ÖN BİLGİ

Bu belge

- https://www.slideshare.net/slideshow/biliim-sularnda-ip-adres-analizi/27487915?from_search=0

resmi adresindeki veya linkin kırık olması ihtimaline karşın alternatif olarak

- https://www.includekarabuk.com/kitaplik/indirmeDeposu/Siber_Guvenlik_Teknik_Makaleler/Teori/BaskalarinaAitMakaleler/Bili%C5%9Fim%20Su%C3%A7lar%C4%B1nda%20IP%20Adres%20Analizi.pdf

adresindeki makaleye çalışılarak elde edilen notlarımı kapsamaktadır. Bu çıkarılan notlar belgemde alıntılar ve/veya kişisel ilavelerim mevcuttur.

1)

IP Adreslerini Kim Dağıtır?
IP adresleri IANA başkanlığında RIR (Regional Internet Registry) olarak adlandırılan organizasyonlar tarafından dağıtılır. Tüm dünyadaki IP dağıtımını üstlenen 5 tane RIR vardır. Bunlar bölgelere göre ayrılmışlardır.

Sıradan internet kullanıcılarına IP dağıtımı ISP tarafından yapılır. Bazı ISP'ler static IP adresi verebilirken bazı ISP'ler dinamik IP adresi atamasında bulunurlar.

(page 4)

2)

IP Adresi Neden Önemli?
Siber dünyada yapılan her işlemde IP adresleri kullanılır. IP adresi kullanılarak yapılan her tür işlemden ise IP adresinin sahibi sorumlu tutulur. İşte bu yüzden IP adresleri önemlidir.

(Page 4)

3)

IP adresleri belirli bir hiyerarşi ve sisteme göre omurga router'lar tarafından dağıtılırlar. Dolayısıyla isteyen istediği IP adresini alamaz. Statik IP sahibi olabilir ama spesifik bir IP benim olsun diyemez.

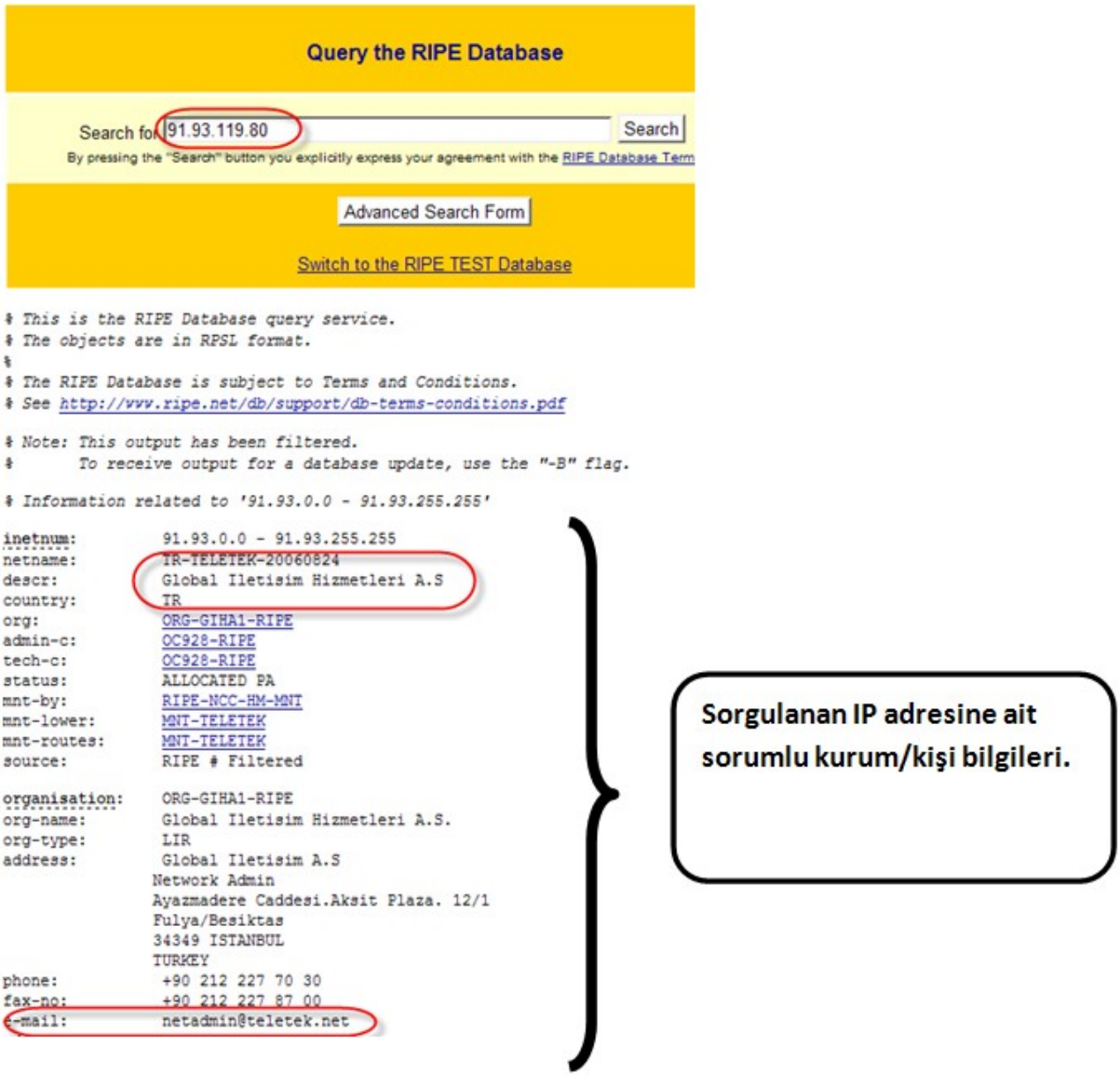
(Page 4)

