

## Re: Hacked Workstations

**Source:** <http://www.derkeiler.com/Newsgroups/microsoft.public.win2000.security/2005-02/0672.html>

---

**From:** Herb Martin (*news\_at\_LearnQuick.com*)

**Date:** 02/26/05

Date: Fri, 25 Feb 2005 20:43:30 -0600

"megascout29" <megascout29@discussions.microsoft.com> wrote in message news:04D0F45E-685D-4C8E-8AAC-7B3CA2320DFA@microsoft.com...

- > *It is a private school. The school makes tens of thousands of dollars for every student that attends. So unless a student is causing the school to lose*
- > *money (causing tens of thousands of dollars in damage would make them unprofitable for the school, but that kind of damage is unlikely) then there*
- > *is no way in hell that they will kick them out.*
- >
- > *These students are not very smart. A few skript kiddiots showed everyone else the few tricks mentioned to get the local admin password. So I was thinking that maybe if I could somehow encrypt the System32 folder using EFS*
- > *or something then they at least wouldn't be able to boot off a Linux CD and*
- > *delete the SAM as the wouldn't be able to find the SAM on the encrypted drive.*
- >
- > *Would that even work though? I don't know much about EFS.*

All NT-type security (with very few exceptions) require PHYSICAL security of the machines.

If you give them the ability to boot the machine then all bets are off.

EFS can protect data files (and even some exe etc.) but it cannot protect many/most system files since they must be readable immediately.

They would ALWAYS be able to "Find" the SAM since EFS protects ONLY files (not the directory structure.)

[Despite common misperception and even the way the prompts in the tools are worded there are no

microsoft.public.win2000.security: Re: Hacked Workstations

"encrypted directories" -- encrypting directories  
means setting the defaults for files created there.]

```
--
Herb Martin
>
> >"Dave" wrote:
>
> >
> > "megascout29" <megascout29@discussions.microsoft.com> wrote in message
> > news:A5453D39-5A91-4868-B22C-BDD540806F12@microsoft.com...
> > > I work at a school where students have been booting off Linux CDs and
> > > deleting the SAM and booting off NT password reset floppies to delete
the
> > > admin password.
> > >
> > > For reasons beyond my control we have to give the students the ability
to
> > > boot off of floppies and CDs.
> > >
> > > My question is how can we stop this from happening?
> >
> > you have a couple options.  the hardest one to get implimented is to
> > discipline anyone caught bypassing security... kick a few of them out of
> > school and maybe the others will get the idea.  or you could live with
the
> > fact that its going to happen and make sure that you have a quick way to
> > restore the proper image to a hacked machine.  maybe even boot from a
> > network instead of the local hard drive.  if you go this way you also
> > probably want to segregate the student machines so they don't have
access to
> > anything important.  basically if you are in a situation where you can't
> > control physical access to the machines you can't stop anyone from doing
> > basically anything they want.
> >
> >
> >
> >
```