

## **Executive Post Graduate Certification in Cyber Security and Ethical Hacking Assignment-2**

**Bhargav Rohit Dhawala**

**22/01/25**

**Problem Statement:** The initial information gathered about the target may not be sufficient to identify all potential vulnerabilities. To uncover more detailed information and possible loopholes, it is necessary to employ various footprinting tools. As an ethical hacker, your task is to gather as much information as possible about the target using OSINT Framework. This additional information will help in identifying vulnerabilities and enhancing the security assessment of the target.

### **Objectives:**

- Footprint a target using the OSINT Framework.
- Gather DNS information using nslookup command line utility and online tool

### **Task to be Completed:**

- A detailed report documenting the steps taken and the information gathered for each tool (Recon-ng, Maltego, OSINT Framework).
- Screenshots of the tools in use and the results obtained.
- Analysis of the collected data, including potential vulnerabilities and loopholes identified.
- Recommendations for improving the security of the target based on the findings.

**Scope:** The scope of this project is to perform a comprehensive footprinting and information gathering exercise on a specified target. For this testing we would be doing passive footprinting where we would be finding sensitive details regarding the target site for eg; ip, domain, subdomain, etc.

**Limitation:** This will be a basic level testing where no such techniques would be in use which might disrupt the service or accessibility. We would not do any active scanning of their resources, 1<sup>st</sup> level scanning. As I had already used recon-ng, and maltego in previous assignment, for this

**Tools to be used:**

- OSINT Framework
- Nslookup
- Whois

**Target:** certifiedhacker.com

**Activity:** Footprinting

## Findings:-

**Domain Enumeration using Whois records:** WHOIS records provide information about the ownership and administrative details of a domain name, IP address, or Autonomous System Number (ASN). These records are managed by registrars and registries in compliance with ICANN regulations.

First, we will check whether the target is active or not by pinging. Hop on to command line and enter below command, if we receive a response then the site is up and active.

```
$ ping certifiedhacker.com
PING certifiedhacker.com (162.241.216.11) 56(84) bytes of data.
64 bytes from box5331.bluehost.com (162.241.216.11): icmp_seq=1 ttl=128
64 bytes from box5331.bluehost.com (162.241.216.11): icmp_seq=2 ttl=128
```

We can understand that host is **bluehost**, target IP is **162.241.216.11** and by the ttl we understand that OS is **Windows**.

In command line, enter the following command `$whois <target>`. We got loads of information from domain name, to registrar details.

```
(kali㉿kali)-[~]
$ whois certifiedhacker.com
Domain Name: CERTIFIEDHACKER.COM
Registry Domain ID: 88849376_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.networksolutions.com
Registrar URL: http://networksolutions.com
Updated Date: 2024-05-30T06:32:29Z
Creation Date: 2002-07-30T00:32:00Z
Registry Expiry Date: 2025-07-30T00:32:00Z
Registrar: Network Solutions, LLC
Registrar IANA ID: 2
Registrar Abuse Contact Email: domain.operations@web.com
Registrar Abuse Contact Phone: +1.8777228662
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Name Server: NS1.BLUEHOST.COM
Name Server: NS2.BLUEHOST.COM
DNSSEC: unsigned
URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
>>> Last update of whois database: 2025-01-22T12:26:02Z <<<

Domain Name: CERTIFIEDHACKER.COM
Registry Domain ID: 88849376_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.networksolutions.com
Registrar URL: http://networksolutions.com
Updated Date: 2024-08-22T07:51:37Z
Creation Date: 2002-07-30T00:32:00Z
Registrar Registration Expiration Date: 2025-07-30T00:32:00Z
Registrar: Network Solutions, LLC
Registrar IANA ID: 2
Reseller:
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
```

```

Registry Registrant ID:
Registrant Name: PERFECT PRIVACY, LLC
Registrant Organization:
Registrant Street: 5335 Gate Parkway care of Network Solutions PO Box 459
Registrant City: Jacksonville
Registrant State/Province: FL
Registrant Postal Code: 32256
Registrant Country: US
Registrant Phone: +1.5707088622
Registrant Phone Ext:
Registrant Fax:
Registrant Fax Ext:
Registrant Email: kq9t994x73e@networksolutionsprivateregistration.com
Registry Admin ID:
Admin Name: PERFECT PRIVACY, LLC
Admin Organization:
Admin Street: 5335 Gate Parkway care of Network Solutions PO Box 459
Admin City: Jacksonville
Admin State/Province: FL
Admin Postal Code: 32256
Admin Country: US
Admin Phone: +1.5707088622
Admin Phone Ext:
Admin Fax:
Admin Fax Ext:
Admin Email: kq9t994x73e@networksolutionsprivateregistration.com
Registry Tech ID:
Tech Name: PERFECT PRIVACY, LLC
Tech Organization:
Tech Street: 5335 Gate Parkway care of Network Solutions PO Box 459
Tech City: Jacksonville
Tech State/Province: FL
Tech Postal Code: 32256
Tech Country: US
Tech Phone: +1.5707088622

