Subject: settare porte su linux mint
Posted by fletcher on Mon, 15 Aug 2011 13:47:17 GMT
View Forum Message <> Reply to Message

Salve a tutti,
ho da pochi giorni installato linux mint e dopo aver scansionato le porte da strumenti di rete, mi appaiono aperte la 139 (netbios) e la 445 (microsoft-ds), tuttavia solo dall'interno in quanto da uno scan sul sito grc.com risultano in stealth.Uso il firewall firestarter ed ho disattivato i servizi di condivisione di file.
Occorre preoccuparmi o Ã¨ tutto regolare?
Grazie a chi mi risponderÃ .
Fletcher

Subject: Re: settare porte su linux mint
Posted by Alessandro Selli on Tue, 16 Aug 2011 10:38:57 GMT
View Forum Message <> Reply to Message

fletcher ha scritto:
> Salve a tutti,
> ho da pochi giorni installato linux mint e dopo aver scansionato le
> porte da strumenti di rete, mi appaiono aperte la 139 (netbios) e la 445
> (microsoft-ds),

Puoi vedere con netstat quali processi hanno aperto quelle porte in ascolto.

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: settare porte su linux mint
Posted by Giuseppe Della Bianca on Tue, 16 Aug 2011 14:22:34 GMT
View Forum Message <> Reply to Message

Alessandro Selli wrote:

> fletcher ha scritto:
>> Salve a tutti,
>> ho da pochi giorni installato linux mint e dopo aver scansionato le

>> porte da strumenti di rete, mi appaiono aperte la 139 (netbios) e la 445
>> (microsoft-ds),
>
> Puoi vedere con netstat quali processi hanno aperto quelle porte in
> ascolto.
>
>
> Ciao,
>
>

samba?

smbd e nmbd probabilmente.

Subject: Re: settare porte su linux mint
Posted by fletcher on Tue, 16 Aug 2011 14:24:56 GMT
View Forum Message <> Reply to Message

Il 16/08/2011 12:38, Alessandro Selli ha scritto:
> fletcher ha scritto:
>> Salve a tutti,
>> ho da pochi giorni installato linux mint e dopo aver scansionato le
>> porte da strumenti di rete, mi appaiono aperte la 139 (netbios) e la 445
>> (microsoft-ds),
>
> Puoi vedere con netstat quali processi hanno aperto quelle porte in
> ascolto.
>
>
> Ciao,
>
>

Grazie per la risposta,
interrogando netstat mi dÃ come servizi attivi :

Protocollo IP sorgente Porta/Servizio Stato
tcp 127.0.0.1 631 LISTEN
tcp 127.0.0.1 25 LISTEN
tcp 127.0.0.1 8123 LISTEN
tcp6 :: 139 LISTEN
tcp6 ::1 631 LISTEN
tcp6 ::1 25 LISTEN
tcp6 :: 445 LISTEN
udp 0.0.0.0 137
udp 0.0.0.0 138

udp 0.0.0.0 45779
udp 0.0.0.0 5353
udp6 :: 5353
udp6 :: 44913

se la porta 631 la mantiene aperta "applet coda di stampa", il servizio nella mia macchina non Ã¨ giÃ attivo e se la 445 la mantiene aperta il servizio di condivisione di files personali anche questo servizio non Ã¨ attivo.
Se invece sono altri i servizi da disattivare, nel caso sia indesiderabile la situazione evidenziata, Vi sarei grato se melo diceste.
Grazie fletcher
Chiedo scusa se ho

Subject: Re: settare porte su linux mint
Posted by fletcher on Tue, 16 Aug 2011 14:39:22 GMT
View Forum Message <> Reply to Message

Il 16/08/2011 16:22, Giuseppe Della Bianca ha scritto:
> Alessandro Selli wrote:
>
>> fletcher ha scritto:
>>> Salve a tutti,
>>> ho da pochi giorni installato linux mint e dopo aver scansionato le
>>> porte da strumenti di rete, mi appaiono aperte la 139 (netbios) e la 445
>>> (microsoft-ds),
>>
>> Puoi vedere con netstat quali processi hanno aperto quelle porte in
>> ascolto.
>>
>>
>> Ciao,
>>
>>
>
> samba?
>
> smbd e nmbd probabilmente.

