VERZEO CS-MAY
MINOR PROJECT

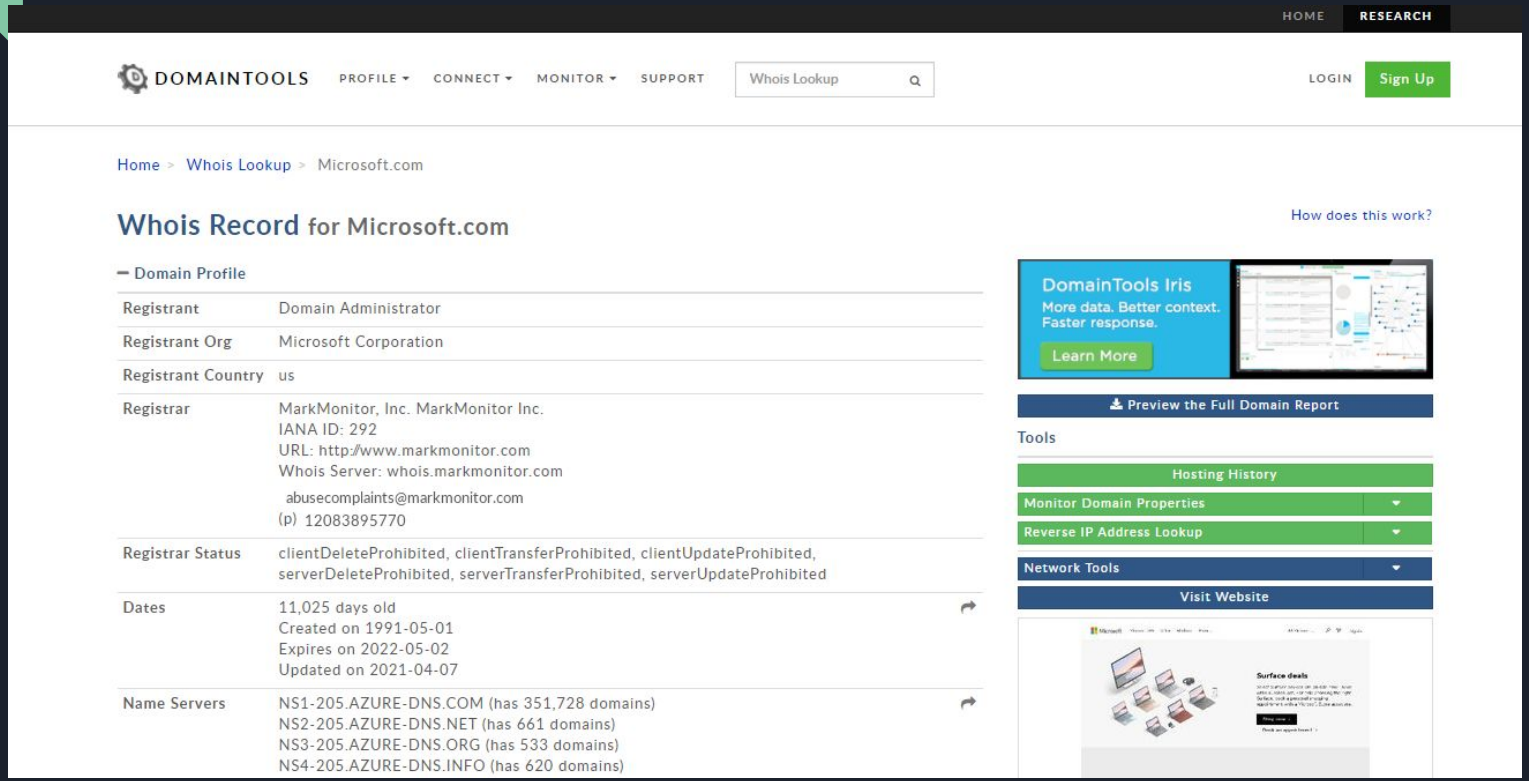
By
Ajay Chandra
ced18i029@iiitdm.ac.in / ajaykorlapati@gmail.com

1. Perform Footprinting on Microsoft Website and gather information about website by using online Websites (Whois / netcraft / Shodan / dnsdumpster., etc.) as much as possible and write report on gathered info along with screenshots

- Footprinting is the process of collecting information about a particular target. It may be a website or an individual person. A Hacker can target a Victim by collecting such critical information.
- Here we are going to do footprinting for the Microsoft Website.
- Our objective is to gain data like Server Software, Operating System, Scripting Language and Platform, etc.
- Website : https://www.microsoft.com/en-in
- Tools Used :
  - WhoIs
  - Netcraft
  - Shodan
  - Dnsdumpster

Microsoft

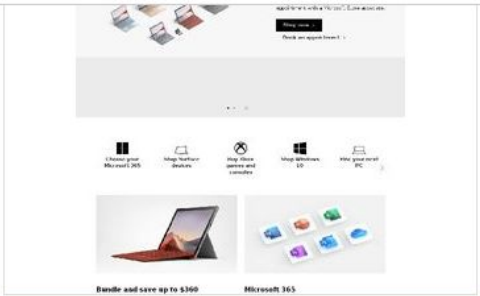
Whois record for Microsoft.com



Name Servers	NS1-205.AZURE-DNS.COM (has 351,726 domains) NS2-205.AZURE-DNS.NET (has 661 domains) NS3-205.AZURE-DNS.ORG (has 533 domains) NS4-205.AZURE-DNS.INFO (has 620 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	- Washington - Seattle - Akamai Technologies Inc.
ASN	AS16625 AKAMAI-AS, US (registered May 30, 2000)
Domain Status	Registered And Active Website
IP History	244 changes on 244 unique IP addresses over 17 years
Registrar History	4 registrars with 1 drop
Hosting History	3 changes on 4 unique name servers over 1 year

− Website

Website Title	Microsoft - Official Home Page
Response Code	200
Terms	747 (Unique: 364, Linked: 305)
Images	24 (Alt tags missing: 8)
Links	141 (Internal: 129, Outbound: 11)



View Screenshot History

Available TLDs

General TLDs | Country TLDs

The following domains are available through our preferred partners. Select domains below for more information. (3rd party site)

Taken domain.
Available domain.
Deleted previously owned domain.

Microsoft.com	View Whois
Microsoft.net	View Whois
Microsoft.org	View Whois
Microsoft.info	View Whois
Microsoft.biz	View Whois

Whois Record (last updated on 20210707)

```
Domain Name: microsoft.com
Registry Domain ID: 2724960_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.markmonitor.com
Registrar URL: http://www.markmonitor.com
Updated Date: 2021-04-07T12:58:15-0700
Creation Date: 1991-05-01T21:00:00-0700
Registrar Registration Expiration Date: 2022-05-02T00:00:00-0700
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: Domain Administrator
Registrant Organization: Microsoft Corporation
Registrant Street: One Microsoft Way,
Registrant City: Redmond
Registrant State/Province: WA
Registrant Postal Code: 98052
Registrant Country: US
Registrant Phone: +1.4258828080
Registrant Phone Ext:
Registrant Fax: +1.4259367329
Registrant Fax Ext:
Registrant Email: admin@domains.microsoft
Registry Admin ID:
Admin Name: Domain Administrator
Admin Organization: Microsoft Corporation
Admin Street: One Microsoft Way,
Admin City: Redmond
Admin State/Province: WA
```

Microsoft.us View Whois

```
Admin Organization: Microsoft Corporation
Admin Street: One Microsoft Way,
Admin City: Redmond
Admin State/Province: WA
Admin Postal Code: 98052
Admin Country: US
Admin Phone: +1.4258828080
Admin Phone Ext:
Admin Fax: +1.4259367329
Admin Fax Ext:
Admin Email: admin@domains.microsoft

Registry Tech ID:
Tech Name: MSN Hostmaster
Tech Organization: Microsoft Corporation
Tech Street: One Microsoft Way,
Tech City: Redmond
Tech State/Province: WA
Tech Postal Code: 98052
Tech Country: US
Tech Phone: +1.4258828080
Tech Phone Ext:
Tech Fax: +1.4259367329
Tech Fax Ext:
Tech Email: msnhst@microsoft.com

Name Server: ns2-205.azure-dns.net
Name Server: ns4-205.azure-dns.info
Name Server: ns3-205.azure-dns.org
Name Server: ns1-205.azure-dns.com
DNSSEC: unsigned
URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/
>>> Last update of WHOIS database: 2021-07-07T00:05:09-0700 <<<

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

If you wish to contact this domain's Registrant, Administrative, or Technical
contact, and such email address is not visible above, you may do so via our web
form, pursuant to ICANN's Temporary Specification. To verify that you are not a
robot, please enter your email address to receive a link to a page that
facilitates email communication with the relevant contact(s).
```

If you wish to contact this domain's Registrant, Administrative, or Technical contact, and such email address is not visible above, you may do so via our web form, pursuant to ICANN's Temporary Specification. To verify that you are not a robot, please enter your email address to receive a link to a page that facilitates email communication with the relevant contact(s).

Web-based WHOIS:
  https://domains.markmonitor.com/whois

If you have a legitimate interest in viewing the non-public WHOIS details, send your request and the reasons for your request to whoisrequest@markmonitor.com and specify the domain name in the subject line. We will review that request and may ask for supporting documentation and explanation.

The data in MarkMonitor's WHOIS database is provided for information purposes, and to assist persons in obtaining information about or related to a domain name's registration record. While MarkMonitor believes the data to be accurate, the data is provided "as is" with no guarantee or warranties regarding its accuracy.

By submitting a WHOIS query, you agree that you will use this data only for lawful purposes and that, under no circumstances will you use this data to:
  (1) allow, enable, or otherwise support the transmission by email, telephone, or facsimile of mass, unsolicited, commercial advertising, or spam; or
  (2) enable high volume, automated, or electronic processes that send queries, data, or email to MarkMonitor (or its systems) or the domain name contacts (or its systems).

