Passive Reconnaissance

Task 1 Introduction (Görev 1 Giriş)

1. Passive Reconnaissance (Pasif Keşif)
2. Active Reconnaissance (Aktif Keşif)
3. Nmap Live Host Discovery (Nmap Canlı Konak Keşfi)
4. Nmap Basic Port Scans (Nmap Temel Port Taramaları)
5. Nmap Advanced Port Scans (Nmap Gelişmiş Port Taramaları)
6. Nmap Post Port Scans (Nmap Post Port Taramaları)
7. Protocols and Servers (Protokoller ve Sunucular)
8. Protocols and Servers 2 (Protokoller ve Sunucular 2)
9. Network Security Challenge (Ağ Güvenliği Mücadelesi)

Bu odada, pasif keşif ve aktif keşfi tanımladıktan sonra, pasif keşifle ilgili temel araçlara odaklanıyoruz. Üç komut satırı aracını öğreneceğiz:

WHOIS ⇒ sunucularını sorgulamak için whois

nslookup ⇒ DNS sunucularını sorgulamak için nslookup

dig ⇒ DNS sunucularını sorgulamak için kazma

WHOIS kayıtlarını sorgulamak için whois kullanırken, DNS veritabanı kayıtlarını sorgulamak için nslookup ve dig kullanıyoruz. Bunların hepsi halka açık kayıtlardır ve bu nedenle hedefi uyarmazlar.

Ayrıca iki çevrimiçi hizmetin kullanımını da öğreneceğiz:

- DNSDumpster
- Shodan.io

Bu iki çevrimiçi hizmet, doğrudan hedefimize bağlanmadan hedefimiz hakkında bilgi toplamamıza olanak tanır.

Önkoşullar: Bu oda, komut satırına temel aşinalık ile birlikte temel ağ bilgisi gerektirir. Network Fundamentals ve Linux Fundamentals modülleri gerektiğinde gerekli bilgiyi sağlar.

Önemli Uyarı: Abone değilseniz, AttackBox'ın İnternet erişimi olmayacağını, bu nedenle İnternet erişimi gerektiren soruları tamamlamak için VPN kullanmanız gerekeceğini lütfen unutmayın.

soru ⇒ Bu oda, tartışılan konuları göstermek için bir hedef sanal makine (VM) kullanmaz. Bunun yerine, TryHackMe'nin sahip olduğu alan adları için genel WHOIS sunucularını ve DNS sunucularını sorgulayacağız. AttackBox'ı başlatın ve hazır olduğundan emin olun. AttackBox'ı daha sonraki görevlerde, özellikle de 3. ve 4. görevlerde soruları yanıtlamak için kullanacaksınız.

Cevap ⇒ Cevap Gerekmemektedir.

Task 2 Passive Versus Active Recon (Görev 2 Pasif Versus Aktif Keşif)

Bu oda, kullanıcının bilgisayar ağları hakkında çalışma bilgisine sahip olmasını bekler. Bu konuyu tazelemek isterseniz, önce Ağ Temelleri modülünü çalışmanız önerilir.

Bilgisayar sistemleri ve ağları ortaya çıkmadan önce, Sun Tzu Savaş Sanatı'nda "Düşmanı ve kendinizi tanırsanız, zaferiniz şüphe götürmez" diye öğretiyordu. Eğer saldırgan rolünü oynuyorsanız, hedef sistemleriniz hakkında bilgi toplamanız gerekir. Savunmacı rolünü oynuyorsanız, düşmanınızın sistemleriniz ve ağlarınız hakkında neler keşfedeceğini bilmeniz gerekir.

Keşif (recon) bir hedef hakkında bilgi toplamak için yapılan ön araştırma olarak tanımlanabilir. Bir sistem üzerinde ilk dayanak noktasını elde etmek için Birleşik Öldürme Zinciri'nin ilk adımıdır. Keşfi şu bölümlere ayırıyoruz:

1. Passive Reconnaissance (Pasif Keşif)
2. Active Reconnaissance (Aktif Keşif)

Pasif keşifte, kamuya açık bilgilere güvenirsiniz. Bu, hedefle doğrudan etkileşime girmeden kamuya açık kaynaklardan erişebileceğiniz bilgidir. Bunu, hedef bölgeye ayak basmadan uzaktan bakıyormuşsunuz gibi düşünün.

Pasif keşif faaliyetleri birçok faaliyeti içerir, örneğin:

- Genel bir DNS sunucusundan bir alan adının DNS kayıtlarını aramak.
- Hedef web sitesi ile ilgili iş ilanlarının kontrol edilmesi.
- Hedef şirket hakkında haber makaleleri okumak.

Öte yandan, aktif keşif bu kadar gizli bir şekilde gerçekleştirilemez. Hedefle doğrudan temas gerektirir. Bunu, diğer potansiyel giriş noktalarının yanı sıra kapı ve pencerelerdeki kilitleri kontrol etmek gibi düşünün.

