ASSIGNMENT 2: PASSIVE RECONNAISSANCE WRITEUP

Introduction

This module focuses on passive reconnaissance, which involves gathering information about a target without directly engaging with it. It begins with defining passive reconnaissance in comparison to active reconnaissance.

We then explored three command-line tools: whois, nslookup, and dig. he whois tool allows us to query WHOIS servers, providing information about the registered owner, contact details, and other details of a domain or IP address. With nslookup and dig, we can query DNS servers and retrieve DNS database records, such as IP addresses, domain names, and more. These tools utilize publicly available records, ensuring that our reconnaissance activities remain discreet.

Additionally, we will explore the usage of two online services: DNSDumpster and Shodan.io. These services offer valuable insights into our target without the need for direct connections.

Task 2: Passive vs Active Reconnaissance (recon)

In this task, we examined the definition of passive reconnaissance which can be defined as preliminary survey to gather information about a target while active reconnaissance is defined as requiring direct engagement with the target.

Task 2 Questions

Question 1: 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

Question 2: 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

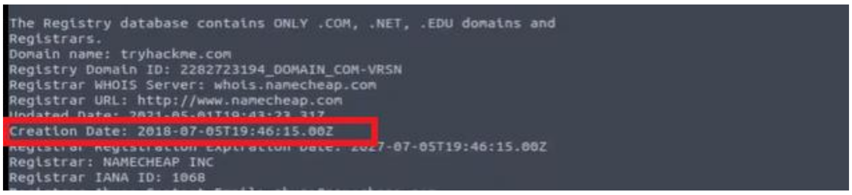
Question 3: You happen to meet the IT administrator of the target company at a party. You try to use social engineering to get more information about their systems and network infrastructure. What kind of reconnaissance activity is this? (A for active, P for passive) A

Task 3: Whois

In this task, we explore the Whois which is a request and response protocol that follows RFC 3912 specification.

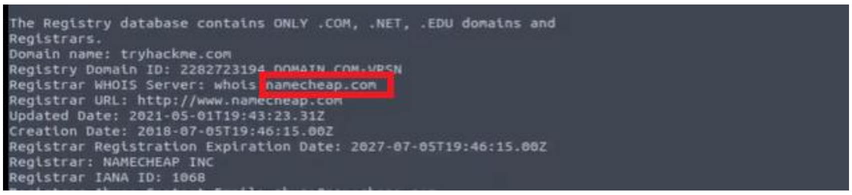
Task 3 Questions

Question 1: When was TryHackMe.com registered? 20180705



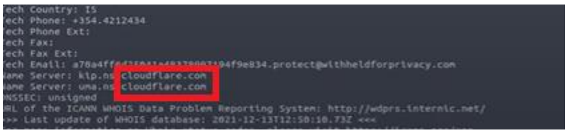
```
The Registry database contains ONLY .COM, .NET, .EDU domains and
Registrars.
Domain name: tryhackme.com
Registry Domain ID: 2282723194_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.namecheap.com
Registrar URL: http://www.namecheap.com
Updated Date: 2021-05-01T19:43:23.31Z
Creation Date: 2018-07-05T19:46:15.00Z
Registrar Registration Expiration Date: 2027-07-05T19:46:15.00Z
Registrar: NAMECHEAP INC
Registrar IANA ID: 1068
```

Question 2: What is the registrar of TryHackMe.com? namecheap.com



```
The Registry database contains ONLY .COM, .NET, .EDU domains and
Registrars.
Domain name: tryhackme.com
Registry Domain ID: 2282723194_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.namecheap.com
Registrar URL: http://www.namecheap.com
Updated Date: 2021-05-01T19:43:23.31Z
Creation Date: 2018-07-05T19:46:15.00Z
Registrar Registration Expiration Date: 2027-07-05T19:46:15.00Z
Registrar: NAMECHEAP INC
Registrar IANA ID: 1068
```

Question 3: Which company is TryHackMe.com using for name servers? Cloudflare.com

