Information Gathering

Muhammed Fatih YILMAZ

mfth78@hotmail.com

İçerik

- Attack Surface Nedir?
- Hedefin Atak Yüzeyi Belirlenirken Neler Elde edilebilir ?
- Information Gathering ve Enumeration
- Cyber Kill Chain
- Toollar
- Migros.com.tr Information Gathering

Attack Surface Nedir?

Attack surface kısaca tanımlayacak olursak saldırılmaya müsait saldırganların yetkisiz verilere erişmesini sağlayacabilecek organizasyona ait alanlar denilebilir. Attack surface ne kadar küçük olursa saldırıların başarılı olma olsaılığı o kadar düşük olur ve yönetilmesi kolaylaşır.

2 tür attack surface vardır.

1)Dijital Surface

2)Fiziksel Surface

1) Dijital attack surface genelde organizasyonun kullanmış olduğu yazılımsal ve donanımsal ürünlerin internetten üzerinden yayınlandığı kısımlar olarak özetleyebiliriz. Yaptığımız araştırmalar neticesince burada olan açıklara göz gezdirip sızma testlerşnde elimize ne geçebilir iyice öğrenebiliriz. Dijital atak yüzeyini 3 kısma ayırabiliriz.

- Bilinen Varlıklar

  Organizasyonunuzun internete açık erişilebilir. Domain adları, name serverları ve bunlara bağlı subdomaim adları örnek olarak verilebilir.

- Bilinmeyen Varlıklar

  Bilinmeyen varlıkları unutulan veya gözden kaçırılan varlıklarda denilebilir. Örnek vermek gerekirse zamanında subdomainlerinizde farklı websiteleri veya uygulamalar yayınladınız ve artık kullanmıyorsunuz. Bu varlıklar örnek olarak verilebilir. Burada olan zafiyetler kullanmadığınızdan dolayı gözden kaçtığı için problem olşturabilir.

- Hileli Varlıklar

  Hileli varlıklar kendisini sizin gibi gösteren hackerlara ait siteler veya uygulamalara verilen addır.

2) Fiziksel attack surface kullanıcının fiziksel olarak etkileşime girdiği cihazlara erişim sağlanması, cihazlara farklı zararlı yazılım veya donanımla müdahele edilmesi fiziksel atak yüzeyine dahil edilebilir. Bu cihazlara erişşim sağlayan hackerlar serverlara, ofis sistemlerine zarar verebilir. Cihazları ele geçirebilmesi fiziksel olarak gidebilir. İçeride çalışanların flash belleklerine zararlı yazılım koyup erişebilir.

Hedefin Atak Yüzeyi Belirlenirken Neler Elde edilebilir ?

Hedefin atak yüzeyi belirlenirken hassas verilerin girip çıkabileceği yollar, authentication gerekli yerler, databaseyle etkileşimde olan pathler göz önünde bulundurulabilir. Bunlara nerelerden erişim sağlandığını öğrenmek için ise internete bağlı kayıtlı domain adresleri, internete açık portları, kullandıkları yazılımsal ve donanımsal cihazlar, organizasyonun mail adresleri kullandıkları teknolojileri yani kısaca güvenlik zafiyeti oluşturabilecek herhangi bir alan ele alınmalıdır. Web servislerinde arkada çalışan uygulamaların zafiyet kapasitesi, şirketin çalışanlarının tedbirleri denetlenebilir. Hangi subdomainlerin kullanılmadığı hangi portların gereksiz yere açık olduğu anlaşılabilir. Bu bahsettiğimiz unsurların bazılarını elde etmek için belli başlı toollar ayarlanmıştır. Tool kullanmadan da gerekli araştırmalar yapılabilir fakat işlemlerimizi kolaylaştırmak ve süreci kısaltmak açısından oldukça önemlidir.

Information Gathering ve Enumeration nedir?

İnformation gathering (bilgi toplama) araştırmalar yaparak gerekli bilgileri elde etmektir. Siber güvenlikte hedefe yönelik kafamızda bir taslak fikir oluşması için çok mühim bir konudur. Elde ettiğimiz sonuçları göz önünde bulundurarak hedefe nasıl bir yaklaşım sergileyeceğimizi belirleriz. Amaçlarımız doğrultusunda daha belirgin şekilde ilerleyebiliriz.

Enumeration temelde saymaktır. Bilgi toplama aşamasından sonra hedef sistem hakkında daha kapsamlı bilginin elde edilmeye çalışıldığı aşamadır. Hedefe bağlantı kurulup güvenlik açıkları sayılır ve değerlendirilir. Hedef sisteme yönelik saldırı ve tehditleri araştırmak için yapılır. Enumeration username password IP blokları config dosylararı vb bilgileri toplamak için kullanılır. Hedef sisteme göre sınıflara ayrılabilir.

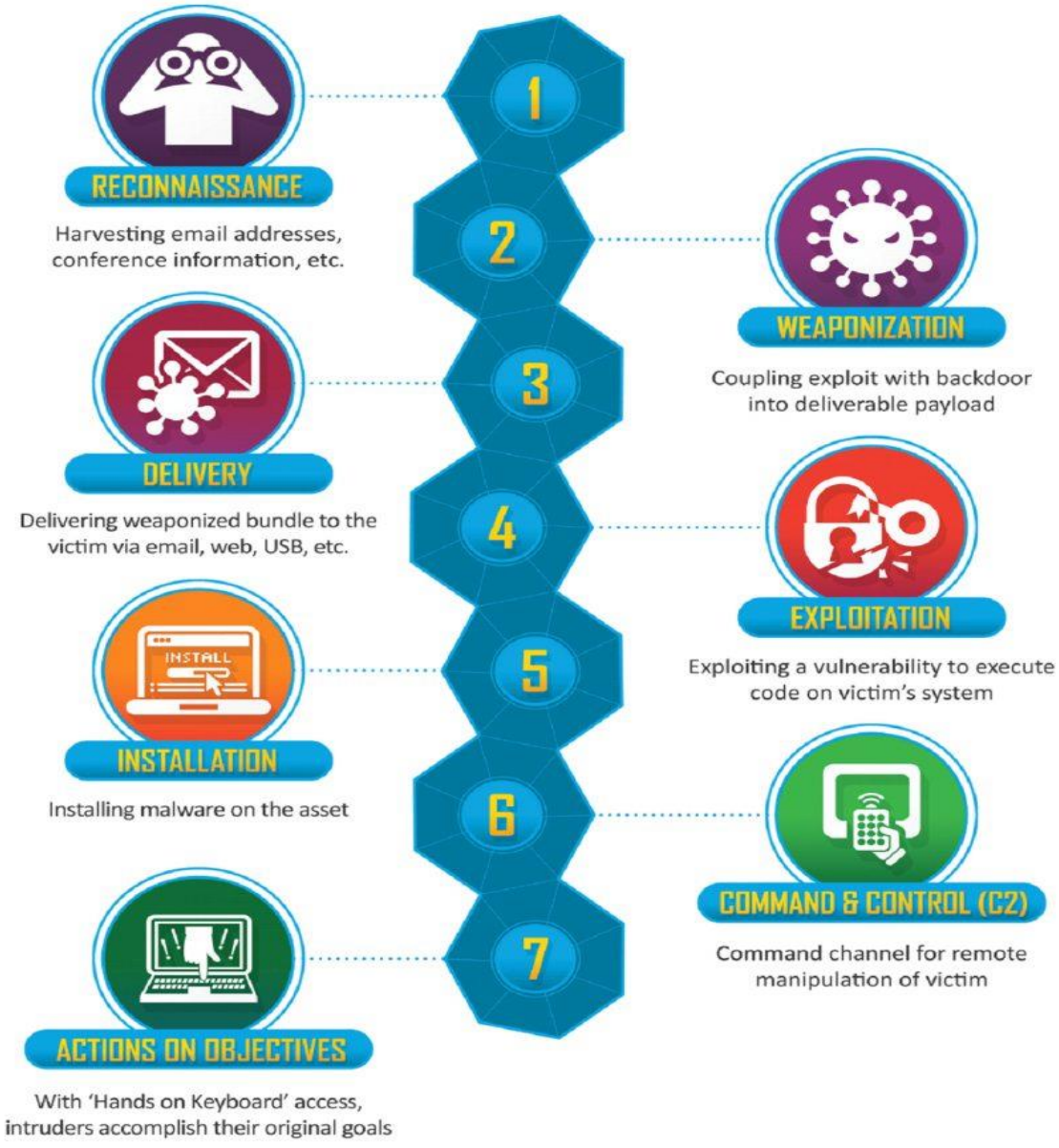
- NETBIOS Enumeration
- SNMP Enumeration
- LDAP Enumeration
- NTP Enumeration
- SMTP Enumeration
- DNS Enumeration