4)

Bir IP adresinin kime, hangi ISP'ye ait olduğu RIR'lar üzerinden yapılacak sorgulamalarla belirlenebilir. Bu sorgulamalara “whois” adı verilir.

4)

Genellikle ISP'de birileri IP adreslerinin alım işlemlerinden sorumlu tutulur ve o kişi IP adreslerini ISP'ye kazandırır. whois sorgularında çıkan bilgiler içerisinde ise ilgili IP'yi kurumuna kazandıran sorumlu kişinin kontak bilgileri yer alır. Böyle bir bilgiye ihtiyaç duyulmasının nedeni IP adresiyle alakalı bir sorun ya da talep olduğu durumlarda IP alımından sorumlu kişiye ulaşılabilsin diyedir.



Resimde görülebileceği üzere sorgulanan IP'yi veren kurumun adı ve ilgili kurumdaki sorumlu kişinin mail adresi kırmızı çember içine alınmıştır. Burada önemli bir husus vardır: Kırmızı çember içine alınan bilgiler IP'nin sahibine ait bilgiler değildir. IP'yi servis eden kuruma ait bilgilerdir. Eğer IP'nin sahibi kendi sistemini whois sorgularına kapamamışsa bu durumda yukarıdaki resimde yer alan bilgilerin arasında IP'nin sahibine ait bilgiler de yer alır.

NOT: Örneğin ben isimtescil.net'ten aldığım domain'in whois ayarını bilgilerimi sakla şeklinde ayarladım. Böylece domain'ime yapılan whois sorgularında benim adım, soyadım, iletişim bilgilerim gibi şeyler dışarı yansıtılmıyor.

5)

Yapılan whois sorgusunda IP adresinin hangi kuruma ait olduğu ortaya çıkacaktır. Buradaki kurum bilgilerini kullanarak IP adresinin gerçek sahibi bulunabilir.

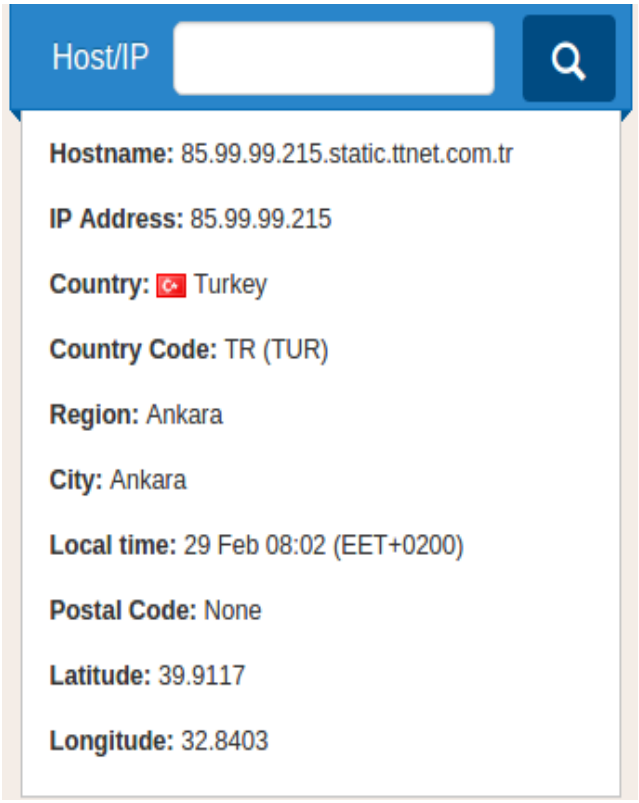
(Page 5)