```

Registrar Abuse Contact Email: domain.operations@web.com

Registrar Abuse Contact Phone: +1.8777228662

URL of the ICANN WHOIS Data Problem Reporting System: <http://wdprs.internic.net/>

>>> Last update of WHOIS database: 2025-01-22T12:26:18Z <<<

To summarize, list of important data was found are as follows:

- Domain name
- Registrar details(owner name, contact details, emails, location)
- Server name
- Time of update.

**Positives:** By observing the creation and updation time, we can appreciate the owner for regularly keeping the site up to date.

**NSLookup:-** The nslookup command is used to query Internet domain name servers (DNS) and obtain information that maps domain names to IP addresses, as well as other DNS records. In short when we enter domain name, we receive IP address and server address.

```

(kali@kali)-[~]
$ nslookup certifiedhacker.com
Server:      10.10.1.2
Address:     10.10.1.2#53

Non-authoritative answer:
Name:   certifiedhacker.com
Address: 162.241.216.11

```

10.10.1.2 is the IP address, and 53 refers to the port number. In my case, 53 is the standard port for DNS (Domain Name System) queries.



**APNIC** : - Asia-Pacific Network Information Centre allocates and manages IP address ranges for the Asia-Pacific region.

- Knowing the CIDR range allows you to perform detailed network scans, identifying all active devices and services within a given range.
- By focusing on a specific IP range, you can conduct more controlled and precise penetration tests, reducing the risk of impacting unrelated systems.

Enter APNIC on to browsers search bar, click on advanced whois which will redirect to the page. Entering the IP address in search bar gives us CIDR /IP ranges assigned for this particular website.

## APNIC Whois Search

To assist you with debugging problems, this whois query was received from IP Address:

**2401:4900:882e:33:3762:9f6f:be0d:1695**

Search for  e.g. 203.119.42.0/24

SearchReset

**NetRange:** 162.240.0.0 - 162.241.255.255

**CIDR:** 162.240.0.0/15

**NetName:** UNIFIEDLAYER-NETWORK-16

**NetHandle:** NET-162-240-0-0-1

**Parent:** NET162 (NET-162-0-0-0-0)

**NetType:** Direct Allocation

**OriginAS:** AS46606

**Organization:** Unified Layer (BLUEH-2)

**RegDate:** 2013-08-22

**Updated:** 2013-08-22

**Ref:** <https://rdap.arin.net/registry/ip/162.240.0.0>

Using APNIC, I found out net ranges and CIDR which will increase efficiency in further investigation. We received a positive results from this as we received what was expected.

## Website footprinting:-

**Photon:** - Photon is an open-source, lightweight, and versatile tool designed for OSINT (Open-Source Intelligence) tasks. This tool proved instrumental in identifying web-based vulnerabilities and gathering actionable data for further analysis.

Photon can extract the following data while crawling:

- URLs (in-scope & out-of-scope)
- URLs with parameters (example.com/gallery.php?id=2)
- Intel (emails, social media accounts, amazon buckets etc.)
- Files (pdf, png, xml etc.)
- Secret keys (auth/API keys & hashes)
- JavaScript files & Endpoints present in them
- Strings matching custom regex pattern
- Subdomains & DNS related data.

