



DNS Güvenliđi ve T nelleme Tehdidi

Hazırlayan: Okan YILDIZ

İçindekiler

DNS Nedir ve Nasıl Çalışır?	3
DNS Güvenliği	3
Saldırganın Bakış Açısından DNS	4
DNS Tehditleri	5
DNSSEC kurulu değil	6
Cisco ve Lync kullanımı	8
DNS Tünelleme	10
DNS Tünellemede Kullanılan Araçlar	10
Iodine	11
DNS güvenliği için öneriler	15

DNS Nedir ve Nasıl Çalışır?

Alan adı sistemi olan DNS (Domain Name System), isim sunucu ve çözümleyicilerden oluşur, internete açılan kapılardır. İsim sunucular, host isimlerine karşılık gelen ip adreslerinin ismini tutar. Çözümleyiciler ise DNS istemciler olarak bilinir ve bu istemcilerde, DNS sunucu yada diğer sunucuların bilgisini tutar.

Web siteleri, URL olarak adlandırılan kolay adres ve IP adresine sahiptir. Kullanıcılar web sitelerini bulmak için URL'leri, bilgisayarlar ise IP adreslerini kullanır. DNS URL'leri IP adreslerine dönüştürür (veya tam tersi). Örneğin, web tarayıcınızdaki adres çubuğuna <http://www.alanadi.com> yazarsanız, bilgisayarınız DNS sunucusuna bir istek gönderir. DNS sunucusu URL'yi IP adresine dönüştürerek bilgisayarınızın Microsoft web sunucusunu bulabilmesini sağlar.[1]

DNS sistemine ait bazı bileşenler aşağıda verilmiştir;

- **A →** Domain Name den IP adresine dönüşüm yapar.
- **MX→** Belli bir Domain' e gelen e-postaların hangi makineye dağıtılacağını bulur
- **NS→** Alan adınızın sorgulanmasında kullanılacak olan isim sunucularıdır.
- **PTR→** Verilen ip adresinin, isim karşılığını bulur.
- **HINFO →** Bilgisayarın donanım ve işletim sistemi gibi bilgilerini yazmak için kullanılır.
- **TXT→** Bilgi vermek amacı ile kullanılır.

DNS Güvenliği

DNS 30 yılı aşkın süreden bu yana gelişmeyi sürdüren ve internetin çekirdek bileşenlerinden bir tanesidir. Bu sebeplerden dolayı saldırganlar ve kötücül yazılım yayınlayanların hedeflerinden bir tanesidir. DNS altyapsının çökmesi ya da saldırganlar tarafında kötüye kullanılması, büyük ölçekli hizmetlerin kesilmesi ve ya DNS üzerinden dışarıya veri sızdırma olaylarıyla sonuçlanabilir. Cisco'nun 2014 Yılındaki Güvenlik Raporuna göre inceleme yapılan ağların %96'sında çalınan sunuculara doğru trafik akışı olduğu görüldü ve %92'sinde ise herhangi bir içeriği bulunmayan sitelere doğru trafik olduğu tespit edildi. DNS

üzerinde gerçekleşen saldırılar arasında en yaygın olanları aşağıda verilmiştir;

- **DNS tünelleme**
- **DoS ve DDoS saldırıları**
- **Ön bellek zehirlenmesi**
- **DNS yeniden yönlendirme (MITM) saldırıları:**
- **İleri Seviye Tehditler (APT)**

Saldırmanın Bakış Açısından DNS

İnternet'i kullanılabilir hale getiren ve bir anlamda belkemiğini oluşturan DNS (Domain Name Server – Alanadı Sunucuları) saldırganlar için de önemli hedeflerdir.

Aşağıdaki ekran görüntüsünde görülebileceği gibi örnek olarak ele aldığım yerlerden birisi web sayfasını basit port taramalarına karşı korumaktadır. NMAP'in hiç bir parametre kullanılmadan yapılan taramalarda kullandığı 1000 port filtreli durumda ve sadece internet sayfasının hizmet verebilmesi için ihtiyaç duyduğu portlar görece açık.

```
Starting Nmap 6.46 ( http://nmap.org ) at 2015-01-01 14:23 EST
Nmap scan report for [REDACTED].tr ([REDACTED])
Host is up (0.20s latency).
rDNS record for [REDACTED]: [REDACTED].tr
Not shown: 998 filtered ports
PORT      STATE SERVICE
80/tcp    open  http
8080/tcp   closed http-proxy

Nmap done: 1 IP address (1 host up) scanned in 53.33 seconds
```

