CERTIFIED ETHICAL HACKING

## ATIQ-UR-REHMAN

### CORVIT SYSTEM MULTAN

**TOPICS:**

# Email and Domain Information Gathering

# - Metadata Analysis

# WHOIS Data and Domain Ownership

# - DNS Enumeration

# Enumeration of Network Services

# Hands-on Practice with an Information Gathering

DATE:27-06-2024

\*Email and Domain Information Gathering:

**“Information gathering** is a process of collecting essential information about the target domain and network . Information can be of various types, like subdomain of target domain ,DNS information ,port information ,server location ,security confrigration ,etc”

 **WHOIS Lookup**: Conduct a WHOIS lookup to gather details about the domain owner, registrar, creation date, and contact information. This provides foundational data about the domain's registration history and ownership.

 **Email Headers Analysis**: Analyze email headers to trace the path of an email message, revealing IP addresses, servers involved in transmission, and sometimes details about the sender's location or system used. This helps in verifying the authenticity of emails and identifying potential threats.

 **Reverse DNS Lookup**: Perform a reverse DNS lookup to find the domain associated with a given IP address. This can be useful for understanding the infrastructure behind a website or email server, verifying sender authenticity, and detecting malicious activity.

# WHOIS LOOKUP:

### TOOLS:

Commands: whois example.com

Whois -I example.com (Is use for see data without filter it)

jwhois example.com (it give additional features than whois command)

# website:

1) https://lookup.icann.org/en/lookup

# DNS RECORD ANALYSIS:

## TOOLS:

COMMANDS: dig example.com

dig -A example.com (for specific record A)