Enter the below command in the command line, as the tool is based on python, we run the tool starting with python3 followed by python script to run the tool followed by the option to run on the target.

```
(kali@kali)-[~/Photon]
$ python3 photon.py -u http://www.certifiedhacker.com
/home/kali/Photon/photon.py:18: SyntaxWarning: invalid escape sequence '\/'
print('%s' %
```



```
Level 1: 1 URLs
[!] Progress: 1/1
Level 2: 2 URLs
[!] Progress: 2/2
Crawling 0 JavaScript files
```

---

```
[+] Internal: 3
[+] External: 2
```

---

```
[!] Total requests made: 4
[!] Total time taken: 0 minutes 4 seconds
[!] Requests per second: 0
[+] Results saved in www.certifiedhacker.com directory
```

```
(kali@kali)-[~/Photon/www.certifiedhacker.com]
$ cat internal.txt
http://www.certifiedhacker.com
http://www.certifiedhacker.com/sample-login.html
http://www.certifiedhacker.com/
```

```
(kali@kali)-[~/Photon/www.certifiedhacker.com]
$ cat external.txt
http://certifiedhacker.com/Under
http://certifiedhacker.com/
```

```

(kali@kali)-[~/Photon]
$ cat www.certifiedhacker.com/exported.json
{
  "files": [],
  "intel": [],
  "robots": [],
  "custom": [],
  "failed": [],
  "internal": [
    "http://www.certifiedhacker.com",
    "http://www.certifiedhacker.com/sample-login.html",
    "http://www.certifiedhacker.com/"
  ],
  "scripts": [],
  "external": [
    "http://certifiedhacker.com/Under",
    "http://certifiedhacker.com/"
  ],
  "fuzzable": [],
  "endpoints": [],
  "keys": []
}

```

From the investigation we could not find much sensitive data as expected but, some **URL** have been extracted which might be usefull. Upon further testing, those links don't hold any significance as it shows 404 error while accessing the link. Overall this test got us a negative result.

**Dnsrecon**: - It's a Python script that performs various DNS enumerations including standard records, zone transfers, and reverse lookups. Helps us in bruteforcing to get A AAAA records.

```

$ dnsrecon -d certifiedhacker.com
[*] std: Performing General Enumeration against: certifiedhacker.com ...
[-] DNSSEC is not configured for certifiedhacker.com
[*] SOA ns1.bluehost.com 162.159.24.80
[*] NS ns2.bluehost.com 162.159.25.175
[*] NS ns1.bluehost.com 162.159.24.80
[*] MX mail.certifiedhacker.com 162.241.216.11
[*] A certifiedhacker.com 162.241.216.11
[*] TXT certifiedhacker.com v=spf1 a mx ptr include:bluehost.com ?all
[*] Enumerating SRV Records
[+] SRV _autodiscover._tcp.certifiedhacker.com autodiscover.bluehost.com 52.98.86.168 443
[+] SRV _autodiscover._tcp.certifiedhacker.com autodiscover.bluehost.com 40.99.60.232 443
[+] SRV _autodiscover._tcp.certifiedhacker.com autodiscover.bluehost.com 40.99.34.216 443
[+] SRV _autodiscover._tcp.certifiedhacker.com autodiscover.bluehost.com 40.99.34.232 443
[+] SRV _autodiscover._tcp.certifiedhacker.com autodiscover.bluehost.com 2603:1046:c06:8a0::8 443
[+] SRV _autodiscover._tcp.certifiedhacker.com autodiscover.bluehost.com 2603:1046:700:70::8 443
[+] SRV _autodiscover._tcp.certifiedhacker.com autodiscover.bluehost.com 2603:1046:c06:8ce::8 443
[+] SRV _autodiscover._tcp.certifiedhacker.com autodiscover.bluehost.com 2603:1046:c06:895::8 443
[+] 8 Records Found

```

SRV (Service) records in DNS are used to specify the location of servers for specific services.

