

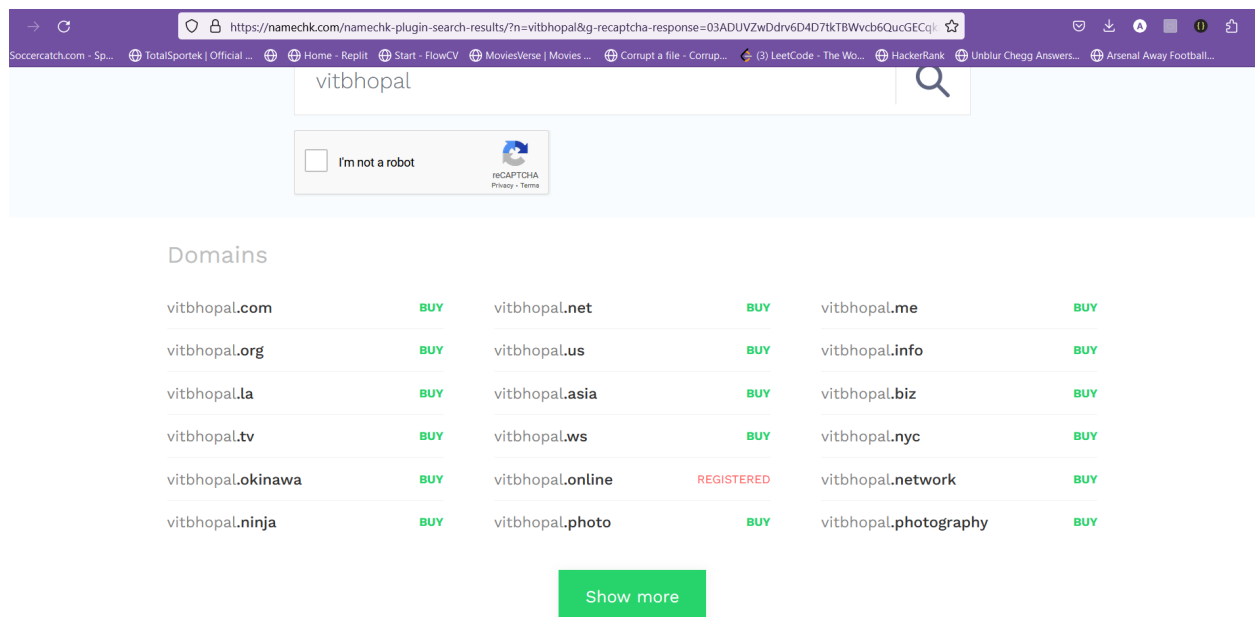
Class 8 - 01/09/2023

Today we installed Kali Linux on VirtualBox.

Task - Information gathering <https://vitbhopal.ac.in/>

We are using OSINT (<https://osintframework.com/>) framework for getting the information on our target:

1. **Username Search Engines:** using the domain name, i found what domains were available for this specific domain name:



2. **DNS Whois Record:** A DNS (Domain Name System) Whois record is a database that contains information about a domain name, such as the domain name owner, contact information, and the domain name's registration status. The Whois DNS record for the targeted website is:

Domain Name: vitbhopal.ac.in
Registry Domain ID: D41440000000585585-IN
Registrar WHOIS Server:
Registrar URL: http://www.ernet.in
Updated Date: 2017-08-18T04:53:00Z
Creation Date: 2016-04-01T06:19:57Z
Registry Expiry Date: 2027-04-01T06:19:57Z
Registrar: ERNET India
Registrar IANA ID: 800068
Registrar Abuse Contact Email:
Registrar Abuse Contact Phone:
Domain Status: ok http://www.icann.org/epp#OK
Registry Registrant ID: REDACTED FOR PRIVACY
Registrant Name: REDACTED FOR PRIVACY
Registrant Organization: VIT University
Registrant Street: REDACTED FOR PRIVACY
Registrant Street: REDACTED FOR PRIVACY
Registrant Street: REDACTED FOR PRIVACY
Registrant City: REDACTED FOR PRIVACY
Registrant State/Province:
Registrant Postal Code: REDACTED FOR PRIVACY
Registrant Country: IN
Registrant Phone: REDACTED FOR PRIVACY
Registrant Phone Ext: REDACTED FOR PRIVACY
Registrant Fax: REDACTED FOR PRIVACY
Registrant Fax Ext: REDACTED FOR PRIVACY
Registrant Email: Please contact the Registrar listed above
Registry Admin ID: REDACTED FOR PRIVACY
Admin Name: REDACTED FOR PRIVACY
Admin Organization: REDACTED FOR PRIVACY
Admin Street: REDACTED FOR PRIVACY
Admin Street: REDACTED FOR PRIVACY
Admin Street: REDACTED FOR PRIVACY
Admin City: REDACTED FOR PRIVACY
Admin State/Province: REDACTED FOR PRIVACY
Admin Postal Code: REDACTED FOR PRIVACY
Admin Country: REDACTED FOR PRIVACY
Admin Phone: REDACTED FOR PRIVACY
Admin Phone Ext: REDACTED FOR PRIVACY
Admin Fax: REDACTED FOR PRIVACY
Admin Fax Ext: REDACTED FOR PRIVACY
Admin Email: Please contact the Registrar listed above
Registry Tech ID: REDACTED FOR PRIVACY
Tech Name: REDACTED FOR PRIVACY
Tech Organization: REDACTED FOR PRIVACY
Tech Street: REDACTED FOR PRIVACY
Tech Street: REDACTED FOR PRIVACY
Tech Street: REDACTED FOR PRIVACY
Tech City: REDACTED FOR PRIVACY
Tech State/Province: REDACTED FOR PRIVACY
Tech Postal Code: REDACTED FOR PRIVACY
Tech Country: REDACTED FOR PRIVACY

```
Tech Phone: REDACTED FOR PRIVACY
Tech Phone Ext: REDACTED FOR PRIVACY
Tech Fax: REDACTED FOR PRIVACY
Tech Fax Ext: REDACTED FOR PRIVACY
Tech Email: Please contact the Registrar listed above
Name Server: ns-1126.awsdns-12.org
Name Server: ns-65.awsdns-08.com
Name Server: ns-797.awsdns-35.net
Name Server: ns-1911.awsdns-46.co.uk
DNSSEC: unsigned
URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
>>> Last update of WHOIS database: 2023-09-01T14:09:24Z <<<
```

