**Open Source Intelligence (OSINT) Investigation Report**

I. Introduction

| A. Purpose of the Investigation | Perform OSINT information on the domain "atomic-nuclear.site" & document sensitive information that is publicly available |
| --- | --- |
| B. Scope | atomic-nuclear.site and its subdomains |

II. Methodology

| A. Tools Used | theHarvester, dnsenum, dnsrecon ,dnsmap, Sublistr3,spiderfoot |
| --- | --- |
| B. Techniques Employed | * Step1 - We will do WHOIS lookup for Domain name availability. * Step2 - Find the subdomains, Ip address, mail serves, email Ids. * Step3 – Proceed with Web analysis, server related information (censys), Relevant Information using Wayback machine and Shadon search engine, using google dorks * Step4 - Location gathering for the List of Ip address * Step5 – Find Social Media Presence * Step6 – Final step Analysis. * Step7 – Using OSINT TOOL like spiderfoot, verify the information. |

III. Findings

A. **WHOIS Information**

| Domain Registration Date | Owner Information | Registration History |
| --- | --- | --- |
| 1994-03-15 | ICANN | - |
|  | | |

B. **DNS Information**

| Domain Records | Subdomains | IP Addresses |
| --- | --- | --- |
| Hostname,nameservermailservers | git.atomic-nuclear.site, sso.atomic-nuclear.site, phish.atomic-nuclear.site, secretserver.atomic-nuclear.site, sso.atomic-nuclear.site | [List of IP Addresses given below] |
|  | | |

C. **Website Analysis**

We used to **google dorks for finding any confidential pdf and found one(link -** , <https://fissilematerials.org/library/nrc14.pdf> )wayback machine and **Shadon search engine** (censys also) for finding information. From **Wayback machine** we do not get any relevant information.

| Content Description | Notable Information | Structure Overview |
| --- | --- | --- |
| Information gathering through website | Screenshot attached below | Hit all the domain on browser for getting any contact details, use robots.txt or sitemap for other URL (can used Dir buster for url enumeration) |
|  | | |

D. **IP Address Investigation**

Here we have used **ghost\_eye tool** for getting location from the IP address.

| IP Address | Location | Associated Domains |
| --- | --- | --- |
| 185.199.109.153 | [Location] | Atomic-nuclear.site |
|  | | |

E. **Social Media Presence**

| Social Media Platform | Profile Information | Tools used |
| --- | --- | --- |
| Facebook | 6 matches found | **Spokeo.com** |
|  | | |