Aktif ve Pasif Bilgi Toplama Nedir ?

Aktif bilgi toplama direkt olarak hedefle etkileşime girdiğiniz işlemlere denir. Örnek vericek olursak herhangi biriyle tanışmak istiyorsunuz ona direkt adını sorarsanız bu aktif bilgi toplamadır fakat çevresindeki kişilerden önceden etkileşime geçtiği kişilerden öğrenirse öğrenirseniz bu da pasif bilgi toplamaya örnek olarak verilebilir. Aktif bilgi toplamada

hedefle direkt iletişim kurduğunuz için karşı tarafta log oluşturursunuz. Yani adını öğrenmek istediğiniz kişi sizin kim olduğunuzu bilir. Pasif de ise böyle bir işlem gerçekleşmez.

Cyber Kill Chain Nedir ?



Türkçesi Siber Ölüm Zinciri anlamına gelen cyber kill chain ilk olarak askeriyede ortaya çıkmıştır. Kısaca cyber kill chain bir siber saldırının aşamalarını tanımlayarak önlem almak için gerekli yöntemlerin geliştirilmesi, strateji ve taktiklerin belirlenmesine yönelik kullanılan

bir metodolojidir. Bu gelişmiş model bir hedefte başarıya ulaşmak için saldırganın hangi aşamalardan geçmesi gerektiğini tanımlar. Burada bir siber saldırının çok karmaşık yapısını aslında basite indirgeyerek ve gruplandırarak analiz etmek önemlidir. Yukarıda resimde görüldüğü üzere belli aşamalardan oluşmaktadır.

1)Reconnaissance (Keşif): Bu aşamada saldırgan hedef hakkında keşif yapar ve bilgiler toplar. Bu bilgi toplama yukarıda bahsettiğimiz yöntemlerle gerçekleşir. Burada hedefin ıp adresi, mail adresleri, name serverları, kullanılan sistemler gibi bilgiler elde edilir. Zafiyet oluşabilecek alanlar belirlermir.

2) Weaponization (Silahlanma): Bu aşamada saldırgan belirlenen hedefler üzerinden zafiyetlerin sömürülmesi için gerekli araç ve yöntemleri hazırlar. Bu aşamada saldırgan zafiyetin sömürülmesi için hazırlık aşamasındadır. Aynı zamanda hedef tarafından anlaşılmamaya çalışır.

3)Delivery (İletim): Saldırgan bu aşamada mail (phishing) ya da herhangi bir şekilde zararlı yazılımı hedefe iletir. Önemli noktalardan bir tanesidir. Saldırgan burada engellenebilir.

4)Exploiton (Sömürme) : Sömürme işlemi hedefe zararlı yazılımı göndermemizle gerçekleşir. Çoğu zaman işletim sistemleri ve uygulamalar hedef alınır. Sistemdeki zafiyet sömürülerek gerekli privilege elde edilebilir.

5)Installation(Yükleme): Sömürme işlemi başarıya ulaştıktan sonra yükleme işlemi gerçekleşir. Saldırganlara erişim sağlayan bir backdoor veya Trojan malware tarafından yüklenir. Artık burada saldırgan kalıcılık sağlayabilmek için kullanıcı yetkilerinde değişiklik yapabilir veya yeni servisler oluşturulabilir. Kritik veriler ele geçirilebilir.

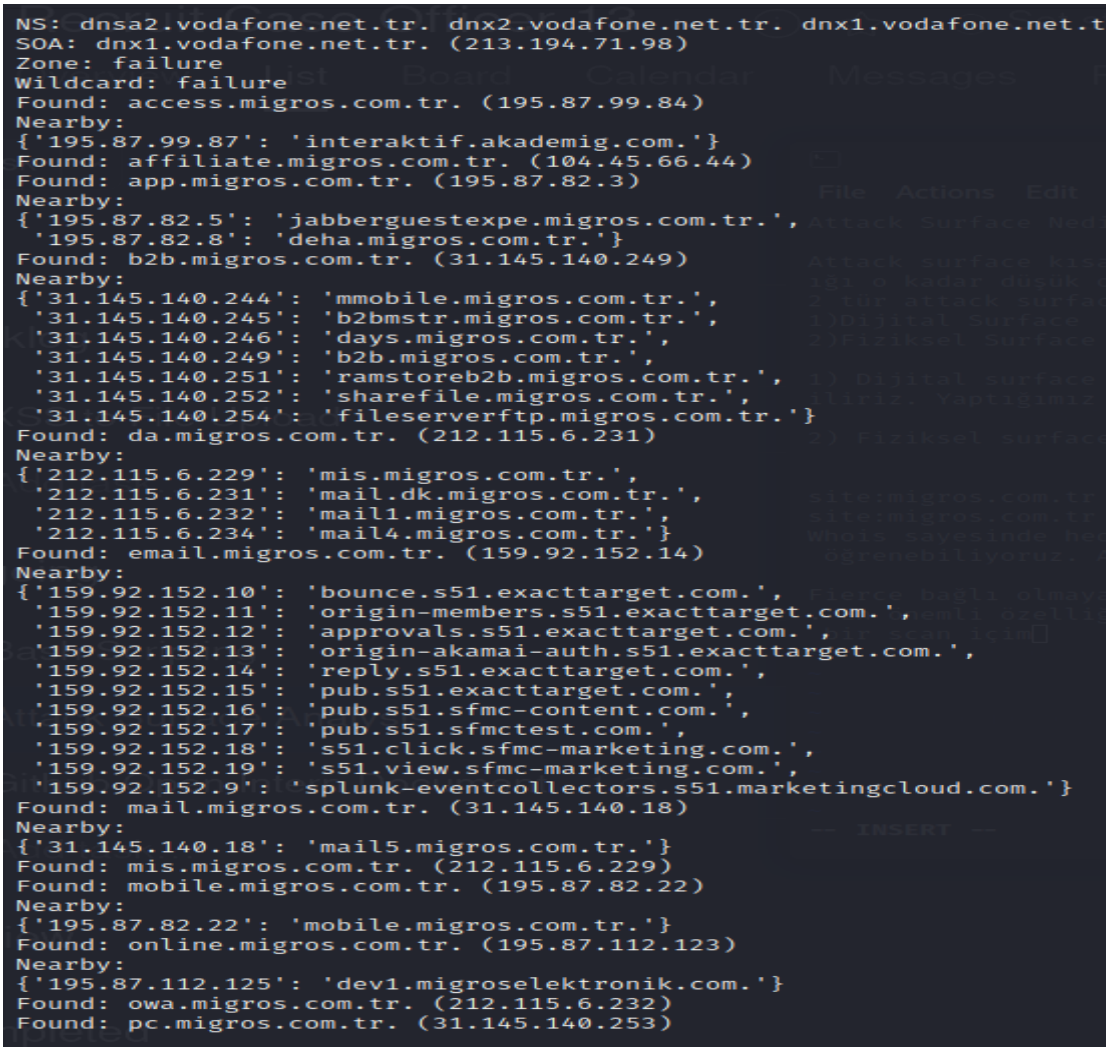
6) Command and Control (Komuta Kontrol): Bu aşamada hedef sistemleri ve ağları ele geçirilmiştir. Saldırgan hedefte kontrolü ele almak için farklı yöntemlerle privilege yükseltebilir. Bu aşamada artık sistem sizin elinizdedir.

