

Red Team Recon

The tasks of this room cover the following topics:

- Types of reconnaissance activities
- WHOIS and DNS-based reconnaissance
- Advanced searching
- Searching by image
- Google Hacking
- Specialized search engines
- Recon-ng
- Maltego

The screenshot shows a web browser window with the URL `tryhackme.com/r/room/redteamrecon`. The browser's tab bar includes 'Inbox', '(56) V', 'CSA2', 'Dashb', 'TryHa', 'Downl', 'Create', 'Docum', 'ChatG', 'Intern', and 'ChatG'. The TryHackMe website header features a navigation bar with 'Dashboard', 'Learn', 'Compete', and 'Other' links, along with buttons for 'Access Machines', 'Go Premium', and a user profile icon. The main content area lists specific objectives for reconnaissance, such as discovering subdomains and gathering publicly available information. It also explains the difference between passive and active reconnaissance, focusing on passive techniques in this room. Below the text, there is a section for 'Answer the questions below' with a 'Correct Answer' button. At the bottom, two task cards are visible: 'Task 2: Taxonomy of Reconnaissance' and 'Task 3: Built-in Tools'.

tryhackme.com/r/room/redteamrecon

TryHackMe

Dashboard Learn Compete Other

Access Machines Go Premium 1

Some specific objectives we'll cover include:

- Discovering subdomains related to our target company
- Gathering publicly available information about a host and IP addresses
- Finding email addresses related to the target
- Discovering login credentials and leaked passwords
- Locating leaked documents and spreadsheets

Reconnaissance can be broken down into two parts — passive reconnaissance and active reconnaissance, as explained in Task 2. In this room, we will be focusing on passive reconnaissance, i.e., techniques that don't alert the target or create 'noise'. In later rooms, we will use active reconnaissance tools that tend to be noisy by nature.

Answer the questions below

We suggest you start the AttackBox and experiment with every command and tool we demonstrate.

No answer needed Correct Answer

Task 2 Taxonomy of Reconnaissance

Task 3 Built-in Tools

tryhackme.com/r/room/redteamrecon

TryHackMe Dashboard Learn Compete Other Access Machines Go Premium 1

Active recon can be classified as:

1. **External Recon:** Conducted outside the target's network and focuses on the externally facing assets assessable from the Internet. One example is running Nikto from outside the company network.
2. **Internal Recon:** Conducted from within the target company's network. In other words, the pentester or red teamer might be physically located inside the company building. In this scenario, they might be using an exploited host on the target's network. An example would be using Nessus to scan the internal network using one of the target's computers.

Answer the questions below

Ensure you have a clear understanding of the different types of recon activities before proceeding.

No answer needed ✓ Correct Answer

Task 3 ☐ Built-in Tools

Task 4 ☐ Advanced Searching

Task 5 ☐ Specialized Search Engines

Task 6 ☐ Recon-ng

Task 7 ☐ Maltego

```
root@kali: /home/kali
File Actions Edit View Help
root@kali: /home/kali/Downloads x root@kali: /home/kali x
[sudo] password for kali:
Sorry, try again.
[sudo] password for kali:
root@kali:~# whois thmredteam.com
Domain Name: THMREDTEAM.COM
Registry Domain ID: 2643258257_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.namecheap.com
Registrar URL: http://www.namecheap.com
Updated Date: 2023-09-30T22:11:17Z
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#clientTransf
erProhibited
Name Server: KIP.NS.CLOUDFLARE.COM
Name Server: UMA.NS.CLOUDFLARE.COM
DNSSEC: unsigned
URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wi
cf/
>>> Last update of whois database: 2024-05-29T17:21:07Z <<<

For more information on Whois status codes, please visit https://icann.org/ep
p

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 expiratio
n
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
```

tryhackme.com/r/room/redteamrecon

nslookup, dig for host to query DNS servers

WHOIS databases and DNS servers hold publicly available information, and querying either does not generate any suspicious traffic.

Moreover, we can rely on Traceroute (traceroute on Linux and macOS systems and tracert on MS Windows systems) to discover the hops between our system and the target host.