Filmlerde gösterilenin aksine hackerlar kolay yolu ararlar, bu durumda bu portları filtreleyen güvenlik cihazını atlatmaya uğraşmaktansa daha kolay istismar edebilecekleri saldırı yüzeyleri arayacaklardır. Sistem yöneticisi olarak kapatamadığımız 3 ana nokta, doğal olarak saldırganların başlıca tercihleri olacaktır bunlar;

E-posta hizmeti: Sosyal mühendislik saldırıları için önemli vektörlerdir. E-posta sunucularının doğru konfigüre edilmediği durumlarda ise saldırganlar, kurum e-posta kaynaklarını kullanarak hem üçüncü şahıslara saldırabilir (istenmeyen e-posta gönderimi ve oltalama

saldırıları), hem de kurumsal ağ, sistemler ve yapı hakkında bilgi elde edebilirler.

Web sayfaları (web uygulamaları): Web sayfaları üzerindeki zafiyetleri istismar eden saldırganlar kurum bilgilerini ele geçirebilir, itibar ve para kaybına yol açabilir.

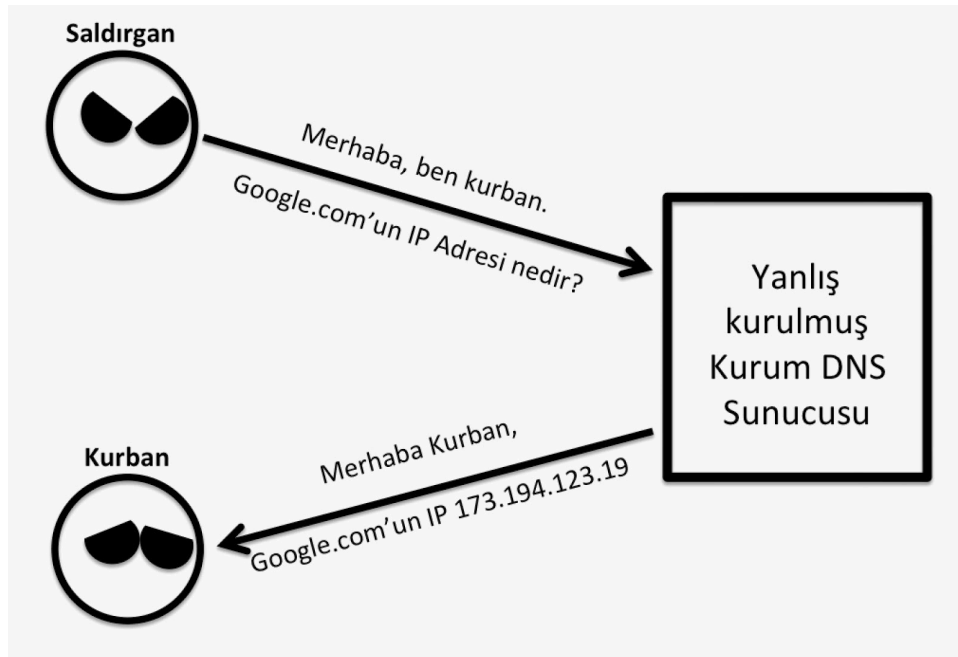
DNS Tehditleri

Saldırganlar DNS sunucularını kullanarak 4 temel saldırı türünü gerçekleştirebilir.

Bilgi Toplama: Özünde bir saldırı olmasa da hedef hakkında bilgi toplamak geçerli saldırıları belirlemek, planlamak ve yürütmek için önemlidir. Saldırganlar hedefin dışarıya bakan ağını nasıl düzenlediği ve yönettiğini DNS üzerinden bilgi toplayarak anlayabilir.

Hizmet dışı bırakma: Alanadı sunucusuna kapasitesinin çok üstünde talep gönderen saldırganlar hedef DNS sunucusunun iş görmez hale gelmesine neden olabilir.

Sahte kaynaktan talep gönderme: Yanlış ayarlanmış bir alanadı sunucusu başka bir hedefe hizmet dışı bırakma saldırısı düzenlenmek için kullanılabilir. Saldırganların hedef ağdan geliyor gibi düzenleyip göndereceği paketlere cevap veren alanadı sunucusu istemeden karşıdaki sunucuyu hizmet veremez hale getirebilir.