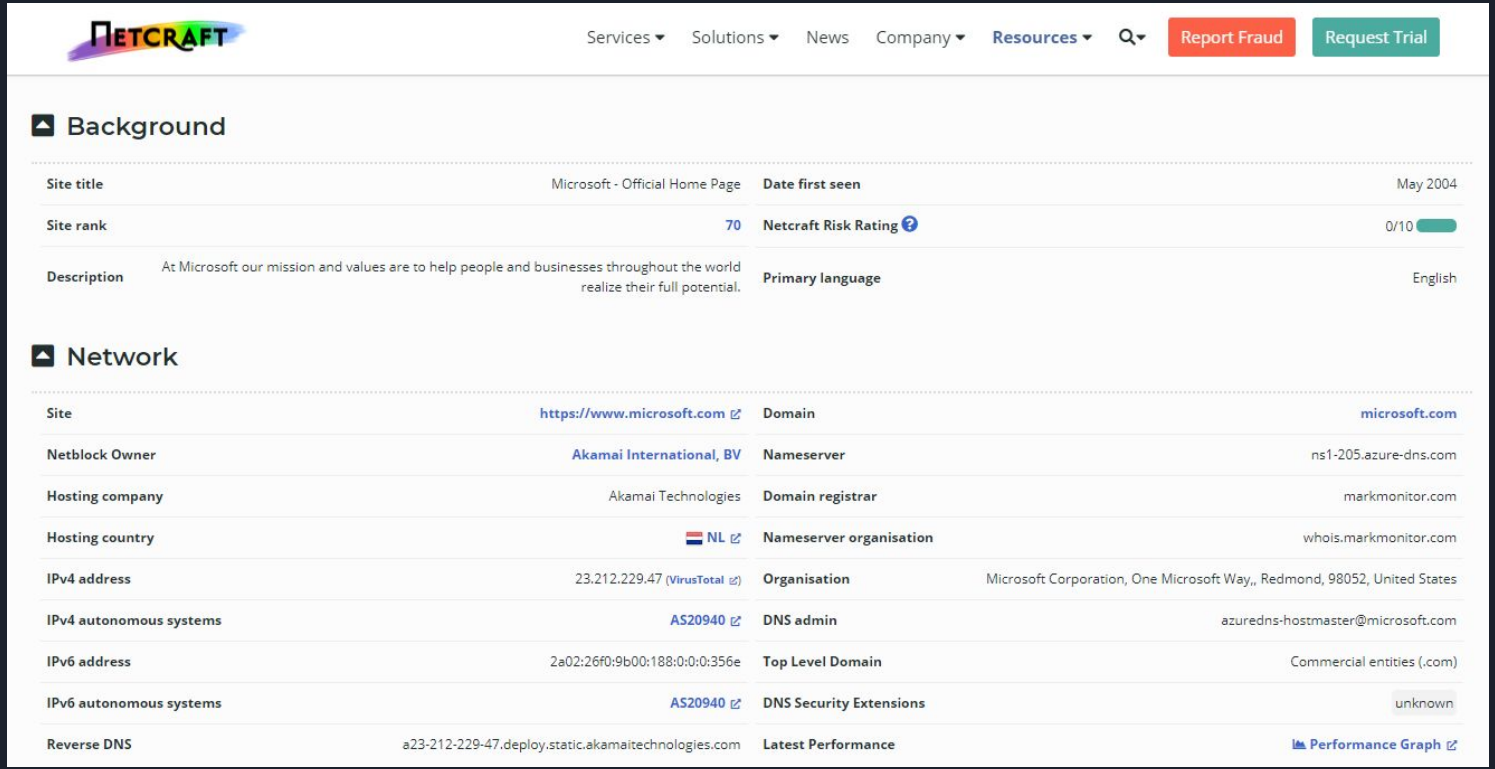
MarkMonitor reserves the right to modify these terms at any time.

By submitting this query, you agree to abide by this policy.

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

Visit MarkMonitor at https://www.markmonitor.com
Contact us at +1.8007459229
In Europe, at +44.02032062220

Netcraft Information on Microsoft.com



NETCRAFT

Services ▾ Solutions ▾ News Company ▾ Resources ▾ Report Fraud Request Trial

Background

Site title	Microsoft - Official Home Page	**Date first seen**	May 2004
Site rank	70	**Netcraft Risk Rating**	0/10
Description	At Microsoft our mission and values are to help people and businesses throughout the world realize their full potential.	**Primary language**	English

Network

Site	https://www.microsoft.com	**Domain**	microsoft.com
Netblock Owner	Akamai International, BV	**Nameserver**	ns1-205.azure-dns.com
Hosting company	Akamai Technologies	**Domain registrar**	markmonitor.com
Hosting country	NL	**Nameserver organisation**	whois.markmonitor.com
IPv4 address	23.212.229.47 (VirusTotal)	**Organisation**	Microsoft Corporation, One Microsoft Way,, Redmond, 98052, United States
IPv4 autonomous systems	AS20940	**DNS admin**	azuredns-hostmaster@microsoft.com
IPv6 address	2a02:26f0:9b00:188:0:0:0:356e	**Top Level Domain**	Commercial entities (.com)
IPv6 autonomous systems	AS20940	**DNS Security Extensions**	unknown
Reverse DNS	a23-212-229-47.deploy.static.akamaitechnologies.com	**Latest Performance**	Performance Graph

IP delegation

IPv4 address (23.212.229.47)

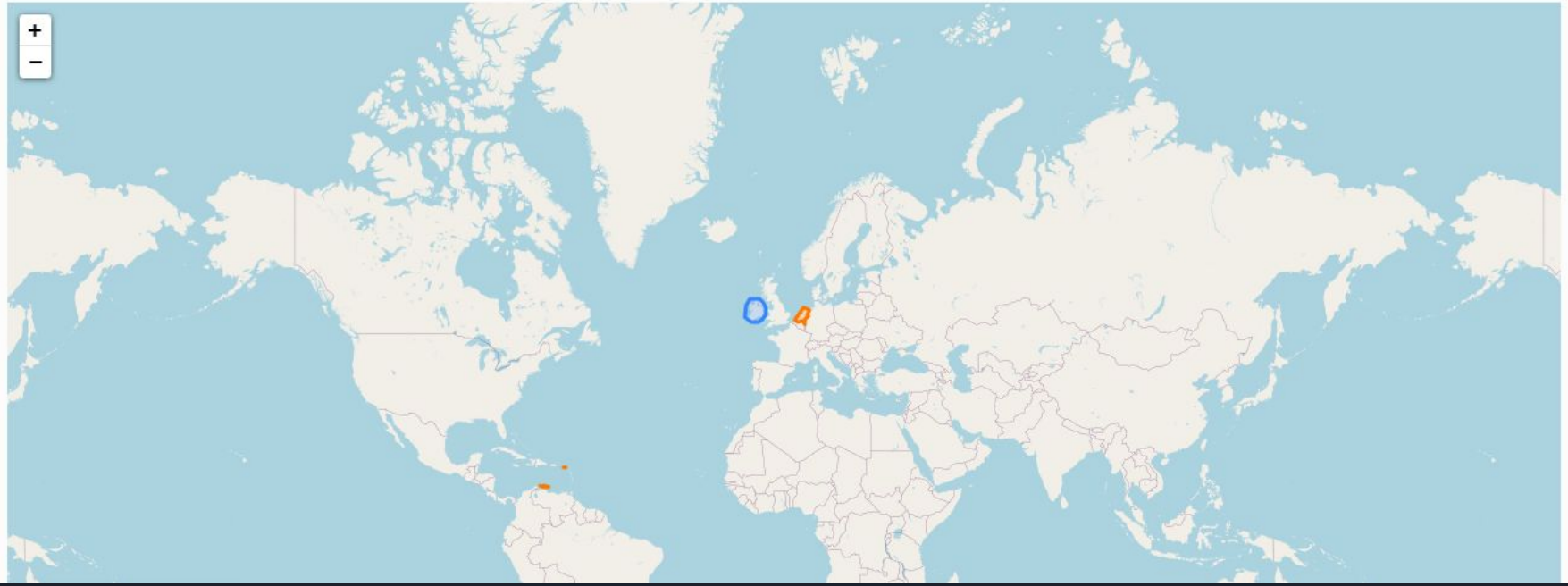
IP range	Country	Name	Description
0.0.0.0-255.255.255.255	N/A	IANA-BLK	The whole IPv4 address space
↳ 23.0.0.0-23.255.255.255	United States	NET23	American Registry for Internet Numbers
↳ 23.192.0.0-23.223.255.255	United States	AKAMAI	Akamai Technologies, Inc.
↳ 23.212.228.0-23.212.231.255	Netherlands	AIBV	Akamai International, BV
↳ 23.212.229.47	Netherlands	AIBV	Akamai International, BV

IPv6 address (2a02:26f0:9b00:188:0:0:0:356e)

IP range	Country	Name	Description
::/0	N/A	ROOT	Root inet6num object
↳ 2a00::/11	European Union	EU-ZZ-2A00	RIPE NCC
↳ 2a00::/12	Netherlands	EU-ZZ-2A00	RIPE Network Coordination Centre
↳ 2a02:26f0::/29	European Union	EU-AKAMAI-20101022	Akamai International B.V.
↳ 2a02:26f0:9b00::/48	European Union	AKAMAI-PA	Akamai Technologies
↳ 2a02:26f0:9b00:188:0:0:0:356e	European Union	AKAMAI-PA	Akamai Technologies

IP Geolocation

We use multilateration to independently determine the location of a server. **Read more.**



SSL/TLS

Assurance	Organisation validation
Common name	www.microsoft.com
Organisation	Microsoft Corporation
State	WA
Country	US
Organisational unit	Microsoft Corporation
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)
Matches hostname	Yes
Server	Not Present

Perfect Forward Secrecy	Yes
Supported TLS Extensions	RFC8446 supported versions, RFC8446 key share, RFC4366 server name, RFC4492 elliptic curves, RFC7301 application-layer protocol negotiation, RFC4366 status request
Application-Layer Protocol Negotiation	h2
Next Protocol Negotiation	Not Present
Issuing organisation	Microsoft Corporation
Issuer common name	Microsoft RSA TLS CA 01
Issuer unit	Not Present
Issuer location	Not Present
Issuer country	US
Issuer state	Not Present

Serial number	0x6b000003f4e3a67a2348550c330000000003f4	**OCSP data generated**	Jul 8 01:23:17 2021 GMT
Cipher	TLS_AES_256_GCM_SHA384	**OCSP data expires**	Jul 12 01:23:17 2021 GMT
Version number	0x02		

Certificate Transparency

Signed Certificate Timestamps (SCTs)

Source	Log	Timestamp	Signature Verification
Certificate	Google Argon 2021 9lyUL9F3MCIUVBgIMJRWjuNNExkzv98MLyALzE7xZOM=	2020-08-28 22:27:05	Success
Certificate	Cloudflare Nimbus 2021 RJRlLrDuzq/EQAfYqP4owNrmgr7YyzG1P9MzlrW2gag=	2020-08-28 22:27:05	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 offered the Heartbeat TLS extension prior to the Heartbleed disclosure, but is using a new certificate and no longer offers Heartbeat.