Answer the questions below

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

2021-09-24 ✓ Correct Answer Hint

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

2 ✓ Correct Answer

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

2 ✓ Correct Answer

Task 4 Advanced Searching

Task 5 Specialized Search Engines

root@kali: /home/kali

```
DNSSEC: unsigned
URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/
>>> Last update of WHOIS database: 2024-05-28T21:21:24.88Z <<<
For more information on Whois status codes, please visit https://icann.org/ep
p

(root@kali)-[/home/kali]
# 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

(root@kali)-[/home/kali]
# recon-ng clinicredteam
usage: recon-ng [-h] [-w workspace] [--no-version] [--no-analytics] [--no-marketplace] [--stealth] [--accessible] [--version]
recon-ng: error: unrecognized arguments: clinicredteam

(root@kali)-[/home/kali]
# recon-ng -w clinicredteam
[*] Version check disabled.

[+] You can find the new [redacted] exist?

There is a single module [redacted] What is its name?

Sponsored by ...

www.blackhillsinfosec.com
retrieves email addresses from the TLS certificates for a company? Who is the author?

PRACTISEC
www.practisec.com

[recon-ng v5.1.2, Tim Tones (@lanmaster53)]

[*] No modules enabled/installed.

[recon-ng][clinicredteam] >
```

```
root@kali: /home/kali
File Actions Edit View Help
root@kali: /home/kali/Downloads x root@kali: /home/kali x
[recon-ng v5.1.2, Tim Tomes (@lanmaster53)]
[*] No modules enabled/installed.
[recon-ng][clinicredteam] > ls
[!] Invalid command 'ls'.
[recon-ng][clinicredteam] > marketplace search domains-
[*] Searching module index for 'domains-' ... [0.00s] To get a list of all available modules.

+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
| Path | Version | Pub. | Status | Updated | D | K |
+-----+-----+-----+-----+-----+-----+-----+
| recon/domains-companies/censys_companies | 2.1 | not installed | 2022-01-31 | * | * | |
| recon/domains-companies/pen | 1.1 | not installed | 2019-10-15 | | | |
| recon/domains-companies/whoxy_whois | 1.1 | not installed | 2020-06-24 | | * | |
| recon/domains-contacts/hunter_io | 1.3 | not installed | 2020-04-14 | | * | |
| recon/domains-contacts/metacrawler | 1.1 | not installed | 2019-06-24 | | * | |
| recon/domains-contacts/pen | 1.1 | not installed | 2019-10-15 | | | |
| recon/domains-contacts/pgp_search | 1.4 | not installed | 2019-10-16 | | | |
| recon/domains-contacts/whois_pocs | 1.0 | not installed | 2019-06-24 | | | |
| recon/domains-contacts/wikileaker | 1.0 | not installed | 2020-04-08 | | | |
| recon/domains-domains/brute_suffix | 1.1 | not installed | 2020-05-17 | | | |
| recon/domains-hosts/binaryedge | 1.2 | not installed | 2020-06-18 | | * | |
| recon/domains-hosts/bing_domain_api | 1.0 | not installed | 2019-06-24 | | * | |
| recon/domains-hosts/bing_domain_web | 1.1 | not installed | 2019-07-04 | | | |
| recon/domains-hosts/brute_hosts | 1.0 | not installed | 2019-06-24 | | | |
| recon/domains-hosts/builtwith | 1.1 | not installed | 2021-08-24 | | * | |
| recon/domains-hosts/censys_domain | 2.1 | not installed | 2022-01-31 | * | * |
| recon/domains-hosts/certificate_transparency | 1.3 | not installed | 2019-09-16 | | | |
| recon/domains-hosts/google_site_web | 1.0 | not installed | 2019-06-24 | | | |
| recon/domains-hosts/hackertarget | 1.1 | not installed | 2020-05-17 | | | |
| recon/domains-hosts/has_spf_ip | 1.0 | not installed | 2019-06-24 | | | |
| recon/domains-hosts/netcraft | 1.1 | not installed | 2020-02-05 | | | |
| recon/domains-hosts/shodan_hostname | 1.1 | not installed | 2020-07-01 | * | * |
| recon/domains-hosts/spyse_subdomains | 1.1 | not installed | 2021-08-24 | | * | |
| recon/domains-hosts/ssl_san | 1.0 | not installed | 2019-06-24 | | | |
| recon/domains-hosts/threatcrowd | 1.0 | not installed | 2019-06-24 | | | |
| recon/domains-hosts/threatminer | 1.0 | not installed | 2019-06-24 | | | |
| recon/domains-hosts/vulnerabilities/ghdb | 1.1 | not installed | 2019-06-26 | | | |
| recon/domains-vulnerabilities/xssed | 1.1 | not installed | 2020-10-18 | | | |

D = Has dependencies. See info for details.
K = Requires keys. See info for details.
[recon-ng][clinicredteam] >
```

tryhackme.com/r/room/redteamrecon

Use **recon-ng** to repeat the steps we carried out against **thmredteam.com** then answer the following questions.