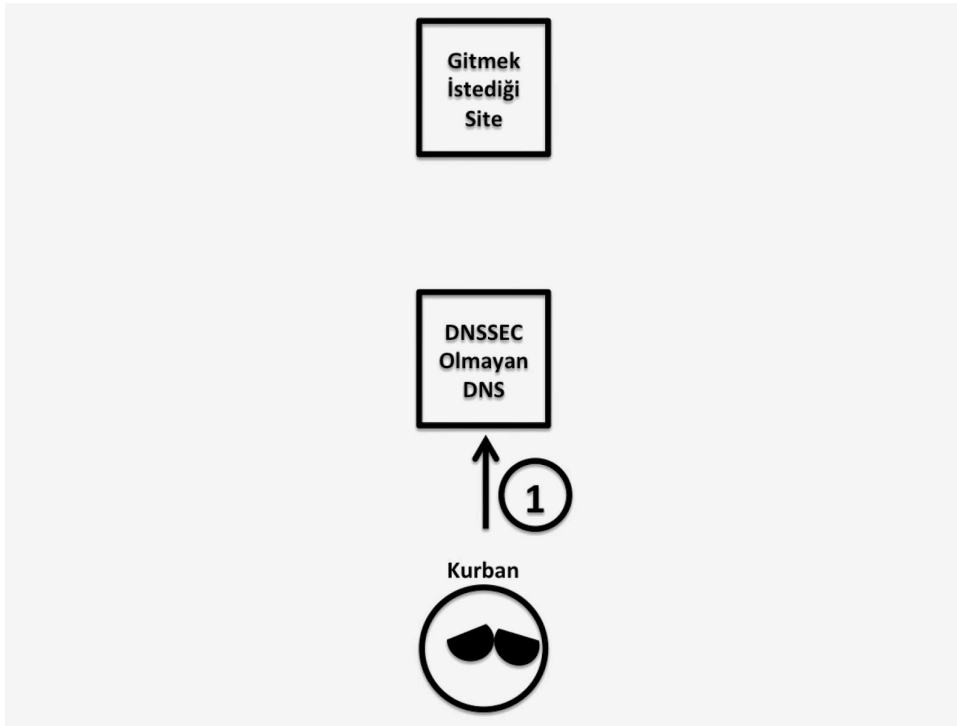
Kayıt yönlendirme: Kurumdan çıkan DNS taleplerini kendi kontrolündeki bir sunucuya yönlendiren saldırgan bu sayede kullanıcıları zararlı içerik barındıran bir siteye veya sosyal mühendislik saldırılarına uygun olarak hazırladığı başka bir siteye yönlendirebilir.

Yukarıda portlarını koruduğunuz bildiğimiz hedefin Alanadı Sunucusuna saldırgan gözüyle bakacak olursak aşağıdaki bilgileri elde edebildiğimizi görebiliriz.

