Reconnaissance Practice Lab

Author: Harshal Harekar
Date: 07/10/2025

This lab focuses on gathering information about a target without directly touching it (OSINT).

1. Gather Domain Info

1. Using the whois command to find registration details

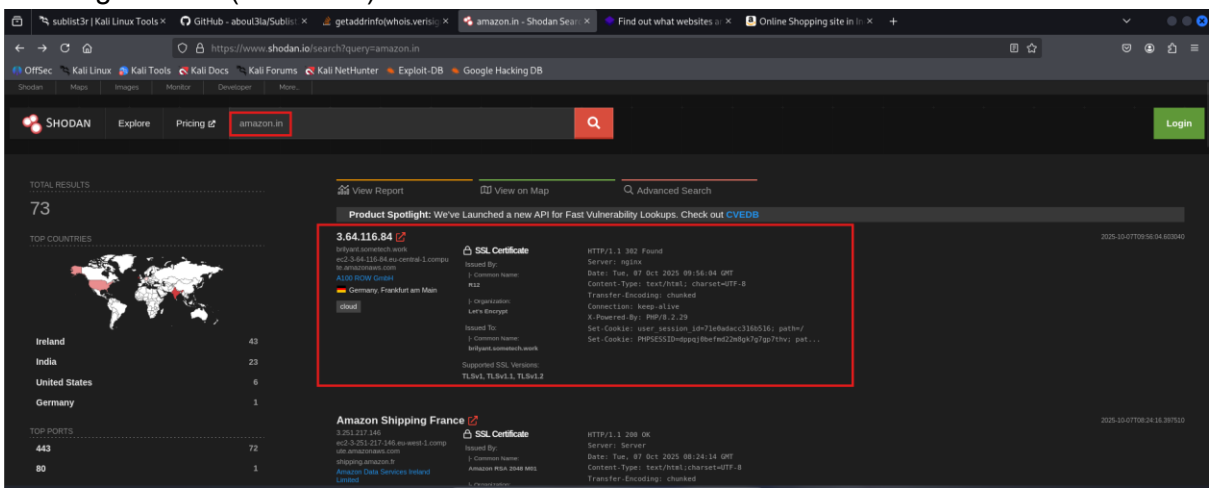
```
└─$ sudo whois amazon.in
Domain Name: amazon.in
Registry Domain ID: D15860-IN
Registrar WHOIS Server: whois.markmonitor.com
Registrar URL: http://www.markmonitor.com
Updated Date: 2025-01-15T09:50:52.705Z
Creation Date: 2005-02-11T11:14:14.378Z
Registry Expiry Date: 2026-02-11T11:14:14.378Z
Registrar: MarkMonitor Inc.
Registrar IANA ID: 292
Registrar Abuse Contact Email: abusecomplaints@markmonitor.com
Registrar Abuse Contact Phone:
Registrar Abuse Contact Email: registryescalations@markmonitor.com
Registrar Abuse Contact Phone:
Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited
Registry Registrant ID: REDACTED FOR PRIVACY
Registrant Name: REDACTED FOR PRIVACY
Registrant Organization: Amazon Technologies, Inc.
Registrant Street: REDACTED FOR PRIVACY
Registrant City: REDACTED FOR PRIVACY
Registrant State/Province: NV
Registrant Postal Code: REDACTED FOR PRIVACY
Registrant Country: US
Registrant Phone: REDACTED FOR PRIVACY
Registrant Fax: REDACTED FOR PRIVACY
Registrant Email: Please query the RDDS service of the Registrar of Record identified in
Registry Admin ID: REDACTED FOR PRIVACY
Admin Name: REDACTED FOR PRIVACY
Admin Organization: REDACTED FOR PRIVACY
Admin Street: REDACTED FOR PRIVACY
Admin City: REDACTED FOR PRIVACY
Admin State/Province: REDACTED FOR PRIVACY
Admin Postal Code: REDACTED FOR PRIVACY
Admin Country: REDACTED FOR PRIVACY
Admin Phone: REDACTED FOR PRIVACY
```

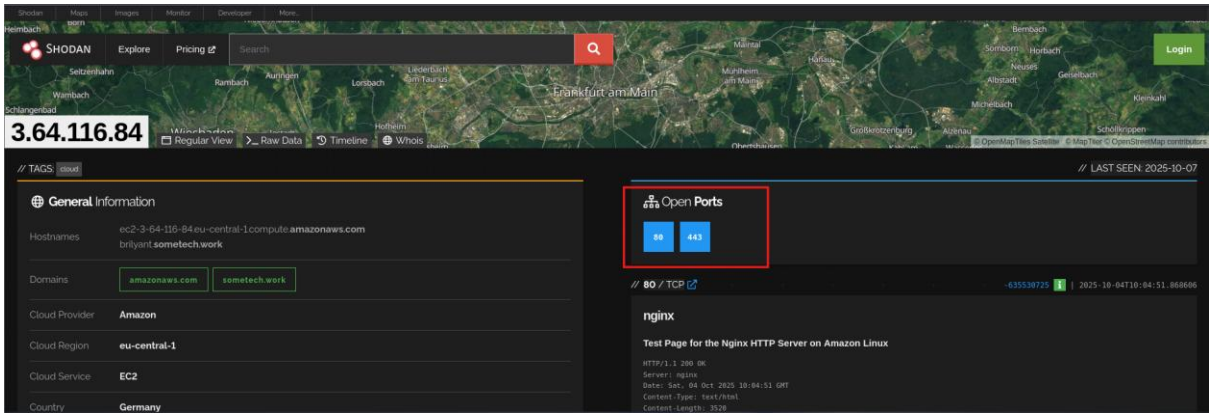
2. Enumerate Subdomains: Using a tool like Sublist3r

```
┌──(aazukaazu㉿kali)-[~]
└─$ sudo git clone https://github.com/aboul3la/Sublist3r.git
Cloning into 'Sublist3r'...
remote: Enumerating objects: 383, done.
remote: Total 383 (delta 0), reused 0 (delta 0), pack-reused 383 (from 1)
Receiving objects: 100% (383/383), 1.12 MiB | 7.00 MiB/s, done.
Resolving deltas: 100% (213/213), done.

┌──(aazukaazu㉿kali)-[~]
└─$ ls
Desktop  Documents  Downloads  Music  nmap_vuln_general.txt  Pictures  Public  Sublist3r  Templates  Videos

┌──(aazukaazu㉿kali)-[~]
└─$ cd Sublist3r
```

