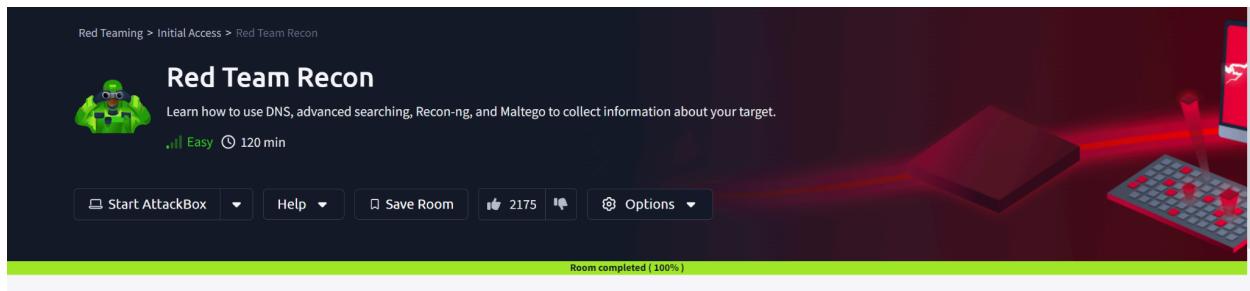


# RED TEAM RECON

## ASSIGNMENT REPORT



**Peter Kinyumu,  
cs-sa07-24067,  
May 22nd, 2024.**

## 1. INTRODUCTION

This room teaches about reconnaissance; the preliminary survey of your target without alerting them to your activities. It covers tools that can help gather more information about your target such as the **whois** command to get the WHOIS records like domain registration details, Google Dorking, **nslookup**, **dig**, **host** for DNS records extractions, **recon-ng** and **Maltego**.

## 2. ANSWERS TO QUESTIONS

### Built-in tools

- When was thmredteam.com created (registered)? (YYYY-MM-DD)

2021-09-24

```
(cvpherpunk㉿votex)-[~]$ whois thmredteam.com
Domain Name: THMREDTTEAM.COM
Registry Domain ID: 2643258257_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.namecheap.com
Registrar URL: http://www.namecheap.com
Updated Date: 2023-09-30T23:11:17Z
Creation Date: 2021-09-24T14:04:16Z
Registry Expiry Date: 2024-09-24T14:04:16Z
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: K1P.NS.CLOUDFLARE.COM
Name Server: UMA.NS.CLOUDFLARE.COM
DNSSEC: unsigned
URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
>>> Last update of Whois database: 2024-05-21T09:55:55Z <<
For more information on Whois status codes, please visit https://icann.org/epp
```

- To how many IPv4 addresses does clinic.thmredteam.com resolve?
- To how many IPv6 addresses does clinic.thmredteam.com resolve?

```
(cvpherpunk㉿votex)-[~]$ host clinic.thmredteam.com
clinic.thmredteam.com has address 172.67.212.249
clinic.thmredteam.com has address 104.21.93.169
clinic.thmredteam.com has IPv6 address 2606:4700:3034::ac43:d4f9
clinic.thmredteam.com has IPv6 address 2606:4700:3034::6815:5da9
(cvpherpunk㉿votex)-[~]
$ 
Two Ips of each type
```

### Advanced Searching

- How would you search using Google for xls indexed for <http://clinic.thmredteam.com>?
- How would you search using Google for files with the word passwords for <http://clinic.thmredteam.com>?

Answer the questions below

How would you search using Google for `xls` indexed for <http://clinic.thmredteam.com>?

`filetype: xls site: clinic.thmredteam.com`

✓ Correct Answer ✗ Hint

How would you search using Google for files with the word `passwords` for <http://clinic.thmredteam.com>?

