Recon & OSINT Mastery Analysis Report

Name:Suranjana B. Samanta
Course:BTech Cyber Security

1.Executive Summary:

Target Organization: World Wide Web Consortium
Domain:w3.org
Reason for selecting the target:

- Ideal for OSINT research,
- Public-facing infrastructure

The World Wide Web Consortium (W3C) was selected as it has a well-documented public-facing infrastructure, making it suitable for ethical OSINT research and digital footprint analysis.This project focuses on analyzing the publicly available digital footprint of the target organization using OSINT techniques.

2.Methodology:

□ **Passive Reconnaissance**

Tools: WHOIS
Google Dorks
Social Media Accounts
Public Documents

Passive reconnaissance was performed to collect publicly available information without direct interaction with the target systems.

□ **Active Reconnaissance**

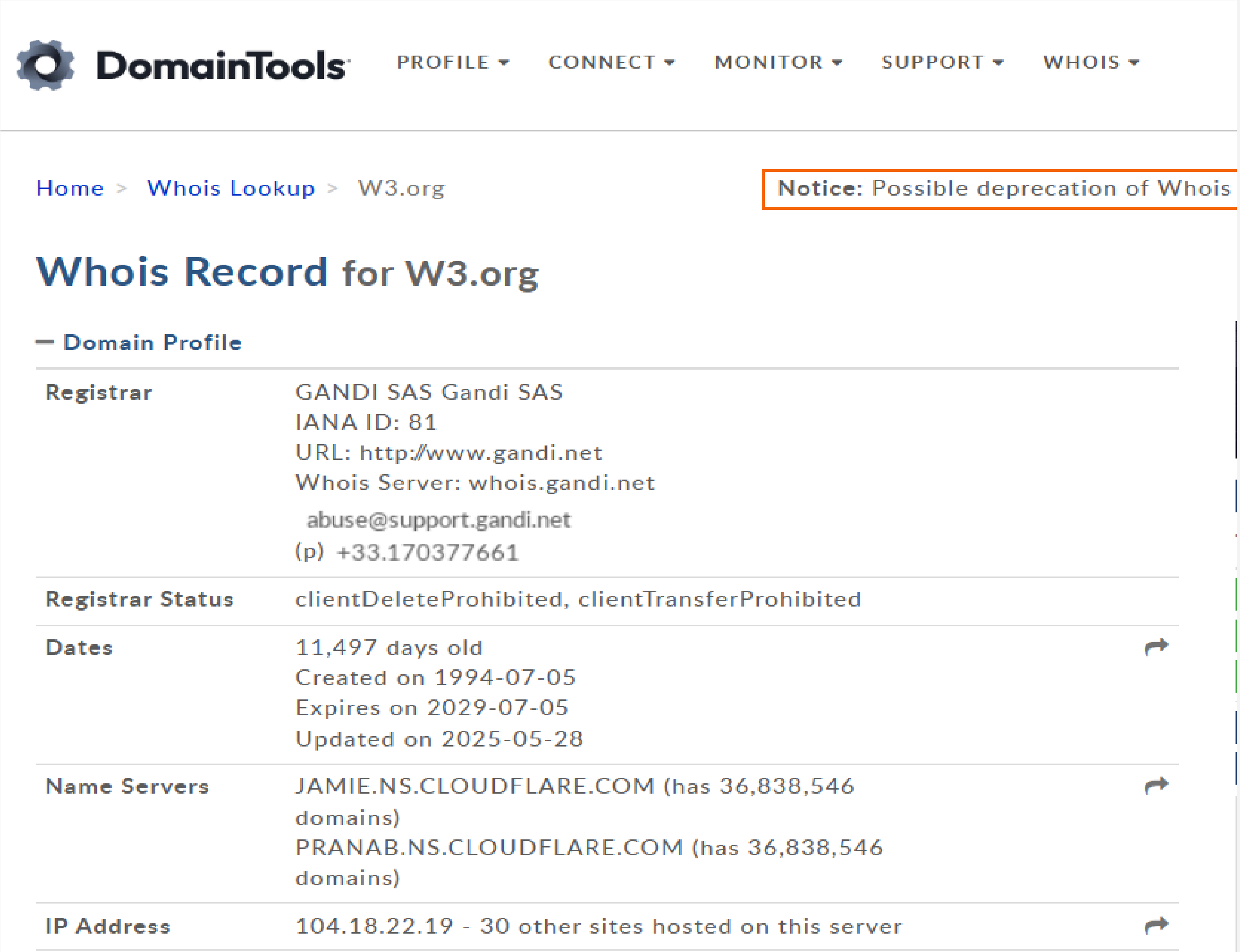
Tools: DNSdumpster
