

Ethical Hacking

(Muhammad Adnan)

Topics:

- Email and Domain information Gathering
 - Metadata Analysis
- WHOIS Data and Domain Ownership
 - DNS Enumeration
- Enumeration of Network Services
- Hands-on Practices with an Information Gathering

Email & Domain Information Gathering

Tools & Techniques:

1. WHOIS Lookup:

Example:

```
adnan@kali: ~  
File Actions Edit View Help  
$ whois hackersmarket.net  
Domain Name: HACKERSMARKET.NET  
Registry Domain ID: 2893430855_DOMAIN_NET-VRSN  
Registrar WHOIS Server: whois.namecheap.com  
Registrar URL: http://www.namecheap.com  
Updated Date: 2024-06-24T07:53:41Z  
Creation Date: 2024-06-24T07:52:19Z  
Registry Expiry Date: 2025-06-24T07:52:19Z  
Registrar: NameCheap, Inc.  
Registrar IANA ID: 1068  
Registrar Abuse Contact Email: abuse@namecheap.com  
Registrar Abuse Contact Phone: +1.6613102107  
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited  
Name Server: HARVEY.NS.CLOUDFLARE.COM  
Name Server: STELLA.NS.CLOUDFLARE.COM  
DNSSEC: unsigned  
URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/  
>>> Last update of whois database: 2024-07-26T07:42:01Z <<<  
  
NOTICE: The expiration date displayed in this record is the date the  
registrar's sponsorship of the domain name registration in the registry is  
currently set to expire. This date does not necessarily reflect the expiration  
date of the domain name registrant's agreement with the sponsoring  
registrar. Users may consult the sponsoring registrar's Whois database to  
view the registrar's reported date of expiration for this registration.  
  
TERMS OF USE: You are not authorized to access or query our Whois  
database through the use of electronic processes that are high-volume and  
automated except as reasonably necessary to register domain names or  
modify existing registrations; the Data in VeriSign Global Registry  
Services' ("VeriSign") Whois database is provided by VeriSign for  
information purposes only, and to assist persons in obtaining information  
about or related to a domain name registration record. VeriSign does not  
guarantee its accuracy. By submitting a Whois query, you agree to abide  
by the following terms of use: You agree that you may use this Data only  
for lawful purposes and that under no circumstances will you use this Data  
to: (1) allow, enable, or otherwise support the transmission of mass  
unsolicited, commercial advertising or solicitations via e-mail, telephone,  
or facsimile; or (2) enable high volume, automated, electronic processes  
that apply to VeriSign (or its computer systems). The compilation,  
repackaging, dissemination or other use of this Data is expressly  
prohibited without the prior written consent of VeriSign. You agree not to  
use electronic processes that are automated and high-volume to access or  
query the Whois database except as reasonably necessary to register
```

2. DNS Record:

Example:

```
(adnan@kali)-[~]
$ dig hackersmarket.net

; <<>> DiG 9.19.25-185-g392e7199df2-1-Debian <<>> hackersmarket.net
;; global options: +cmd
;; Got answer:
;; ->HEADER<- opcode: QUERY, status: NOERROR, id: 47885
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags:; udp: 1220
;; COOKIE: 4131e504a3339d8f0056cc9566a354934bb164f0710e5f15 (good)
;; QUESTION SECTION:
;hackersmarket.net.                IN      A

;; ANSWER SECTION:
hackersmarket.net.      300     IN      A      172.67.205.69
hackersmarket.net.      300     IN      A      104.21.44.241

;; Query time: 379 msec
;; SERVER: 192.168.1.1#53(192.168.1.1) (UDP)
;; WHEN: Fri Jul 26 03:47:31 EDT 2024
;; MSG SIZE rcvd: 106
```

3. DNSRECON:

DNSRecon is a powerful command-line tool used for DNS reconnaissance, enumeration, and information gathering.

