

Forum:[Hack Forums](#)

Thread: [Mount with Extended Attribute.](#)

pwntoken - February 11, 2015, 6:13 pm

How do I mount ReiserFS filesystem with extended attributes?

I have this:

Code Linux gh0st 2.6.31-14-generic-pae #48-Ubuntu SMP Fri Oct 16 15:22:42 UTC 2009 i686 GNU/Linux

I need to mount the /apachelogs/ directory with such extended attributes. There are obvious reasons which are for test purposes

Code <http://www.exploit-db.com/exploits/12130/>
Here is what I get via using

Code mount

Code /dev/mapper/ghost-root on / type ext4 (rw,errors=remount-ro)

proc on /proc type proc (rw)

none on /sys type sysfs (rw,noexec,nosuid,nodev)

none on /sys/fs/fuse/connections type fusectl (rw)

none on /sys/kernel/debug type debugfs (rw)

none on /sys/kernel/security type securityfs (rw)

udev on /dev type tmpfs (rw,mode=0755)

none on /dev/pts type devpts (rw,noexec,nosuid,gid=5,mode=0620)

none on /dev/shm type tmpfs (rw,nosuid,nodev)

none on /var/run type tmpfs (rw,nosuid,mode=0755)

none on /var/lock type tmpfs (rw,noexec,nosuid,nodev)

none on /lib/init/rw type tmpfs (rw,nosuid,mode=0755)

/dev/sdc1 on /tmp type ext2 (rw,noexec,nosuid)

/dev/sda5 on /boot type ext2 (rw)

Could someone explain me the logic behind this?

Betty Blue - February 11, 2015, 6:18 pm

PHP Code

```
<?php
```

```
mount -t reiserfs
```

What do you mean extended attributes? Read/write access?

Code /dev/mapper/ghost-rootChances are this is already mounted. I don't really understand the output of what you are giving. What command was run? What arguments? I can't really tell by the examples you have given.

pwntoken - February 11, 2015, 6:35 pm

(Feb 11, 2015 07:18 PM)Matthew Shultz Wrote: [\[CITE\]](#) PHP Code

```
<?php
```

```
mount -t reiserfs
```

What do you mean extended attributes? Read/write access?

Code /dev/mapper/ghost-rootChances are this is already mounted. I don't really understand the output of what you are giving. What command was run? What arguments? I can't really tell by the

examples you have given.

The command which I ran was:

Code mount

It gave me the output sample you just saw. Now, I have to enumerate which one particularly is ReiserFS? and yes, by EA i mean, r/w access.

Betty Blue - February 11, 2015, 8:31 pm

(Feb 11, 2015 07:35 PM)pwntoken Wrote: [\[CITE\]](#) The command which I ran was:

Code mount

It gave me the output sample you just saw. Now, I have to enumerate which one particularly is ReiserFS? and yes, by EA i mean, r/w access. Still don't quite understand.

You're trying to find, with that output, which one is the ReiserFS?

If that is what you mean, try using

PHP Code

```
<?php
```

```
mount -l
```

And piping the output to grep with a query.

Benign - February 12, 2015, 5:32 am

I don't see any reiserfs file systems mounted on your system.

Have you got a device on which to build your reiserfs filesystem?

If so, and you have already partitioned and built it, then just mount it to the apache logs mount point with:

```
mount -t reiserfs /device/with/reiserfs /apache/logs/
```

It will mount it rw by default.

pwntoken - February 12, 2015, 12:11 pm

(Feb 12, 2015 06:32 AM)Benign Wrote: [\[CITE\]](#) I don't see any reiserfs file systems mounted on your system.

Have you got a device on which to build your reiserfs filesystem?

If so, and you have already partitioned and built it, then just mount it to the apache logs mount point with:

```
mount -t reiserfs /device/with/reiserfs /apache/logs/
```

It will mount it rw by default.

and how about enumerating the device (in-case I had no idea what device was created in the first place since it's a remote server and we were given to break into the box as per exam rules for penetration testing).