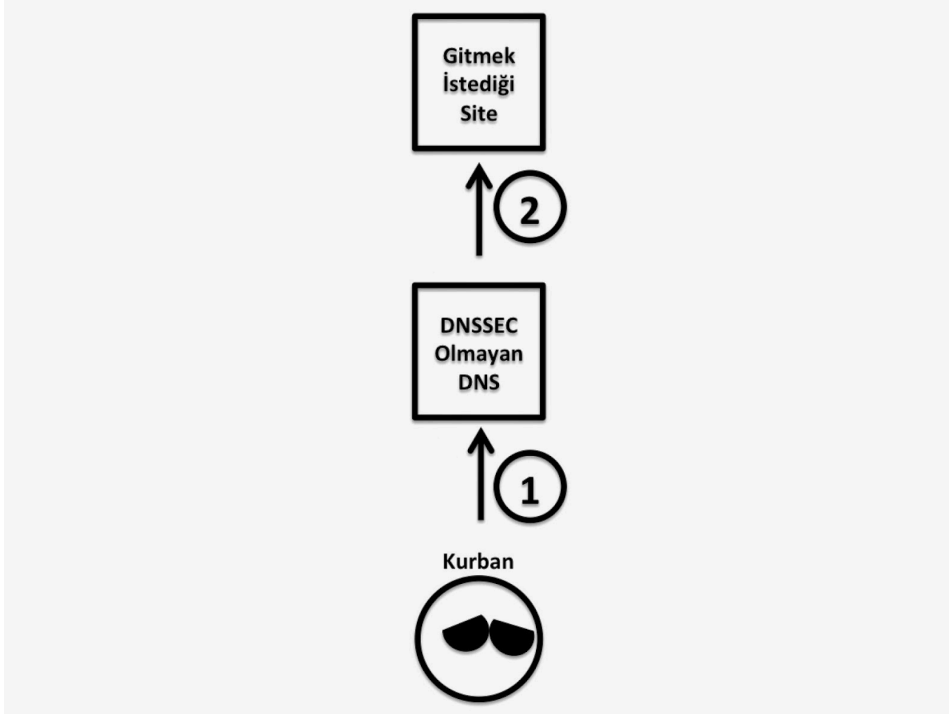
DNSSEC kurulu değil

DNSSEC kullanılmadığı durumlarda saldırganlar DNS trafiğini yakalayıp değiştirebilirler. Aşağıdaki 4 grafik DNSSEC kullanmayan bir sunucuya yönelik düzenlenebilecek etkili bir saldırıyı özetlemektedir.

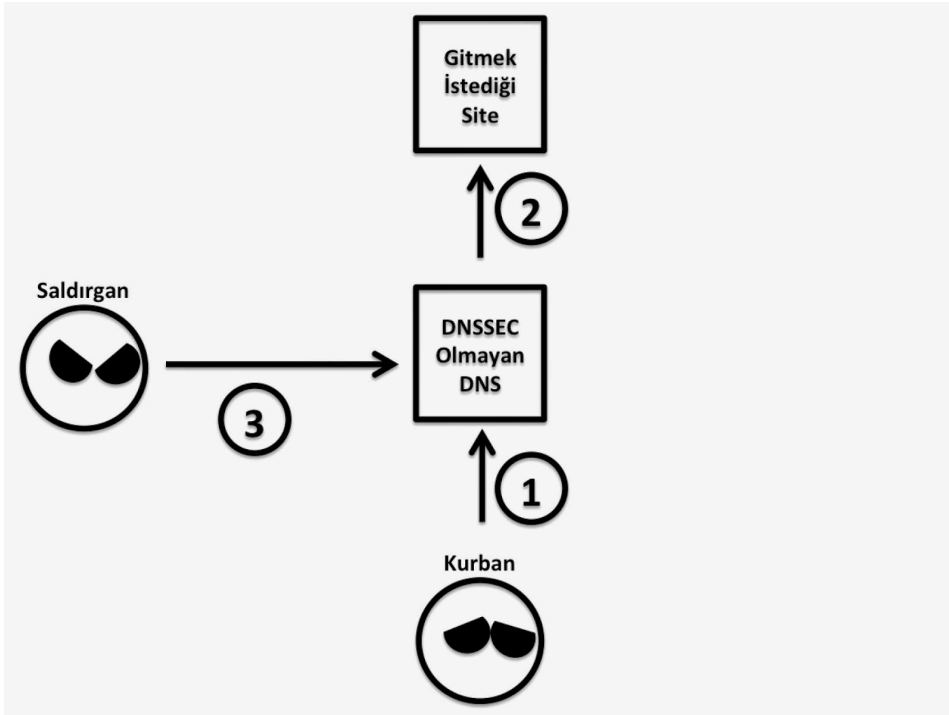
Adım 1: Kurban tarayıcının adres çubuğuna gitmekistediğimsite.com yazar ve tarayıcı bu sitenin IP adresini tespit edebilmek için DNS sunucusuna bir sorgu gönderir.