F. Other Relevant Information using **OSINT tool spiderfoot**

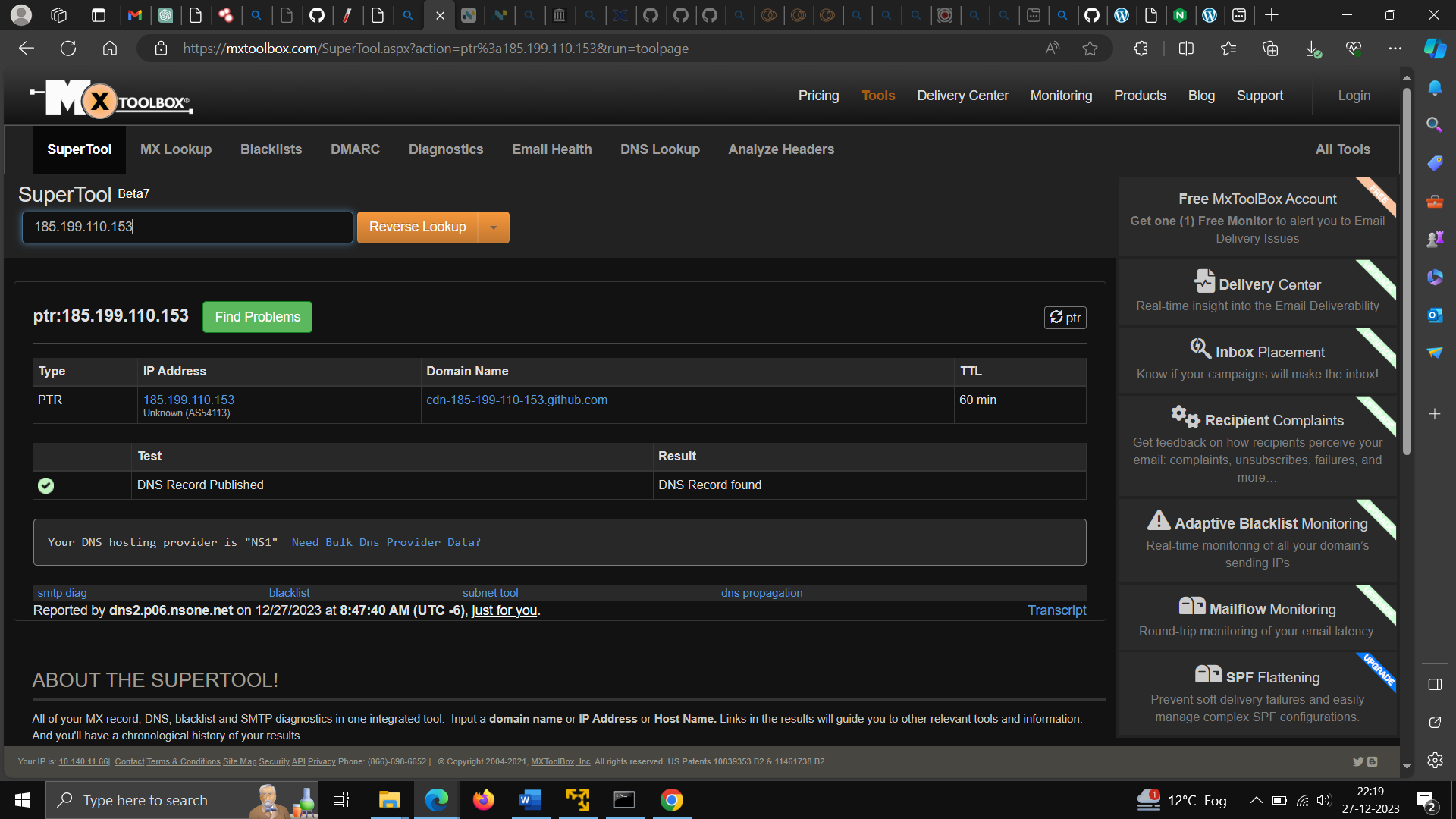
| Source | Information Details |
| --- | --- |
| SPIDERFOOT | External, Internal account, Malicious IP, parent Domain etc. |
|  | |

