Reconnaissance Practice

Activities

Tools:

- **Maltego** (relationship mapping, entity discovery)
- **Shodan** (internet-exposed devices/services)
- **Google Docs**
- **WHOIS**
- **Sublist3r**
- **Wappalyzer**

Domain Information

Domain: graceintlgroup.com
Registered On: 2015-09-22
Expires On: 2029-09-22
Updated On: 2024-09-16
Status:
client delete prohibited
client renew prohibited
client transfer prohibited
client update prohibited
Name Servers:
coby.ns.cloudflare.com
may.ns.cloudflare.com

Registrar Information

Registrar: GoDaddy.com, LLC
IANA ID: 146
Abuse Email: abuse@godaddy.com
Abuse Phone: 480-624-2505

Subdomain Identified

www.graceintigroup.com
au.graceintigroup.com
www.au.graceintigroup.com
australia.graceintigroup.com
www.australia.graceintigroup.com
cpanel.australia.graceintlgroup.com
cpcalendars.australia.graceintlgroup.com
cpcontacts.australia.graceintigroup.com
mail.australia.graceintigroup.com
webdisk.australia.graceintigroup.com
webmail.australia.graceintigroup.com
autodiscover.graceintigroup.com
cpanel.graceintigroup.com
cpcalendars.graceintigroup.com
cpcontacts.graceintigroup.com
fair.graceintigroup.com
www.fair.graceintigroup.com
cpanel.fair.graceintigroup.com
cpcalendars.fair.graceintigroup.com
cpcontacts.fair.graceintigroup.com
mail.fair.graceintigroup.com
webdisk.fair.graceintigroup.com
webmail.fair.graceintigroup.com
india.graceintigroup.com
www.india.graceintigroup.com
kenya.graceintigroup.com
www.kenya.graceintigroup.com
mail.graceintigroup.com
melboume.graceintigroup.com
www.melbourne.graceintigroup.com
portal.graceintigroup.com
qr.graceintigroup.com
ress.graceintigroup.com
www.ress.graceintigroup.com
seminar.graceintigroup.com
www.seminar.graceintigroup.com
india.graceintlgroup.com
www.india.graceintigroup.com
kenya.graceintigroup.com
www.kenya.graceintigroup.com
mail.graceintlgroup.com
melbourne.graceintigroup.com
www.melbourne.graceintigroup.com
portal.graceintigroup.com
qr.graceintigroup.com
ress.graceintigroup.com
www.ress.graceintigroup.com
seminar.graceintigroup.com
www.seminar.graceintigroup.com
cpanel.seminar.graceintigroup.com
cpcalendars.seminar.graceintlgroup.com
cpcontacts.seminar.graceintlgroup.com
mail.seminar.graceintigroup.com
webdisk.seminar.graceintlgrou
webmail.seminar.graceintigroup.com
study.graceintigroup.com
www.study.graceintigroup.com
wc.graceintigroup.com
webdisk.graceintlgroup.com
webmail.graceintigroup.com
worldcup.graceintigroup.com
www.worldcup.graceintlgroup.com
cpanel.worldcup.graceintigroup.com
cpcalendars.worldcup.graceintigroup.com
cpcontacts.worldcup.graceintigroup.com
mail.worldcup.graceintigroup.com
webdisk.worldcup.graceintlgroup.com
webmail.worldcup.graceintigroup.com

Exposed Services

IP/Host	Port	Service	Source (Tool)	Notes
143.0.138.186	80	HTTP	Shodan	Boa Webserver; Device type: Webcam; Basic Auth realm: "Webadmin"
177.131.129.255	80	HTTP	Shodan	Boa Webserver; Device type: Webcam
120.217.7.89	554	RTSP	Shodan	Common for streaming video; likely IP camera
	81	HTTP	Shodan	May host web admin interface
39.10.156.56	554	RTSP	Shodan	Exposed video stream
	81	HTTP	Shodan	Web interface possibly unsecured
172.102.1.217	554	RTSP	Shodan	Vulnerable to CVE-2017-17106, CVE-2018-10088, and others
	81	HTTP	Shodan	Admin panel exposed; multiple known vulnerabilities

Asset Mapping Log

Timestamp	Tool	Finding
2025-11-20 07:30:00	Shodan	Exposed HTTP on 143.0.138.186 (Boa Webserver, Webcam, Brazil)
2025-11-20 07:35:00	Shodan	Exposed HTTP on 177.131.129.255 (Boa Webserver, Webcam, Brazil)
2025-11-20 07:40:00	Shodan	Exposed RTSP & HTTP on 120.217.7.89 (Likely IP camera, China)
2025-11-20 07:45:00	Shodan	Vulnerable device at 172.102.1.217 (CVE-2017-17106, CVE-2018-10088, etc.)
2025-11-20 07:50:00	Sublist3r	Found 53 subdomains for greenwing.com (e.g., dev.greenwing.com, vpn.greenwing.com)
2025-11-20 07:55:00	Wappalyzer	Tech stack for grace.edu.np: WordPress, Apache, PHP, jQuery, Google Tag Manager
2025-11-20 08:00:00	Domain Map	Mapped subdomains of epornerfree.com (e.g., smtp.epornerfree.com, webmail.epornerfree.com)

Summary

Reconnaissance involved gathering public information using Shodan, Maltego, and Sublist3r. Domain details, subdomains, exposed services, and the technology stack were identified. Findings were documented in structured logs and checklists. This phase provided a clear view of external assets, potential exposure points, and relationships useful for later security testing.