

DNS Tünelleme

1. DNS Servisi nasıl çalışır?
 - a. Rekursif dns sorgular
 - b. Iterative dns dorgulamaları
2. DNS kullanarak Tünelleme
 - a. DNS Tünelleme Araçları
 - b. DNS Tünelleme Nasıl Çalışır?
 - c. Pratik Uygulama(Iodine)
 - Sunucu tarafı yapılandırma
 - İstemci tarafı yapılandırma
3. DNS Tünellemeyi nasıl Engellerim?
4. Kaynaklar

Huzeyfe ÖNAL
huzeyfe@enderUNIX.org
<http://www.enderunix.org/huzeyfe>

DNS Servisi Nasıl Çalışır?

DNS sistemi basitçe internet üzerinde kullanılan isim-IP eşleşmesini ve maillerin yönlendirilmesi amaçlı kullanılır. Günümüzde DNS'siz bir ağ düşünülemez denilebilir. Her yerel ağda –ve tüm internet ağında- hiyerarşik bir DNS yapısı vardır.

DNS sistemine ait temel bileşenler;

DNS sistemi çeşitli kayıt tiplerinden oluşur , bu tipler;

- a. A: isimden IP çözmek için
- b. MX: belirtilen isme ait mail sunucuyu bulur
- c. PTR: verilen IP için isim karşılığını bulur
- d. TXT: sunucuya ait çeşitli özellikleri almak için

...

...

Kullanılırlar.

Sıradan bir dns sorgusu UDP/53 kullanırken cevabı 512 bytedan büyük olan dns istekleri TCP/53 kullanır. Bu sebeple genellikle güvenlik duvarlarında UDP ve TCP 53 portları açık olur.

DNS sisteminde iki çeşit sorgu tipi vardır. Bunlar, iterative sorgular ve recursive sorgulardır.

Recursive dns sorgular

Recursive sorgulama tipinde istemci dns sunucuya rekursif bir sorgu gönderir ve cevap olarak sorgusuna karşılık gelen tam cevabı – sorguladığı domaine ait cevap- ya da bir hata bekler.

DNS sorgulamaları için kullanılan nslookup komutu öntanımlı olarak rekursif sorgular gönderir, non rekursif sorgu göndermek için nslookup komutu **set norecurse** seçenekleri ile çalıştırılması gerekir.

```
# nslookup
> set all
Default server: 192.168.206.1
Address: 192.168.206.1#53

Set options:
novc          nodebug      nod2
search        recurse
timeout = 0    retry = 2    port = 53
querytype = A  class = IN
srchlist = localdomain
>set norecurse
```

Iterative dns sorgular

Iterative sorgu tipinde, istemci dns sunucuya sorgu yollar ve ondan verebileceği en iyi cevabı vermesini bekler, yani gelecek cevap ya ben bu sorgunun cevabını bilmiyorum şu DNS sunucuya sor ya da bu sorgunun cevabı şudur şeklindedir.

Ön Belleğe alma(caching): Yapılan dns sorgusu sonrası sunucudan dönen cevap bir TTL alanı içerir ve bu alan istemcinin aynı domaine aynı tipte yapacağı bir sonraki sorgulama zamanını belirler.

DNS kullanarak Tünelleme

DNS Tünelleme aslında çok uzun zamandır teorik olarak bilinen fakat pratik kullanımına sık rastlanmayan bir konu. Poc amaçlı Yazılan uygulamaların kurulum ve kullanımının uzmanlık gerektirmesi pratik kullanımına engel olan önemli hususlardan.

DNS tünelleme ne amaçla kullanılır diye bir soru takılabilir aklımıza. DNS tünelleme ilk olarak yıllar önce Slashdot'da okuduğum bir haber sonrası dikkatimi çekmişti ve sadece konunun teorik kısmını araştırmakla yetinmiştim.. Birgün ücretli kablosuz ağ hizmeti veren bir firmanın güvenlik testlerini yaparken aklıma dns tünelleme yöntemi geldi ve çabucak test ortamımı hazırladım...

