Project 1: Reconnaissance and Information Gathering:

Objective: Perform passive footprinting and advanced information gathering on a target website.

Skills Developed: Digital footprint analysis, website reconnaissance, information gathering.

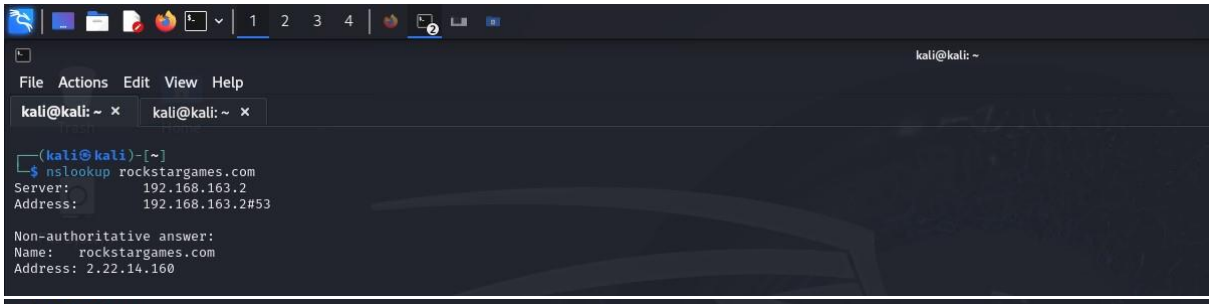
Step 1: Choose a Target Website:

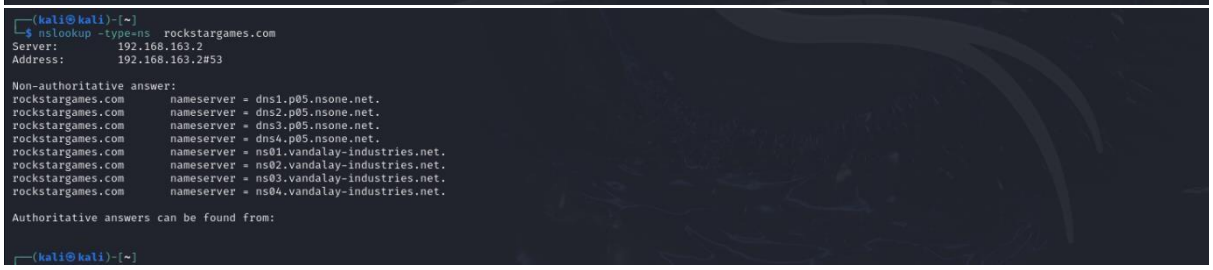
1. Select a website that you have permission to analyze. It could be your own website or a publicly available website. Ensure that you are acting within ethical boundaries. –

   Here I chose rockstargames.com. rockstargames.com is the **official website** of **Rockstar Games**, a major American video game developer and publisher known for blockbuster franchises like *Grand Theft Auto*, *Red Dead Redemption*, *Max Payne*, and more.

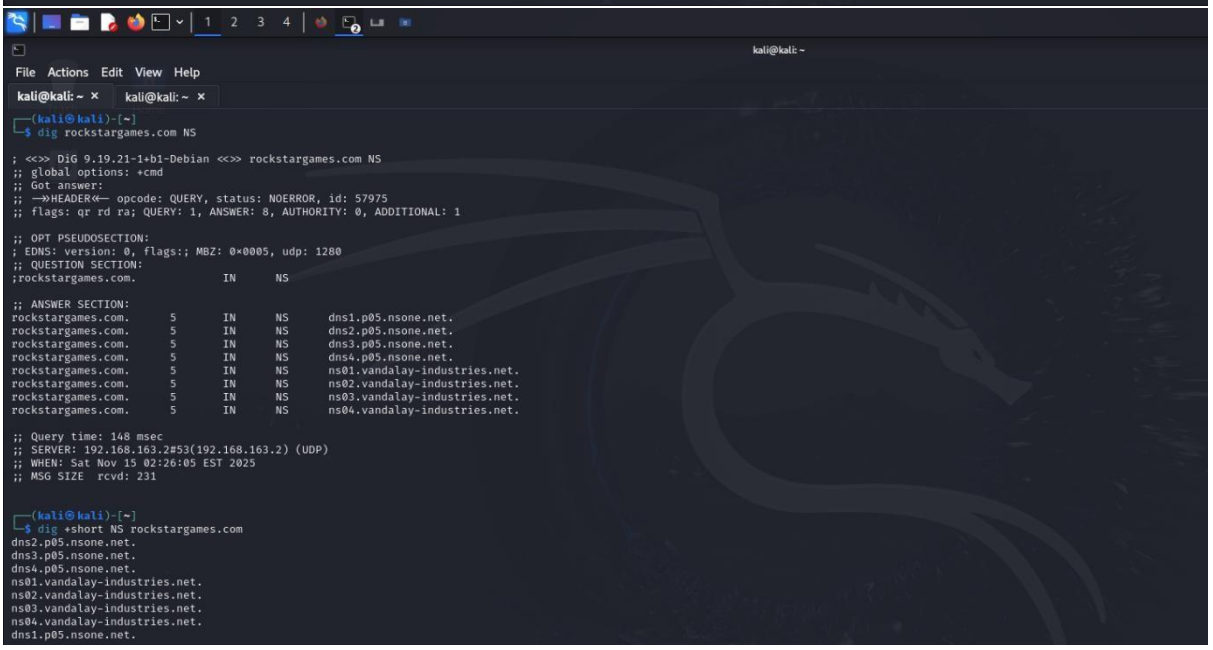
   Step 2: Passive Footprinting:

   1. DNSInformation:
   ○ Usethenslookup commandinyour commandprompttofind the target website's DNS information. Run: nslookup targetwebsite.com
   ○ NotedowntheIPaddress andthe authoritative DNS servers.





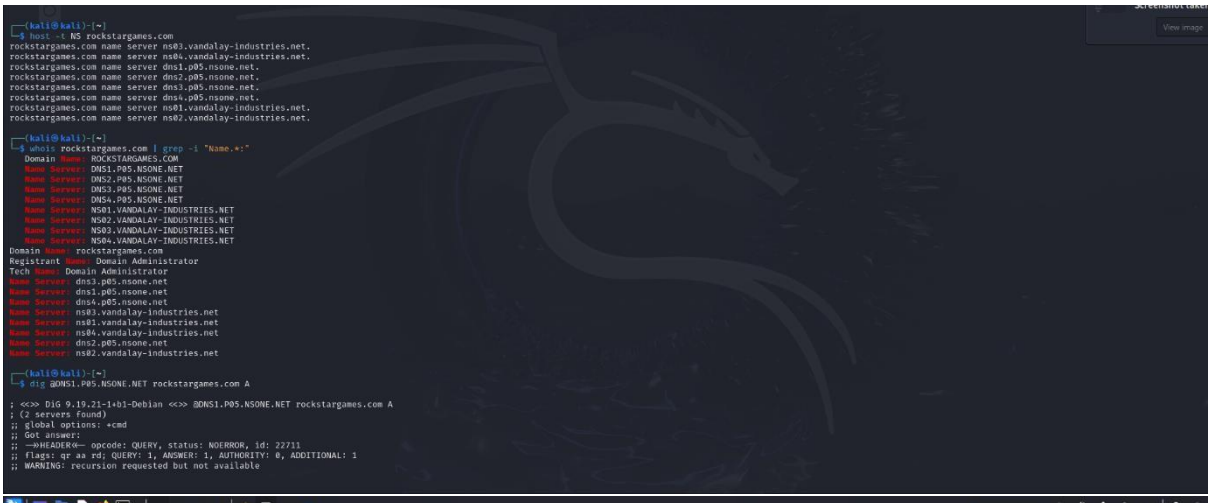
```
┌──(kali㉿kali)-[~]
└─$ nslookup rockstargames.com dns1.p05.nsone.net
Server:         dns1.p05.nsone.net
Address:        198.51.44.5#53

Name:   rockstargames.com
Address: 23.15.146.78


┌──(kali㉿kali)-[~]
└─$ dig rockstargames.com

; <<>> DiG 9.19.21-1+b1-Debian <<>> rockstargames.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 62946
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; MBZ: 0x0005, udp: 1280
;; QUESTION SECTION:
;rockstargames.com.             IN      A

;; ANSWER SECTION:
rockstargames.com.      5       IN      A       23.58.17.229

;; Query time: 384 msec
;; SERVER: 192.168.163.2#53(192.168.163.2) (UDP)
;; WHEN: Sat Nov 15 02:21:09 EST 2025
;; MSG SIZE  rcvd: 62


┌──(kali㉿kali)-[~]
└─$ dig rockstargames.com NS

; <<>> DiG 9.19.21-1+b1-Debian <<>> rockstargames.com NS
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 57975
;; flags: qr rd ra; QUERY: 1, ANSWER: 8, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; MBZ: 0x0005, udp: 1280
;; QUESTION SECTION:
;rockstargames.com.             IN      NS

;; ANSWER SECTION:
rockstargames.com.      5       IN      NS      dns1.p05.nsone.net.
rockstargames.com.      5       IN      NS      dns2.p05.nsone.net.
```

