Assignment-1

Bhargav Rohit .D

20-01-2025

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 Recon-ng, Maltego. This additional information will help in identifying vulnerabilities and enhancing the security assessment of the target.

Objectives:

- Footprint a target using Recon-ng.
- Footprint a target using Maltego.

Task to be Completed:

- A detailed report documenting the steps taken and the information gathered for each tool (Recon-ng, Maltego).
- 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. The aim is to identify potential vulnerabilities and security loopholes by collecting detailed data about the target, which will inform further security assessments and recommendations.

Limitation: - Footprinting would be conducted on a basic level, active or passive. No direct engagement would be performed to disrupt the services. We will be using modules without API key which will limit our finding. Modules like whois, or whoxy can't be used as the key not available or paid services.

Objective: - Footprinting on my target to find vulnerabilities or find sensitive data (like pdfs, bat, etc), weak encryption, malicious files,

Tools to be used: -

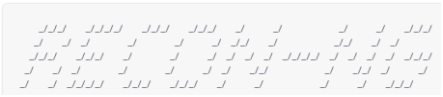
- Recon-ng
- Maltego

Target: -

Certifiedhacker.com.

Activity: - Footprinting.

Findings: -



Recon-NG: - It is an Opensource Intelligence command line tool consisting of all the tools required for domain discovery, vulnerability discovery, host enumeration, information disclosure. There are many tools which would require API, for this assignment we would only use those modules which wouldn't require any API for the tools.

Introduction/Basics: -

Let's first discover commands available for us using help.

```
[recon-ng][default] > help

Commands (type [help|?] <topic>):
---------------------------------
back            Exits the current context
dashboard       Displays a summary of activity
db              Interfaces with the workspace's database
exit            Exits the framework
help            Displays this menu
index           Creates a module index (dev only)
keys            Manages third party resource credentials
marketplace     Interfaces with the module marketplace
modules         Interfaces with installed modules
options         Manages the current context options
pdb             Starts a Python Debugger session (dev only)
script          Records and executes command scripts
shell           Executes shell commands
show            Shows various framework items
snapshots       Manages workspace snapshots
spool           Spools output to a file
workspaces      Manages workspaces
```

We will be using mostly commands like, marketplace, load, key, modules, options.

Troubleshooting or Installing Modules: -

First, we will discover what all tools are available and what tools are to be installed.

```
[recon-ng][default] > marketplace search

+-------------------------------------------------------------------------------------------+
|                                Path                               | Version |   Status  | Updated    | D | K |
+-------------------------------------------------------------------------------------------+
| discovery/info_disclosure/cache_snoop                             | 1.1     | installed | 2020-10-13 |   |   |
| discovery/info_disclosure/interesting_files                       | 1.2     | installed | 2021-10-04 |   |   |
| exploitation/injection/command_injector                           | 1.0     | installed | 2019-06-24 |   |   |
| exploitation/injection/xpath_bruter                               | 1.2     | installed | 2019-10-08 |   |   |
| import/csv_file                                                   | 1.1     | installed | 2019-08-09 |   |   |
| import/list                                                       | 1.1     | installed | 2019-06-24 |   |   |
| import/masscan                                                    | 1.0     | installed | 2020-04-07 |   |   |
| import/nmap                                                       | 1.1     | installed | 2020-10-06 |   |   |
| recon/companies-contacts/bing_linkedin_cache                      | 1.0     | installed | 2019-06-24 |   | * |
| recon/companies-contacts/censys_email_address                     | 2.1     | installed | 2022-01-31 | * | * |
| recon/companies-contacts/pen                                      | 1.1     | installed | 2019-10-15 |   |   |
| recon/companies-domains/censys_subdomains                         | 2.1     | disabled  | 2022-01-31 | * | * |
| recon/companies-domains/pen                                       | 1.1     | installed | 2019-10-15 |   |   |
| recon/companies-domains/viewdns_reverse_whois                     | 1.1     | installed | 2021-08-24 |   |   |
| recon/companies-domains/whoxy_dns                                 | 1.1     | installed | 2020-06-17 |   | * |
| recon/companies-multi/censys_org                                  | 2.1     | installed | 2022-01-31 | * | * |
| recon/companies-multi/censys_tls_subjects                         | 2.1     | installed | 2022-01-31 | * | * |
| recon/companies-multi/github_miner                                | 1.1     | installed | 2020-05-15 |   | * |
| recon/companies-multi/shodan_org                                  | 1.1     | installed | 2020-07-01 | * | * |
```

I have installed all the tools prior to documentation where I had no modules installed.