Bahsettiğim kablosuz ağ ortamı bugünlerde oldukça sık rastlayabileceğimiz paralı kablosuz ağ hizmetlerinden. Kullanıcı kablosuz ağa bağlanır ve herhangi bir web sitesini açmak istediğinde otomatik olarak bir sayfaya yönlendirilir ve burada kullanıcı adı parola sorulur. Eğer geçerli bir kullanıcı adı parola varsa sistem kullanıcıya belirli bir süreliğine erişim izni verir(captive portal). Burada captive portal yazılımları kullanıcıdan gelen dns isteklerini önce çözümleyerek sonra ilgili kontrol sayfasına yönlendiriyor. Herhangi birisi de DNS tünelleme yazılımını kullanarak ilk sorgulama yaptığı domain üzerinden sınırsız internet erişimi kazanabiliyor.

DNS Tünelleme Nasıl Çalışır?

DNS protokolünden bahsederken çeşitli kayıt tiplerinden oluştuğunu ve sorgulamaların bu kayıtlar aracılığı ile yapıldığını belirtmiştik. Dns tünellemeye de bu sorgu tiplerini kullanıyoruz. Mesela bir TXT kaydı her bir kayıt için base64 formatında 220 byte veri taşıyabiliyor. Diğer yaygın kullanılmayan dns kayıt tipleri ile çok daha fazla veri taşıyabiliyor. Burada önemli olan tek bir kayıt tipi ile max ne kadar veri taşıyabileceğidir.

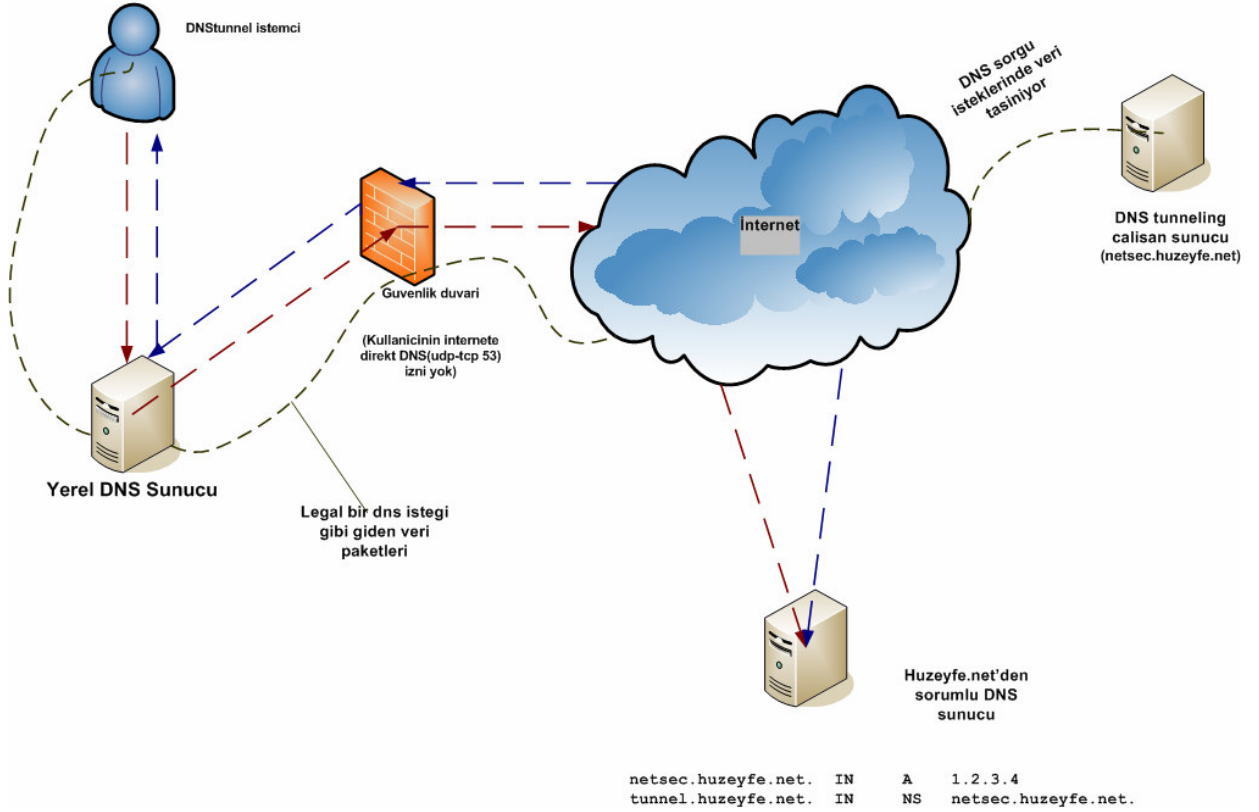
Tekrardan DNS sisteminin nasıl çalıştığını hatırlatalım: Yerel ağınızdaki makinenizden **abc.tunnel.huzeefe.net** adresinin sorgulandığında aşağıdaki adımlar yürütülür.