nstlookup -type=TXT example.com

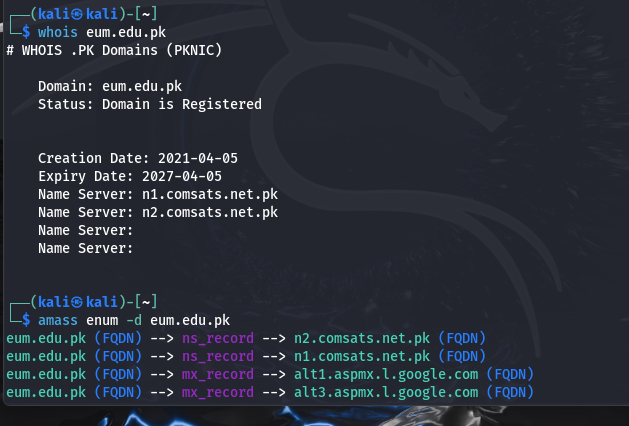
nslookup -type=MX example.com

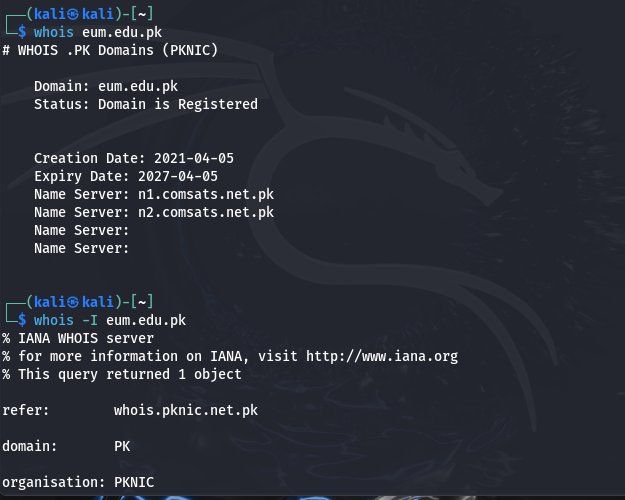
host example.com

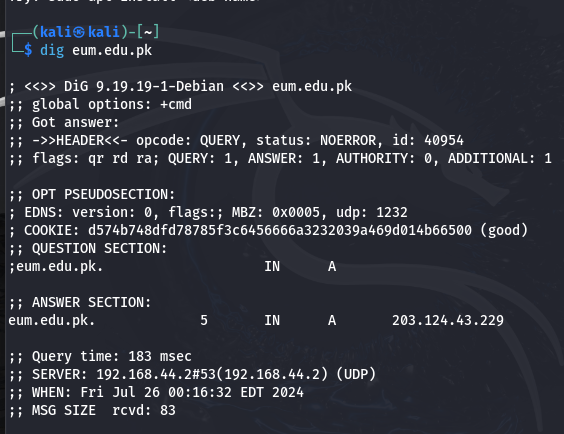
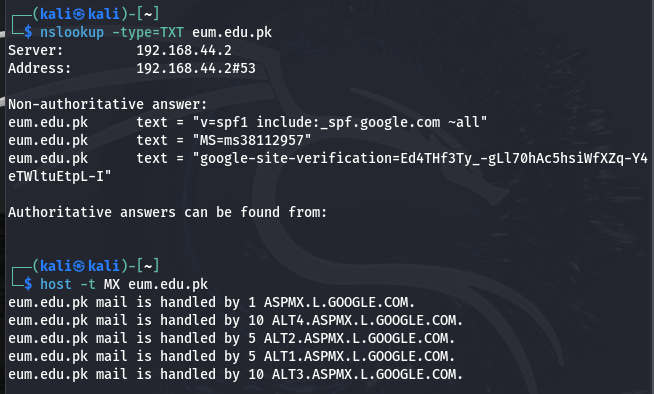
host -t MX example.com

# Website:

1. MXtoolbox







# EMAIL ADDRESS SEARCH:

## TOOLS:

COMMANDS: theHarvester example.com

theHarvester -d example.com -b google

# Website:

1. Hunter.io

# REVERSE EMAIL LOOKUP:

## TOOLS:

COMMANDS: no command

# Website:

1) pipl

2) Spokeo (premium)



# \*METADATA ANALYSIS:

“**Metadata analysis** refers to the process of examining metadata associated with digital files or content to extract meaningful insights, patterns, or information. Metadata provides descriptive or structural data about the content it accompanies, rather than the content itself. This analysis can be applied to various types of digital information, including documents, images, videos, audio files, and more.”

## DOCUMENT METADATA EXTRACTION:

## TOOLS:

COMMANDS: exiftool document.txt

pdfinfo filename.pdf (for .pdf files)

exif filename.jpg (for jpg files)

# IMAGE MATADATA ANALYSIS:

## TOOLS:

COMMANNDS: exiftool imagename

exiv2 imagename

identiy -v imagename

jhead filename.jpg

## WEBSITE:

1. Jeffrey's Image Metadata Viewer

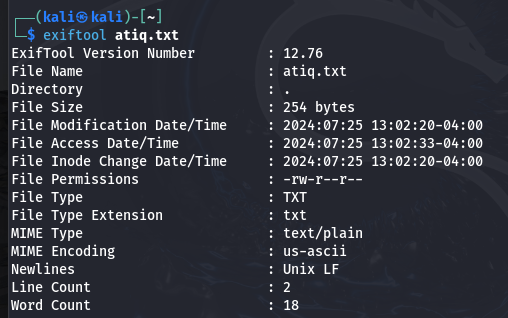
# ONLINE MATADATA ANLYSIS:

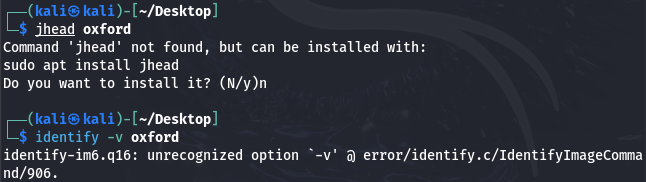
## TOOLS:

COMMANDS: no commands

## WEBSITE:

1. [Get-Metadata](http://get-metadata.com/)
2. Metashield Analyzer





# DNS ENUMIRATION:

DNS enumeration is the process of querying DNS servers to gather information about a domain's DNS records and structure. This typically involves collecting details such as:

* **Hostnames**: Identifying all the subdomains and associated hostnames under a domain.
* **IP Addresses**: Discovering the IP addresses associated with those hostnames.
* **Mail Servers**: Identifying mail exchange (MX) servers responsible for handling emails for the domain.
* **Name Servers**: Finding out which DNS servers are authoritative for the domain.
* **Other Records**: Gathering various other DNS records like TXT records, which can contain additional information such as SPF records for email authentication.