Nmap

Active reconnaissance was limited to non-intrusive scanning techniques for identifying subdomains, open ports, and exposed services.

3.Findings:

A. WHOIS (Domain Information)

After searching for the required domain we can get the information about the domain profile, Registrar, Registrar Status and the IPs .



Notice: Possible deprecation of Whois

Whois Record for W3.org

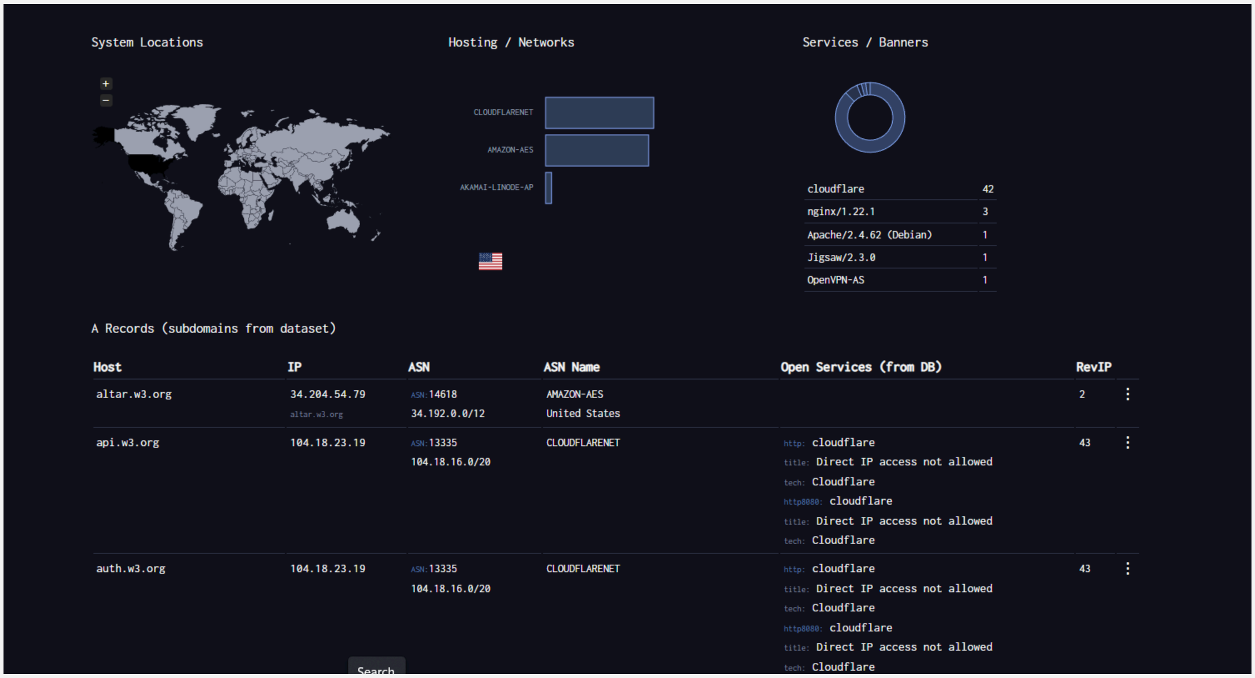
– Domain Profile

Registrar	GANDI SAS Gandi SAS IANA ID: 81 URL: http://www.gandi.net Whois Server: whois.gandi.net abuse@support.gandi.net (p) +33.170377661
Registrar Status	clientDeleteProhibited, clientTransferProhibited
Dates	11,497 days old Created on 1994-07-05 Expires on 2029-07-05 Updated on 2025-05-28
Name Servers	JAMIE.NS.CLOUDFLARE.COM (has 36,838,546 domains) PRANAB.NS.CLOUDFLARE.COM (has 36,838,546 domains)
IP Address	104.18.22.19 - 30 other sites hosted on this server