Aktif keşif faaliyetlerine örnek olarak şunlar verilebilir:

- HTTP, FTP ve SMTP gibi şirket sunucularından birine bağlanma.
- Bilgi almak amacıyla şirketi aramak (sosyal mühendislik).
- Tamirci gibi davranarak şirket tesislerine girmek.

Aktif keşif faaliyetinin istilacı doğası göz önünde bulundurulduğunda, uygun yasal izin alınmadığı takdirde yasal sorunlarla karşılaşmak işten bile değildir.

Sorular

Soru ⇒ Hedef şirketin Facebook sayfasını ziyaret ederek bazı çalışanlarının isimlerini öğrenmeyi umuyorsunuz. Bu ne tür bir keşif faaliyetidir? (Aktif için A, pasif için P)

Cevap ⇒ P

Soru ⇒ ICMP trafiğinin engellenip engellenmediğini kontrol etmek için şirket web sunucusunun IP adresine ping atıyorsunuz. Bu ne tür bir keşif faaliyetidir? (Aktif için A, pasif için P)

Cevap ⇒ A

Soru ⇒ Bir partide hedef şirketin BT yöneticisiyle tanışıyorsunuz. Sistemleri ve ağ altyapıları hakkında daha fazla bilgi almak için sosyal mühendislik kullanmaya çalışıyorsunuz. Bu ne tür bir keşif faaliyetidir? (Aktif için A, pasif için P)

Cevap ⇒ A

Task 3 Whois (Görev 3 Whois)

WHOIS, RFC 3912 spesifikasyonunu takip eden bir istek ve yanıt protokolüdür. Bir WHOIS sunucusu, gelen talepler için TCP bağlantı noktası 43'ü dinler. Alan adı kayıt kuruluşu, kiraladığı alan adları için WHOIS kayıtlarının tutulmasından sorumludur. WHOIS sunucusu, talep edilen alan adıyla ilgili çeşitli bilgilerle yanıt verir. Özellikle ilgi çekici olanları öğrenebiliriz:

- Kayıt Şirketi: Alan adı hangi kayıt kuruluşu aracılığıyla kaydedildi?
- Kayıt sahibinin iletişim bilgileri: Diğer şeylerin yanı sıra ad, kuruluş, adres, telefon. (bir gizlilik hizmeti aracılığıyla gizli hale getirilmediği sürece)
- Oluşturma, güncelleme ve sona erme tarihleri: Alan adı ilk ne zaman kaydedildi? En son ne zaman güncellendi? Ve ne zaman yenilenmesi gerekiyor?
- İsim Sunucusu: Alan adını çözümlemek için hangi sunucuya sorulmalı?

Bu bilgiyi almak için bir whois istemcisi veya çevrimiçi bir hizmet kullanmamız gerekir. Birçok çevrimiçi hizmet whois bilgilerini sağlar; ancak, yerel whois istemcinizi kullanmak genellikle daha hızlı ve daha kullanışlıdır. AttackBox'ı (ya da Parrot veya Kali gibi yerel Linux makinenizi) kullanarak, whois istemcinize terminalden kolayca erişebilirsiniz. Sözdizimi whois DOMAIN_NAME şeklindedir, burada DOMAIN_NAME hakkında daha fazla bilgi almaya çalıştığınız etki alanıdır. Aşağıdaki whois tryhackme.com çalıştırma örneğini göz önünde bulundurun.

```
user@TryHackMe$ whois tryhackme.com[Querying whois.verisign-grs.com]
[Redirected to whois.namecheap.com]
[Querying whois.namecheap.com]
```

```
[whois.namecheap.com]
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
Registrar Abuse Contact Email: abuse@namecheap.com
Registrar Abuse Contact Phone: +1.6613102107
Reseller: NAMECHEAP INC
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferP
rohibited
Registry Registrant ID:
Registrant Name: Withheld for Privacy Purposes
Registrant Organization: Privacy service provided by Withheld for Privacy ehf
[...]
URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.intern
ic.net/
>>> Last update of WHOIS database: 2021-08-25T14:58:29.57Z <<<
For more information on Whois status codes, please visit https://icann.org/ep
p
```

Çok sayıda bilgi görebiliyoruz; bunları görüntülenen sırayla inceleyeceğiz. İlk olarak, bilgilerimizi almak için whois.namecheap.com adresine yönlendirildiğimizi fark ediyoruz. Bu durumda ve şu anda, namecheap.com bu alan adı için WHOIS kaydını tutuyor. Ayrıca, oluşturma tarihi ile birlikte son güncelleme tarihi ve son kullanma tarihini de görebiliyoruz.

Daha sonra, kayıt kuruluşu ve kayıt sahibi hakkında bilgi ediniriz. Herhangi bir gizlilik hizmeti kullanmıyorlarsa, alan adı sahibinin adını ve iletişim bilgilerini bulabiliriz. Yukarıda gösterilmemesine rağmen, bu alan adı için yönetici ve teknik irtibat kişilerini alıyoruz. Son olarak, bakmamız gereken herhangi bir DNS kaydı varsa sorgulamamız gereken alan adı sunucularını görüyoruz.

