

Footprinting ve Reconnaissance

BGM 531 - Sızma Testleri ve Güvenlik Denetlemeleri

Bilgi Güvenliği Mühendisliği

Yüksek Lisans Programı

Dr. Ferhat Özgür Çatak
ozgur.catak@tubitak.gov.tr

İstanbul Şehir Üniversitesi
2018 - Güz

İçindekiler

- 1 Footprinting Konsepti
 - Tanım
 - Footprinting Hedefleri
 - 2 Yöntem
 - Arama Motorları
 - Document Metadata
 - Google Teknikleri
 - Sosyal Ağ Siteleri
 - Website Footprinting
 - Email Footprinting
 - WHOIS
 - DNS Footprinting
 - 3 Araçlar
 - Maltego
 - FOCA
 - 4 Countermeasure
 - Countermeasure
 - 5 Lab
 - Windows Komut Satırı
 - Çevirimiçi Kişi Bilgi Arama Servisleri
 - Path Analyzer Pro kullanarak Network Route Tracing
 - Maltego

İçindekiler

- 1 Footprinting Konsepti
 - Tanım
 - Footprinting Hedefleri
- 2 Yöntem
 - Arama Motorları
 - Document Metadata
 - Google Teknikleri
 - Sosyal Ağ Siteleri
 - Website Footprinting
 - Email Footprinting
 - WHOIS
 - DNS Footprinting

- Sosyal Mühendislik
- Yöntemleriyle Footprinting
- 3 Araçlar
 - Maltego
 - FOCA
- 4 Countermeasure
 - Countermeasure
- 5 Lab
 - Windows Komut Satırı
 - Çevirimci Kişisel Bilgi Arama Servisleri
 - Path Analyzer Pro kullanarak Network Route Tracing
 - Maltego

Footprinting Nedir?

Footprinting

- ▶ Kuruluşun ağ sistemine müdahale etmek için çeşitli yolları belirlemek üzere, **hedef ağ hakkında olabildiğince fazla bilgi toplama sürecidir.**
- ▶ Bilgi sistemlerine yönelik herhangi bir saldırının ilk adımıdır;
 - ▶ Saldırgan, sosyal mühendislik, sistem ve ağ saldırıları vb. kullanarak hassas bilgileri toplamaktadır.

Güvenlik durumu

Saldırganın hedef organizasyonun dış güvenlik durumunu bilmesine sağlar.

Odak Azaltma

Saldırgan: belirli IP adresleri, ağlar, alan adları, uzaktan erişim vb. indirger.

Zafiyetleri Bul

Uygun istismarları seçmek için hedef sistemdeki güvenlik açıklarını tanımasını sağlar.

Ağ Haritası

Hedef kuruluşun ağ altyapısının harmasını çıkarmasını sağlar.

Footprinting Hedefleri

Hedefler

► Ağ Bilgisinin Toplanması

- ▶ Domain Name
- ▶ Internal domain names
- ▶ Network blocks
- ▶ IP of the reachable systems
- ▶ TCP/UDP hizmetleri

- ▶ ACL
- ▶ VPN noktaları
- ▶ IDS bilgisi
- ▶ Kimlik doğrulama
- ▶ e-mail

► Sistem Bilgisinin Toplanması

- ▶ Kullanıcı/Grup isimleri
- ▶ Routing tabloları

- ▶ Sistem mimarisi
- ▶ Parolalar

► Kuruluş Bilgilerini Toplanması

- ▶ Çalışan detayları
- ▶ Web sitesi
- ▶ Telefon numaraları

- ▶ **HTML kodları comments**
- ▶ Güvenlik Politikaları
- ▶ Kuruluşun Website Linkleri

İçindekiler

- 1 Footprinting Konsepti
 - Tanım
 - Footprinting Hedefleri
 - 2 Yöntem
 - Arama Motorları
 - Document Metadata
 - Google Teknikleri
 - Sosyal Ağ Siteleri
 - Website Footprinting
 - Email Footprinting
 - WHOIS
 - DNS Footprinting
 - 3 Araçlar
 - Maltego
 - FOCA
 - 4 Countermeasure
 - Countermeasure
 - 5 Lab
 - Windows Komut Satırı
 - Çevirimiçi Kişisel Bilgi Arama Servisleri
 - Path Analyzer Pro kullanarak Network Route Tracing
 - Maltego

Public ve Kısıtlanmış Websiteslerinin Bulunması

- ▶ Hedefin dış URL bilgilerinin **Google**, **Bing** gibi arama motorları ile bulunması
 - ▶ Kuruluşun farklı birimleri için kullanılan URL bilgileri ile erişim sağlanabilir
 - ▶ <http://www.netcraft.com>

Search: search tips

example: site contains .netcraft.com

Results for tubitak.gov.tr

Found 10 sites

Site	Site Report	First seen	Netblock	OS
1. bilgem.tubitak.gov.tr		february 2011	tubitak - uekae	unknown
2. www.tubitak.gov.tr		august 1995	tubitak	unknown
3. sge.bilgem.tubitak.gov.tr		march 2014	tubitak - uekae	citrix netscaler
4. journals.tubitak.gov.tr		october 2004	tubitak	unknown
5. ulakbim.tubitak.gov.tr		march 2014	tubitak - uekae	unknown
6. online.journals.tubitak.gov.tr		june 2010	tubitak	unknown
7. www.bilimgenc.tubitak.gov.tr		december 2014	tubitak	unknown
8. www.dijitaldonusum.yte.bilgem.tubitak.gov.tr			tubitak - uekae	unknown
9. mcs.bilgem.tubitak.gov.tr		june 2016	tubitak - uekae	unknown
10. tubitak.gov.tr		january 2016	tubitak	unknown

İşletim Sistemi Bilgisinin Elde Edilmesi

Netcraft kullanılarak hedef organizasyonun **İşletim Sistemi** bilgisinin elde edilmesi

Results for tubitak.gov.tr

Found 10 sites				
Site	Site Report	First seen	Netblock	OS
1. bilgen.tubitak.gov.tr		february 2011	tubitak - seleas	unknown
2. www.tubitak.gov.tr		august 1995	tubitak	unknown
3. ege.bilgen.tubitak.gov.tr		march 2014	tubitak - seleas	citrix netscaler
4. journals.tubitak.gov.tr		october 2004	tubitak	unknown
5. uludem.tubitak.gov.tr		March 2014	tubitak - seleas	unknown
6. online.journals.tubitak.gov.tr		june 2010	tubitak	unknown
7. www.bilimgen.tubitak.gov.tr		december 2014	tubitak	unknown
8. www.dijitalosman.yte.bilgen.tubitak.gov.tr			tubitak - seleas	unknown
9. mcu.bilgen.tubitak.gov.tr		june 2016	tubitak - seleas	unknown
10. tubitak.gov.tr		January 2016	tubitak	unknown

Hosting History

Netblock owner	IP address	OS	Web server	Last seen
TUBITAK	193.140.81.167	unknown	Apache-Coyote/1.1	4-Jan-2017
TUBITAK	193.140.81.167	Linux	Apache-Coyote/1.1	29-Aug-2015
TUBITAK	193.140.80.202	Linux	Apache/2.2.3 Red Hat	9-Jun-2014
TUBITAK	193.140.80.202	Linux	Apache/2.0.52 Red Hat	12-Nov-2007
unknown	193.140.80.201	Linux	Apache/2.0.52 Red Hat	27-Jun-2013
unknown	193.140.80.201	Linux	Apache	21-May-2005
unknown	193.140.80.201	Linux	Apache/2.0.52 Unix mod_ssl/2.0.52 OpenSSL/0.9.7a mod_auth_pgsql/2.0.1 PHP/4.3.2	12-Feb-2005

Shodan I

<http://www.shodan.io>

Shodan, çevirmiçi spesifik cihazlar için arama motorudur. En popüler olanları: **webcam**, **linksys**, **cisco**, **SCADA**, v.s.