B.DNSDumpster (Subdomains)

After searching for the domains we can get to know about all the domains and can analyze the attack surface.

Through the screenshot we can get to know about the wide spread overall, also the legal information about the servers domains.



System Locations

Hosting / Networks

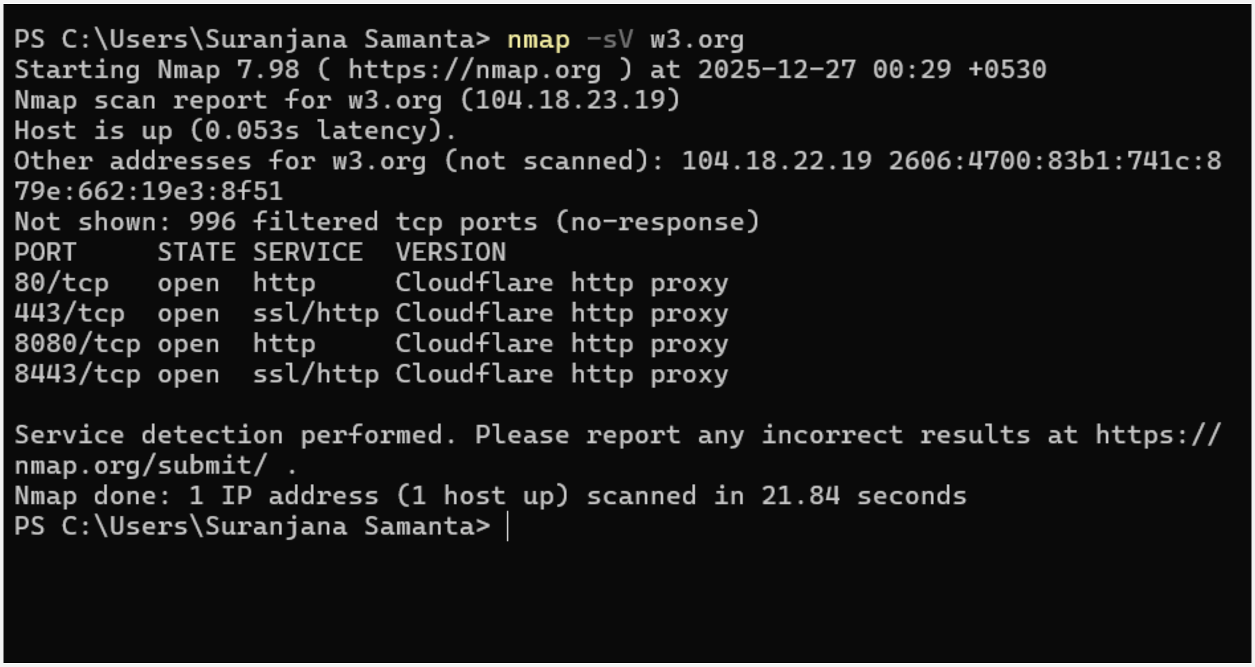
Services / Banners

cloudflare	42
nginx/1.22.1	3
Apache/2.4.62 (Debian)	1
Jigsaw/2.3.0	1
OpenVPN-AS	1

A Records (subdomains from dataset)

