Passive Reconnaissance Report

Internship Assignment – Passive Footprinting & Reconnaissance

Submitted By : Prashant Sengar

To: Skill Horizon

1. Target Information

Chosen Target Domain: Nigc.gov

Scope: Public Bug Bounty

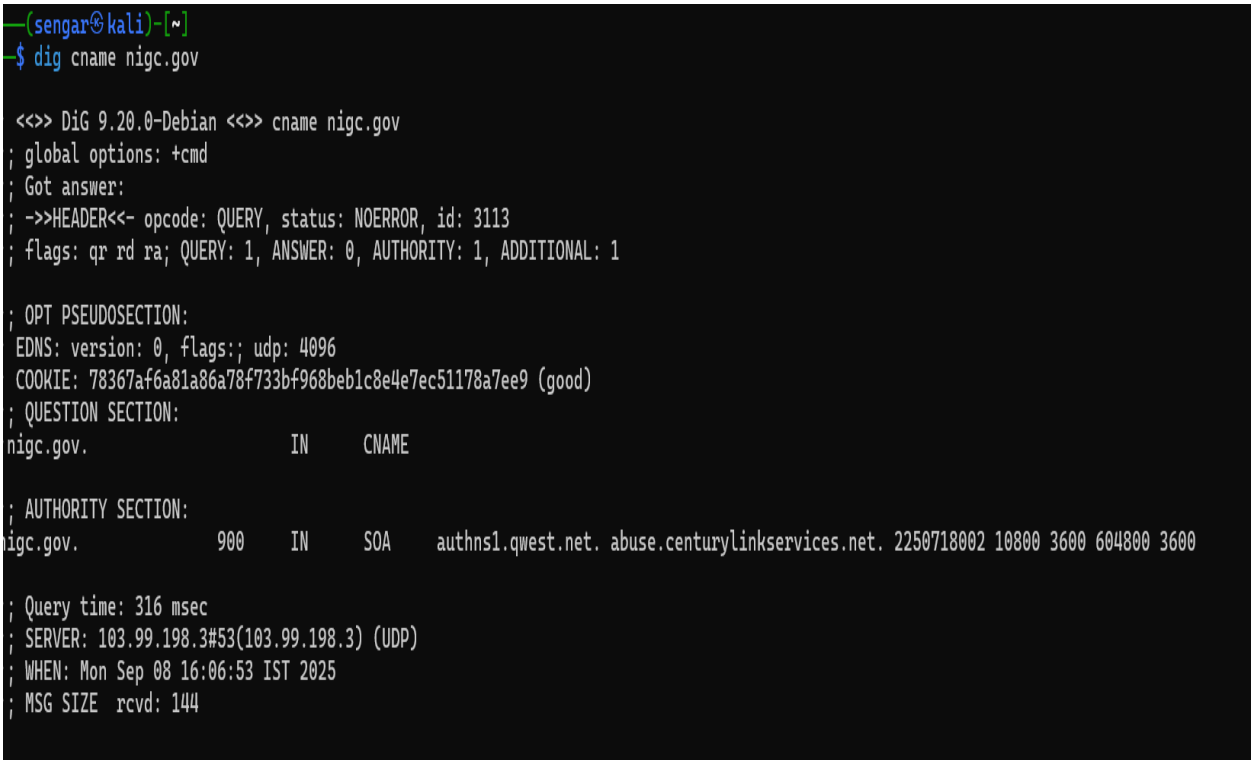
Program

2. WHOIS & DNS Findings Registrar:

```
┌──(sengar㉿kali)-[~]
└─$ nslookup -type=mx nigc.gov
Server:         103.99.198.3
Address:        103.99.198.3#53

Non-authoritative answer:
nigc.gov        mail exchanger = 0 nigc-gov.mail.protection.outlook.com.

Authoritative answers can be found from:
nigc.gov        nameserver = authns2.qwest.net.
nigc.gov        nameserver = authns1.qwest.net.
authns1.qwest.net       internet address = 63.150.72.4
authns2.qwest.net       internet address = 208.44.130.120
authns1.qwest.net       has AAAA address 2001:428::5
authns2.qwest.net       has AAAA address 2001:428::6
```

```
┌──(sengar㉿kali)-[~]
└─$ whois nigc.gov
Domain Name: nigc.gov
Registrar WHOIS Server: whois.nic.gov
Registrar URL: https://get.gov
Updated Date: 2025-06-14T16:20:01Z
Creation Date: 1998-05-12T14:55:02Z
Registry Expiry Date: 2025-09-30T04:00:00Z
Registrar: get.gov
Registrar IANA ID: 8888888