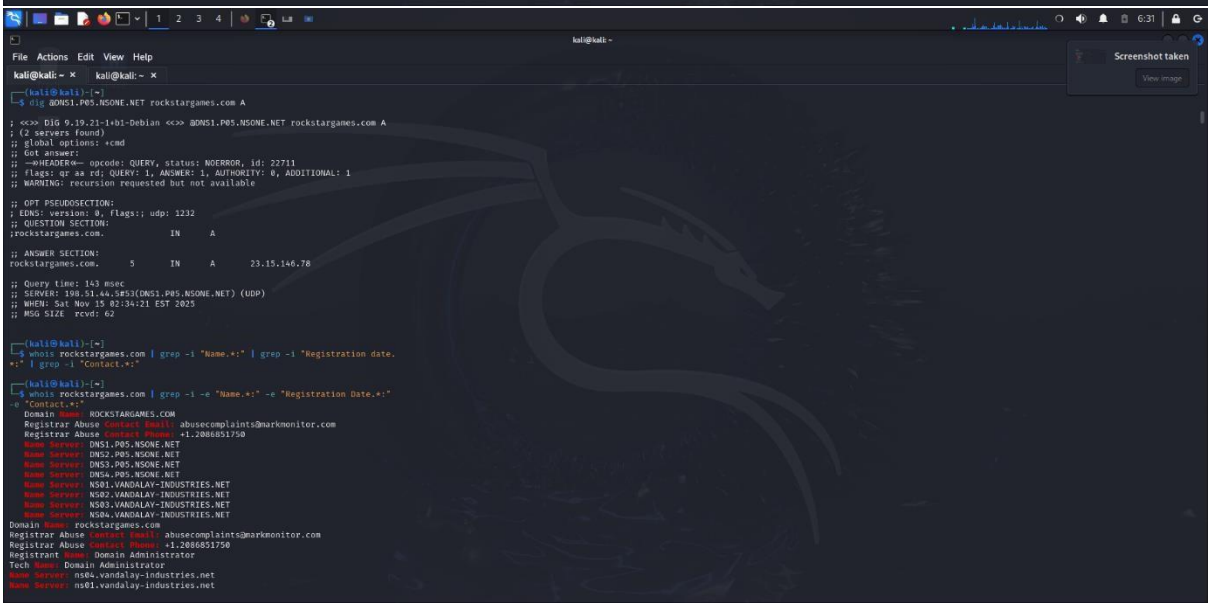


```
File  Actions  Edit  View  Help
kali@kali: ~ ×   kali@kali: ~ ×
┌──(kali㉿kali)-[~]
└─$ dig rockstargames.com NS

; <<>> DiG 9.19.21-1+b1-Debian <<>> rockstargames.com NS
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 57975
;; flags: qr rd ra; QUERY: 1, ANSWER: 8, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; MBZ: 0x0005, udp: 1280
;; QUESTION SECTION:
;rockstargames.com.             IN      NS

;; ANSWER SECTION:
rockstargames.com.      5       IN      NS      dns1.p05.nsone.net.
rockstargames.com.      5       IN      NS      dns2.p05.nsone.net.
rockstargames.com.      5       IN      NS      dns3.p05.nsone.net.
rockstargames.com.      5       IN      NS      dns4.p05.nsone.net.
rockstargames.com.      5       IN      NS      ns01.vandalay-industries.net.
rockstargames.com.      5       IN      NS      ns02.vandalay-industries.net.
rockstargames.com.      5       IN      NS      ns03.vandalay-industries.net.
rockstargames.com.      5       IN      NS      ns04.vandalay-industries.net.

;; Query time: 148 msec
;; SERVER: 192.168.163.2#53(192.168.163.2) (UDP)
;; WHEN: Sat Nov 15 02:26:05 EST 2025
;; MSG SIZE  rcvd: 231


┌──(kali㉿kali)-[~]
└─$ dig +short NS rockstargames.com
dns2.p05.nsone.net.
dns3.p05.nsone.net.
dns4.p05.nsone.net.
ns01.vandalay-industries.net.
ns02.vandalay-industries.net.
ns03.vandalay-industries.net.
ns04.vandalay-industries.net.
dns1.p05.nsone.net.
```

2. Whois Lookup:

○ PerformaWhoislookup using online tools or command-line utilities to gather information about the domain registration. Note down details like domain owner, registration date, and contact information.