The image shows the Shodan search interface. At the top, there's a navigation bar with links for Shodan, Developers, Book, View All..., Explore, Downloads, Reports, Enterprise Access, and Contact Us. The main search bar has a placeholder 'Search' and a red search button. Below the search bar, a large red banner features the text 'The search engine for the Internet of Things'. Underneath the banner, a subtext reads 'Shodan is the world's first search engine for Internet-connected devices.' At the bottom, there are two buttons: 'Create a Free Account' (red) and 'Getting Started' (blue). To the right of the banner, there's a 3D globe visualization with numerous red dots representing discovered devices, with some specific IP addresses like '20.69.105.20', '56.87.75.184', and '104.184.18.61, 231' labeled.



Explore the Internet of Things

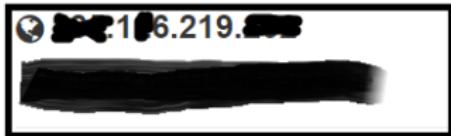
Use Shodan to discover which of your devices are connected to the Internet, where they are located and who is using them.



See the Big Picture

Websites are just one part of the Internet.
refrigerators and much more that can be fo

Shodan II



Country Turkey

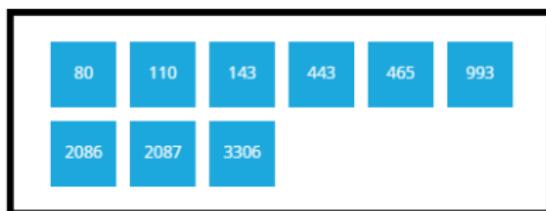
Organization

ISP Onur Eken

Last Update 2016-11-22T05:45:29.864699

Hostnames

Ports



Services



Shodan III

Anahtar Kelimeler

- ▶ **country**: Belirtilen ülke kodunda arama yapar.
 - ▶ **city**: Belirtilen şehirde filtreleme yapar.
 - ▶ **geo**: Koordinatlarda arama yapar.
 - ▶ **hostname**: Hostname yada domain bilgisine göre filtreleme yapar.
 - ▶ **net**: Özel IP yada subnet aralığında filtreleme yapar.
 - ▶ **os**: İşletim sistemine göre filtreleme yapar.
 - ▶ **port**: Port bilgisine göre filtreleme yapar.

Document Metadata I

Document Metadata

- ▶ Birçok doküman formatı oldukça fazla sayıda metadata (data about data) bilgisi içermektedir.
 - ▶ Dökümanların nasıl formatlandığı ve nasıl gösterilmesi gereği ile ilgili bilgiler
 - ▶ Fakat bazı metadatalar daha fazla bilgi içerir
 - ▶ Metadata içerisinde olabilecek olan bilgiler
 - ▶ **Usernames:** Sızma testi yapan kişiler genellikle, istismar ve şifre tahmin saldırularına yönelik kullanıcı adlarına ihtiyaç duyarlar.
 - ▶ **File system paths:** hedef kuruluş hakkında önemli bilgilere, önemli dosya sunucularına, kritik dizinlere ve verilen kullanıcının genel uygulamalarına ilişkin ipuçları
 - ▶ **E-mail addresses:** Penetrasyon testi kapsamı "kimlik avı testleri" ni içeriyorsa (bağlantıları tıklatacak mı yoksa ekleri mi açacaklarını görmek için hedef personele e-posta göndemek)
 - ▶ Client-side software in use (Office suite, PDF-generating tool, operating system type, and such)
 - ▶ **Diger bilgiler:** Other information not displayed on the screen from within the application associated with the document ("undo" data, previous revisions, hidden or obscured fields, and more)

Document Metadata II

Meta Veri'de Zengin Olan Belge Türleri

- ▶ pdf files
 - ▶ ppt, pot, and ppth files
 - ▶ doc, dot, and docx files
 - ▶ jpg and jpeg
 - ▶ xis, xlt, and xlsx files
 - ▶ html and htm

Document Metadata III

Meta Veri Analizi için Belgeleri Alma

- ▶ Testin planlanması sırasında hedef sistem personeli tarafından gönderilen belgeleri gözden geçirin (sözleşmeler, NDA'lar, sözleşme vb.)
 - ▶ E-posta ile gönderilebilecek çeşitli tipteki belgeleri isteyin
 - ▶ Web spyder kullanarak dokümanları web sitesinden çekin
 - ▶ Kurum içi dosya sunuculardan belgeler toplanabilir.

Document Metadata IV

Belge Meta Verilerini Analiz Etme Araçları

- ▶ Belge meta verilerini analiz etmek için çok farklı araçlar vardır:
 - ▶ Exif
 - ▶ FOCA
 - ▶ The Metadata Extraction Tool was developed by the National Library of New Zealand
 - ▶ strings

Document Metadata V

Exif Tool

- ▶ **ExifTool**: Reads, writes, and changes metadata
 - ▶ Freely distributed, written by Phil Harvey
<https://www.sno.phy.queensu.ca/~phil/exiftool/>
 - ▶ Runs on Windows, Linux, and Mac OS X
 - ▶ Supports more than 100 file types and many metadata formats
 - ▶ Original focus was on image and audio files
 - ▶ Many different image types, pulling out camera type, editing tools, and geotags if they are present
 - ▶ Now it has been expanded to include many file types, including various document file types (doc, docx, xis, xlsx, ppt, pptx, pdf, and so on)
 - ▶ Parses out specific fields, and is handy for determining usernames and software versions used to create or edit files
 - ▶ Processes entire directories, with recursion supported

Document Metadata VI

Strings komutu

- ▶ bir dosyada yazdırılabilir metni görüntüler.
 - ▶ Good for finding nonstructured data or data for which you don't know the structure
 - ▶ Included in most Linux distributions and UNIX varieties
 - ▶ Available as separate download for Windows

<https://docs.microsoft.com/en-us/sysinternals/downloads/strings>

Document Metadata VII

Uygulama

- ▶ Hedef bir hesaptan PDF, Word, Excel dosyalarının elde edilmesi

```
# wget -nd -r -A pdf,doc,xls,-P /home/bqm531/metadata [tgt_domain]
```

- #### ► Options we used:

- ▶ -nd: No directories (places all files in specified directory)
 - ▶ -r: Recursive download
 - ▶ -P [directory]: Prefix output file locations with [directory]
 - ▶ -R/A: Restrict or allow file types or patterns

- ## ► Exif

- strings -n 10

Lokasyon Bilgisi

Google Maps

Hedefin fiziksel lokasyonun bulunması amacıyla Google Maps kullanılabilir



Araclar

- ▶ **Google maps**
<https://maps.google.com>
 - ▶ **Wikimapia**
<http://wikimapia.org>
 - ▶ **National Geographic Maps**
<https://www.nationalgeographic.com/maps/>
 - ▶ **Yahoo Maps**
<https://maps.yahoo.com>
 - ▶ **Bing Maps**
<https://www.bing.com/maps>

Kişi Arama

- ▶ Sosyal Ağ siteleri, kuruluş ve kişiler hakkında bilgi toplamak için oldukça iyi bir kaynaktır.
 - ▶ Kişiler hakkında aramalar sonucunda **hem kişi hem kuruluşlar hakkında bilgile elde edilebilmektedir.**
 - ▶ Ev adresleri, e-posta
 - ▶ Tel no, doğum tarihi
 - ▶ Fotolar, sosyal ağ profilleri
 - ▶ Blog URL bilgileri
 - ▶ Adreslerin uydu fotoğrafları
 - ▶ Yeni yapılacak projeler

Çevrimiçi Hizmetler

Çevrimiçi Hizmetler

- ▶ **AnyWho**
<https://www.anywho.com>
 - ▶ **US Search**
<http://www.ussearch.com>
 - ▶ **Intelius**
<https://www.intelius.com>
 - ▶ **411**
<https://www.411.com>
 - ▶ **Peoplefinders**
www.peoplefinders.com
 - ▶ **PeopleSmart**
www.peoplesmart.com
 - ▶ **Veromi**
<https://www.veromi.net>
 - ▶ **PrivateEye**
www.privateeye.com
 - ▶ **People Search Now**
www.peoplesearchnow.com
 - ▶ **PublicBackgroundChecks**
publicbackgroundchecks.com

[İş İlanı Siteleri](#)

İş ilanı/Kariyer siteleri kullanılarak kuruluş hakkında bilgiler toplanabilir.

