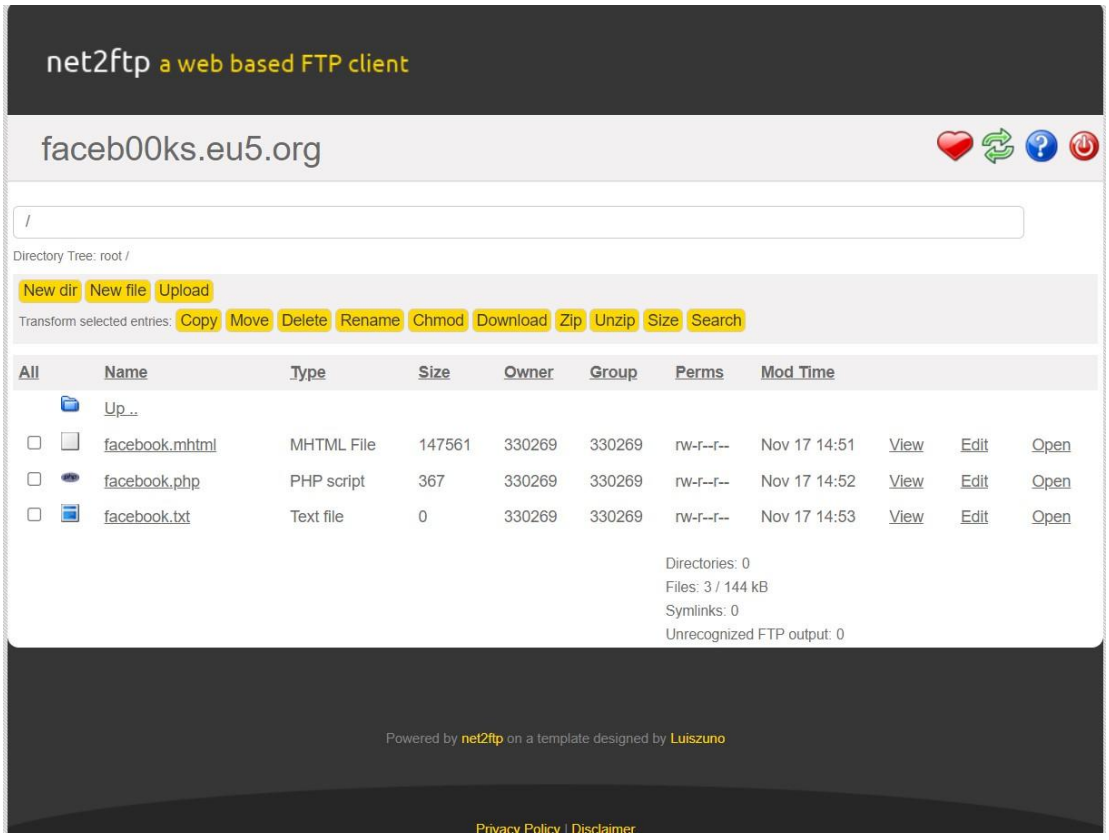
A phishing website is a domain similar in name and appearance to an official website. They're made in order to fool someone into believing it is legitimate.