- 1)Sorgu ilk olarak yerel DNS sunucuya iletilecektir,
- 2)Yerel DNS sunucu kendi ön belleğini kontrol ederek böyle bir kayıttan haberdar olup olmadığına bakacaktır ve eğer kayıt varsa kullanıcıya cevap dönecektir
- 3)Eğer kendi üzerinde kayıt yoksa öncelikle huzeefe.net'ten sorumlu DNS sunucuyu bulacaktır
- 4)huzeefe.net'ten sorumlu DNS sunucuyu bulduktan sonra tunnel.huzeefe.net alt domaininden kimin sorumlu olduğunu soracaktır ve alacağı cevaba abc.tunnel.huzeefe.net adresini soracaktır.

Evet ne oldu? Benim yerel ağdan yaptığım masumane dns isteği geldi tunnel.huzeefe.net'den sorumlu dns sunucuya(netsec.huzeefe.net oldugunu varsayalım).

Peki ben özel bir dns isteği oluştursam ve sorgulama kısmının haricinde kalan alana(xyz byte) istediğim verileri yerleştirsem ve göndersem aynı istek netsec.huzeefe.net adresine(netsec.huzeefe.net adresinin udp/53 portuna) gelecek mi? Evet, hem de hiçbir değişikliğe uğramadan. O zaman ben *netsec.huzeefe.net* adresinde özel bir uygulama çalıştırarak yine özel istemcimden gelen verileri yorumlayabilir miyim. Yeterli bilgim ve deneyimim varsa neden olmasın? Ya da bunu birileri bizim yerimize yaptıysa..

Kısaca DNS tünelleme, bir istemci ve bu istemcinin ürettiği paketlerden anlayacak bir sunucudan oluşur. Sunucunun DNS portundan çalıştırılarak gerçek bir DNS sunucu gibi gözükmesi sağlanır.



DNS Tünelleme Araçları

UNIX/Linux dünyasında birçok DNS tünelleme yazılımı olmakla birlikte bunların çoğu oldukça zahmetli bir kurulum ve kullanım gerektirir. Bu yazı için üç farklı DNS tünelleme uygulamasından bahsedeceğim ve bunlardan biri -ki diğerlerine göre kurulumu, kullanımı oldukça basit- ile sistemin nasıl çalıştığını örneklemeye çalışacağım.

UNIX Dünyasındaki popüler DNS Tünelleme Yazılımları;

Ozymandns

Perl ile yazılmış ve en sık kullanılan Dns tünelleme yazılımlarından biri. (<http://www.doxpara.com/>) Kullanımı için gerekli olan perl modüllerinin fazlalığı ve perl'un threads desteği olmadığı durumlarda problem çıkarması sebebi ile benim tercih etmediğim bir yazılım. Kurulum sonrası kullanımı ise kurulumun tam tersi olarak oldukça kolay.

Ozymandns'in sağlıklı çalışabilmesi için sistemde kurulu olması gereken perl modülleri

```
Fcntl;
Net::DNS;
```

Net::DNS::Nameserver;
LWP::Simple;
LWP::UserAgent;
Time::HiRes qw (usleep gettimeofday);
MIME::Base64;
MIME::Base32 qw (RFC);
IO::Socket;
Class::Struct;
threads;
threads::shared;
Thread::Queue;
Getopt::Long;
English;

Nstx

nstx ozzyman'a gore biraz daha kararli ve her iki ucta Linux gerektiriyor.. Kurulum ve kullanımı oldukça kolay. Sahte tun arabirimleri ile gerçek bir VPN gibi çalıştırılabilir. Sadece Linux sistemlerde çalışması bir dezavantaj olarak göze çarpıyor.