Registrar Abuse Contact Email:
```

```
┌──(sengar㉿kali)-[~]
└─$ dig  nigc.gov A

; <<>> DiG 9.20.0-Debian <<>> nigc.gov A
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 3176
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 2, ADDITIONAL: 5

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: 888a3bb410192b97ba9b63a668beb1fdebf4d66be2c48e70 (good)
;; QUESTION SECTION:
;nigc.gov.                      IN      A

;; ANSWER SECTION:
nigc.gov.               900     IN      A       51.54.101.43

;; AUTHORITY SECTION:
nigc.gov.               10707   IN      NS      authns1.qwest.net.
nigc.gov.               10707   IN      NS      authns2.qwest.net.

;; ADDITIONAL SECTION:
authns1.qwest.net.      15684   IN      A       63.150.72.4
authns2.qwest.net.      15684   IN      A       208.44.130.120
authns1.qwest.net.      15684   IN      AAAA    2001:428::5
authns2.qwest.net.      15684   IN      AAAA    2001:428::6

;; Query time: 328 msec
;; SERVER: 103.99.198.3#53(103.99.198.3) (UDP)
;; WHEN: Mon Sep 08 16:07:45 IST 2025
;; MSG SIZE  rcvd: 222
```



Findings :

Registrar: _____ Registrant Organization: _____

Name Servers: _____ A Record: _____ MX Record:

_____ [Inserted WHOIS/DNS screenshots]

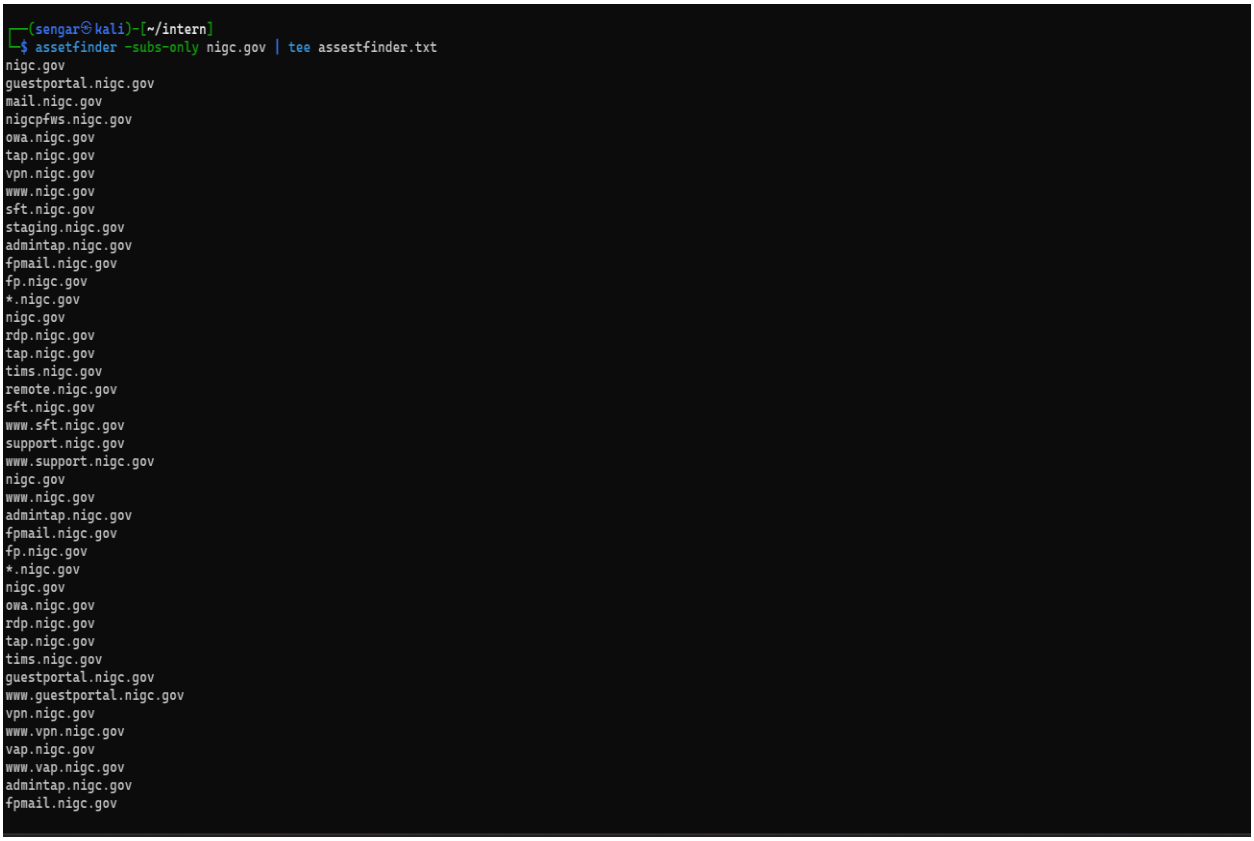
3. Subdomain Enumeration

Tools used: subfinder, assetfinder, amass (passive)