Answer the questions below

How do you start **recon-ng** with the workspace **clinicredteam**?

recon-ng -w clinicredteam ✓ Correct Answer Hint

How many modules with the name **virustotal** exist?

2 ✓ Correct Answer

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

migrate_hosts ✓ Correct Answer

censys_email_address is a module that "retrieves email addresses from the TLS certificates for a company." Who is the author?

Censys Team ✓ Correct Answer

Task 7 Maltego

Task 8 Summary

cs-sa07-24019
John_Mbithi_Mutave

```
root@kali: /home/kali
[sudo] password for kali:
Sorry, try again.
[sudo] password for kali:
root@kali: /home/kali
# whois thmredteam.com
Domain Name: THMREDTEAM.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#clientTransf
erProhibited
Name Server: KIP.NS.CLOUDFLARE.COM
Name Server: UMA.NS.CLOUDFLARE.COM
DNSSEC: unsigned
URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wi
cf/
>>> Last update of whois database: 2024-05-29T17:21:07Z <<<
For more information on Whois status codes, please visit https://icann.org/ep
p
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 expiratio
n
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
```

```
root@kali: /home/kali
Admin Email: e17b7976233e4e72a76b3dadbid574bd.protect@withheldforprivacy.com
Registry Tech ID:
Tech Name: Redacted for Privacy
Tech Organization: Privacy service provided by Withheld for Privacy ehf
Tech Street: Kalkofnsvegur 2
Tech City: Reykjavik
Tech State/Province: Capital Region
Tech Postal Code: 101
Tech Country: IS
Tech Phone: +354.4212434
Tech Phone Ext:
Tech Fax:
Tech Fax Ext:
Tech Email: e17b7976233e4e72a76b3dadbid574bd.protect@withheldforprivacy.com
Name Servers: kip.ns.cloudflare.com (created/registered) (YYYY-MM-DD)
Name Server: uma.ns.cloudflare.com
DNSSEC: unsigned
URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.n
et/
>>> Last update of WHOIS database: 2024-05-28T21:21:24.88Z <<<
For more information on Whois status codes, please visit https://icann.org/ep
p
root@kali: /home/kali
# 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 2606:4700:3834::ac43:d4f9
clinic.thmredteam.com has IPv6 address 2606:4700:3834::6815:5da9
root@kali: /home/kali
```

The screenshot shows a web browser window with the URL `tryhackme.com/r/room/redteamrecon`. The page header includes the TryHackMe logo, navigation links (Dashboard, Learn, Compete, Other), and buttons for 'Access Machines', 'Go Premium', and a user profile icon. The main content area is titled 'nslookup, dig or host to query DNS servers'. It explains that WHOIS databases and DNS servers hold publicly available information and that Traceroute can be used to discover hops between systems. Below this, there are three tasks: 'Answer the questions below', 'When was thmredteam.com created (registered)? (YYYY-MM-DD)', and 'To how many IPv4 addresses does clinic.thmredteam.com resolve?'. The first task has a text input field with '2021-09-24' and a 'Correct Answer' button. The second task has a text input field with '2' and a 'Correct Answer' button. The third task has a text input field with '2' and a 'Correct Answer' button. At the bottom, there are two task cards: 'Task 4: Advanced Searching' and 'Task 5: Specialized Search Engines'.

nslookup, dig or host to query DNS servers

WHOIS databases and DNS servers hold publicly available information, and querying either does not generate any suspicious traffic.

Moreover, we can rely on Traceroute (traceroute on Linux and macOS systems and tracert on MS Windows systems) to discover the hops between our system and the target host.