- Kariyer.net ► Linkedin ► Indeed ► Monster

GENEL NİTELİKLER

[REDACTED] one of the largest telecommunications companies in the world, has mobile operations in 26 countries (partnering with mobile networks in 55 more) and fixed broadband operations in 17 markets, serving 446 million mobile customers and 12 million fixed broadband customers around the world. Vodafone is strongly committed to lead the digital transformation in the Turkish Market, where the company has been operating and investing heavily since 2006.

- At least 10 years experience in a data warehouse environment
 - Strong background in data warehouse concepts / strategie
 - Capacity monitoring and management capabilities
 - Configure new Oracle Databases, implementing new releases and patches
 - Tuning of SQL and PL/SQL
 - Managing and monitoring of Oracle Exadata database machine
 - Deep understanding of Oracle Exadata machine
 - Implementation of Oracle Recovery Manager for online database backups
 - Managing and monitoring 10g/11g/12c Data Guard systems
 - Managing 11g EM and 12c/13c Grid Control
 - Strong query and database tuning skills
 - Extensive UNIX shell scripting, PLSQL, and SQL skills
 - Fast troubleshooting and resolution skills
 - Extensive experience with very large data warehousing systems
 - Data Replication (Oracle GoldenGate, Data Integration, Abinitio etc.) experience
 - Fluency in English

Google Teknikleri I

Query String

- ▶ **Google Hacking:** hassas veya gizli bilgileri çıkarmak için karmaşık arama soruları oluşturmak

Savunmasız Hedefler

- ▶ Saldırganlara savunmasız hedefleri bulabilmesinde yardımcı olur.

Google Operators

- ▶ Arama sonuçlarında belirli metin dizelerini bulmak için gelişmiş Google arama operatörlerini kullanmak

Google Teknikleri II

Search Operators

- ▶ [cache :] "Google Cache"de saklanan web sayfalarını görüntüler
 - ▶ [link :] Belirtilen web sitesine link veren sayfaları listeler
 - ▶ [related :] Belirtilen web sitesine benzer sayfaları listeler
 - ▶ [info :] Web sitesi hakkında bazı bilgiler verir
 - ▶ [site :] Web sayfasının domain'i içinde yer alan sayfaları listeler
 - ▶ [allintitle :] Aranan kelimelerinin **hepsinin** başlık bilgisinde yer alması durumunda sonuçları gösterir
 - ▶ [intitle :] Aranan kelimenin başlık bilgisinde yer alması durumunda sonuçları gösterir
 - ▶ [allinurl :] Aranan kelimelerinin **hepsinin** URL'de yer alması durumunda sonuçları gösterir
 - ▶ [inurl :] Aranan kelimelerinin URL'de yer alması durumunda sonuçları gösterir

Google Teknikleri III

Tümü Haberler Görseller Videolar Alışveriş Daha fazla Ayarlar Araçlar

Yaklaşık 264.000 sonuç bulundu (0,39 saniye)

[PDF] **HİZMETE ÖZEL T.C SAĞLIK BAKANLIĞI Türkiye İlaç ve Tıbbi Cihaz ...**
<https://www.titck.gov.tr/PortalAdmin/Uploads/UnitPageAttachment/uCKfDEHd.pdf> ▾
8 Haz 2016 - 01.03.2016 tarihi itibarıyle Kurumumuz bünyesinde kullanılan elektronik veri sisteminde değişiklik yapılmış olup, söz konusu sistem TİTCK ...

[PDF] **Metotreksat iç - Türkiye İlaç ve Tıbbi Cihaz Kurumu**
<https://www.titck.gov.tr/PortalAdmin/Uploads/Titck/Dynamic/metotreksat.pdf> ▾
2 Kas 2017 - Metotreksat etkin maddesini içeren, kullanıma hazır şırınga/enjektör formunda olan ilaçların, kısa ürün bilgilerinin ilgili bölümlerde yer alan ...

[PDF] **Bilgi Varlıklarının Gizlilik Derecelerinin Sınıflandırılması Kılavuzu**
www.udhb.gov.tr/doc/siberg/siberbilgi.pdf ▾
Bu gizlilik dereceleri ağırlıklı olarak "ÇOK GİZLİ", "GİZLİ", "ÖZEL", ... Ayrıca yönerge ile "HİZMETE ÖZEL" milli gizlilik derecesi de dahil olmak üzere gizlilik ...

[PDF] **Evrap Yönetimi Usul ve Esasları - Sayıştay**
https://www.sayistay.gov.tr/tr/Upload/95906369/.../Evrap_Yonetim_UsulEsaslar.pdf ▾
MADDE 1- (1) Bu Usul ve Esasların amacı; Sayıştayın hizmet ve faaliyetleri ... h) Gizlilik dereceli evrap: Üzerinde çok gizli, gizli, özel ve hizmete özel ibaresi.

[PDF] **hizmete özel - KAYSİS**
<https://kms.kaysis.gov.tr/Home/Goster/73064> ▾

Google Hacking Databases

Google Hacking Database (GHDB)

Search the Google Hacking Database or browse GHDB categories

Files Containing Passwords ▾ Search Search

<< prev 1 2 3 4 5 6 >> next

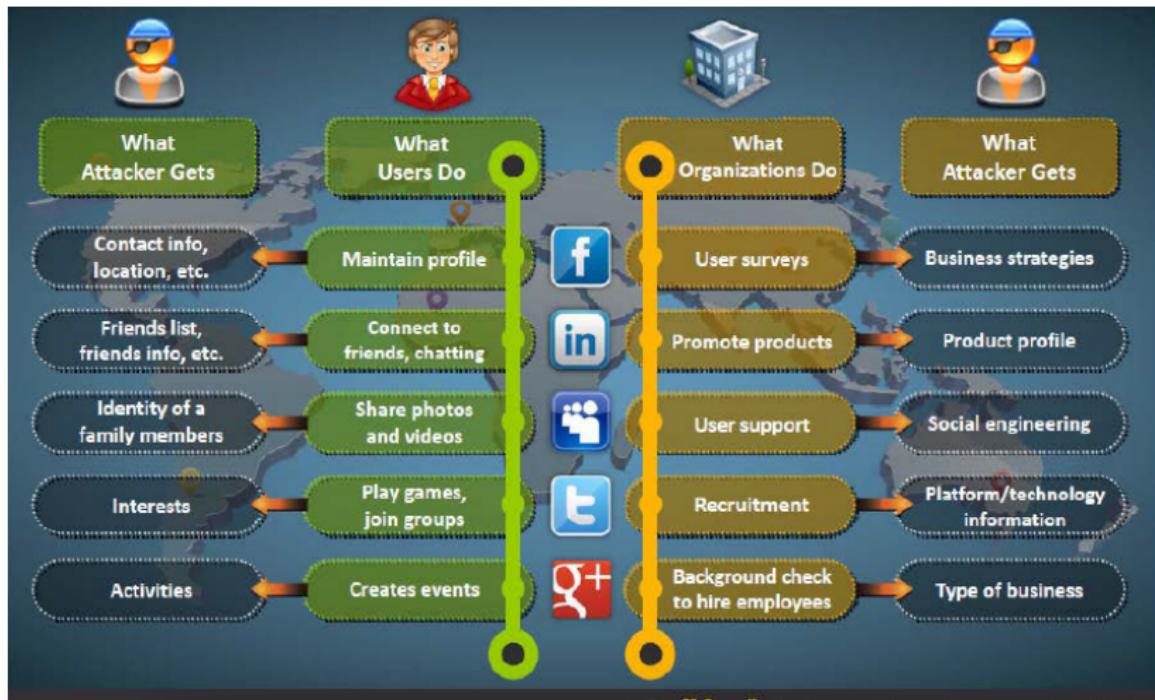
Date	Title	Summary
2017-10-30	site:trello.com password	Files Containing Passwords This will bring public Trello boards often containing user names and passwords. It can also help to find the context from the other cards published or fine-tune ...
2017-10-30	inurl:"gradle.properties" intext:"proxyPassword"	Files Containing Passwords Google Dork: Files Containing Passwords Exploit Author: Huijun Chen
2017-10-17	intext:connectionString & inurl:web & ext:config	Files Containing Passwords *Categories* Files containing passwords *Summary* A Google dork that gives you access to connection strings for various databases.