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	Baltimore CyberTrust Root
Organisational unit	CyberTrust
Organisation	Baltimore
Validity period	From 2000-05-12 to 2025-05-12

↓

Common name	Microsoft RSA TLS CA 01
Organisational unit	Not Present
Organisation	Microsoft Corporation
Validity period	From 2020-07-21 to 2024-10-08

Hosting History

Netblock owner	IP address	OS	Web server	Last seen
Akamai Technologies, Inc. 145 Broadway Cambridge MA US 02142	104.110.245.246	Linux	unknown	6-Jul-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

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**.

Warning: It appears that this host does not have an SPF record. There may be an SPF record on microsoft.com: Check the **site report**.

Setting up an SPF record helps prevent the delivery of forged emails from your domain. Please note that an SPF record will only protect the domain it is added to and not any **mail-enabled subdomains**. It is recommended to add an SPF record to any subdomain with an MX record.

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**.

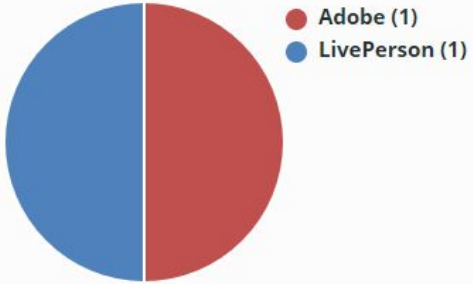
This host does not have a DMARC record. There may be a DMARC record on the site report for microsoft.com: Check the **site report**.

Web Trackers

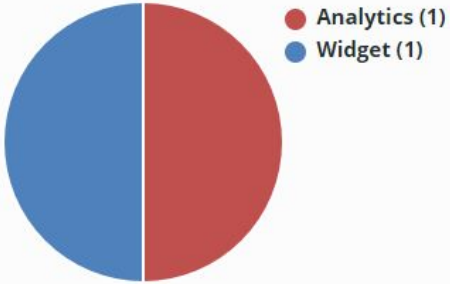
Web Trackers are third-party resources loaded onto a webpage. Trackable resources include social sharing widgets, javascript files, and images. These trackers can be used to monitor individual user behaviour across the web. Data derived from these trackers are primarily used for advertising or analytics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

2 known trackers were identified.

Companies



Categories



Company	Primary Category	Tracker	Popular Sites with this Tracker
Adobe	Analytics	Omniture	www.hl.co.uk, www.capitalone.com, www.ziggogo.tv
LivePerson	Widget	Liveperson	www.delltechnologies.com

Site Technology (fetched 25 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	
Using ASP.NET	ASP.NET is running on the server	www.wordreference.com, www.cnblogs.com, bscscan.com

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
Web Worker	*No description*	www.pearltrees.com, www.verajohn.com, www.origin.com
Asynchronous Javascript	*No description*	www.bloomberg.com, www.researchgate.net, www.primevideo.com
Local Storage	*No description*	www.amazon.es, www.roblox.com, smile.amazon.com
Session Storage	*No description*	www.cnet.com, www.dell.com, www.huobi.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
jQuery	A JavaScript library used to simplify the client-side scripting of HTML	www.amazon.co.uk, www.instagram.com, www.amazon.in
AJAX	*No description*	www.imdb.com, mail.google.com, teams.microsoft.com

Content Delivery Network

A content delivery network or content distribution network (CDN) is a large distributed system of servers deployed in multiple data centers in the Internet. The goal of a CDN is to serve content to end-users with high availability and high performance.

Technology	Description	Popular sites using this technology
Akamai	Web Content Delivery service provider	www.accuweather.com, www.disneyplus.com, www.irs.gov

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.homedepot.com, www.apple.com

Character Encoding

A character encoding system consists of a code that pairs each character from a given repertoire with something else such as a bit pattern, sequence of natural numbers, octets, or electrical pulses in order to facilitate the transmission of data (generally numbers or text) through telecommunication networks or for data storage.

Technology	Description	Popular sites using this technology
UTF8	UCS Transformation Format 8 bit	

HTTP Compression

HTTP compression is a capability that can be built into web servers and web clients to make better use of available bandwidth, and provide greater transmission speeds between both.

Technology	Description	Popular sites using this technology
Gzip Content Encoding	Gzip HTTP Compression protocol	www.instructables.com, www.seznam.cz, www.newsit.gr

Web Browser Targeting

Web browser targeting enables software applications to make use of specific functions of the browser as well as optimizing the application for specific browser versions.

Technology	Description	Popular sites using this technology
Strict Transport Security	Web security policy mechanism whereby a web server declares that complying user agents are to interact with it using only secure HTTP connections	www.binance.com, web.whatsapp.com, accounts.google.com

Privacy Management

Privacy policy is a statement or a legal document (privacy law) that discloses some or all of the ways a party gathers, uses, discloses and manages a customer or client's data.

Technology	Description	Popular sites using this technology
P3P	Platform for Privacy Preferences Project allows websites to express their privacy practices	www.aliexpress.com, www.pinterest.com, us02web.zoom.us

Doctype

A Document Type Declaration, or DOCTYPE, is an instruction that associates a particular SGML or XML document (for example, a webpage) with a Document Type Definition (DTD).

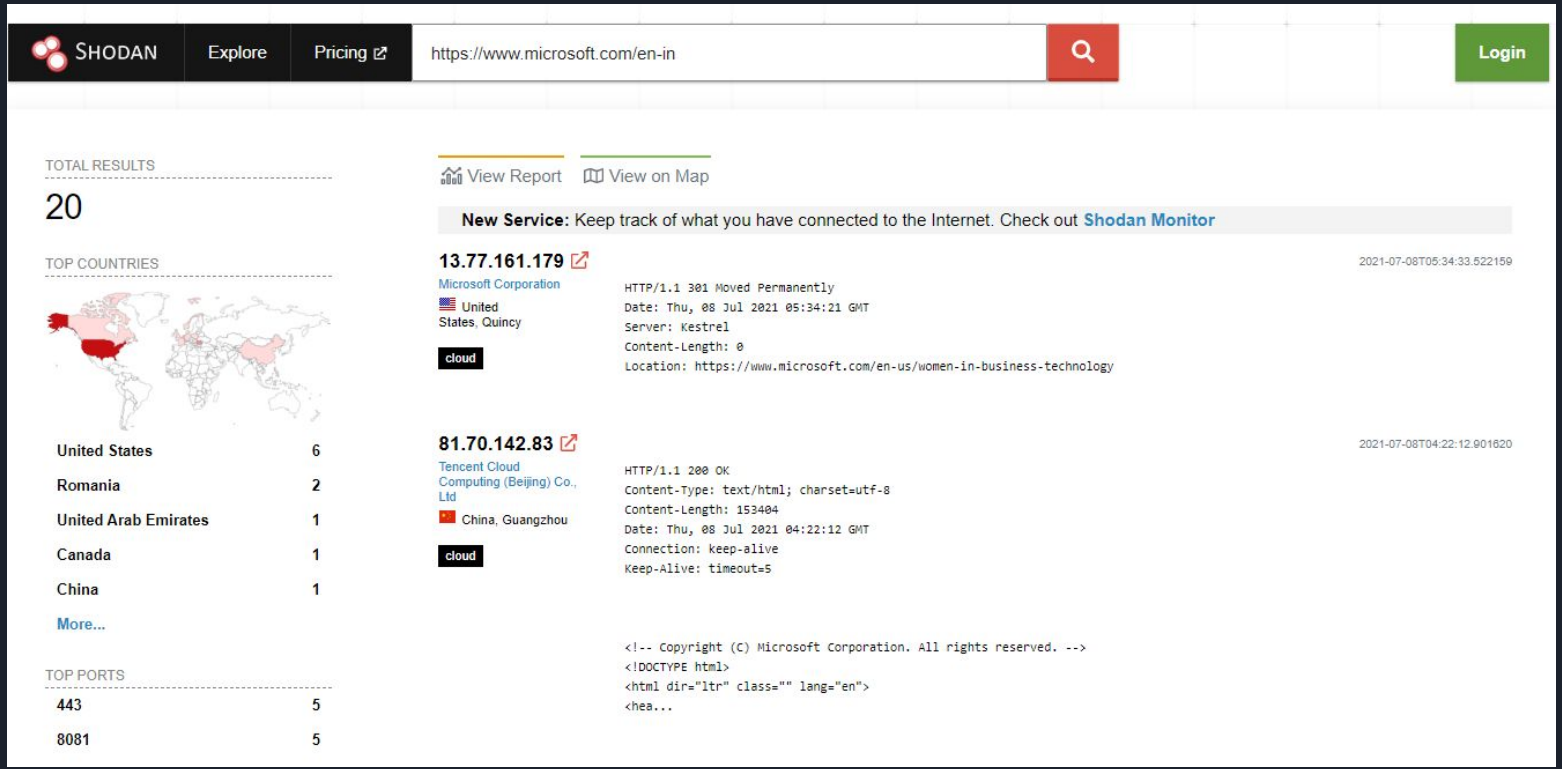
Technology	Description	Popular sites using this technology
HTML5	Latest revision of the HTML standard, the main markup language on the web	

HTML 5

HTML5 is a markup language for structuring and presenting content for the World Wide Web and a core technology of the Internet. It is the fifth revision of the HTML standard.

Technology	Description	Popular sites using this technology
Viewport meta tag	HTML5 tag usually used for mobile optimization	

Shodan Information on Microsoft.com



9000	3
80	1
3001	1

More...

TOP ORGANIZATIONS

DigitalOcean, LLC	3
Aruba S.p.A. - CLoud Services UK	1
BORLAND SOFTWARE CORPORATION	1
Comcast Cable Communications, LLC	1
DXTL HK	1

More...