1- Subfinder Findings

Command used : subfinder –d nigc.gov >> subfinder.txt

2- Assestfinder Findings



Command Used:-assestfinder –subs-only nigc.gov | tee assestfinder.txt

3-Amass enum –passive nigc.gov

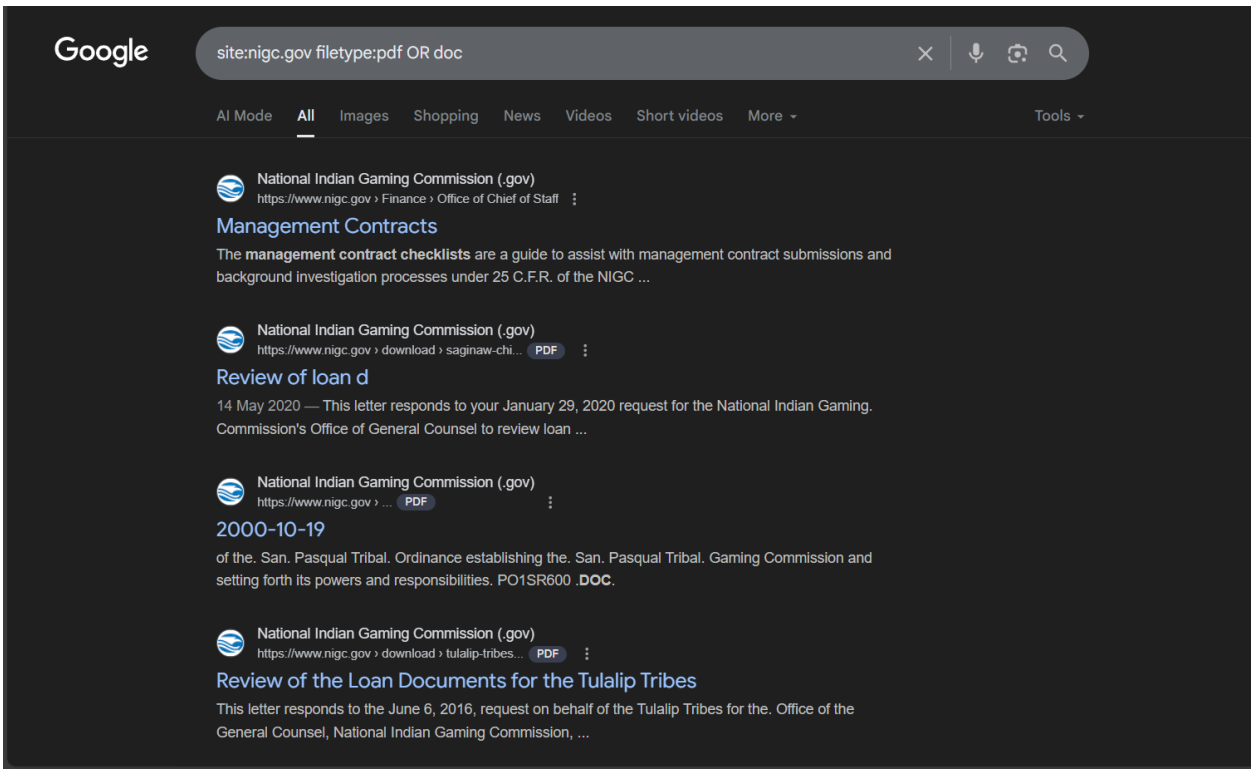
4. Email & Employee Data

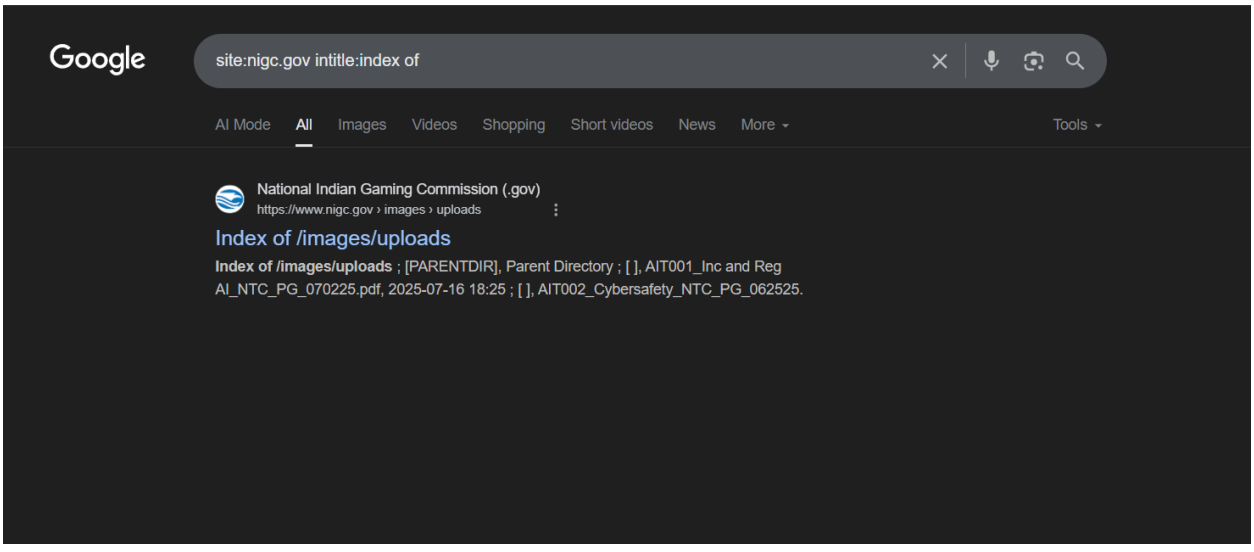
Tools Used: theHarvester

Findings Emails..

5. Google Dorking To find some PII leak

Site:nigc.gov intitle:”index of”