<http://nstx.dereference.de/nstx/>

Yapılandırması ile ilgili detay bilgiye [5] adresinden erişilebilir.

Iodine(IP over DNS is now easy)

Iodine(IP over dns now easy)dns tünelleme yazılımları arasında hem platform bağımsız olması hem de kolay kurulum ve kullanımı ile en iyi dns tünelleme yazılımı sayılabilir.

Iodine Linux , FreeBSD ve OpenBSD vs üzerinde problemsiz çalışmakta. Benim test ortamımda istemci tarafında FreeBSD , sunucu tarafında OpenBSD makine bulunmakta.

DNS Tünelleme Uygulaması

Sunucu tarafında yapılması gereken işlemler

Ana DNS sunucuda Yapılacak Konfigurasyon

Not: Ayarlar BIND için geçerlidir, diğer DNS sunucular için denenmemiştir..

```
netsec.huzeyfe.net. IN A 1.2.3.4  
tunnel.huzeyfe.net. IN NS netsec.huzeyfe.net.
```

NOT:1.2.3.4 IP adresi DNS tunneling sunucusunu çalıştırdığınız sistemin IP adresi.

Böylece abc.tunnel.huzeife.net adresli bird ns sorgulaması yapıldığında bu sorgular 1.2.3.4 IP adresinde gidecektir.

Bu kayıtları girdikten sonra nslookup ile abc.tunnel.huzeife.net adresini sorguladım ve aynı zamanda 1.2.3.4 IP adresli makinede udp 53 paketlerini dinlemeye aldım, sonuç?

```
#tcpdump -i r10 -ttnn udp port 53
tcpdump: listening on r10, link-type EN10MB

1158514012.004200 2.1.2.2.32775 > 1.2.3.4.53: 14404% [1au] A?

abc.tunnel.huzeife.net. (51) (DF)
1158514014.005862 2.1.2.2.32775 > 1.2.3.4.53: 17191% [1au] A?

abc.tunnel.huzeife.net. (51) (DF)
1158514016.007745 2.1.2.2.32775 > 1.2.3.4.53: 31022% [1au] A?

abc.tunnel.huzeife.net. (51) (DF)
1158514024.011724 2.1.2.2.32775 > 1.2.3.4.53: 60844 A? abc.tunnel.huzeife.net.

(40) (DF)
```

Çıktılardanda görüldüğü gibi DNS sorgulamaları sunucuya kadar ulaşıyor fakat sunucu üzerinde udp/53'u dinleyen herhangi bir uygulama olmadığı için cevap dönülüyor.

DNS sunucudan bu yönlendirmeleri yaptıktan sonra sunucu tarafı yazılımını kuralım.

```
#pwd
/tmp
#mkdir dns
#cd dns
#wget http://code.kryo.se/iodine/iodine-0.3.2.tar.gz
--20:28:51-- http://code.kryo.se/iodine/iodine-0.3.2.tar.gz
=> `iodine-0.3.2.tar.gz'
Resolving code.kryo.se... done.
Connecting to code.kryo.se[194.47.250.229]:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 13,014 [application/x-gzip]

100%[=====
=====>] 13,014 59.95K/s ETA 00:00

20:28:52 (59.95 KB/s) - `iodine-0.3.2.tar.gz' saved [13014/13014]
```

```
#tar zxvf iodine-0.3.2.tar.gz
iodine-0.3.2
iodine-0.3.2/TODO
iodine-0.3.2/encoding.c
iodine-0.3.2/encoding.h
iodine-0.3.2/Makefile
iodine-0.3.2/dns.c
iodine-0.3.2/dns.h
iodine-0.3.2/tun.c
iodine-0.3.2/tun.h
iodine-0.3.2/README
iodine-0.3.2/iodined.c
iodine-0.3.2/structs.h
iodine-0.3.2/CHANGELOG
iodine-0.3.2/read.c
iodine-0.3.2/read.h
iodine-0.3.2/test.c
iodine-0.3.2/iodine.c
```

```
#cd iodine-0.3.2
#make
OS is OPENBSD
CC iodine.c
CC tun.c
CC dns.c
CC read.c
CC encoding.c
LD iodine
CC iodined.c
LD iodined
CC test.c
LD tester
Running tests...
** iodine test suite
* Testing read/putshort... OK
* Testing read/putlong... OK
* Testing readname... OK
** All went well :)
```