- ▶ intext:connectionString & inurl:web & ext:config - örnek site
http://bangskeem.dk/Web.config

Sosyal Ağ Siteleri I

- ▶ Saldırganlar, **Facebook, Linkedin, Twitter, Pinterest** ve **Google+** gibi sosyal ağ sitelerinden hassas bilgi toplamak için sosyal mühendislik kullanırlar.
 - ▶ Saldırganlar, sosyal paylaşım sitelerinde **sahte profil** oluştururlar ve bunu kullanarak kuruluş çalışanlarından hassas bilgileri elde etmeye çalışırlar.
 - ▶ Çalışanlar, doğum tarihi, eğitim ve iş geçmişleri, eş adları vs. gibi kişisel bilgilerinin yanında **kuruluş ile ilgili olarak**, potansiyel müşteriler ve iş ortakları, şirketlerin ticari sırları, web siteleri, şirketin gelecek haberleri, birleşmeleri, satın almaları gibi hakkında bilgi verebilir.
 - ▶ Saldırganlar, **çalışanlarının ilgi alanlarını**, gruplarını izleyerek toplamaktadırlar ve daha fazla bilgiye sahip olmak için çalışanı kandırmayı hedeflemektedirler.

Sosyal Ağ Siteleri II



Website Footprinting I

Hedef kuruluşun web sitesini izleme ve inceleme

- ▶ Kullanılan yazılım ve versiyon bilgisi
- ▶ İşletim sistemi
- ▶ Sub-directories
- ▶ Dosya, klasör, veritabanı alanadı, SQL
- ▶ Scripting platform
- ▶ İletişim detayları

```

GET /research/iframe_parent?input=http://localhost HTTP/1.1
Host: labs-linux:81
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.11; rv:45.0) Gecko/20100101 Firefox/45.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-GB,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://labs-linux:81/research/
Connection: close
    
```

Burp suite, Zaproxy, Paros Proxy, Website Informer, Firebug araçları ile

- ▶ Connection-status, content-type
- ▶ Accept-ranges
- ▶ Last-Modified
- ▶ X-Powered-By
- ▶ Web server ve versiyon

Website Footprinting II

HTML Kaynak Kodu

- ▶ Comments in source code
 - ▶ Contact details of web developer and admin
 - ▶ File system structure
 - ▶ Script Type

Coockies

- ▶ Software in use and its behaviour
 - ▶ Scripting platform used

Web Spiders

Web Spiders

- ▶ **Web spider** kullanımı ile hedef sitenin otomatize edilerek sorgulanması ile beraber çalışan isimleri, email adresleri, gibi birçok bilgi toplanabilmektedir.
 - ▶ Saldırganlar bu bilgileri kullanarak footprinting ve sosyal mühendislik saldıruları için kullanılmaktadırlar.

Araclar

- ▶ GSA Email Spider
 - ▶ Web Data Extractor

Sitenin Kopyasının Alınması

Offline Mirroring Website

- ▶ Websitesinin tamamının çevirdiği olarak lokal bilgisayar kopyalanması ile klasör yapısı ve diğer bilgiler elde edilebilmektedir.
 - ▶ Bütün klasörler, HTML, images, flash, videos, ve diğer bilgiler
 - ▶ config.php.bak, config.asp.bak gibi backup dosyaları

Araclar

- ▶ HTTrack Web Site Copier
 - ▶ SurfOffline

<http://www.archive.org>

Web sayfasının arşivelenmiş versiyonlarına erişimi sağlamaktadır.

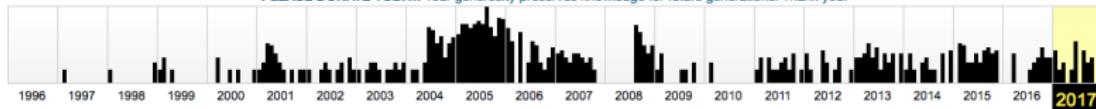


Explore more than 308 billion web pages saved over time

Sayed 848 times between February 4, 1997 and October 19, 2017

Summary of tubitak.gov.tr

PLEASE DONATE TODAY. Your generosity preserves knowledge for future generations. Thank you.



JAN							FEB							MAR							APR									
1	2	3	4	5	6	7	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4				
8	9	10	11	12	13	14	5	6	7	8	9	10	11	5	6	7	8	9	10	11	2	3	4	5	6	7	8			
15	16	17	18	19	20	21	12	13	14	15	16	17	18	12	13	14	15	16	17	18	9	10	11	12	13	14	15			
22	23	24	25	26	27	28	19	20	21	22	23	24	25	19	20	21	22	23	24	25	16	17	18	19	20	21	22			
29	30	31					26	27	28					26	27	28	29	30	31					23	24	25	26	27	28	29

Website-Watcher I

Website-Watcher ile değişiklikleri ve güncellemeleri otomatik olarak izlenmesi

The screenshot shows the Website-Watcher 2010 application interface. On the left, there's a sidebar with a tree view of bookmarks categorized into General, Magazines, News, and private sections. The 'General' section has 18 items, including 'AutoWatch' (19), 'wswatch' (1), 'Website-Watcher - Down...' (4), 'Website-Watcher - Sup...' (4), and 'WSW Forum RSS' (18). Below this is a detailed view of the 'WSW Forum RSS' entry, which points to [www.website-watcher.com](http://www.website-watcher.com/forum/). The main pane displays the forum's RSS feed with 23 items. A yellow callout box highlights the first item: '(WebSite-Watcher Support) -- RE: Report if bookmark is filtered/unfiltered? -- (Martin Aignesberger)'. The text in this item discusses command-line parameters for starting the application minimized.

RSS/Atom feeds with new articles. Feeds are automatically converted into a readable format.

Name	URL	Last change	Status	Last check
DIR: wswatch	D:\wswatch	12:58	OK	12:58
Website-Watcher - Down...	http://www.a...	12:45	OK	12:45
Website-Watcher - Sup...	http://www.a...	12:46	OK, phpBB2 PL...	12:46
WSW Forum RSS	http://www.a...	11:03	OK	12:41
www.website-watcher.c...	http://www.a...	12:53	OK	12:52
www.website-watcher.c...	http://aig...	2006-07-08 15:12:59	OK	2006-07-08 ...
news://asp.memberste...	news://asp.me...	09:51	OK	09:51

Website-Watcher II

Diger Araclar

- ▶ Change Detection
 - ▶ Follow That Page
 - ▶ Page2RSS
 - ▶ Watch That Page
 - ▶ Check4Change
 - ▶ OnWebChange
 - ▶ Infominder
 - ▶ TrackedContent
 - ▶ Websnitcher
 - ▶ UpdateScanner