But how to install modules if not available?

Using the below command will start the installation process. It will give the warning of all the tools which won't work without API key.

```
[recon-ng][default] > marketplace install all
[*] Module installed: discovery/info_disclosure/cache_snoop
[*] Module installed: discovery/info_disclosure/interesting_files
[*] Module installed: exploitation/injection/command_injector
[*] Module installed: exploitation/injection/xpath_bruter
[*] Module installed: import/csv_file
[*] Module installed: import/list
[*] Module installed: import/masscan
[*] Module installed: import/nmap
[*] Module installed: recon/companies-contacts/bing_linkedin_cache
[*] Module installed: recon/companies-contacts/censys_email_address
[*] Module installed: recon/companies-contacts/pen
[*] Module installed: recon/companies-domains/censys_subdomains
[*] Module installed: recon/companies-domains/pen
[*] Module installed: recon/companies-domains/viewdns_reverse_whois
[*] Module installed: recon/companies-domains/whoxy_dns
```

API key for many tools is important for them to work properly. We would only add Shodan API key for this testing.

How to check list of keys to be added?

We use this command to list all the keys. Lists all the tools which might require keys to work.

```
[recon-ng][default] > keys list
+-------------------------+
|       Name      | Value |
+-------------------------+
| binaryedge_api  |       |
| bing_api        |       |
| builtwith_api   |       |
| censysio_id     |       |
| censysio_secret |       |
| flickr_api      |       |
| fullcontact_api |       |
| github_api      |       |
| google_api      |       |
| hashes_api      |       |
| hibp_api        |       |
| hunter_io       |       |
| ipinfodb_api    |       |
| ipstack_api     |       |
| namechk_api     |       |
| shodan_api      |       |
| spyse_api       |       |
| twitter_api     |       |
| twitter_secret  |       |
| virustotal_api  |       |
| whoxy_api       |       |
+-------------------------+
```

And next we will add API key for Shodan. We can also remove by just replacing "remove" in place of "add" from the command below.

```
[recon-ng][default] > keys add shodan WcjaunaEJlylJW00YM6Mrgl7aXx8Xyfu
[*] Key 'shodan' added.
```

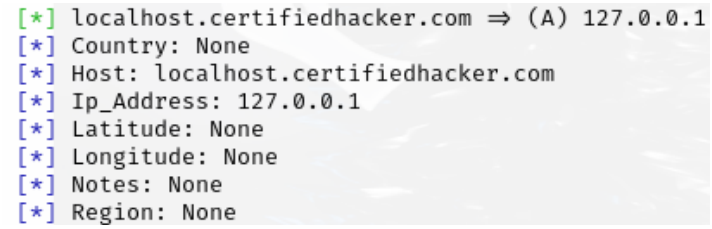
Now as we are done with all the introduction of this tools and basic, we will start recording the attacks with details for each tool's findings.