TOP PRODUCTS

Microsoft IIS httpd	6
Apache httpd	4

94.177.255.108

host108-255-177-94.static.arubacloud.com

Aruba S.p.A. - CLoud Services UK

United Kingdom, London

2021-07-06T21:02:57.002621

```
HTTP/1.1 200 OK
Content-Length: 40108
Content-Type: text/html; charset=utf-8
Set-Cookie: .Nop.Customer=; expires=Thu, 01 Jan 1970 00:00:00 GMT; path=/; samesite=lax
Set-Cookie: .Nop.Customer=cc155f81-f852-478f-ba14-674f15f7bccb; expires=Wed, 06 Jul 2022 21:02:55 GMT; path=/; samesite=lax; ht
```

45.79.3.82

li1102-82.members.linode.com

Linode

United States, Richardson

cloud

2021-07-06T13:45:52.809808

```
HTTP/1.1 200 OK
Accept-Ranges: bytes
Content-Type: text/html; charset=UTF-8
Date: Tue, 06 Jul 2021 13:45:52 GMT
Etag: W/"9d6-AfdsI4Vd0hRKhUeZaAbZp4oH/Yw"
Server: Caddy
Vary: Accept-Encoding
X-Powered-By: Express
Transfer-Encoding: chunked

9d6
<!doctype html>
<html lang="en">
  <head>
...
```

68.183.202.182

tearmann.ca

DigitalOcean, LLC

Canada, Toronto

cloud

2021-07-06T13:16:16.134206

```
HTTP/1.1 200 OK
Date: Tue, 06 Jul 2021 13:16:15 GMT
Server: Apache
Cache-Control: no-cache, max-age=0, must-revalidate, no-transform
Vary: Accept-Encoding
Transfer-Encoding: chunked
Content-Type: text/html; charset=utf-8

62ee
<!DOCTYPE html>
```

141.85.228.5

Politehnica University of Bucharest

Romania, Bucharest

2021-07-06T00:06:04.949824

```
HTTP/1.1 200 OK
Date: Tue, 06 Jul 2021 00:06:04 GMT
Server: Apache/2.4.10 (Ubuntu)
Last-Modified: Fri, 18 Aug 2017 00:57:16 GMT
ETag: "17b5-556fc9c3bfd51"
Accept-Ranges: bytes
Content-Length: 6069
Vary: Accept-Encoding
Content-Type: text/html

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 3.2...
```

93.122.198.29

Orange Romania

Romania, Bucharest

2021-07-05T01:32:14.077246

```
HTTP/1.1 401 Access Denied
Server: Microsoft-IIS/5.1
Date: Mon, 05 Jul 2021 01:32:12 GMT
WWW-Authenticate: Basic realm="93.122.198.29"
Connection: close
Content-Length: 4431
Content-Type: text/html

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 3.2 Final//EN">
<html dir=ltr>

<head>
<style>...
```

143.186.119.116

BORLAND SOFTWARE CORPORATION

United States, Rockville

2021-07-03T05:43:28.045404

```
HTTP/1.1 500 Internal Server Error
Server: Microsoft-IIS/5.0
Date: Sat, 03 Jul 2021 05:43:26 GMT
X-Powered-By: ASP.NET
Content-Length: 3522
Content-Type: text/html
Expires: Sat, 03 Jul 2021 05:43:26 GMT
Cache-control: private


<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 3.2 Final//EN">

...
```

159.69.108.150

static.150.108.69.159.clients.your-server.de

Hetzner Online GmbH

Germany, Nürnberg

2021-06-30T04:14:04.045409

```
HTTP/1.1 200 OK
Server: nginx/1.16.0
Date: Wed, 30 Jun 2021 04:14:03 GMT
Content-Type: text/html
Content-Length: 4509
Last-Modified: Tue, 29 Jun 2021 09:05:34 GMT
Connection: keep-alive
ETag: "60dae25e-119d"
Accept-Ranges: bytes

<!doctype html><html lang="en"><head><meta charset="utf-8...
```

213.190.193.29

sv29.netmadeira.com

nos madeira comunicacoes s.a

Portugal, Funchal

2021-06-26T05:04:40.342851

```
HTTP/1.1 403 Access Forbidden
Server: Microsoft-IIS/5.0
Date: Sat, 26 Jun 2021 05:04:40 GMT
Connection: close
Content-Length: 4083
Content-Type: text/html

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 3.2 Final//EN">
<html dir=ltr>

<head>
<style>
a:link                {font:8pt/11pt ver...
```

Dnsdumpster Information on Microsoft.com

DNS Servers

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

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

"docusign=d5a3737c-c23c-4bd0-9095-d2ff621f2840"
"v=spf1 include:_spf-a.microsoft.com include:_spf-b.microsoft.com include:_spf-c.microsoft.com include:_spf-ssg-a.microsoft.com include:spf-a.hotmail.com include:_spf1-meo.microsoft.com -all"
"google-site-verification=Zv1IvEEZg4N9wbEXpBSSyAiIjDyyB3S-fzfFClb7D1E"
"adobe-sign-verification=c1fea9b4cdd4df0d5778517f29e0934"
"docusign=52998482-393d-46f7-95d4-15ac6509bfdd"
"google-site-verification=8-zFCaUXhhPcvN29EVw2RvtASDCaDPQ02L1HJ8Om8I0"

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

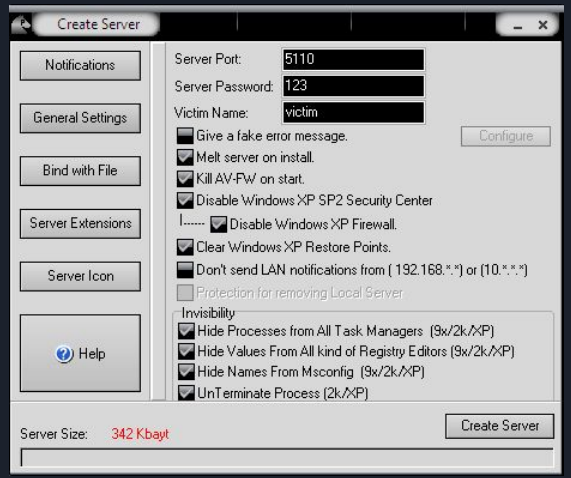
microsoft.com HTTP: Kestrel HTTPS: Kestrel	40.112.72.205	MICROSOFT-CORP-MSN-AS-BLOCK Ireland
tide500.microsoft.com	131.107.0.70 tide500.microsoft.com	MICROSOFT-CORP-AS United States
msonlineppe2010.microsoft.com	70.37.188.23 msonlineppe2010.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK United States
ppeteam2010.microsoft.com	70.37.188.29 ppe2010my.microsoft.com	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	70.37.188.29 ppe2010my.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK United States
ppespsites2010.microsoft.com	70.37.188.29 ppe2010my.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK United States
my2010.microsoft.com	70.37.188.22	MICROSOFT-CORP-MSN-AS-BLOCK United States
ppemy2010.microsoft.com	70.37.188.29 ppe2010my.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK United States

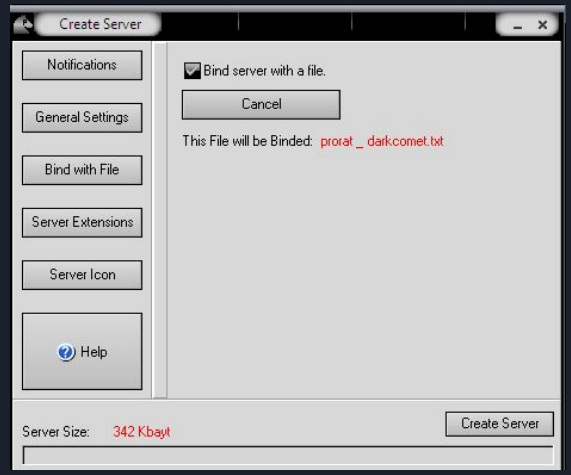
wwwco1test51.microsoft.com	157.56.62.51 wwwco1test51.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK United States
www.cy1test51.microsoft.com	23.103.192.31 www.cy1test51.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK United States
cmscy1test51.microsoft.com	23.103.192.29 cmscy1test51.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK United States
cmsco2test51.microsoft.com	134.170.184.36 cmsco2test51.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK United States
wwwco2test51.microsoft.com	134.170.185.19 wwwco2test51.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK United States
cmsby2test51.microsoft.com	134.170.188.88 cmsby2test51.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK United States
co2vlsctest51.microsoft.com	134.170.184.170 co2vlsctest51.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK United States
by2vlsctest51.microsoft.com	134.170.188.61 by2vlsctest51.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK United States
tide161.microsoft.com	131.107.8.42 tide161.microsoft.com	MICROSOFT-CORP-AS United States
wwwbn1test61.microsoft.com	134.170.22.94 wwwbn1test61.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK United States
www.cy1test61.microsoft.com	23.103.192.37 www.cy1test61.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK United States
cmsco2test61.microsoft.com	134.170.184.46 cmsco2test61.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK United States

2. Test the System Security by using PRORAT / Darkcomet (Anyone Tool) Trojan by hacking virtual machine and try to take screenshots & Keystrokes along with change data in Desktop. Write a report on vulnerability issue along with screenshots how you performed and suggest the security patch to avoid these type of attacks. Hacker Machine : Windows 7 / Windows 10
Victim machine : Windows XP / Windows 7

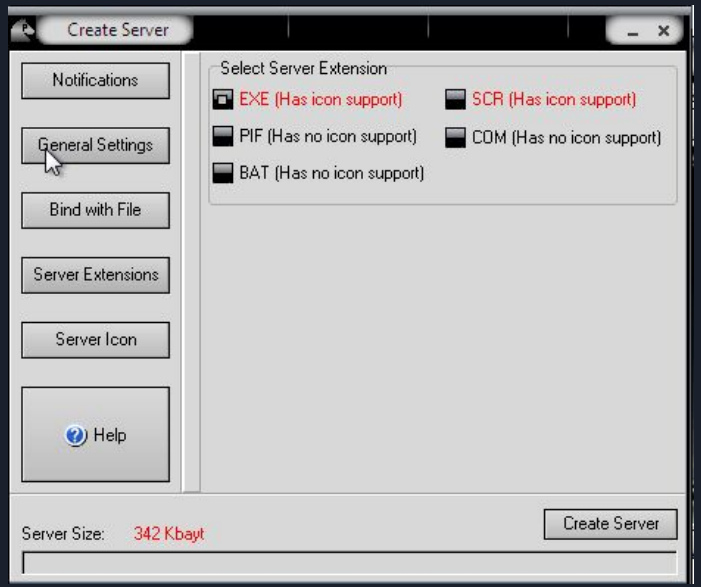
- Trojan Software used : Prorat
- Hacker Machine : Windows 7
- Victim Machine : Windows XP