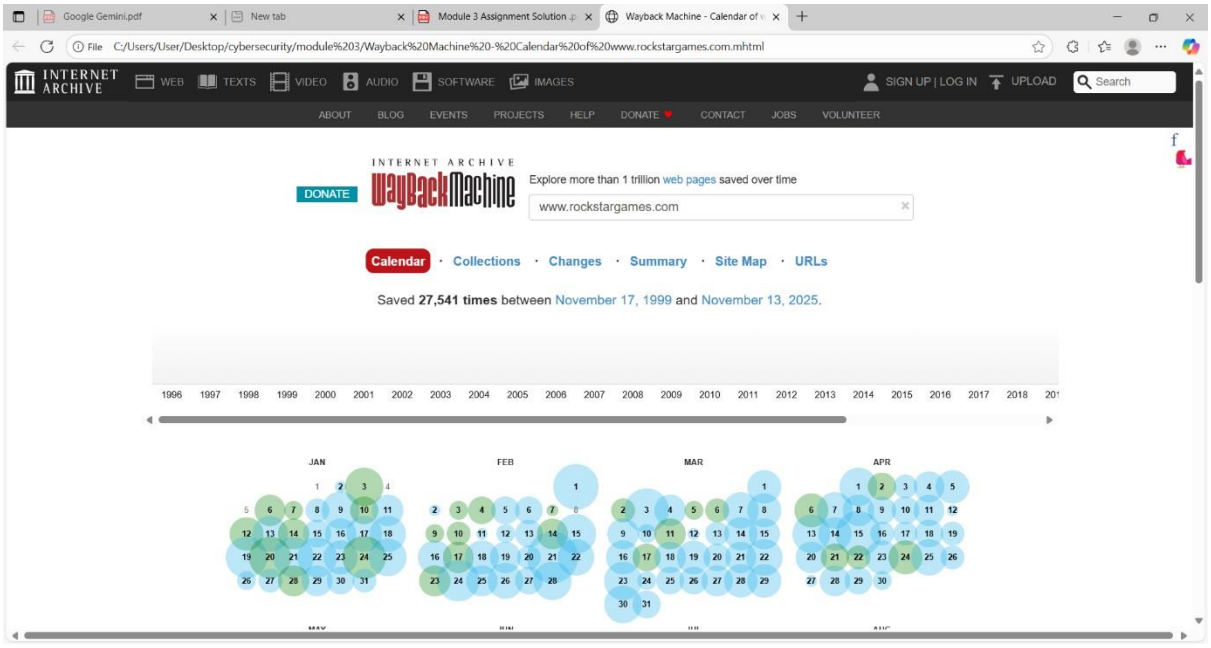




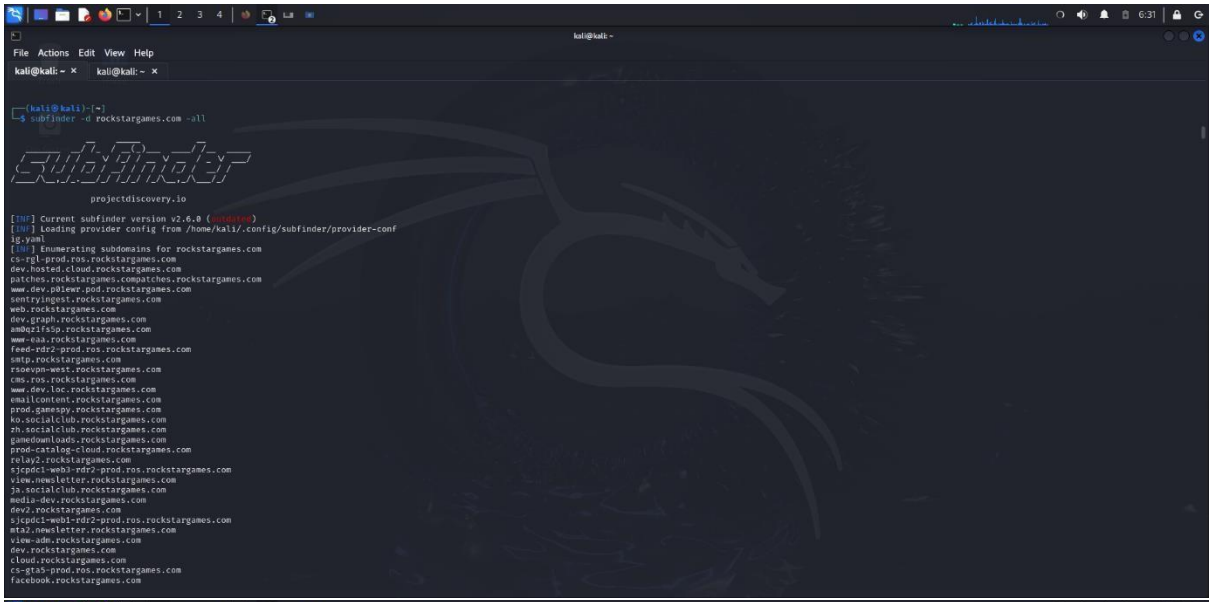
2. WebArchive Search

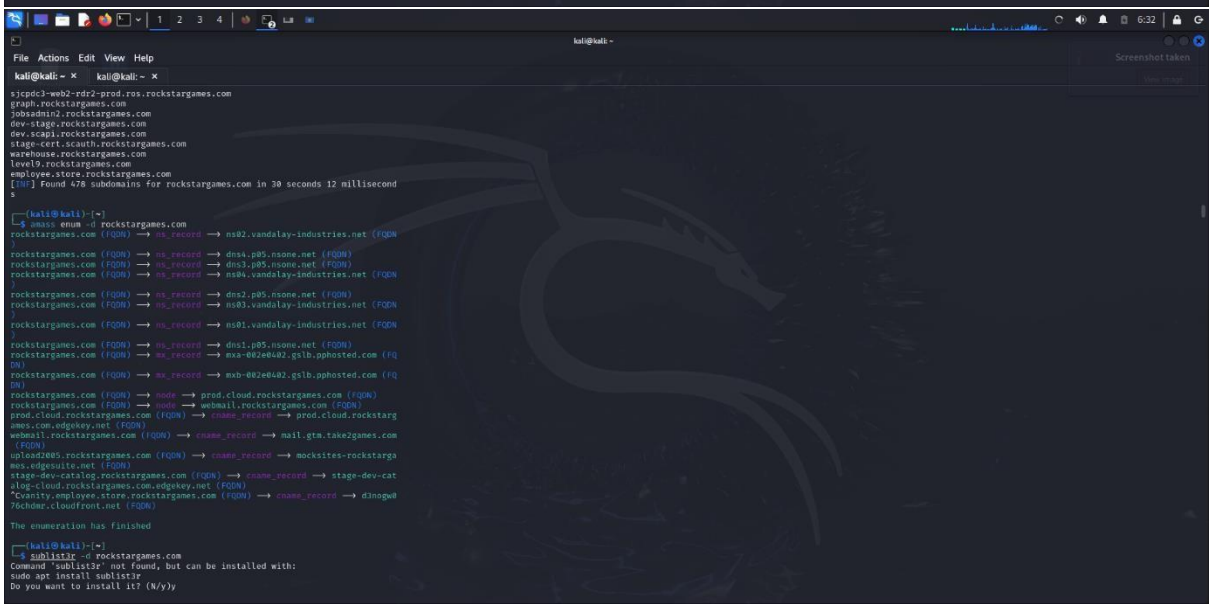
○ Usetoolslike the Wayback Machine (archive.org) to view historical snapshots of the website. This might reveal past content, design changes, or information that's no longer available

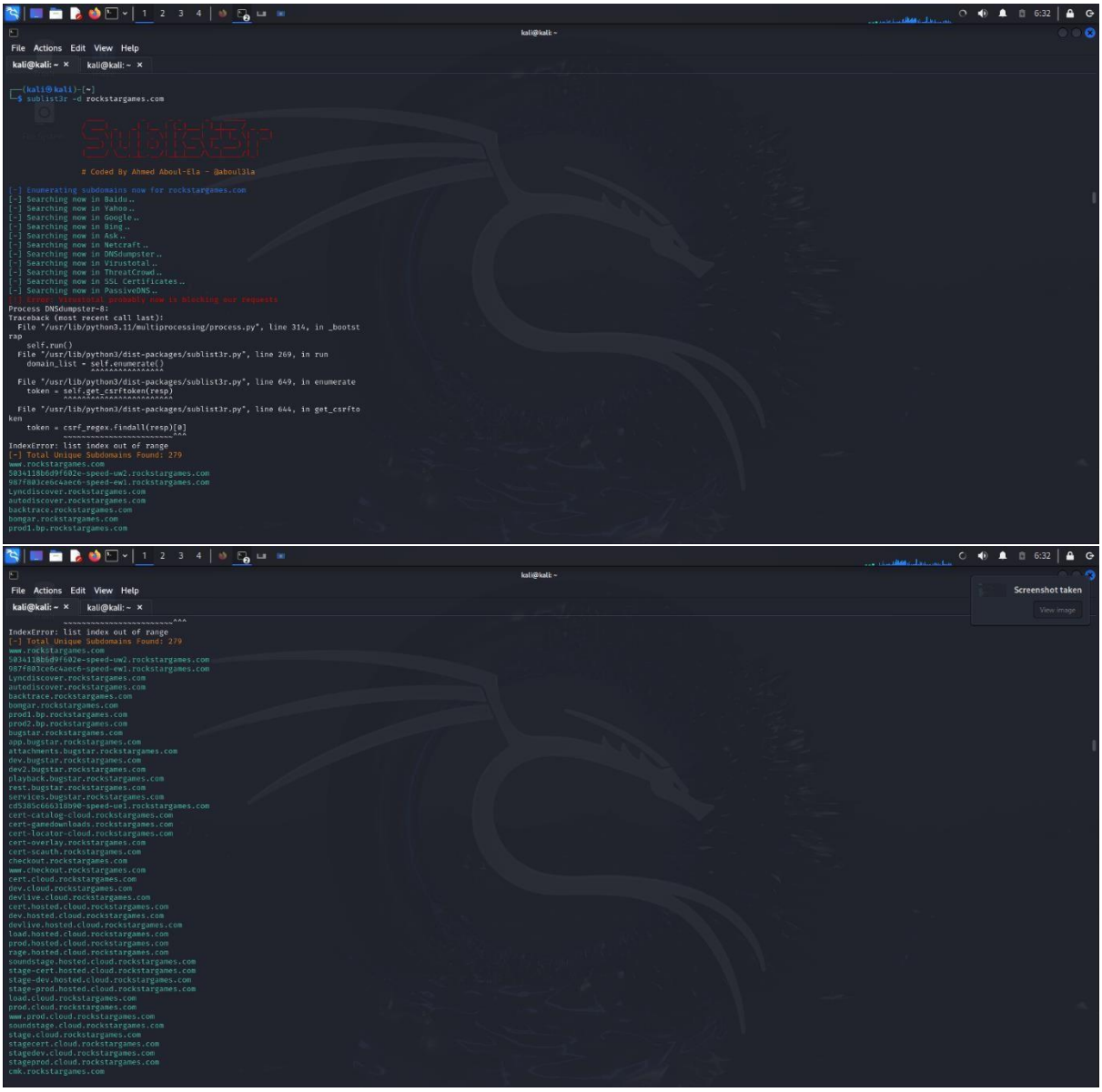
ColorThe circles are primarily **blue** or **green** (with some variations in the past). Historically, green captures might indicate a successful redirect capture, but generally, both colors signify a **successful capture**.Both colors indicate a snapshot exists, making that date a target for investigation.**Size**The **size of the circle** is the most important visual indicator. **A larger circle** means there were **more captures** of the page on that day.**Larger circles are often better.** More captures mean more changes were occurring that day (e.g., updates, news releases, or infrastructure changes), making it more likely to find useful, ephemeral information.**No Circle (or Faint/Grey)**Indicates **zero or very few** successful captures on that date.The website was likely static or the Wayback Machine bots did not visit on that day.