Email Header

Delivered-To: mr.google@gmail.com
 Received: by 10.112.38.167 with SMTP id q7cs
 Sat, 1 Jun 2013 21:24:01 -0700 (PDT)
 Return-Path: <mr.google@gmail.com>
 Received-SMTP: pass (google.com domain of
 sender) Client-ip:10.224.205.137
 Authentication-Results: mr.google.com spf=pass
 10.224.205.137 (permitted sender) smtp.mail:
 header.i=mr.google.com
 Received: from mr.google.com ([10.224.205.137])
 by 10.224.205.137 with SMTP id fq9m-8578570qab.39.1
 Sat, 01 Jun 2013 21:24:00 -0700 (PDT)
 DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed;
 s=gmail-smtp-in20120114;
 d=gmail.com; s=20120114;
 h=mime-version:in-reply-to:references:
 content-type:to:subject:from:to
 bh=TSEIBh4i17gFQG+ghh7OKPjx+tc/1AC1
 b=MguzLTifg24QZxxZKex1NvfcnD/+P4+Nc5HxSPtG7bRX0eFv/hGR4de2P+75MxDR8
 blPNk3eJ3Uf/CsaBZWDIT0XLakOAGrP35b0C92MCZFrXUQ9uwL/xHALSnskeUIEEeKgq0C
 ca9hD59D3oX1E9AC72mbh1GzXmV4D1WffCL9942aM8C0cMzRw0WW1k95a138aqtfP
 ZhrWFxKh5xSnZxsE73xZPEYzp7yeCcQuyHENGslxco7QjeZuw+HMK/VRE6xChDapZ4
 K5ZRaFYZmzIKFX+VdL3qu7YGFry&HeuP16yS/C2fXHViemuYamMT/yecvhCVo80g7FKt6
 /KZw=
 MIME-Version: 1.0
 Received: by 10.224.205.137 with SMTP id fq9m
 Sat, 01 Jun 2013 21:24:00 -0700 (PDT)
 Received: by 10.229.230.79 with HTTP/ Sat, 1
 In-Reply-To: <CAOYWAAT1lzdDXKE3o8D2rh1E8p12MtV0uhro6r+7Mu7cubp@Eq@mail.gmail.com>
 References: <CAOYWAAT1lzdDXKE3o8D2rh1E8p12MtV0uhro6r+7Mu7cubp@Eq@mail.gmail.com>
 Date: Sun, 2 Jun 2013 09:53:59 +0530
 Message-ID: <CAMSVOXIUGEfNFWsJDSzQhnn=EMJgfgX+mUfjb_t2sy2dR@mail.gmail.com>
 Subject: [REDACTED] LUTIONS :::
 From: [Mirza <\[REDACTED\]@erma@gmail.com>](mailto:Mirza <[REDACTED]@erma@gmail.com>)
 To: [\[REDACTED\]@erma@gmail.com](mailto:[REDACTED]@erma@gmail.com), [\[REDACTED\]@erma@yahoo.com](mailto:[REDACTED]@erma@yahoo.com), [\[REDACTED\]@er@yahoo.com](mailto:[REDACTED]@er@yahoo.com)

The address from which the message was sent
 Sender's IP address
 Sender's mail server
 Designates 10.224.205.137 as permitted
 in of mr.google@gmail.com designates
 b6m; dkim-pass
 Date and time received
 by the originator's
 email servers
 Authentication system
 used by sender's
 mail server
 Object: from to
 Date and time of
 message sent
 A unique number assigned
 by mr.google.com to
 identify the message
 Sender's full name

WHOIS I

WHOIS veritabanları **Regional Internet Registries** tarafından işletilmektedir.
Domain sahipleri hakkında kişisel bilgiler içermektedir.

Sorgu Sonuçları

- ▶ Domain name detayları
 - ▶ Domain sahibinin iletişim bilgileri
 - ▶ Domain name sunucuları
 - ▶ NetRange
 - ▶ Domain oluşturma tarihi
 - ▶ Bitiş kayıtları
 - ▶ Son güncelleme

Saldırgan

Sosyal mühendislik saldırıları için kişisel bilgiler

RIRs

- ARIN ► AFRINIC ► RIPE ► APNIC

WHOIS II



tubitak.gov.tr is already registered*

**** Registrant:**

Türkçe Bilimsel ve Teknik Araştırmalar Kurumu
Atatürk Bulvarı No:221 Kavaklıdere
06100
Ankara,
Türkiye
root@tubitak.gov.tr
+ 90-312-4272388-
+ 90-312-4677264

**** Administrative Contact:**

NIC Handle : ttb73-metu
Organization Name : T?B?TAK T?rkiye Bilimsel ve Teknolojik Ara?t?rma Kurumu
Address : T?B?TAK Ba?kan?k Tunus Caddesi No:80 06100 Kavaklı

Ankara, 06100
T?rkiye
Phone : + 90-312-4685300-1064
Fax : + 90-312-4688613-

**** Technical Contact:**

NIC Handle : ttb73-metu
Organization Name : T?B?TAK T?rkiye Bilimsel ve Teknolojik Ara?t?rma Kurumu
Address : T?B?TAK Ba?kan?k Tunus Caddesi No:80 06100 Kavaklı

DNS Footprinting I

Saldırgan DNS bilgisiyle ağ üzerinde yer alan sunucular hakkında bilgi toplayarak bunlara sosyal mühemdislik saldıruları yapmayı hedeflemektedir.

Record Type	Description
A	Host's IP address
MX	Domain's mail server
NS	Host's name server
CNAME	Canonical naming allows aliases to a host
SDA	Authority for domain
SRV	Service records
PTR	Maps IP address to a hostname
RP	Responsible person
HINFO	Host information record includes CPU types and OS
TXT	Unstructured text records

DNS Footprinting II

DNS records

name	class	type	data	time to live
tubitak.gov.tr	IN	SOA	server: ns1.tubitak.gov.tr email: root@tubitak.gov.tr serial: 2017092701 refresh: 60 retry: 1800 expire: 604800 minimum ttl: 60	60s (00:01:00)
tubitak.gov.tr	IN	NS	ns1.tubitak.gov.tr	60s (00:01:00)
tubitak.gov.tr	IN	NS	ns2.tubitak.gov.tr	60s (00:01:00)
tubitak.gov.tr	IN	A	193.140.80.208	60s (00:01:00)
tubitak.gov.tr	IN	MX	preference: 10 exchange: sfmail01.tubitak.gov.tr	60s (00:01:00)
tubitak.gov.tr	IN	TXT	v=spf1 mx a:tubitak.gov.tr a:mta01.tubitak.gov.tr a:sfmail01.tubitak.gov.tr ip4:193.140.13.192/27 ip4:193.140.80.89/32 a:mail.ume.tubitak.gov.tr a:smtp.ume.tubitak.gov.tr mx:bilgi.tubitak.gov.tr a:mail.pardus.org.tr -all	60s (00:01:00)
208.80.140.193.in-addr.arpa	IN	PTR	tubitak.gov.tr	86400s (1.00:00:00)
80.140.193.in-addr.arpa	IN	SOA	server: ns1.tubitak.gov.tr email: root@tubitak.gov.tr serial: 2017072401 refresh: 3600 retry: 1800 expire: 604800 minimum ttl: 60	86400s (1.00:00:00)

Şekil: Domain Dossier

DNS Footprinting III

Araçlar

- ▶ **DIG**
www.kloth.net
 - ▶ **myDNSTools**
www.mydnstools.info
 - ▶ **Professional Toolset**
www.dnsstuff.com
 - ▶ **DNS Records**
network-tools.com
 - ▶ **DNSData View**
www.ultratools.com
 - ▶ **www.nirsoft.net**
 - ▶ **DNSWatch**
www.dnswatch.info
 - ▶ **DomainTools**
www.domaintools.com
 - ▶ **DNS Query Utility**
www.dnsqueries.com
 - ▶ **DNS Lookup**
www.ultratools.com

Network Range

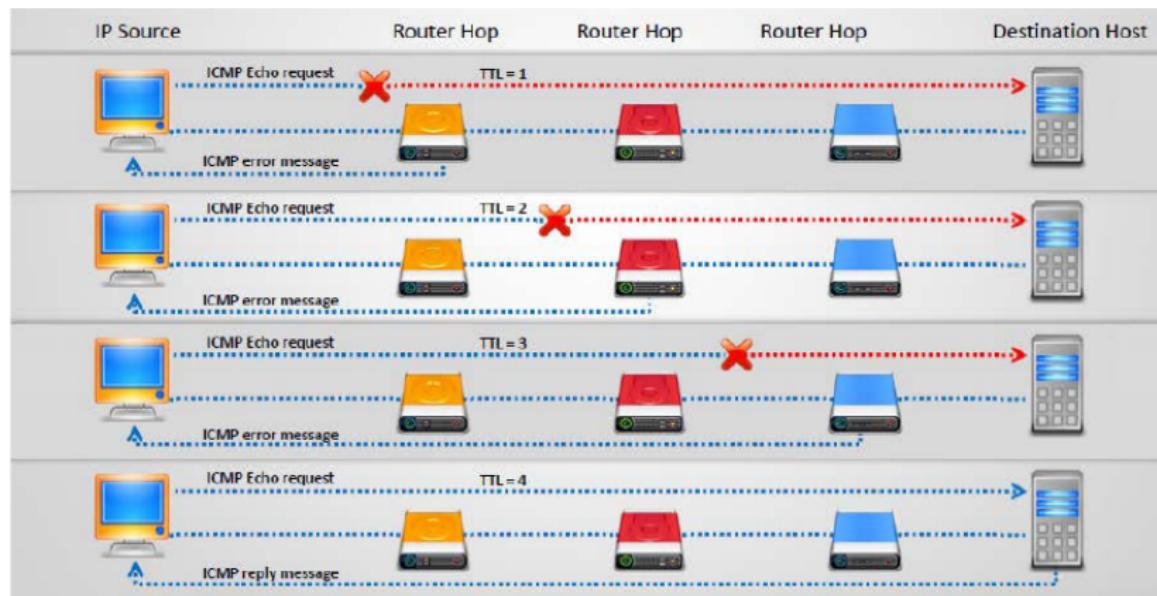
Network Range

- ▶ **Network range** bilgisini kullanarak saldırganlar **hedef ağ haritası** oluşturmaktadır.
 - ▶ **ARIN whois veritabanı arama** aracı kullanılarak **IP range** bilgisini bul.
 - ▶ **Regional Internet Registry** (RIRs) kullanılarak hedef kuruluşun **IP adres aralığı** bulunabilir.