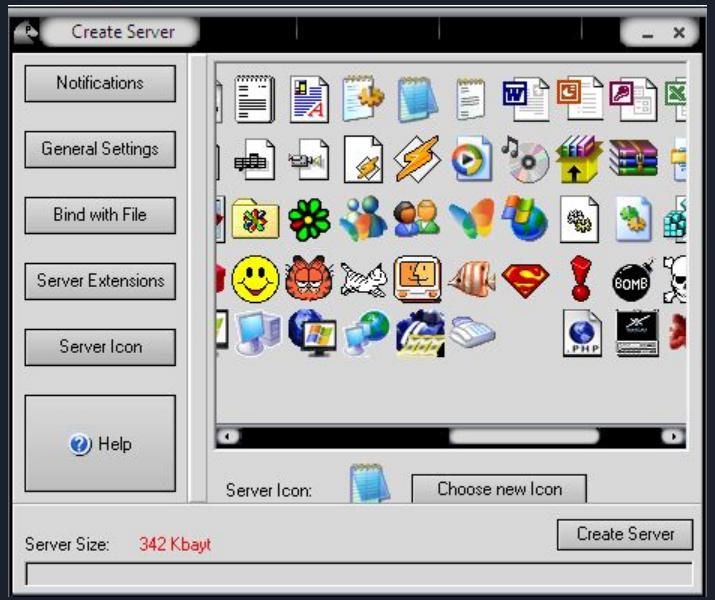
- Launch Prorat in Hacker Machine.
- Create a new Prorat Server.
- We will be selecting the following Options :
  - Melt Server on Install (Deletes Trojan File once executed).
  - Kill AV-FW on install (Disables Antivirus and Firewall once executed).
  - Disable Windows XP SP2 Firewall Center.
  - Clear Windows XP Restore Points.
  - Invisibility (to keep process invisible from the victim).
- We will also bind the trojan with a fake notepad file



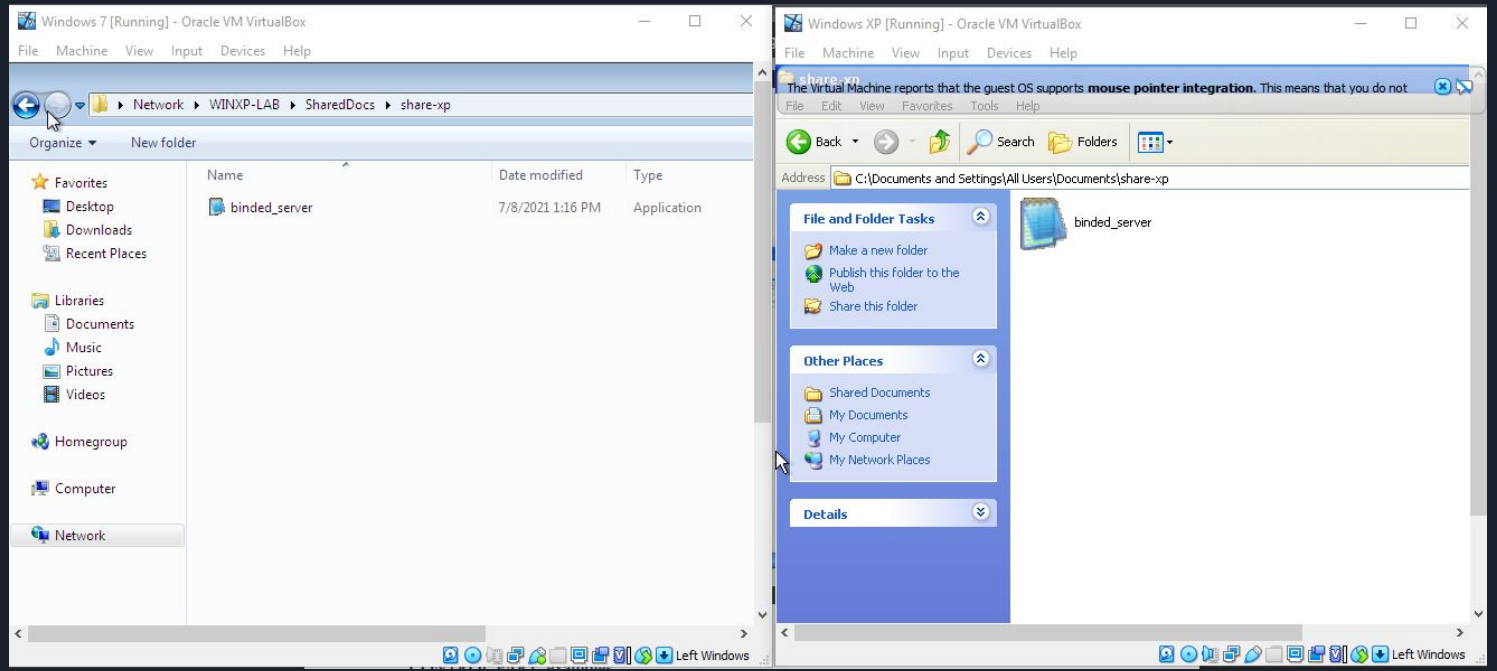


- We will set the server extension as exe.
- We can also change the file icon to be used for the server.
- This way, we can create the server.



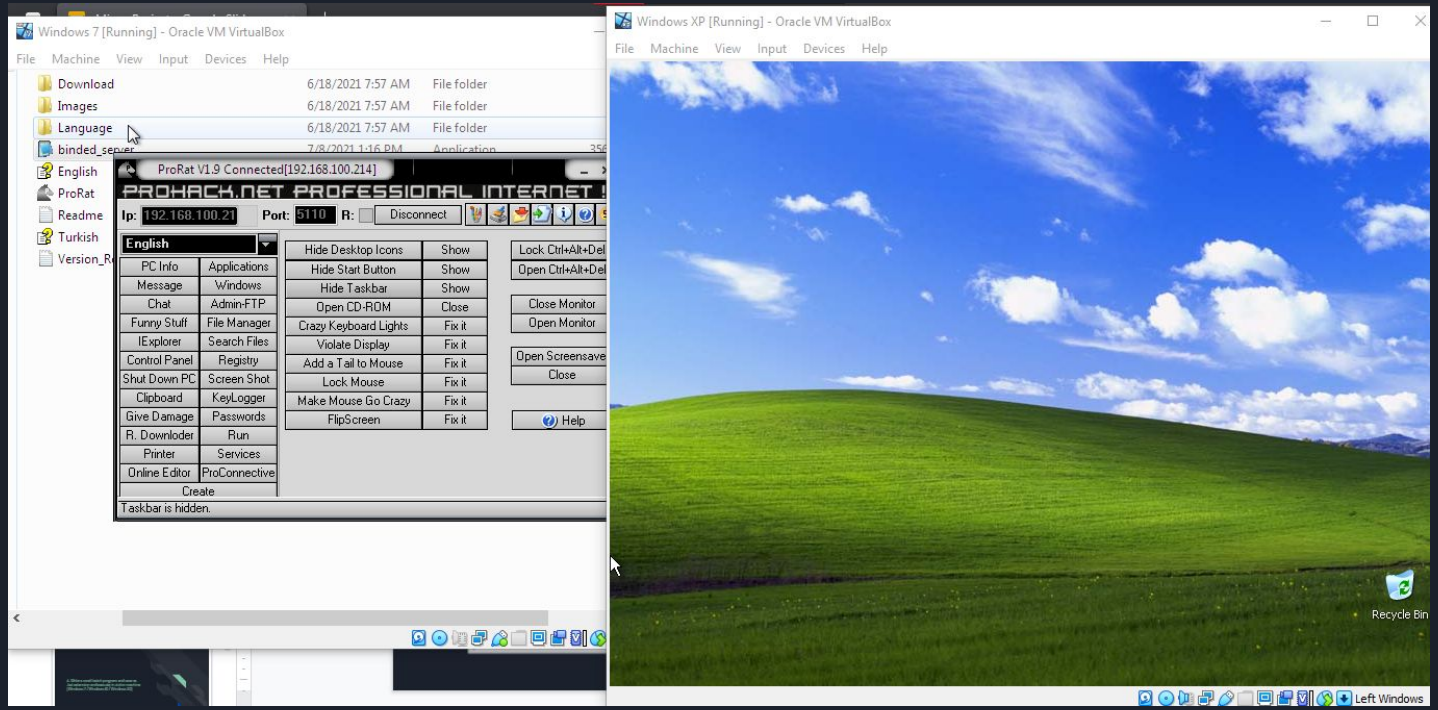


- We then send the newly created server to the victim.
- And then we run the server on the Victim Machine.
- From Prorat, we can connect to the Victim Machine by using it's IP Address, Port Number and the Password we created earlier.



- Coming Back to the Hacker Machine, we can access all kinds of information of the Victim once the server has been started.

- We can also do many kinds of activities pre-built into Prorat (Ex: Hiding the Taskbar).



- We can also record Keylogs i.e. whatever is typed on the Victim machine using Prorat.