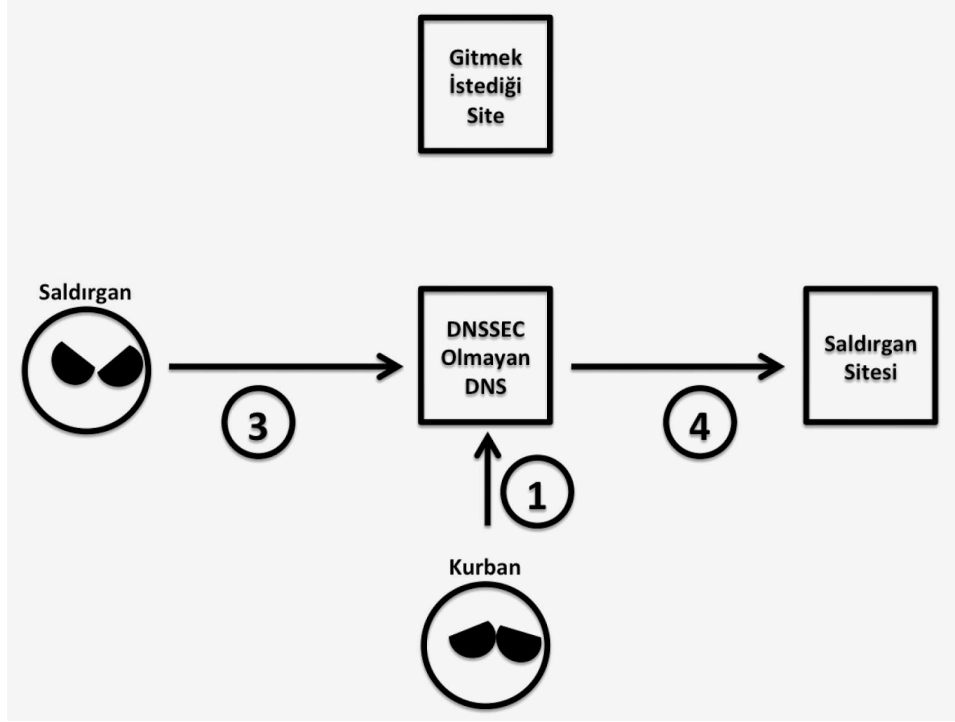
Adım 2: DNS sunucusu gerekli bilgilendirmeyi yaparak kurbanı gitmek istediği siteye yönlendirir.



Adım 3: DNSSEC olmamasından faydalanan saldırgan DNS sorgularına müdahale eder.



Adım 4: Kurban gitmekistediğimsite.com adresini yazmasına rağmen farkında olmadan saldırgan tarafından hazırlanmış siteye yönlendirilir.



Cisco ve Lync kullanımı

Aşağıdaki ekran görüntüsünde görüldüğü gibi örnek olarak ele aldığım şirket Cisco video konferans sistemi olduğunu tahmin ettiğim (vcse. ile başlayan alandı ve 5060/5061 portlarını ipucu olarak değerlendirerek yürüttüğüm bir tahmin) ve Microsoft LYNC'i haberleşme için kullanıyorlar.

```
[*] Enumerating SRV Records
[*] SRV _[redacted].tr vcse.[redacted].tr [redacted] 5
060 10
[*] SRV _[redacted].tr vcse.[redacted].tr [redacted] 5
060 10
[*] SRV _[redacted].tr vcse.[redacted].tr [redacted]
5061 10
[*] SRV _[redacted].tr vcse.[redacted].tr [redacted]
9 1720 10
[*] SRV _[redacted].tr vcse.[redacted].tr [redacted]
9 1719 10
[*] SRV _[redacted].tr lync.[redacted].tr [redacted]
```

İlginç altalanadları

Smtip., test. Vpn. Gibi saldırgan açısından ilgi çekici olabilecek bir kaç altalanadının yanında hedefin kullandığı IP adresleri aralıkları hakkında da bilgi sahibi olduk.


```
smtp. .tr
sharepoint. .tr
test. .tr
vpn. .tr
webmail. .tr
. .tr
. .tr
. .tr
Subnets found (may want to probe here using nmap or unicornscan):
0-255 : 1 hostnames found.
.0-255 : 3 hostnames found.
.0-255 : 1 hostnames found.
.0-255 : 2 hostnames found.
.0-255 : 1 hostnames found.
.0-255 : 2 hostnames found.
.0-255 : 12 hostnames found.
.0-255 : 2 hostnames found.
.0-255 : 4 hostnames found.
.0-255 : 12 hostnames found.
.0-255 : 1 hostnames found.
```

DNS güvenliği konusunda ülke olarak ne durumda olduğumuzu anlamak için 21 Bakanlık DNS sunucuları üzerinde yaptığım çalışmada gördüğüm şunlar oldu;