7) Actions on Objective (Eyleme Geçme): Son aşamada artık saldırgan hedeflediği işlemleri sistem üzerinde gerçekleştirmeye başlar. Dataları çıkartabilir, silebilir, değiştirebilir.

TOOLLAR

Whois sayesinde hedefe ait pasif bilgi toplama gerçekleştirebiliyoruz. Hedefin kime kayıtlı olduğunu kimin kayıt ettiğini ve DOMAIN serverlarını bu sayede öğrenebiliyoruz. Ayrıca öğrendiğimiz ifralara ait tel noları ve adreslerine de buradan ulaşabiliyoruz.

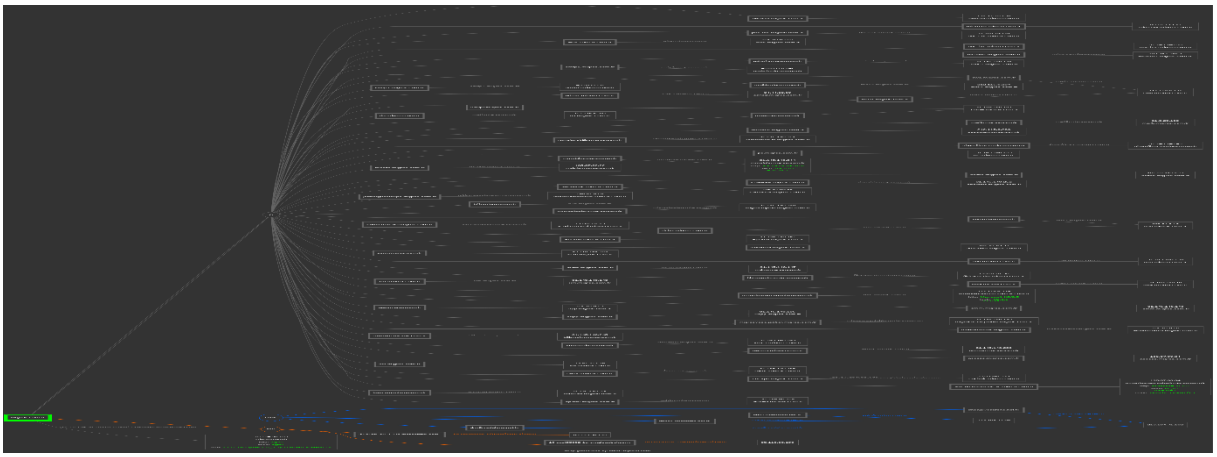
Fierce bağlı olmayan Ip adreslerine yani bir özet adresi çıkarılamayan farklı subnetlerde olan hedefin adreslerine yönelik dns sorguları gerçekleştirliyor. En önemli özelliği bilmediğimiz hedef domain adından bilmediğimiz ıp aralıklarını da kontrol etmesi örneğin nmapte ıp aralığını belirtmen lazım herhangi bir scan içim



Robtex.com da ise domaine ait nameserverlar mail serverlar listelenip bunların adları ve kayıtları gözükmektedir. Aynı zamanda CDIR bilgileride gözükmektedir. OSINT(Açık Kaynak İstihbarat) yaparken kullanılan ilk araçlardan biridir.Robtex IP numaraları, alan adları, subdomain, ana bilgisayar adı, otonom sistemler gibi araştırmalar için kullanılabiliyor Robtex'i kullanmak için websitesine girip arama yapmak istediğimiz domaini yazıp sonuçları getiriyoruz.

dnsdumpster isminden de anlaşılacağı üzere DNS'le alakalı bilgileri DNS serverları, mx kayıtları , txt kayıtları , A kayıtları , Domain haritasını görebiliyoruz.. Dnsdumpster ayrıntılı

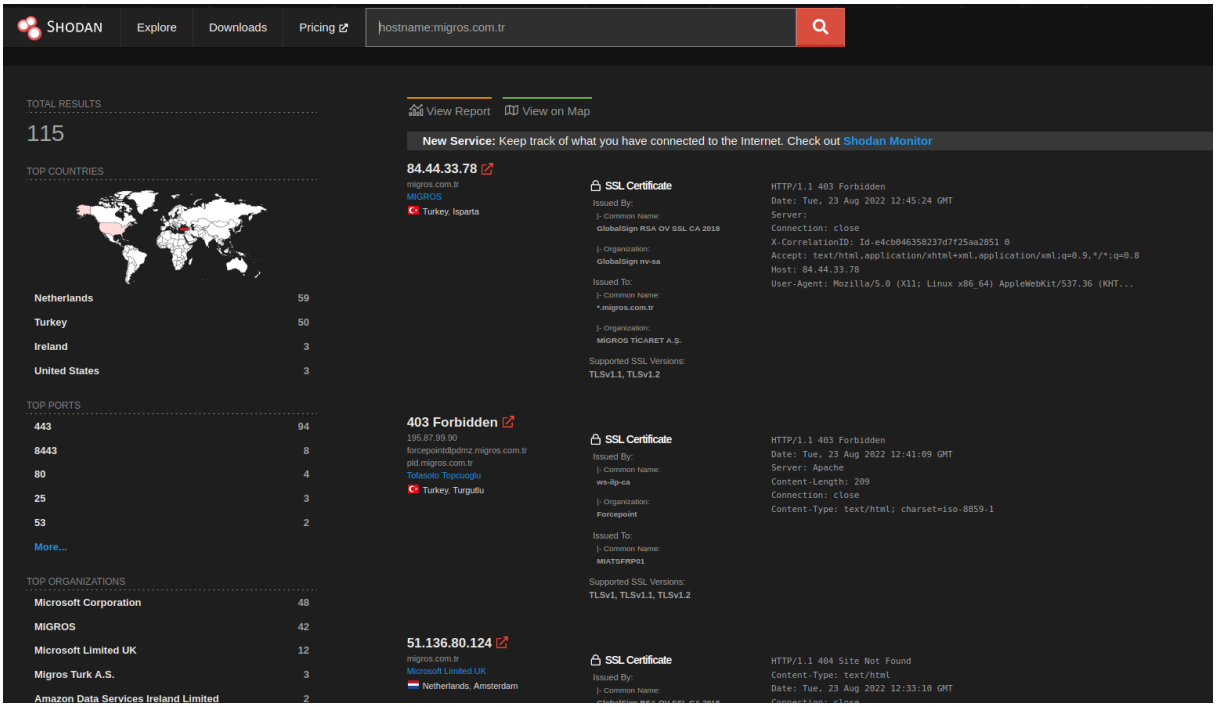
şekilde ıp blok sahiplerini ve kullandığı teknolojileri sürümleriyle birlikte gösteriyor. en son bunları grafiğe dönüştürerek anlaşılmasını kolaylaştırıyor.