E-posta adreslerini toplamak için WHOIS sorgularını kötüye kullanan otomatik araçlar nedeniyle, birçok WHOIS hizmetinin buna karşı önlem aldığını belirtmek önemlidir. Örneğin, e-posta adreslerini redakte edebilirler. Ayrıca, birçok kayıt sahibi e-posta adreslerinin spam gönderenler tarafından toplanmasını önlemek ve bilgilerini gizli tutmak için gizlilik hizmetlerine abone olur.

AttackBox'ta terminali açın ve aşağıdaki soruları yanıtlamak için ihtiyacınız olan bilgileri almak üzere whois tryhackme.com komutunu çalıştırın.

Sorular ⇒

Soru ⇒ TryHackMe.com ne zaman tescil edildi (İpucu ⇒ YYYYMMDD biçimini kullanın)?

Cevap ⇒ 20180705

Soru ⇒ TryHackMe.com'un kayıt kuruluşu nedir(İpucu ⇒ Alan adını verin)?

Cevap ⇒ namecheap.com

Soru ⇒ TryHackMe.com isim sunucuları için hangi şirketi kullanıyor(İpucu ⇒ Alan adını verin)?

Cevap ⇒ cloudflare.com

Task 4 nslookup and dig (Görev 4 nslookup ve dig)

Bir önceki görevde, aradığımız alan adı hakkında çeşitli bilgiler almak için WHOIS protokolünü kullandık. Özellikle, kayıt şirketinden DNS sunucularını alabildik.

İsim Sunucusu Arama anlamına gelen nslookup'ı kullanarak bir alan adının IP adresini bulun. Örneğin, nslookup tryhackme.com gibi nslookup DOMAIN_NAME komutunu vermeniz gerekir. Ya da daha genel olarak nslookup OPTIONS DOMAIN_NAME SERVER kullanabilirsiniz. Bu üç ana parametre şunlardır:

- OPTIONS aşağıdaki tabloda gösterildiği gibi sorgu türünü içerir. Örneğin, IPv4 adresleri için A ve IPv6 adresleri için AAAA kullanabilirsiniz.
- DOMAIN_NAME aradığınız alan adıdır.

- SERVER, sorgulamak istediğiniz DNS sunucusudur. Sorgulamak için herhangi bir yerel veya genel DNS sunucusu seçebilirsiniz. Cloudflare 1.1.1.1 ve 1.0.0.1, Google 8.8.8.8 ve 8.8.4.4 ve Quad9 9.9.9.9 ve 149.112.112.112 sunar. ISP'nizin DNS sunucularına alternatifler istiyorsanız, aralarından seçim yapabileceğiniz daha birçok genel DNS sunucusu vardır.

Query type	Result
A	IPv4 Addresses
AAAA	IPv6 Addresses
CNAME	Canonical Name
MX	Mail Servers
SOA	Start of Authority
TXT	TXT Records

Örneğin, tryhackme.com tarafından kullanılan tüm IPv4 adreslerini döndürmek için nslookup -type=A tryhackme.com 1.1.1.1 (veya büyük/küçük harfe duyarlı olmadığı için nslookup -type=a tryhackme.com 1.1.1.1) kullanılabilir.

```
user@TryHackMe$ nslookup -type=A tryhackme.com 1.1.1.1Server:         1.1.1.1
Address: 1.1.1.1#53

Non-authoritative answer:
Name: tryhackme.com
Address: 172.67.69.208
Name: tryhackme.com
Address: 104.26.11.229
Name: tryhackme.com
Address: 104.26.10.229
```

A ve AAAA kayıtları sırasıyla IPv4 ve IPv6 adreslerini döndürmek için kullanılır. Bu aramayı sızma testi açısından bilmek faydalıdır. Yukarıdaki örnekte, bir alan adı ile başladık ve üç IPv4 adresi elde ettik. Bu IP adreslerinin her biri, sızma testinin kapsamı dahilinde oldukları varsayılarak, güvensizlikler açısından daha fazla kontrol edilebilir.

Diyelim ki belirli bir alan adı için e-posta sunucuları ve yapılandırmaları hakkında bilgi edinmek istiyorsunuz. nslookup -type=MX tryhackme.com komutunu verebilirsiniz. İşte bir örnek:

```
user@TryHackMe$ nslookup -type=MX tryhackme.comServer:      127.0.0.53
Address: 127.0.0.53#53

Non-authoritative answer:
tryhackme.com  mail exchanger = 5 alt1.aspmx.l.google.com.
tryhackme.com  mail exchanger = 1 aspmx.l.google.com.
tryhackme.com  mail exchanger = 10 alt4.aspmx.l.google.com.
tryhackme.com  mail exchanger = 10 alt3.aspmx.l.google.com.
tryhackme.com  mail exchanger = 5 alt2.aspmx.l.google.com.
```

tryhackme.com'un mevcut e-posta yapılandırmasının Google'ı kullandığını görebiliriz. MX, Posta Değişim sunucularını aradığından, bir posta sunucusu @tryhackme.com adresine e-posta göndermeye çalıştığında, 1. sıradaki aspmx.l.google.com adresine bağlanmaya çalışacağını fark ediyoruz. Meşgulse veya kullanılamıyorsa, posta sunucusu bir sonraki sıradaki posta değişim sunucularına bağlanmayı deneyecektir, alt1.aspmx.l.google.com veya alt2.aspmx.l.google.com.