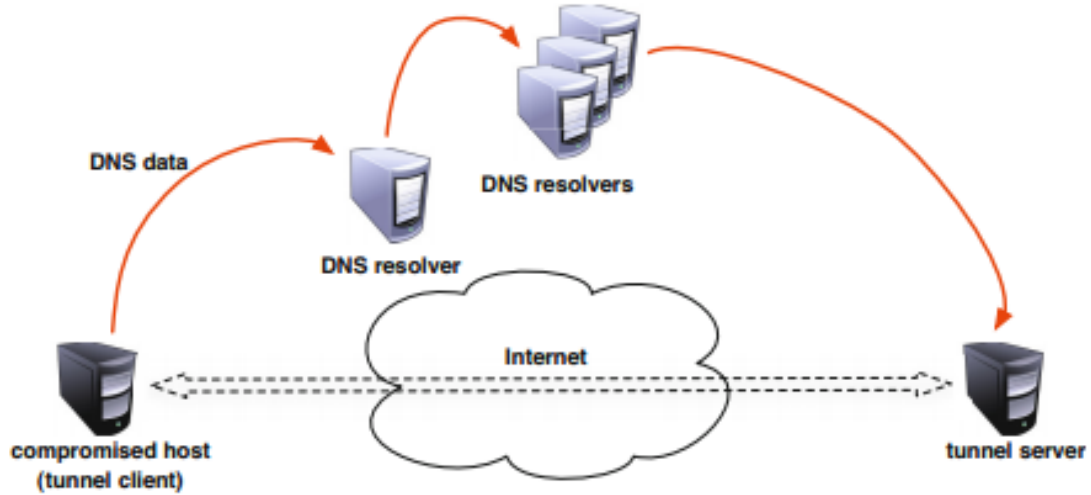
21 Bakanlık içerisinde;

- 20 tanesinde DNSSEC kullanılmadığını,
- 5 tanesinin DNS sunucusunun dışarıdan gelen isteklere cevap verdiği için başka hedeflere karşı hizmet dışı bırakma saldırılarında kullanılabileceğini,
- 3 tanesinde Microsoft Lync kullanıldığını,
- 8 tanesinin internet üzerinden telefon görüşmesi yaptığını sadece DNS sorguları aracılığıyla tespit etmek mümkün olmuştur.

DNS Tünelleme

DNS tünelleme, DNS paketleri içerisinde herhangi bir TCP/UDP paketinin taşıma işlemine verilen isimdir. Bu saldırılarda, saldırganın amacı bir sunucunun DNS portu üzerinden çalıştırılıp, gerçek bir DNS sunucu gözükmesini sağlayıp veri sızdırmaktır. Bu saldırılarda DNS sunucu kendisinden sorgulanan bir DNS isteğine önce önbelleğini kontrol ederek yanıt vermek ister eğer alan adı DNS önbelleğinde yoksa, sorgulanan alan adından sorumlu DNS sunucuyu bulur ve ona sorar. Sorgulanan alan adından yetkili DNS sunucu ilgili DNS kaydı için yanıt verir ve DNS sunucu bu yanıtı istemciye iletir.

DNS tünellemeyi daha iyi anlamamız için, saldırının genel yapısı aşağıda verilmiştir.



Özet olarak DNS tünelleme bir istemci tarafından üretilen DNS paketlerinin sunucu tarafından işleme alınması ile oluşur. Sunucu DNS portu üzerinden çalıştığı için gerçek bir DNS sunucusu gibi görünür.

DNS Tünellemede Kullanılan Araçlar

DNS tünel araçları, DNS sorgu bölümündeki veriyi encode ederek ISP'nin (daha doğrusu tünel sunucusunun sahibinin) DNS sunucusuna iletir. Sunucu üzerindeki DNS portunda tünelleme sunucusu çalışır. Aracın sunucu tarafı da, gelen isteği decode eder ve ilgili isteğe yanıtı istemciye geri gönderir.

Bu saldırılarda kullanılan araçlar aşağıda verilmiştir;