Sunucu Tarafında Iodine Çalıştırma

```
#!/iodined -f 5.5.5.1 abc.tunnel.huzeyfe.net
Opened /dev/tun0
Setting IP of tun0 to 5.5.5.1
Adding route 5.5.5.1/24 to 5.5.5.1
add net 5.5.5.1: gateway 5.5.5.1
```

Setting MTU of tun0 to 1024
Opened UDP socket
Listening to dns for domain abc.tunnel.huzeife.net

İstemci tarafı Kurulum

İstemci tarafında da aynı yazılımı indirerek sunucu kurulumundaki gibi kurulması gerekir. İstemci ve sunucu arasındaki tek fark çalıştırılmaları sırasında alacakları parametredir.

İstemci tarafı iodine çalıştırma

#iodine -f Sunucu_ip_adresi abc.tunnel.huzeife.net

Bu adımdan sonra istemci ve sunucu tarafında yeni tun arabirimleri oluşarak 5.5.5.1 ve 5.5.5.2 IP adreslerini alacaktır. İstemciden sunucuya erişim kontrolü için

\$ping 5.5.5.1 komutu çalıştırılabilir.

Bundan sonrası yazılacak yönlendirmelerle tüm trafik yeni kurulan tünel aracılığı ile yönetilebilir.

Bağlantı testi;

```
$ scp -P 2000 huzeife@5.5.5.1:/tmp/test.exe .  
huzeife@5.5.5.1's password:  
test.exe 100% 1000KB 111.1KB/s  
00:09
```

DNS Tünellemeyi nasıl Engellerim?

DNS tünellemeyi engellemek için ilk akla gelen yöntem gereksiz gibi görünen kayıt tiplerini yasaklamaktır. Mesela txt kayıtları gibi. (TXT kayıtlarını engelleyerek yaparsak SPFLerde çalışmaz.). Fakat bazı yazılımlar A kaydı gibi kullanılması zorunlu kayıt tiplerini de kullanabildiği için bu yöntemi eliyoruz.

Engellemenin en sağlıklı çözümü ağda bir IDS/IPS sistemi çalıştırmak ve anormal dns trafiklerini farkedecek şekilde yapılandırmaktır. Ya da ağ trafiği raporlama yazılımları kullanarak DNS trafiğinin kullanım oranını takip etmek .

Internette bazı dns tünelleme yazılımları için yazılmış Snort kuralları dolanıyor fakat çoğu benim testlerim sonucu sağlıklı sonuçlar vermedikleri için buraya almadım.

NSTX aracını belirlemek için Snort kuralı

```
alert udp $EXTERNAL_NET any -> $HOME_NET 53 (msg:"Potential NSTX DNS Tunneling"; content:"\01 00\"; offset:2; within:4; content:"cT"; offset:12; depth:3; content:"\00 10 00 01\"; within:255; classtype:bad-unknown; sid:1000 2;)
```

Bunların haricinde ağ ortamınıza göre çeşitli yöntemler bulabilirsiniz(dns proxy vs)

Kaynaklar:

- [1] <http://www.daemon.be/maarten/dns.html>
- [2] <http://htun.runlinux.net/>
- [3] <http://www.daemon.be/maarten/dnstunnel.html>
- [4] <http://www.digitalsec.es/stuff/texts/dns-tunnelingv0.2-en.txt>
- [5] <http://thomer.com/howtos/nstx.html>
- [6] <http://infosecpotpourri.blogspot.com/2006/05/traffic-analysis-approach-to-detecting.html>
- [7] <http://www.csnc.ch/estatic/services/research/dnstunnel.html>
- [8] DNS tunneling test aracı:
https://infosecuritymag.techtarget.com/articles/may01/columns_tech_talk.shtml
- [9] <http://www.dnstunnel.de>