Listelenen posta sunucularını Google sağlar; bu nedenle, posta sunucularının güvenlik açığı olan bir sunucu sürümü çalıştırmasını beklememeliyiz. Ancak, diğer durumlarda, yeterince güvenli olmayan veya yamalanmamış posta sunucuları bulabiliriz.

Bu tür bilgiler, hedefinizin pasif keşfine devam ederken değerli olabilir. Benzer sorguları diğer alan adları için de tekrarlayabilir ve -type=txt gibi farklı türleri deneyebilirsiniz. Yolunuz boyunca ne tür bilgiler keşfedebileceğinizi kim bilebilir!

Daha gelişmiş DNS sorguları ve ek işlevler için, merak ediyorsanız "Domain Information Groper "ın kısaltması olan dig'i kullanabilirsiniz. MX kayıtlarını aramak ve nslookup ile karşılaştırmak için dig kullanalım. dig DOMAIN_NAME kullanabiliriz, ancak kayıt türünü belirtmek için dig DOMAIN_NAME TYPE kullanacağız. İsteğe bağlı olarak, dig @SERVER DOMAIN_NAME TYPE kullanarak sorgulamak istediğimiz sunucuyu seçebiliriz.

- SERVER, sorgulamak istediğiniz DNS sunucusudur.
- DOMAIN_NAME aradığınız alan adıdır.
- TYPE, daha önce verilen tabloda gösterildiği gibi DNS kayıt türünü içerir.

```
user@TryHackMe$ dig tryhackme.com MX; <<>> DiG 9.16.19-RH <<>> tryhac
kme.com MX
;; global options: +cmd
;; Got answer:
;; ->>HEADER<
```

nslookup ve dig çıktıları arasında hızlı bir karşılaştırma yapıldığında, dig'in varsayılan olarak TTL (Time To Live) gibi daha fazla bilgi döndürdüğü görülür. Eğer 1.1.1.1 DNS sunucusunu sorgulamak istiyorsanız, dig @1.1.1.1 tryhackme.com MX komutunu çalıştırabilirsiniz.

AttackBox'ı kullanarak terminali açın ve aşağıdaki soruyu yanıtlamak için ihtiyacınız olan bilgileri almak üzere nslookup veya dig komutunu kullanın.

Soru ⇒ thmlabs.com'un TXT kayıtlarını kontrol edin. Oradaki bayrak nedir?

Cevap ⇒ THM{a5b83929888ed36acb0272971e438d78}

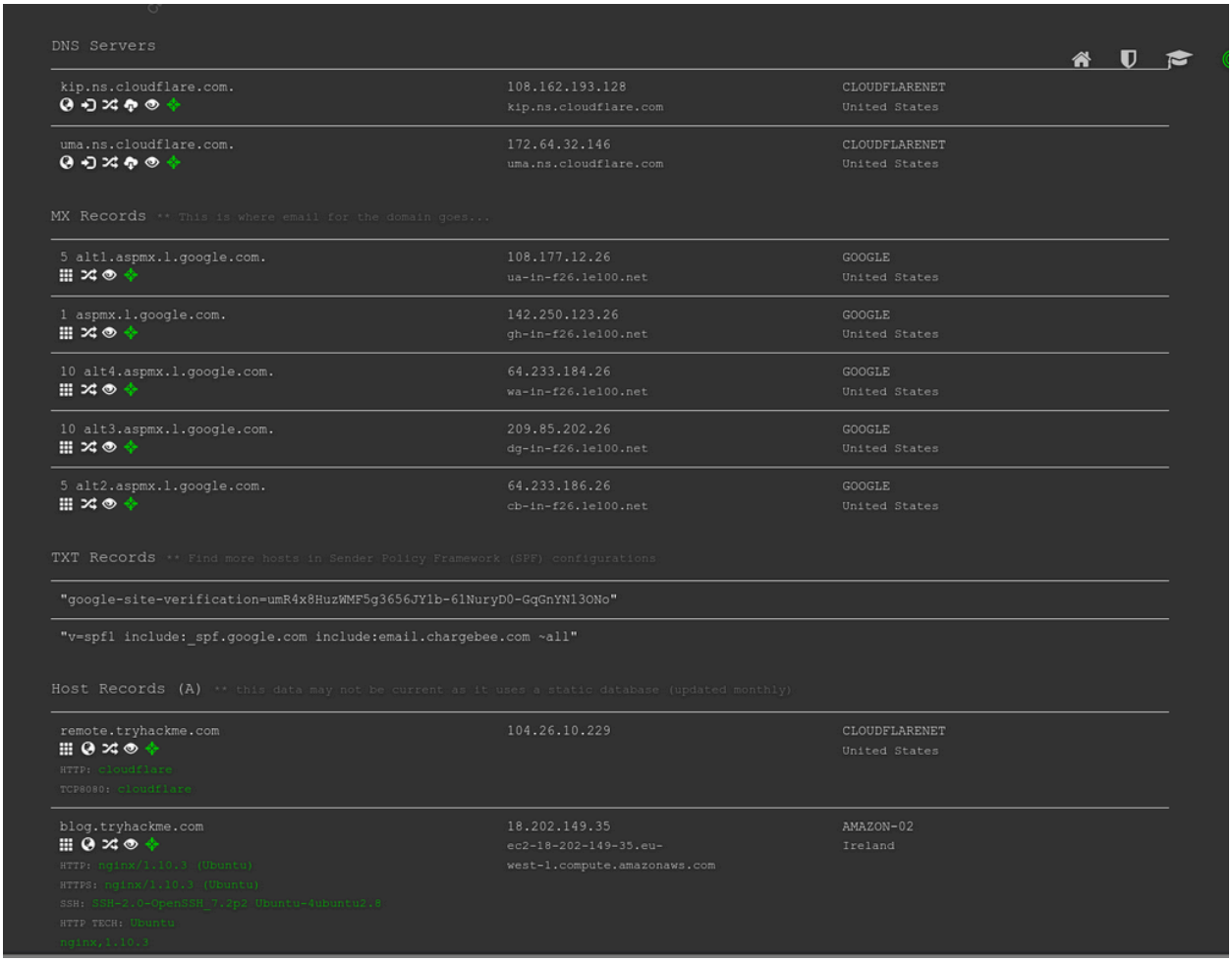
Task 5 DNSDumpster (Görev 5 DNSDumpster)