Measures to keep the System safe from these kinds of attacks

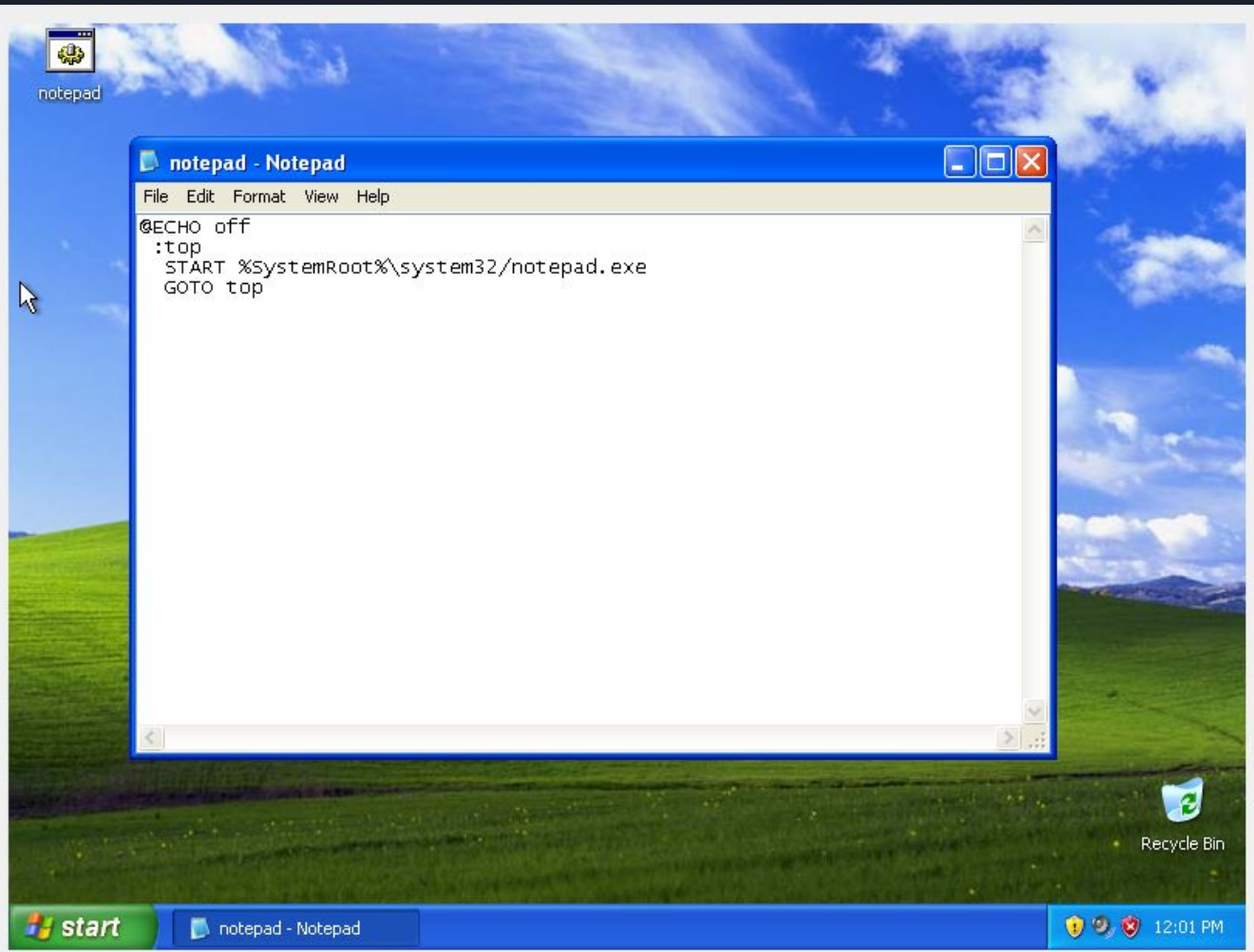
- Keeping the Firewall and Antivirus Active all the time.
- Updating the Antivirus and Firewall definitions to the latest ones (Keep them updated).
- Checking and Analyzing for any suspicious files or activities running in the system.
- Since trojans like Prorat and Darkcomet use a binding file to execute their servers, we have to be on alert and check a file before we try to open it.

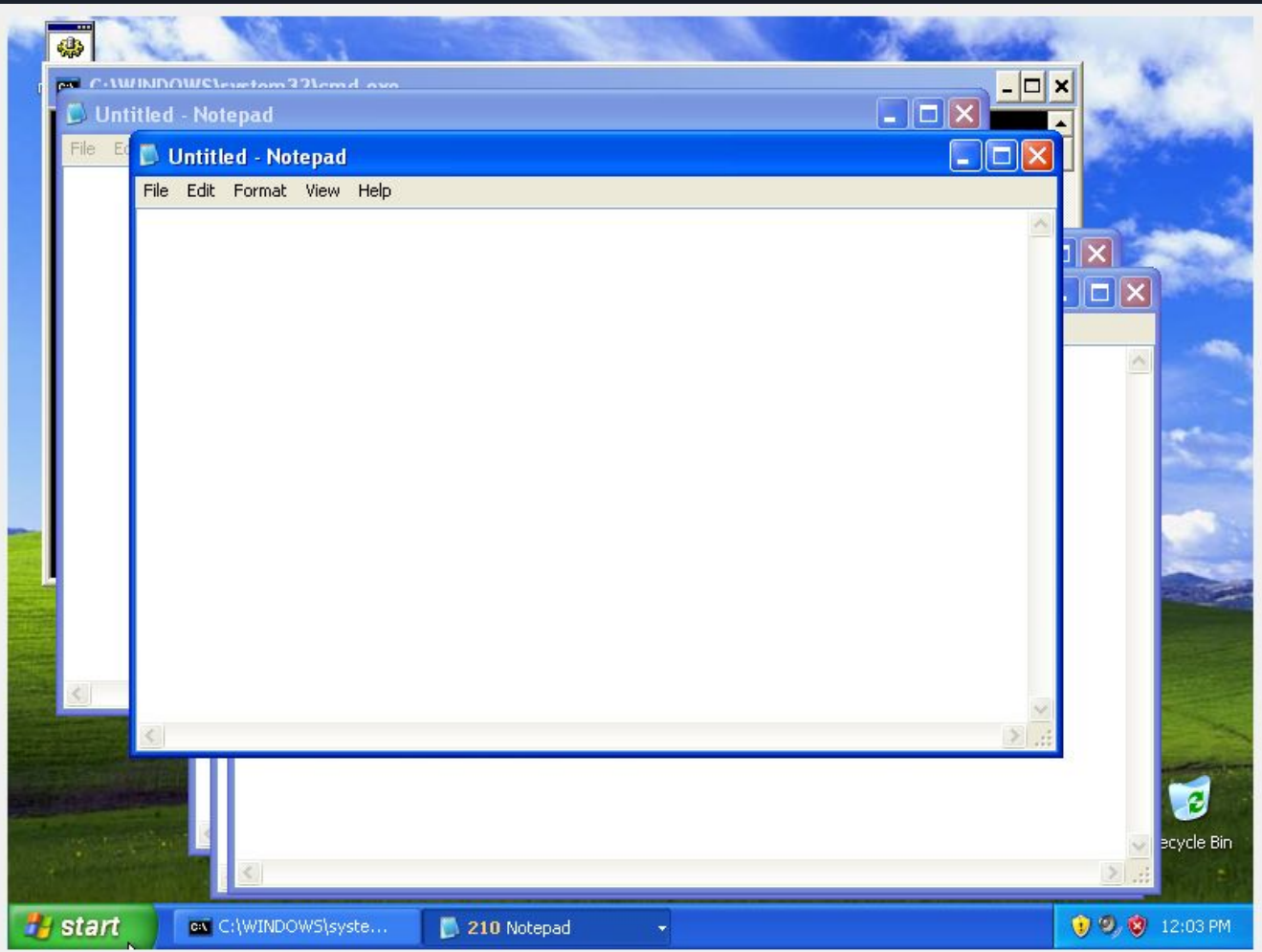
4. Write a small batch program and save as .bat extension and execute in victim machine (Windows 7 / Windows 10 / Windows XP)

- Victim Machine : Windows XP
- Code :

```
@ECHO off

: top

START %SystemRoot%\system32\notepad.exe

GOTO top
```

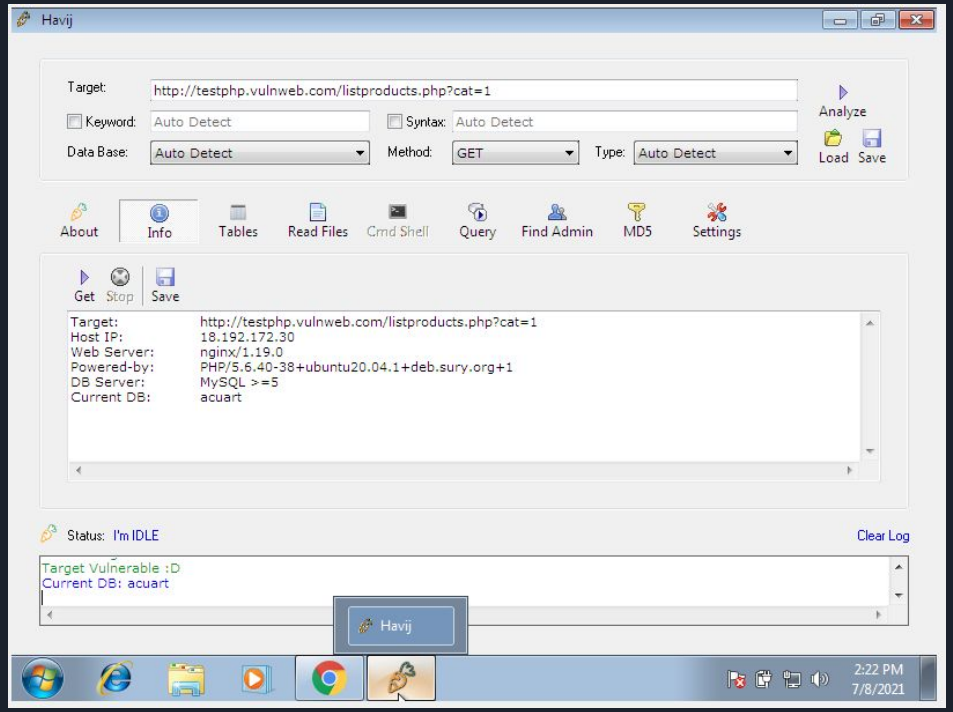
- Create a file with the above Code and save it as .bat extension in the Victim Machine.
- Then execute the bat file in the Victim Machine.
- This code will create endless Notepad Windows in the Victim Machine as shown in the below pictures.


notepad
notepad - Notepad
File Edit Format View Help
@ECHO off
:top
START %SystemRoot%\system32/notepad.exe
GOTO top
Recycle Bin
start
notepad - Notepad
12:01 PM