Step 3: Advanced Information Gathering: 1. Subdomain Enumeration: ○ Usetoolslike Sublist3r, Amass, or Subfinder to discover subdomains of the target website. These tools might uncover additional web services or resources

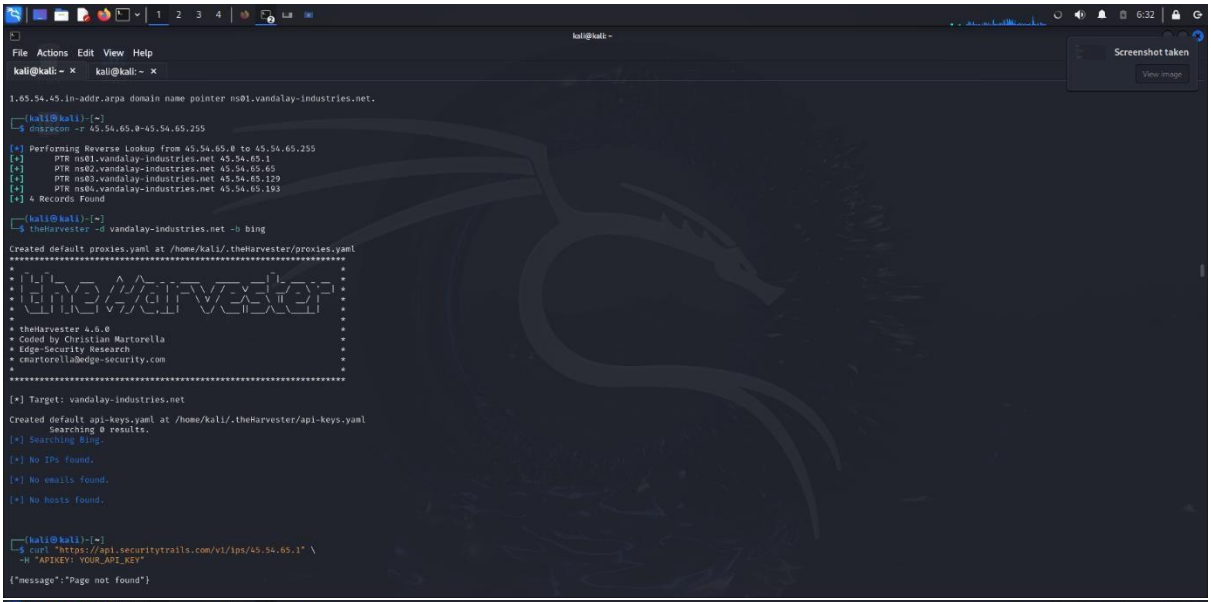

kali@kali: ~
File Actions Edit View Help
kali@kali: ~
kali@kali: ~
(kali㉿kali)-[~]
$ subfinder -d rockstargames.com -all
projectdiscovery.io
[INF] Current subfinder version v2.6.0 (outdated)
[INF] Loading provider config from /home/kali/.config/subfinder/provider-conf
ig.yaml
[INF] Enumerating subdomains for rockstargames.com
cs-rgl-prod.ros.rockstargames.com
dev.hosted.cloud.rockstargames.com
patches.rockstargames.compatches.rockstargames.com
www.dev.p01ewr.pod.rockstargames.com
sentryingest.rockstargames.com
web.rockstargames.com
dev.graph.rockstargames.com
smdx2ifs9.rockstargames.com
www-eaa.rockstargames.com
feed-rdr2-prod.ros.rockstargames.com
smtp.rockstargames.com
rsoevpn-west.rockstargames.com
cms.ros.rockstargames.com
www.dev.loc.rockstargames.com
emailcontent.rockstargames.com
prod.gamespy.rockstargames.com
ko.socialclub.rockstargames.com
zh.socialclub.rockstargames.com
gamedownloads.rockstargames.com
prod-catalog-cloud.rockstargames.com
relay2.rockstargames.com
sjcpdc1-web3-rdr2-prod.ros.rockstargames.com
view.newsletter.rockstargames.com
ja.socialclub.rockstargames.com
media-dev.rockstargames.com
dev2.rockstargames.com
sjcpdc1-web1-rdr2-prod.ros.rockstargames.com
mta2.newsletter.rockstargames.com
view-adm.rockstargames.com
dev.rockstargames.com
cloud.rockstargames.com
cs-gta5-prod.ros.rockstargames.com
facebook.rockstargames.com