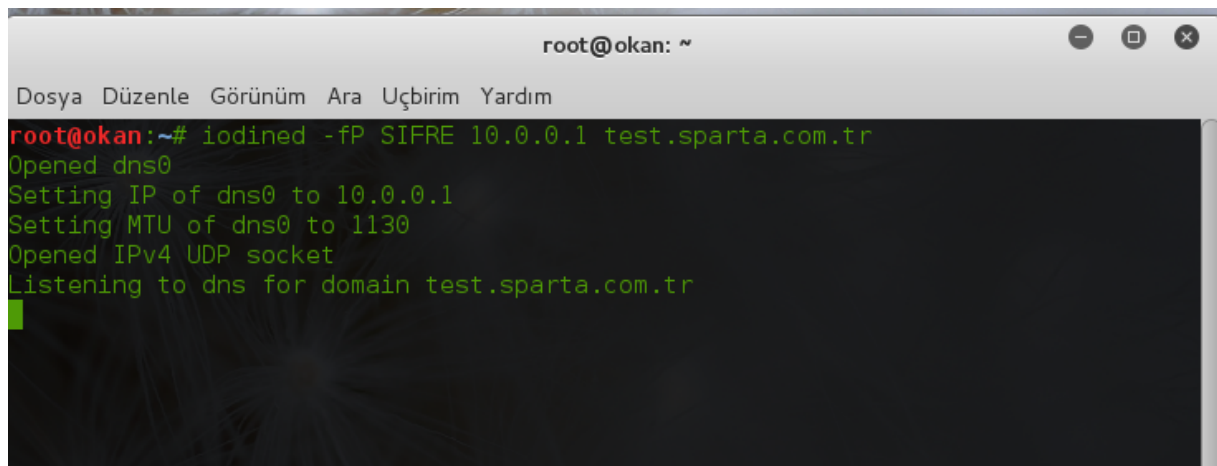
- OzymanDNS
- Dns2tcp
- Iodine
- Heyoka
- DNSChat
- NSTX
- DNScapy
- MagicTunnel, Element53, VPN-over-DNS (Android)
- VPN over DNS

Iodine

Iodine DNS tünellemede kullanılan en popüler araçların başında gelir. Hem platform bağımsız olması hem de kolay kurulum ve kullanımı ile en iyi DNS tünelleme yazılımı sayılabilir. Iodine ile ipv4 üzerinden, DNS sunucu aracılığıyla tünelleme yapılabilmektedir. İstemci tarafında çalıştırılıp, sunucuya erişim kontrolü sağlandıktan sonra yazılacak yönlendirmelerle tüm trafik yeni kurulan tünel aracılığı ile yönetilebilir.

Aşağıda Iodine ile Ipv4 üzerinden veri dinlemeye örnek olması açısından bir uygulama verilmiştir.

Aşağıda iodine hem sunucu hemde client tarafında çalıştırılmıştır. Burada SIFRE yazan yer bağlantıya atadığımız şifre.



```
root@okan: ~  
Dosya Düzenle Görünüm Ara Uçbirim Yardım  
root@okan:~# iodined -fP SIFRE 10.0.0.1 test.sparta.com.tr  
Opened dns0  
Setting IP of dns0 to 10.0.0.1  
Setting MTU of dns0 to 1130  
Opened IPv4 UDP socket  
Listening to dns for domain test.sparta.com.tr
```


Wireshark ile yakaladığımız gizli veriyi barındıran paketi açıyoruz.



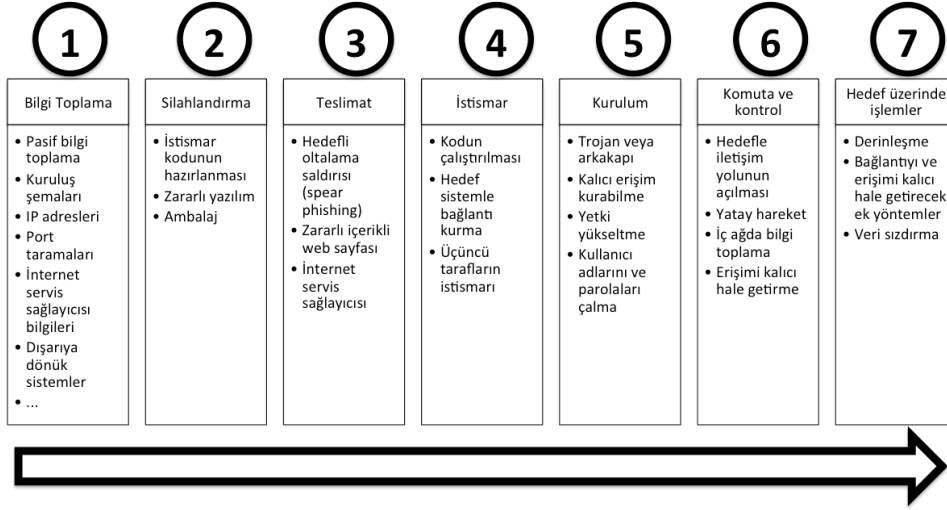
Yukarıdaki örnekte görüleceği üzere çok basit araçlarla herhangi bir veriyi DNS sorgusu gibi kuruluş ağının dışına göndermek mümkündür.