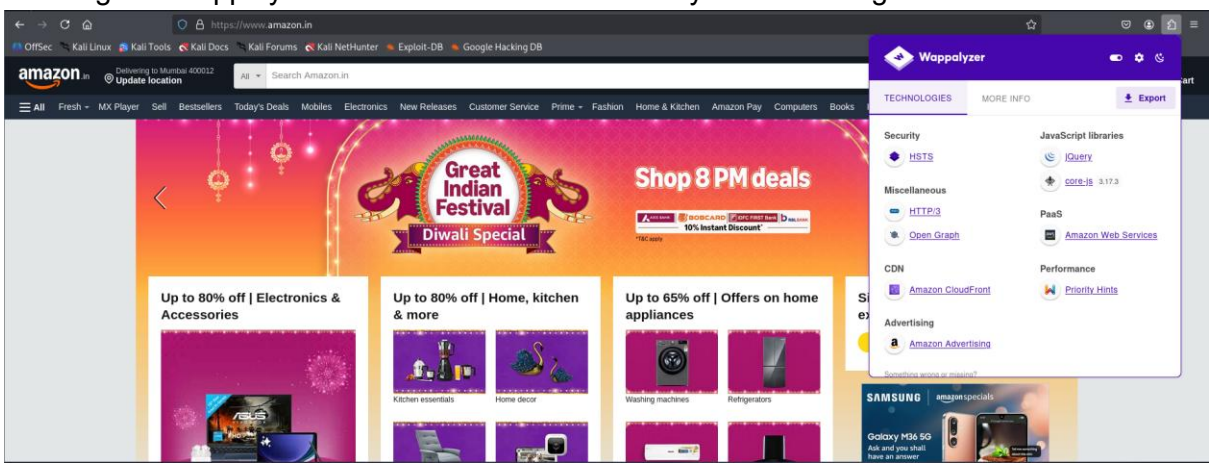
```
┌──(aazukaazu㉿kali)-[~/Sublist3r]
└─$ sudo python sublist3r.py -d amazon.in
/home/aazukaazu/Sublist3r/sublist3r.py:78: SyntaxWarning: invalid escape sequence '\_'
  \___ \| | | | '_ \| | / __| __| |_ \| '__|
/home/aazukaazu/Sublist3r/sublist3r.py:286: SyntaxWarning: invalid escape sequence '\/'
  link_regx = re.compile('<cite.*?>(.*?)<\/cite>')
/home/aazukaazu/Sublist3r/sublist3r.py:343: SyntaxWarning: invalid escape sequence '\/'
  link = re.sub("<(\/)?b>", "", link)
/home/aazukaazu/Sublist3r/sublist3r.py:439: SyntaxWarning: invalid escape sequence '\/'
  link = re.sub('<(\/)?strong>|<span.*?>|<|>', '', link)
/home/aazukaazu/Sublist3r/sublist3r.py:658: SyntaxWarning: invalid escape sequence '\/'
  tbl_regex = re.compile('<a name="hostanchor"><\/a>Host Records.*?<table.*?>(.*?)<\/table>', re.S)
/home/aazukaazu/Sublist3r/sublist3r.py:898: SyntaxWarning: invalid escape sequence '\-'
  domain_check = re.compile("^(http|https)?[a-zA-Z0-9]+([\-\.]{1}[a-zA-Z0-9]+)*\.[a-zA-Z]{2,}$")
/home/aazukaazu/Sublist3r/subbrute/subbrute.py:374: SyntaxWarning: invalid escape sequence '\.'
  domain_match = re.compile("([a-zA-Z0-9_-]*\.[a-zA-Z0-9_-]*\.[a-zA-Z0-9_-]*)+")

                 ____        _  _ _   _____
                / ___| _   _| |_| (_)___|___ / _ __
                \___ \| | | | __| | | / __| |_ \| '__|
                 ___) | |_| | |_| | | \__ \___) | |
                |____/ \__,_|\__|_|_|_|___/____/|_|

                # Coded By Ahmed Aboul-Ela - @aboul3la

[-] Enumerating subdomains now for amazon.in
[-] Searching now in Baidu..
[-] Searching now in Yahoo..
[-] Searching now in Google..
[-] Searching now in Bing..
```

3. Using Shodan (shodan.io) to search for IPs associated with





4. Using the Wappalyzer browser extension to identify the technologies used



2. Asset Mapping

Timestamp	Tools used	Findings
07-10-2025 22:35	whois	Registrar: MarkMonitor Inc.
07-10-2025 22:52	Sublist3r	Found 31 unique sub-domains
07-10-2025 23:07	Shodan	Found port 80, 443 open for one of the sub-domain
07-10-2025 23:11	Wappalyzer	Main site uses jQuery and JS

3. Recon Summary

Reconnaissance on amazon.in revealed key infrastructure details. The domain is registered via MarkMonitor Inc. We identified 31 subdomains. Main site uses jQuery and JS. Further investigation is needed to determine if any exposed services on associated IP addresses are running outdated, vulnerable software versions.