

# **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 nignc.gov A
```

```
; <<> DiG 9.20.0-Debian <<> nignc.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: 888a3bb410192b97ba9b63a668beb1fdeb4d66be2c48e70 (good)  
;; QUESTION SECTION:  
;nignc.gov. IN A
```

```
;; ANSWER SECTION:  
nignc.gov. 900 IN A 51.54.101.43
```

```
;; AUTHORITY SECTION:  
nignc.gov. 10707 IN NS authns1.qwest.net.  
nignc.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
```

```

(sengar@kali)-[~]
$ dig cname nigc.gov

<<>> DiG 9.20.0-Debian <<>> cname nigc.gov
; global options: +cmd
; Got answer:
; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 3113
; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 1

; OPT PSEUDOSECTION:
EDNS: version: 0, flags:; udp: 4096
COOKIE: 78367af6a81a86a78f733bf968beb1c8e4e7ec51178a7ee9 (good)
; QUESTION SECTION:
nigc.gov.                IN      CNAME

; AUTHORITY SECTION:
nigc.gov.                900     IN      SOA     authns1.qwest.net. abuse.centurylinkservices.net. 2250718002 10800 3600 604800 3600

; Query time: 316 msec
; SERVER: 103.99.198.3#53(103.99.198.3) (UDP)
; WHEN: Mon Sep 08 16:06:53 IST 2025
; MSG SIZE rcvd: 144

```

## *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*

```
(sengar@kali) ~[~/intern]
$ subfinder -d nigc.gov | tee subfinder.txt

projectdiscovery.io

[INF] Current subfinder version v2.8.0 (latest)
[INF] Loading provider config from /home/sengar/.config/subfinder/provider-config.yaml
[INF] Enumerating subdomains for nigc.gov
[INF] Found 39 subdomains for nigc.gov in 6 seconds 973 milliseconds
support.nigc.gov
vpn.nigc.gov
enterpriseregistration.nigc.gov
sts.nigc.gov
owa.nigc.gov
www.sts.nigc.gov
www.nigc.gov
www.vap.nigc.gov
nigc-cas.nigc.gov
enterpriseenrollment.nigc.gov
autodiscover.nigc.gov
rdp.nigc.gov
remote.nigc.gov
vap.nigc.gov
lyncdiscover.nigc.gov
sip.nigc.gov
www.guestportal.nigc.gov
admin.tap.nigc.gov
certauth.sts.nigc.gov
www.tap.nigc.gov
fp.nigc.gov
sft.nigc.gov
www.sft.nigc.gov
www.vpn.nigc.gov
```

**Command used : subfinder -d nigc.gov >>  
subfinder.txt**

## 2- Assestfinder Findings

```
(sengar@kali)~[/intern]
$ assetfinder -subs-only nignc.gov | tee assestfinder.txt
nignc.gov
guestportal.nignc.gov
mail.nignc.gov
nigncpfws.nignc.gov
owa.nignc.gov
tap.nignc.gov
vpn.nignc.gov
www.nignc.gov
sft.nignc.gov
staging.nignc.gov
admintap.nignc.gov
fpmail.nignc.gov
fp.nignc.gov
*.nignc.gov
nignc.gov
rdp.nignc.gov
tap.nignc.gov
tims.nignc.gov
remote.nignc.gov
sft.nignc.gov
www.sft.nignc.gov
support.nignc.gov
www.support.nignc.gov
nignc.gov
www.nignc.gov
admintap.nignc.gov
fpmail.nignc.gov
fp.nignc.gov
*.nignc.gov
nignc.gov
owa.nignc.gov
rdp.nignc.gov
tap.nignc.gov
tims.nignc.gov
guestportal.nignc.gov
www.guestportal.nignc.gov
vpn.nignc.gov
www.vpn.nignc.gov
vap.nignc.gov
www.vap.nignc.gov
admintap.nignc.gov
fpmail.nignc.gov
```

*Command Used:-assetfinder -subs-only  
nignc.gov | tee assestfinder.txt*

### 3-Amass enum -passive nigc.gov

## 4. Email & Employee Data

### Tools Used: theHarvester

```
(sengar@kali)~[/intern]
$ theHarvester -d nigc.gov -b bing,yahoo,crtsh
Read proxies.yaml from /home/sengar/.theHarvester/proxies.yaml
*****
*                                     *
* [t]h[e]h[a]r[v]e[s]t[e]r         *
* [t]h[e]h[a]r[v]e[s]t[e]r         *
* theHarvester 4.6.0                *
* Coded by Christian Martorella      *
* Edge-Security Research             *
* cmartorella@edge-security.com      *
*                                     *
*****

[*] Target: nigc.gov

Read api-keys.yaml from /home/sengar/.theHarvester/api-keys.yaml
Searching 0 results.
[*] Searching Bing.
[*] Searching Yahoo.
[*] Searching CRTsh.

