

ETHICAL HACKING

Topics

Email & Domain information Gathering

--> **Metadata Analysis**

WHOIS Data & Domain Ownership

--> **DNS Enumeration**

Enumeration of network Services

Hands-on Practise with an information Gathering

Email & Domain information Gathering

Email and Domain Information Gathering is the process of collecting, organizing and analyzing data and intelligence about email addresses, domains, to identify vulnerabilities that can be used for research, threat analysis, strategic planning, or exploited for offensive or defensive operations.

Example

WHOIS Lookup

```
kali@kali: ~  
File Actions Edit View Help  
(kali@kali)-[~]  
$ whois aumc.edu.pk  
# WHOIS .PK Domains (PKNIC)  
  
Domain: aumc.edu.pk  
Status: Domain is Registered  
  
Creation Date: 2013-06-11  
Expiry Date: 2025-06-11  
Name Server: ns1.stackdns.com  
Name Server: ns2.stackdns.com  
Name Server: ns3.stackdns.com  
Name Server: ns4.stackdns.com
```

Example

DNS Records

dig

```
kali@kali: ~  
File Actions Edit View Help  
  
(kali@kali)-[~]  
$ dig aumc.edu.pk  
  
; <<>> DiG 9.19.19-1-Debian <<>> aumc.edu.pk  
;; global options: +cmd  
;; Got answer:  
;; ->HEADER<- opcode: QUERY, status: NOERROR, id: 16582  
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1  
  
;; OPT PSEUDOSECTION:  
; EDNS: version: 0, flags:; udp: 512  
;; QUESTION SECTION:  
;aumc.edu.pk.                IN      A  
  
;; ANSWER SECTION:  
aumc.edu.pk.                 3600    IN      A      185.151.30.193  
  
;; Query time: 176 msec  
;; SERVER: 192.168.100.1#53(192.168.100.1) (UDP)  
;; WHEN: Fri Jul 26 05:08:06 UTC 2024  
;; MSG SIZE  rcvd: 56
```

Example

dnsrecon

```
kali@kali: ~  
File Actions Edit View Help  
(kali@kali)-[~]  
$ dnsrecon -d aumc.edu.pk  
[*] std: Performing General Enumeration against: aumc.edu.pk ...  
[-] DNSSEC is not configured for aumc.edu.pk  
[-] Exception "The DNS operation timed out." while resolving SOA record.  
[-] Error while resolving SOA while using 192.168.100.1 as nameserver.  
[*] NS ns4.stackdns.com 104.196.137.209  
[-] Recursion enabled on NS Server 104.196.137.209  
[*] NS ns2.stackdns.com 146.148.28.88  
[-] Recursion enabled on NS Server 146.148.28.88  
[*] NS ns3.stackdns.com 35.198.79.191  
[*] NS ns1.stackdns.com 35.197.225.59  
[-] Recursion enabled on NS Server 35.197.225.59  
[*] MX ASPMX.L.GOOGLE.COM 66.102.1.26  
[*] MX ALT3.ASPMX.L.GOOGLE.COM 142.250.150.27  
[*] MX ALT1.ASPMX.L.GOOGLE.COM 142.250.153.27  
[*] MX ALT4.ASPMX.L.GOOGLE.COM 74.125.200.27  
[*] MX ALT2.ASPMX.L.GOOGLE.COM 142.251.9.27  
[*] MX ALT3.ASPMX.L.GOOGLE.COM 2a00:1450:4010:c1c::1a  
[*] MX ALT1.ASPMX.L.GOOGLE.COM 2a00:1450:4013:c16::1a  
[*] MX ALT2.ASPMX.L.GOOGLE.COM 2a00:1450:4025:c03::1a  
[*] A aumc.edu.pk 185.151.30.193  
[*] AAAA aumc.edu.pk 2a07:7800::193  
[*] TXT aumc.edu.pk v=spf1 include:_spf.google.com include:spf.stackmail.com -all  
[*] Enumerating SRV Records  
[-] No SRV Records Found for aumc.edu.pk
```

Email information Gathering

Email and Domain Information Gathering is the process of collecting, organizing and analyzing data and intelligence about email addresses, domains, to identify vulnerabilities that can be used for research, threat analysis, strategic planning, or exploited for offensive and/or defensive operations.