Important records received after investigation: -

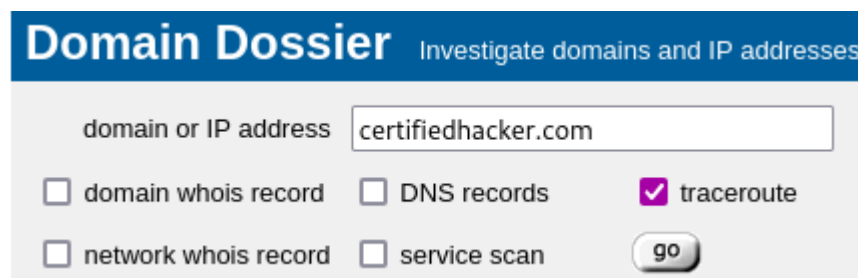
- Mail server (MX) - Containing the info where the domain's email should be routed to and mail servers priority.
- Name Server (NS)- Containing information about the authoritative nameservers of a domain
- A (IPv4) - Containing the IPv4 address info of the hostname.
- TXT - is commonly used for other DNS records configurations like SPF, DKIM, or DMARC records.
- SOA - Start of authority is responsible for holding and specifying information about the DNS zone.

## Network Foot printing: -

**Domain Dossier:** - It is a OSINT tool is an all-inclusive resource for gathering detailed information about a domain<sup>2</sup>. This tool can check a domain's availability, retrieve historical WHOIS data, monitor DNS records, IP addresses, and reveal its ownership.

We will find out the traceroute of the target. Reason for finding out the trace rout:-

- **Path Discovery:** It reveals the path packets take to reach a destination, showing each intermediate device (router) en route.
- **Latency Measurement:** Measures the time taken for packets to travel to each hop, identifying delays within the network



### Traceroute

Tracing route to [certifiedhacker.com](#) [162.241.216.11]...

hop	rtt	rtt	rtt	ip address	fully qualified domain name
1	2	1	1	169.254.158.58	
2	1	1	1	169.48.118.156	ae103.ppr01.dal13.networklayer.com
3	1	0	0	169.48.118.136	88.76.30a9.ip4.static.sl-reverse.com
4	*	8	3	169.45.18.38	ae17.cbs01.dr01.dal04.networklayer.com
5	2	2	2	169.45.18.97	61.12.2da9.ip4.static.sl-reverse.com
6	2	2	2	213.248.101.8	dls-b24-link.ip.twelve99.net
7	2	2	2	62.115.139.130	dls-bb2-link.ip.twelve99.net
8	*	*	*		
9	19	19	19	62.115.137.114	den-bb2-link.ip.twelve99.net
10	28	28	28	62.115.132.207	salt-b4-link.ip.twelve99.net
11	29	29	29	62.115.136.107	salt-b5-link.ip.twelve99.net
12	43	41	41	80.239.167.103	newfolddigital-ic-380138.ip.twelve99-cust.net
13	41	41	41	69.195.64.103	69-195-64-103.unifiedlayer.com
14	40	41	41	162.144.240.131	po97.prv-leaf1b.net.unifiedlayer.com
15	41	41	41	162.241.216.11	box5331.bluehost.com

Trace complete

We found out that it take 15 hops to actually reach the destination. It is taking a long route in return costing us more time to reach the target. We received a positive result on our investigation.



**Geo Locaton of IP:** - Finding the geo location is an important step in a footprinting documentation. It tells lot about where target is been stored and hosted. One effective method is through geolocation of an IP address using tools like **Netcraft**.

**Netcraft:** - This tool is same as whois record which offers an IP lookup service where you can enter an IP address. This will provide detailed information about the IP, including geographic location. For this investigation we would focus on this geo location.

#### IP Geolocation

We use multilateration to independently determine the location of a server. [Read more.](#)



We can conclude that the Site is been hosted in Unite States of America. Blue marking also confirms the co-ordinates we received while using whois tool are accurate.

**Conclusion:** - I hereby conclude by findings of my investigation by listing it below: -

- Domain registrar details including contact number, email, name, server/host, location including pin code.
- CIDR and IP range.
- Sensitive URL's
- Standard records such as SOA, MX, A, etc.
- Network route
- Exact Geo location

-----END-----