[*] No IPs found.

[*] Emails found: 4
-----
becky.darwazeh@nigc.gov
contactus@nigc.gov
debra.bailey@nigc.gov
traci.reiner@nigc.gov

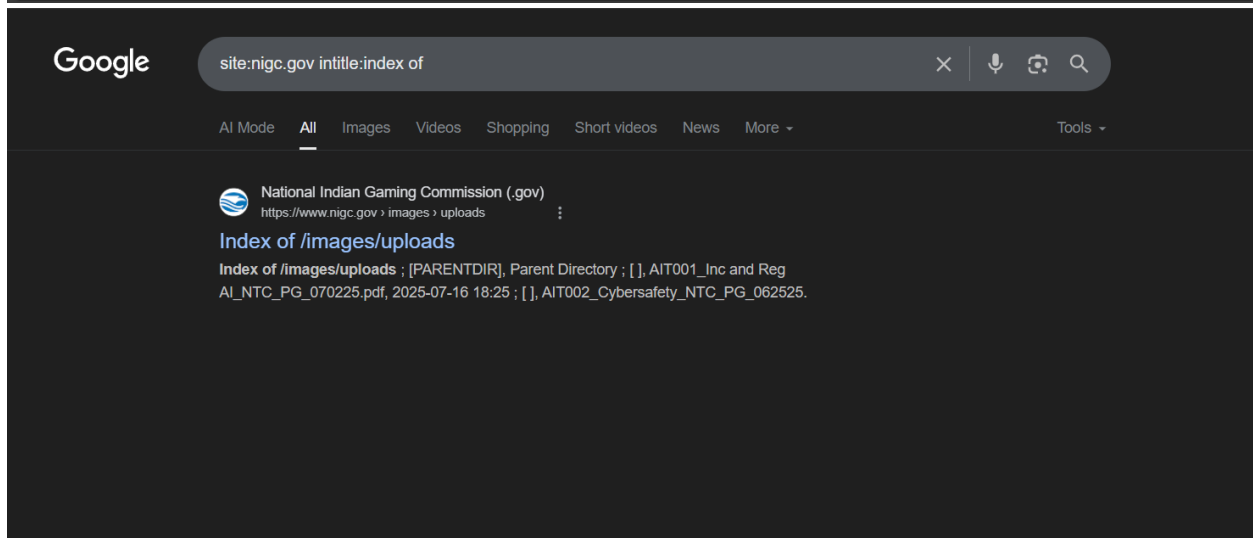
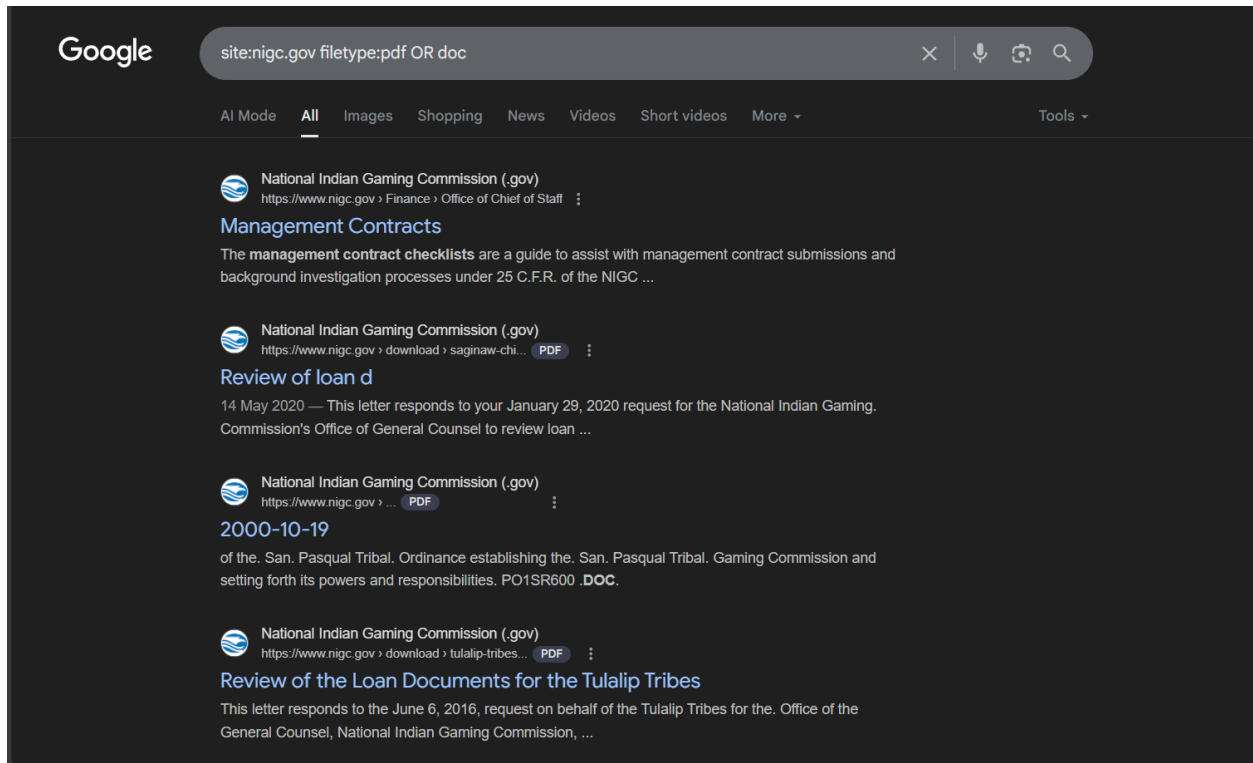
[*] Hosts found: 26
-----
*.nigc.gov
adfs.nigc.gov
admin.tap.nigc.gov
admintap.nigc.gov
autodiscover.nigc.gov
certauth.sts.nigc.gov
enterpriseregistration.nigc.gov
fp.nigc.gov
```

## 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

[illegible]

# Tool Used: jsleak