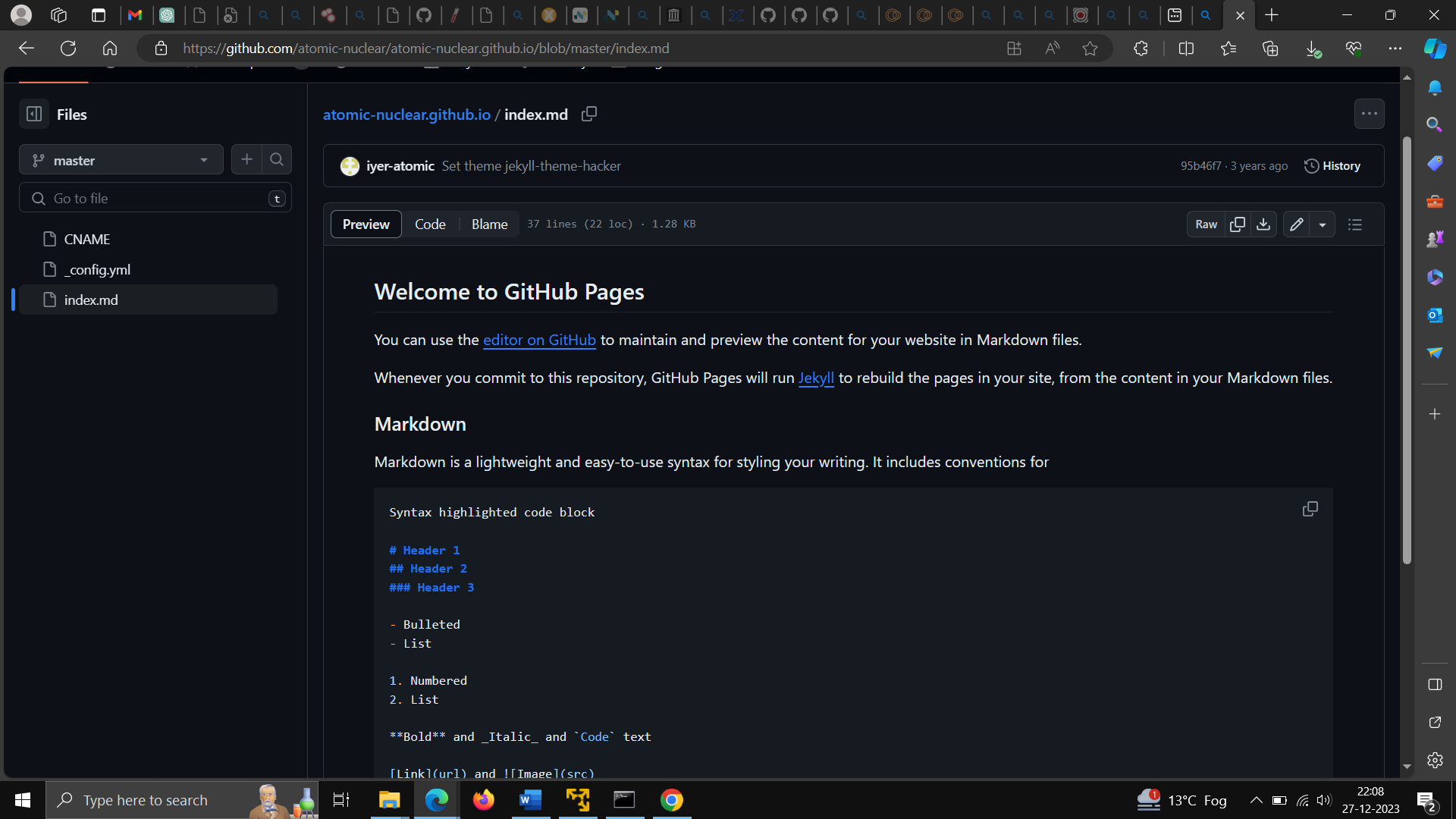
G. **Analysis**

| A. Patterns and Trends | Identify patterns or trends in the collected information that may be relevant to the investigation. |
| --- | --- |
| B. Correlations | Highlight any correlations between different pieces of information gathered. |