Steps to create a Phishing website and host it using free web hosting platform

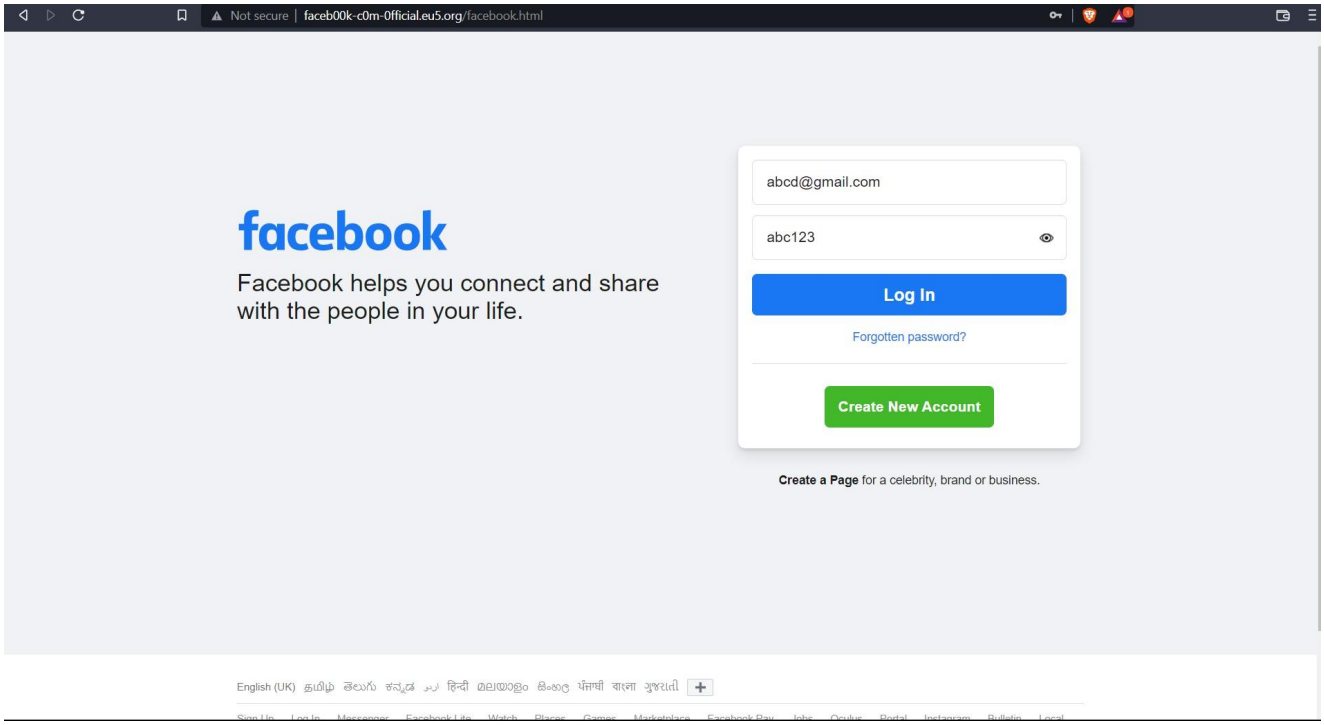
Select the available Domain from free web hosting platform

Download the html page of the legit website and save it , create a php file and a empty text file . Paste the name of php file in the action area of the cloned html file and save it. Php file helps to redirect to the original website and the text file helps to store the data entered by the victim. Upload all three files in the web hosting area created.

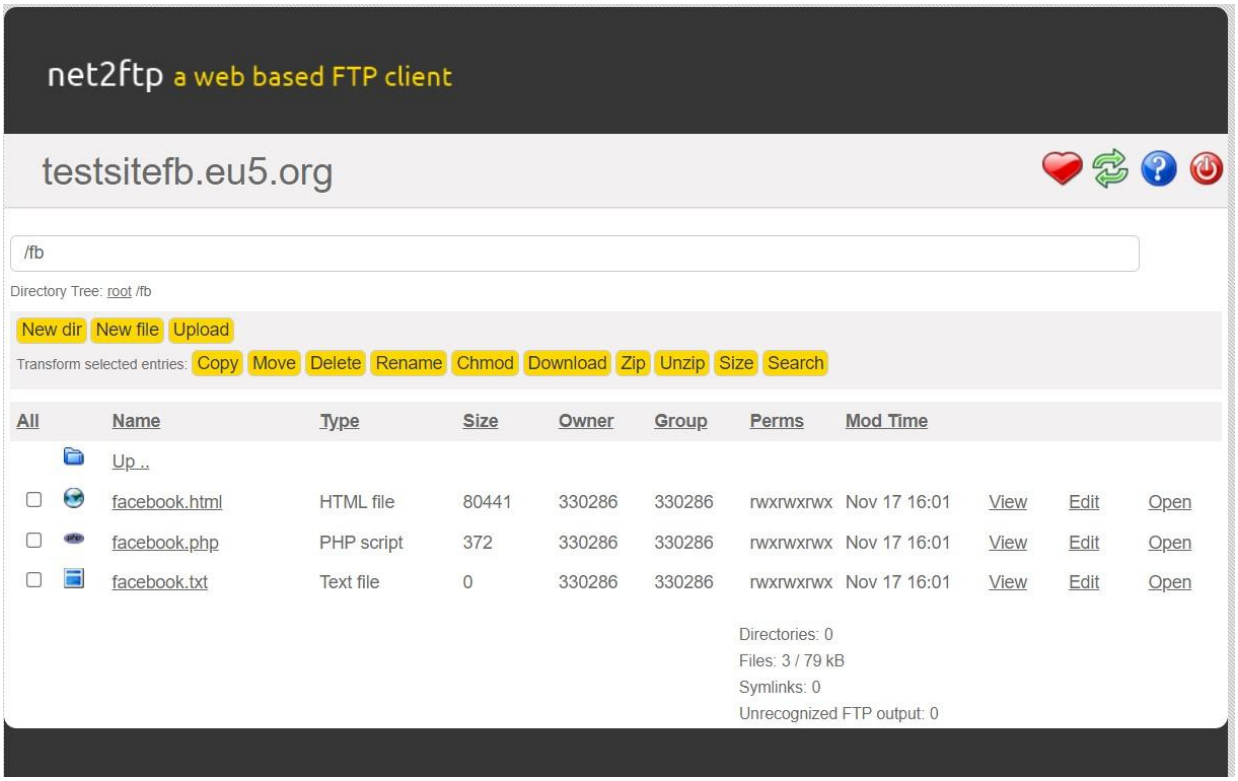




Copy the link of your website and send to the victim through emails or any other social media platform and wait till he opens the link. If he opens and enter the details it will redirect to the original website by this victim does not know that his data got theft



