

**RALAYALA SEEMA
UNIVERSITY KURNOOL
SRI SANKARS DEGREE
COLLEGE IN KURNOOL**

k.Yella raju

Bsc microbiology

21367008005

Project title:driven information gathering threat intellignece

- ▣ Team ID : LTVIP2024TMID14080
- ▣ Team Size : 5
- ▣ Team Leader : Akthar Shaik Shavali
- ▣ Team member : Boggula Mani Kumar
- ▣ Team member : Darur Rajesh
- ▣ Team member : Gollakatikala Manohar
- ▣ Team member : Kalagondla Yella Raju

index

SNO	TOPICNAME	PAGE NO
1.	Osnit frame work into source key points	5
2.	Osnit frame work on the tools for for dns information gathering	6
3.	Dns for maping source for ruk website detalis analysis	7
4.	Ruk webste details report for tools	8
5.	Srv details and txt for records on the ruk website	9 10 11
6.	Osnit frame work analysis	
7.	Information source intellignce	12
8.	Ibomma website details analysis web cheker and them analysis	13
9.	Tls security for issuses site feature	
10.	Website into web cheker.com target domain 1tamil.mv	14-15

DRIVEN INFORMATION GATHERING THREAT AND INTELLIGENCE

When we use osnit frame work on use
service threat intelligence

Osnit frame work into source key points

- ▣ It seems like you're referring to the OSSTMM (Open Source Security Testing Methodology Manual) framework. Here are some key points about the OSSTMM framework:
- ▣ **Comprehensive Methodology:** OSSTMM is a comprehensive framework for security testing, providing guidelines, techniques, and methodologies for assessing the security posture of systems, networks, and applications.
- ▣ **Open Source:** As the name suggests, OSSTMM is an open-source framework, which means it is freely available for anyone to use, modify, and distribute.
- ▣ **Risk-Based Approach:** OSSTMM emphasizes a risk-based approach to security testing, focusing on identifying and prioritizing security risks based on their potential impact on the organization.
- ▣ **Seven Sections:** The OSSTMM framework is organized into seven main sections:
 - Information Security Foundation
 - Information Security Testing
 - Security Operations
 - Legalities
 - Data Destruction
 - Social Engineering
 - Tools
- ▣ **Methodologies and Techniques:** Within each section, OSSTMM provides detailed methodologies and techniques for conducting various types of security tests, including penetration testing, vulnerability assessment, security auditing, and social engineering assessments.

Osnit frame work on the tools for dns information gathering

IP2Location

IP:	172.17.0.1
Country:	N/A
State:	N/A
City:	N/A
Latitude:	N/A
Longitude:	N/A
ISP:	N/A

IP Location Services by: IP2Location

Updated: April 01 2024



IPInfo.io


IP:	172.17.0.1
Country:	N/A
State:	N/A
City:	N/A
Latitude:	N/A
Longitude:	N/A
ISP:	N/A
Proxy:	No



Dns for maping source for ruk web site details analysis

Jump to: [A Records](#) [AAAA Records](#) [CNAME Records](#) [MX Records](#) [NS Records](#) [PTR Records](#) [SRV Records](#) [SOA Records](#) [TXT Records](#) [CAA Records](#) [DS Records](#) [DNSKEY Records](#)

A

Type	Domain Name	TTL	Address
A	www.rayalaseemauniversity.ac.in/	14400	116.206.105.72 Check IP Blacklist Owner: Bigrock Solutions Ltd  WHOIS AS394695


AAAA

Sorry no record found!

CNAME

Type	Domain Name	TTL	Canonical Name
CNAME	www.rayalaseemauniversity.ac.in/	14400	rayalaseemauniversity.ac.in.

MX

Type	Domain Name	TTL	Preference	Address
MX	www.rayalaseemauniversity.ac.in/	14400	0	rayalaseemauniversity.ac.in.(116.206.105.72 Check IP Blacklist) Owner: Bigrock Solutions Ltd  WHOIS AS394695

NS

Type	Domain Name	TTL	Canonical Name
------	-------------	-----	----------------

Ruk website into report for domain

MX Records

MX records for **www.rayalaseemauniversity.ac.in**:

Record	Type	Priority	Target	TTL
rayalaseemauniversity.ac.in	MX	0	rayalaseemauniversity.ac.in.	14400

```
id 50240, opcode QUERY, rcode NOERROR, flags QR RD RA
;QUESTION
www.rayalaseemauniversity.ac.in. IN MX
;ANSWER
www.rayalaseemauniversity.ac.in. 14400 IN CNAME rayalaseemauniversity.ac.in.
rayalaseemauniversity.ac.in. 14400 IN MX 0 rayalaseemauniversity.ac.in.
;AUTHORITY
;ADDITIONAL
```

[Show results globally →](#)

NS Records

NS records for **www.rayalaseemauniversity.ac.in**:

Record	Type	Value	TTL
rayalaseemauniversity.ac.in	NS	ns2.cp-in-17.bigrockservers.com.	21600
rayalaseemauniversity.ac.in	NS	ns1.cp-in-17.bigrockservers.com.	21600

```
id 9613, opcode QUERY, rcode NOERROR, flags QR RD RA
;QUESTION
www.rayalaseemauniversity.ac.in. IN NS
;ANSWER
```