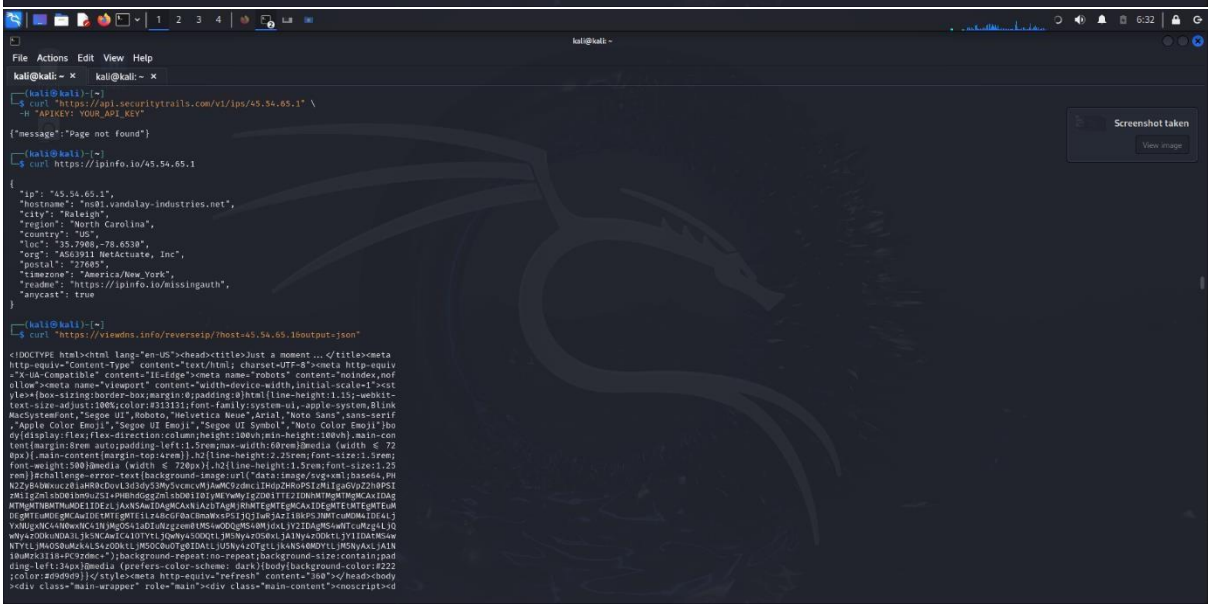

kali@kali: ~
File Actions Edit View Help
kali@kali: ~
kali@kali: ~
sjcpdc3-web2-rdr2-prod.ros.rockstargames.com
graph.rockstargames.com
jobsadmin2.rockstargames.com
dev-stage.rockstargames.com
dev.scapi.rockstargames.com
stage-cert.scauth.rockstargames.com
warehouse.rockstargames.com
level9.rockstargames.com
employee.store.rockstargames.com
[INF] Found 478 subdomains for rockstargames.com in 30 seconds 12 milliseconds
(kali㉿kali)-[~]
$ amass enum -d rockstargames.com
rockstargames.com (FQDN) --> ns_record --> ns02.vandalay-industries.net (FQDN)
rockstargames.com (FQDN) --> ns_record --> dns4.p05.nsone.net (FQDN)
rockstargames.com (FQDN) --> ns_record --> dns3.p05.nsone.net (FQDN)
rockstargames.com (FQDN) --> ns_record --> ns04.vandalay-industries.net (FQDN)
rockstargames.com (FQDN) --> ns_record --> dns2.p05.nsone.net (FQDN)
rockstargames.com (FQDN) --> ns_record --> ns03.vandalay-industries.net (FQDN)
rockstargames.com (FQDN) --> ns_record --> ns01.vandalay-industries.net (FQDN)
rockstargames.com (FQDN) --> ns_record --> dns1.p05.nsone.net (FQDN)
rockstargames.com (FQDN) --> mx_record --> mxa-002e6402.gslb.pphosted.com (FQDN)
rockstargames.com (FQDN) --> mx_record --> mxb-002e6402.gslb.pphosted.com (FQDN)
rockstargames.com (FQDN) --> node --> prod.cloud.rockstargames.com (FQDN)
rockstargames.com (FQDN) --> node --> webmail.rockstargames.com (FQDN)
prod.cloud.rockstargames.com (FQDN) --> cname_record --> prod.cloud.rockstargames.com.edgekey.net (FQDN)
webmail.rockstargames.com (FQDN) --> cname_record --> mail.gtm.take2games.com (FQDN)
upload2005.rockstargames.com (FQDN) --> cname_record --> mocksites-rockstargames.edgesuite.net (FQDN)
stage-dev-catalog.rockstargames.com (FQDN) --> cname_record --> stage-dev-catalog-cloud.rockstargames.com.edgekey.net (FQDN)
^Cvanity.employee.store.rockstargames.com (FQDN) --> cname_record --> d1nogw876chdmr.cloudfront.net (FQDN)
The enumeration has finished
(kali㉿kali)-[~]
$ sublist3r -d rockstargames.com
Command 'sublist3r' not found, but can be installed with:
sudo apt install sublist3r
Do you want to install it? (N/y)y



2. Reverse IP Lookup:

○ Perform a reverse IP lookup using tools like ipinfo.io or online services. This might reveal other websites hosted on the same IP address.

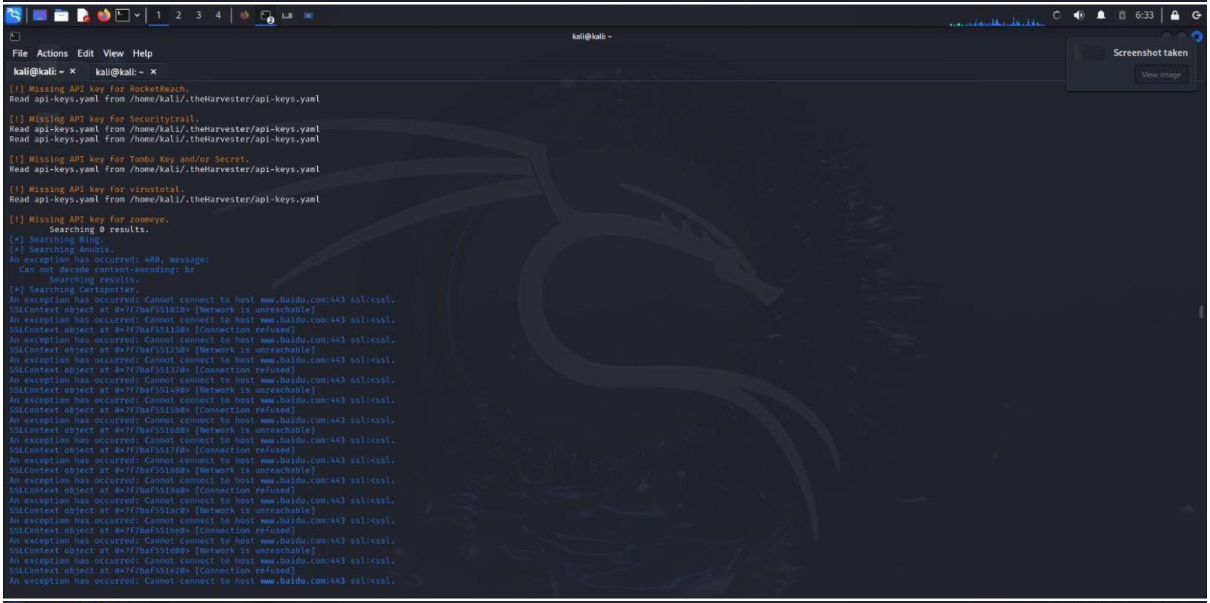


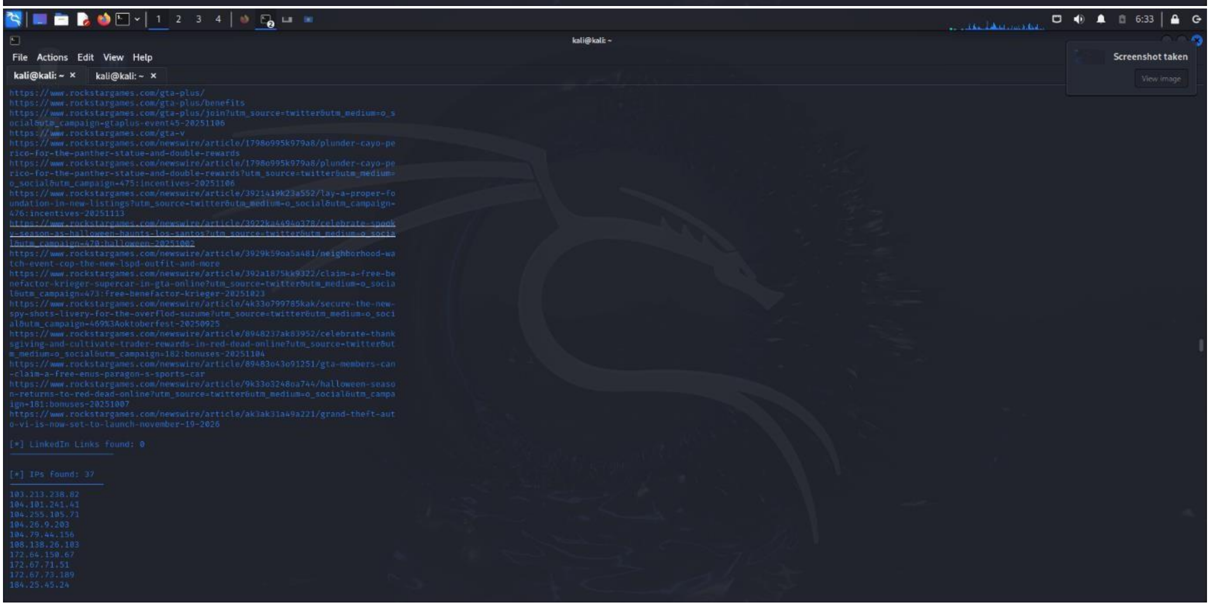


3. SSL Certificate Analysis:

○ UseonlineSSL certificate analysis tools to gather information about the target website's certificate. Identify the certificate authority, expiration date, and sometimes subdomains.