Example:

```
(adnan@kali)-[~]
$ dnsrecon -d hackersmarket.net
[*] std: Performing General Enumeration against: hackersmarket.net ...
[-] DNSSEC is not configured for hackersmarket.net
[*] SOA harvey.ns.cloudflare.com 108.162.195.152
[*] SOA harvey.ns.cloudflare.com 172.64.35.152
[*] SOA harvey.ns.cloudflare.com 162.159.44.152
[*] SOA harvey.ns.cloudflare.com 2606:4700:58::a29f:2c98
[*] SOA harvey.ns.cloudflare.com 2a06:98c1:50::ac40:2398
[*] SOA harvey.ns.cloudflare.com 2803:f800:50::6ca2:c398
[*] NS harvey.ns.cloudflare.com 108.162.195.152
[*] Bind Version for 108.162.195.152 "2024.7.2"
[*] NS harvey.ns.cloudflare.com 172.64.35.152
[*] Bind Version for 172.64.35.152 "2024.7.2"
[*] NS harvey.ns.cloudflare.com 162.159.44.152
[*] Bind Version for 162.159.44.152 "2024.7.2"
[*] NS harvey.ns.cloudflare.com 2606:4700:58::a29f:2c98
[*] NS harvey.ns.cloudflare.com 2a06:98c1:50::ac40:2398
[*] NS harvey.ns.cloudflare.com 2803:f800:50::6ca2:c398
[*] NS stella.ns.cloudflare.com 172.64.34.154
[*] Bind Version for 172.64.34.154 "2024.7.2"
[*] NS stella.ns.cloudflare.com 108.162.194.154
[*] Bind Version for 108.162.194.154 "2024.7.2"
[*] NS stella.ns.cloudflare.com 162.159.38.154
[*] Bind Version for 162.159.38.154 "2024.7.2"
[*] NS stella.ns.cloudflare.com 2606:4700:50::a29f:269a
[*] NS stella.ns.cloudflare.com 2a06:98c1:50::ac40:229a
[*] NS stella.ns.cloudflare.com 2803:f800:50::6ca2:c29a
[*] A hackersmarket.net 172.67.205.69
[*] A hackersmarket.net 104.21.44.241
[*] AAAA hackersmarket.net 2606:4700:3030::6815:2cf1
[*] AAAA hackersmarket.net 2606:4700:3032::ac43:cd45
[*] Enumerating SRV Records
[-] No SRV Records Found for hackersmarket.net
```

Email Information Gathering

1. theHarvester:

Example:

```
(adnan@kali)-[~]
$ theHarvester -d hackersmarket.net
Read proxies.yaml from /home/adnan/.theHarvester/proxies.yaml
*****
*                               *
*                               *
*                               *
*                               *
*                               *
* theHarvester 4.6.0             *
* Coded by Christian Martorella  *
* Edge-Security Research         *
* cmartorella@edge-security.com  *
*                               *
*****

[*] No IPs found.
[*] No emails found.
[*] No hosts found.
```

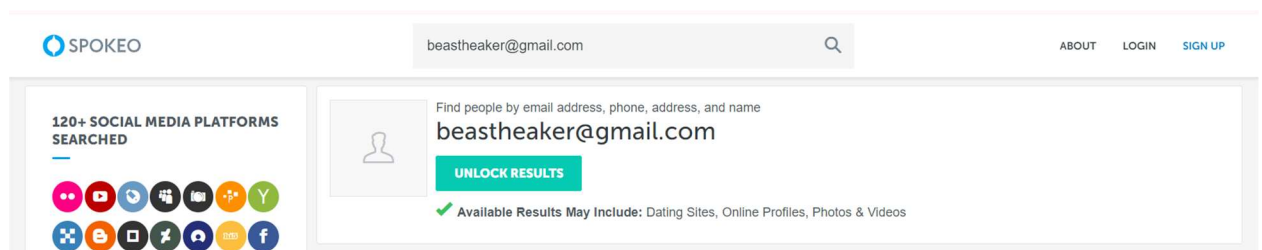
Reverse Email Lookup Tool

Extension:

SEON Chrome Extension.

Website:

Spokeo



DNS Enumeration

1. nslookup:


Example:

```
(adnan@kali)-[~]
$ nslookup -d hackersmarket.net
*** Invalid option: d
Server: 192.168.1.1
Address: 192.168.1.1#53

Non-authoritative answer:
Name: hackersmarket.net
Address: 104.21.44.241
Name: hackersmarket.net
Address: 172.67.205.69
Name: hackersmarket.net
Address: 2606:4700:3030::6815:2cf1
Name: hackersmarket.net
Address: 2606:4700:3032::ac43:cd45
```

Websites

MX toolbox:

SupertoolLogin

SuperTool Beta9

DNS Lookup

a:hackersmarket.net

Find Problems

↻ a

Type	Domain Name	IP Address	TTL
TypeA	Domain Namehackersmarket.net	IP Address172.67.205.69 Cloudflare, Inc. (AS13335)	TTL5 min
TypeA	Domain Namehackersmarket.net	IP Address104.21.44.241 Cloudflare, Inc. (AS13335)	TTL5 min

	Test	Result
Status✔	NameDNS Record Published	ResponseDNS Record found

Your DNS hosting provider is "Cloudflare" [Need Bulk Dns Provider Data?](#)

[dns check](#)

[mx lookup](#)

[dmarc lookup](#)

[spf lookup](#)

[dns propagation](#)

Reported by [stella.ns.cloudflare.com](#) on 7/26/2024 at 3:09:53 AM (UTC -5), [just for you.](#)

Transcript

Virus Total:

URL, IP address, domain or file hash

Sign in

0 / 94

Community Score

No security vendors flagged this URL as malicious

Reanalyze Search Graph API

http://hackersmarket.net/
hackersmarket.net

Status
200

Content type
text/html; charset=UTF-8

Last Analysis Date
18 days ago

text/html

external-resources

multiple-redirects

DETECTION

DETAILS

COMMUNITY

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Security vendors' analysis

Do you want to automate checks?

Bfore.AI PreCrime	Suspicious	Ermes	Not Recommended
Abusix	Clean	Acronis	Clean
ADMINUSLabs	Clean	AILabs (MONITORAPP)	Clean
AlienVault	Clean	alphaMountain.ai	Clean

Enumeration of Network Services

Network enumeration is the process of identifying devices, systems, and services connected within a specific network. During enumeration, network administrators analyze and enhance network security by retrieving information such as host details, connected devices, usernames, group information, and related data.

Command:

Nmap

```
(adnan@kali)-[~]
$ nmap -d hackersmarket.net
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-26 04:39 EDT
PORTS: Using ports open on 0% or more average hosts (TCP:1000, UDP:0, SCTP:0)

Timing report
hostgroups: min 1, max 100000
rtt-timeouts: init 1000, min 100, max 10000
max-scan-delay: TCP 1000, UDP 1000, SCTP 1000
parallelism: min 0, max 0
max-retries: 10, host-timeout: 0
min-rate: 0, max-rate: 0

Initiating Ping Scan at 04:39
Scanning hackersmarket.net (172.67.205.69) [2 ports]
Completed Ping Scan at 04:39, 0.14s elapsed (1 total hosts)
Overall sending rates: 14.23 packets / s.
mass_rdns: Using DNS server 192.168.1.1
Initiating Parallel DNS resolution of 1 host. at 04:39
mass_rdns: 0.28s 0/1 [#: 1, OK: 0, NX: 0, DR: 0, SF: 0, TR: 1]
Completed Parallel DNS resolution of 1 host. at 04:39, 0.28s elapsed
DNS resolution of 1 IPs took 0.28s. Mode: Async [#: 1, OK: 0, NX: 1, DR: 0, SF: 0, TR: 1, CN: 0]
Initiating Connect Scan at 04:39
Scanning hackersmarket.net (172.67.205.69) [1000 ports]
Discovered open port 8080/tcp on 172.67.205.69
Discovered open port 80/tcp on 172.67.205.69
Discovered open port 443/tcp on 172.67.205.69
Discovered open port 8443/tcp on 172.67.205.69
Completed Connect Scan at 04:39, 13.76s elapsed (1000 total ports)
Overall sending rates: 145.60 packets / s.
Nmap scan report for hackersmarket.net (172.67.205.69)
Host is up, received syn-ack (0.16s latency).
Other addresses for hackersmarket.net (not scanned): 104.21.44.241 2606:4700:3030::6815:2cf1 2606:4700:3032::ac43
Scanned at 2024-07-26 04:39:26 EDT for 14s
Not shown: 996 filtered tcp ports (no-response)
PORT      STATE SERVICE      REASON
80/tcp    open  http         syn-ack
443/tcp   open  https        syn-ack
8080/tcp   open  http-proxy   syn-ack
8443/tcp   open  https-alt    syn-ack
Final times for host: srth: 158246 rttvar: 46150 to: 342846

Read from /usr/bin/./share/nmap: nmap-protocols nmap-services.
Nmap done: 1 IP address (1 host up) scanned in 14.64 seconds
(adnan@kali)-[~]
```