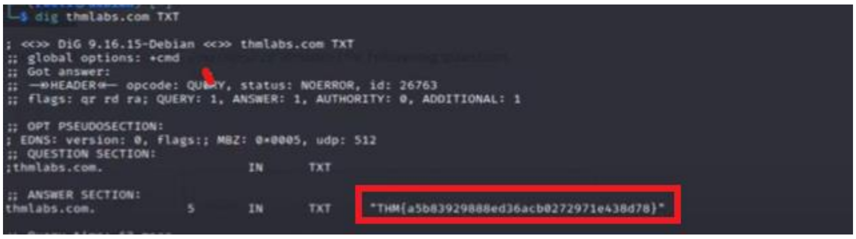


```
ech Country: IS
ech Phone: +354.4212434
ech Phone Ext:
ech Fax:
ech Fax Ext:
ech Email: a78a4ff[illegible]94f9e834.protect@withheldforprivacy.com
ame Server: kip.ns.cloudflare.com
ame Server: uma.ns.cloudflare.com
NSSEC: unsigned
RL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/
>> Last update of WHOIS database: 2021-12-13T12:58:18.73Z <<<
```

Task 4: nslookup and dig

In this task, we examined the nslookup to find the IP adresss of a domain name and dig (Domain Information Groper) to look up the MX records and we then compared the two.

Task 4 Question: Check the TXT records of thmlabs.com. What is the flag there? THM{a5b83929888ed36acb0272971e438d78}



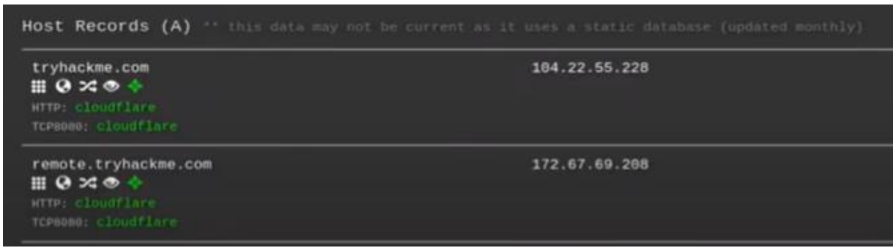
```
└─$ dig thmlabs.com TXT

; <<>> DiG 9.16.15-Debian <<>> thmlabs.com TXT
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 26763
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; MBZ: 0x0005, udp: 512
;; QUESTION SECTION:
;thmlabs.com.                   IN      TXT

;; ANSWER SECTION:
thmlabs.com.            5       IN      TXT     "THM{a5b83929888ed36acb0272971e438d78}"
```

Task 5: DNSDumpster

In this task we then looked at the DNSDumpter, an online service that offers detailed answers to DNS queries to avoid such a time-consuming search.

Task 5 Question:

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



```
Host Records (A) ** this data may not be current as it uses a static database (updated monthly)

tryhackme.com                                          104.22.55.228
HTTP: cloudflare
TCP8080: cloudflare

remote.tryhackme.com                                   172.67.69.208
HTTP: cloudflare
TCP8080: cloudflare
```

Task 6: Shodan.io

In this task, we went through shodan.io service and how it can be helpful in passive recon. Shodan.io enables users to search for specific devices or services based on various criteria, including geolocation, device type, operating system, open ports, and vulnerabilities. It provides information about the devices it discovers, including IP addresses, hostnames, organization details, and even screenshots of web interfaces when available.

Task 6 Questions

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? 8888

Conclusion

In conclusion, this module has provided me with a comprehensive understanding of gathering information about a target network discreetlyWe have explored the definitions of passive reconnaissance and active reconnaissance, and through the command-line tools whois, nslookup, and dig, we have acquired the ability to query WHOIS and DNS servers, retrieving essential details about domain names, IP addresses, and registered owners. Moreover, by utilizing the online services DNSDumpster and Shodan.io, we have gained valuable insights into our target network without the need for direct connections.

100%

Task 1 ✓ Introduction

Task 2 ✓ Passive Versus Active Recon

Task 3 ✓ Whois

Task 4 ✓ nslookup and dig

Task 5 ✓ DNSDumpster

Task 6 ✓ Shodan.io

Task 7 ✓ Summary