Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Security Essentials: Network, Endpoint, and Cloud (Security 401)"
at http://www.giac.org/registration/gsec

GSEC Practical Assignment
Version 1.4b Option 2
Case Study

© SANS Institute 2004, Author retains full rights.

By
Bruno Lanthier

Security Measure in a K12 Public School environment
February 6 2004

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Introduction:

We are a French public school board with 34 schools offering elementary, secondary and adult education. We cover a territory of over 37 000 km² and we have around 10 000 students. Each school has a connection to the wan network. All schools are connecting to the main office to share internet resources.

School environment offer a great challenge in the security point of view. We need to cover a lot of aspects and provide a lot of services. Kids are curious and some of them take network as a playground without thinking as to the impact of their action. We also need to give secure access to internet and some applications.

Security is a large and never ending process that evolves with technology. In this paper I will cover some of the issues we had and how we assess them at this point. I will talk about securing a web access (outgoing), securing network segments and securing school labs. My intent in that paper is to demonstrate what kind of security needs we have, how we address them and what solutions are best for us.

Securing Web access:

We need to provide a secure access to the internet for the kids. The need here is giving them access to internet contents and protecting them from inappropriate sites. These sites are sites without educational purposes or sites with illegal/offensive contents. Failure to do that can cause damage to the reputation of the school board and bad publicity.

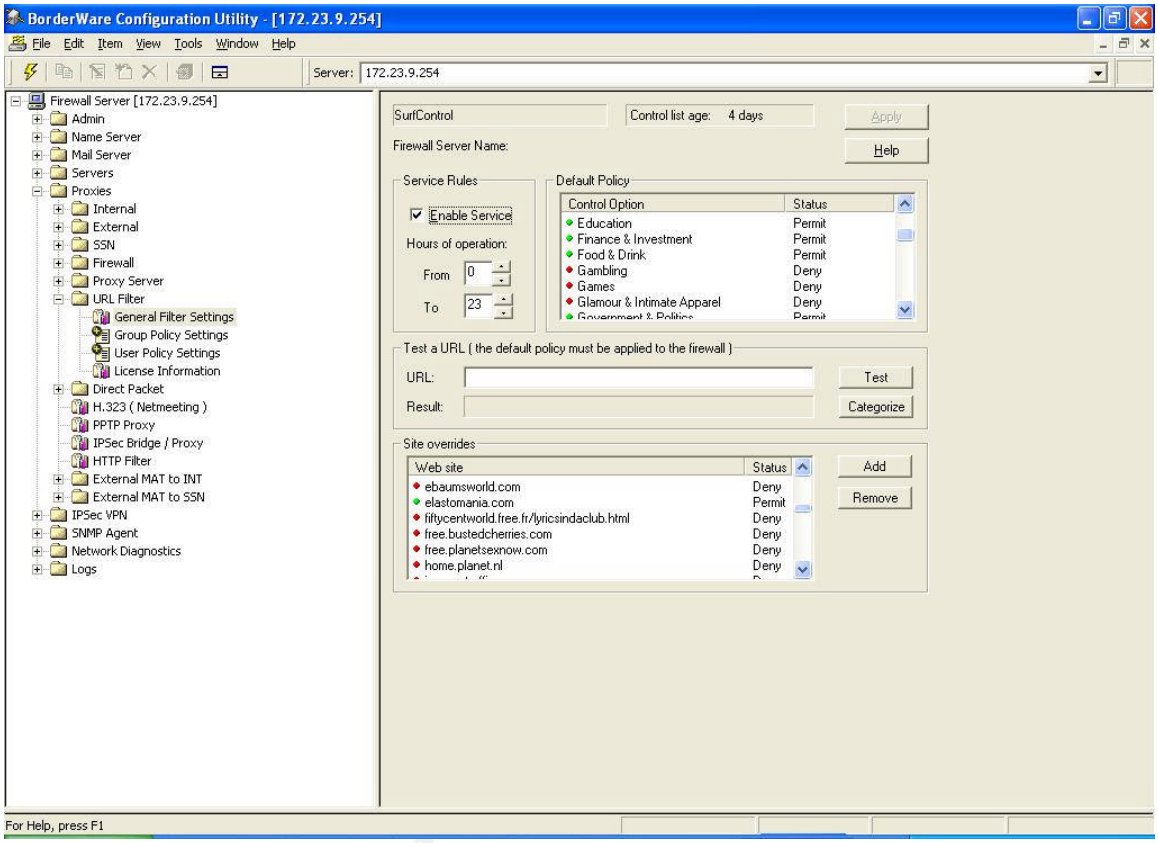
The list of sites that must be available is so big, that it was impossible to use a solution like entering in the firewalls some rules to allow only the good sites to be reached. Also the needs are changing, so we had to find a dynamic solution. We then thought about a URL filter.