Example

the harvester

```
kali@kali: ~  
File Actions Edit View Help  
(kali@kali)-[~]  
$ theHarvester -d aumc.edu.pk  
Read proxies.yaml from /home/kali/.theHarvester/proxies.yaml4  
*****  
* theHarvester 4.5.1 *  
* Coded by Christian Martorella *  
* Edge-Security Research *  
* cmartorella@edge-security.com *  
* *  
*****  
[*] No IPs found.  
[*] No emails found.  
[*] No hosts found.
```



Reverse email lookup


pipl
spokeo

 SPOKEO

fatiqm072@gmail.com

120+ SOCIAL MEDIA PLATFORMS
SEARCHED





Find people by email address, phone
fatiqm072@gmail.
[UNLOCK RESULTS](#)
✓ Available Results May Include:

Reverse email lookup

Example

SEON chrome extension

COCO finder

Meta Data Analysis

Metadata is used to provide additional context about files and other data stored on a computer or network. This can be useful for cyber forensics cases because it provides information that may not be immediately clear from the file itself, such as when and how it was modified or accessed by an attacker.

Example

Exiftool

Foca

Maltego

```
kali@kali: ~/Downloads
File Actions Edit View Help
$ exiftool ocint.jpeg
ExifTool Version Number      : 12.76
File Name                    : ocint.jpeg
Directory                   : .
File Size                    : 14 kB
File Modification Date/Time  : 2024:07:26 05:50:06+00:00
File Access Date/Time       : 2024:07:26 05:50:06+00:00
File Inode Change Date/Time  : 2024:07:26 05:50:06+00:00
File Permissions             : -rw-r--r--
File Type                    : JPEG
File Type Extension         : jpg
MIME Type                    : image/jpeg
JFIF Version                 : 1.01
Resolution Unit              : None
X Resolution                 : 1
Y Resolution                 : 1
Image Width                  : 259
Image Height                 : 194
Encoding Process             : Baseline DCT, Huffman coding
Bits Per Sample              : 8
Color Components             : 3
Y Cb Cr Sub Sampling         : YCbCr4:2:0 (2 2)
Image Size                   : 259x194
Megapixels                   : 0.050
```

Example

Website :
GetMetadata

METADATA2GO.com		All tools ▾	
Files	Tools	File List	ocint.json
file_name	ocint.jpeg		
file_size	14 kB		
file_type	JPEG		
file_type_extension	jpg		
mime_type	image/jpeg		
jfif_version	1.01		
resolution_unit	None		
x_resolution	1		
y_resolution	1		
image width	259		

Example

binwalk

Command: binwalk.....

DNS Enumeration

DNS enumeration is a critical process in cybersecurity that uncovers all DNS records associated with a domain, providing valuable insights for security professionals and cybercriminals alike. By detailing hostnames, IP addresses, and DNS record types, it reveals a domain's footprint and potential vulnerabilities.

Example

dig

```
kali@kali: ~  
File Actions Edit View Help  
  
(kali@kali)-[~]  
$ dig aumc.edu.pk  
  
; <<>> DiG 9.19.19-1-Debian <<>> aumc.edu.pk  
;; global options: +cmd  
;; Got answer:  
;; ->HEADER<- opcode: QUERY, status: NOERROR, id: 16582  
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1  
  
;; OPT PSEUDOSECTION:  
; EDNS: version: 0, flags:; udp: 512  
;; QUESTION SECTION:  
;aumc.edu.pk.                IN      A  
  
;; ANSWER SECTION:  
aumc.edu.pk.                 3600    IN      A      185.151.30.193  
  
;; Query time: 176 msec  
;; SERVER: 192.168.100.1#53(192.168.100.1) (UDP)  
;; WHEN: Fri Jul 26 05:08:06 UTC 2024  
;; MSG SIZE  rcvd: 56
```