1 DNS DUMPSTER GRAFİK

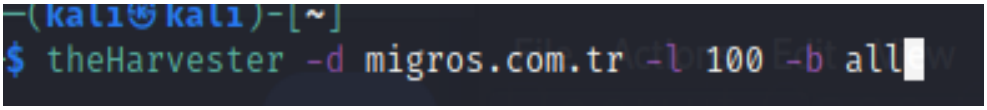
Shodan google gibi fakat internete bağlı olan cihazların aramasını yapan bir arama motorudur. Yukarıda hostname:migros.com.tr yapınca bu hosta ait cihazları bize getirdi fakat ücretsiz olarak ilk 2 sayfa arama sonucu gösteriyor.

Bundan dolayı tam erişim sağlayamıyorsun fakat sistemlere ait hangi portların açık olduğunu hangi teknolojileri kullandığını gözlemleyebiliyoruz.



honeyscore subdomaini ile karşıdaki sistemin honeypot tuzak bir sistem olup olmadığını anlıyorsun

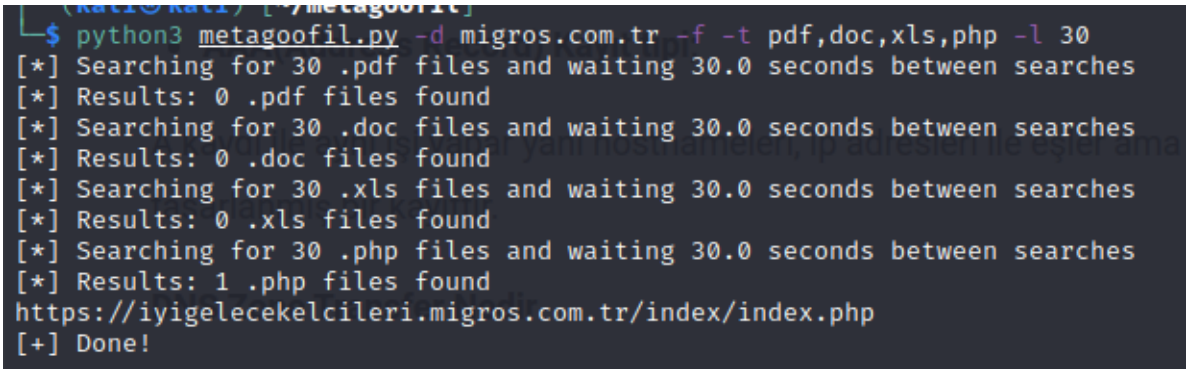
theHarvester pythonla yazılmış mükemmel bir tool . Pasif bilgileri arama motorları linkedin, diğer arama motorları üzerinden bilgileri getirebiliyor. Kullanımı çok basit theHarvester yazıp -d domaini yazıyosun ardından timeout olmaması için limit koyabiliyorsun -l ile istediğin kadar limit koyabiliyorsun -b ile de hangi kaynaklardan aramak istediğini belirtiyorsun.



dnsrecon dns kayıtlarını ve diğer mx ,a,soa,srv kayıtlarını bize getirir. dnsrecon -d migros.com.tr -a

Foca ise bize verdiğimiz domain adresine göre metadataları getirmeyi sağlayan programdır. Windows işletim sisteminde çalışmaktadır. Seçtiğimiz data türlerini domainde google bing duckduckgo da search edip elde ettiği dosyaları arayüzde getirir

Metagoofil buda Foca gibi dosya türlerini getiriyor fakat bunu yaparken Googledan bloklanmanız muhtemel bunun için ssh tunelling yapıyorlarmış onu tam anlamadım. Bende VPN kullanarak denedim.



Google üzerinden araştırma yaparken aşağıdaki filtreleri uyguladum. Bing ve Yahoo yu toollar üzerinden eriştim.

site:migros.com.tr -site:"www.migros.com.tr" Bu sayede subdomainlere google üzerinden erişilebiliyoruz

site:migros.com.tr filetype:pdf

Ben ayrıca gobuster dns -d Migros.com.tr -w dns wordlisti verip kullandım daha ayrıntılı ve daha uzun sürdü

Migros.com.tr Bilgi Toplama

Recon-ng ,dnsdumpster,whois kullandım aşağıdaki bilgileri elde ederken mailleri için site ücretliydi onun yerine alternatiflerini denedim. theHarvester ayrıca çok yardımcı oldu metagoofili kullanırken Google blokluyordu onu vpn çözerek hallettim ama belli başlı 30 limitli olarak çektim sadece index.php geldi.

Name Servers

dnsa1.vodafone.net.tr.	286	IN	A	213.194.71.98
dnx1.vodafone.net.tr.	215	IN	A	213.194.71.98
dnsa2.vodafone.net.tr.	252	IN	A	213.194.71.102
dnx2.vodafone.net.tr.				

MX RECORDS

cust53852-1.in.mailcontrol.com.	3600	IN	A	85.115.56.190	ALMANYA
cust53852-2.in.mailcontrol.com.	3600	IN	A	85.115.58.190	ALMANYA

ASNS RECORDS

AS15169
AS15924
AS16509
AS8075

A RECORDS

5mmigroskop.migros.com.tr
access.migros.com.tr
adns1.migros.com.tr
adns2.migros.com.tr
affiliate.migros.com.tr
apidev.migros.com.tr
app.migros.com.tr
as.ocscwa.migros.com.tr
autodiscover.migros.com.tr

awrms.migros.com.tr

awtunnel.migros.com.tr

awtunnel.migros.com.tr

b2b.migros.com.tr

b2bmstr.migros.com.tr

banner.migros.com.tr

basvuru.migros.com.tr

bformmutabakat.migros.com.tr

cockpit.migros.com.tr

da.migros.com.tr

days.migros.com.tr

deha.migros.com.tr

disneymasallari.migros.com.tr

disneymasallari.migros.com.tr

download.ocscwa.migros.com.tr

earsiv.migros.com.tr

emm.migros.com.tr

espor.migros.com.tr

fikirsepetim.migros.com.tr

fileserverftp.migros.com.tr

hermes.migros.com.tr

ikportal.migros.com.tr

iyigelecekelcileri.migros.com.tr

jabberguestexpe.migros.com.tr

katalog.migros.com.tr

katalog.migros.com.tr

mag.migros.com.tr

mail.dk.migros.com.tr

mail.maya.migros.com.tr

mail.migros.com.tr

mail1.migros.com.tr

mail3.migros.com.tr

mail4.migros.com.tr

mail5.migros.com.tr

maya.migros.com.tr

mdm.migros.com.tr

mi1srv1.migros.com.tr

migrasrv.migros.com.tr

migroskop.migros.com.tr

migrostoptan.migros.com.tr

migrostv.migros.com.tr

migrosvcse.jabber.migros.com.tr

mis.migros.com.tr

mmobile.migros.com.tr

test.migros.com.tr

test2.migros.com.tr.