When victim enters the data it will store it on our empty txt file which we uploaded on our site. We can view that when ever we want.



Preventive Measures:-

- Check the URL before enter in it
- Verify a Site’s Security.
- Have a second step authentication to avoid unauthorized logins.
- Check Your Online Accounts Regularly.
- Use Firewalls.
- Be Wary of Pop-Ups.
- Never Give Out Personal Information.
- Use Antivirus Software.

Q7) Write article on how to change the IP address by using proxies and mention the differences between
proxies and VPN

proxy to change your IP address

Proxies work similarly to VPNs but with far less versatility and security. Your internet connection goes through a middleman server so that websites and other online resources see the proxy server's IP address and not your own. Unlike VPNs, proxies often lack encryption, only affect certain apps, and can leak your IP address through other means.

A few different types of proxies can be used to change your IP address

- HTTP/S proxies – Usually either browser extensions or special websites that work like a browser within your browser. They only change the IP address on data sent to and from your browser, but do not affect other apps or even DNS traffic. If encryption is included, these are sometimes called SSL proxies.
- SOCKS proxies – General purpose proxy servers that can be configured for specific apps including most web browsers. SOCKS5, the latest version, includes support for encryption.
- SSH proxies – SSH proxies forward internet traffic from apps like your web browser through a Secure Shell (SSH) connection to a server, so your IP address is changed to that of the server. Although encryption is included, SSH is not a particularly fast protocol, and many websites and apps might not function properly when connected.

Steps to change IP address by using proxies:

- Open Settings.
- Click Network & Internet. ...
- Click Proxy. ...
- In the Manual Proxy Setup section, set the Use a Proxy Server switch to On.
- In the Address field, type the IP address.
- In the Port field, type the port.
- Click Save; then close the Settings window.

Differences between proxies and VPN

Both VPNs and proxies enable a higher degree of privacy than you might otherwise have, allowing you to access the internet anonymously by hiding your IP in various ways. But how they do that is quite different.

PROXY	VPN
A proxy acts as a gateway – it's ideal for basic functions like anonymous web browsing and managing (or circumventing) content restrictions. Proxy servers excel at IP masking and misdirection, making them good for viewing geographically limited content. They allow users to bypass content restrictions and monitoring, or enforce website content restrictions – so that you can't log into certain web pages on company time.	A VPN client on your computer establishes a secure tunnel with the VPN server, replacing your local ISP routing. VPN connections encrypt and secure all of your network traffic, not just the HTTP or SOCKS calls from your browser like a proxy server.VPNs are great when you need to use the WIFI at a local coffee shop: using a VPN instead of the potentially completely unencrypted local WIFI adds another layer of privacy – who knows who is lurking on that network,

Proxy and VPN Drawbacks

If you're using proxy servers to mask your internet activity, you might see performance issues that prevent you from streaming or downloading the thing you are trying to get. High ping times and other traffic on the proxy server can cause web pages to load slowly. For this reason, some users pay for a private proxy server which limits the number of users that access it, speeding up your connections.

Proxies are also vulnerable to security exploits: they can be open to attack, allowing the bad guys to infiltrate networks or steal private data. Some proxies can still track (and store) your browsing habits, as well as recording usernames and passwords – rendering that promise of anonymity null.

VPNs can also suffer from performance issues, depending on proximity to the VPN server you're connecting with. VPNs use a local client to create the connection to the VPN server, so any local CPU or memory issues will slow down the connections. VPNs are typically more expensive to use (and maintain) than a proxy server, and they are often more complex to manage.

Just like proxy servers, VPNs can't guarantee anonymity while browsing. Neither of these services will always encrypt your traffic all the way to the web server. A VPN only guarantees an end-to-end encrypted connection if you use the HTTPS protocol when you go to a new web address. Your data will be encrypted to the VPN, but from that point on, it could be unencrypted to the web server. For some sites, this may be irrelevant: an information-only webpage with no login or payment options for example, but for any sites that require a login or online payments – or any sensitive data – make sure the website is enabled to use HTTPS. Remember, the S stands for moderately more secure.