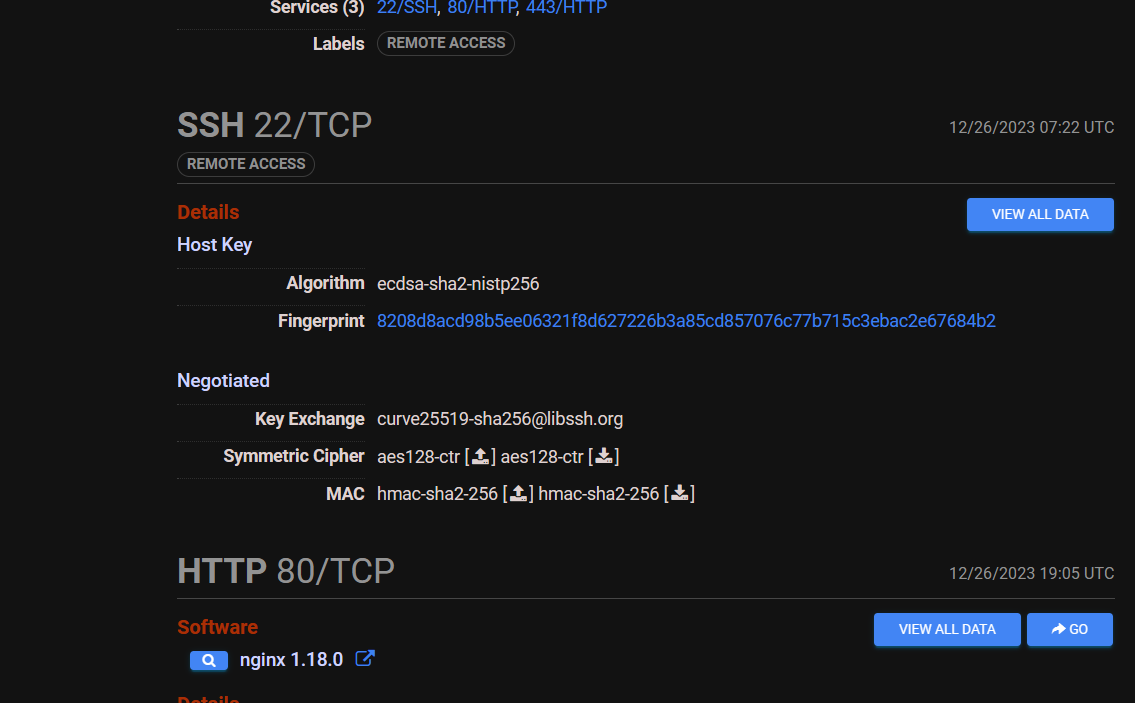
**OTHER INFORMATION FROM DIFFERENT RESOURCES**

-**REVERSE LOOK UP -INFO**

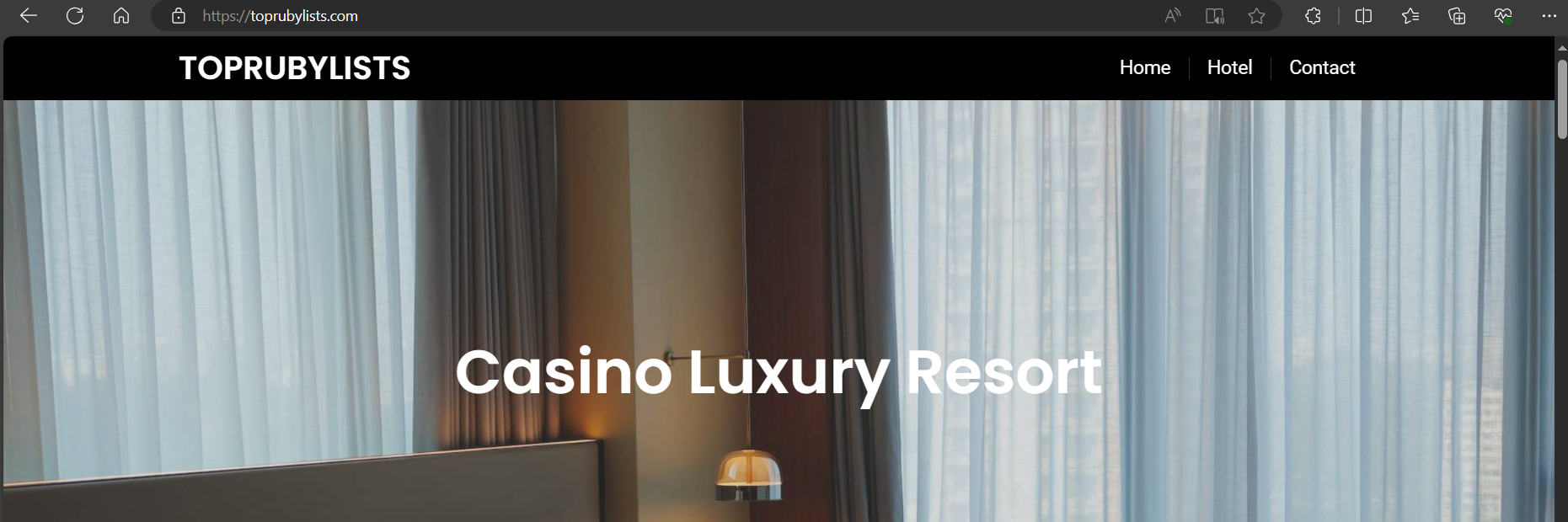


-**JEYLL tool used for Deployment.**

-**Ports Used in Communication**



**-secretserver.atomic-nuclear.site redirects to below website(WordPress used)-**

****