traefik.migros.com.tr

mobile.migros.com.tr

ocscwa.migros.com.tr

online.migros.com.tr

owa.migros.com.tr

owasrv.migros.com.tr

pc.migros.com.tr

pld.migros.com.tr

poc-ctx.migros.com.tr

poc-hrz.migros.com.tr

ramstoreb2b.migros.com.tr

rest.migros.com.tr

rest.migros.com.tr

sanalsinif.migros.com.tr

scm.migros.com.tr

servismasasi.migros.com.tr

sharefile.migros.com.tr

sharefileszc.migros.com.tr

smentegrasyon.migros.com.tr

smentegrasyontest.migros.com.tr

smtp1.migros.com.tr

smtp2.migros.com.tr

sts.migros.com.tr

uag.migros.com.tr

vc.migros.com.tr

vpn.migros.com.tr

wbx.migros.com.tr

webexserver.migros.com.tr

www.basvuru.migros.com.tr

www.maya.migros.com.tr

www.migros.com.tr

x22ikportal.migros.com.tr

x22www.migros.com.tr

xapp.migros.com.tr

xm.migros.com.tr

xmcs.migros.com.tr

xmgw.migros.com.tr

kaptan.migros.com.tr

seg.migros.com.tr

webcon.migros.com.tr

boss.migros.com.tr

IP BLOCK OWNERS

IP BLOCK

migros.com.tr ip blocks:

_____

31.145.140.18/32

31.145.140.49/32

31.145.140.50/31

31.145.140.130/32

31.145.140.134/32

31.145.140.143/32

31.145.140.145/32

31.145.140.147/32

31.145.140.156/32

31.145.140.236/32

31.145.140.244/31

31.145.140.246/32

31.145.140.249/32

31.145.140.251/32

31.145.140.252/32

31.145.140.254/32

195.87.82.5/32

195.87.82.8/31

195.87.82.10/32

195.87.82.22/32

195.87.82.29/32

195.87.82.30/32

195.87.99.90/32

212.115.6.229/32

212.115.6.231/32

212.115.6.232/32

212.115.6.234/32

PHONES

41 2937 272

+90 216 418 19 10

+90 534 341 72 39

27 9975 959

+90 850 955 0463

+90 850 310 2071

+90 216 349 23 70

058 573 37 00

+90 312 988 11 06

+90 242 742 98 00

+34 120 39 253

37 2146 449

530 300 13 00

253 39 120

28 3644 064

SRV RECORDS

SRV _sip._udp.migros.com.tr migrosvcse.jabber.migros.com.tr 31.145.140.130 5060

SRV _sips._tcp.migros.com.tr migrosvcse.jabber.migros.com.tr 31.145.140.130 5061

SRV _sip._tcp.migros.com.tr migrosvcse.jabber.migros.com.tr 31.145.140.130 5060

SRV _h323cs._tcp.migros.com.tr migrosvcse.jabber.migros.com.tr 31.145.140.130 1720

SRV _h323ls._udp.migros.com.tr migrosvcse.jabber.migros.com.tr 31.145.140.130 1719

SRV _sipfederationtls._tcp.migros.com.tr access.migros.com.tr 195.87.99.84 5061

SRV _autodiscover._tcp.migros.com.tr owasrv.migros.com.tr 212.115.6.238 443

SRV _sip._tls.migros.com.tr migrosvcse.jabber.migros.com.tr 31.145.140.130 5061

EMAİL

amzn-noc-contact@amazon.com

support@builtwith.com

yatirimci@migros.com.tr

surdurulebilirlik@migros.com.tr

migrosticaretas@hs01.kep.tr

iletisim@migros.com.tr

dnsadmin@migros.com.tr.

sinemk@migros.com.tr

handeo@migros.com.tr

moneykurumsal@migros.com.tr

umite@migros.com.tr

im@migros.com.tr

rkiye@migros.com.tr

ozgurk@migros.com.tr

marka@migros.com.tr

moneykurumsal@migros.com.tr

eticaretdestek@migros.com.tr

iletisim@migros.com.tr

malimigros@migros.com.tr

x22iletisim@migros.com.tr

x22malimigros@migros.com.tr

İnternete açık siteler

ikportal.migros.com.tr

katalog.migros.com.tr

toptantahsilat.migros.com.tr

earsiv.migros.com.tr

toptan.migros.com.tr

espor.migros.com.tr

iyigelecekelcileri.migros.com.tr

www.money.com.tr

mis.migros.com.tr

www.migros.com.tr

migrostv.migros.com.tr

b2b.migros.com.tr

sosyal.migros.com.tr

mis.migros.com.tr

https://xapp.migros.com.tr/

DNS NAME

site.migros.com.tr

smentegrasyontest.migros.com.tr

email.migros.com.tr

urunlisteleme-test.migros.com.tr

mail.migros.com.tr

test.hermes.migros.com.tr

test2.rest.migros.com.tr

mail1.migros.com.tr

toptantahsilattest.migros.com.tr

test.migros.com.tr

kaptantest.migros.com.tr

mail5.migros.com.tr

efaturatest.migros.com.tr

migros.com.tr

toptantahsilat.migros.com.tr

sosyaladmin.migros.com.tr

mag.migros.com.tr

urunlisteleme.migros.com.tr

aractakip.migros.com.tr

mta.email.migros.com.tr

stage.rest.migros.com.tr

iyigelecekelcileri.migros.com.tr

migrostv.migros.com.tr

filesharing.migros.com.tr

awrms.migros.com.tr

Registrant:

Migros Türk T.A.Ş.

Caferağa Mah. Damga Sk. No:23-25 Kadıköy

34710

İstanbul,

Türkiye

marka@migros.com.tr

+ 90-216-4181910-

+ 90-216-3492370

Registrar:

NIC Handle : ogv40-metu

Organization Name : ODTÜ GELİŞTİRME VAKFI BİLGİ TEKNOLOJİLERİ SAN. VE TİC. A.Ş.

Address : ÜNİVERSİTELER MAH. İHSAN DOĞRAMACI BLV.