Answer the questions below

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

2021-09-24 ✓ Correct Answer ? Hint

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

2 ✓ Correct Answer

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

2 ✓ Correct Answer

Task 4: Advanced Searching

Task 5: Specialized Search Engines

The screenshot shows a web browser window with the URL `tryhackme.com/r/room/redteamrecon`. The page header is the same as the previous screenshot. The main content area continues with the text 'their ads. Moreover, it is always worth checking their website for any job opening and seeing if this can leak any interesting information.' and 'Note that the Wayback Machine can be helpful to retrieve previous versions of a job opening page on your client's site.' Below this, there are two tasks: 'Answer the questions below', 'How would you search using Google for xls indexed for http://clinic.thmredteam.com?', and 'How would you search using Google for files with the word passwords for http://clinic.thmredteam.com?'. The first task has a text input field with 'filetype:xls site:clinic.thmredteam.com' and a 'Correct Answer' button. The second task has a text input field with 'passwords site:clinic.thmredteam.com' and a 'Correct Answer' button. At the bottom, there are four task cards: 'Task 5: Specialized Search Engines', 'Task 6: Recon-ng', 'Task 7: Maltego', and 'Task 8: Summary'.

their ads. Moreover, it is always worth checking their website for any job opening and seeing if this can leak any interesting information.

Note that the Wayback Machine can be helpful to retrieve previous versions of a job opening page on your client's site.

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

Task 5: Specialized Search Engines

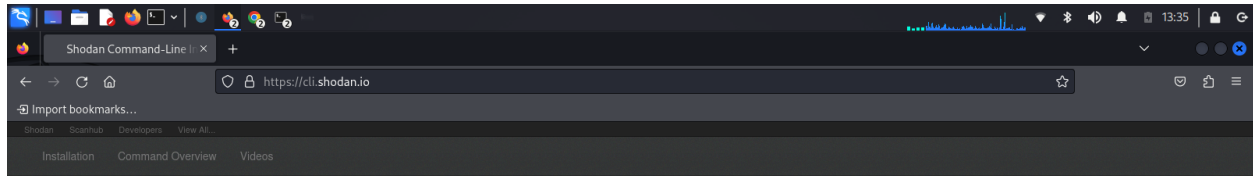
Task 6: Recon-ng

Task 7: Maltego

Task 8: Summary

cs-sa07-24019

John_Mbithi_Mutave



myip

Returns your Internet-facing IP address.

Example

```
$ shodan myip  
199.30.49.210
```

parse

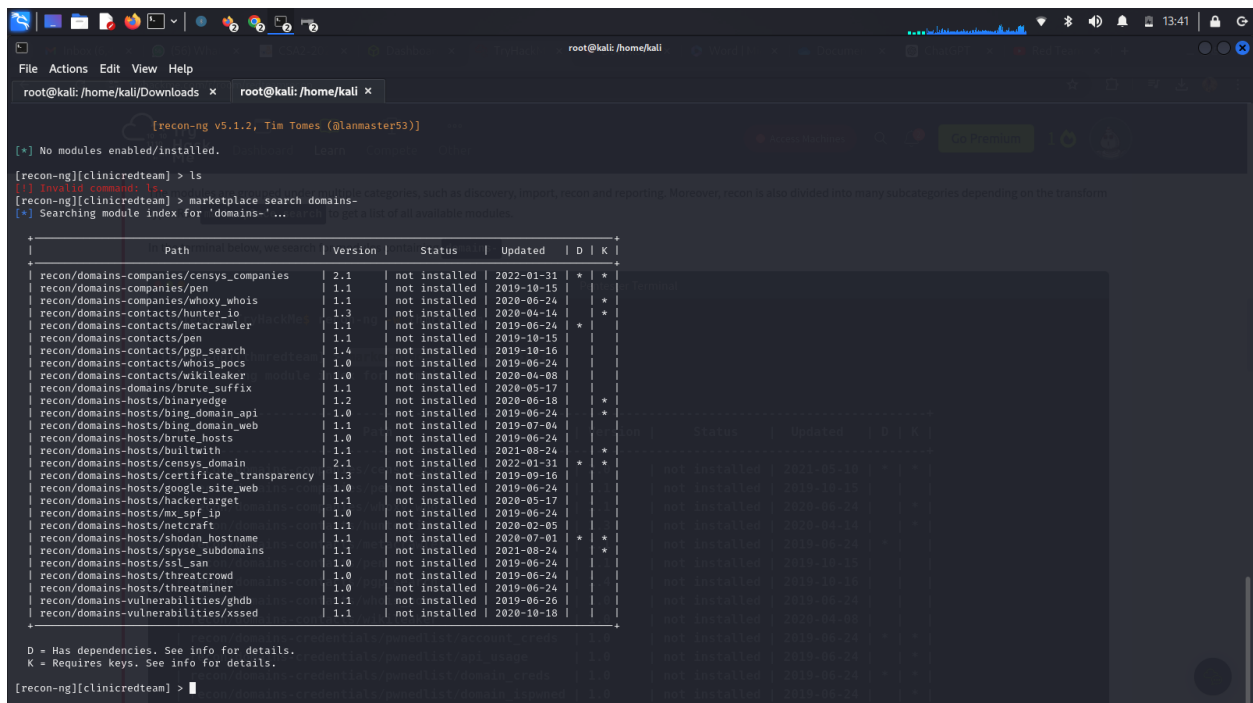
Use **parse** to analyze a file that was generated using the **download** command. It lets you filter out the fields that you're interested in, convert the JSON to a CSV and is friendly for pipe-ing to other scripts.