Now since, I do not know which device was created which had the mount point and if it was ReiserFS, how do I go about enumerating these? so that I could complete my assignment of exploiting the ReiserFS with an exploit which requires a ReiserFS to be mounted first. The Linux kernel version used is exactly the same which the exploit was written for. Only that there are no immediate ReiserFS

FS I can see from.

Code mount -l

according to another user who replied in this thread. ?

Betty Blue - February 12, 2015, 12:13 pm

(Feb 12, 2015 01:11 PM)pwntoken Wrote: [\[CITE\]](#) and how about enumerating the device (in-case I had no idea what device was created in the first place since it's a remote server and we were given to break into the box as per exam rules for penetration testing).

Now since, I do not know which device was created which had the mount point and if it was ReiserFS, how do I go about enumerating these? so that I could complete my assignment of exploiting the ReiserFS with an exploit which requires a ReiserFS to be mounted first. The Linux kernel version used is exactly the same which the exploit was written for. Only that there are no immediate ReiserFS I can see from.

Code mount -l

according to another user who replied in this thread. ?

PHP Code

<?php

mount -l

I as in love.

not 1 as in one.

All this does is list mounted devices and their FS types.

MoonCakeRuler - February 12, 2015, 6:59 pm

(Feb 11, 2015 07:13 PM)pwntoken Wrote: [\[CITE\]](#) How do I mount ReiserFS filesystem with extended attributes?

There's actually a mini-section about this on Hardened Linux From Scratch. Finally some use out of reading it. XD

But yeah, here's how you mount it. First, open your /etc/fstab file and add user_xattr to your file system's entry. For example, let's say /dev/sda5 is your ReiserFS partition. Your line may look like this:

Code /dev/sda5 /directory/to/mount/on reiserfs defaults,user_xattr 0 2 You can then simply mount the file system as usual. If it was already mounted, you'll need to remount it.

I'm actually pretty sure that's how it's supposed to be done in your case as well. I checked the exploitdb script you linked to. If you check lines 54 through 60, you'll notice that the script is reading /etc/fstab and looking for the user_xattr option in that line.

I don't understand which filesystem you want to mount though. /dev/mapper/ghost-root seems to be ext4 already. And I'm not sure about /apachelogs. But hopefully you'll get the idea. If not, maybe someone can help once you provide some additional details.

EDIT: Since you're working with extended attributes, you should read [this man page](#). While you're at it, you can also check out setfattr and getfattr, which let you set and read the name=value pair attributes.

pwntoken - February 12, 2015, 7:08 pm

(Feb 12, 2015 07:59 PM)MoonCakeRuler Wrote: [\[CITE\]](#) There's actually a mini-section about this on Hardened Linux From Scratch. Finally some use out of reading it. XD

But yeah, here's how you mount it. First, open your `/etc/fstab` file and add `user_xattr` to your file system's entry. For example, let's say `/dev/sda5` is your ReiserFS partition. Your line may look like this:

Code `/dev/sda5 /directory/to/mount/on reiserfs defaults,user_xattr 0 2` You can then simply mount the file system as usual. If it was already mounted, you'll need to remount it.

I'm actually pretty sure that's how it's supposed to be done in your case as well. I checked the `exploitdb` script you linked to. If you check lines 54 through 60, you'll notice that the script is reading `/etc/fstab` and looking for the `user_xattr` option in that line.

I don't understand which filesystem you want to mount though. `/dev/mapper/ghost-root` seems to be `ext4` already. And I'm not sure about `/apachelogs`. But hopefully you'll get the idea. If not, maybe someone can help once you provide some additional details.

Okay if:

Code `/dev/mapper/ghost-root`

If `ext4`, is there any way possible I convert the `ext4` to Reiserfs as you have given the procedure and then mount the `/dev/mapper/ghost-root` instead?