File Actions Edit View Help
kali@kali: ~
(kali㉿kali)-[~]
$ theHarvester -d rockstargames.com -l 500 -b all
Read proxies.yaml from /home/kali/.theHarvester/proxies.yaml
* theHarvester 4.6.0
* Coded by Christian Martorella
* Edge-Security Research
* cmartorella@edge-security.com
[*] Target: rockstargames.com
Read api-keys.yaml from /home/kali/.theHarvester/api-keys.yaml
[!] Missing API key for bevigil.
Read api-keys.yaml from /home/kali/.theHarvester/api-keys.yaml
[!] Missing API key for binaryedge.
Read api-keys.yaml from /home/kali/.theHarvester/api-keys.yaml
Read api-keys.yaml from /home/kali/.theHarvester/api-keys.yaml
Read api-keys.yaml from /home/kali/.theHarvester/api-keys.yaml
[!] Missing API key for bufferoverun.
Read api-keys.yaml from /home/kali/.theHarvester/api-keys.yaml
Read api-keys.yaml from /home/kali/.theHarvester/api-keys.yaml
[!] Missing API key for Censys ID and/or Secret.
Read api-keys.yaml from /home/kali/.theHarvester/api-keys.yaml
[!] Missing API key for criminalip.
Read api-keys.yaml from /home/kali/.theHarvester/api-keys.yaml
[!] Missing API key for fullhunt.
Read api-keys.yaml from /home/kali/.theHarvester/api-keys.yaml
[!] Missing API key for Github.
Read api-keys.yaml from /home/kali/.theHarvester/api-keys.yaml
[!] Missing API key for Hunter.
Read api-keys.yaml from /home/kali/.theHarvester/api-keys.yaml
Screenshot taken
View image


File Actions Edit View Help
kali@kali: ~
[!] Missing API key for RocketReach.
Read api-keys.yaml from /home/kali/.theHarvester/api-keys.yaml
[!] Missing API key for Securitytrail.
Read api-keys.yaml from /home/kali/.theHarvester/api-keys.yaml
Read api-keys.yaml from /home/kali/.theHarvester/api-keys.yaml
[!] Missing API key for Tomba Key and/or Secret.
Read api-keys.yaml from /home/kali/.theHarvester/api-keys.yaml
[!] Missing API key for virustotal.
Read api-keys.yaml from /home/kali/.theHarvester/api-keys.yaml
[!] Missing API key for zoomeye.
Searching 0 results.
[*] Searching Bing.
[*] Searching Anubis.
An exception has occurred: 400, message:
Can not decode content-encoding: br
Searching results.
[*] Searching Certspotter.
An exception has occurred: Cannot connect to host www.baidu.com:443 ssl:<ssl.
SSLContext object at 0x7f7baf551010> [Network is unreachable]
An exception has occurred: Cannot connect to host www.baidu.com:443 ssl:<ssl.
SSLContext object at 0x7f7baf551130> [Connection refused]
An exception has occurred: Cannot connect to host www.baidu.com:443 ssl:<ssl.
SSLContext object at 0x7f7baf551250> [Network is unreachable]
An exception has occurred: Cannot connect to host www.baidu.com:443 ssl:<ssl.
SSLContext object at 0x7f7baf551370> [Connection refused]
An exception has occurred: Cannot connect to host www.baidu.com:443 ssl:<ssl.
SSLContext object at 0x7f7baf551490> [Network is unreachable]
An exception has occurred: Cannot connect to host www.baidu.com:443 ssl:<ssl.
SSLContext object at 0x7f7baf5515b0> [Connection refused]
An exception has occurred: Cannot connect to host www.baidu.com:443 ssl:<ssl.
SSLContext object at 0x7f7baf5516d0> [Network is unreachable]
An exception has occurred: Cannot connect to host www.baidu.com:443 ssl:<ssl.
SSLContext object at 0x7f7baf5517f0> [Connection refused]
An exception has occurred: Cannot connect to host www.baidu.com:443 ssl:<ssl.
SSLContext object at 0x7f7baf551880> [Network is unreachable]
An exception has occurred: Cannot connect to host www.baidu.com:443 ssl:<ssl.
SSLContext object at 0x7f7baf5519a0> [Connection refused]
An exception has occurred: Cannot connect to host www.baidu.com:443 ssl:<ssl.
SSLContext object at 0x7f7baf551ac0> [Network is unreachable]
An exception has occurred: Cannot connect to host www.baidu.com:443 ssl:<ssl.
SSLContext object at 0x7f7baf551be0> [Connection refused]
An exception has occurred: Cannot connect to host www.baidu.com:443 ssl:<ssl.
SSLContext object at 0x7f7baf551d00> [Network is unreachable]
An exception has occurred: Cannot connect to host www.baidu.com:443 ssl:<ssl.
SSLContext object at 0x7f7baf551e20> [Connection refused]
An exception has occurred: Cannot connect to host www.baidu.com:443 ssl:<ssl.
Screenshot taken
View image


File Actions Edit View Help
kali@kali: ~
https://www.rockstargames.com/gta-plus/
https://www.rockstargames.com/gta-plus/benefits
https://www.rockstargames.com/gta-plus/join?utm_source=twitter&utm_medium=o_social&utm_campaign=gtaplus-event45-20251106
https://www.rockstargames.com/gta-v
https://www.rockstargames.com/newswire/article/1798o995k979a8/plunder-cayo-perico-for-the-panther-statue-and-double-rewards
https://www.rockstargames.com/newswire/article/1798o995k979a8/plunder-cayo-perico-for-the-panther-statue-and-double-rewards?utm_source=twitter&utm_medium=o_social&utm_campaign=475:incentives-20251106
https://www.rockstargames.com/newswire/article/3921419k23a552/lay-a-proper-foundation-in-new-listings?utm_source=twitter&utm_medium=o_social&utm_campaign=476:incentives-20251113
https://www.rockstargames.com/newswire/article/3922ka4494o378/celebrate-spooky-season-as-halloween-haunts-los-santos?utm_source=twitter&utm_medium=o_social&utm_campaign=470:halloween-20251002
https://www.rockstargames.com/newswire/article/3929k59oa5a481/neighborhood-watch-event-cop-the-new-lspd-outfit-and-more
https://www.rockstargames.com/newswire/article/392a1875kk9322/claim-a-free-benefactor-krieger-supercar-in-gta-online?utm_source=twitter&utm_medium=o_social&utm_campaign=473:free-benefactor-krieger-20251023
https://www.rockstargames.com/newswire/article/4k33o799785kak/secure-the-new-spy-shots-livery-for-the-overflod-suzume?utm_source=twitter&utm_medium=o_social&utm_campaign=469%3Aoktoberfest-20250925
https://www.rockstargames.com/newswire/article/8948237ak83952/celebrate-thanksgiving-and-cultivate-trader-rewards-in-red-dead-online?utm_source=twitter&utm_medium=o_social&utm_campaign=182:bonuses-20251104
https://www.rockstargames.com/newswire/article/89483o43o91251/gta-members-can-claim-a-free-enus-paragon-s-sports-car
https://www.rockstargames.com/newswire/article/9k33o3248oa744/halloween-season-returns-to-red-dead-online?utm_source=twitter&utm_medium=o_social&utm_campaign=181:bonuses-20251007
https://www.rockstargames.com/newswire/article/ak3ak31a49a221/grand-theft-auto-vi-is-now-set-to-launch-november-19-2026
[*] LinkedIn Links found: 0
[*] IPs found: 37
103.213.238.82
104.101.241.41
104.255.105.71
104.26.9.203
104.79.44.156
108.138.26.103
172.64.150.67
172.67.71.51
172.67.73.189
184.25.45.24
Screenshot taken
View image

3. Social Media Analysis: ○ Search social media platforms for official accounts associated with the target website. This can provide insights into the website's branding, updates, and potentially employees associated with it.
4.