```
(sengar@kali) ~/intern
$ cat js3.txt | jsleak -l -s
[+] Found link: [/html/body] in [https://www.nigc.gov/wp-content/plugins/wp-rocket/assets/js/wpr-beacon.min.js]
[+] Found link: [//fonts.googleapis.com/css] in [https://www.nigc.gov/wp-content/plugins/wp-google-maps-pro/js/v8/wp-google-maps-pro.combined.js]
[+] Found link: [https://www.wpgmaps.com/documentation/creating-a-google-maps-api-key/] in [https://www.nigc.gov/wp-content/plugins/wp-google-maps-pro/js/v8/wp-google-maps-pro.combined.js]
[+] Found link: [https://wpgmaps.us-3.evennode.com/api/v1/] in [https://www.nigc.gov/wp-content/plugins/wp-google-maps-pro/js/v8/wp-google-maps-pro.combined.js]
[+] Found link: [7/28/49] in [https://www.nigc.gov/wp-content/plugins/wp-google-maps-pro/js/v8/wp-google-maps-pro.combined.js]
[+] Found link: [https://console.cloud.google.com/google/maps-hosted] in [https://www.nigc.gov/wp-content/plugins/wp-google-maps-pro/js/v8/wp-google-maps-pro.combined.js]
[+] Found link: [/features/] in [https://www.nigc.gov/wp-content/plugins/wp-google-maps-pro/js/v8/wp-google-maps-pro.combined.js]
[+] Found link: [/markers/] in [https://www.nigc.gov/wp-content/plugins/wp-google-maps-pro/js/v8/wp-google-maps-pro.combined.js]
[+] Found link: [/features/] in [https://www.nigc.gov/wp-content/plugins/wp-google-maps-pro/js/v8/wp-google-maps-pro.combined.js]
[+] Found link: [markers.xml] in [https://www.nigc.gov/wp-content/plugins/wp-google-maps-pro/js/v8/wp-google-maps-pro.combined.js]
[+] Found link: [markers.xml] in [https://www.nigc.gov/wp-content/plugins/wp-google-maps-pro/js/v8/wp-google-maps-pro.combined.js]
[+] Found link: [/features/] in [https://www.nigc.gov/wp-content/plugins/wp-google-maps-pro/js/v8/wp-google-maps-pro.combined.js]
[+] Found link: [text/javascript] in [https://www.nigc.gov/wp-content/plugins/wp-google-maps-pro/js/v8/wp-google-maps-pro.combined.js]
[+] Found link: [markers.xml] in [https://www.nigc.gov/wp-content/plugins/wp-google-maps-pro/js/v8/wp-google-maps-pro.combined.js]
[+] Found link: [markers.xml] in [https://www.nigc.gov/wp-content/plugins/wp-google-maps-pro/js/v8/wp-google-maps-pro.combined.js]
[+] Found link: [/features/] in [https://www.nigc.gov/wp-content/plugins/wp-google-maps-pro/js/v8/wp-google-maps-pro.combined.js]
[+] Found link: [text/javascript] in [https://www.nigc.gov/wp-content/plugins/wp-google-maps-pro/js/v8/wp-google-maps-pro.combined.js]
[+] Found link: [/markers/] in [https://www.nigc.gov/wp-content/plugins/wp-google-maps-pro/js/v8/wp-google-maps-pro.combined.js]
[+] Found link: [/base64] in [https://www.nigc.gov/wp-content/plugins/wp-google-maps-pro/js/v8/wp-google-maps-pro.combined.js]
[+] Found link: [/rest-api/] in [https://www.nigc.gov/wp-content/plugins/wp-google-maps-pro/js/v8/wp-google-maps-pro.combined.js]
[+] Found link: [admin.php?page=wp-google-maps-menu&action=welcome_page] in [https://www.nigc.gov/wp-content/plugins/wp-google-maps-pro/js/v8/wp-google-maps-pro.combined.js]
[+] Found link: [/integration-tools/] in [https://www.nigc.gov/wp-content/plugins/wp-google-maps-pro/js/v8/wp-google-maps-pro.combined.js]
[+] Found link: [/performance-tools/] in [https://www.nigc.gov/wp-content/plugins/wp-google-maps-pro/js/v8/wp-google-maps-pro.combined.js]
[+] Found link: [https://wpgmaps.us-3.evennode.com/api/v1/autocomplete] in [https://www.nigc.gov/wp-content/plugins/wp-google-maps-pro/js/v8/wp-google-maps-pro.combined.js]
