The Art Of Stealth Scanning

Playing With Proxies

Fardin Allahverdinazhand (0x0ptim0us)

Security Researcher
Founder Of Websploit Framework
Twitter : 0x0ptim0us

چه خود ساخته هایی که مرا سوخت ، و چه سوختن هایی که مرا ساخت

ای خدای من ، مرا فهمی عطا کن ، که از سوختنم

ساخته ای آباد از من بجا ماند . . .

در این مقاله که پیش روی شماست به روش‌های اسکن پنهان و تغییر هویت و بازی با پراکسی ها خواهیم پرداخت ،

یکی از دغدغه های پنتستر ها هنگام پنتست یک سیستم به صورت غیر قانونی و بدون مجوز این است که مبادا اطلاعاتی از خود در سرور هدف به جای بگذاریم که فردا قربیان گیر ما شود ...

البته ما خدا رو شاکریم که هر روز فرهنگ امنیت در کشورمان بالا و بالاتر می‌رود !

تو این مقاله ، مثل سایر مقالات این‌جانب از زیاده گویی پرهیز خواهم کرد و فقط تکنیک ها رو برسی خواهیم کرد و صد البته سعی خواهیم کرد بر روی ابزار های معروف این کار رو انجام بدیم تا یک مثال بارز باشه و حوصله شما هم از خوندن مقاله سر نره ...

ابتدا باید یک سری ابزار روی سیستم نصب کنیم بنده از ubuntu 12.04 استفاده میکنم و شما میتونید با هر کدوم از توزیع‌های موجود که راحتین این کار رو انجام بدین ...

پس به ترتیب میخوایم مباحث زیر رو دنبال کنیم :

- نصب tor در توزیع
- نصب و کانفیگ ابزار proxychains
- ارتباط و ارسال سیگنال به tor
- طراحی یک ابزار ساده برای تغییر هویت به صورت اتوماتیک
- اسکن TCP با nmap با عبور ترافیک از سرویس tor
- اکسپلویت و اسکن آسیب پزیری با Sqlmap و Nikto و عبور ترافیک از پراکسی

مباحث این مقاله رو کاهش دادم که طولانی نشه و همین که تونستید این کار رو انجام بدید روی یکی از ابزار ها بقیه ابزار ها هم مثل همین هست ...

خوب برسیم سر اصل مطلب ، ابتدا باید سرویس tor رو روی توزیع نصب کنیم برای اینکار اگه مثل خود من حوصلشو ندارید میتونید از مخازن خود توزیع نصبش کنید :

```
sudo apt-get install tor
```

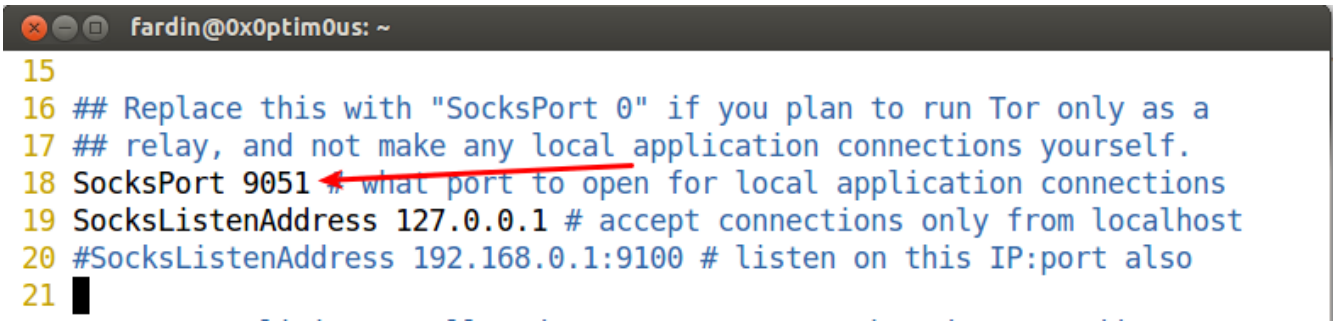
بعد از نصب با دستور زیر سرویس رو استارت کنید :

```
sudo service tor start
```

خوب حالا باید پورت مورد نظر رو روش تنظیم کنیم اگه اشتباه نکنم پورت پیش‌فرض ۹۰۵۰ هست البته چک میکنیم الان :

```
vim /etc/tor/torrc
```

تقریباً تو لاین ۱۸ میتونید پورت رو تنظیم کنید البته به صورت پیش‌فرض ۹۰۵۰ هست که من به ۹۰۵۱ تغییر دادم:



خوب تنظیمات رو سیو کنید میریم سراغ نصب و پیکربندی proxychains ...

