

Iptables and SAMBA – I'm going MAAAAAAAAAAAAAAAAAAAAAADDDDDDD!!!

Source: <http://linux.derkeiler.com/Newsgroups/comp.os.linux.networking/2003-11/0651.html>

From: Arsenio Lupin (*lupiniii__SPAMMERDIMERXX_at_hotmail.com*)

Date: 11/13/03

Date: Thu, 13 Nov 2003 18:33:07 GMT

Hi,

i'm trying to setup a firewall with netfilter/iptables increasing security from than one i actually have, on the linux box i use to share my adsl modem (USB). On this linux box i have two net cards that go to two clients (the two subnets: 192.168.0.x/255.255.255.0 and 10.0.0.x/255.255.255.0).

The script works well, but it doesn't work at all with my samba share.

(samba works perfectly if i shut down iptables)

Can someone help me to access SAMBA?

Thanks!

My firewall script is:

```
##### DEBUGGING ###
```

```
set -x
```

```
### FLUSHING CHAIN ### Azzera e pulisce ogni regola esistente
```

```
iptables -F
```

```
iptables -F -t nat
```

```
iptables -X
```

```
iptables -Z
```

```
### DEFAULT CHAIN ### Imposta le policy di default
```

```
iptables -P INPUT DROP
```

```
iptables -P FORWARD DROP
```

```
iptables -P OUTPUT DROP
```

```
iptables -t nat -P POSTROUTING DROP
```

```
### SETTING IPFORWARDING ### Abilita il forwarding di pacchetti non locali –  
FONDAMENTALE
```

```
/bin/echo "1" > /proc/sys/net/ipv4/ip_forward
```

comp.os.linux.networking: Iptables and SAMBA – I'm going MAAAAAAAAAAAAAAAAAAAAADDDDDDD!!!

```
### DISABLE RESPOND TO BROADCAST ### Non risponde ai ping inviati al  
broadcast della subnet  
/bin/echo "1" > /proc/sys/net/ipv4/icmp_echo_ignore_broadcasts
```

```
### ENABLE BAD ERROR MESSAGE PROTECTION ### Ignora finti messaggi di errore  
ICMP  
/bin/echo "1" > /proc/sys/net/ipv4/icmp_ignore_bogus_error_responses
```

```
### DISABLE ICMP REDIRECT ACCEPTANCE ### Non accetta pacchetti ICMP di route  
redirection  
/bin/echo "0" > /proc/sys/net/ipv4/conf/all/accept_redirects
```

```
### SETTING ANTISPOOFING PROTECTION ###  
/bin/echo "1" > /proc/sys/net/ipv4/conf/all/rp_filter
```

```
### DON'T RESPOND TO BROADCAST PINGS ###  
/bin/echo "1" > /proc/sys/net/ipv4/conf/all/log_martians
```

```
### Qui vengono definite alcune variabili che successivamente sono usate  
#nelle regole – MODIFICARE SECONDO I PROPRI PARAMETRI  
# External Public Interface  
EXTIF="ppp0"
```

```
# Internal Private Interface  
INTIF_1="eth0"  
INTIF_2="eth1"
```

```
# Internal LAN IP  
LANIN_1="192.168.0.0/24"  
LANIN_2="10.0.0.0/24"
```

```
# RFC IPs Classi di indirizzi dedicate a utilizzi privati o particolari e  
#non routate su Internet  
LOOPBACK="127.0.0.0/8"
```

```
# ANTISPOOF Adesso iniziano le regole vere e proprie.  
iptables -A INPUT -i $EXTIF -d $LOOPBACK -j DROP
```

```
# LOOP RULE Permettiamo il traffico di loopback  
iptables -A INPUT -s $LOOPBACK -j ACCEPT  
iptables -A OUTPUT -d $LOOPBACK -j ACCEPT
```

```
# LAN IN ACCESS Regole che permettono l'accesso al firewall Linux dagli IP  
#della rete Interna  
iptables -A INPUT -i $INTIF_1 -s $LANIN_1 -j ACCEPT  
iptables -A INPUT -i $INTIF_2 -s $LANIN_2 -j ACCEPT  
iptables -A OUTPUT -o $INTIF_1 -d $LANIN_1 -j ACCEPT  
iptables -A OUTPUT -o $INTIF_2 -d $LANIN_2 -j ACCEPT
```

```
# LAN IN OUT Seguono le regole che gestiscono il masquerading della rete  
interna
```