3. Analyzing DNSSEC problems for the domain name vitbhopal

DNSSEC (Domain Name System Security Extensions) is a set of security extensions to the Domain Name System (DNS) protocol. It helps to protect against DNS spoofing and cache poisoning attacks.

.	✔ Found 2 DNSKEY records for .
.	✔ DS=20326/SHA-256 verifies DNSKEY=20326/SEP
.	✔ Found 1 RRSIGs over DNSKEY RRset
.	✔ RRSIG=20326 and DNSKEY=20326/SEP verifies the DNSKEY RRset
.	⚠ Zone . (192.112.36.4) returns NXDOMAIN for vitbhopal
.	✔ Found 1 RRSIGs over NSEC RRset
.	✔ RRSIG=11019 and DNSKEY=11019 verifies the NSEC RRset
.	✔ NSEC proves no records exist with name vitbhopal
.	✔ NSEC proves no records exist with name *

4. Domain Reputation:

Report Overview

URL
vitbhopal.ac.in/

IP
14.99.16.252

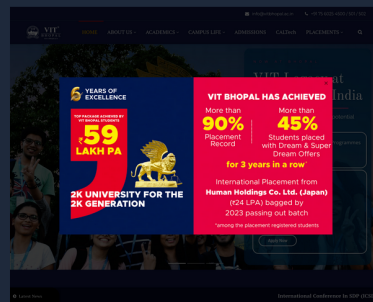
Submitted
2023-09-03T06:47:13Z

Tags
None

urlquery detections
No alerts detected

ASN
#45820 Tata Teleservices ISP AS

Access
public



Detections

urlquery	Network Intrusion Detection	Threat Detection Systems
0	4	0

Domain Summary

DOMAIN	RANK	FIRST SEEN	LAST SEEN	SENT	RECEIVED	IP
vitbhopal.ac.in (100)	371224	2017-03-07 09:30:47	2023-08-31 04:16:10	59459	6741793	14.99.16.252
fonts.gstatic.com (13)	unknown	2014-09-09 02:40:21	2023-09-03 06:25:08	7049	288655	142.250.74.3
www.googletagmanager.com (3)	75	2013-05-22 04:07:37	2023-09-03 07:10:05	1317	224270	142.250.74.168
jnn-pa.googleapis.com (6)	2640	2021-11-16 07:12:21	2023-09-03 06:34:07	3737	67589	142.250.74.74
api.hubapi.com (1)	4102	2012-06-25 20:13:07	2023-09-02 05:23:56	493	1957	104.17.200.204
ocsp.godaddy.com (1)	698	2012-05-20 21:28:57	2023-09-03 05:09:22	330	2615	192.124.249.23
embed.tawk.to (3)	8650	2014-03-19 22:03:49	2023-09-02 05:52:34	1364	6956	172.67.38.66
lytimg.com (2)	109	2012-10-03 19:11:04	2023-09-03 06:34:07	1094	57978	142.250.74.118
yt3.ggpht.com (2)	203	2014-01-15 17:55:17	2023-09-03 05:32:24	970	10304	142.250.74.161
ajax.googleapis.com (1)	12905	2013-08-16 11:51:31	2023-09-03 07:39:45	430	7774	142.250.74.138
ocsp.pki.goog (19)	175	2018-07-01 08:43:07	2023-09-03 05:10:35	6327	13293	142.250.74.131
fonts.googleapis.com (2)	8877	2013-06-10 22:14:26	2023-09-03 06:16:22	990	36635	142.250.74.106

www.youtube.com (15)	90	2013-04-13 09:43:20	2023-09-03 05:10:03	9087	2019600	142.250.74.78
forms.hsforms.com (1)	5160	2018-03-07 16:21:13	2023-09-02 08:44:21	483	1014	104.17.207.249
www.google.com (5)	7	2015-05-10 13:11:19	2023-08-28 20:45:32	3118	34573	142.250.74.132
www.google.no (3)	25607	2016-04-05 21:50:59	2023-09-03 07:28:48	2205	2274	142.250.74.163