nslookup

```
(kali@kali)-[~]  
$ nslookup -d aumc.edu.pk  
*** Invalid option: d  
Server:                192.168.104.129  
Address:               192.168.104.129#53  
  
Non-authoritative answer:  
Name: aumc.edu.pk  
Address: 185.151.30.193  
Name: aumc.edu.pk  
Address: 2a07:7800::193
```


Example

Website:
MX toolbox

mx:aumc.edu.pk

Find Problems

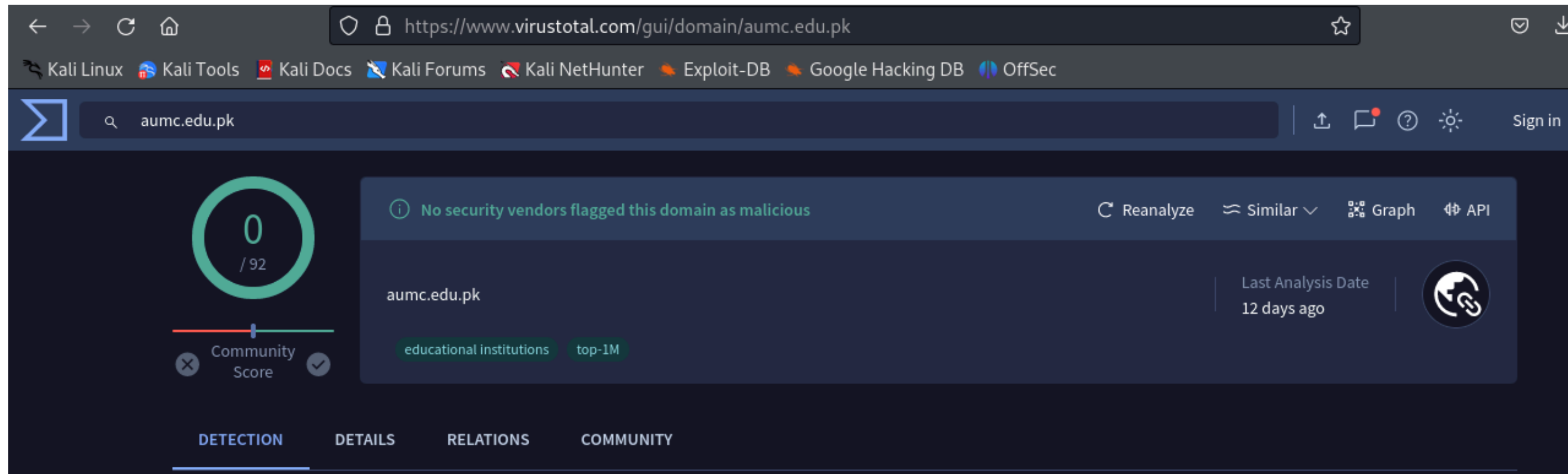
Solve Email Delivery Problems

Gmail & Yahoo are now requiring DMARC - Get your's setup with Delivery Center

Pref	Hostname	IP Address	TTL		
1	ASPMX.L.GOOGLE.COM	172.253.63.27 Google LLC (AS15169)	60 min	Blacklist Check	SMTP Test
1	ASPMX.L.GOOGLE.COM	2607:f8b0:4004:c09::1b	60 min	Blacklist Check	
5	ALT1.ASPMX.L.GOOGLE.COM	209.85.202.27 Google LLC (AS15169)	60 min	Blacklist Check	SMTP Test
5	ALT1.ASPMX.L.GOOGLE.COM	2a00:1450:400b:c00::1b	60 min	Blacklist Check	
5	ALT2.ASPMX.L.GOOGLE.COM	64.233.184.26 Google LLC (AS15169)	60 min	Blacklist Check	SMTP Test
5	ALT2.ASPMX.L.GOOGLE.COM	2a00:1450:400c:c0b::1b	60 min	Blacklist Check	
10	ALT3.ASPMX.L.GOOGLE.COM	142.250.27.27 Google LLC (AS15169)	60 min	Blacklist Check	SMTP Test
10	ALT3.ASPMX.L.GOOGLE.COM	2a00:1450:4025:401::1a	60 min	Blacklist Check	
10	ALT4.ASPMX.L.GOOGLE.COM	142.250.153.26 Google LLC (AS15169)	60 min	Blacklist Check	SMTP Test
10	ALT4.ASPMX.L.GOOGLE.COM	2a00:1450:4013:c16::1a	60 min	Blacklist Check	

Example

Website:
Virus Total



Example

Gobuster

Enumeration of Network Services

Enumeration of network services is a common technique hackers use to discover open doors or weak points in a network. A port scan attack helps cyber criminals find open ports and figure out whether they are receiving or sending data. It can also reveal whether active security devices like firewalls are being used by an organization.

Example

Command :
Nmap

```
kali@kali: ~  
File Actions Edit View Help  
(kali@kali)-[~]  
$ nmap -d aumc.edu.pk  
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-26 06:22 UTC  
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 06:22  