MoonCakeRuler - February 12, 2015, 7:32 pm

(Feb 12, 2015 08:08 PM)pwntoken Wrote: [\[CITE\]](#) Okay if:

Code `/dev/mapper/ghost-root`

If `ext4`, is there any way possible I convert the `ext4` to Reiserfs as you have given the procedure and then mount the `/dev/mapper/ghost-root` instead?

That may not be possible. I don't think there is a simple way to convert it, other than to you know, back up your stuff, boot into a live medium, re-format your filesystem to reiserfs and then retrieve your files. However, that is extremely messy, dangerous and I'm not sure if you can attempt that on your assignment.

In your original post you say that you want to mount `/apachelogs`? Can you provide details about it? Do you want to mount `/apachelogs` on a ReiserFS instead?

pwntoken - February 12, 2015, 9:23 pm

(Feb 12, 2015 08:32 PM)MoonCakeRuler Wrote: [\[CITE\]](#) That may not be possible. I don't think there is a simple way to convert it, other than to you know, back up your stuff, boot into a live medium, re-format your filesystem to reiserfs and then retrieve your files. However, that is extremely messy, dangerous and I'm not sure if you can attempt that on your assignment.

In your original post you say that you want to mount `/apachelogs`? Can you provide details about it? Do you want to mount `/apachelogs` on a ReiserFS instead?

no. It has been done. Thanks a ton to you. However, I made certain changes to the exploit you saw in the original code. I mounted the ReiserFS, but now, the python exploit code which I have modified says:

Code File "root.py", line 38

```
if ret != 0
```

```
^
```

SyntaxError: invalid syntax

Here is the code:

<http://pastebin.com/raw.php?i=1raFye0A>

MoonCakeRuler - February 12, 2015, 9:54 pm

(Feb 12, 2015 10:23 PM)pwntoken Wrote: [\[CITE\]](#) no. It has been done. Thanks a ton to you. However, I made certain changes to the exploit you saw in the original code. I mouted the ReiferFS, but now, the python exploit code which I have modified says:

Code File "root.py", line 38

```
if ret != 0
^
```

SyntaxError: invalid syntax

Here is the code:

<http://pastebin.com/raw.php?i=1raFye0A>

That's a rather simple error. :3 You forgot the colon at the end of the if statement. Your if statement should look like this:

Code if ret != 0:

You've made the same mistake on the next if statement. Also, on the os.system() call to setfattr, you need to save the return integer to a new variable and use that in the if statement or you need to change that line (line 41) to look like this:

Code ret = os.system('setfattr -n "user.hax" -v "hax" /var/log/apache_logs/data/team-edward')

And, don't forget the colons on line 42. Three changes all in all so far unless I missed something.

pwntoken - February 13, 2015, 8:19 pm

(Feb 12, 2015 10:54 PM)MoonCakeRuler Wrote: [\[CITE\]](#) That's a rather simple error. :3 You forgot the colon at the end of the if statement. Your if statement should look like this:

Code if ret != 0:

You've made the same mistake on the next if statement. Also, on the os.system() call to setfattr, you need to save the return integer to a new variable and use that in the if statement or you need to change that line (line 41) to look like this:

Code ret = os.system('setfattr -n "user.hax" -v "hax" /var/log/apache_logs/data/team-edward')

And, don't forget the colons on line 42. Three changes all in all so far unless I missed something.

Hey I changed the entire script and w00t. Thank you and kudos to you sir. Respected for the help.

szrusko - December 1, 2017, 6:04 am

(Feb 13, 2015 09:19 PM)pwntoken Wrote: [\[CITE\]](#) Hey I changed the entire script and w00t. Thank you and kudos to you sir. Respected for the help.

Hy,

Pls help me, how can you mount the ReiferFS? or how can you convert it? or how worked this exploit for you?

Because I have a same problem now :/

Thanks