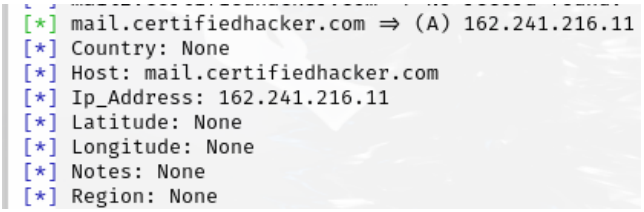
Domain Enumeration: -

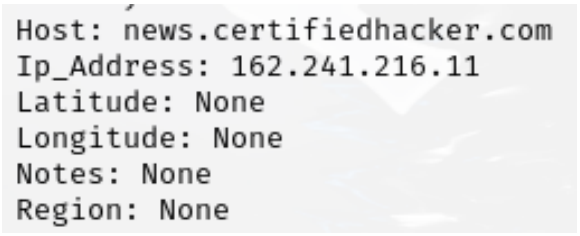
Module brute_hosts: - Performs brute-forcing to find subdomains.

```
[recon-ng][default][whois_orgs] > modules load recon/domains-hosts/brute_hosts
[recon-ng][default][brute_hosts] > options set shource certifiedhacker.com
[!] Invalid option name.
[recon-ng][default][brute_hosts] > options set source certifiedhacker.com
SOURCE ⇒ certifiedhacker.com
[recon-ng][default][brute_hosts] > run
[*] autodiscover.certifiedhacker.com ⇒ (A) 162.241.216.11
[*] Country: None
[*] Host: autodiscover.certifiedhacker.com
[*] Ip_Address: 162.241.216.11
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] Country: None
[*] Host: blog.certifiedhacker.com
[*] Ip_Address: 162.241.216.11
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] demo.certifiedhacker.com ⇒ (A) 162.241.216.11
[*] Country: None
[*] Host: demo.certifiedhacker.com
[*] Ip_Address: 162.241.216.11
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] events.certifiedhacker.com ⇒ (A) 162.241.216.11
[*] Country: None
[*] Host: events.certifiedhacker.com
[*] Ip_Address: 162.241.216.11
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] Host: ftp.certifiedhacker.com
[*] Ip_Address: 162.241.216.11
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
```

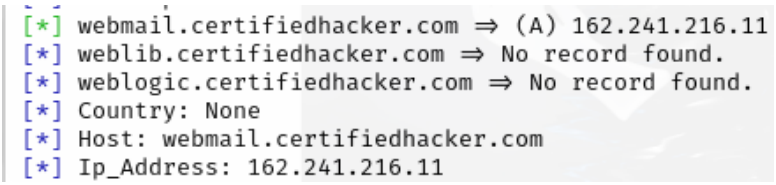

[*] imap.certifiedhacker.com ⇒ (CNAME) mail.certifiedhacker.com
[*] Country: None
[*] Host: mail.certifiedhacker.com
[*] Ip_Address: None
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ——
[*] Country: None
[*] Host: imap.certifiedhacker.com
[*] Ip_Address: None
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ——
[*] imap.certifiedhacker.com ⇒ (A) 162.241.216.11
[*] Country: None
[*] Host: imap.certifiedhacker.com
[*] Ip_Address: 162.241.216.11
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None

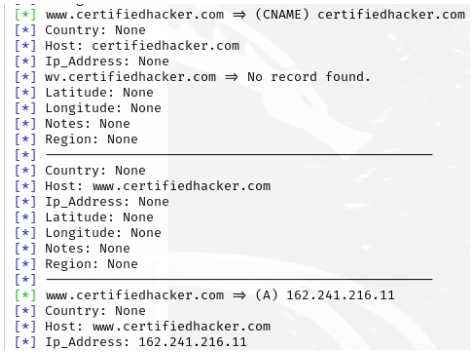

[*] localhost.certifiedhacker.com ⇒ (A) 127.0.0.1
[*] Country: None
[*] Host: localhost.certifiedhacker.com
[*] Ip_Address: 127.0.0.1
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None


[*] mail.certifiedhacker.com ⇒ (A) 162.241.216.11
[*] Country: None
[*] Host: mail.certifiedhacker.com
[*] Ip_Address: 162.241.216.11
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None


Host: news.certifiedhacker.com
Ip_Address: 162.241.216.11
Latitude: None
Longitude: None
Notes: None
Region: None


Host: mail.certifiedhacker.com
Ip_Address: None
Latitude: None
Longitude: None
Notes: None
Region: None
——
Country: None
Host: pop.certifiedhacker.com
Ip_Address: None
Latitude: None
Longitude: None
Notes: None
Region: None
——
pop.certifiedhacker.com ⇒ (A) 162.241.216.11
Country: None
Host: pop.certifiedhacker.com
Ip_Address: 162.241.216.11
Latitude: None
Longitude: None
Notes: None
Region: None