rockstargames

Rockstar Games

19 posts **29.8M** followers **1,009** following

The official home of Rockstar Games on Instagram

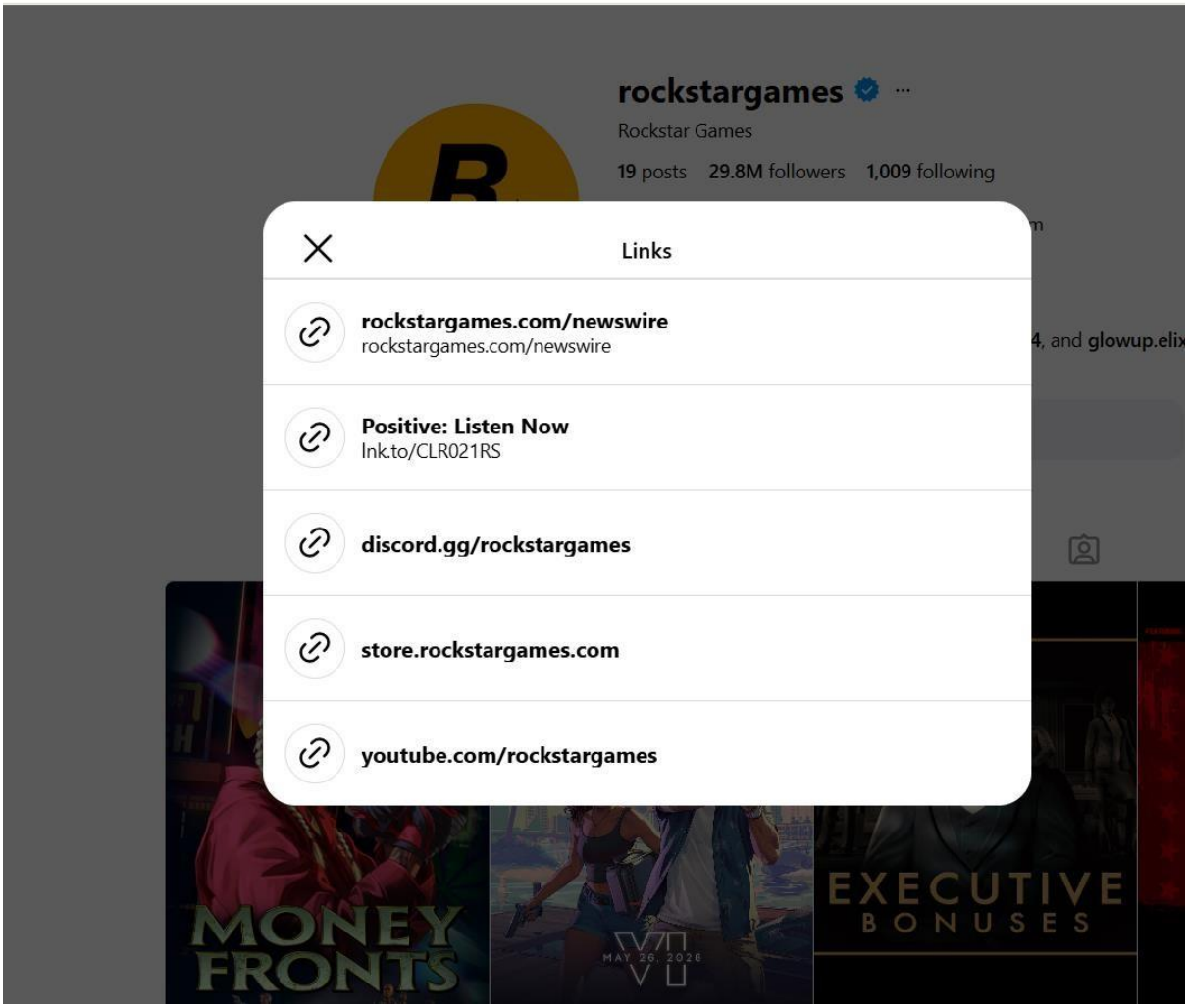
rockstargames.com/newswire and 4 more

rockstargames

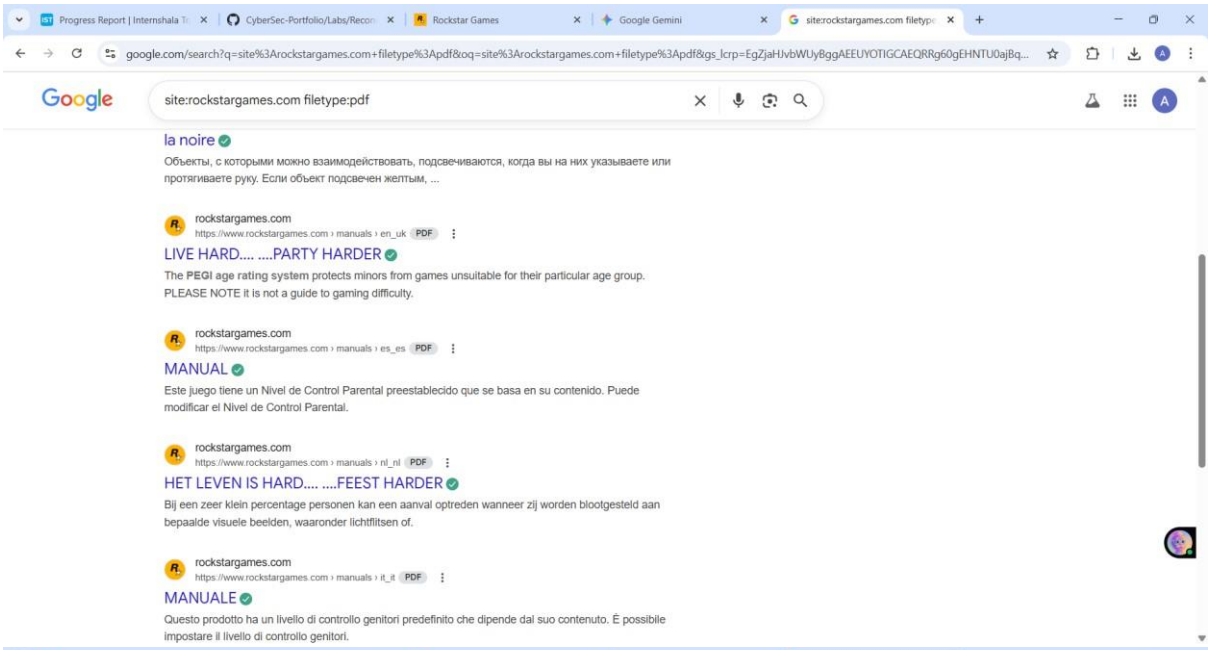
Followed by **akshatsah_**, **ethics404**, and **glowup.elix**

