Corelan Team

:: Knowledge is not an object, it's a flow ::

Free tool : Find out where your AD Users are logged on into

Corelan Team (corelanc0d3r) · Sunday, July 12th, 2009

Hi,

I decided to release another free utility I wrote a while ago. This small command-line utility can be used to find out where Active Directory users are logged on into, and/or to find out who is logged on on specific machines. This should include local users, users that are logged in via RDP, user accounts that are used to run services and scheduled tasks (only when the task is running at that time). I have not fully tested all scenario's yet, but the first results look quite ok.

You can download the utility from http://www.corelan.be:8800/index.php/my-free-tools/ad-cs/pve-find-ad-user/. You need .Net framework 2.0 on the machine that you are running the tool off, and you also need to have admin access on the computers you are running the utility against.

The tool is compiled on a 32bit system, but it should run fine on 64bit systems as well.

Open a command prompt and start the utility without parameters :

```
----------------------------------------
 PVE Find AD Users
 Peter Van Eeckhoutte
 (c) 2009 - http://www.corelan.be:8800
 Version : x.x.x.x
----------------------------------------

Syntax : pveFindADUser.exe <parameters>

Valid parameters are :
-h
  show help
-u
  check for updates
-v
  show a little bit more info (verbose)
-current ["username"]
  The -current parameters shows the currently logged on user on each PC
  in the domain. If you specify a username (between quotes), then only
  the PC's where that specific user is logged on will be displayed.
  If you don't specify a username, all PC's with logged on users will be
  displayed in the report.
-last ["username"]
  The -last parameters shows the last logged on user on each PC in the domain.
  If you specify a username (between quotes), then only the PC's where that
  user has logged on last time will be shown
  If you don't specify a username, all PC's with the last logged
  on users will be reported.

  In both cases, the username should contain the domain name !
  (DOMAIN\username)

  If you specify DOMAIN\*username* (with 2 asterisks), then
  all users containing the 'username' string will be displayed

-noping
  Do not ping target computer before trying to enumerate user logons
-p <nr of pings>
  If ping is enabled, set number of pings for verifying that host is alive
  If -p is not specified, 2 pings will be sent
-rootpath rootpath
  Where rootpath is written in distinguishedName notation
    Example : OU=Computers,dc=domain,dc=com
-target hostname.domain.com,hostname2.domain.com,hostname3.domain.com
  Optional parameter that allows you to specify the list of hosts
  (fqdn) to run the query against
  Without this -target parameter, queries will be executed against
  all hosts in the current domain
-stopfound
  Stop searching when first match has been found.
  This parameter works only when looking for currently logged on users

Output will be written to console and to a file called report.csv
```

While most options are self-explanatory, I'll go through them anyway :

-h : show help. Not much to say about that.

-u : check if there is an updated version of the utility. You can use this parameter in conjunction with other parameters

-current ["username"] : This parameter can do 2 things. If you only specify -current then the utility will simply get all currently logged on users on all target machines. If you specify a username (*DOMAIN\Username*) then only the computers where this user is logged on, will be displayed. The utility will try to get the current logged on users from the registry first. If that fails, it will try to get the users via WMI. When the users are collected via WMI, you may see the user account that you are using the run the utility as a logged on user. This user may not be logged on interactively, it just may show up because you are connecting to the host via WMI. Just be aware of this.

-last [“username”] : This parameter can do 2 things as well. If you only specify -last then the utility will attempt to get the last logged on user on the target computer. If you specify a username (*DOMAIN\Username*) then only the computers that have this user account as last logon, will be displayed. Note that, depending on your company policy, the last logon username may be hidden and the tool may not be able to get it.

-noping : this option will prevent the tool from performing a ping (well, in fact, by default the tool does 2 pings) before trying to get the user logon information.

-target : this optional parameter allows you to specify the hosts to query. If you don’t specify this -target parameter, then all hosts in the current domain will be queried. If you decide to specify -target, followed with a comma-separated list of hostnames, make sure to use the FQDN of the target hosts.

In its most simple form, you could just run pveadfinduser.exe -current to show all currently logged on users on all machines (computers, servers, domain controllers, ...) in the domain.

The tool will write the output of the queries into a csv file called report.csv. This file will contain the following fields :

computername, username, mode and technique.

Mode can be "current" (for currently logged on users) and "last" (for last logged on users). Technique can be "registry" or "wmi", depending on the technique that was used to gather the information.

This entry was posted
on Sunday, July 12th, 2009 at 7:45 pm and is filed under 001_Security, Active Directory, My Free Tools, Scripts
You can follow any responses to this entry through the Comments (RSS) feed. You can leave a response, or trackback from your own site.