[*] webmail.certifiedhacker.com ⇒ (A) 162.241.216.11
[*] weblib.certifiedhacker.com ⇒ No record found.
[*] weblogic.certifiedhacker.com ⇒ No record found.
[*] Country: None
[*] Host: webmail.certifiedhacker.com
[*] Ip_Address: 162.241.216.11



Module mx_spf_ip: - Identifies MX and SPF records for a domain.

```
[recon-ng][default][brute_hosts] > modules load recon/domains-hosts/mx_spf_ip
[recon-ng][default][mx_spf_ip] > options set source certifiedhacker.com
SOURCE ⇒ certifiedhacker.com
[recon-ng][default][mx_spf_ip] > run
[*] Retrieving MX records for certifiedhacker.com.
[*] Country: None
[*] Host: mail.certifiedhacker.com
[*] Ip_Address: None
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ---
[*] Retrieving SPF records for certifiedhacker.com.
[*] TXT record: "v=spf1 a mx ptr include:bluehost.com ?all"

SUMMARY
[*] 1 total (0 new) hosts found.
```

Host Enumeration: -

Module reverse_resolve: - Performs reverse DNS lookups on IP addresses. But we couldn't find anything helpful using this module.

```
[recon-ng][default][whois_miner] > modules load recon/hosts-hosts/reverse_resolve
[recon-ng][default][reverse_resolve] > options set source 162.241.216.11
SOURCE ⇒ 162.241.216.11
[recon-ng][default][reverse_resolve] > run
[*] Country: None
[*] Host: box5331.bluehost.com
[*] Ip_Address: 162.241.216.11
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
```

Vulnerability Discovery: -

To find vulnerability in the website we have two modules namely ghdb and xssed, and both of them have given us no result.

Module ghdb and xssed: - Uses Google Hacking Database queries to discover vulnerabilities

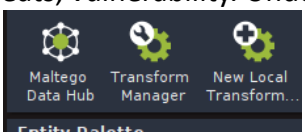
```
[recon-ng][default][resolve] > modules load recon/domains-vulnerabilities/ghdb
[recon-ng][default][ghdb] > options set source certifiedhacker.com
SOURCE => certifiedhacker.com
[recon-ng][default][ghdb] > run

------------------
CERTIFIEDHACKER.COM
------------------
[recon-ng][default][ghdb] > modules load recon/domains-vulnerabilities/xssed
[recon-ng][default][xssed] > options set source certifiedhacker.com
SOURCE => certifiedhacker.com
[recon-ng][default][xssed] > run

------------------
CERTIFIEDHACKER.COM
------------------
[*] No vulnerabilites found.
```

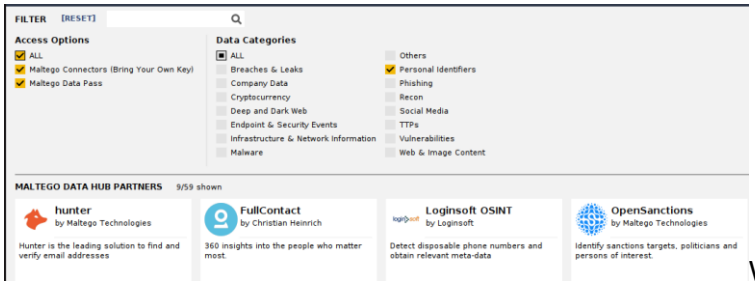
Result: - We could only find subdomain, mail server records and host details which are easily available. I couldn't find any sensitive data or files and vulnerability using this tool.

Drawback: - Overall, the tool might be a one stop solution for all OSINT tools but it is not efficient, after repeated updating of recon-ng, I still faced issue in finding details which costed me hours of struggle which could be done in few minutes if used individual tools. Either the tool was crashing or won't sow any result due to lack of API key.

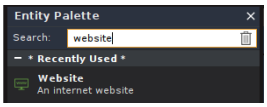
Maltego: - Maltego is well known OSINT tool which helps in investigation or foot printing on the target. It has a unique way of displaying results in form of trees connections which helps us understand relationship between the findings. There are many tools which are integrated and need API. I have used or plugins which has free API available or which won't require API. One of example would be using virustotal.