ARGE VE EĞİTİM MERKEZİ NO:13 ÇANKAYA

Ankara,06800

Türkiye

Phone : + 90-312-9881106-

Fax : +

KULLANILAN TEKNOLOJİLER

5MMIGROSKOP.MIGROS.COM.TR ngnix AMAZON cloud, ASP.NET

SOSYALAPI.MIGROS.COM.TR→ IIS 10

MIGROSTAR.MIGROS.COM.TR→ Jquery,IIS10

MIGROSTV.MIGROS.COM.TR →Wordpress,PHP7 Microsoft AZure, CDN JS

ESPOR.MIGROS.COM.TR → PERL

SOSYAL.MIGROS.COM.TR→ Angular, IIS 10 , LİNUX

PC.MIGROS.COM.TR → Apache Server

B2B.migros.com.tr→ ASP.NET,4.0.30319 IIS,10.0

mag.migros.com.tr → Microsoft-IIS/8.5 ASP.NET

TXT RECORDS

"apple-domain-verification=aZO2mznu9QoDMMKh"

"globalsign-domain-verification=FJIJzKNM4Sk_0pkKoApLSYGEJBfeGV4Vz9l2estO1i"

"google-site-verification=RA-zfdctcgn7Af6aVmt7IcAzVzeAwUYpqyzTvDObpwE"

"google-site-verification=QyduSIMAn7NpNVHpMvX6ZtuGNyQeutHXUMb3GuKC3ys"

"v=spf1 ip4:40.68.220.242 ip4:40.68.221.8 ip4:81.8.25.153 ip4:51.136.98.24 ip4:31.145.140.18 include:mailcontrol.com include:spf.protection.outlook.com -all"

"MS=ms27777964"

"pquS870DLP95cYWIT0igfUQsPMwdg6mdkk/AjTW/SMo="

"6Gr2vD8Xth7DPX3YbniKrIimyJ9ZOMxeH7RqD3ApNGg="

"globalsign-domain-verification=Cp93X4NeAkdAWt93fqCpmYFor5fc-wwWUgMUuEslAU"

PORT SCAN OF SUBDOMAİNS

Bunun içinde nmap'ın -iL opsiyonunu kullandım çektiğim subdomainleri txt dosyasına kaydettim. -iL ile de nmap tek tek tarama yaptı.

Failed to resolve "kaptantest.migros.com.tr".

Nmap scan report for 5mmigroskop.migros.com.tr (52.85.5.125)

Host is up (0.073s latency).

Other addresses for 5mmigroskop.migros.com.tr (not scanned): 52.85.5.107 52.85.5.72 52.85.5.30

rDNS record for 52.85.5.125: server-52-85-5-125.sof50.r.cloudfront.net

Not shown: 999 filtered tcp ports (no-response)

PORT   STATE SERVICE

443/tcp open https

Nmap scan report for adns1.migros.com.tr (31.145.140.134)

Host is up (0.073s latency).

Not shown: 999 filtered tcp ports (no-response)

PORT   STATE SERVICE

80/tcp open http

Nmap scan report for affiliate.migros.com.tr (104.45.66.44)

Host is up (0.098s latency).

Not shown: 999 filtered tcp ports (no-response)

PORT   STATE SERVICE

443/tcp open https

Nmap scan report for app.migros.com.tr (195.87.82.3)

Host is up (0.067s latency).

Not shown: 999 filtered tcp ports (no-response)

PORT   STATE SERVICE

80/tcp open http

Nmap scan report for as.ocscwa.migros.com.tr (212.115.6.236)

Host is up (0.065s latency).

Not shown: 996 filtered tcp ports (no-response)

PORT   STATE SERVICE

443/tcp open https

8080/tcp open http-proxy

8083/tcp open us-srv

8443/tcp open https-alt

Nmap scan report for autodiscover.migros.com.tr (40.101.78.104)

Host is up (0.069s latency).

Other addresses for autodiscover.migros.com.tr (not scanned): 40.101.55.136 52.97.181.72 40.101.69.200 2603:1026:302:78::8 2603:1026:301:9a::8 2603:1026:300:b3::8 2603:1026:301:54::8

Not shown: 999 filtered tcp ports (no-response)

PORT   STATE SERVICE

80/tcp open http

Nmap scan report for awrms.migros.com.tr (31.145.140.236)

Host is up (0.064s latency).

Not shown: 994 filtered tcp ports (no-response)

PORT   STATE SERVICE

80/tcp   open http

443/tcp open https

2001/tcp open dc

2010/tcp open search

2020/tcp open xinupageserver

8443/tcp open https-alt

Nmap scan report for awtunnel.migros.com.tr (195.87.82.27)

Host is up (0.064s latency).

Not shown: 994 filtered tcp ports (no-response)

PORT   STATE SERVICE

80/tcp   open http

443/tcp open https

2001/tcp open dc

2010/tcp open search

2020/tcp open xinupageserver

8443/tcp open https-alt

Nmap scan report for awtunnel.migros.com.tr (195.87.82.27)

Host is up (0.065s latency).

Not shown: 995 filtered tcp ports (no-response)

PORT   STATE SERVICE

80/tcp   open http

443/tcp open https

2001/tcp open dc

2010/tcp open search

8443/tcp open https-alt

Nmap scan report for b2b.migros.com.tr (31.145.140.249)

Host is up (0.059s latency).

rDNS record for 31.145.140.249: migrostoptan.migros.com.tr

Not shown: 998 filtered tcp ports (no-response)

PORT   STATE SERVICE

80/tcp open http

443/tcp open https

Nmap scan report for b2bmstr.migros.com.tr (31.145.140.245)

Host is up (0.065s latency).

Not shown: 998 filtered tcp ports (no-response)

PORT   STATE SERVICE

80/tcp open http

443/tcp open https

Nmap scan report for banner.migros.com.tr (52.137.29.195)

Host is up (0.094s latency).

Not shown: 998 filtered tcp ports (no-response)

PORT   STATE SERVICE

80/tcp open http

443/tcp open https

Nmap scan report for basvuru.migros.com.tr (52.137.30.76)

Host is up (0.099s latency).

Not shown: 998 filtered tcp ports (no-response)

PORT   STATE SERVICE

80/tcp open http

443/tcp open https

Nmap scan report for bformmutabakat.migros.com.tr (51.145.181.8)

Host is up (0.095s latency).

Not shown: 999 filtered tcp ports (no-response)

PORT   STATE SERVICE

443/tcp open https

Nmap scan report for cockpit.migros.com.tr (99.83.247.121)

Host is up (0.076s latency).

rDNS record for 99.83.247.121: a28e1da254b52eb76.awsglobalaccelerator.com

Not shown: 998 filtered tcp ports (no-response)

PORT   STATE SERVICE

80/tcp open http

443/tcp open https

Nmap scan report for days.migros.com.tr (31.145.140.246)

Host is up (0.064s latency).

Not shown: 998 filtered tcp ports (no-response)

PORT   STATE SERVICE

443/tcp open https

2020/tcp open xinupageserver

Nmap scan report for disneymasallari.migros.com.tr (52.85.5.63)

Host is up (0.12s latency).

Other addresses for disneymasallari.migros.com.tr (not scanned): 52.85.5.48 52.85.5.51 52.85.5.64

rDNS record for 52.85.5.63: server-52-85-5-63.sof50.r.cloudfront.net

Not shown: 998 filtered tcp ports (no-response)

PORT   STATE SERVICE

80/tcp open http

443/tcp open https

Nmap scan report for disneymasallari.migros.com.tr (52.85.5.51)

Host is up (0.14s latency).