[+] Found link: [/geocode-cache] in [https://www.nigc.gov/wp-content/plugins/wp-google-maps-pro/js/v8/wp-google-maps-pro.combined.js]
[+] Found link: [https://nominatim.openstreetmap.org/search] in [https://www.nigc.gov/wp-content/plugins/wp-google-maps-pro/js/v8/wp-google-maps-pro.combined.js]
[+] Found link: [//cdn.datatables.net/plugin-ins/1.10.12/i18n/English.json] in [https://www.nigc.gov/wp-content/plugins/wp-google-maps-pro/js/v8/wp-google-maps-pro.combined.js]
[+] Found link: [languages/datatables/Afrikaans.json] in [https://www.nigc.gov/wp-content/plugins/wp-google-maps-pro/js/v8/wp-google-maps-pro.combined.js]
[+] Found link: [languages/datatables/Albanian.json] in [https://www.nigc.gov/wp-content/plugins/wp-google-maps-pro/js/v8/wp-google-maps-pro.combined.js]
[+] Found link: [languages/datatables/Amharic.json] in [https://www.nigc.gov/wp-content/plugins/wp-google-maps-pro/js/v8/wp-google-maps-pro.combined.js]
[+] Found link: [languages/datatables/Arabic.json] in [https://www.nigc.gov/wp-content/plugins/wp-google-maps-pro/js/v8/wp-google-maps-pro.combined.js]
```

## Command Used: cat js.txt | jsleak -l -s

## 7. OSINT Findings

USED :- SHODAN to find sensitive information  
or login pannels to esclate attack surface

The image shows two screenshots. The top screenshot is a web browser window displaying the Kiteworks login page. The URL bar shows 'https://100.27.104.151/#/'. The page has a blue background with the 'Kiteworks' logo and a 'Sign in' section. The 'Sign in' section includes a 'Username or email' input field, a 'Next' button, and a link to 'Login via the external SSO provider'. Below the login section, there are links for 'English', 'Getting Started?', and 'Contact Us'. At the bottom, there is a 'PDN' logo and a notice from the Department of the Interior (DOI) regarding monitoring of the system.

The bottom screenshot is a Shodan search results page. The search query is 'hostname:nigc.gov'. The page shows 8 total results. The left sidebar lists top ports (443, 8083, 8085) and top organizations (Microsoft Corporation, Amazon Data Services NoVa, Microsoft Limited, National Indian Gaming Commission). The main content area displays two results. The first result is for '100.27.104.151' and shows an 'Access Granted' status. The second result is for '403 Forbidden' and shows a '403 Forbidden' status. Both results include details about the SSL certificate and the HTTP response.

**Shodan Search Results:**

IP Address	Port	Organization	Status	SSL Certificate Details	HTTP Response
100.27.104.151	443	National Indian Gaming Commission	Access Granted	Issued By: DigiCert Global G2 TLS RSA SHA256 2020 CA1 Issued To: stl.nigc.gov Issued To: stl.nigc.gov Issued To: National Indian Gaming Commission Supported SSL Versions: TLSv1.2, TLSv1.3	HTTP/1.1 200 OK Date: Sat, 06 Sep 2025 17:53:23 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: keep-alive Pragma: no-cache Expires: 0 Cache-Control: no-store, no-cache, must-revalidate, max-age=0 Strict-Transport-Security: max-age=31536000; includeSubdom...
92.227.224.186	443	Microsoft Corporation	403 Forbidden	Issued By: DigiCert Global G2 TLS RSA SHA256 2020 CA1 Issued To: stl.nigc.gov Issued To: National Indian Gaming Commission Supported SSL Versions: TLSv1.2, TLSv1.3	HTTP/1.1 403 Forbidden Server: Microsoft-Azure-Application-Gateway/v2 Date: Sat, 06 Sep 2025 06:41:28 GMT Content-Type: text/html Content-Length: 581 Connection: keep-alive

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