nslookup ve dig gibi DNS arama araçları alt alan adlarını kendi başlarına bulamazlar. İncelediğiniz alan adı, hedef hakkında çok fazla bilgi verebilecek farklı bir alt alan adı içerebilir. Örneğin, tryhackme.com wiki.tryhackme.com ve webmail.tryhackme.com alt alan adlarına sahipse, hedefiniz hakkında bilgi hazinesi barındırabilecekleri için bu ikisi hakkında daha fazla bilgi edinmek istersiniz. Bu alt alan adlarından birinin kurulmuş olması ve düzenli olarak güncellenmemesi ihtimali vardır. Düzenli güncellemelerin yapılmaması genellikle hizmetlerin savunmasız kalmasına neden olur. Peki bu tür alt alan adlarının var olduğunu nasıl bilebiliriz?

Herkesçe bilinen alt alan adlarının bir listesini derlemek için birden fazla arama motoru kullanmayı düşünebiliriz. Tek bir arama motoru yeterli olmayacaktır; dahası, ilginç veriler bulmak için en az onlarca sonucu gözden geçirmeyi beklemeliyiz. Sonuçta, açıkça reklamı yapılmayan alt alan adlarını arıyorsunuz ve bu nedenle arama sonuçlarının ilk sayfasına ulaşmak gerekli değildir. Bu tür alt alan adlarını keşfetmek için başka bir yaklaşım, hangi alt alan adlarının DNS kayıtlarına sahip olduğunu bulmak için kaba zorlama sorgularına güvenmek olacaktır.

Bu kadar zaman alan bir aramadan kaçınmak için, DNSDumpster gibi DNS sorgularına ayrıntılı yanıtlar sunan çevrimiçi bir hizmet kullanılabilir. DNSDumpster'da tryhackme.com için arama yaparsak, tipik bir DNS sorgusunun sağlayamayacağı blog.tryhackme.com alt alan adını keşfedeceğiz. Buna ek olarak, DNSDumpster toplanan DNS bilgilerini okunması kolay tablolar ve bir grafik halinde geri gönderecektir. DNSDumpster ayrıca dinleme sunucuları hakkında toplanan tüm bilgileri de sağlayacaktır.

Beklenen çıktıya bir göz atmak için DNSDumpster'da tryhackme.com için arama yapacağız. Sonuçlar arasında, aradığımız alan adı için DNS sunucularının bir listesini aldık. DNSDumpster ayrıca alan adlarını IP adreslerine çözümledi ve hatta coğrafi konumlarını belirlemeye çalıştı. MX kayıtlarını da görebiliyoruz; DNSDumpster beş posta değişim sunucusunu da ilgili IP adreslerine çözümledi ve sahip ve konum hakkında daha fazla bilgi sağladı. Son olarak, TXT kayıtlarını görebiliriz. Pratikte tüm bu bilgileri almak için tek bir sorgu yeterliydi.



DNS Servers

kip.ns.cloudflare.com.	108.162.193.128 kip.ns.cloudflare.com	CLOUDFLARENET United States
uma.ns.cloudflare.com.	172.64.32.146 uma.ns.cloudflare.com	CLOUDFLARENET United States

MX Records ** This is where email for the domain goes...