`passwords site: clinic.thmredteam.com`

✓ Correct Answer ✗ Hint

Task 5 ✓ Specialized Search Engines

## Shodan

- a. What is the shodan command to get your Internet-facing IP address?  
**shodan myip**

```
(cyberpunk㉿votex)-[~]
$ shodan -h
Usage: shodan [OPTIONS] COMMAND [ARGS]...
Options:
-h, --help Show this message and exit.
Commands:
alert      Manage the network alerts for your account
convert    Convert the given input data file into a different format.
count      Returns the number of results for a search
data       Bulk data access to Shodan
domain    View all available information for a domain
download   Download search results and save them in a compressed JSON...
honeyscore Check whether the IP is a honeypot or not.
host      View all available information for an IP address
info       Shows general information about your account
init      Initialize the Shodan command-line
myip      Print your external IP address
org       Manage your organization's access to Shodan
parse     Extract information out of compressed JSON files.
radar    Real-Time Map of some results as Shodan finds them.
scan      Scan an IP/ netblock using Shodan.
search   Search the Shodan database
stats    Provide summary information about a search query
stream   Stream data in real-time.
trends   Search Shodan historical database
version  Print version of this tool.
(cyberpunk㉿votex)-[~]
$
```

## Recon-ng

- a. How do you start recon-**ng** with the workspace **clinicredteam**?  
b. How many modules with the name **virustotal** exist?

Two modules exist with the name virustotal.

c. There is a single module under hosts-domains. What is its name?

```
[recon-ng][clinicredteam] > marketplace search hosts-domains
[*] Searching module index for 'hosts-domains'...

+-----+-----+-----+-----+-----+
|       Path          | Version | Status    | Updated   | D | K |
+-----+-----+-----+-----+-----+
| recon/hosts-domains|migrate_hosts| 1.1      | not installed | 2020-05-17 |   |   |
+-----+-----+-----+-----+-----+

D = Has dependencies. See info for details.
K = Requires keys. See info for details.

[recon-ng][clinicredteam] > █
```

d. censys\_email\_address is a module that “retrieves email addresses from the TLS certificates for a company.” Who is the author? (Formart \*\*\*\*\* \*\*\*\*)

```
[recon-ng][clinicreditteam] > marketplace info censys_email_address
+-----+
| path      | recon/companies-contacts/censys_email_address
| name      | Censys - Emails by Company
| author    | Censys, Inc. <support@censys.io>
| version   | 2.1
| last_updated | 2022-01-31
| description | Retrieves email addresses from the TLS certificates for a company. This module queries the 'services.tls.certificates.leaf_data.subject.email_address' field and updates the 'contacts' table with the results.
| required_keys | ['censysio_id', 'censysio_secret']
| dependencies | ['censys>=2.1.2']
| files     | []
| status     | not installed
+-----+
[recon-ng][clinicreditteam] >
```

## Maltego

- a. What is the name of the transform that queries NIST's National Vulnerability Database?

The screenshot shows the Maltego website with the URL [maltego.com/transform-hub/nist-nvd](https://www.maltego.com/transform-hub/nist-nvd). The page features a dark header with the Maltego logo and navigation links. Below the header, there's a section titled "NIST NVD Transforms for Maltego".

## NIST NVD Transforms for Maltego

Founded in 1901, National Institute of Standards and Technology (NIST) is a non-regulatory federal agency within the U.S. Department of Commerce. The National Vulnerability Database (NVD) is a product of the NIST Computer Security Division, Information Technology Laboratory.

NVD is the U.S. government repository of standards-based vulnerability management data. The data is represented using the Security Content Automation Protocol (SCAP) and enables automation of vulnerability management, security measurement, and compliance.

The NVD includes databases of security checklist references, security-related software flaws, misconfigurations, product names, and impact metrics.