Basics: - Before starting we would need to install attachment or tool to run inside maltego to fetch different information like contact details, email, domain, threats, vulnerability. Under which tab can we find it? Select Transforms-> Maletgo data hub.

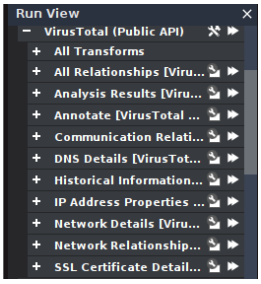


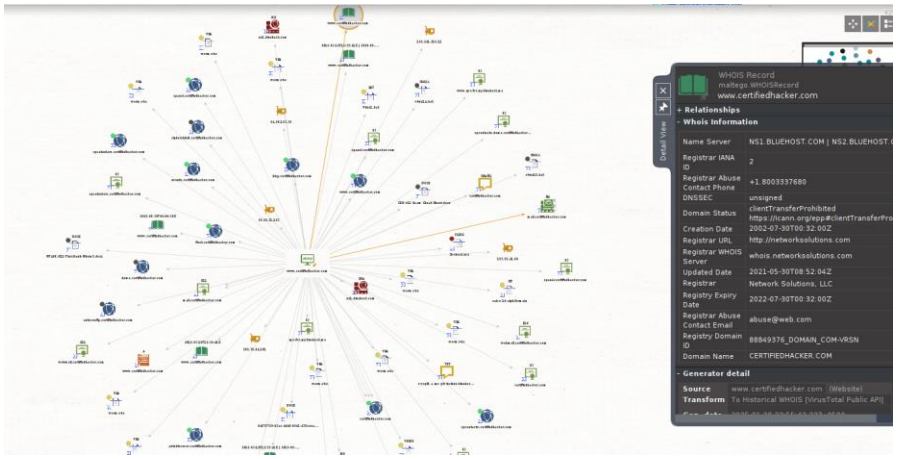


We can see all the tools over here, not just download from here also find details of tools and usage. The tools are curated in categories to help us find suitable tools for our Usage. As our target is a website, under search bar enter website, drag and drop the first option available to us and change the domain to targets domain which is certifiedhacker.com



Findings: - Right click on it, and click play icon beside virustotal. We can see what all information would be extracted which includes SSL certs, DNS, IP or any harmful file.