5 alt1.aspmx.l.google.com.	108.177.12.26 ua-in-f26.1e100.net	GOOGLE United States
1 aspmx.l.google.com.	142.250.123.26 gh-in-f26.1e100.net	GOOGLE United States
10 alt4.aspmx.l.google.com.	64.233.184.26 wa-in-f26.1e100.net	GOOGLE United States
10 alt3.aspmx.l.google.com.	209.85.202.26 dg-in-f26.1e100.net	GOOGLE United States
5 alt2.aspmx.l.google.com.	64.233.186.26 cb-in-f26.1e100.net	GOOGLE United States

TXT Records ** Find more hosts in Sender Policy Framework (SPF) configurations

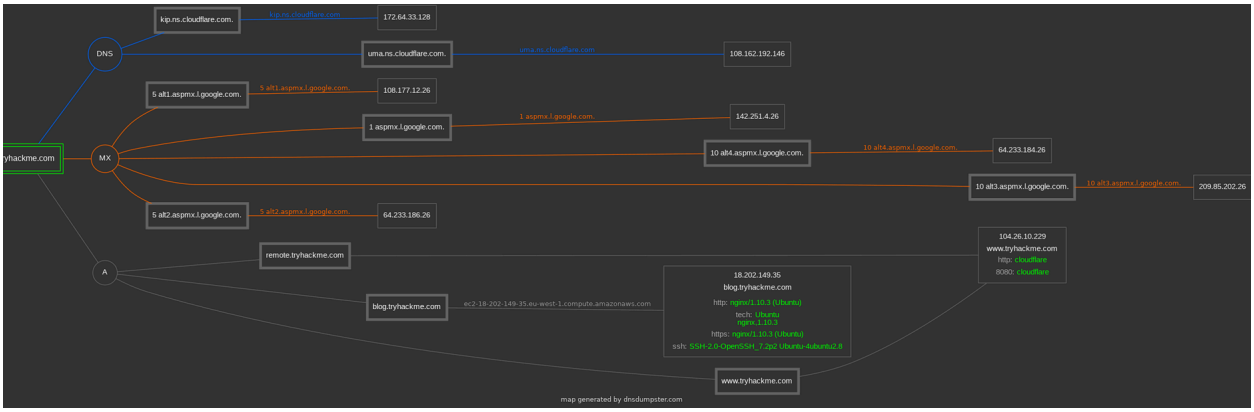
"google-site-verification=umR4x8HuzWMF5g3656JY1b-61NuryD0-GqGnYN13ONo"

"v=spf1 include:_spf.google.com include:email.chargebee.com ~all"

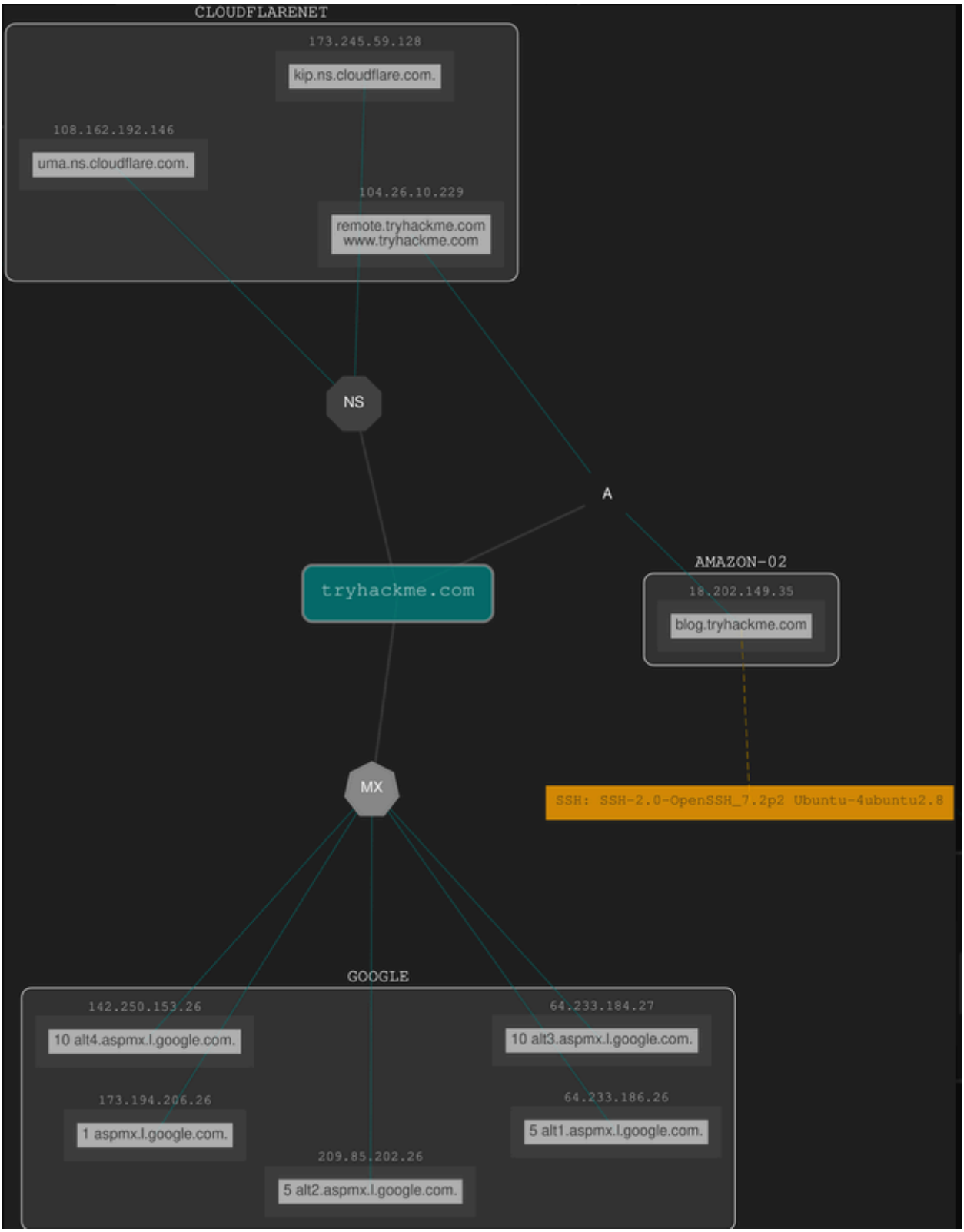
Host Records (A) ** this data may not be current as it uses a static database (updated monthly)

