



KUMARAGURU
college of technology
character is life

**KUMARAGURU COLLEGE OF TECHNOLOGY
COIMBATORE**

TEAM – SCRIPT KIDDIES

TEAM MEMBERS

RAJHESHWAR V

MANAVALLAN S

VISHAL M L

DHANUSHKUMAR S G

MENTOR

DR. N. SUGANTHI

Professor

Department of Computer Science and Engineering

Tracking Phishing Message

Problem Statement

It's required to trace the phishing messages to locate the cyber attacker on citizens, who fell into the trap on clicking the link shared. So, Police to get a handy interface with a solution that can fetch the details of servers or mobile numbers (dynamically changing in this case) and provide investigators sufficient information to trace and track the perpetrator.

Solution

An easy-to-use User Interface that can retrieve information about the domain's origin. Using Open-Source, Free API, and MIT Licensed tools, our solution focuses on gathering information and traces back to the attacker. We automate scripts like NMAP Scripting Engine (Network Mapper), and APIs like Shodan, Wappalyzer, WHOIS, URL Extender, DNS Resolver, and concepts like NS Lookup, SSL Certificate Gathering, Username Enumeration, Favicon Examination, DNS Enumeration, Subdomain Enumeration, Mobile Number Lookup, Email ID Lookup, Address Parsing in a webpage, Adult Site Identifier and collecting data from Censys Database to trace IP. Implementing the framework will acquire the origin of the phishing message.

Methodology Adopted

1. WHOIS Enumeration

In this Phase, we get the WHOIS information like Hosting IP Address, Mail Server, Name Server, Domain Registrant, Address, Mobile Number of the Phishing Site.

2. Subdomain Enumeration

In this phase, we can enumerate the subdomains that are associated with the domain.

3. NMAP Scanning

In this phase, we can get the details of the port that are open and the service running in the server.

4. Directory Enumeration

This will help to find the interesting directories that are allowed to a user.

5. DNS Lookup

This will be useful to enumerate the IP address of the domain from multiple sources.

6. Reverse Number Lookup

This will be useful to check the details of the mobile that we gathered from the above phases

7. IP Address Lookup

This will be useful to gather details about the IP Address like Server location, ISP (Internet Service Provider)

8. Email Lookup

In this phase, we can get details whether the Email ID is valid and reachable.

9. Username Enumeration

In this phase we can find whether any social media account have the same username as the attacker. This will give a better information about the attacker.

10. Technology Stack Enumeration

This phase will give a detailed information about the technology stack used in that domain and the version of the plugins used. So that we can perform a penetration testing to gain access of the domain.

11. SSL Certificate Enumeration

Even in WHOIS enumeration the Registrant details will be anonymized. But sometimes we can get better results from analysing the SSL Certificate.

12. URL Expander

This will be useful to bypass the shortened URL and go directly to the phishing site.

Technology Stack

APIs Used

- Shodan
- Wappalyzer
- What CMS
- DNS For Family
- WHOIS
- Censys
- IP API

Python Packages

- DNS Resolver
- Shodan

Framework Used

- Django

Languages Used

- HTML
- CSS
- Python

Advantages

- Our automation framework with a user-friendly UI can obtain information about the domain in a finely tuned manner than compared to manual Enumeration.
- This tool uses Django Framework – a simple and less resource-intensive framework which is capable to run very efficiently on lower-end devices.
- There is a very low level of maintenance as we use Open-Source API and tools.





Prototype

OPEN Vuln Scanner

This is a open source OSINT Scanner where you can Enumerate IP, Subdomains, Nmap Scanning, etc.

WHOIS Details



IP Address	164.100.134.104
IP Version	IPv4
Network	164.100.128.0/21
City	Bengaluru
Region	Karnataka
Region Code	KA
Country Name	India
Country Code	IN
Country Capital	New Delhi
Country TLD	.in
Latitude	12.9634
Longitude	77.5855
Time Zone	Asia/Kolkata
Country Calling Code	+91
Currency	INR
Organisation	NKN Core Network
ASN	AS55824







WHOIS Module

OPEN Vuln Scanner

This is a open source OSINT Scanner where you can Enumerate IP, Subdomains, Nmap Scanning, etc.

