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.

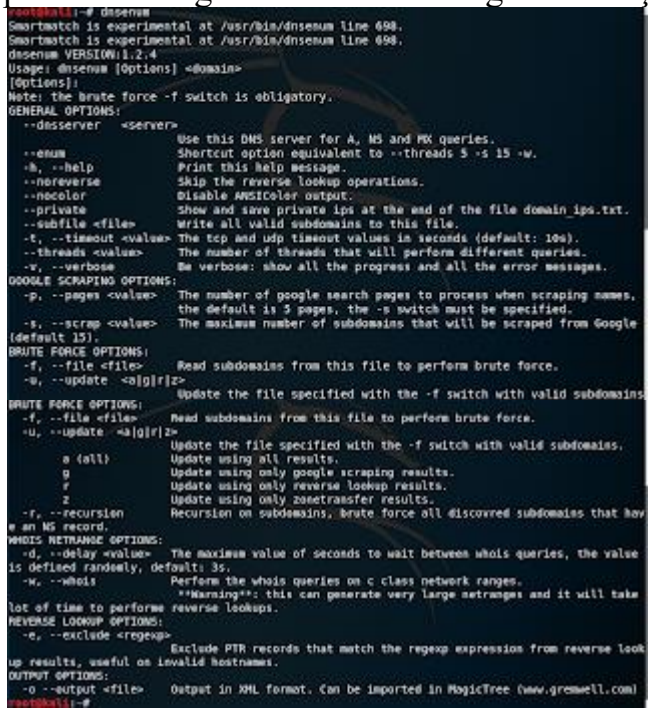
Ofansif ise saldırı olarak dilimize çevrilmektedir. Kali Linux üzerinden çeşitli saldırılarda bulunacağız. Ve bu saldırlar ofansif kısımda yer alacaktır. Saldırılara başlamadan önce ilk adım olarak saldırı yapacağımız sistem hakkında çeşitli bilgiler toplamaya başlayacağız.

1.SALDIRI İÇİN BİLGİ TOPLAMA

Bir saldırıyı başlatmak içim 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 enumarations(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.



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

Kullanacağımız ikinci araçta **dnsmap** kodudur. Dnsmap 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.


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