Scanning aumc.edu.pk (185.151.30.193) [2 ports]  
Completed Ping Scan at 06:22, 0.30s elapsed (1 total hosts)  
Overall sending rates: 6.62 packets / s.  
mass_rdns: Using DNS server 192.168.104.129  
Initiating Parallel DNS resolution of 1 host. at 06:22  
mass_rdns: 0.20s 0/1 [#: 1, OK: 0, NX: 0, DR: 0, SF: 0, TR: 1]  
Completed Parallel DNS resolution of 1 host. at 06:22, 0.20s elapsed  
DNS resolution of 1 IPs took 0.20s. Mode: Async [#: 1, OK: 1, NX: 0, DR: 0, S  
F: 0, TR: 1, CN: 0]  
Initiating Connect Scan at 06:22  
Scanning aumc.edu.pk (185.151.30.193) [1000 ports]  
Discovered open port 443/tcp on 185.151.30.193  
Discovered open port 80/tcp on 185.151.30.193  
Discovered open port 53/tcp on 185.151.30.193
```

Example

Command:
Nmap
Masscan

Example

Command :
netstat

```
kali@kali: ~/Downloads
File Actions Edit View Help
net tdb          Show information from tdb records
net vfs          Filesystem operation through the VFS stack
net help         Print usage information

(kali@kali)-[~/Downloads]
$ netstat
Active Internet connections (w/o servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 192.168.104.135:33920    mct01s20-in-f3.1e1:http TIME_WAIT
tcp        0      0 192.168.104.135:44608    mct01s20-in-f6.1e:https TIME_WAIT
tcp        0      0 192.168.104.135:36388    204.79.197.237:https    ESTABLISH
tcp        0      0 192.168.104.135:38672    ec2-34-252-144-17:https TIME_WAIT
tcp        0      0 192.168.104.135:60678    ec2-54-84-92-154.:https TIME_WAIT
tcp        0      0 192.168.104.135:53684    mct04s04-in-f2.1e:https TIME_WAIT
tcp        0      0 192.168.104.135:39080    mct04s01-in-f3.1e:https TIME_WAIT
```


The background of the image is a low-angle, upward-looking shot of a modern skyscraper. The building's facade is composed of a grid of windows and structural elements, creating a strong geometric pattern. The lighting is very dark, with the building appearing almost entirely black against a slightly lighter, cloudy sky. The overall mood is dramatic and professional.

THANK YOU