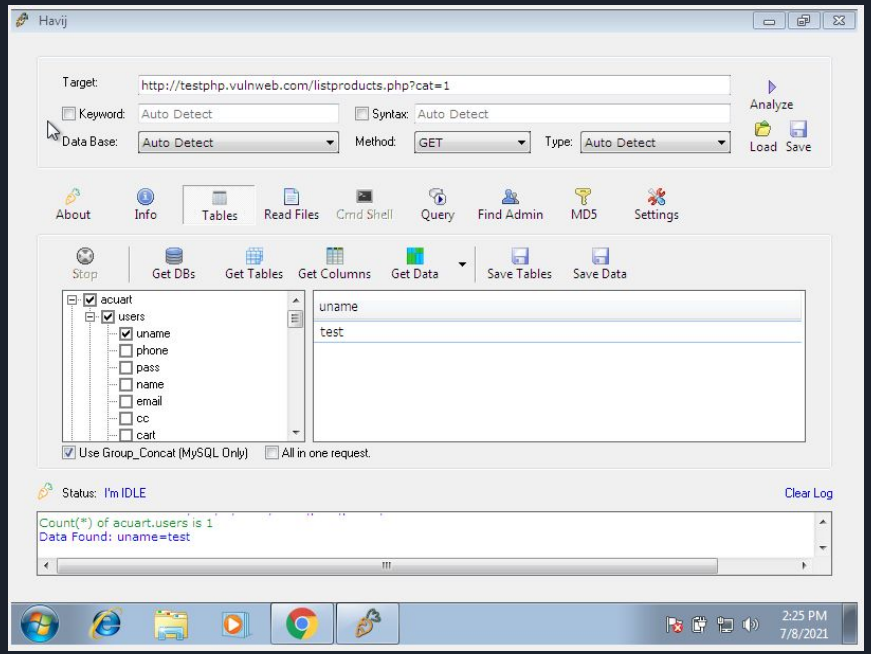

Untitled - Notepad
File Edit Format View Help
Untitled - Notepad
start
C:\WINDOWS\syste...
210 Notepad
12:03 PM

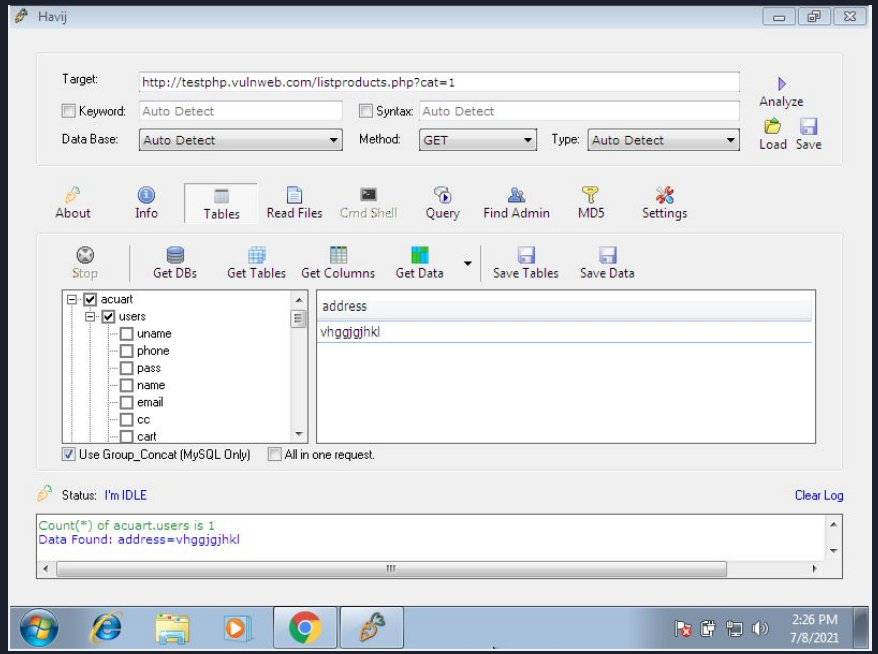
5. Perform SQL injection on by using Havij Tool(Download it from Internet) on http://testphp.vulnweb.com Write a report along with screenshots and mention preventive steps to avoid SQL injections.

- Install Havij in your system.
- Launch the Havij Tool.
- Enter the website to be hacked in the target field in the tool and perform the analysis.



- From here, we can get the Database details, each Row and Column and also each data using the Havij Tool.



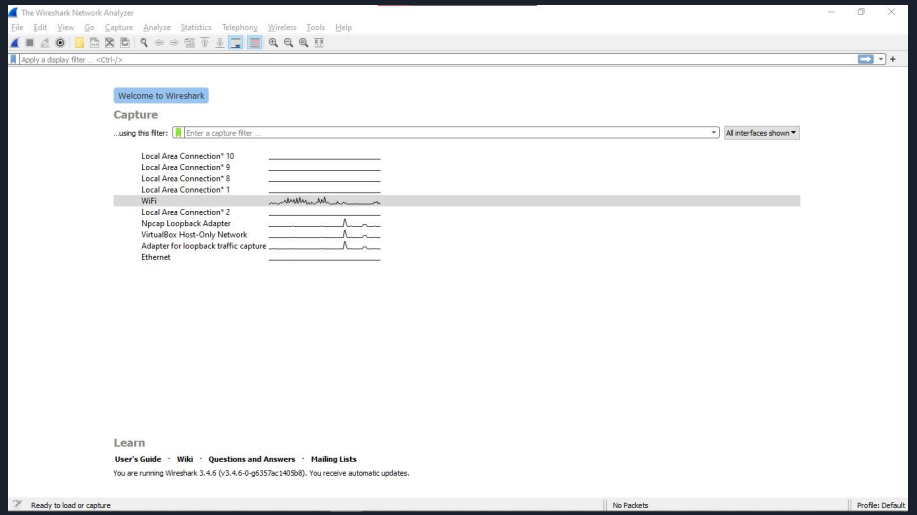


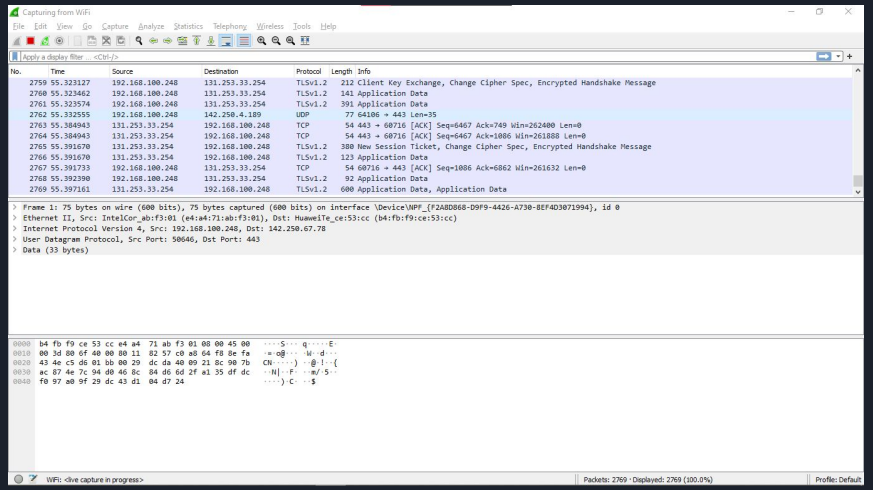
Steps to Prevent SQL Injections

- Input Validation : Validating Input before passing it as an SQL Query.
- Limiting Special Character Inputs.
- Updating Database Security Definitions.
- Restricting Access to admin privileges.
- Using Web Application Firewalls

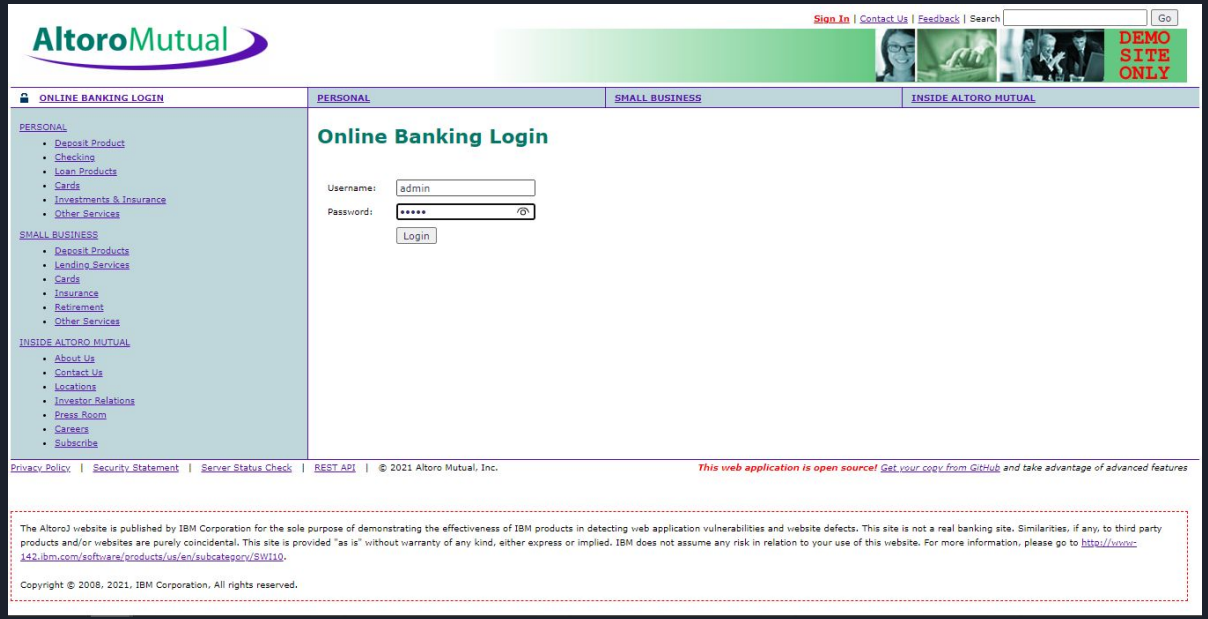
6. Use Wireshark Tool(Download it from Internet) to sniff the data and try to get the username and password of http://demo.testfire.net/

- Install Wireshark on the Physical Machine.
- Launch the Wireshark Application as an Administrator.
- Select on Wifi to start capturing and sniffing data.

