# Bilindik engelleme yöntemlerinin dışında olan, kurumsal web filitreleri nasıl aşılır ?

Not : Yazdıklarım tamamen öğretim amaçlıdır. Yaşanacak her türlü sıkıntının sorumlusu uygulayan kişidir. Sorumluluk kabul etmediğimi belirtirim.

Bu döküman www.teknotrik.com tarafından paylaşılmıştır.

# ANALİZ

Kurumsal engelleme yapan yazılımlar farklı olarak ne yapar ?

- Proxy kullanamazsınız çünkü standart http headerleri denetlendiği için proxy isteği anında anlaşılır ve bloklanır. Headerleri inceleyince çok net fark görülüyor zaten.
- ssh tünelleme mükemmel çözüm fakat, istemci ve sunucu şifreli iletişime geçmeden önceki tanışma faslını temsil eden mesajlar plain text olduğundan tanınır ve bloklanır.
- SSL sertifikası kurumunuza aitse işiniz çok daha zor . Zira artık güvenli mesajlaşma protokülünüz kurumunuzun inisiyatifindedir. tüm içerikleriniz filitrelenebilir, kara listedeki kelimeler vb istekler engellenir.

Bunları tespit etmem 2-3 günümü aldı. Engeli aşmak için kafamdaki senaryo belliydi fakat ihtiyacım olan python bilgisine sahip olmadığımdan işim dahada zorlaşmıştı.

# SENARYO

Yapmam gereken bir proxy scripti bulup, kurum dışında bir makinede çalıştırıp bu bilgisayarı vekil olarak kullanmaktı. Tabi bilindik yöntemlerden farklı olmalıydı

Http headerlerini localde kendime göre biçimlendirip bunu sunucuya gönderdikten sonra tekrar düzenli halde kullanmam gerekiyordu. Onlarca deneme ve haftalarca araştırmalarım sonunda nihayet bir çözüm buldum. Hem en iyisi diye bilirim. Başka çözümde var tahminim fa onu denemedim. hele bunu tüketelim :)

# İhtiyaçlar

- 1. Kurum dışında bir PC. Mümkünse yurt dışından bir VDS . Bu yoksa evinizdeki bilgisayarda olur (Evdeki PC için modemden 80. portu PC nize yönlendirmelisiniz)
- Modifiye ettiğim bu python scripti Aşağıdaki örnek kodlarda simpleproxy\_cln\_ham.py veya simpleproxy\_haw.py olarak kullandım. Sizin indirdiğiniz dosya adı proxy.py. Siz bunu yazın.
- 3. Windows istemciler için putty yazılımı
- 4. Sabır ve sabır...

# KISA ANLATIM

1. Sunucu tarafındaki 80 nolu portu boşa çıkartın . varsa kullanan programı kapatın.(mesala apache gibi)



2. Sunucu da SSH configini düzenleyin. (RSA keyi istemeden sadece parolalı giriş için bir düzenleme)



3. proxy.py scriptini sunucu tarafında çalıştırın.



10.0.66.136.80 olan ip sunucun yerel ip si. Bazı sunucularda WAN ip sini yazınca oluyor.

- 4. Local istemci pc de scripti çalıştırın (sonra konsolu kapatmayın açık kalsın)
  - a. linux makinede python script çalıştırmak için simpleproxy\_cln\_ham.py scriptin adı. Sizin indirdiğiniz dosya adı proxy.py. Siz bunu yazın root@debian:/home/\_\_\_\_Masaüstü/proxy02# python simpleproxy\_cln\_ham.py localhost:22 u\_\_\_\_\_\_\_.
  - b. Win makinelerde python script çalıştırmak için Win makinelerde python3x i kurun komut satırını açın. python.exe dizinine gidin. bu dizinde iken c:\........................>python.exe proxy.py localhost:22 server\_adresi:80

import fcntl hatası alırsanız proxy.py de ilgili satırı silin. Kaydedip tekrar deneyin.

Win de python çalıştırmak için Bu linkteki belgeyi inceleyin. Windows bölümüne bakın lütfen

5. Local pc de yeni bir konsolda tünel açalım .

(Benim sunucumdaki kullanıcı adım okul Değiştirmeyi unutmayın)

Bu döküman <u>www.teknotrik.com</u> tarafından paylaşılmıştır.