Traceroute I

- ▶ **ICMP protokolü ve ICMP paketlerinde yer alan TTL alanı** kullanılarak hedef bilgisayara erişmek için kullanılan yol üzerinde bulunan router'lar keşfedilmektedir.

Traceroute II



Traceroute III

- ▶ **Network topology, trusted routers ve firewall location** gibi bilgiler elde edilebilmektedir.
 - ▶ Örnek: birkaç traceroute işleminden sonra şu bilgilere erişilebilir.

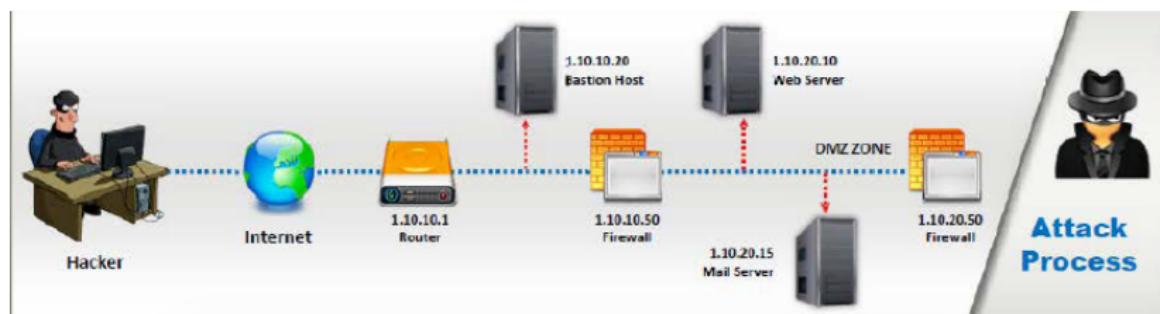
traceroute 1.10.10.20, second last hop is 1.10.10.1

traceroute 1.10.20.10, third to last hop is 1.10.10.1

traceroute 1.10.20.10, second to last hop is 1.10.10.50

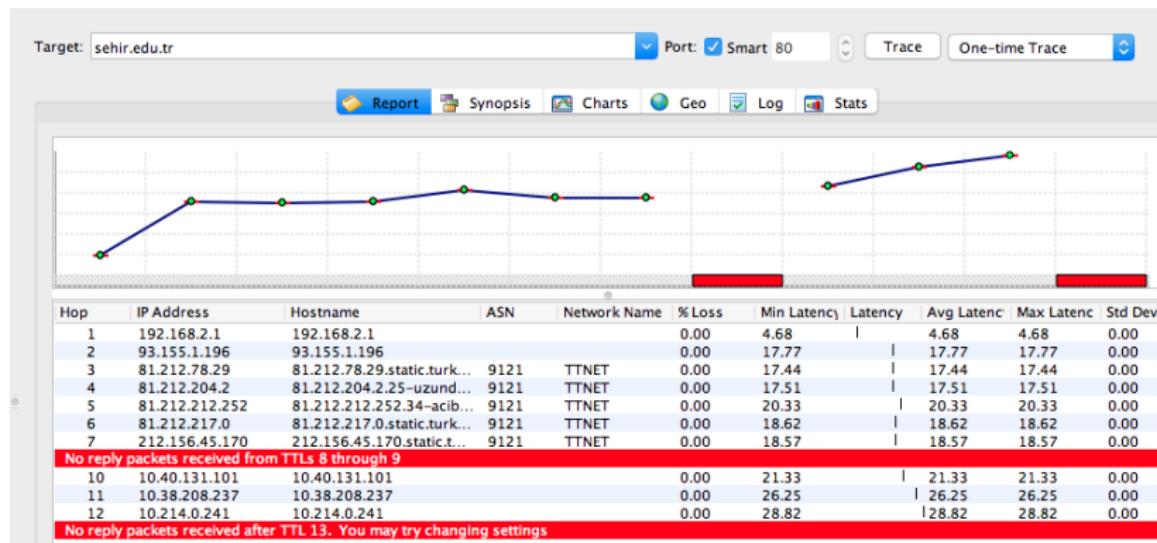
traceroute 1-10-20-15; third to last hop is 1-10-10-1

traceroute 1.1.1.1, child to last hop is 1.1.1.1
traceroute 1 10 20 15 - second to last hop is 1.10.10.50





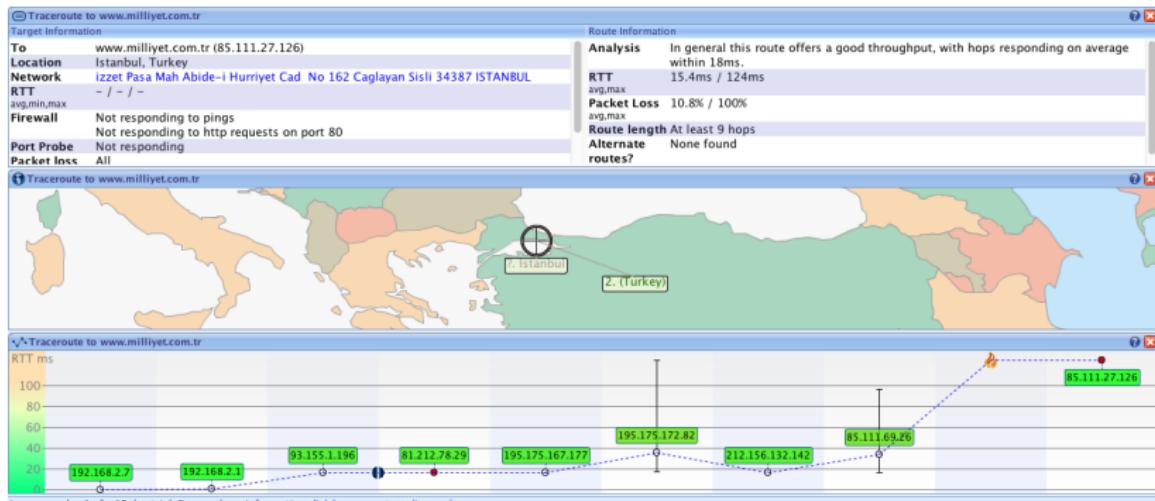
Traceroute IV



Şekil: Path Analyzer Pro



Traceroute V



Şekil: VisualRoute

Sosyal Mühendislik Yöntemleriyle Footprinting

- ▶ **Gizli bilgileri ele geçirmek** amacıyla **insan davranışlarının manipülasyonu**
 - ▶ İnsanların sahip olduğu değerli fakat farkında olmadıkları bilgilerin ele geçirilmesi

Sosyal Mühendisliğin Saldırıları

- ▶ Kredi kartı bilgisi
 - ▶ Kullanıcı adı ve şifreler
 - ▶ Güvenlik bileşenleri
 - ▶ İşletim sistemi ve versiyonu
 - ▶ Ağ mimarisi
 - ▶ Sunucuların IP adresleri

Sosyal Mühendislik Teknikleri

- ▶ Dinleme (Eavesdropping)
 - ▶ Omuzdan bakma (Shoulder Surfing)
 - ▶ Çöp karıştırma (Dumpster Diving)
 - ▶ Sosyal Ağlardan Kimlik elde edilmesi