## DNS QUERIES:

## TOOLS:

COMANDS: nslookup example.com

nslookup -type=TXT example.com

dig example.com

dig example.com MX

host example.com

host -t MX example.com

## WEBSITE:

1. MXToolbox

## DNS ENUMIRATION:

## TOOLS:

COMMANDS: fierce -dns example.com

fierce -dns example.com -dnsserver 8.8.8.8 (for scan specific server)

dnsenum example.com

dnsenum --enum --zone-transfer example.com (perform zone transfer)

dnsrecon -d example.com

dnsrecon -d example.com -a (for zone transfer)

sublist3r -d example.com

## SUBDOMAIN ENUMIRATION:

## TOOLS:

COMMANDS: sublist3r -d example.com

sublist3r -d example.com -t 50 (for specific threat)

amass enum -d example.com

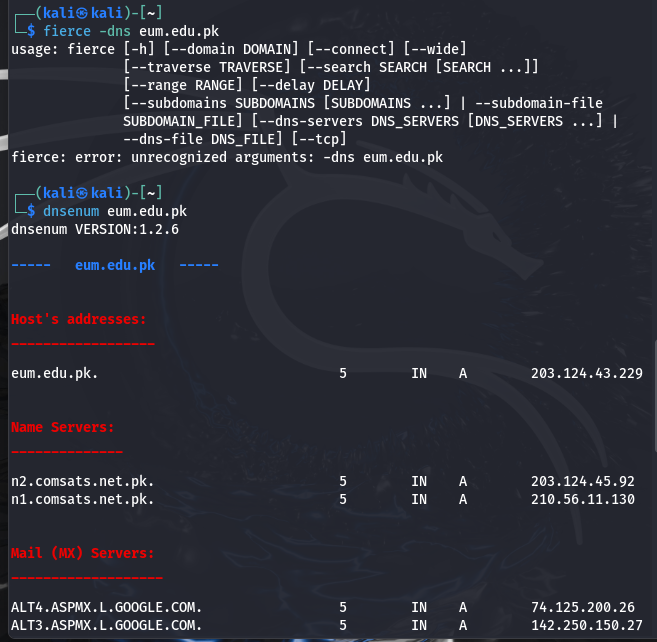
amass enum -d example.com -passive ( for passive enumeration)

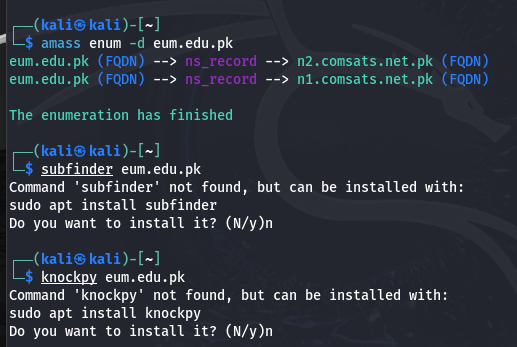
subfinder -d example.com

knockpy example.com

## WEBSITE:

1. [VirusTotal](https://www.virustotal.com/) (for discovering subdomains via DNS records)







# ENUMERATION OF NETWORK SERVICES:

“The enumeration of network services refers to the systematic process of identifying and gathering detailed information about the services and applications running on networked devices. This process typically involves discovering which network services are available, their configurations, and their associated versions. This information is crucial for network administrators to manage and secure their networks effectively and for security professionals to identify potential vulnerabilities.”

# TECHNIQUES:

## PORT SCANNING:

## TOOLS:

COMMANDS: nmap -sT 2example.com

nmap -SS example.com

nmap -SV example.com

masscan 192.168.1.0/24 -p1-65535

nc -zv example.com 1-1000 (netcat for multiple ports)

zmap -p 80 192.168.1.0/24 (for specific port scan)

## SERVICES VERSION DETECTION:

## TOOLS:

COMMANDS: banner example.com 80

nikto -h <http://192.168.1.1> (scan for web services version)

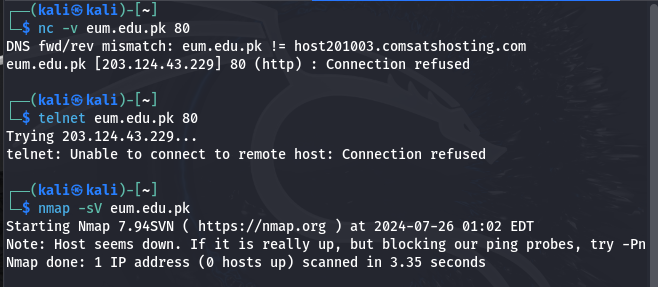
telnet example.com 80

nc -v example.com 80

nmap -sV example.com

## 





# THE END

BY ATIQ-UR-REHMAN