Srv details and txt records on the ruk website

SRV Records

No SRV records found for **www.rayalaseemauniversity.ac.in**.

```
id 39154, opcode QUERY, rcode NOERROR, flags QR RD RA
;QUESTION
www.rayalaseemauniversity.ac.in. IN SRV
;ANSWER
www.rayalaseemauniversity.ac.in. 14400 IN CNAME rayalaseemauniversity.ac.in.
;AUTHORITY
rayalaseemauniversity.ac.in. 1800 IN SOA ns1.cp-in-17.bigrockservers.com. sales.bigrock.in. 2024022701 86400 7200 3600000 86400
;ADDITIONAL
```

[Show results globally →](#)

TXT Records

TXT records for **www.rayalaseemauniversity.ac.in**:

Record	Type	Value	TTL
rayalaseemauniversity.ac.in	TXT	"v=spf1 ip4:116.206.105.72 +a +mx ~all"	14400

```
id 31031, opcode QUERY, rcode NOERROR, flags QR RD RA
;QUESTION
www.rayalaseemauniversity.ac.in. IN TXT
;ANSWER
www.rayalaseemauniversity.ac.in. 14400 IN CNAME rayalaseemauniversity.ac.in.
rayalaseemauniversity.ac.in. 14400 IN TXT "v=spf1 ip4:116.206.105.72 +a +mx ~all"
;AUTHORITY
;ADDITIONAL
```

[Show results globally →](#)

Osnit frame work anaylsis for

Sources of Cyber Threat Intelligence

Cyber Threat Intelligence (CTI) refers to information gathered from collated data on present and potential threats. In order to gather information, there has to be sources to obtain them from. There are many sources of CTI and they can be categorised into one of the following:

Open-Source Intelligence (OSINT)

This refers to intelligence that has been made publicly available for use. This comprises of the resources found on the internet such as Social media (Facebook, Twitter, Instagram), Video sharing websites (YouTube) and other types of websites that provide information (Wikipedia, Pastebin, VirusTotal, Shodan, FireEye), Media like Newspapers and Magazines, and Professional/Academic publications that can be found at Libraries. This is the most commonly used source of CTI mainly because of vastness as well as being the only free source.



Figure showing the OSINT Framework [4]

Information source intelligence

Commercial Vendors

The term refers to companies and businesses that specialize in everything Cyber Security and they provide services and information to other companies that require. The information obtained from or services rendered by these commercial vendors can be company specific, geographical location specific or cybercrime specific depending on the needs of the company hiring. However, as a result of the type of services rendered, there is a fee to be paid and depending on the reputation of the commercial vendor it could be very expensive. Symantec is currently one of the world's leading Cyber Security Vendors and they provide security for small, medium and enterprise businesses. Other Vendors include Blackberry, AT&T, Fortinet, Proofpoint.[5]

In-House Threat Intelligence

This is obtained when a company runs internal tests and diagnostics on its networks and systems to determine its security level. These tests could be in form of vulnerability tests to see if there are any vulnerabilities with regards to applications and servers connected to the company's network or monitoring of network activities to check for malicious activities. The results from these tests (also known as Security analytics) can be used to strengthen security levels. Company staff in charge of these tasks include incident response teams, security operations centre (SOC) personnel, and security analysts.[6]

Human Intelligence (HUMINT)

This refers to information gathered from contact with another individual. An example is having a one-on-one conversation with an employee (who could be a friend) of a rival company that was recently involved in a Cyber-attack whereby the individual outlines the methodologies of the **Advanced Persistent Threat (APT)**. Another example is attending a symposium/seminar whose subject matter could be an APT. The information obtained from both cases can be used to protect a company against that certain APT.

To ensure getting the information from the best source, the following should be considered:

- Are they updated regularly (monthly, yearly, or how)?
- How will the information be delivered to you?
- Which file formats is the information?
- Does the vendor provide alerts and reports? Will that be company specific or generic to everyone?

Ibomma web site details anaylsis for webcheker.site in them analysis

21 jobs successful 4 jobs skipped 8 jobs failed

Finished in 19300 ms

Show Details

Show Filters

Export Data

Learn About The Results

More Tools

View GitHub

SSL Certificate

Subject

ibomma.re

Issuer

Google Trust Servic...

Expires

24 May 2024

Renewed

24 February 2024

Serial Num

D8DE35E045495A78114...

Fingerprint

FF:3F:0E:F3:FE:13:B...

Extended Key Usage

TLS Web Server Authentication

HTTP Security

Content Security Policy

No

Strict Transport Policy

No

X-Content-Type-Options

No

X-Frame-Options

No

X-XSS-Protection

No

DNSSEC

DNSKEY

DNSKEY - Present?

No

DS

DS - Present?

No

RRSIG

Domain Whois

Title

ibOMMA - Watch Telugu mov...

Description

ibOMMA - Watch Telugu mov...

Canonical URL

https://run.ibomma.re/tel...