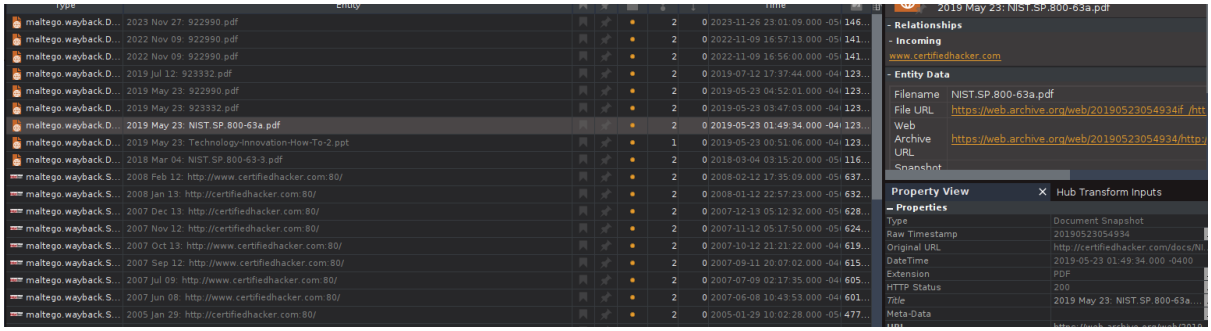


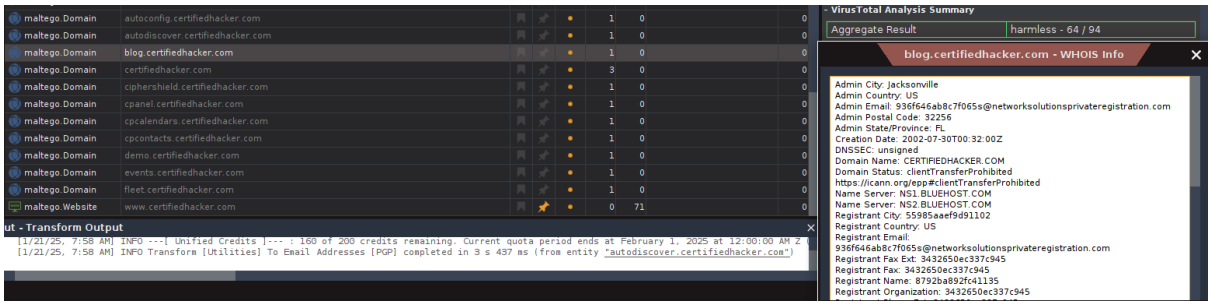
Now we can see the results showing the relationship with the domain.It is difficult to understand individually, so we will change it to tabular view.

maltego.IPv4Address	162.241.216.11	maltego.NSRecord	ns2.bluehost.com
maltego.IPv4Address	183.82.41.50	maltego.virustotal....	NT405.O11-ThucHanh-Nhom8.docx
maltego.IPv4Address	202.75.54.101	maltego.virustotal....	secure.docx
maltego.IPv4Address	64.90.163.30	maltego.virustotal....	Svchost.exe
maltego.IPv4Address	69.89.31.193	maltego.X509Certifi...	uyr.fvr.mybluehost.me
maltego.Domain	autoconfig.certifiedhacker.com	maltego.Phrase	v=spf1 a mx ptr include:bluehost.com ?all
maltego.Domain	autodiscover.certifiedhacker.com	maltego.virustotal....	Virus1.bat
maltego.virustotal....	b4879730-b3ac-4d40-b9e1-472ceeaa95da	maltego.virustotal....	virus14.bat
maltego.Domain	blog.certifiedhacker.com	maltego.virustotal....	virus15.bat
maltego.virustotal....	CEH v11 Exam Cheat Sheet.docx	maltego.X509Certifi...	webmail.certifiedhacker.com
maltego.virustotal....	ceh-v-10.zip&formats	maltego.X509Certifi...	webmail.certifiedhacker.com
maltego.X509Certifi...	certifiedhacker.com	maltego.virustotal....	worm.vbs
maltego.Domain	certifiedhacker.com	maltego.virustotal....	worm.vbs
maltego.Phrase	certifiedhacker.com	maltego.virustotal....	worm.vbs
maltego.virustotal....	Chrome_Installer.exe	maltego.virustotal....	worm.vbs
maltego.Domain	ciphershield.certifiedhacker.com	maltego.virustotal....	worm.vbs
maltego.Domain	cpanel.certifiedhacker.com	maltego.virustotal....	worm.vbs
maltego.X509Certifi...	cpanel.certifiedhacker.com	maltego.virustotal....	worm.vbs
maltego.X509Certifi...	cpanel.certifiedhacker.com	maltego.virustotal....	worm.vbs
maltego.Domain	cpcalendars.certifiedhacker.com	maltego.virustotal....	worm.vbs
maltego.X509Certifi...	cpcalendars.certifiedhacker.com	maltego.WHOISRec...	www.certifiedhacker.com
maltego.Domain	cpcontacts.certifiedhacker.com	maltego.WHOISRec...	www.certifiedhacker.com
maltego.X509Certifi...	cpcontacts.demo.certifiedhacker.com	maltego.WHOISRec...	www.certifiedhacker.com
maltego.Domain	demo.certifiedhacker.com	maltego.WHOISRec...	www.certifiedhacker.com
maltego.virustotal....	DFFD.bat	maltego.WHOISRec...	www.certifiedhacker.com
maltego.Domain	events.certifiedhacker.com	maltego.X509Certifi...	www.certifiedhacker.com
maltego.Domain	fleet.certifiedhacker.com	maltego.X509Certifi...	www.certifiedhacker.com
maltego.X509Certifi...	mail.certifiedhacker.com	maltego.Domain	www.certifiedhacker.com
maltego.MXRecord	mail.certifiedhacker.com	maltego.ARecord	www.certifiedhacker.com
maltego.NSRecord	ns1.bluehost.com	maltego.Website	www.certifiedhacker.com
maltego.NSRecord	ns1.bluehost.com	maltego.X509Certifi...	www.uyr.fvr.mybluehost.me

worm

Here we get all the important information regarding IP, domains (admin/registrar city, email, phone no., domain/server name), SSL certification, NSRecord, and files (like pdf, bat, vbs).