- a. Linux makinelerde root@debian:/home/\_\_\_\_/Masaüstü/proxy02# ssh -D 8080 okul@localhost okul@localhost's password:
- b. **win makinelerde** Win makineler için putty kullanımı aşağıdaki geniş anlatımda mevcut
- Firefox için proxy ayarı Aşağıda geniş anlatımda mevcut

# DETAYLI ANLATIM

1. Sunucu olarak kullancağımız bilgisayarda 80 nolu port boşta olmalı.

apache vb varsa kaldırın yada port unu değiştirin. Fakat 80 kesinlikle bizim olmalı onu biz kullanacağız. Kurumunuzun internetinde port yasaklama yoksa istediğinizi kullanabilirsiniz.



#### 2. SSH için ön hazırlık.

• ssh güvenlik olarak RSA kullanır ve key oluşturmak gerekir. Fakat sunucunuzdaki ssh configinde bir satırı değiştirerek sadece password ile giriş yapmak daha pratik.



Olarak değiştirin dosyayı kaydedip kapatın

• Sonra ssh servisini restart edin.



3. proxy.py scriptini sunucuda çalıştırmak için linux makinelerde root olduktan sonra aşağıdaki komutu verin.

#### #python proxy.py 10.0.66.136:80 localhost:22

(80 . porta gelen isteği 22 nolu porta yönlendiriyoruz. tabi bu istek filitreleme sistemi anlamasın diye encrypt ettim , karşıya ulaşınca decrypt ediliyorum )

sizin yapmanız gereken **10.0.66.136** bu IP yi değiştirmek. Burası önemli vds kullanıyorsanız yerel ağ IP sini (deneme yapmak lazım) yada gerçek IP yi yazmalısınız (*! 127 x x x değil*). Ev deki PC nizi kullanacaksanız sanırım aynı şey geçerli, ev PC mi server olarak henüz denemedim. Not :linux makinelerde yerel ağ ip sini *ifconfig* komutuyla alabilirsiniz.

Not : linux makinelerde yerel ag ip sini *ifconfig* komutuyla alabilirsiniz.

okul: ~ \$ sudo su
root: /home/okul \$ python simpleproxy\_haw.py 10.0.66.136:80 localhost:22

ilk satırda root oldum ikinci satırda scripti çalıştıracak komutu yazdım ve entere bastım. scriptin bulunduğu dizinde olduğunuzdan emin olun.

#### 4. İstemci bilgisayarda (ofisinizdeki pc)

#### Linux makinelerde

Gene aynı scripti çalıştırın. fakat bu sefer argümanlar farklı

#### #python proxy.py localhost:22 server\_adresi:80

(localdeki 22 nolu porta gelen istekleri uzak sunucudaki 80 nolu porta gönderiyoruz tabiki şifreli olarak maksat filitreden kaçmak :) )

Bu komut satırında server\_adresi sizin VDS nizin yada evdeki PC nizin adresi / IP si olacak.

root@debian:/home/\_\_\_\_/Masaüstü/proxy02# python simpleproxy\_cln\_ham.py localhost:22 u\_.80

# Win makinelerde

python3x i kurun

Bu döküman www.teknotrik.com tarafından paylaşılmıştır.

komut satırını açın. python.exe dizinine gidin. bu dizinde iken c:\..................>python.exe *proxy.py localhost:22 server\_adresi:80* 

import fcntl hatası alırsanız proxy.py de ilgili satırı silin. Kaydedip tekrar deneyin.

# 5. Buraya kadar sorunsuz geldiniz umarım. Artık offisimizdeki PC de ssh ile tünel açama safhasına geldik.

Amacımız yerel pc mizdeki 8080 nolu porta gelen istekleri. Gene yerel pc de çalışan python scribine yönlendirmek. scriptimiz gelen istekleri şifreleyip sunucuya 80 . portan yönlendirecek. datalar şifreli olduğu için filitreden geçebilecek.

Sunucuya gelen şifreli datalar decrypt edilip sunucunun 22 nolu portunu dinleyen ssh a iletilecek. Cevapta aynı yolu izleyerek bize şifreli olarak gelecek.

