

SecurityFocus Microsoft: RE: Cached Domain Password on Notebook, secure?

## RE: Cached Domain Password on Notebook, secure?

*Source:* <http://www.derkeiler.com/Mailing-Lists/securityfocus/focus-ms/2002-02/0205.html>

---

**From:** Gino Genari ([mail226518@pop.net](mailto:mail226518@pop.net))

**Date:** 02/25/02

From: "Gino Genari" <[mail226518@pop.net](mailto:mail226518@pop.net)>

To: <[Rowan.Smith@csiro.au](mailto:Rowan.Smith@csiro.au)>, <[focus-ms@securityfocus.com](mailto:focus-ms@securityfocus.com)>, <[Daniel.Varga@de.bosch.com](mailto:Daniel.Varga@de.bosch.com)>

Date: Mon, 25 Feb 2002 15:19:03 -0500

What exactly are you trying to protect against? If you are only worried about the domain accounts, that is one thing. If you are trying to protect information on the notebook itself, that is another. If someone lost their notebook, resetting their password on the domain would make cracking their cached password useless.

If you are trying to protect the notebook, utilities like ERD Commander can reset the local administrator password without knowing the previous one.

I have never tried to use EFS to encrypt the entire disk, so can not give you any information on that, or if ERD could still reset the ADMIN password with that setup.

In my opinion, they way to protect both would be to use a tool like Safeboot, that encrypts the entire disk outside of the OS.

If software purchase is out of the question, please excuse my ramblings.

Gino.

-----Original Message-----

From: [Rowan.Smith@csiro.au](mailto:Rowan.Smith@csiro.au) [<mailto:Rowan.Smith@csiro.au>]

Sent: Sunday, February 24, 2002 5:43 PM

To: [focus-ms@securityfocus.com](mailto:focus-ms@securityfocus.com)

Subject: RE: Cached Domain Password on Notebook, secure?

My philosphy is that until someone actually releases a tool to crack the cached passwords then they are reasonably secure as someone is going to have to go through a lot of effort to obtain the password including writing the algorithm to crack it!

Does anyone know of any tools to brute force the "cached" passwords?

I have looked and have failed to find any tools to do this. I also wonder how computationally expensive the generation of the hash verifier is?

RE: Cached Domain Password on Notebook, secure?

SecurityFocus Microsoft: RE: Cached Domain Password on Notebook, secure?

–Rowan

-----Original Message-----

From: Eric [mailto:[ews@tellurian.net](mailto:ews@tellurian.net)]  
Sent: Wednesday, 20 February 2002 5:20 AM  
To: Varga Daniel (QI/RZS4) \*; '[focus-ms@securityfocus.com](mailto:focus-ms@securityfocus.com)'  
Subject: Re: Cached Domain Password on Notebook, secure?

It is not a 'cachedpassword' as the reg key name implies. It is an OWF hash verifier of the password hash – it is not possible to reverse this value to obtain either the LM or NTLM hashes, nor the clear-text password.

At 06:17 PM 2/18/2002 +0100, Varga Daniel (QI/RZS4) \* wrote:

>Hi all,  
>  
>do you know, whether it is possible for an attacker to crack the cached  
>credentials of a domain user on an offline notebook?  
>  
>I tried lsadump2  
([http://razor.bindview.com/tools/desc/lsadump2\\_readme.html](http://razor.bindview.com/tools/desc/lsadump2_readme.html))  
>but cannot judge whether this information is any useful for an attacker to  
>get the cached password of a domain user. Does anyone of you?  
>  
>We plan to roll out EFS to secure our notebooks in case they get lost but  
as  
>I see the security of EFS stands and falls with the security of the  
password  
>of the user.  
>  
>Thanks,  
>--  
>Daniel

- 
- **Previous message:** [Frank Heyne: "RE: Cached Domain Password on Notebook, secure?"](#)
  - **In reply to:** [Rowan.Smith@csiro.au: "RE: Cached Domain Password on Notebook, secure?"](#)
  - **Next in thread:** [Rowan.Smith@csiro.au: "RE: Cached Domain Password on Notebook, secure?"](#)
  - **Messages sorted by:** [\[ date \] \[ thread \] \[ subject \] \[ author \] \[ attachment \]](#)