برای نصب این ابزار من از مخازن خود اوبونتو استفاده میکنم :

```
sudo apt-get install proxychains
```

خوب بعد نصب یه دستی روی کانفیگ میکشیم :

```
vim /etc/proxychains.conf
```

خوب برید آخر فایل کانفیگ درست مثل تصویر زیر :

همینطور که تو عکس بالا هم دیدید خودش به صورت پیش‌فرض برای tor کانفیگ شده اگر هم غیر این بود مثل تصویر بالا کانفیگش کنید.

خوب حالا نوبتی هم باشه نوبت ارتباط با tor هست ...

برای ارتباط با tor شما هم میتونید از کتابخانه TorCtl در پیتون استفاده کنید و یا میتونید به پورت مذکور telnet کنید ... دلیل اتصال ما به tor چیزی جر تغییر هویت در یک بازه زمانی نیست ... ما میخوایم در اصل ip خودمون رو در یک بازه زمانی عوض کنیم که چندتا مزیت داره ، یکی اینکه زمان اسکن میتونیم از دست فایروال خلاص شیم به این صورت که تعداد درخواست با یک آیپی میاد پایین چون مدام در حال تغییر آیپی هستیم ، و دیگری اینکه درصد trace شدنمون میاد پایین.

من ۳ تا روش برای اتصال به tor و تغییر هویت رو در ادامه مطرح میکنم و هر کدوم رو دوست داشتین میتونید پیاده کنید راه سوم واسه تنبلی مثل من جواب میده ...

اتصال به tor با استفاده از پیتون و کتابخانه TorTcl :

```
#!/usr/bin/python

from TorCtl import TorCtl

connect = TorCtl.connect(controlAddr="127.0.0.1",
controlPort=9050, passphrase="")
torCtl.Connection.send_signal(conn, "NEWNYM")
```

این کد یک کد ساده که میتونید با اجراش هویت رو عوض کنید ... البته این کتابخونه به صورت پیش‌فرض

نصب نیست و باید روی سیستمتون نصبش کنید. این‌ام دنگو فنگ های خواص خودشو داره مثل روش پایینی ...

راه دوم استفاده از telnet هست :

```
telnet localhost 9051
AUTHENTICATE
SIGNAL NEWNYM
QUIT
```

این روش رو من پیشنهاد نمیکنم ! (نه بابا) ، دلیلش اینه که برخی از ورژن های tor همین که telnet میزنی بهش crash میکنن تو بخش bug report این پروژه میتونید چک کنید ... البته به غیر از اون مشکل refuse کانکشن هست که نمیدونم کانفیگ iptables میخواد و فلان کلا به صلاحتون نیست (به قول حاج آقای فیلم رسوایی) ...

اما روش سوم که مورد علاقه منه روش ارسال یک سیگنال HUP به پروسه هست، HUP مخفف کلمه hung-up هستش که در اصل به پروسه میگه دست نگه دار، اما با ارسال این سیگنال به پروسه tor، این سرویس اقدام به تغییر ID میکنه اما روش کار چطوریه ...

تو لینوکس ما باید پروسه tor رو پیدا کنیم سپس اقدام به استخراج PID کنیم، برای اینکار شما میتونید از regular expression استفاده کنید برای مثال به تصویر زیر دقت کنید :

