

Re: pptp mppe as other than root?

Source: <http://linux.derkeiler.com/Newsgroups/comp.os.linux.networking/2004-09/0648.html>

From: stephen (*stephen_at_aloss.net*)

Date: 09/18/04

Date: Sat, 18 Sep 2004 03:57:31 GMT

On Fri, 17 Sep 2004 06:55:59 +0000, Tauno Voipio wrote:

Thanks, Tauno. I've filled in below:

> *stephen wrote:*

>> *Finally! after much dickering around, swatting, and so on, I've managed to connect to my employer's windows vpn and access my work files. But I have to do it as root.*

>>

>> *I don't like that. I work for a software shop and there are some very smart people (yes there are some smart windows geeks) with idle evenings who love to poke around. As the first linux user in our company to do this, I'm going to be a target. I prefer that if someone pokes into my box that they poke into some place that does not have root access to the rest of my life. They can poke into my work stuff – fine! They know it all anyway since it's all in the abysmal VSS. But I want to be fairly sure that they'll get 'access denied' to any other area of my personal life.*

>>

>> *Ideally I could put all the vpn components under a group that does not have access.*

>>

>> *Can I do that? I've looked through the docs at <http://pptpclient.sourceforge.net/> and I've googled my fingers sore, but all I see is stuff like "Solution: you have to be root".*

>>

>> *Say it isn't so or say that I'm just being silly and that I'm in some magically way protected from intrusions.*

>>

>

> *There are too little details to give meaningful advice.*

>

> *Please describe the connection and printouts from:*

>

> *ifconfig -a*

eth0 Link encap:Ethernet HWaddr xxx

inet addr:192.168.0.101 Bcast:192.168.0.255 Mask:255.255.255.0

UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1

comp.os.linux.networking: Re: pptp mppe as other than root?

RX packets:1491 errors:0 dropped:0 overruns:0 frame:0
TX packets:371 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:549984 (537.0 Kb) TX bytes:33929 (33.1 Kb)
Interrupt:10 Base address:0x4000

lo Link encap:Local Loopback

inet addr:127.0.0.1 Mask:255.0.0.0
UP LOOPBACK RUNNING MTU:16436 Metric:1
RX packets:2356 errors:0 dropped:0 overruns:0 frame:0
TX packets:2356 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:0
RX bytes:1794391 (1.7 Mb) TX bytes:1794391 (1.7 Mb)

ppp0 Link encap:Point-to-Point Protocol

inet addr:10.12.1.57 P-t-P:10.12.1.50 Mask:255.255.255.255
UP POINTOPOINT RUNNING NOARP MULTICAST MTU:1496 Metric:1
RX packets:9 errors:0 dropped:0 overruns:0 frame:0
TX packets:9 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:3
RX bytes:114 (114.0 b) TX bytes:126 (126.0 b)

> route -n

Kernel IP routing table

Destination	Gateway	Genmask	Flags	Metric	Ref	Use	Iface
10.12.1.50	0.0.0.0	255.255.255.255	UH	0	0	0	ppp0
192.168.0.0	0.0.0.0	255.255.255.0	U	0	0	0	eth0
169.254.0.0	0.0.0.0	255.255.0.0	U	0	0	0	eth0
10.12.0.0	0.0.0.0	255.255.0.0	U	0	0	0	ppp0
127.0.0.0	0.0.0.0	255.0.0.0	U	0	0	0	lo
0.0.0.0	192.168.0.1	0.0.0.0	UG	0	0	0	eth0

>

> taken when the tunnel is up. If you like, you can
> obscure the top part of public IP addresses. If the
> internal networks use RFC 1918 addresses (10.x.y.z,
> 172.16.x.y-172.31.x.y, 192.168.x.y), please do not
> obscure them.

>

> Do you use Samba to access the Windows files?

Yes:

```
# Samba config file created using SWAT
# from 127.0.0.1 (127.0.0.1)
# Date: 2004/09/15 18:29:08
```

```
# Global parameters
```

```
[global]
```

```
workgroup = #HIDING COMPANY NAME
log file = /var/log/samba/%m.log
```

Re: pptp mppe as other than root?

comp.os.linux.networking: Re: pptp mppe as other than root?

```
max log size = 50
socket options = TCP_NODELAY SO_RCVBUF=8192 SO_SNDBUF=8192
domain logons = Yes
dns proxy = No
wins server = 10.12.0.11
```

[printers]

```
comment = All Printers
path = /var/spool/samba
printable = Yes
browseable = No
```

- >
- > *The VPN is just a network connection. In Linux, building*
- > *and ripping network connections is considered to be such*
- > *tasks that they should be limited to root only. This does*
- > *not mean that the connections should be used as root only.*
- > *This means that the tunnel should be started as root and*
- > *log in as a normal user for using the tunnel.*

My current configuration requires me to mount as root.

ls -l /dev | grep ppp shows all listings like this:

```
crw----- 1 root root 45, 128 Sep 15 2003 ippp0
```

This crw is new to me!

- >
- > *There are plenty of different ways to build a VPN*

So I have discovered! But only one that works so far.

- > *tunnel, so details are also needed here (PPTP?).*

PPTP with MPPE

- >
- > *You should be able to armour your system against intrusions*
- > *from the company network in the same way as it has to be*
- > *done for Internet connections. You do have a firewall in*
- > *place, do you?*

My iptables are out-of-the-box Fedora Core 1. When I was experimenting I found that iptables on or off made no difference to the VPN connection. So the current configuration probably offers no protection. I have of course done some research into iptables, but don't understand them well enough to feel secure in this situation. I am working through a stack of books and enjoying it, but right now I'd like to meet my employment obligations without reinstalling windows.

Re: pptp mppe as other than root?

comp.os.linux.networking: Re: pptp mppe as other than root?

>
> *There are reports that the average break-in time to an
> unprotected WinXP computer is 20 minutes, if the computer
> is connected to a broadband connection. We have practical
> experience – a freshly installed Windows 2000 workstation
> was broken in before it had time to get all the Microsoft
> patches needed to protect it (pretty near the reported
> average time: 17 minutes).*

Given an opportune moment, I suspect that a knowledgeable intruder could make root on my vpn-ed linux box in five minutes or less.

I know I have a lot to learn, and I am eager to learn that lot.

Thanks for your help.

>
> *HTH*
>
> *Tauno Voipio*
> *tauno voipio (at) iki fi*
>
> *protect against the intruders.*