

Forum:[Hack Forums](#)

Thread: [Determine logged on user on Windows computer from Linux](#)

hack3rcon - November 23, 2016, 8:12 am

Hello.

Can I use "net rpc" command for determine who is logged on Windows? I know Windows has a nice tools with the name "Psloggedon.exe" but can Linux has some kind of tools like it?

I found "<https://nmap.org/nsedoc/scripts/smb-enum-users.html>" but not worked :(

Thank you.

kiasa - November 23, 2016, 5:58 pm

There are many techniques to fingerprinting, but none that I am aware of using...

So you'll probably be better off searching google for OS fingerprinting techniques.

hack3rcon - November 24, 2016, 1:24 am

(Nov 23, 2016 06:58 PM)kiasa Wrote: [\[CITE\]](#) There are many techniques to fingerprinting, but none that I am aware of using...

So you'll probably be better off searching google for OS fingerprinting techniques.

OS fingerprinting is not my goal, I like to find who is login via linux.

SuckySucky - November 25, 2016, 7:19 am

Yes it is possible using SAMBA.

<https://www.samba.org/samba/docs/man/Samba-HOWTO-Collection/NetCommand.html#id2599400>

hack3rcon - November 25, 2016, 10:53 pm

(Nov 25, 2016 08:19 AM)SuckySucky Wrote: [\[CITE\]](#) Yes it is possible using SAMBA.

<https://www.samba.org/samba/docs/man/Samba-HOWTO-Collection/NetCommand.html#id2599400>

Can you tell me the correct syntax if IP is 192.168.72.1 ?

Fladrif - November 28, 2016, 3:19 am

The following MSF module is your friend:

https://www.rapid7.com/db/modules/auxiliary/scanner/smb/smb_enumusers_domain

Also, if you have a meterpreter:

https://www.rapid7.com/db/modules/post/windows/gather/enum_logged_on_users

And if you have SMB creds then: rpcclient ?U <username> 192.168.72.1

Then use enumdomusers / lookupnames / queryuser commands at the rpcclient command line.

datguy.dev - November 29, 2016, 3:36 pm

They have Powershell for Linux now. (<https://github.com/PowerShell/PowerShell>) I haven't tried it yet, so I'm not sure how limited it is. But you might be able to use Psloggedon.exe that way. Outside of Samba, you may be able to do some packet sniffing or what have you of the HomeGroup

protocol. If you send the right request, it may shoot back a response to whether.... ([https://winprotocoldoc.blob.core.windows.net/productionwindowsarchives/MS-HGRP/\[MS-HGRP\].pdf](https://winprotocoldoc.blob.core.windows.net/productionwindowsarchives/MS-HGRP/[MS-HGRP].pdf)) I don't know, just a brain fart.

hack3rcon - November 30, 2016, 9:24 am

(Nov 29, 2016 04:36 PM)datguy.dev Wrote: [\[CITE\]](#) They have Powershell for Linux now. (<https://github.com/PowerShell/PowerShell>) I haven't tried it yet, so I'm not sure how limited it is. But you might be able to use Psloggedon.exe that way. Outside of Samba, you may be able to do some packet sniffing or what have you of the HomeGroup protocol. If you send the right request, it may shoot back a response to whether.... ([https://winprotocoldoc.blob.core.windows.net/productionwindowsarchives/MS-HGRP/\[MS-HGRP\].pdf](https://winprotocoldoc.blob.core.windows.net/productionwindowsarchives/MS-HGRP/[MS-HGRP].pdf)) I don't know, just a brain fart. Ah, PowerShell has "PsTools"?

datguy.dev - November 30, 2016, 3:46 pm

(Nov 30, 2016 10:24 AM)hack3rcon Wrote: [\[CITE\]](#) Ah, PowerShell has "PsTools"?
The only PSTools I know of are Windows binaries. I don't know what kind of luck you'd have running them under Wine with the Linux PS package installed. That might be worth trying.

But my main point was psloggedon.exe essentially just uses the "net session" command. You could write your own PowerShell script. ->
<https://blogs.technet.microsoft.com/heyscriptingguy/2011/06/04/use-powershell-to-find-logon-session/>