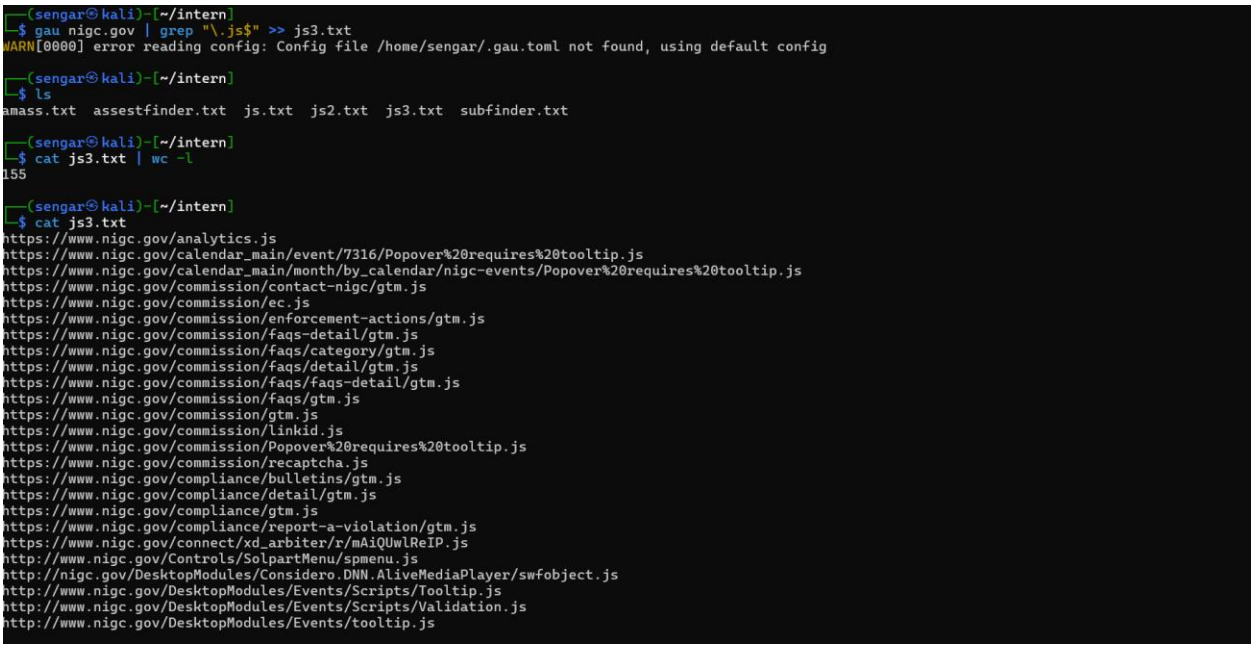




6-JavaScript Analysis

!..

First gather all .js files from Tools like katana ,gau ,waybackurls



Findings Hidden Links in .JS to Find potential Leaks like api key etc..

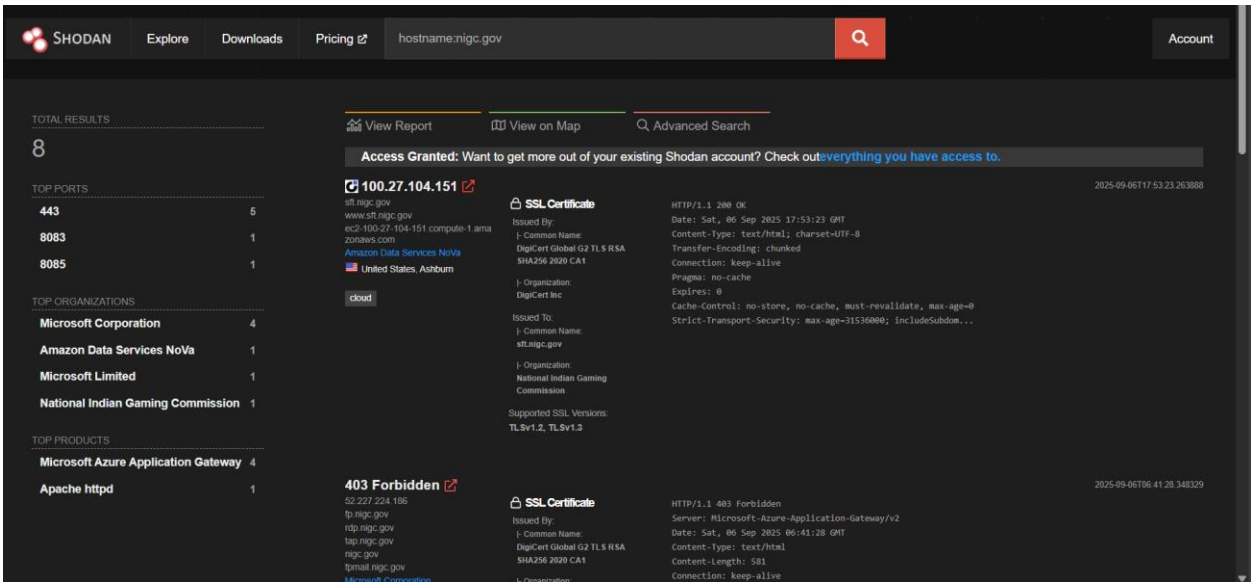
Tool Used: jsleak

Command Used: cat js.txt | jsleak –l –s

7. OSINT Findings

USED :- SHODAN to find senstive information

or login pannels to esclate attack surface



Findings: Found internal login panel which can be used for further attack mapping