6)

IP Adresinin Ait Olduğu Ülkenin Bulunması
IP adresleri dağıtılırken sistematik ve hiyerarşik bir yapı kullanıldığından bahsetmiştik. Bu sistematik yapıda IP adreslerinin hangi ülkeye ait olduğu bilgisi rahatlıkla bulunabilir. Bu iş için google üzerinden “geo ip” veyahut “country ip blocks” anahtar kelimeleriyle yapılacak aramalarda bir IP adresinin hangi ülkeye ait olduğu bilgisi otomatize bir şekilde edinilebilir. Örneğin;

https://geoiptool.com/

Output:

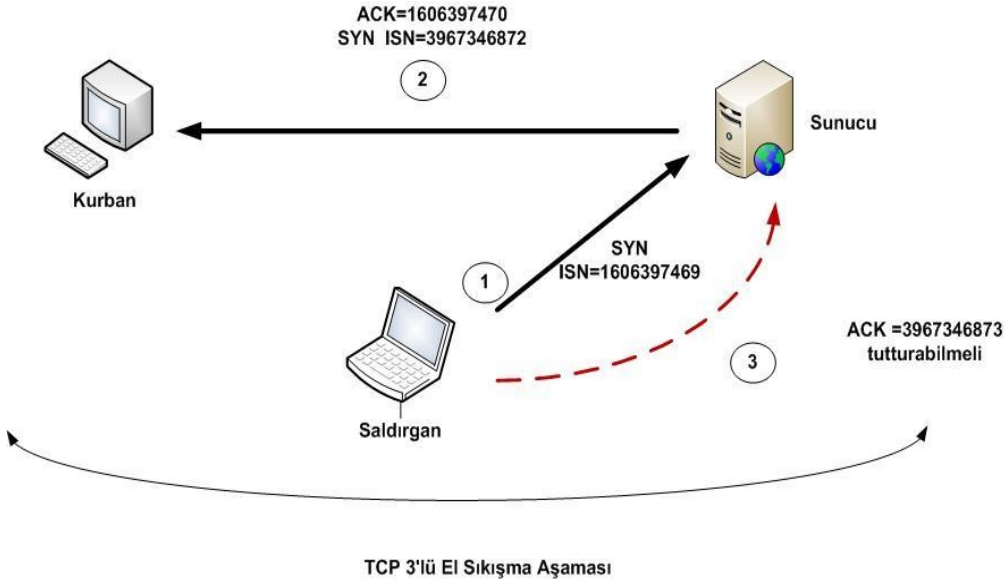


(Page 6)

7)

Internetin çalışmasını sağlayan TCP/IP protokol ailesi geliştirilirken güvenlik temel amaç olmadığı için olabildiğince esnek davranılmıştır. Bu esneklik birinin bir başkasıymış gibi kendisini gösterebilmesini sağlamıştır. Bu işleme IP Spoofing denmektedir. Ip spoofing yaparak başkasının IP adresinden istenilen internet aktivitesi gerçekleştirilebilir. Son yazdığımız cümle bundan on sene öncesi için geçerli olsa da günümüzde pratik olarak geçersizdir. Bunun temel nedeni günümüz modern işletim sistemlerinin protokoldeki eksik noktalara kalıcı çözüm getirmeleridir. Örn; TCP 3 lü El Sıkışma gibi...

Özellikle internetde en sık kullanılan HTTP, SMTP, HTTPS gibi protokollerin temelinde bulunan TCP bu tip sahtecilik işlemlerini engelleme amaçlı bir yöntem kullanır. Bu yöntem 3 lü eş sıkışma olarak adlandırılır. Bu prosedüre göre kullanıcı bir işlem yapmadan once sunucu ile bir iletişim kanalı kurar. Bu kanal oluşturulmadan paket alışverişi başlamaz. İletişim kanalının oluşturulması şart koşulduğundan dolayı IP spoofing yapılamaz.



