Subject: Blocco sblocco della porta 5900 - Come farlo con iptables
Posted by Michele Barbato on Wed, 17 Aug 2011 13:21:42 GMT
View Forum Message <> Reply to Message

Quella sotto è la configurazione iptables del mio server, costruita grazie all'aiuto ottenuto in questo NG.
Confido di nuovo nel vostro aiuto per un paio di comandi che mi consentano di bloccare/sbloccare la porta 5900 utilizzata per il desktop remoto. La porta rimarrebbe sempre bloccata, se ne avessi bisogno mi collegherei con ssh e la sbloccherei.

Grazie.
Mik

iptables -t nat -A OUTPUT -p tcp -m owner ! --uid-owner proxy --dport 80 -j
REDIRECT --to-port 8080

sysctl -w net.ipv4.ip_forward=1

iptables -t nat -I POSTROUTING -j MASQUERADE

iptables -F FORWARD

iptables -P FORWARD ACCEPT

iptables -A FORWARD -m state --state ESTABLISHED,RELATED -j ACCEPT

iptables -t nat -A PREROUTING -i eth0 -p tcp --dport 80 -j
REDIRECT --to-port 8080

#26.7.2011 Forward su telecamere

iptables -t nat -I PREROUTING -p tcp -i eth1 --dport 9001 -j
DNAT --to-destination 192.168.0.7

iptables -t nat -I PREROUTING -p tcp -i eth1 --dport 9002 -j
DNAT --to-destination 192.168.0.8

iptables -t nat -I PREROUTING -p tcp -i eth1 --dport 9003 -j
DNAT --to-destination 192.168.0.9

iptables -t nat -I PREROUTING -p tcp -i eth1 --dport 9004 -j
DNAT --to-destination 192.168.0.10

Subject: Re: Blocco sblocco della porta 5900 - Come farlo con iptables
Posted by Giuseppe Della Bianca on Wed, 17 Aug 2011 15:12:49 GMT

View Forum Message <> Reply to Message

Michele Barbato wrote:

> Quella sotto Ã¨ la configurazione iptables del mio server, costruita grazie
> all'aiuto ottenuto in questo NG.
> Confido di nuovo nel vostro aiuto per un paio di comandi che mi consentano
> di bloccare/sbloccare la porta 5900 utilizzata per il desktop remoto. La
> porta rimarrebbe sempre bloccata, se ne avessi bisogno mi collegherei con
> ssh e la sbloccherei.
]zac[

Con iptables le regole possono essere aggiunte e rimosse, ti basterebbe fare uno script che aggiunge e toglie la regola.

Probabilmente prima di rimuovere la regola devi cercare che numero di sequenza gli e' stato assegnano (grep + cut dovrebbe bastare), o potresti creare una catena apposta solo per quello (opzione -N di iptables se ricordo bene).

Subject: Re: Blocco sblocco della porta 5900 - Come farlo con iptables
Posted by Giuseppe Della Bianca on Wed, 17 Aug 2011 15:18:14 GMT
View Forum Message <> Reply to Message

Michele Barbato wrote:

> Quella sotto Ã¨ la configurazione iptables del mio server, costruita grazie
> all'aiuto ottenuto in questo NG.
]zac[

http://forum.ubuntu-it.org/index.php?topic=256001.0

Subject: Re: Blocco sblocco della porta 5900 - Come farlo con iptables
Posted by Michele Barbato on Wed, 17 Aug 2011 16:24:34 GMT
View Forum Message <> Reply to Message

[...]
> Con iptables le regole possono essere aggiunte e rimosse, ti basterebbe
> fare
> uno script che aggiunge e toglie la regola.
>

Il punto è che non so come scrivere la regola che blocca la porta 5900.

Subject: Re: Blocco sblocco della porta 5900 - Come farlo con iptables
Posted by Alessandro Selli on Wed, 17 Aug 2011 16:40:21 GMT
View Forum Message <> Reply to Message

Giuseppe Della Bianca ha scritto:

[...]

> Probabilmente prima di rimuovere la regola devi cercare che numero di
> sequenza gli e' stato assegnano (grep + cut dovrebbe bastare), o potresti
> creare una catena apposta solo per quello (opzione -N di iptables se ricordo
> bene).