Example

The following command outputs the IP address, port and organization in CSV format for the previously downloaded Microsoft-IIS data:

```
$ shodan parse --fields ip_str,port,org --separator , microsoft-data.json.gz
```

```
216.28.245.171,80,Web Force Systems,  
103.61.16.147,80,  
218.244.142.211,80,China Network Information Center,  
81.22.98.166,80,Writer: Internet H12.Ltd.Sti.,  
75.149.30.139,443,Comeau's Business Communications,  
23.108.235.205,80,Mobis Technology Group, LLC,  
207.57.69.157,8080,Verio Web Hosting,  
66.129.113.13,80,Peak 10,  
168.149.6.120,8080,Verio Web Hosting,  
218.0.2.54,80,China Telecom Ningbo,  
104.202.81.231,80,  
98.191.178.20,443,Cox Communications,
```



cs-sa07-24019
John_Mbithi_Mutave

The screenshot shows the TryHackMe website interface. The browser's address bar displays `tryhackme.com/r/room/redteamrecon`. The navigation bar includes links for Dashboard, Learn, Compete, and Other, along with buttons for Access Machines, Go Premium, and a user profile icon. The main content area features a quiz titled "Using Maltego requires activation, even if you opt for Maltego CE (Community Edition). Therefore, the following questions can be answered by visiting Maltego Transform Hub or by installing and activating Maltego CE on your own system (not on the AttackBox).". Below this, there are two questions with input fields and buttons for "Correct Answer" and "Hint".

Answer the questions below

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

NIST NVD

✓ Correct Answer

🔍 Hint

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

MISP Project

✓ Correct Answer

🔍 Hint

Task 8 Summary

Created by	Room Type	Users In Room	Created
	Free Room. Anyone can deploy virtual machines in the room (without being subscribed)!	78,156	891 days ago

Copyright TryHackMe 2018-2024

The screenshot shows the TryHackMe website interface with a "Congratulations!" modal displayed. The modal text reads: "You've completed the room! Share this with your friends:". Below this text are three buttons for sharing: Twitter, Facebook, and LinkedIn. A "Leave feedback" link is also present. The background shows the "Red Team Recon" room page, which includes a list of tasks: Task 1 Introduction, Task 2 Taxonomy of Reconnaissance, Task 3 Built-in Tools, Task 4 Advanced Searching, and Task 5 Specialized Search Engines.

Red Teaming > Initial Access > Red Team Recon

Red Team Recon

Learn how to use DNS, and more. Easy 120 min

Start AttackBox Help

Congratulations!

You've completed the room! Share this with your friends:

Twitter Facebook LinkedIn

Leave feedback

Task 1 Introduction

Task 2 Taxonomy of Reconnaissance

Task 3 Built-in Tools

Task 4 Advanced Searching

Task 5 Specialized Search Engines

Shareable link: <http://www.tryhackme.com/r/room/redteamrecon>

Conclusion

We have reviewed essential built-in tools such as **whois**, **dig**, and **tracert**. Moreover, we explored the power of search engines to aid in our passive reconnaissance activities. Finally, we demonstrated two tools, Recon-ng and Maltego, that allow us to collect information from various sources and present them in one place.

The purpose is to expand our knowledge about the target and collect various information that can be leveraged in the subsequent attack phases. For instance, hosts that are discovered can be scanned and probed for vulnerabilities, while contact information and email addresses can be used to launch phishing campaigns efficiently. In brief, the more information we gather about the target, the more we can refine our attacks and increase our chances of success.