TCP 3'lü El Sıkışma Aşaması

Yukarıdaki resme bakacak olursak saldırgan sunucuya 3 lü el sıkışma gereği bir SYN paketi yollar. Fakat bu SYN paketindeki kaynak IP'ye kurbanınkini koyar. Yani IP Spoofing yapmaya çalışır. Paketi alan sunucu ise 3 lü el sıkışma gereği paketin kaynak IP'sine bakıp kurbana SYN/ACK paketi yollar. Bu noktada kurban hiç bu işlerle alakalı olmadığı için doğal olarak paketi yanıtlamayacaktır. Bu nedenle de 3 lü el sıkışma tamamlanamayacaktır ve saldırgan kurban adına bir sunucu üzerinde bir işlem gerçekleştiremeyecektir.

Teoride 3 lü el sıkışmaya rağmen IP spoofing yapabilmenin yolu sunucunun kurbana gönderdiği paketin numarasını saldırganın tahmin etmesinden geçmektedir. Eğer saldırgan o numarayı tahmin edilebilirse onun bir fazlası değerine sahip numaralı bir ACK paketini sunucuya göndererek 3 lü el sıkışma tamamlanmış olur. Artık saldırgan sunucuya sanki kurban paket gönderiyormuş gibi paket gönderebilir ve kurban adına sunucu üzerinde suç dahi işleyebilir. Yani IP Spoofing yapabilmiş olur. Bu teoride iyi, güzel, mümkün gibi görünse de pratikte mümkün değildir. Çünkü ACK paketinin numarasını tahmin etmek güç olduğu gibi bir de paketlerin zamanlama periyodunu tutturmak gibi iki imkansızın kombinasyonu pek akıl karı bir iş değildir. Dolayısıyla TCP uygulamalarında IP Spoofing yapılamaz. Fakat DNS gibi UDP kullanan uygulamalarda IP spoofing

yapmak hala mümkündür. Çünkü UDP protokolünde 3 lü el sıkışma gibi bir prosedür yoktur. Dolayısıyla istenilen IP numarası kullanılarak mesela DOS saldırısı yapılabilir.

(Page 6-7)

8)

IP Spoofing yöntemiyle başkasının IP adresinden suç işlemek günümüzde mümkün değildir. Fakat aşağıdaki yöntemler kullanılarak başkasının IP adresinden suç işlemek mümündür:

a. Kurbanın makinesine zararlı yazılım bulaştırıp bu zararlı programa suç işletmek

- Böylece zararlı yazılıma sahip kurbanın makinası suçu işlemiş gibi görünür.

b. Kurbanın IP adresi eğer NAT işlemine tabi tutuluyorsa ilgili ağda bulunan herhangi bir makineye zararlı yazılım bulaştırırarak o yazılıma suç işletmek

- Böylece network'teki zayıf halkaya zararlı yazılımı bulaştırıp suçu işleterek ilgili makinenin bulunduğu network'ün public IP'si suçu işlemiş gibi görünür.

c. IP adresi eğer kablosuz erişime açıksa bu kablosuz ağa sızılarak ilgili IP adresinden suç işlemek.

- Saldırgan kendi makinesinden suç işlemesine rağmen sızdığı network'ün public IP'si suçu işlemiş gibi görünür.

(Page 7-8)

9)

İstenilen Ülkenin IP Adresini Kullanma
Proxy yazılımları sayesinde internette dilediğimiz IP adresi ile gezebiliriz. Aşağıdaki ekran görüntüsü proxy'lerden ülke olarak Kanada'nın seçilmesi sonrası alınmıştır.

Böylesi proxy'lerle yapılacak işlemlerde asıl faili bulmak oldukça zordur. Çünkü internet üzerinde çalışan binlerce proxy servisi hangi kullanıcının hangi zaman dilinminde nereye bağlandığı bilgisini tutmamaktadır.

(Page 10)

10)

Sonuç
Bir adli bilişimci internet altyapısının kullanılarak yapılan suçlara karşı şüpheci davranmalıdır. Ele geçirilen IP adresinin proxy ile edinilmiş bir IP adresi olma ihtimali kuvvetle yüksektir. Bu gibi durumlarda suçluyu bulmak gerçek hayata göre biraz zor görünse de konusunun uzmanı bir adli bilişimci suçlunun nereden geldiğini, kendisini gizleyip gizlemediğini, gizlediyse hangi yöntemleri, araçları kullanarak gizlediğini ortaya çıkarabilir.

(Page 11)