# LİNUX MAKİNELERDE SSH TÜNEL AÇALIM

Benim uzak sunucudaki kullanıcı adım **okul** siz kendi kullanıcı adınızı yazmalısınız root@debian:/home/\_\_\_\_/Masaüstü/proxy02# ssh -D 8080 okul@localhost okul@localhost's password:

İlk satırdaki kodu girdikten sonra entere basın uzaktaki sunucu sizden parola isteyecektir. kullanıcı parolasını girdikten sonra ssh oturumu açılacaktır muhtemelen aşağıdaki görüntüyü elde edeceksiniz.

```
* Documentation: https://help.ubuntu.com/
 System information as of Tue Jun 7 10:28:13 UTC 2016
 System load: 0.0
                                  Processes:
                                                        112
 Usage of /: 57.8% of 2.82GB Users logged in:
 Memory usage: 21%
                                  IP address for eth0: 10.0.66.136
 Swap usage:
                \Theta^{9_{6}}
 Graph this data and manage this system at:
   https://landscape.canonical.com/
 Get cloud support with Ubuntu Advantage Cloud Guest:
   http://www.ubuntu.com/business/services/cloud
250 packages can be updated.
155 updates are security updates.
*** /dev/xvdal should be checked for errors ***
Last login: Tue Jun 7 10:28:13 2016 from localhost
okul: ~ $
```