The NVD performs analysis on CVEs that have been published to the CVE Dictionary. The NVD team analyzes CVEs by



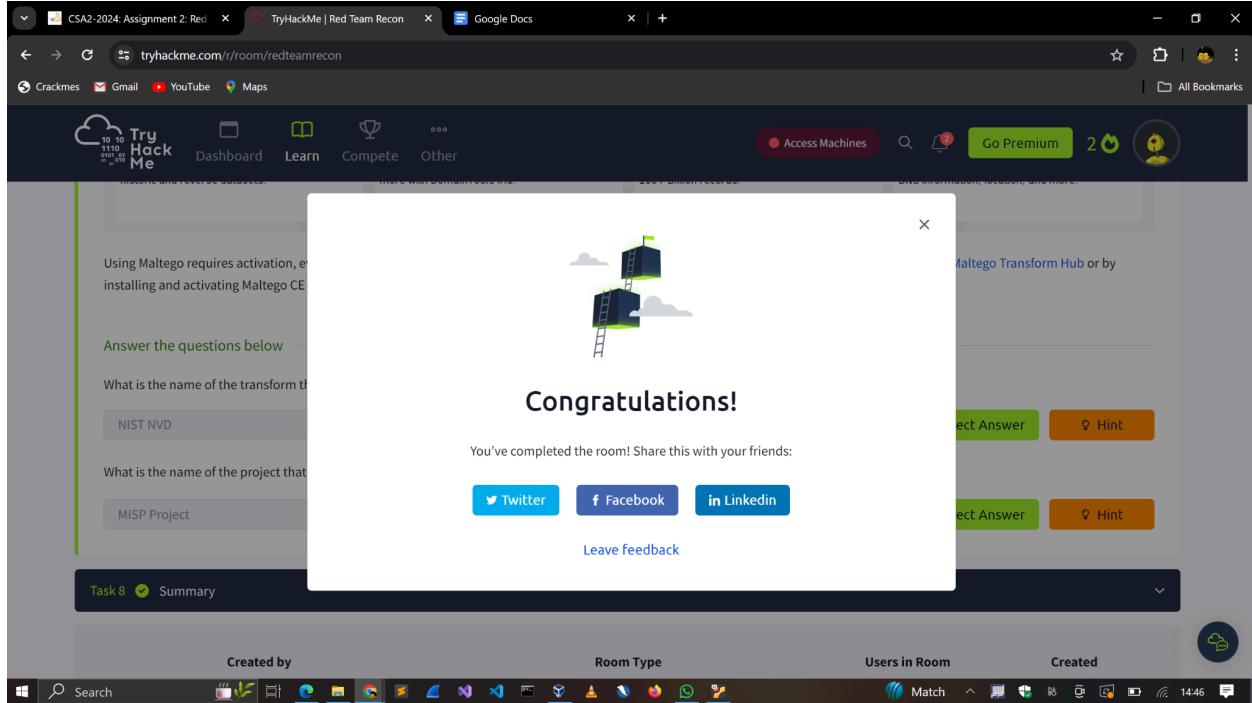
- b. What is the name of the project that offers a transform based on ATT&CK?

The screenshot shows the Maltego website with the URL <https://www.maltego.com/transform-hub/att-ck-misp-misp-and-mitre-attack/>. The page displays a grid of transform cards. One card for "ATT&CK - MISP" is highlighted with a red border. Other cards include "ThreatMiner" and "ZeroFOX". A "LOAD MORE" button is at the bottom of the grid.

### 3. MODULE COMPLETION

Below is the link to my THM profile, which displays completed rooms, including this room, Red Team Recon.

<https://tryhackme.com/p/c1ph3rbnuk>



### 4. CONCLUSION

I am excited to have learned a lot about Reconnaissance and OSINT from this assignment. I learnt how to use the **whois** command to view domain registration details and WHOIS records. I have also learnt to extract DNS information using tools like **dig**, **nslookup**, and **host**. Additionally, I have learnt to perform advanced searching on Google with queries like **site:example.com**, **filetype:pdf**, etc. I have learnt how to use special search engines like ViewDNS.info, Shodan and Censys to gather more information about target IP addresses. Lastly, I have enjoyed using **recon-ng**, a framework that automates OSINT work.

I look forward to applying this knowledge on reconnaissance in my penetration testing process.