Se si conosce il numero progressivo della vecchia regola, si puÃ² sostituire con la nuova regola in un passo solo. Ad esempio, partendo con una catena vuota:

```
~ # iptables -vL INPUT
Chain INPUT (policy ACCEPT 170K packets, 66M bytes)
 pkts bytes target     prot opt in     out     source
destination
```

Aggiungo una regola:

```
~ # iptables -A INPUT -s 10.0.0.0/8 -d 176.16.20.15 -p tcp --dport 80 -j
REJECT

~ # iptables -vL INPUT
Chain INPUT (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source
destination
    0     0 REJECT     tcp  --  any    any     10.0.0.0/8
176.16.20.15        tcp dpt:http reject-with icmp-port-unreachable
```

Supponiamo che voglia sostituire questa regola con una simile ma che blocchi la porta SSH (22) e non quella HTTP (80). Si puÃ² fare cosÃ¬:

```
~ # iptables -R INPUT 1 -s 10.0.0.0/8 -d 176.16.20.15 -p tcp --dport 22
-j REJECT

~ # iptables -vL INPUT
Chain INPUT (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source
destination
    0     0 REJECT     tcp  --  any    any     10.0.0.0/8
```

176.16.20.15 tcp dpt:ssh reject-with icmp-port-unreachable

Fossero le regole troppo numerose per contarle ad occhio, si puÃ² usare
lo switch --line-numbers, ad es.:

~ # iptables --line-numbers -vL INPUT
Chain INPUT (policy ACCEPT 146 packets, 19274 bytes)
num pkts bytes target prot opt in out source
destination
1 0 0 REJECT tcp -- any any 10.0.0.0/8
176.16.20.15 tcp dpt:ssh reject-with icmp-port-unreachable

Ciao,

--
Alessandro Selli http://alessandro.route-add.net
AVVERTENZA: i messaggi inviati a "trappola" non mi arriveranno.
WARNING: messages sent to "trappola" will never reach me.

Subject: Re: Blocco sblocco della porta 5900 - Come farlo con iptables
Posted by Giuseppe Della Bianca on Thu, 18 Aug 2011 15:21:44 GMT
View Forum Message <> Reply to Message

Michele Barbato wrote:

> [...]
>> Con iptables le regole possono essere aggiunte e rimosse, ti basterebbe
>> fare
>> uno script che aggiunge e toglie la regola.
>>
>
> Il punto Ã¨ che non so come scrivere la regola che blocca la porta 5900.

Per esempio:

iptables -A INPUT -p tcp -m multiport --dports 1433,1434,80 -j DROP

Subject: Re: Blocco sblocco della porta 5900 - Come farlo con iptables
Posted by Michele Barbato on Fri, 19 Aug 2011 13:11:43 GMT
View Forum Message <> Reply to Message

"Giuseppe Della Bianca" <bepi-zac@zac-adria.it> ha scritto nel messaggio
news:89nvh8-746.ln1@exnet.gdb.it...

> iptables -A INPUT -p tcp -m multiport --dports 1433,1434,80 -j DROP

Ok, grazie. Ad intuito e per tentativi alla fine ero arrivato a scrivere:

iptables -A INPUT -p tcp -i eth1 --dport 5900 -j DROP

considerando che eth1 è la porta collegata verso l'esterno.

Vedo che nella tua regola c'è un -m multiport in più che non so a cosa
serva, comunque ora verifico.

Grazie ancora.
Mik.

Subject: Re: Blocco sblocco della porta 5900 - Come farlo con iptables
Posted by Giuseppe Della Bianca on Sat, 20 Aug 2011 11:52:43 GMT
View Forum Message <> Reply to Message

Michele Barbato wrote:

> "Giuseppe Della Bianca" <bepi-zac@zac-adria.it> ha scritto nel messaggio
> news:89nvh8-746.ln1@exnet.gdb.it...
>
>> iptables -A INPUT -p tcp -m multiport --dports 1433,1434,80 -j DROP
>
> Ok, grazie. Ad intuito e per tentativi alla fine ero arrivato a scrivere:
>
> iptables -A INPUT -p tcp -i eth1 --dport 5900 -j DROP
]zac[

porte multiple, nota le porte e non la (sola) porta specificabile

Prego.