Grazie per le risposte,
interrogando netstat mi dÃ i serzi attivi seguenti :

Protocollo	IP sorgente	Porta/Servizio	Stato
tcp	127.0.0.1	631	LISTEN
tcp	127.0.0.1	25	LISTEN
tcp	127.0.0.1	8123	LISTEN

tcp6 :: 139 LISTEN
tcp6 ::1 631 LISTEN
tcp6 ::1 25 LISTEN
tcp6 :: 445 LISTEN
udp 0.0.0.0 137
udp 0.0.0.0 138
udp 0.0.0.0 45779
udp 0.0.0.0 5353
udp6 :: 5353
udp6 :: 44913

se la porta 631 la mantiene aperta "applet coda di stampa", il servizio nella mia macchina non Ã¨ giÃ attivo e se la 445 la mantiene aperta il servizio di "condivisione di files personali" anche questo servizio non Ã¨ attivo.Nell'elenco dei servizi attivi "applicazioni di avvio", a cosa corrispondono smbd (samba) e nmbd? Io ho pensato che samba corrispondesse a "condivisione files personali" ed nmbd lo ignoro del tutto.

Grazie fletcher

Subject: Re: settare porte su linux mint
Posted by Giuseppe Della Bianca on Tue, 16 Aug 2011 15:28:35 GMT
View Forum Message <> Reply to Message

fletcher wrote:

> Il 16/08/2011 16:22, Giuseppe Della Bianca ha scritto:
>> Alessandro Selli wrote:
>>
>>> fletcher ha scritto:
>>>> Salve a tutti,
>>>> ho da pochi giorni installato linux mint e dopo aver scansionato le
>>>> porte da strumenti di rete, mi appaiono aperte la 139 (netbios) e la
>>>> 445 (microsoft-ds),
>>>
>>> Puoi vedere con netstat quali processi hanno aperto quelle porte in
>>> ascolto.
>>>
>>>
>>> Ciao,
>>>
>>>
>>
>> samba?
>>
>> smbd e nmbd probabilmente.

>
>
> Grazie per le risposte,
> interrogando netstat mi dÃ i serzi attivi seguenti :
>
]zac[

Controlla meglio, per esempio con

netstat -ap o -anp

per esempio:

netstat -anp | grep '139\|445'

```
tcp        0      0 :::139                  :::*
LISTEN      3371/smbd
tcp        0      0 :::445                  :::*
LISTEN      3371/smbd
.....
```

Subject: Re: settare porte su linux mint
Posted by Giuseppe Della Bianca on Tue, 16 Aug 2011 15:37:38 GMT
View Forum Message <> Reply to Message

fletcher wrote:

]zac[
> se la porta 631 la mantiene aperta "applet coda di stampa", il servizio
> nella mia macchina non Ã¨ giÃ attivo e se la 445 la mantiene aperta il
> servizio di "condivisione di files personali" anche questo servizio non
> Ã¨ attivo.Nell'elenco dei servizi attivi "applicazioni di avvio", a cosa
> corrispondono smbd (samba) e nmbd? Io ho pensato che samba
> corrispondesse a "condivisione files personali" ed nmbd lo ignoro del
> tutto.
>
> Grazie fletcher

Ci sono un sacco di servizi che partono prima e anche se il server grafico
(X server) il desktop manager (la parte grafica che usi) non parte.

Poi ci sono le applicazioni di avvio/servizi del sistema grafico.

Dovresti avere un qualche tool con nome configura servizi o simile sotto
amministrazione, impostazioni, o altra roba simile.

Comunque normalmente non sono servizi che creano problemi anche perchÃ© di solito sono accessibili sono dal sistema su cui girano.

In /etc/services (/etc = configurazioni di sistema) c'e' una breve descrizione, via google sono accessibile delle descrizione estese.

Subject: Re: settare porte su linux mint
Posted by fletcher on Tue, 16 Aug 2011 16:24:18 GMT
View Forum Message <> Reply to Message

Il 16/08/2011 17:28, Giuseppe Della Bianca ha scritto:
> netstat -anp | grep '139\|445'

Dal responso del suddetto comando ti estraggo i dati che penso siano i piÃ¹ salienti:

tcp6 0 0 :::139 :::*
LISTEN -
tcp6 0 0 :::445 :::*
LISTEN -

per cui da una ricerca su google, la risposta non potrebbe essere questa del link anche se il quesito partiva da una macchina uso server?

http://forum.ubuntu-it.org/index.php?topic=134333.0

che ne dici?