Siber olaylara müdahale raporlarında rastladığımız “saldırganlar, tespit edilmeden önce, kuruluş ağında ortalama 220 gün geçiriyorlar” gibi ilk bakışta bize inanılmaz gelen rakamlara ulaşılmasını sağlayan bunun gibi basit ve etkili teknikleri kullanmalarıdır.

DNS tünelleme, saldırıları engellemeye odaklı mimarilerin (firewall, IPS/IDS, vs. “güvenlik” bileşenlerinin ön planda olduğu ağlarda) yetersiz kaldığı pek çok senaryodan sadece bir tanesidir.

Son yıllarda karşılaşılan yüksek profilli saldırılardan çıkarttığımız derslere bakarak saldırıların ağ ve sistemlerimize sızmalarını engellemenin neredeyse imkansız olduğudur. Bu nedenle saldırının kuruluş ağına girdiği anda tespit edilmesi ve aşağıda “siber ölüm zinciri” olarak özetlediğimiz genel saldırı anatomisini de düşünerek birden fazla hamlesinin fark edilmesini sağlayacak yapıların kurulması gerekmektedir.

Siber Ölüm Zinciri Döngüsü



Yaşanan, neredeyse bütün, güvenlik ihlallerinde bu 7 adımın atıldığını ve saldırganların başarılı bir sonuca ancak her adımda başarılı olmaları halinde ulaşabildiklerini görüyoruz. Bu zincirin kurulabileceği senaryoların ve saldırganların ulaşabileceği sonuçların (veri çalınması, sistemlerin devre dışı kalması, vb.) iş süreçlerimize etkileriyle birlikte ortaya konulması önemlidir.

Kuruluş ağı ve sistemleri için geçerli olabilecek senaryoları, iş süreçleri için ortaya çıkabilecek tehditleri ve genel risk seviyesinin anlaşılması için yapılabilecek çalışmalar arasında en kıymetlisi sızma testi olacaktır. Bu testlerin sonucunda saldırganın kullanabileceği saldırı teknikleri ve araçları arasında mevcut güvenlik tedbirlerimizin tespit edemedikleri ve/veya siber güvenlik ve siber olaylara müdahale yönetimi kapsamımızın ele almadıkları ortaya çıkartılır. Sızma testi çalışmaları sonucunda başlatılan iyileştirme çalışmaları güvenlik hattımızın eksik kalan noktalarının tamamlanmasını sağlar.

DNS güvenliđi için öneriler

Alanadı sunucunuzun güvenliđini sađlamak için kullanabileceđiniz tek bir hap ne yazık ki yoktur. Bilgi güvenliđiyle ilgili diđer bütün konularda olduđu gibi gizlilik, bütünlük ve erişilebilirlik başlıkları ayrı olarak deđerlendirilmelidir. Güvenlik seviyesini hızlıca arttırmanızı sađlayacak bazı öneriler şunlar olabilir;

DNS sunucunuz sadece kurumunuza hizmet etmelidir ve DNS sunucunuza sadece yetkisi olanlar erişebilmelidir.

DNS taleplerinin trafiđinin denetlenmesi gereklidir: Bu sayede hem DNS'e gelebilecek saldırıları fark eder hem de saldırganların DNS tüneli benzeri yöntemlerle kurum dışına veri kaçırdığını tespit edebilirsiniz.

DNS sunucularınız güncel tutulmalıdır: Diđer bütün sistemlerde olduđu gibi DNS yazılımları için güvenlik güncellemeleri ve yamaları yayınlanır, bunların zamanında kurulması çok önemlidir.

DNS sunucunuz üzerinde çalışan servisleri sınırlayın: DNS sunucunuz üzerinde FTP, HTTP, SMTP gibi hizmetleri kaldırmakta fayda var.

Sparta Biliřim Ankara merkezli, kamu, enerji, finans ve eřitli sektörlerde büyük řirketlere hizmet veren bir siber güvenlik firmasıdır. Sızma testi ve siber güvenlik danışmanlığı hizmetlerinin yanında; SOME (Siber Olaylara Müdahale Ekibi) kurulumu gibi pek ok alanda anahtar teslim proje sunmaktadır.

© 2015 Sparta Biliřim Teknolojileri Danıřmanlık San. ve Tic. Ltd. řti