

Merhabalar ilk yazımla karşınızdayım. Sizlere burada kısa zaman aralıkları arasında çalışma alanım siber güvenlik ve alt alanları üzerine çeşitli paylaşımlarda bulunacağım. İlk konu başlığı olarak Kali ile ofansif(saldırı) güvenlik ile karşınıza çıkmış bulunmaktayım. İlk adımda Kali ve Ofansif hakkında bilgilendirmede bulunacağım.

Kali Linux, Debian tabanlı bir Linux dağıtımıdır. Her renkten şapkalı bilgisayar korsanlarının kullandığı araçları içerisinde barındırır. Ve çoğu çalışmam da bu dağıtımdan faydalanacağım.

Ofansif ise saldırı olarak dilimize çevrilmektedir. Kali Linux üzerinden çeşitli saldırılarda bulunacağız. Ve bu saldırılar ofansif kısmında yer alacaktır. Saldırıları başlamadan önce ilk adım olarak saldırı yapacağımız sistem hakkında çeşitli bilgiler toplamaya başlayacağız.

1.SALDIRI İÇİN BİLGİ TOPLAMA

Bir saldırıyı başlatmak için bilgi toplamak için hedefimiz hakkında temel bilgileri bilmemiz gerekmektedir. Ne kadar çok bilgi alırsak , başarılı bir saldırı yapma olasılığımız o kadar artar. Kali de çeşitli bilgi toplama araçları yer almaktadır. Bunun dışında terminal penceresinde ilgili aracın başlatma komutu ile çalıştırabilirsiniz.

1.1 DNS Servislerinin Belirlenmesi

DNS enumerations(numaralandırma), bir kuruluşun tüm DNS sunucularını ve DNS girdilerini bulma işlemidir. DNS numaralandırma, kullanıcı adı,bilgisayar adı, IP adresi ve benzeri gibi organizasyon hakkında kritik bilgileri toplamamızı sağlar. Bu işlem için **dnsenum** kodunu terminalde bastığımızda komutla beraber kullanabileceğimiz parametreler görüntülenir. Ekran görüntüsü şu şekilde olur.

```
root@kali:~# dnsenum
Smartmatch is experimental at /usr/bin/dnsenum line 698.
Smartmatch is experimental at /usr/bin/dnsenum line 698.
dnsenum VERSION:2.4
Usage: dnsenum [options] <domain>
[options]:
Note: the brute force -f switch is obligatory.
GENERAL OPTIONS:
--dnsserver <server> Use this DNS server for A, NS and MX queries.
--enum Shortcut option equivalent to --threads 5 -s 15 -w.
-h, --help Print this help message.
--noreverse Skip the reverse lookup operations.
--nocolor Disable ANSIColor output.
--private Show and save private ips at the end of the file domain_ips.txt.
--subfile <file> Write all valid subdomains to this file.
-t, --timeout <value> The tcp and udp timeout values in seconds (default: 10s).
--threads <value> The number of threads that will perform different queries.
-v, --verbose Be verbose: show all the progress and all the error messages.
GOOGLE SCRAPING OPTIONS:
-p, --pages <value> The number of google search pages to process when scraping names,
the default is 3 pages, the -p switch must be specified.
-s, --scrap <value> The maximum number of subdomains that will be scraped from Google
(default 15).
BRUTE FORCE OPTIONS:
-f, --file <file> Read subdomains from this file to perform brute force.
-u, --update <dir|rz> Update the file specified with the -f switch with valid subdomains.
BRUTE FORCE OPTIONS:
-f, --file <file> Read subdomains from this file to perform brute force.
-u, --update <dir|rz> Update the file specified with the -f switch with valid subdomains.
a (all) Update using all results.
g Update using only google scraping results.
r Update using only reverse lookup results.
z Update using only zonetransfer results.
-r, --recursion Recursion on subdomains, brute force all discovered subdomains that have
an NS record.
WHOIS NETRANGE OPTIONS:
-d, --delay <value> The maximum value of seconds to wait between whois queries, the value
is defined randomly, default 3s.
-W, --whois Perform the whois queries on c class network ranges.
**Warning**: this can generate very large netrangs and it will take
lot of time to perform reverse lookups.
REVERSE LOOKUP OPTIONS:
-e, --exclude <regex> Exclude PTR records that match the regex expression from reverse look
up results, useful on invalid hostnames.
OUTPUT OPTIONS:
-o, --output <file> Output in XML format. Can be imported in Nmap (www.gromwell.com)
root@kali:~#
```

Herhangi bir parametre kullanmadan **dnsenum domain.com** şeklinde kullandığımızda tüm kayıtlar (Host's adress, Name Servers,Mail Servers) gözükmemektedir.

Kullanacağımız ikinci araçta **dnsmmap** kodudur. Dnsmmap çoğunlukla altyapı güvenlik değerlendirmelerinin bilgi toplama aşamasında Pentestler tarafından kullanılır. Hedef sistemin IP bloklarını, alan adlarını, telefon numaraları gibi araçlarını keşfetmeye yarar.

1.2 Ağ Aralığını Belirleme

Hedef sistemin ağ aralığını belirlemek için temel araçlardan biri olan **dimitry** aracını kullanacağız. Bu araç bir host hakkında olduğunca fazla bilgi toplayabilir. Bunlar olası alt alan ağları, e-posta adresleri, çalışma zaman bilgileri , TCP port taraması who.is araması gibi verileri elde edebiliriz. **-o** parametresini kullanarak klasörleri sonuçları .txt olarak yazdırabiliriz.

```
person:      Ag Sistem Yonetimi
address:     Sakarya Universitesi Bilgi Islem Daire Baskanligi
phone:       +90 0264 295 5106
nic-hdl:     ASY13-RIPE
mnt-by:      ULAKNET-MNT
created:     2011-06-03T07:52:11Z
last-modified: 2011-06-03T07:52:11Z
source:      RIPE # Filtered

% Information related to '193.140.252.0/23AS24614'

route:       193.140.252.0/23
descr:       Sakarya University
origin:      AS24614
mnt-by:      ULAKNET-MNT
created:     2002-03-08T15:24:06Z
last-modified: 2002-03-08T15:24:06Z
source:      RIPE

% Information related to '193.140.252.0/23AS8517'
```

```
% Information related to '193.140.252.0/23AS8517'

route:       193.140.252.0/23
descr:       ULAKNET
origin:      AS8517
mnt-by:      ULAKNET-MNT
created:     2000-12-30T13:46:22Z
last-modified: 2000-12-30T13:46:22Z
source:      RIPE

% This query was served by the RIPE Database Query Service version 1.91.2 (HELEFORD)

Gathered Inic-whois information for sakarya.edu.tr
-----
** Registrant:
  Sakarya Üniversitesi
  Söğütözü Kampüsü Bilgi İşlem Dairesi Başkanlığı
```

```
root@kali:~# dmitry www.sakarya.edu.tr
Deepmagic Information Gathering Tool
"There be some deep magic going on"

HostIP:193.140.253.140
HostName:www.sakarya.edu.tr

Gathered Inet-whois information for 193.140.253.140
-----

inetnum:      193.140.252.0 - 193.140.253.255
netname:      SAKARYA-NET
descr:        Sakarya University Computer Center
descr:        Sakarya
country:      TR
admin-c:      ASY13-RIPE
tech-c:       ASY13-RIPE
status:       ASSIGNED PA
mnt-by:       ULAKNET-MNT
created:      1970-01-01T00:00:00Z
last-modified: 2011-06-03T07:53:43Z
source:       RIPE
```