Grazie anche per le delucidazioni che mi hai dato nel messaggio successivo. Se risolvo Vi farÃ² sapere.
Ciao fletcher

Subject: Re: settare porte su linux mint
Posted by Alessandro Selli on Tue, 16 Aug 2011 22:15:19 GMT
View Forum Message <> Reply to Message

fletcher ha scritto:
> Il 16/08/2011 17:28, Giuseppe Della Bianca ha scritto:
>> netstat -anp | grep '139\|445'
>
> Dal responso del suddetto comando ti estraggo i dati che penso siano i
> piÃ¹ salienti:
>
> tcp6 0 0 :::139 :::* LISTEN -

> tcp6 0 0 :::445 :::* LISTEN -

Sembri aver eseguito il comando da utente non privilegiato: l'ultima colonna non riporta i processi che hanno creato i socket di ascolto.

Anteponi sudo al comando o, se non Ã¨ configurato per farti eseguire netstat con i diritti del superutente, apriti un terminale con una shell di root e ripeti il comando. Samba Ã¨ il sospettato numero uno, comunque, come ha scritto Giuseppe.

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: settare porte su linux mint
Posted by fletcher on Wed, 17 Aug 2011 06:44:39 GMT
View Forum Message <> Reply to Message

Il 17/08/2011 00:15, Alessandro Selli ha scritto:

> Sembri aver eseguito il comando da utente non privilegiato: l'ultima
> colonna non riporta i processi che hanno creato i socket di ascolto.
>
> Anteponi sudo al comando o, se non Ã¨ configurato per farti eseguire
> netstat con i diritti del superutente, apriti un terminale con una shell
> di root e ripeti il comando. Samba Ã¨ il sospettato numero uno,
> comunque, come ha scritto Giuseppe.
>
>
> Ciao,
>
>

Il responso di sudo netstat -anp | grep '139\|445 Ã¨ il seguente

tcp6 0 0 :::139 :::*
LISTEN 984/smbd
tcp6 0 0 :::445 :::*
LISTEN 984/smbd
unix 3 [ ] STREAM CONNECTED 20139 2802/gconfd-2

unix 3 [ ] STREAM CONNECTED 8445
850/dbus-daemon /var/run/dbus/system_bus_socket

da inesperto di informatica avevo sospettato che potesse dipendere
dall'ipv6, in effetti Ã¨ samba che mantiene aperte le suddette porte,
quindi come devo proseguire?
Grazie fletcher

Subject: Re: settare porte su linux mint
Posted by fletcher on Wed, 17 Aug 2011 13:16:44 GMT
View Forum Message <> Reply to Message

Il 17/08/2011 08:44, fletcher ha scritto:
> Il 17/08/2011 00:15, Alessandro Selli ha scritto:
>
>> Sembri aver eseguito il comando da utente non privilegiato: l'ultima
>> colonna non riporta i processi che hanno creato i socket di ascolto.
>>
>> Anteponi sudo al comando o, se non Ã¨ configurato per farti eseguire
>> netstat con i diritti del superutente, apriti un terminale con una shell
>> di root e ripeti il comando. Samba Ã¨ il sospettato numero uno,
>> comunque, come ha scritto Giuseppe.
>>
>>
>> Ciao,
>>
>>

E dopo aver rimosso Samba dal gestore dei pacchetti, ho digitato:

sudo netstat -anp | grep '139\|445' e mi dÃ

unix 3 [ ] STREAM CONNECTED 13997 2330/cat

unix 3 [ ] STREAM CONNECTED 13996 2268/python

unix 3 [ ] STREAM CONNECTED 11392 670/X
@/tmp/.X11-unix/X0
unix 3 [ ] STREAM CONNECTED 11391
634/gdm-simple-slav

in cui il 139 Ã¨ evidenziato in rosso, come si deve interpretare?

Ciao fletcher

Subject: Re: settare porte su linux mint
Posted by Giuseppe Della Bianca on Wed, 17 Aug 2011 14:59:22 GMT

fletcher wrote:

]zac[
> E dopo aver rimosso Samba dal gestore dei pacchetti, ho digitato:
>
> sudo netstat -anp | grep '139\|445' e mi dÃ
>
> unix 3   [ ]   STREAM   CONNECTED   13997   2330/cat
>
> unix 3   [ ]   STREAM   CONNECTED   13996   2268/python
>
> unix 3   [ ]   STREAM   CONNECTED   11392   670/X
>   @/tmp/.X11-unix/X0
> unix 3   [ ]   STREAM   CONNECTED   11391
> 634/gdm-simple-slav
>
> in cui il 139 Ã¨ evidenziato in rosso, come si deve interpretare?
>
> Ciao fletcher

ehmm ... credo che ti convenga leggere qualche how-to tipo linux da zero, da windows a linux, ecc. .