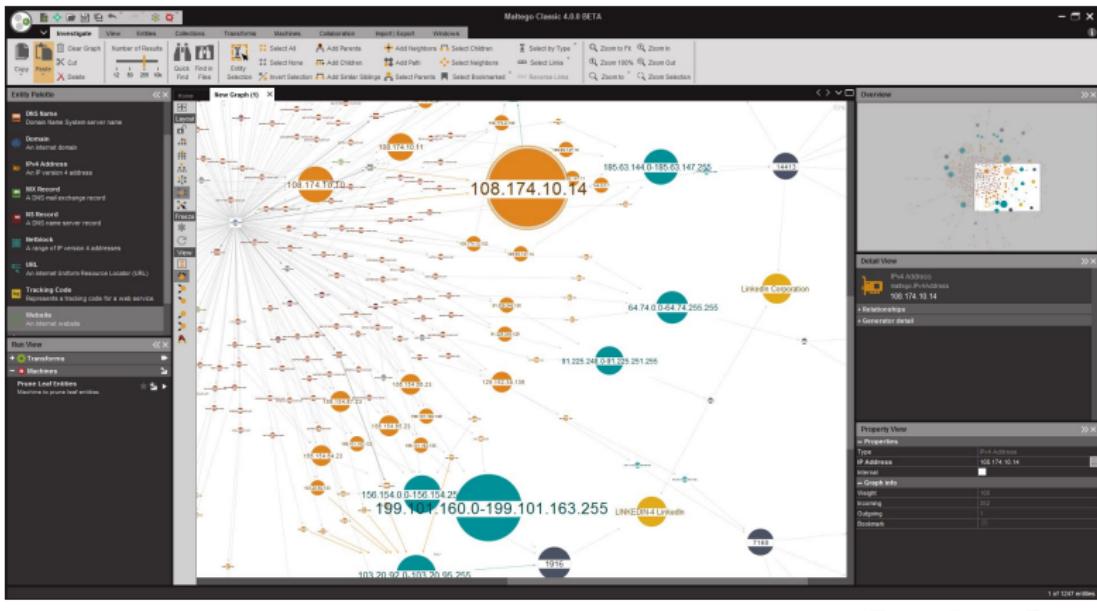
İçindekiler

- 1 Footprinting Konsepti
 - Tanım
 - Footprinting Hedefleri
 - 2 Yöntem
 - Arama Motorları
 - Document Metadata
 - Google Teknikleri
 - Sosyal Ağ Siteleri
 - Website Footprinting
 - Email Footprinting
 - WHOIS
 - DNS Footprinting
 - 3 Araçlar
 - Maltego
 - FOCA
 - 4 Countermeasure
 - Countermeasure
 - 5 Lab
 - Windows Komut Satırı
 - Çevirimiçi Kişisel Bilgi Arama Servisleri
 - Path Analyzer Pro kullanarak Network Route Tracing
 - Maltego

Maltego

Kişiler, gruplar (sosyal ağ), şirketler, organizasyonlar, web siteleri, dosyalar arasında bulunan ilişkiler ve linkleri bulmak için kullanılan bir uygulamadır.

<https://www.paterva.com>



FOCA

FOCA (Fingerprinting Organizations with Collected Archives), arama motorları kullanarak dökümanlar içerisinde yer alan gizli bilgilerin ve metadata bilgilerinin çıkarılmasını sağlamaktadır.

The screenshot shows the FOCA Free 2.6 application window. At the top, there's a navigation bar with links for File, Metadata, Domain Enumeration, Software Recognition, Tools, Logs, Options, and About. Below the navigation bar is a toolbar with icons for Network data, Metadata, and a search field. The main area features a cartoon character of a pink bear wearing a red 'FOCA' t-shirt. To the right of the character is a promotional box for 'Download the New FOCA 2.6' which lists '-DNS Snooping', '-Fingerprinting', '-HTTP Methods', and '-...and more'. On the left, there's a sidebar titled 'Custom search' with a tree view showing categories like Documents (0/207), Metadata Summary, Users, Folders, Printers, Software, and Operating Systems. The main content area displays a table of search results:

ID	Type	URL	Download	Download Date	Size	Analyzed	Modified Date
[1]0	doc	http://www.windowsecurity.com/uplaticle/10/21stcent...	x	-	169.5 KB	x	-
[1]1	doc	http://www.windowsecurity.com/uplaticle/8/probes.doc	x	-	176.5 KB	x	-
[1]2	doc	http://www.windowsecurity.com/uplaticle/information_...	x	-	57.5 KB	x	-
[1]3	doc	http://www.windowsecurity.com/uplaticle/10/IP_Secur...	x	-	124.5 KB	x	-
[1]4	doc	http://www.windowsecurity.com/uplaticle/10/RPFSec...	x	-	946.5 KB	x	-
[1]5	doc	http://www.windowsecurity.com/uplaticle/10/95virus.d...	x	-	6.11 MB	x	-
[1]6	doc	http://www.windowsecurity.com/uplaticle/10/uvw3.0.1...	x	-	121 KB	x	-
[1]7	doc	http://www.windowsecurity.com/uplaticle/18/LeverSec...	x	-	1.9 MB	x	-
[1]8	doc	http://www.windowsecurity.com/uplaticle/policyandsta...	x	-	737 KB	x	-
[1]9	pdf	http://www.windowsecurity.com/uplaticle/2/Access_C...	x	-	112.71 KB	x	-
[1]10	pdf	http://www.windowsecurity.com/uplaticle/websecurity/...	x	-	1.54 MB	x	-
[1]11	pdf	http://www.windowsecurity.com/uplaticle/1/ip-overve...	x	-	345.19 KB	x	-
[1]12	pdf	http://www.windowsecurity.com/uplaticle/18/rpfbstat...	x	-	89.33 KB	x	-
[1]13	pdf	http://www.windowsecurity.com/uplaticle/4/part3.pdf	x	-	293.29 KB	x	-
[1]14	pdf	http://www.windowsecurity.com/uplaticle/4/part4.pdfs...	x	-	55.66 KB	x	-
[1]15	pdf	http://www.windowsecurity.com/uplaticle/4/micrc.pdf	x	-	64.07 KB	x	-
[1]16	pdf	http://www.windowsecurity.com/uplaticle/4/part7.pdf	x	-	524.03 KB	x	-
[1]17	pdf	http://www.windowsecurity.com/uplaticle/5/banners.pdf	x	-	183.91 KB	x	-
[1]18	pdf	http://www.windowsecurity.com/uplaticle/4/random.pdf	x	-	167 KB	x	-
[1]19	pdf	http://www.windowsecurity.com/uplaticle/4/orxy.pdf	x	-	155.51 KB	x	-
[1]20	pdf	http://www.windowsecurity.com/uplaticle/4/frog.pdf	x	-	193.47 KB	x	-

At the bottom left, it says 'Error found searching in Exalead/Web'. On the right side, there are sections for 'Search engines' (Google, Bing, Exalead) and 'Extensions' (doc, ppt, pdf, xlsx, xls, ods, docx, xlsx, pdf, xps, vnd). A 'Search All' button is located at the bottom right.