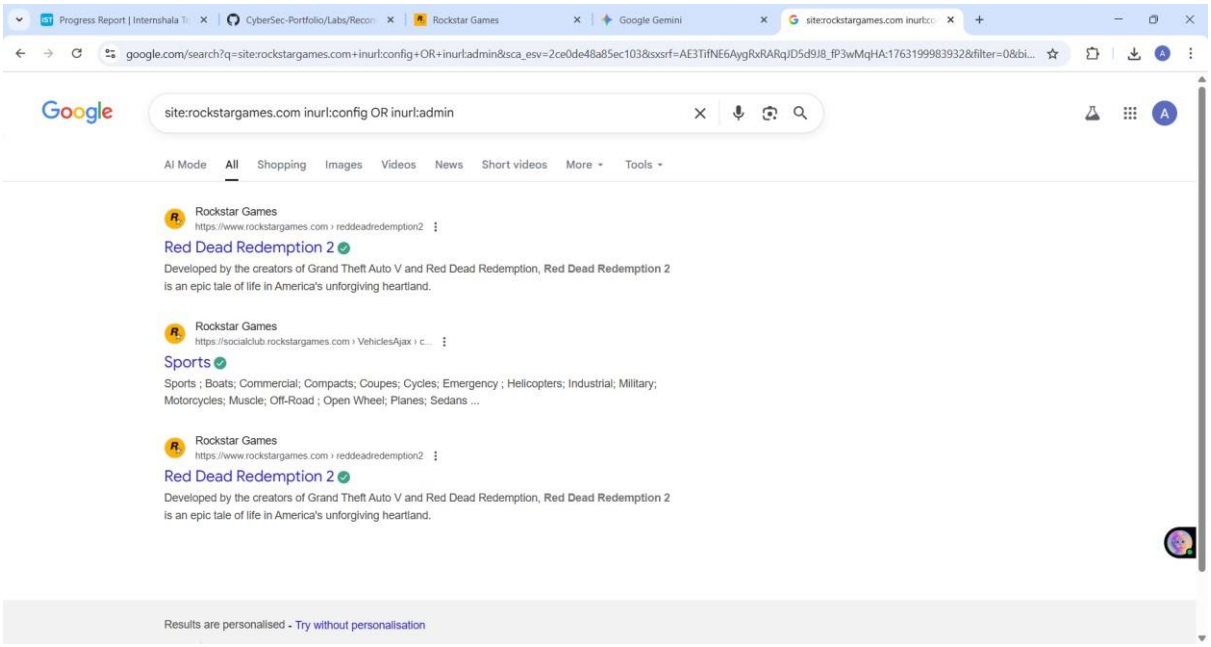
Follow | Message

argames/



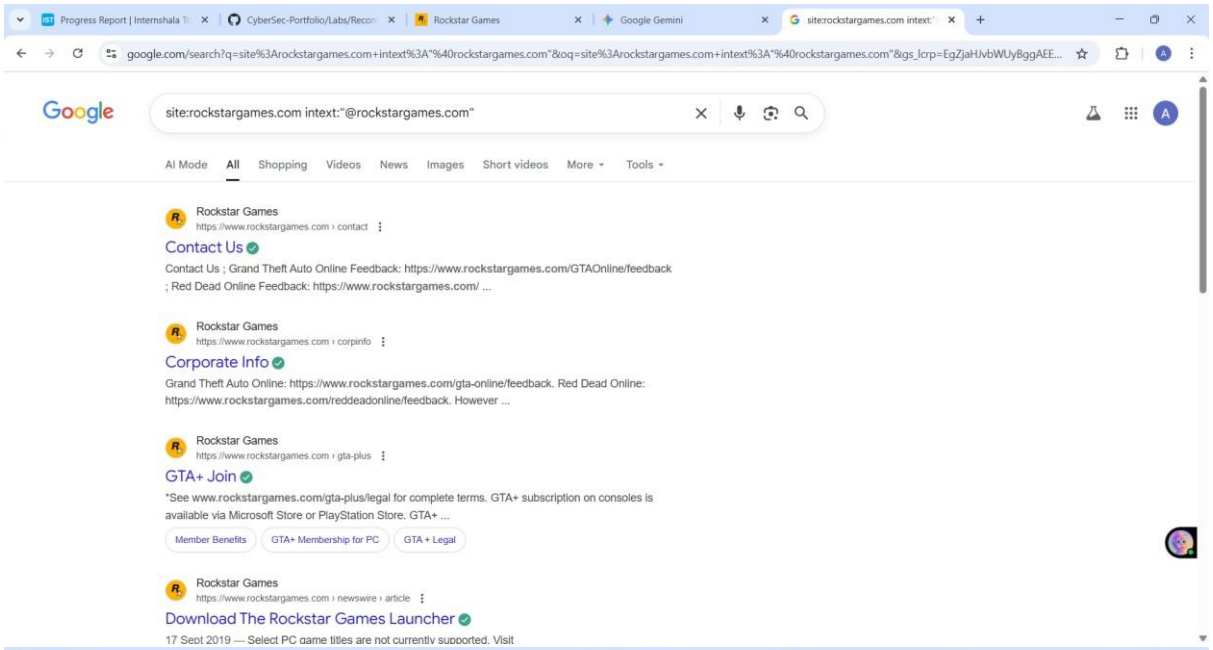
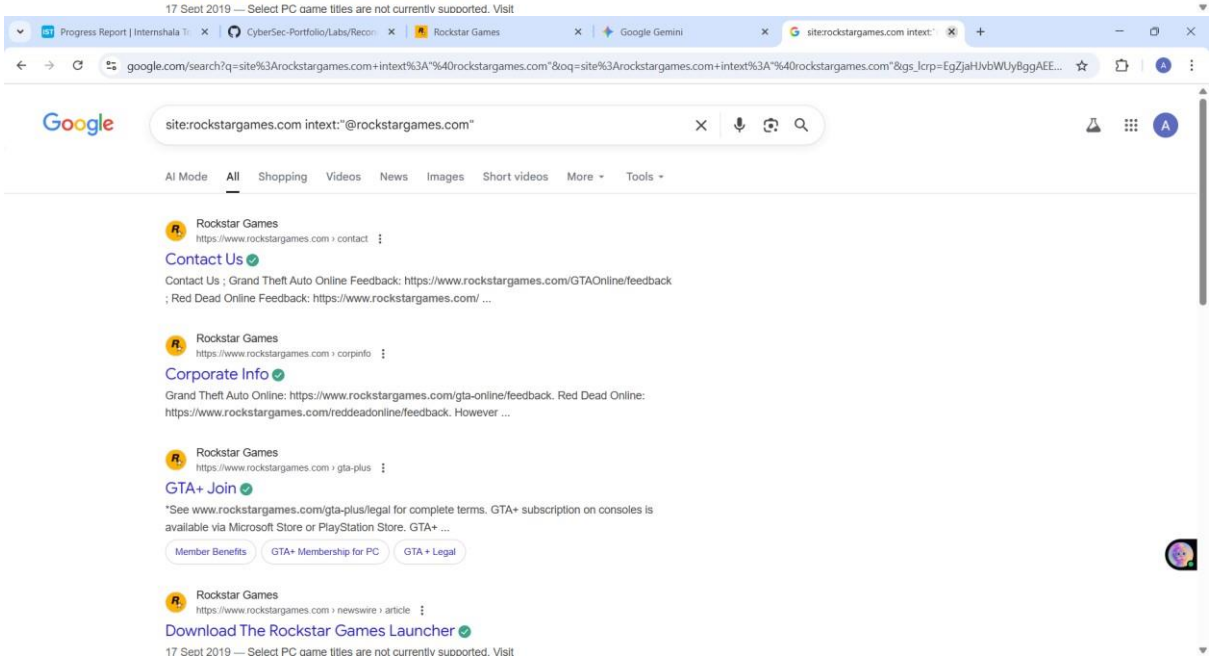
5. Google Hacking (Dorking):
○ UseGoogleadvanced search operators ("dorks") to find sensitive information or hidden content on the target website. For example, try searching for site:targetwebsite.com filetype:pdf to find PDF files on the site





6. Email Harvesting:

○ Searchfor email addresses associated with the target website. These can be found in contact pages, "About Us" sections, or using tools designed for email harvesting


Progress Report | Internshala T
CyberSec-Portfolio/Labs/Recon
Rockstar Games
Google Gemini
site:rockstargames.com intext:"
google.com/search?q=site%3Arockstargames.com+intext%3A"%40rockstargames.com"&oq=site%3Arockstargames.com+intext%3A"%40rockstargames.com"&gs_lcrp=EgZjaHJvbWUyBggAEE...
Google
site:rockstargames.com intext:"@rockstargames.com"
AI Mode
All
Shopping
Videos
News
Images
Short videos
More
Tools
Rockstar Games
https://www.rockstargames.com › contact
Contact Us
Contact Us ; Grand Theft Auto Online Feedback: https://www.rockstargames.com/GTAOnline/feedback ; Red Dead Online Feedback: https://www.rockstargames.com/ ...
Rockstar Games
https://www.rockstargames.com › corpinfo
Corporate Info
Grand Theft Auto Online: https://www.rockstargames.com/gta-online/feedback. Red Dead Online: https://www.rockstargames.com/reddeadonline/feedback. However ...
Rockstar Games
https://www.rockstargames.com › gta-plus
GTA+ Join
*See www.rockstargames.com/gta-plus/legal for complete terms. GTA+ subscription on consoles is available via Microsoft Store or PlayStation Store. GTA+ ...
Member Benefits
GTA+ Membership for PC
GTA+ Legal
Rockstar Games
https://www.rockstargames.com › newswire › article
Download The Rockstar Games Launcher
17 Sept 2019 — Select PC game titles are not currently supported. Visit

Progress Report | Internshala T
CyberSec-Portfolio/Labs/Recon
Rockstar Games
Google Gemini
site:rockstargames.com intext:"
google.com/search?q=site%3Arockstargames.com+intext%3A"%40rockstargames.com"&oq=site%3Arockstargames.com+intext%3A"%40rockstargames.com"&gs_lcrp=EgZjaHJvbWUyBggAEE...
Google
site:rockstargames.com intext:"@rockstargames.com"
AI Mode
All
Shopping
Videos
News
Images
Short videos
More
Tools
Rockstar Games
https://www.rockstargames.com › contact
Contact Us
Contact Us ; Grand Theft Auto Online Feedback: https://www.rockstargames.com/GTAOnline/feedback ; Red Dead Online Feedback: https://www.rockstargames.com/ ...
Rockstar Games
https://www.rockstargames.com › corpinfo
Corporate Info
Grand Theft Auto Online: https://www.rockstargames.com/gta-online/feedback. Red Dead Online: https://www.rockstargames.com/reddeadonline/feedback. However ...
Rockstar Games
https://www.rockstargames.com › gta-plus
GTA+ Join
*See www.rockstargames.com/gta-plus/legal for complete terms. GTA+ subscription on consoles is available via Microsoft Store or PlayStation Store. GTA+ ...
Member Benefits
GTA+ Membership for PC
GTA+ Legal
Rockstar Games
https://www.rockstargames.com › newswire › article
Download The Rockstar Games Launcher
17 Sept 2019 — Select PC game titles are not currently supported. Visit