In linux i comandi testuali possono passare il testo visualizzato ad un altro comando che lo elabora.

Quindi netstat passa la visualizzazione a grep, e grep visualizza solo le righe che contengono il testo 139 0 445.

La parte in rosso e' quella parte che combacia con testo voluto, e quelle righe sono relative ad altre cose.

Potevi ottenere la stessa cosa manualmente ' netstat -an | less ' scorrendo il testo e cercando la parte che interessa (q (quit) per uscire).

Subject: Re: settare porte su linux mint
Posted by Giuseppe Della Bianca on Wed, 17 Aug 2011 15:06:22 GMT

fletcher wrote:

]zac[
>

> che ne dici?
>
> Grazie anche per le delucidazioni che mi hai dato nel messaggio
> successivo. Se risolvo Vi farÃ² sapere.
> Ciao fletcher

Che dovresti prima documentarti un po' su linux, anche solo come informazioni generiche senza dover per forza capire tutti i dettagli.

In linux non c'e' una netta distinzione tra sistema operativo server, desktop, ecc., e' solo questione di installare rimuovere, configurare i vari pacchetti.

In ogni caso anche se lasciavi samba non avevi problemi.

Volendo potevi semplicemente disabilitare il servizio invece di rimuovere il pacchetto.

Subject: Re: settare porte su linux mint
Posted by fletcher on Wed, 17 Aug 2011 17:43:52 GMT
View Forum Message <> Reply to Message

Il 17/08/2011 17:06, Giuseppe Della Bianca ha scritto:
> fletcher wrote:
>
>]zac[
>>
>> che ne dici?
>>
>> Grazie anche per le delucidazioni che mi hai dato nel messaggio
>> successivo. Se risolvo Vi farÃ² sapere.
>> Ciao fletcher
>

> Che dovresti prima documentarti un po' su linux, anche solo come
> informazioni generiche senza dover per forza capire tutti i dettagli.
>

Hai perfettamente ragione, cito dei link per chi, come me, ha lacune in materia

http://lug.42019.it/index.php/Script_e_comandi_utili
http://www.mimante.net/doc/comandi.txt

> In linux non c'e' una netta distinzione tra sistema operativo server,
> desktop, ecc., e' solo questione di installare rimuovere, configurare i vari
> pacchetti.
>
>
> In ogni caso anche se lasciavi samba non avevi problemi.
>
> Volendo potevi semplicemente disabilitare il servizio invece di rimuovere il
> pacchetto.

Ho usato anche Opensuse, in quella distro c'Ã¨ il tool editor dei
runlevel che ti permette di disabilitare i servizi inutili, ma non ho
trovato qualcosa di simile su Mint a parte le applicazioni d'avvio.
DovrÃ² impararmi, grazie ai comandi da console, a risolvere i problemi
senza ricorrere sempre ai tool grafici.

Grazie mille fletcher

Subject: Re: settare porte su linux mint
Posted by Giuseppe Della Bianca on Thu, 18 Aug 2011 15:18:18 GMT
View Forum Message <> Reply to Message

fletcher wrote:

]zac[
> Ho usato anche Opensuse, in quella distro c'Ã¨ il tool editor dei
> runlevel che ti permette di disabilitare i servizi inutili, ma non ho
> trovato qualcosa di simile su Mint a parte le applicazioni d'avvio.
> DovrÃ² impararmi, grazie ai comandi da console, a risolvere i problemi
> senza ricorrere sempre ai tool grafici.
>

E' utile anche come emergenza, come base comune per chiedere e discutere con
altri che magari usano altre distribuzioni.

Altrimenti per distribuzioni particolari e non diffusissime conviene
utilizzare la documentazione del loro sito e i loro forum.

Poi e' utile saper cercare con google tipo mint + linux + disable + service
+ console .

P.S.

chkconfig --list smb

chkconfig smb off

chkconfig smb on

> Grazie mille fletcher

Prego, di niente.