Host	IP	ASN	ASN Name	Open Services (from DB)	RevIP
altar.w3.org	34.204.54.79 altar.w3.org	ASN:14618 34.192.0.0/12	AMAZON-AES United States		2
api.w3.org	104.18.23.19	ASN:13335 104.18.16.0/20	CLOUDFLARENET	http: cloudflare title: Direct IP access not allowed tech: Cloudflare http8080: cloudflare title: Direct IP access not allowed tech: Cloudflare	43
auth.w3.org	104.18.23.19	ASN:13335 104.18.16.0/20	CLOUDFLARENET	http: cloudflare title: Direct IP access not allowed tech: Cloudflare http8080: cloudflare title: Direct IP access not allowed tech: Cloudflare	43

C.Nmap Scan :



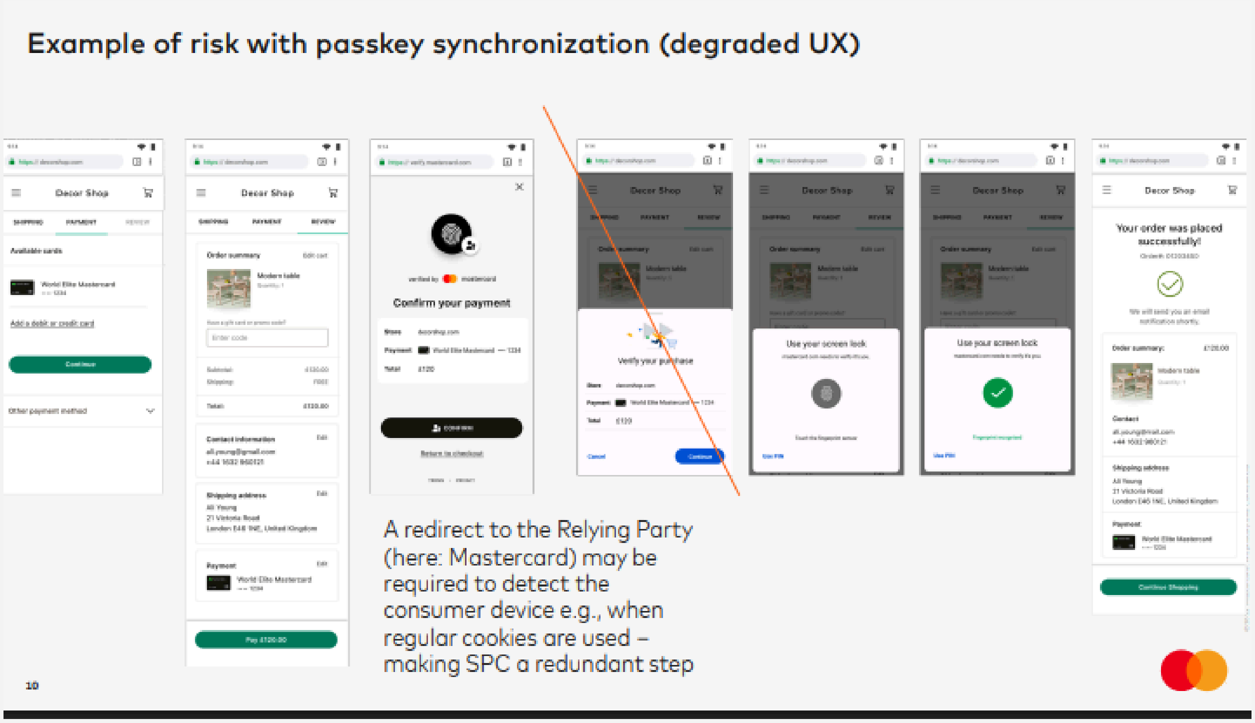
```
PS C:\Users\Suranjana Samanta> nmap -sV w3.org
Starting Nmap 7.98 ( https://nmap.org ) at 2025-12-27 00:29 +0530
Nmap scan report for w3.org (104.18.23.19)
Host is up (0.053s latency).
Other addresses for w3.org (not scanned): 104.18.22.19 2606:4700:83b1:741c:8
79e:662:19e3:8f51
Not shown: 996 filtered tcp ports (no-response)
PORT     STATE SERVICE  VERSION
80/tcp   open  http     Cloudflare http proxy
443/tcp  open  ssl/http Cloudflare http proxy
8080/tcp open  http     Cloudflare http proxy
8443/tcp open  ssl/http Cloudflare http proxy

Service detection performed. Please report any incorrect results at https://
nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 21.84 seconds
PS C:\Users\Suranjana Samanta>
```

After completing these scans we can get to know about the open ports , version of the services.