# WINDOWS MAKINELERDE PUTTY ILE SSH TÜNEL AÇMA

Datasa	
Lategory:	
🗐 Session	Options controlling SSH port forwarding
Logging	Port forwarding
🚊 Terminal	
- Keyboard	Local ports accept connections from other hosts
Bell	Remote ports do the same (SSH-2 only)
Features	Forwarded ports: Bemove
🖃 Window	
Appearance	
Behaviour	
Translation	
Selection	Add new forwarded port: 1
Colours	Source port 8080
E Connection	
Data	Destination
Data	O Local Bemote Dupartic
Telect	
Placin	
niogin e cou	
E 33H	
- Nex	
Auth	
- X11	
- I unnels	×
About	Open Cancel
	lon
Category:	ion
Category:	Options controlling SSH port forwarding
Category:	Options controlling SSH port forwarding
Category:	Options controlling SSH port forwarding Port forwarding
Category: Session Logging Terminal Kevboard	Options controlling SSH port forwarding     Port forwarding     Local ports accept connections from other hosts
Category:	Options controlling SSH port forwarding     Port forwarding     Local ports accept connections from other hosts     Remote ports do the same (SSH-2 only)
Category: Session Logging Terminal Keyboard Bell Features	Options controlling SSH port forwarding     Port forwarding     Local ports accept connections from other hosts     Remote ports do the same (SSH-2 only)     Forwarded ports:
Category: Session Logging Terminal Keyboard Bell Features Window	Options controlling SSH port forwarding     Port forwarding     Local ports accept connections from other hosts     Remote ports do the same (SSH-2 only)     Forwarded ports:     Remove
ategory: Session Logging Terminal Keyboard Bell Features Window Appearance	Options controlling SSH pot forwarding     Port forwarding     Local ports accept connections from other hosts     Remote ports do the same (SSH-2 only)     Forwarded ports:     Remove
Category: Session Logging Terminal Keyboard Bell Features Window Appearance Behaviour	Options controlling SSH port forwarding     Port forwarding     Local ports accept connections from other hosts     Remote ports do the same (SSH-2 only)     Forwarded ports:     Remove      D8080
Category: Session Logging Terminal Keyboard Bell Features Window Appearance Behaviour Translation	Options controlling SSH port forwarding     Port forwarding     Local ports accept connections from other hosts     Remote ports do the same (SSH-2 only)     Forwarded ports:     Remove     D8080
Category: Category: Cogging Terminal Keyboard Bell Features Window Appearance Behaviour Translation Selection	Options controlling SSH port forwarding     Port forwarding     Local ports accept connections from other hosts     Remote ports do the same (SSH-2 only)     Forwarded ports:     Remove     D8080     Add new forwarded port:
Category: Session Logging Terminal Keyboard Bell Features Window Appearance Behaviour Translation Selection Colours	Options controlling SSH pot forwarding     Port forwarding     Local ports accept connections from other hosts     Remote ports do the same (SSH-2 only)     Forwarded ports:     Remove     D8080     Add new forwarded port:     Source port     Add
Category: Session Logging Terminal Keyboard Bell Features Window Appearance Behaviour Translation Selection Colours Compending	Options controlling SSH port forwarding     Port forwarding     Local ports accept connections from other hosts     Remote ports do the same (SSH-2 only)     Forwarded ports:     Remove     D8080     Add new forwarded port:     Source port     Add
Category: Session Logging Terminal Keyboard Bell Features Window Appearance Behaviour Translation Selection Colours Connection Data	Options controlling SSH port forwarding     Port forwarding     Local ports accept connections from other hosts     Remote ports do the same (SSH-2 only)     Forwarded ports:     Remove     D8080     Add new forwarded port:     Source port     Add     Destination
Category: Session Logging Terminal Keyboard Bell Features Window Appearance Behaviour Translation Selection Colours Connection Data Prove:	
Category: Session Logging Terminal Keyboard Bell Features Window Appearance Behaviour Translation Colours Connection Data Proxy Locot	Options controlling SSH port forwarding     Port forwarding     Local ports accept connections from other hosts     Remote ports do the same (SSH-2 only)     Forwarded ports:     Remove     D8080     Add new forwarded port:     Source port     Add     Destination     Local     Remote     Options     Options
Category: Session Logging Terminal Keyboard Bell Features Window Appearance Behaviour Translation Selection Colours Connection Pata Proxy Telnet Data Proxy Telnet	Options controlling SSH port forwarding     Port forwarding     Local ports accept connections from other hosts     Remote ports do the same (SSH-2 only)     Forwarded ports:     Remove     D8080     Add new forwarded port:     Source port     Add     Destination     Local     Remote     Options
Category: Session Logging Terminal Keyboard Bell Features Window Appearance Behaviour Translation Selection Colours Connection Data Proxy Telnet Rlogin	
Category: Session Logging Terminal Keyboard Bell Features Window Appearance Behaviour Translation Selection Colours Connection Data Proxy Telnet Riogin SSH	Options controlling SSH port forwarding Port forwarding Local ports accept connections from other hosts Remote ports do the same (SSH-2 only) Forwarded ports: Page 2000 Remove D8080 Add new forwarded port: Source port Add new forwarded port: Source port Add Destination Local Remote Dynamic Auto IPv4 IPv6
Category: Session Logging Terminal Keyboard Bell Features Window Appearance Behaviour Translation Selection Colours Connection Data Proxy Telnet Rlogin SSH Kex	Options controlling SSH port forwarding     Port forwarding     Local ports accept connections from other hosts     Remote ports do the same (SSH-2 only)     Forwarded ports:         Remove     D8080     Add new forwarded port:     Source port     Add     Destination     Local     Remote     Options     Options     Auto     IPv4     IPv6
Category: Session Logging Terminal Keyboard Bell Features Window Appearance Behaviour Translation Selection Colours Connection Data Proxy Teinet Riogin SSH Kex Auth	Options controlling SSH port forwarding     Port forwarding     Local ports accept connections from other hosts     Remote ports do the same (SSH-2 only)     Forwarded ports:     Remove     D8080     Add new forwarded port:     Source port     Add     Destination     Local     Remote     Options     Auto     IPv4     IPv6
Category: Session Logging Terminal Keyboard Bell Features Window Appearance Behaviour Translation Selection Colours Connection Data Proxy Telnet Rlogin SSH Kex Auth X11	Options controlling SSH port forwarding     Port forwarding     Local ports accept connections from other hosts     Remote ports do the same (SSH-2 only)     Forwarded ports:     Remove     D8080     Add new forwarded port:     Source port     Add     Destination     Local     Remote     Options     Auto     IPv4     IPv6
Category: Session Logging Terminal Keyboard Bell Features Window Appearance Behaviour Translation Selection Colours Connection Data Proxy Telnet Rlogin SSH Kex Auth X11 Tunnels	Options controlling SSH port forwarding Port forwarding Local ports accept connections from other hosts Remote ports do the same (SSH-2 only) Forwarded ports: Remove D8080 Add new forwarded port: Source port Add Destination Local Remote Options Options Auto IPv4 IPv6
Category: Session Logging Terminal Keyboard Bell Features Window Appearance Behaviour Translation Selection Colours Connection Data Proxy Telnet Rlogin SSH Kex Auth X11 Tunnels	Options controlling SSH port forwarding Port forwarding Local ports accept connections from other hosts Remove B8080 Add new forwarded port: Source port Add Destination Local Remote Opynamic Auto IPv4 IPv6