İçindekiler

- 1 Footprinting Konsepti
 - Tanım
 - Footprinting Hedefleri
 - 2 Yöntem
 - Arama Motorları
 - Document Metadata
 - Google Teknikleri
 - Sosyal Ağ Siteleri
 - Website Footprinting
 - Email Footprinting
 - WHOIS
 - DNS Footprinting
 - 3 Araçlar
 - Maltego
 - FOCA
 - 4 Countermeasure
 - Countermeasure
 - 5 Lab
 - Windows Komut Satırı
 - Çevirimiçi Kişisel Bilgi Arama Servisleri
 - Path Analyzer Pro kullanarak Network Route Tracing
 - Maltego

Countermeasure I

Countermeasure II

Genel Çözümler

- ▶ Kurum çalışanlarının, kurum internet bağlantısını kullanarak **sosyal ağ sitelerine erişimi kısıtlanmalıdır.**
 - ▶ **Web sunucularından bilgi kaçağını** engelleyecek şekilde konfigure edilmelidir.
 - ▶ Blog, grup ve forumlarda yer alan sahte hesaplara karşı çalışanlar eğitilmelidir.
 - ▶ **Ürün katalogları, basın duyuruları, yıllık raporlar** gibi açık erişime sahip olacak yerlerde kritik bilgiler yer almamalıdır.
 - ▶ Website/Internet ortamında olabildiğince kısıtlı bilgi yayınlayın
 - ▶ Footprinting tekniklerini kendinize karşı uygulayarak hassas bilgi paylaşımlarını bulup kaldırın
 - ▶ Arama motorlarının sitenizde yer alan sayfaları cache'lemesini engelleyin
 - ▶ <META NAME="ROBOTS" CONTENT="NOARCHIVE">
 - ▶ robots.txt
 - User-agent: ia_archiver
 - Disallow: /

Countermeasure III

Genel Çözümler

- ▶ Çalışanlarınız tarafından üçüncü kişilerle paylaşılabilcek bilgiler için güvenlik politikaları uygulayın
 - ▶ Internal ve external DNS'leri ayırin veya DNS'leri bölün.
 - ▶ Web sunucularda yer alan **directory listing** özelliğini kapatın
 - ▶ Çalışanlarına, **sosyal mühendislik hileleri ve riskleri** hakkında çeşitli eğitimler verin
 - ▶ Hassas bilgilerinin şifrelenmiş ve parola korumalı erişebilecek şekilde ayarlayın

İçindekiler

- 1 Footprinting Konsepti
 - Tanım
 - Footprinting Hedefleri
 - 2 Yöntem
 - Arama Motorları
 - Document Metadata
 - Google Teknikleri
 - Sosyal Ağ Siteleri
 - Website Footprinting
 - Email Footprinting
 - WHOIS
 - DNS Footprinting
 - 3 Araçlar
 - Maltego
 - FOCA
 - 4 Countermeasure
 - Countermeasure
 - 5 Lab
 - Windows Komut Satırı
 - Çevirimiçi Kişi Bilgi Arama Servisleri
 - Path Analyzer Pro kullanarak Network Route Tracing
 - Maltego

Windows Komut Satırı I

Lab Senarvo

Windows işletim sisteminde yer alan *ping*, *nslookup* ve *tracert* gibi araçlar kullanılarak hedef ağ hakkında **IP adres**, **max Packet Frame Size** gibi bilgiler elde edilebilir.

Lab adımları:

1. Komut satırında **ping www.tubitak.gov.tr** yazarak IP adresini elde edin.
 2. Hedef domain'in **IP adres bilgisiyle beraber gönderilen/alınan paket sayısı, kayıp paket sayısı, yaklaşık round-trip time** gibi bilgilerde elde edilmektedir.
 3. Maximum frame size'ın bulunması için **ping www.tubitak.gov.tr -f -l 1500** yazın.
 4. Gelen cevap **Packet needs to be fragmented but DF** şeklinde olacaktır. Anlamı frame boyu çok fazla bu nedenle fragmente edilmesi gerekmektedir. Fakat **-f (Set Don't Fragment flag in packet)** parametresi kullandığımız için paket gönderilemeyecektir. Bu sebeple hata mesajı almaktayız.
 5. **ping www.tubitak.gov.tr -f -l 1300** yazın. Gönderilen packetlerin 1300'den yüksek 1500'den az olduğunu gözlemleyin.
 6. **ping www.tubitak.gov.tr -f -l 1472** yazın. Paketlerin gönderildiğini gözlemleyeceksiniz.
Not: **Maximum frame size**, hedef ağa göre farklılıklar gösterecektir.

Windows Komut Satırı II

7. TTL (Time to Live) değeri bittiğinde ne olur? Eğer TTL değeri 0 olursa router paketi siler. Komut satırında **ping www.tubitak.gov.tr -i 3** yazın. **Not:** verilebilecek maksimum değer 255'dir.
 8. **TTL expired in transmit** hata mesajının anlamı router'ın frame silmesidir (TTL expired - reached 0).
 9. Komut satırında **tracert www.tubitak.gov.tr** yazın. İsteğin geçtiği adresleri gözlemleyin (İş/ev/açık ağ bağlantılarınıza göre sonuçları farklılık gösterecektir). Kaç adet hop geçmektedir?
 10. Komut satırında **nslookup** yazın. **Default server** ve **IP Address** bilgisini gösterir.
 11. **nslookup** içinde **set type=a** yazarak verilen bir domain'in IP adresi bulunmaya çalışılır. Yine **nslookup** içinde **www.tubitak.gov.tr** yazıp enter'a basarak bilgilere erişin.

Çevirimiçi Kişisel Bilgi Arama Servisleri

Lab Senaryo

Kişisel bilgilerin pipl (<http://pipl.com>) aracılığı ile bulunması

Lab adımları:

1. Web Tarayıcıdan <http://pipl.com> adresini açın
 2. İsim, e-posta, kullanıcı adı, telefon gibi bilgilerle arama yapın (Örnek: Donald Trump)
 3. **Places** link'ine tıklayarak kişinin ziyaretleri takip edilebilir.

Path Analyzer Pro kulanarak Network Route Tracing

Lab Senaryo

Bu lab kapsamında ağ yollarının (network paths) trace edilmesi yapılacaktır.

Lab adımları:

1. **Path Analyzer Pro** aracını **Administrator** yetkileri ile açın.
 2. **Protocol** kısmında **ICMP** radio button seçili olduğuna emin olun.
 3. **Stop on control messages (ICMP)** seçili olduğuna emin olun
 4. Trace işlemi için **Target** alanına www.google.com yazın.
 5. Menuden **Timed Trace** seçip **Trace**'e tıklayın
 6. Açılan **Type time of trace** pop-up ekranında dakika olarak **3** girin
 7. **Report** sekmesinde bilgisayarınız ve hedef arasında kaç adet hop olduğu bilgisi elde edilmektedir.
 8. **Synopsis** sekmesinde tek-sayfalık özet bir rapor paylaşılmaktadır. (IP adresi, DNS gibi)
 9. **Geo** sekmesinde, Dünya haritası üzerinde **trace route** gösterilmektedir.

Maltego I

Lab Senaryo

Bu lab kapsamında **Maltego** kullanılarak hedef hakkında olabildiğince fazla bilgiler toplanmaya çalışılacaktır.

Lab adımları:

1. GUI'de yer alan + simgesine tıklayın
 2. Sol tarafta yer alan **Entity Palette** menüsünden **Website** sürükle bırakın
 3. Sağ tarafta yer alan menüden Website olarak www.certifiedhacker.com yazın
 4. Sağ menü ile **Run Transform** → **All Transforms** → **To Server Technologies Website** seçin
 5. Palet üzerinde sunucuda yer alan teknolojiler listelenecektir. İnternet üzerinde bu teknolojilerin olabilecek zafiyetleri araştırılabilir.
 6. Web sitesi sağ menü ile **Run Transform** → **All Transforms** → **To Domain [DNS]**
 7. Sayfaya gelen domain bilgisi üzerinde sağ menü ile **Run Transform** → **All Transforms** → **Domain to DNS Name Schema**. subdomain bilgileri gelecektir.
 8. Yine, sayfaya gelen domain bilgisi üzerinde sağ menü ile **Run Transform** → **All Transforms** → **to DNS Name - SOA (Start of Authority)**
 9. Sayfaya gelen domain bilgisi üzerinde sağ menü ile **Run Transform** → **All Transforms** → **to DNS Name - MX (mail server)**

Maltego II

10. Web site bilgisi üzerinde sağ menü ile **Run Transform → All Transforms → to IP Address [DNS]**) IP adres bilgisi elde edilir. IP Adres bilgisi üzerinde sağ menü ile **Run Transform → All Transforms → to Location [country,city]**) seçilerek ülke ve şehir bilgisi elde edilir.
 11. Ekran temizlenmeden, Websayfası üzerinde sağ menü ile **Run Transform → All Transforms → To Domain [DNS]** seçilir. Nameserver üzerinde sağ menü ile **Run Transform → All Transforms → To Entities from whois [Alchemy]** ile birçok bilgiye erişilir.