Other addresses for disneymasallari.migros.com.tr (not scanned): 52.85.5.63 52.85.5.48 52.85.5.64

rDNS record for 52.85.5.51: server-52-85-5-51.sof50.r.cloudfront.net

Not shown: 998 filtered tcp ports (no-response)

PORT   STATE SERVICE

80/tcp open http

443/tcp open https

Nmap scan report for download.ocscwa.migros.com.tr (212.115.6.236)

Host is up (0.065s latency).

Not shown: 996 filtered tcp ports (no-response)

PORT   STATE SERVICE

443/tcp open https

8080/tcp open http-proxy

8083/tcp open us-srv

8443/tcp open https-alt

Nmap scan report for earsiv.migros.com.tr (20.234.200.231)

Host is up (0.095s latency).

Not shown: 998 filtered tcp ports (no-response)

PORT   STATE SERVICE

80/tcp open http

443/tcp open https

Nmap scan report for emm.migros.com.tr (31.145.140.146)

Host is up (0.067s latency).

Not shown: 994 filtered tcp ports (no-response)

PORT   STATE SERVICE

80/tcp   open http

443/tcp open https

2001/tcp open dc

2010/tcp open search

2020/tcp open xinupageserver

8443/tcp open https-alt

Nmap scan report for espor.migros.com.tr (20.50.45.123)

Host is up (0.10s latency).

Not shown: 998 filtered tcp ports (no-response)

PORT   STATE SERVICE

80/tcp open http

443/tcp open https

Nmap scan report for fikirsepetim.migros.com.tr (195.87.82.30)

Host is up (0.066s latency).

Not shown: 997 filtered tcp ports (no-response)

PORT   STATE SERVICE

80/tcp open http

443/tcp open https

2020/tcp open xinupageserver

Nmap scan report for ikportal.migros.com.tr (31.145.140.151)

Host is up (0.061s latency).

Not shown: 994 filtered tcp ports (no-response)

PORT   STATE SERVICE

80/tcp open http

443/tcp open https

7777/tcp open cbt

8100/tcp open xprint-server

8888/tcp open sun-answerbook

9999/tcp open abyss

Nmap scan report for iyigelecekelcileri.migros.com.tr (52.236.144.130)

Host is up (0.11s latency).

Not shown: 998 filtered tcp ports (no-response)

PORT   STATE SERVICE

80/tcp open http

443/tcp open https

Nmap scan report for katalog.migros.com.tr (52.212.227.145)

Host is up (0.13s latency).

Other addresses for katalog.migros.com.tr (not scanned): 52.210.121.7

rDNS record for 52.212.227.145: ec2-52-212-227-145.eu-west-1.compute.amazonaws.com

Not shown: 998 filtered tcp ports (no-response)

PORT   STATE SERVICE

80/tcp open http

443/tcp open https

Nmap scan report for katalog.migros.com.tr (52.210.121.7)

Host is up (0.13s latency).

Other addresses for katalog.migros.com.tr (not scanned): 52.212.227.145

rDNS record for 52.210.121.7: ec2-52-210-121-7.eu-west-1.compute.amazonaws.com

Not shown: 998 filtered tcp ports (no-response)

PORT   STATE SERVICE

80/tcp open http

443/tcp open https

Nmap scan report for mag.migros.com.tr (31.145.140.142)

Host is up (0.058s latency).

Not shown: 997 filtered tcp ports (no-response)

PORT   STATE SERVICE

80/tcp   open http

443/tcp open https

2020/tcp open xinupageserver

Nmap scan report for mail4.migros.com.tr (212.115.6.234)

Host is up (0.070s latency).

Not shown: 996 filtered tcp ports (no-response)

PORT   STATE SERVICE

443/tcp open https

8080/tcp open http-proxy

8083/tcp open us-srv

8443/tcp open https-alt

Nmap scan report for migrasrv.migros.com.tr (31.145.140.131)

Host is up (0.065s latency).

Not shown: 999 filtered tcp ports (no-response)

PORT STATE SERVICE

443/tcp open https

Nmap scan report for migroskop.migros.com.tr (52.85.5.29)

Host is up (0.065s latency).

Other addresses for migroskop.migros.com.tr (not scanned): 52.85.5.53 52.85.5.127 52.85.5.25

rDNS record for 52.85.5.29: server-52-85-5-29.sof50.r.cloudfront.net

Not shown: 998 filtered tcp ports (no-response)

PORT STATE SERVICE

80/tcp open http

443/tcp open https

Nmap scan report for migrostoptan.migros.com.tr (31.145.140.249)

Host is up (0.071s latency).

rDNS record for 31.145.140.249: b2b.migros.com.tr

Not shown: 998 filtered tcp ports (no-response)

PORT STATE SERVICE

80/tcp open http

443/tcp open https

Nmap scan report for migrostv.migros.com.tr (40.74.19.130)

Host is up (0.094s latency).

Not shown: 998 filtered tcp ports (no-response)

PORT STATE SERVICE

80/tcp open http

443/tcp open https

Nmap scan report for migrosvcse.jabber.migros.com.tr (31.145.140.130)

Host is up (0.067s latency).

rDNS record for 31.145.140.130: vc.migros.com.tr

Not shown: 990 filtered tcp ports (no-response)

PORT STATE SERVICE

53/tcp open domain

80/tcp open http

161/tcp open snmp

443/tcp open https

873/tcp open rsync

2222/tcp open EtherNetIP-1

5060/tcp open sip

5061/tcp open sip-tls

7001/tcp open afs3-callback

8443/tcp open https-alt

Nmap scan report for mis.migros.com.tr (212.115.6.229)

Host is up (0.15s latency).

Not shown: 995 filtered tcp ports (no-response)

PORT STATE SERVICE

80/tcp open http

443/tcp open https

7777/tcp open cbt

8100/tcp open xprint-server

8888/tcp open sun-answerbook

Nmap scan report for mmobile.migros.com.tr (31.145.140.244)

Host is up (0.068s latency).

Not shown: 998 filtered tcp ports (no-response)

PORT STATE SERVICE

80/tcp open http

443/tcp open https

Nmap scan report for ocscwa.migros.com.tr (212.115.6.236)

Host is up (0.065s latency).

Not shown: 996 filtered tcp ports (no-response)

PORT STATE SERVICE

443/tcp open https

8080/tcp open http-proxy

8083/tcp open us-srv

8443/tcp open https-alt

Nmap scan report for online.migros.com.tr (195.87.112.123)

Host is up (0.066s latency).

Not shown: 998 filtered tcp ports (no-response)

PORT STATE SERVICE

80/tcp open http

443/tcp open https

Nmap scan report for pc.migros.com.tr (31.145.140.253)

Host is up (0.081s latency).

Not shown: 997 filtered tcp ports (no-response)

PORT STATE SERVICE

53/tcp open domain

80/tcp open http

443/tcp open https

Nmap scan report for ramstoreb2b.migros.com.tr (31.145.140.251)

Host is up (0.078s latency).

Not shown: 997 filtered tcp ports (no-response)

PORT STATE SERVICE

80/tcp open http

443/tcp open https

2020/tcp open xinupageserver

Nmap scan report for rest.migros.com.tr (52.16.40.245)

Host is up (0.13s latency).