Iptables and SAMBA – I'm going MAAAAAAAAAAAAAAAAAAAAADDDDDDD!!!

comp.os.linux.networking: Iptables and SAMBA – I'm going MAAAAAAAAAAAAAAAAAAAAADDDDDDD!!!

```
#Forwarda tutti i pacchetti dalla rete interna a qualsiasi destinazione
iptables -A FORWARD -s $LANIN_1 -d 0/0 -j ACCEPT
iptables -A FORWARD -s $LANIN_2 -d 0/0 -j ACCEPT
iptables -A FORWARD -m state --state ESTABLISHED,RELATED -j ACCEPT

#DROPPA i nuovi pacchetti che dall'esterno cercano di raggiungere la rete
interna
#(TCP con flag SYN attivo)
iptables -A FORWARD -s 0/0 -d $LANIN_1 -p tcp --syn -j DROP
iptables -A FORWARD -s 0/0 -d $LANIN_2 -p tcp --syn -j DROP

#Lascia invece passare tutti gli altri pacchetti
iptables -A FORWARD -s 0/0 -d $LANIN_1 -j ACCEPT
iptables -A FORWARD -s 0/0 -d $LANIN_2 -j ACCEPT

#Maschera gli IP sorgenti Interni con l'IP dell'interfaccia pubblica
iptables -t nat -A POSTROUTING -o $EXTIF -s $LANIN_1 -j MASQUERADE
iptables -t nat -A POSTROUTING -o $EXTIF -s $LANIN_2 -j MASQUERADE

# GENERAL Regole generali per permettere all'host locale di collegarsi a
#IP remoti e ricevere i pacchetti di risposta (Nota: si riferiscono alle
#attività che vengono fatte direttamente dalla macchina Linux locale e non
#dagli host che la usano come firewall)
iptables -A OUTPUT -p tcp -m state --state NEW,ESTABLISHED -j ACCEPT
iptables -A INPUT -p tcp -m state --state ESTABLISHED -j ACCEPT
iptables -A OUTPUT -p udp -m state --state NEW,ESTABLISHED -j ACCEPT
iptables -A INPUT -i $EXTIF -p udp -m state --state ESTABLISHED -j ACCEPT
iptables -A OUTPUT -p icmp -m state --state NEW,ESTABLISHED,RELATED -j
ACCEPT
iptables -A INPUT -p icmp -m state --state ESTABLISHED,RELATED -j ACCEPT

# DNS Regole per permettere di ricevere risposta (dai server DNS
#specificati) a query DNS fatte dalla macchina locale

iptables -A OUTPUT -p udp -s 0/0 --dport 53 -j ACCEPT
iptables -A OUTPUT -p tcp -s 0/0 --dport 53 -j ACCEPT
iptables -A INPUT -p tcp -s 0/0 --sport 53 -j ACCEPT
iptables -A INPUT -p udp -s 0/0 --sport 53 -j ACCEPT

# SAMBA
iptables -A INPUT -p udp -s $LANIN_1 -d $LANIN_1 -m multiport --dports
135,137,138,631 -j ACCEPT
iptables -A INPUT -p tcp -s $LANIN_1 -d $LANIN_1 -m multiport --dports
135,137,138,139,445,631 -j ACCEPT
iptables -A OUTPUT -p udp -s $LANIN_1 -d $LANIN_1 -m multiport --sports
135,137,138,631 -j ACCEPT
iptables -A OUTPUT -p tcp -s $LANIN_1 -d $LANIN_1 -m multiport --sports
135,137,138,139,445,631 -j ACCEPT
#iptables -A OUTPUT -m state --state ESTABLISHED,RELATED -j ACCEPT

--
```

Iptables and SAMBA – I'm going MAAAAAAAAAAAAAAAAAAAAADDDDDDD!!!