remote.tryhackme.com HTTP: cloudflare TCP8080: cloudflare	104.26.10.229	CLOUDFLARENET United States
blog.tryhackme.com HTTP: nginx/1.10.3 (Ubuntu) HTTPS: nginx/1.10.3 (Ubuntu) SSH: SSH-2.0-OpenSSH_7.2p2 Ubuntu-4ubuntu2.8 HTTP TECH: Ubuntu nginx,1.10.3	18.202.149.35 ec2-18-202-149-35.eu-west-1.compute.amazonaws.com	AMAZON-02 Ireland

DNSDumpster toplanan bilgileri grafik olarak da gösterir. DNSDumpster tablodaki verileri daha önce bir grafik olarak gösterdi. DNS ve MX'in kendi sunucularına dallandığını ve IP adreslerini de gösterdiğini görebilirsiniz.



Şu anda grafiği dışa aktarmanıza da olanak tanıyan bir beta özelliği var. Grafiği manipüle edebilir ve gerekirse blokları hareket ettirebilirsiniz.


CLOUDFLARENET
173.245.59.128
kip.ns.cloudflare.com.
108.162.192.146
uma.ns.cloudflare.com.
104.26.10.229
remote.tryhackme.com
www.tryhackme.com
NS
A
tryhackme.com
AMAZON-02
18.202.149.35
blog.tryhackme.com
MX
SSH: SSH-2.0-OpenSSH_7.2p2 Ubuntu-4ubuntu2.8
GOOGLE
142.250.153.26
10 alt4.aspmx.l.google.com.
64.233.184.27
10 alt3.aspmx.l.google.com.
173.194.206.26
1 aspmx.l.google.com.
64.233.186.26
5 alt1.aspmx.l.google.com.
209.85.202.26
5 alt2.aspmx.l.google.com.

Aşağıdaki soruyu yanıtlamak için AttackBox'taki veya sisteminizdeki web tarayıcısını kullanın.

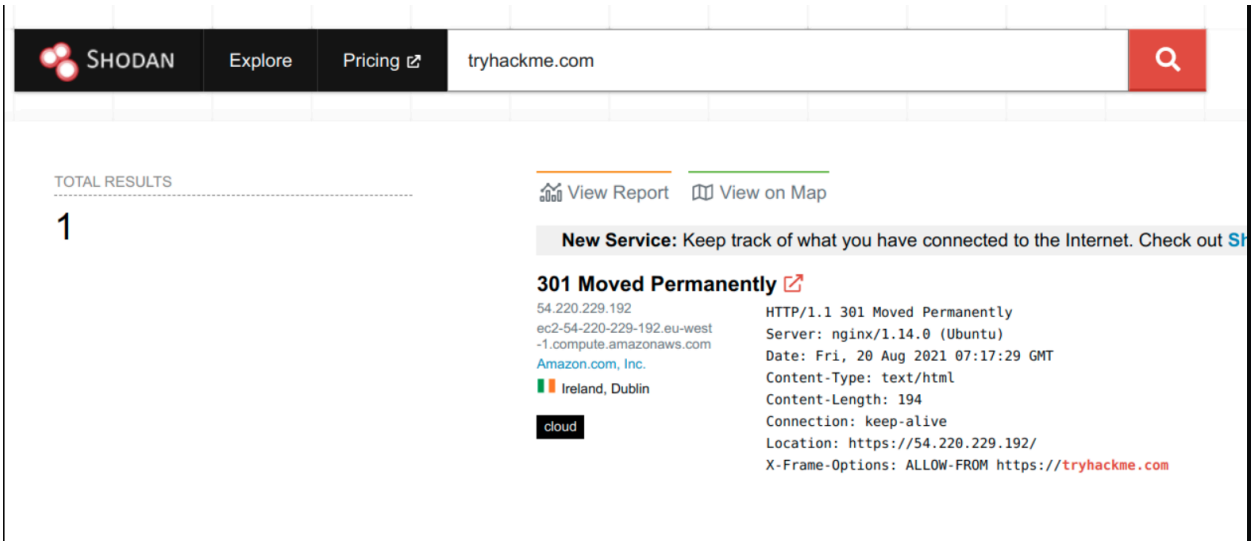
Soru ⇒ DNSDumpster'da tryhackme.com'a bakın. www ve blog'a ek olarak keşfedeceğiniz ilginç bir alt alan adı nedir?