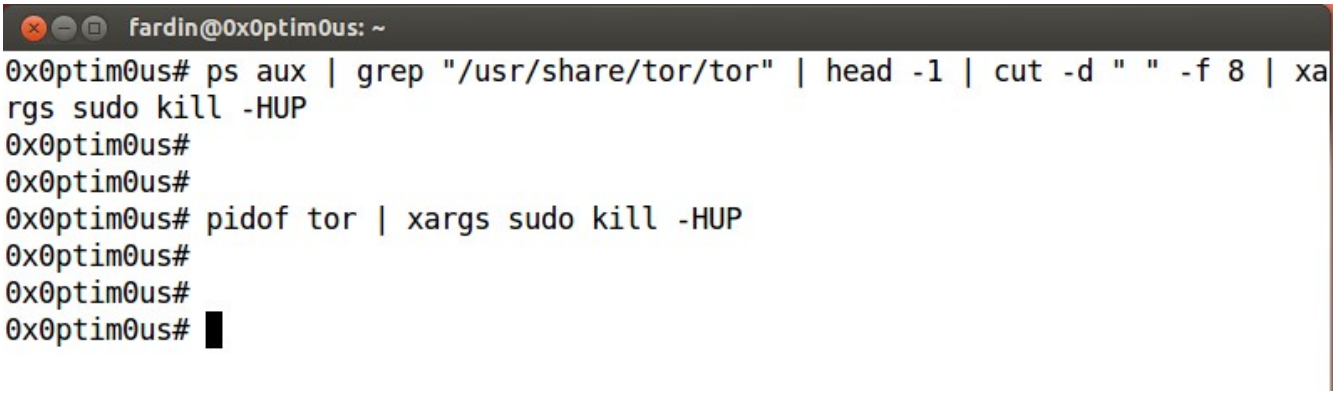
```
fardin@0x0ptim0us: ~
0x0ptim0us# ps aux | grep "/usr/share/tor/tor" | head -1 | cut -d " " -f 8
1250
0x0ptim0us#
0x0ptim0us#
0x0ptim0us# pidof tor
1250
0x0ptim0us#
```

اولین دستور با استفاده از RE اومدیم اسم پروسسه رو تو لیست پروسسه ها پیدا کردیم بعد مسیر رو grep کردیم سپس اضافی ها رو ریختیم دور و در نهایت با استفاده از فاصله اومدیم row رو column بندی کردیم و در نهایت در هشدومین column به PID رسیدیم، یا مثل دستور اولی عمل کنید یا با استفاده از ابزار

pidof بیاید PID رو پیدا کنید بنده دو روش رو هم نوشتم که نتیجه هر کدوم ۱۲۵۰ بود ...

خوب حالا باید با استفاده از دستور kill و کمک گرفتن از دستور xargs این سیگنال رو بفرستیم

خوب من تو تصویر زیر با استفاده از دو روش بالا سیگنال HUP رو ارسال میکنم :



کارایی دستور xargs اینجا اینه که خروجی پشت پایپ رو میندازه انتهای دستورتون بعد پایپ ...

خوب هر دو روش بالا یکی هست و ما سیگنال HUP رو با سویچ HUP- فرستادیم ...

حالا به دور از مقاله این دستور HUP و این تکنیک من رو یاد یک جمله جالب از کتاب «خاطرات سفر با موتور سیکلت» نوشته چگوارا انداخت که شرح حال خود و دوستشون به نام «آلبرتو» رو توش نوشته که با یک موتور سیکلت ۵۰۰ سی سی پا میشن میرن امریکای جنوبی واسه کمک به بیماران جزامی ...