itegory:	_		
Session	^	Basic options for your PuTTY	session
Logging ∃ Terminal Keuboard		Specify your connection by host name Host Name (or IP address)	or IP address Port
Bell		server.domain.com	22
Features Window		Protocol: ORaw OTelnet ORlogin	⊙ SSH
- Appearance - Behaviour - Translation		Load, save or delete a stored session Saved Sessions	
- Selection	.=		
Connection		Default Settings	Load
Data			Save
Proxy			
Telnet Riogin			Delete
- Kex - Auth - X11		Close window on exit: Always Never Only o	n clean exit
Tunnels	~		

Dikkat Host Name kutusuna localhost yazmalısınız

₿ <sup>8</sup>	.tr - PuTTY	
Biggin as:       evren@         evren@joy ~1       [evren@joy ~1]         [evren@joy ~1]       [evren@joy ~1]         [evren@joy ~1]       [evren@joy ~1]	.tr - PuTTY m .tr's password:	
		3

Kaynak : http://shukko.com/tunel/index.html

putty ile ilgili daha geniş bilgiyi araştırın

Artık uzak makinede ssh oturumu açtınız. Tünelimiz hazır.

Firefox u açıp SOCKS ayarını aşağıdaki gibi yapın. Artık sisteminiz hazır. Güle güle kullanın.

😺 Connection Setti	ngs		- 6 ×
Configure Proxies	to Access the Internet		
O Auto-detect pro:	xy settings for this network		
O Use system pro	xy settings		
<u>Manual proxy co</u>	onfiguration:		
HTTP Proxy:		Port:	0
	Use this proxy server for	all protoc	ols
SS <u>L</u> Proxy:		Port:	0
ETP Proxy:		Port:	0
SO <u>C</u> KS Host:	localhost	Por <u>t</u> :	80 80
<u>N</u> o Proxy for:	○ SOC <u>K</u> S v4	Remot	e <u>D</u> NS
localhost, 127	.0.0.1		
Example: .moz	illa.org, .net.nz, 192.168.1.0	/24	
O <u>A</u> utomatic proxy	configuration URL:		
			Reload
Do not prompt for	authentication if password	is saved	
B Help		Cancel	Сок

**Not 1** : Kurumunuzdaki bir pc tünel oluşturduysa diğerleride bunun üzerinden internete çıkabilir. Yapmaları gereken firefox ta SOCK kısmına localhost yerine tünel sahibi PC nin IP sini yazmak. Linux makinenizi paylaşmak için ssh tünel açma komutuna bir parametre eklemelisiniz ssh -g -D 8080 kullanici\_adi@llocalhost

> win makinelerde paylaşım için Tabi putty den yönlendirme izni almak lazım. Local port acc... i işaretleyin.

2 Only)
Remove

Not 2 : Kaliteli bir VDS alınabilir. ve onlarca kişi ortak kullanabilir.

Bu yolu evimde denedim hız normal bağlantıdan hiç farklı değil . Fakat kurumsal internet filitre yazılımı ve donanımı hızı çok düşürüyor. Bedava sirke baldan tatlıdır hesabı çaresiz kullanıyorum.

Not 3 : Adress already using.. benzeri hata alıyorsanız. 80 ve 22 nolu portlar başka yazılımlar tarafından kullnılıyor demektir. onları kapatın. linux makinelerde root iken # service apache2 stop

# service ssh stop

#### DÜŞÜNCE SU GİBİDİR, KOLAY YOLU SEÇER. DOĞRU OLDUĞUNDAN EMİN OLUN