Theme Color

#1d1d1d

BOOKMARK US

WWW.IBOMMA.ONE

Headers

date

7 April 2024

content-type

text/html

transfer-encoding

chunked

connection

close

last-modified

7 April 2024

cache-control

max-age=120

cf-cache-status

HIT

age

4239

report-to

{"endpoints":[{"url":"htt...

nel

{"success_fraction":0,"re...

vary

Accept-Encoding

server

cloudflare

cf-ray

87078d9888c26361-LHR

alt-svc

h3=":443"; ma=86400

Security.Txt

Present

No

Having a security.txt ensures security researchers know how and where to safely report vulnerabilities.

Threats

Google Safe Browsing

Safe

Phishing Status

No Phishing Found

DNS Records

A

104.21.64.198

AAAA

104.21.64.198

172.67.155.136

MX

2606:4700:3033::6815:40c6

2606:4700:3033::ac43:9b88

Firewall

Firewall

Yes

WAF

Cloudflare

TLS Cipher Suites

0

No cipher suites found. This sometimes happens when the report didn't finish generating in-time, you can try re-requesting it.

Refetch Report

Linked Pages

[illegible]

Website into webchecker 1tamil.mv after analysis and dns servers

web-check.xyz/results/https%3A%2F%2Fwww.1tamilmv.yt

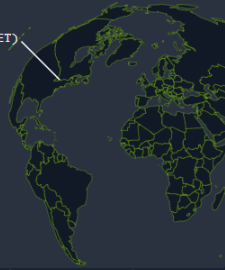
Wix Website Editor

Show FiltersExport DataLearn About The ResultsMore ToolsView GitHub

Server Location

City	M5A, Toronto, Ontario
Country	Canada 🇨🇦
Timezone	America/Toronto
Languages	en-CA, fr-CA, iu
Currency	Dollar (CAD)

Server (CLOUDFLARENET)



Latitude: 43.709, Longitude: -79.4057

Cookies

▶ ips4_IPSSessionFront

oqilmnvsejpp62f35sula3bds5

HTTP Security

Content Security Policy	✗ No
Strict Transport Policy	✗ No
X-Content-Type-Options	✗ No

SSL Certificate

Subject	1tamilmv.yt
Issuer	Google Trust Servic...
Expires	4 July 2024
Renewed	5 April 2024
Serial Num	65C72601B2E4AF650DF...
Fingerprint	57:2E:8A:86:FC:6F:8...

Extended Key Usage

TLS Web Server Authentication

Headers

date	7 April 2024
content-type	1 August 2001
transfer-encoding	chunked
connection	close
set-cookie	ips4_IPSSessionFront=iak2...
x-ips-loggedin	1 January 2000
vary	Cookie, Accept-Encoding
x-xss-protection	1 January 2000
x-frame-options	sameorigin
referrer-policy	strict-origin-when-cross...
x-ips-cached-response	7 April 2024
last-modified	7 April 2024
expires	7 April 2024
cache-control	max-age=30, public, s-max...
x-turbo-charged-by	LiteSpeed
cf-cache-status	DYNAMIC
report-to	{\"endpoints\": [{\"url\": \"htt...
nel	{\"success_fraction\": 0, \"re...

Domain Whois

DNS Records

A	104.21.2.63
AAAA	104.21.2.63
	172.67.128.214
MX	
	2606:4700:3036::ac43:80d6
	2606:4700:3032::6815:23f

Security.Txt

Present

✗ No

Having a security.txt ensures security researchers know how and where to safely report vulnerabilities.

HSTS Check

HSTS Enabled?

✗ No

Site does not serve any HSTS headers.

TLS Handshake Simulation

No entries available to analyze. This sometimes happens when the report didn't finish generating in-time, you can try re-requesting it.

Server Info

Organization	Cloudflare, Inc.
ASN Code	AS13335
Ports	8080,2082,2083,2053,2086,...
IP	104.21.2.63
Type	cdn
Location	San Francisco, United Sta...

Host Names

Domains

stockholmguesthouse.com

Hosts

stockholmguesthouse.com

DNS Server

DNS Server #1

IP Address	104.21.2.63
DoH Support	✗ No*

DNS Server #2

IP Address	172.67.128.214
DoH Support	✗ No*

* DoH Support is determined by the DNS server's response to a DoH query. Sometimes this gives false negatives, and it's also possible that the DNS server supports DoH but does not respond to DoH queries. If the DNS server does not support DoH, it may still be possible to use DoH by using a DoH proxy.





Dns to domain ip adderss for on tamil.mv scaning report

View


www.1tamilmv.yt

DNS Results

A

A	Prefix	ASN
104.21.2.63	104.21.0.0/20	  AS13335 - Cloudflare, Inc.
172.67.128.214	172.67.128.0/20	  AS13335 - Cloudflare, Inc.

AAAA

AAAA	Prefix	ASN
2606:4700:3036::ac43:80d6	2606:4700:3036::/48	  AS13335 - Cloudflare, Inc.
2606:4700:3032::6815:23f	2606:4700:3032::/48	  AS13335 - Cloudflare, Inc.

Queried from the local bgp.tools unbound DNS instance. (lookup bgp.tools for source IPs)