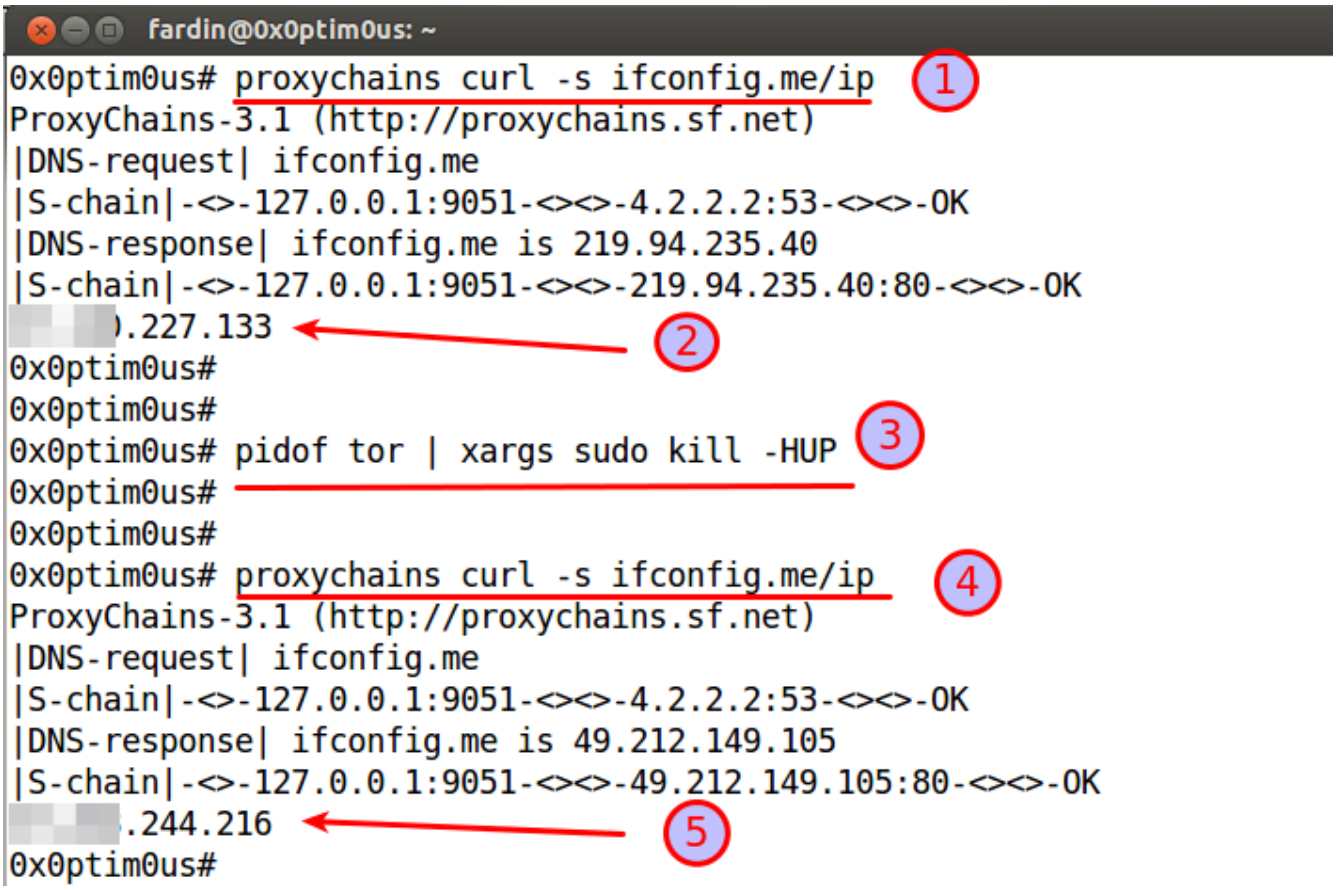
چگوار میگه هر وقت جایی از موتور خراب میشد و یا پیچی شل میشد و می‌افتاد آلبرتو با یک تیکه سیم اون قسمت رو سفت میکرد و می‌گفت : وقتی یک تیکه سیم کار یک پیچ رو انجام میده پس همین سیم و عشقه ... حالا دقیقاً تو مقاله ما هم همین HUP رو عشقه ...

اگه یادتون باشه قبل این بحث ما بحث proxychains رو داشتیم حالا بیاید curl رو از طریق همین proxychains از tor عبور بدیم و دوباره سیگنال HUP رو بفرستیم و بازم هم با curl چک کنیم ببینیم آیپی ما عوض میشه یا نه !

پس در اصل ما یک درخواست GET به آدرس ifconfig.me/ip میفرستیم و آیپی فعلیمون رو در میاریم سپس یک سیگنال HUP به tor میفرستیم و سپس دوباره به آدرس بالا یک درخواست میفرستیم تا ببینیم

آیپی عوض شده یا نه ...