Nmap scanning showed only standard web service ports(80/443), indicating a hardened external perimeter.However,publicly accessible services still require continuous monitoring and patching.

D.Google Dorking (Documents and Public Data)

Publicly accessible PDFs , public presentations.



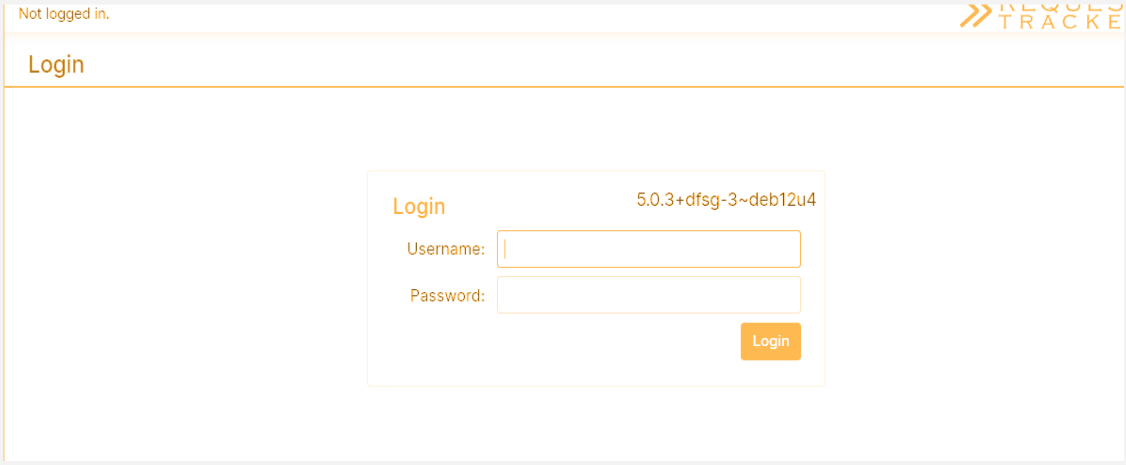
Example of risk with passkey synchronization (degraded UX)

A redirect to the Relying Party (here: Mastercard) may be required to detect the consumer device e.g., when regular cookies are used – making SPC a redundant step

10

Publicly accessible presentation describing passkey synchronization and payment authentication flow found via Google Dorking.

Login Page:



Not logged in.

5.0.3+dfsg-3~deb12u4

A publicly accessible login page was identified that disclosed software version information (version 5.0.3). Such version disclosure may assist attackers in technology fingerprinting if not intentionally exposed.
The login page showing the details about the version of software may create an attack surface.

4. Analysis:

No directly found vulnerabilities.
Workflow documentation may reduce attacker effort.

1. Google Dorking: It revealed publicly accessible documents,presentations,and login interfaces.While no sensitive credentials were found,exposure of software versions details may assist attackers in understanding system behavior and planning targeted attacks.

2. DNSDumpster: The presence of multiple subdomains increases the overall attack surface.Test or development related subdomains may pose configuration risks if not properly secured.

3. Nmap : Nmap scanning showed only standard web service ports(80/443), indicating a hardened external perimeter.However,publicly accessible services still require continuous monitoring and patching.

Finding	Risk Level	Impact
Public PPT with auth workflow	Medium	Aids attack planning
Login page with version info	Medium	Tech fingerprinting
Multiple subdomains	Low–Medium	Expanded attack surface
Public PDFs	Low	Information disclosure

5.Mitigation / Recovery :

Under **Recovery Simulation**:

Immediate

- Review publicly available documents for sensitive workflow exposure

Short-Term

- Sanitize slides before public release
- Remove unnecessary internal diagrams

Long-Term

- Implement document classification policy
- OSINT monitoring for exposed materials.