Other addresses for rest.migros.com.tr (not scanned): 99.81.187.60 108.129.42.46

rDNS record for 52.16.40.245: ec2-52-16-40-245.eu-west-1.compute.amazonaws.com

Not shown: 998 filtered tcp ports (no-response)

PORT   STATE SERVICE

80/tcp open http

443/tcp open https

Nmap scan report for rest.migros.com.tr (108.129.42.46)

Host is up (0.12s latency).

Other addresses for rest.migros.com.tr (not scanned): 99.81.187.60 52.16.40.245

rDNS record for 108.129.42.46: ec2-108-129-42-46.eu-west-1.compute.amazonaws.com

Not shown: 998 filtered tcp ports (no-response)

PORT   STATE SERVICE

80/tcp open http

443/tcp open https

Nmap scan report for sanalsinif.migros.com.tr (195.87.99.88)

Host is up (0.079s latency).

Not shown: 998 filtered tcp ports (no-response)

PORT   STATE SERVICE

443/tcp open https

2020/tcp open xinupageserver

Nmap scan report for sharefile.migros.com.tr (31.145.140.252)

Host is up (0.066s latency).

Not shown: 997 filtered tcp ports (no-response)

PORT STATE SERVICE

80/tcp open http

443/tcp open https

2020/tcp open xinupageserver

Nmap scan report for smentegrasyon.migros.com.tr (212.115.6.229)

Host is up (0.072s latency).

rDNS record for 212.115.6.229: mis.migros.com.tr

Not shown: 994 filtered tcp ports (no-response)

PORT STATE SERVICE

80/tcp open http

443/tcp open https

7777/tcp open cbt

8100/tcp open xprint-server

8888/tcp open sun-answerbook

9999/tcp open abyss

Nmap scan report for smentegrasyontest.migros.com.tr (195.87.99.94)

Host is up (0.072s latency).

Not shown: 994 filtered tcp ports (no-response)

PORT STATE SERVICE

80/tcp open http

443/tcp open https

2001/tcp open dc

2010/tcp open search

2020/tcp open xinupageserver

8080/tcp open http-proxy

Nmap scan report for sts.migros.com.tr (13.81.212.76)

Host is up (0.100s latency).

Not shown: 999 filtered tcp ports (no-response)

PORT   STATE SERVICE

443/tcp open https

Nmap scan report for uag.migros.com.tr (31.145.140.156)

Host is up (0.057s latency).

Not shown: 995 filtered tcp ports (no-response)

PORT   STATE SERVICE

80/tcp   open http

443/tcp open https

2001/tcp open dc

2020/tcp open xinupageserver

8443/tcp open https-alt

Nmap scan report for wbx.migros.com.tr (195.87.82.10)

Host is up (0.075s latency).

Not shown: 991 filtered tcp ports (no-response)

PORT   STATE SERVICE

53/tcp   open domain

80/tcp   open http

443/tcp open https

873/tcp open rsync

2222/tcp open EtherNetIP-1

5060/tcp open sip

5222/tcp open xmpp-client

7001/tcp open afs3-callback

8443/tcp open https-alt

Nmap scan report for webexserver.migros.com.tr (195.87.82.9)

Host is up (0.067s latency).

Not shown: 991 filtered tcp ports (no-response)

PORT STATE SERVICE

53/tcp open domain

80/tcp open http

161/tcp open snmp

443/tcp open https

873/tcp open rsync

2222/tcp open EtherNetIP-1

5061/tcp open sip-tls

5222/tcp open xmpp-client

7001/tcp open afs3-callback

Nmap scan report for www.migros.com.tr (52.16.40.245)

Host is up (0.12s latency).

Other addresses for www.migros.com.tr (not scanned): 99.81.187.60 108.129.42.46

rDNS record for 52.16.40.245: ec2-52-16-40-245.eu-west-1.compute.amazonaws.com

Not shown: 998 filtered tcp ports (no-response)

PORT STATE SERVICE

80/tcp open http

443/tcp open https

Nmap scan report for xapp.migros.com.tr (31.145.140.135)

Host is up (0.072s latency).

Not shown: 998 filtered tcp ports (no-response)

PORT STATE SERVICE

53/tcp open domain

443/tcp open https

Nmap scan report for xm.migros.com.tr (31.145.140.143)

Host is up (0.065s latency).

Not shown: 998 filtered tcp ports (no-response)

PORT STATE SERVICE

443/tcp open https

2001/tcp open dc

Nmap scan report for xmcs.migros.com.tr (31.145.140.145)

Host is up (0.074s latency).

Not shown: 995 filtered tcp ports (no-response)

PORT STATE SERVICE

80/tcp open http

443/tcp open https

2001/tcp open dc

2010/tcp open search

8443/tcp open https-alt

Nmap scan report for xmgw.migros.com.tr (31.145.140.142)

Host is up (0.066s latency).

Not shown: 999 filtered tcp ports (no-response)

PORT STATE SERVICE

443/tcp open https

Nmap scan report for kaptan.migros.com.tr (40.118.126.132)

Host is up (0.097s latency).

Not shown: 998 filtered tcp ports (no-response)

PORT STATE SERVICE

80/tcp open http

443/tcp open https

Nmap scan report for seg.migros.com.tr (13.93.15.83)

Host is up (0.087s latency).

All 1000 scanned ports on seg.migros.com.tr (13.93.15.83) are in ignored states.

Not shown: 1000 filtered tcp ports (no-response)

Nmap scan report for boss.migros.com.tr (20.105.196.149)

Host is up (0.090s latency).

Not shown: 998 filtered tcp ports (no-response)

PORT STATE SERVICE

80/tcp open http

443/tcp open https

Nmap scan report for ikportal.migros.com.tr (31.145.140.151)

Host is up (0.059s latency).

Not shown: 994 filtered tcp ports (no-response)

PORT STATE SERVICE

80/tcp open http

443/tcp open https

7777/tcp open cbt

8100/tcp open xprint-server

8888/tcp open sun-answerbook

9999/tcp open abyss

Nmap scan report for katalog.migros.com.tr (52.210.121.7)

Host is up (0.13s latency).

Other addresses for katalog.migros.com.tr (not scanned): 52.212.227.145

rDNS record for 52.210.121.7: ec2-52-210-121-7.eu-west-1.compute.amazonaws.com

Not shown: 998 filtered tcp ports (no-response)

PORT STATE SERVICE

80/tcp open http

443/tcp open https

Nmap scan report for toptantahsilat.migros.com.tr (51.137.18.197)

Host is up (0.090s latency).

Not shown: 998 filtered tcp ports (no-response)

PORT   STATE SERVICE

80/tcp open http

443/tcp open https

Nmap scan report for earsiv.migros.com.tr (20.234.200.231)

Host is up (0.098s latency).

Not shown: 998 filtered tcp ports (no-response)

PORT   STATE SERVICE

80/tcp open http

443/tcp open https

Nmap scan report for toptan.migros.com.tr (51.136.80.124)

Host is up (0.10s latency).

Not shown: 998 filtered tcp ports (no-response)

PORT   STATE SERVICE

80/tcp open http

443/tcp open https

Nmap scan report for espor.migros.com.tr (20.50.45.123)

Host is up (0.095s latency).

Not shown: 998 filtered tcp ports (no-response)

PORT   STATE SERVICE

80/tcp open http

443/tcp open https