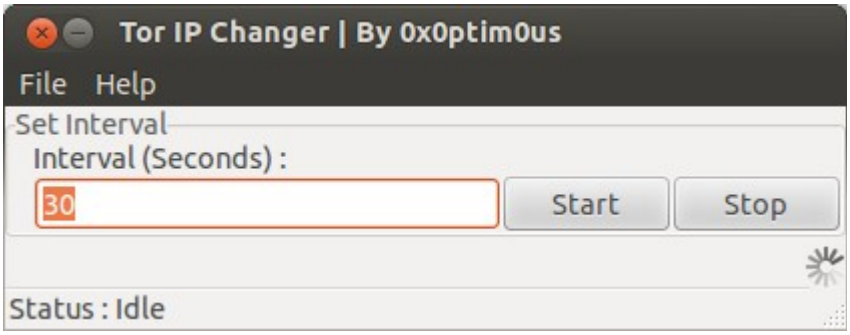
نکته : اجرای ابزار proxychains قبل دستور یادتون نره



به دستوراتی که زیرشون خط کشیدیم توجه کنید و به ایپی هایی که با فلش اشاره کردم ...

پس تا اینجای کار ما تونستیم سرویس tor رو به خوبی پیاده کنیم ...

خوب حالا باید یک اسکریپت ترتیب بدیم که با گرفتن یک interval ساده بر حسب ثانیه بیاد آیپی رو واسمون به صورت auto عوض کنه برای اینکه شما میتونید از هر زبونی که خوشتون میاد برای نوشتنش استفاده کنید من یکی با استفاده از gtk و پیتون نوشتم به این صورت :



میتونید از اینجا دانلودش کنید.

اما اگه دلتون نخواست یه اسکریپت دیگه تو bash نوشتم که همین کار رو انجام میده :

```
#!/bin/bash
# Simple TOR IP Changer
# By 0x0ptim0us

if [[ $EUID -ne 0 ]];then
        echo "You must be root to run this script. Aborting...";
        exit 1;
fi
        while true; do
                echo "[+]Sending HUP Signal ..."

                pid=`pidof tor`
                kill -HUP $pid

                echo "[+]Done. Waiting ..."
                sleep 30
        done
```

با اجرای این اسکریپت با دسترسی روت هر ۳۰ ثانیه یک بار سیگنال ارسال میشه که میتونید مقدار sleep رو کم یا زیاد کنید اما به نظر من بهتره بین ۳۰ ثانیه تا ۲ دقیقه باشه ...

حالا که همه چی خوب پیش رفته من بهتره برسیم سر اسکن با nmap ...

یه نکته‌ای رو بگم تنها مشکل این روش آینه که شما نمیتونید برای مثال با همین nmap بیاید udp اسکن انجام بدید چرا ؟ چون tor واسه tcp طراحی شده پس شما باید تو اسکن توسط nmap سویچ sS- رو فراموش

کنید و بجاش از sT- استفاده کنید پس :

```
proxychains nmap -Pn -sT 127.0.0.1
```

خوب حالا برسیم به sqlmap این ابزار خوشبختانه سویچ برای پشتیبانی از tor داره پس نیازی نیست ما از proxychains برای عبور ترافیک استفاده کنیم اما باید تنظیماتی رو در کانفیگ تور انجام بدیم پس به ابتدای مقاله رجوع میکنیم و فایل کانفیگ رو باز کرده و پورت tor رو به ۹۰۵۰ تغییر میدیم البته چون من در ابتدای مقاله این پورت رو به ۹۰۵۱ تغییر دادم به همین دلیل اگه شما تغییر ندادید خوش به حالتون ...

خوب دستور sqlmap میشه این :

```
./sqlmap.py --tor --tor-type=SOCKS5 -u "http://target.com/index.php?id=1"
```

خوب حالا ابزار nikto رو هم میتونید از طریق proxychains ترافیکشو عبور بدین ...

برسیم به سخن پایانی :

این مقاله و بحثی که در بر گرفته به هیچ عنوان کامل نیست و این مقاله اندکی از این بحث رو پوشش داده بلاخره هرچند کوچک اومیدوارم مورد رضایت شما قرار گرفته باشه ...

خود من همیشه دوست دارم مباحث به صورت شفاف بیان بشه و خلاصه، هم وقت خواننده گرفته نشه و هم اصل مطلب انتقال پیدا کنه و من امیدوارم این مقاله تونسته باشه اصل مطلب رو برسونه ...

باز هم متشکرم که وقت گذاشتید و مطالعه کردید.

خدایا ، حکمت قدم هایی را که برایم بر میداری بر من آشکار کن

تا درهایی را که بسویم می گشایی ، ندانسته نبندم

و درهایی که به رویم میبندی ، به اصرار نگشایم . . .

موفق و مؤید باشد.