**Passive Reconnaissance**

1. **Nội dung học**

A close up of a sign

Description automatically generated

A white background with black text

Description automatically generated

1. **Passive Versus Active Recon**

* Passive Reconnaissance: thu thập các thông tin public
* Active Reconnaissance: thu thập các thông tin cụ thể, riêng tư hơn
* You visit the Facebook page of the target company, hoping to get some of their employee names. What kind of reconnaissance activity is this? (A for active, P for passive)

P

* You ping the IP address of the company webserver to check if ICMP traffic is blocked. What kind of reconnaissance activity is this? (A for active, P for passive)

A

* You happen to meet the IT administrator of the target company at a party. You try to use social engineering to get more information about their systems and network infrastructure. What kind of reconnaissance activity is this? (A for active, P for passive)

A

1. **Whois**

Truy vấn các thông tin đăng ký của tên miền

* When was TryHackMe.com registered?

20180705

A screen shot of a computer

Description automatically generated



* What is the registrar of TryHackMe.com?

namecheap.com

A computer screen with white text

Description automatically generated



* Which company is TryHackMe.com using for name servers?

cloudflare.com

A computer screen shot of a computer

Description automatically generated



1. **Nslookup and dig**

Nslookup: tra cứu địa chỉ IP của tên miền

Dig: thu thập tên miền

* Check the TXT records of thmlabs.com. What is the flag there?

THM{a5b83929888ed36acb0272971e438d78}

A computer screen shot of a code

Description automatically generated



1. **DNSDumpster**

* Lookup tryhackme.com on DNSDumpster. What is one interesting subdomain that you would discover in addition to www and blog?

remote

A screenshot of a computer

Description automatically generated



1. **Shodan.io**

* According to Shodan.io, what is the 2nd country in the world in terms of the number of publicly accessible Apache servers?

Germany

* Based on Shodan.io, what is the 3rd most common port used for Apache?

8080

* Based on Shodan.io, what is the 3rd most common port used for nginx?

5001