Related reports

DOMAIN

IP

ASN

SCREENSHOT

DATE	UQ / IDS / TDS	URL	IP
2023-09-03T06:47:13Z	0 - 4 - 0	vitbhopal.ac.in/	 14.99.16.252

Network Intrusion Detection Systems

Suricata /w Emerging Threats Pro

TIMESTAMP	SEVERITY	SOURCE IP	DESTINATION IP	ALERT
2023-09-03T06:46:42Z	medium	Client IP	Internal IP	ET DNS Query for .to TLD
2023-09-03T06:46:42Z	medium	Client IP	Internal IP	ET DNS Query for .to TLD
2023-09-03T06:46:50Z	medium	Client IP	Internal IP	ET DNS Query for .to TLD
2023-09-03T06:46:50Z	medium	Client IP	Internal IP	ET DNS Query for .to TLD

Threat Detection Systems

Public InfoSec YARA rules

No alerts detected

OpenPhish

No alerts detected

PhishTank

No alerts detected

Fortinet's Web Filter
























No alerts detected

mnemonic secure dns

No alerts detected

Quad9 DNS


No alerts detected

URL	IP	RESPONSE	SIZE
  vitbhopal.ac.in/	 14.99.16.252	200 OK	62219
 vitbhopal.ac.in/ext/PW-Pro-News-Ticker-For-VC//css/fontawesome/font-awesome.css	 14.99.16.252		6838
 ocsp.pki.goog/gts1c3	 142.250.74.131		472
 ocsp.pki.goog/gts1c3	 142.250.74.131		472
 vitbhopal.ac.in/ext/PW-Pro-News-Ticker-For-VC//css/public.css	 14.99.16.252		6900
 ocsp.pki.goog/gts1c3	 142.250.74.131		472
 ocsp.godaddy.com/	 192.124.249.23		2107
 vitbhopal.ac.in/ext/PW-Pro-News-Ticker-For-VC//css/bx-slider/jquery.bxslider.css	 14.99.16.252		1830
 vitbhopal.ac.in/ext/PW-Pro-News-Ticker-For-VC//css/magnific-popup/magnific-popup.css	 14.99.16.252		5120
 vitbhopal.ac.in/ext/PW-Pro-News-Ticker-For-VC//css/marquee/queue.css	 14.99.16.252		768
 vitbhopal.ac.in/ext/PW-Pro-News-Ticker-For-VC//css/custom-css.css	 14.99.16.252	200 OK	116
 vitbhopal.ac.in/ext/instagram-feed-pro/css/sbi-styles.min.css	 14.99.16.252		13740
 vitbhopal.ac.in/ext/contact-form-7/includes/css/styles.css	 14.99.16.252		1302

5. DNS records for https://vitbhopal.ac.in/

The Cloudflare DNS server responded with these DNS records.

A records

IPv4 address	Revalidate in
>  182.73.197.20	1m
>  14.99.16.252	1m

AAAA records




No AAAA records found.

CNAME record

No CNAME record found.

TXT records

Site ownership verification

 Facebook suex5g8znin6g9n1m3c 4cu21chfabd Revalidate in 1m	 Google iKGsPSECwdJGhLq9FVX D- EPCJZ9PGJHCw_nQem5 E55U Revalidate in 1m	 Microsoft 3B1F6E5FC0788A485A8 3BF7E283F279BF1D414 00 Revalidate in 1m
---	--	--

SPF record

This record is valid for 1m.

Include the SPF record at _spf.google.com and pass if it matches the sender's IP.	include:_spf.google.com
Or else, mark the email as fail .	-all


Other TXT records

TXT data	Revalidate in
"4i0oq59273qjsq0pfdpimm02i6"	1m
"ff9qe5moo9inb759raethf1qb5"	1m
"vh66pai2iftjr062fj21t9db49"	1m

NS records

Name server	Revalidate in
ns-1126.awsdns-12.org.	1m
ns-1911.awsdns-46.co.uk.	1m
ns-65.awsdns-08.com.	1m
ns-797.awsdns-35.net.	1m

MX records

Mail server	Priority	Revalidate in
aspmx.l.google.com. 	1 Primary	1m
alt1.aspmx.l.google.com.	5	1m
alt2.aspmx.l.google.com.	5	1m
alt3.aspmx.l.google.com.	10	1m
alt4.aspmx.l.google.com.	10	1m

SOA data		Revalidate in
Start of authority	ns-1126.awsdns-12.org.	15m
Email	awsdns-hostmaster@amazon.com	
Serial	1	
Refresh	2h	
Retry	15m	
Expire	336h	
Negative cache TTL	24h	