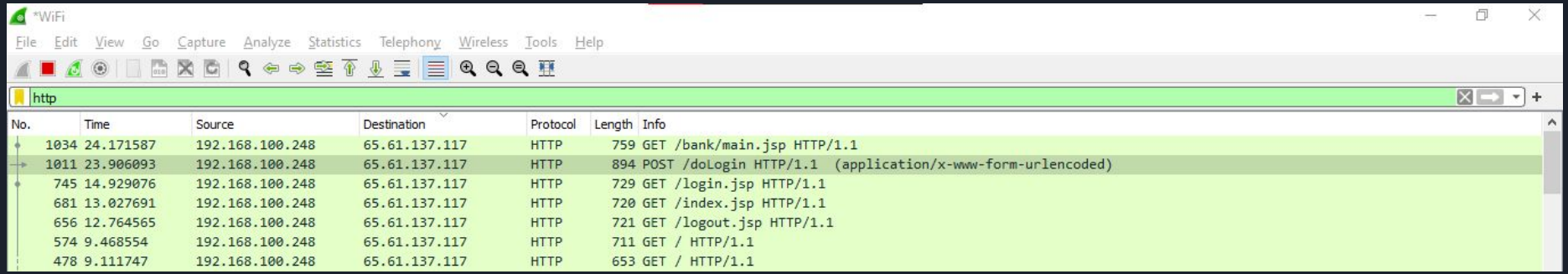




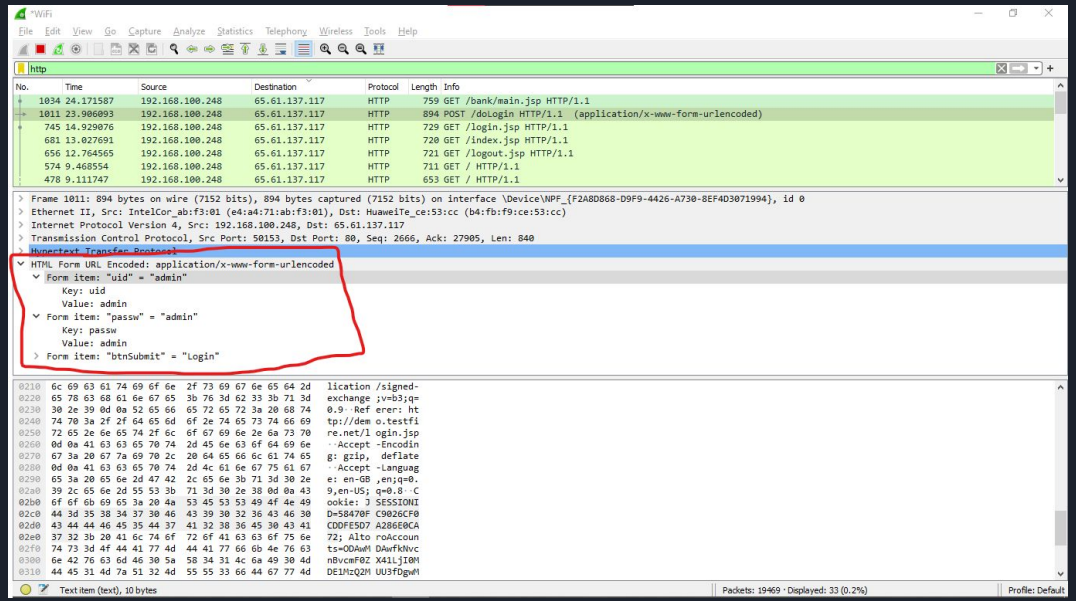
- Launch the Website in a new tab of your browser.
- Click on the Login Section of the Website.
- Enter any fake/real login username and password to login to the account.
- We will be entering Username : admin, Password : admin as login.



- Once we have successfully logged in, open the Wireshark Window.
- Type the ‘http’ filter in the filter box and search for the data.
- Look for the IP address of the website and also the login packets sent and received from the website.



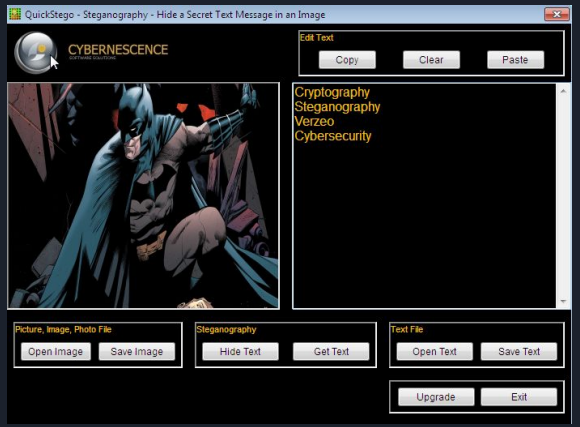
- Open the data packet with POST Info from our website's IP address.
- Open the HTML Form URL Encoded section of the data packet to see the details.
- There we can see the entered Username and Password we used to login to our account.

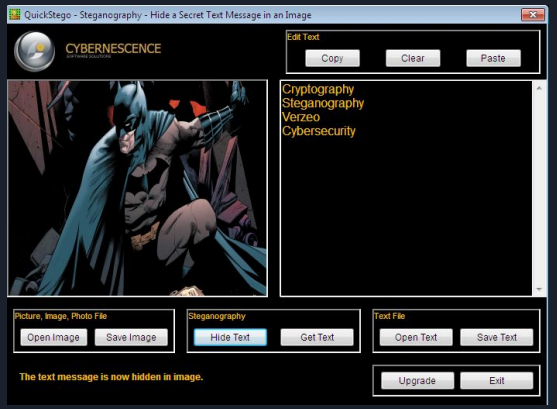


8. Try to Encrypt the Data in image file using quick stego tool (Download from Internet) and command prompt also and show them how to decrypt also. Write a report advantages of cryptography and steganography.

Encryption and Decryption using Quick Stego Tool

- Install the quick stego tool in your system.
- Choose and Image and a text file.
- Open the text and Image file inside the Quick Stego tool.
- Then click on Hide Text Option to encrypt the data inside the Image.
- Save the new image.

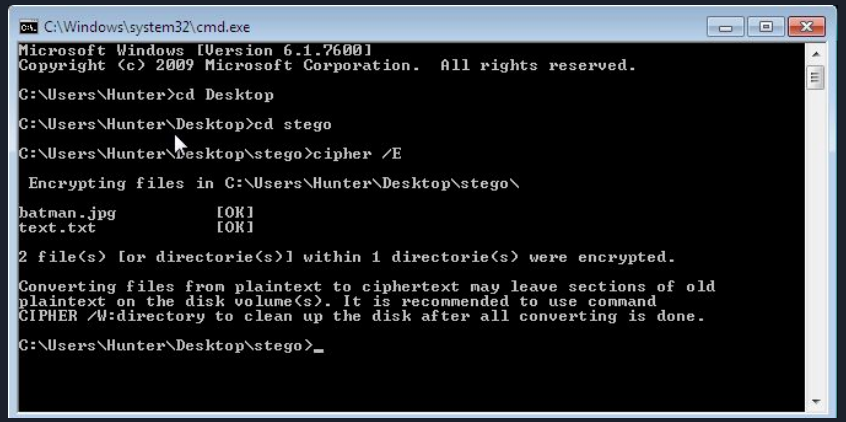




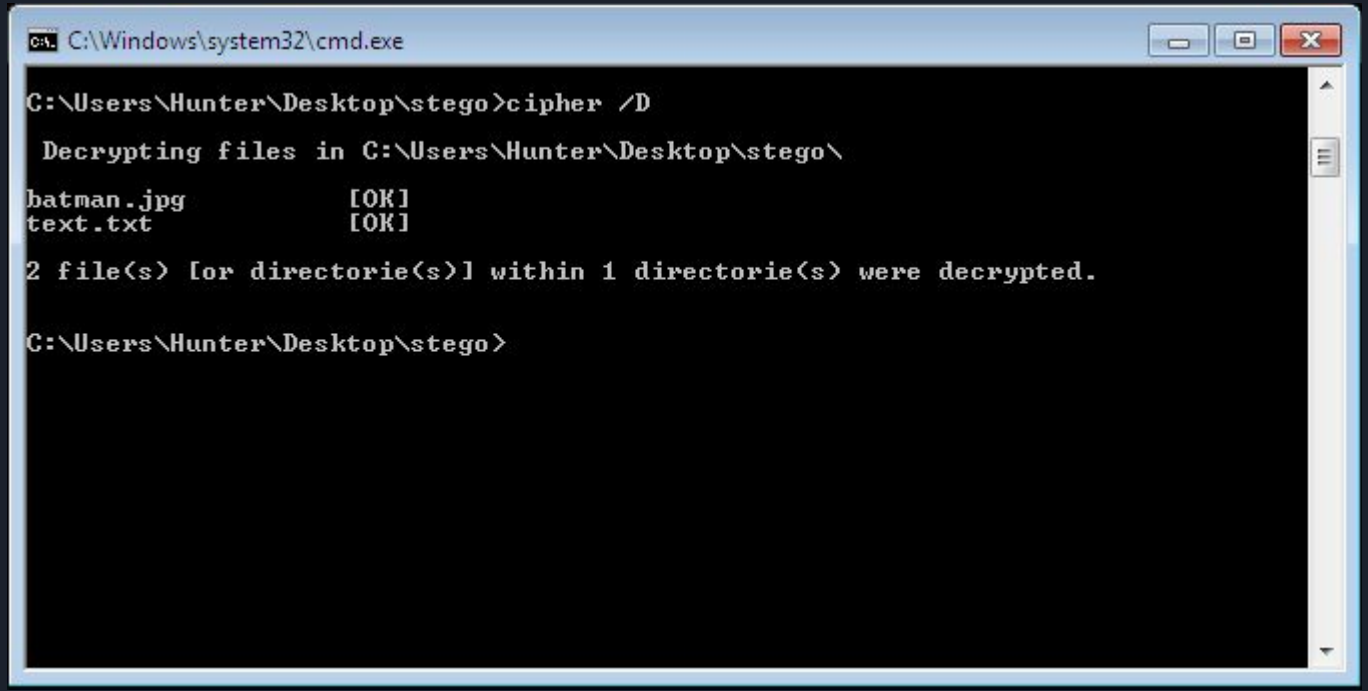
- To decrypt the Encrypted Image, open the encrypted image first in the quick stego tool.
- Once the image is opened, the tool will automatically display the Hidden text.

Encryption and Decryption using CMD

- We can use the cipher command to encrypt and decrypt a specific file/folder from Command Prompt.
- Open CMD first and navigate to the folder to encrypt the contents inside the folder.
- Enter the command cipher /E to encrypt the contents of the Folder.



- To decrypt the contents of the folder, use the command cipher /D while being in the same folder in CMD.



Advantages of Cryptography and Steganography

- The main advantage of Cryptography is confidentiality of the information. Even if the data is hacked, the hackers may not be able to see the actual data if it is encrypted properly.
- Data Encryption also allows the data to remain separate from the worries of Device Security.
- Steganography can be used to hide sensitive and critical data in the middle of simple data as we have seen in the earlier Quick Stego tutorial.

THANK YOU