Cevap ⇒ remote

Task 6 Shodan.io (Görev 6 Shodan.io)

Pasif keşif aşamasının bir parçası olarak belirli hedeflere karşı bir sızma testi yapmakla görevlendirildiğinizde, Shodan.io gibi bir hizmet, aktif olarak bağlanmadan müşterinin ağı hakkında çeşitli bilgileri öğrenmek için yardımcı olabilir. Ayrıca, savunma tarafında, kuruluşunuza ait bağlı ve açık cihazlar hakkında bilgi edinmek için Shodan.io'nun farklı hizmetlerini kullanabilirsiniz.

Shodan.io, web sayfaları için bir arama motorunun aksine, bağlı "şeylerin" bir arama motorunu oluşturmak için çevrimiçi olarak erişilebilen her cihaza bağlanmaya çalışır. Bir yanıt aldığında, hizmetle ilgili tüm bilgileri toplar ve aranabilir hale getirmek için veritabanına kaydeder. tryhackme.com sunucularından birinin kaydedilmiş kaydını düşünün.



Bu kayıt bir web sunucusunu gösterir; ancak, daha önce de belirtildiği gibi, Shodan.io çevrimiçi olarak bağlı bulabildiği herhangi bir cihazla ilgili bilgileri toplar.

Shodan.io üzerinde tryhackme.com araması yapmak en azından yukarıdaki ekran görüntüsünde gösterilen kaydı gösterecektir. Bu Shodan.io arama sonucu aracılığıyla, aramamızla ilgili birkaç şey öğrenebiliriz, örneğin:

- IP adresi
- barındırma şirketi
- coğrafi konum
- sunucu türü ve sürümü

DNS aramalarından elde ettiğiniz IP adreslerini aramayı da deneyebilirsiniz. Bunlar elbette daha fazla değişime tabidir. Yardım sayfalarında, Shodan.io'da bulunan tüm arama seçenekleri hakkında bilgi edinebilir ve TryHackMe'nin Shodan.io'suna katılmaya teşvik edilirsiniz.

Aşağıdaki soruları yanıtlamak için Shodan.io'yu ziyaret etmek en iyisi olacaktır; ancak, yanıtları premium hesaba ihtiyaç duymadan Shodan.io'da bulabileceğinizi unutmayın.

Sorular

Soru ⇒ Shodan.io'ya göre, halka açık Apache sunucularının sayısı bakımından dünyanın 2. ülkesi hangisidir (İpucu ⇒ Cevabı bulmak için Shodan.io'da Apache'yi arayabilirsiniz.)?

Cevap ⇒ Germany

Soru ⇒ Shodan.io'ya göre, Apache için kullanılan en yaygın 3. bağlantı noktası hangisidir (İpucu ⇒ Cevabı bulmak için Shodan.io'da Apache'yi arayabilirsiniz.)?

Cevap ⇒ 8080

Soru ⇒ Shodan.io'ya göre, nginx için kullanılan en yaygın 3. bağlantı noktası nedir(İpucu ⇒ Cevabı bulmak için Shodan.io'da nginx araması yapabilirsiniz.)?

Cevap ⇒ 5001

Task 7 Summary (Görev 7 Özet)

Bu odada pasif keşif üzerine odaklandık. Özellikle, whois, nslookup ve dig komut satırı araçlarını ele aldık. Ayrıca halka açık iki hizmet olan DNSDumpster ve Shodan.io'dan da bahsettik. Bu tür araçların gücü, hedeflerinize doğrudan bağlanmadan onlar hakkında bilgi toplayabilmenizdir. Dahası, bu tür araçları kullanarak bulabileceğiniz bilgi hazinesi, arama seçeneklerinde ustalaştığınızda ve sonuçları okumaya alıştığınızda çok büyük olabilir.

Purpose	Commandline Example
Lookup WHOIS record	`whois tryhackme.com`
Lookup DNS A records	`nslookup -type=A tryhackme.com`
Lookup DNS MX records at DNS server	`nslookup -type=MX tryhackme.com 1.1.1.1`
Lookup DNS TXT records	`nslookup -type=TXT tryhackme.com`
Lookup DNS A records	`dig tryhackme.com A`
Lookup DNS MX records at DNS server	`dig @1.1.1.1 tryhackme.com MX`
Lookup DNS TXT records	`dig tryhackme.com TXT`

DNS hakkında daha fazla bilgi için DNS in Detail.

Soru ⇒ Bu odada tartışılan tüm noktaları, özellikle de komut satırı araçlarının sözdizimini not ettiğinizden emin olun.

Cevap ⇒ Cevap Gerekmemektedir.