 Identity Search  Group by Issuer

Criteria	Type: Identity	Match: ILIKE	Search: 'kct.ac.in'				
Certificates	crt.sh ID	Logged At	Not Before	Not After	Common Name	Matching Identities	Issuer Name
	8051919683	2022-11-24	2022-11-24	2023-02-22	*kct.ac.in	*kct.ac.in	C=US, O=Google Trust Services LLC, CN=GTS CA 1P5
	79433020918	2022-11-10	2022-11-10	2023-02-08	entry.kct.ac.in	entry.kct.ac.in	C=US, O=Let's Encrypt, CN=R3
	7943293068	2022-11-10	2022-11-10	2023-02-08	entry.kct.ac.in	entry.kct.ac.in	C=US, O=Let's Encrypt, CN=R3
	7844210215	2022-10-27	2022-10-27	2023-01-25	rigathon.kct.ac.in	rigathon.kct.ac.in	C=US, O=Let's Encrypt, CN=R3
	7844193344	2022-10-27	2022-10-27	2023-01-25	rigathon.kct.ac.in	rigathon.kct.ac.in	C=US, O=Let's Encrypt, CN=R3
	7715897125	2022-10-07	2022-10-07	2023-01-05	admin.placement.kct.ac.in	admin.placement.kct.ac.in	C=US, O=Let's Encrypt, CN=R3
	7705659506	2022-10-07	2022-10-07	2023-01-05	admin.placement.kct.ac.in	admin.placement.kct.ac.in	C=US, O=Let's Encrypt, CN=R3
	7715882112	2022-10-07	2022-10-07	2023-01-05	admissions.kct.ac.in	admissions.kct.ac.in	C=US, O=Let's Encrypt, CN=R3
	7616688412	2022-10-07	2022-10-07	2023-01-05	admissions.kct.ac.in	admissions.kct.ac.in	C=US, O=Let's Encrypt, CN=R3
	7674901347	2022-10-03	2022-10-03	2023-01-01	placement.kct.ac.in	placement.kct.ac.in	C=US, O=Let's Encrypt, CN=R3
	7673780615	2022-10-03	2022-10-03	2023-01-01	placement.kct.ac.in	placement.kct.ac.in	C=US, O=Let's Encrypt, CN=R3
	7619413143	2022-09-26	2022-09-26	2022-12-25	*kct.ac.in	*kct.ac.in	C=US, O=Google Trust Services LLC, CN=GTS CA 1P5
	7599262385	2022-09-22	2022-09-22	2022-12-21	rigathon.kct.ac.in	rigathon.kct.ac.in	C=US, O=Let's Encrypt, CN=R3
	75932927759	2022-09-22	2022-09-22	2022-12-21	rigathon.kct.ac.in	rigathon.kct.ac.in	C=US, O=Let's Encrypt, CN=R3
	7592258882	2022-09-22	2022-09-22	2022-12-21	rigathon.kct.ac.in	rigathon.kct.ac.in	C=US, O=Let's Encrypt, CN=R3
	7593055310	2022-09-22	2022-09-22	2022-12-21	rigathon.kct.ac.in	rigathon.kct.ac.in	C=US, O=Let's Encrypt, CN=R3
	7617577496	2022-09-11	2022-09-11	2022-12-10	entry.kct.ac.in	entry.kct.ac.in	C=US, O=Let's Encrypt, CN=R3
	7517575224	2022-09-11	2022-09-11	2022-12-10	entry.kct.ac.in	entry.kct.ac.in	C=US, O=Let's Encrypt, CN=R3
	7490335983	2022-09-07	2022-09-07	2022-12-06	rigathon.kct.ac.in	rigathon.kct.ac.in	C=US, O=Let's Encrypt, CN=R3
	7490350312	2022-09-07	2022-09-07	2022-12-06	rigathon.kct.ac.in	rigathon.kct.ac.in	C=US, O=Let's Encrypt, CN=R3
	7465122360	2022-09-03	2022-09-03	2023-10-04	*kct.ac.in	*kct.ac.in	C=US, O=DigiCert Inc, OU=www.digicert.com, CN=GeoTrust RSA CA 2018
	7293541522	2022-08-08	2022-08-08	2022-11-06	admissions.kct.ac.in	admissions.kct.ac.in	C=US, O=Let's Encrypt, CN=R3
	7293541535	2022-08-08	2022-08-08	2022-11-06	admissions.kct.ac.in	admissions.kct.ac.in	C=US, O=Let's Encrypt, CN=R3
	7288548308	2022-08-07	2022-08-07	2022-11-05	admin.placement.kct.ac.in	admin.placement.kct.ac.in	C=US, O=Let's Encrypt, CN=R3
	7288543176	2022-08-07	2022-08-07	2022-11-05	admin.placement.kct.ac.in	admin.placement.kct.ac.in	C=US, O=Let's Encrypt, CN=R3
	7268763075	2022-08-04	2022-08-04	2022-11-02	placement.kct.ac.in	placement.kct.ac.in	C=US, O=Let's Encrypt, CN=R3
	7268763075	2022-08-04	2022-08-04	2022-11-02	placement.kct.ac.in	placement.kct.ac.in	C=US, O=Let's Encrypt, CN=R3



SSL Certificate Enumeration

Innovation

- We use our developed script to scrap username and Email from the website, which can be useful to enumerate further details about the attacker.
- We integrate the tools in a strategical manner so that it works in a well-structured flow to gather information.
- This tool is built in a time efficient manner to gather information about the domain and the attacker.

Feasibility

- With guidance of the Authority of Police and with the paid APIs, comparatively, can gather a lot of information about the attacker rather than a normal search mechanism.