In my investigation, I could find some vulnerability with potential risk. Here are some of findings: -

- Sensitive files accessible to public, potential risk of data breach.
- History of changes to website were visible with a time line.
- Files containing worms and virus file were present, it is downloadable file and can cause system compromise if downloaded by user by mistake.
- Using outdated or weak encryption algorithms can make the SSL connection vulnerable to attacks.

Analysis and Implications:

The vulnerabilities identified could lead to various attacks, such as data theft, malware distribution, and man-in-the-middle attacks. Weak encryption and misconfigured SSL certificates further increase the risk of data tampering and unauthorized access.

Common Vulnerabilities:

1. **SQL Injection**: Allows attackers to manipulate backend SQL queries by injecting malicious code through user inputs.
2. **Cross-Site Scripting (XSS)**: Enables attackers to inject malicious scripts into web pages viewed by other users.
3. **Broken Authentication**: Weaknesses in authentication mechanisms that allow attackers to compromise passwords, keys, or session tokens.
4. **Security Misconfigurations**: Improperly configured systems that expose sensitive information or allow unauthorized access.

5. **Insecure Direct Object References**: Occurs when an application provides direct access to objects based on user-supplied input.
6. **Cross-Site Request Forgery (CSRF)**: Tricks users into performing actions they didn't intend to on a web application where they are authenticated.
7. **Unvalidated Redirects and Forwards**: Allows attackers to redirect users to malicious sites.
8. **Insufficient Transport Layer Security (TLS)**: Weaknesses in encryption protocols that can be exploited to intercept data.
9. **Insecure Cryptographic Storage**: Poorly implemented encryption that can be broken to access sensitive data.
10. **Exposure of Sensitive Files**: Sensitive files left publicly accessible can be exploited to gain unauthorized access or information
11. **Insufficient encryption**: - Weak encryption consisting storing of data may affect integrity and availability.

Possible Attacks:

1. **Malware Distribution**: Attackers can use vulnerabilities to distribute malware, including viruses and worms, to infect systems.
2. **Data Theft**: Exploiting vulnerabilities to steal sensitive information such as personal data, financial information, or login credentials.
3. **Denial of Service (DoS)**: Overwhelming a system with traffic to make it unavailable to users.
4. **Phishing**: Using compromised websites to trick users into providing sensitive information.
5. **Man-in-the-Middle (MitM) Attack**: Intercepting and potentially altering communications between two parties.
6. **Ransomware**: Encrypting data on the victim's system and demanding a ransom for decryption.
7. **Privilege Escalation**: Gaining higher-level access to resources that are normally protected from an application or user.
8. **Session Hijacking**: Taking over a user's session to gain unauthorized access to their account.
9. **Code Injection**: Executing arbitrary code on the server or client-side to manipulate the application.

10. **Zero-Day Exploits**: Exploiting unknown vulnerabilities for which no fix is available

Conclusion: - I would like to wrap up my documentation with suitable recommendation which should be implemented by the developers to strengthen overall security.

Recommendation: -

- **Implement Access Controls**: Use role-based access control (RBAC) to manage permissions.
- **Remove or Relocate Sensitive Files**: Remove unnecessary sensitive files from public directories, or relocate them to secure locations.
- **Regular Audits**: Conduct regular audits to identify and secure any exposed sensitive files.

- **Conduct Malware Scanning**: Use reliable antivirus and anti-malware tools to scan and remove any detected malicious files.
- **Implement Web Application Firewalls (WAF)**: Protect against common web threats by filtering and monitoring HTTP traffic.
- **Update Expired Certificates**
- **Use Strong Encryption**: - such as AES-256, and avoid outdated protocols like SSL 3.0 and TLS 1.0.
- **Regular Certificate Management**: Monitor and manage SSL certificates regularly to maintain their validity and security.
- **Implement Multi-Factor Authentication (MFA).**
- **Apply Software Updates and Patches.**

----------END----------