Then the question was which one to choose. The final choice was Surfcontrol[1] because our firewall has the surfcontol feature embedded. We then only have to buy the license saving us money because we don't have to setup another box. The surfcontrol list is flexible and regularly updated in an automated way. We also have the possibility to choose what kind of content is blocked with a list of categories. There is a possibility to still override the setting for some sites in those categories. Let say in example that we decided to block the games group, but a teacher made a request to keep one site accessible for a reward to kids that have been working well, then we can do that easily.

[1] Http://www.surfcontrol.com

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Since the firewall (Borderware[2]) have the surf control embedded, it's easy to manage and keep an eye on it. Also the interface is pretty simple as you can see in the following screen capture.



We also have the possibility directly from that screen, to test if a site is permitted or denied. So far, the filters are doing a good job. We have very few reports of inappropriate surfing.

Securing network segment:

In our security evaluation process, we identify vulnerability in our network design. Since we didn't have any limitations on the wan usage, if a school was compromised by an attacker or even a spreading virus, there were no boundaries to protect the other schools. Each school is connected to the wan cloud by its own connection. The only advantage we had is the fact that a school can't connect directly to another one without passing through the main office.

[2]Http://www.borderware.com

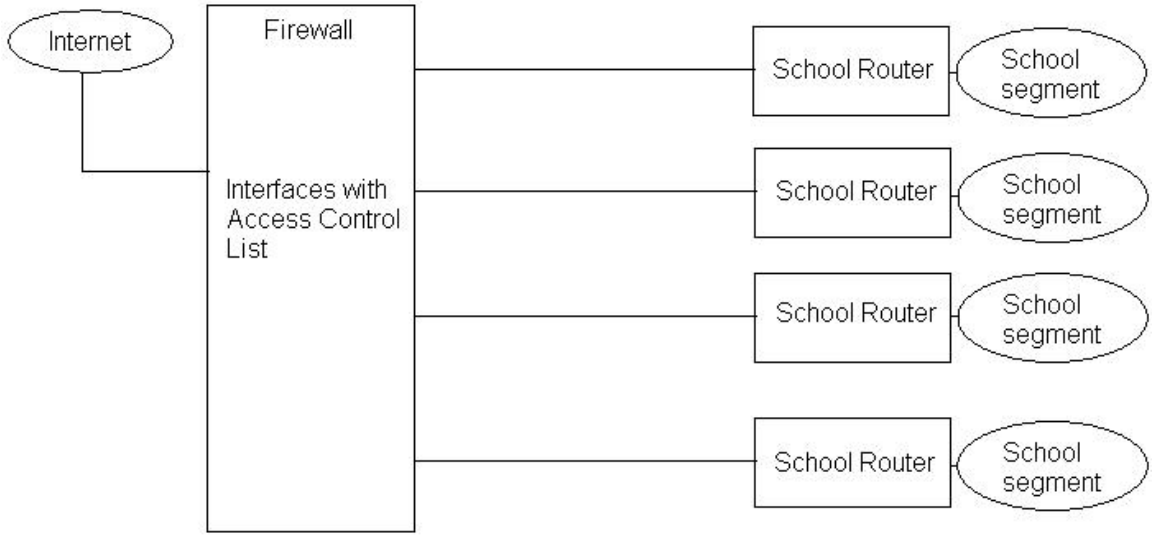
© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

What solutions do we have?:

-Put a firewall with one interface for each school at the main office.

That solution would be costly and represent a risk since it is a single point of failure. It also adds an extra burden on the firewall. We could have multiple firewalls to prevent single point of failure and reduce the work load but that would increase the cost as well.

It would look like the following.

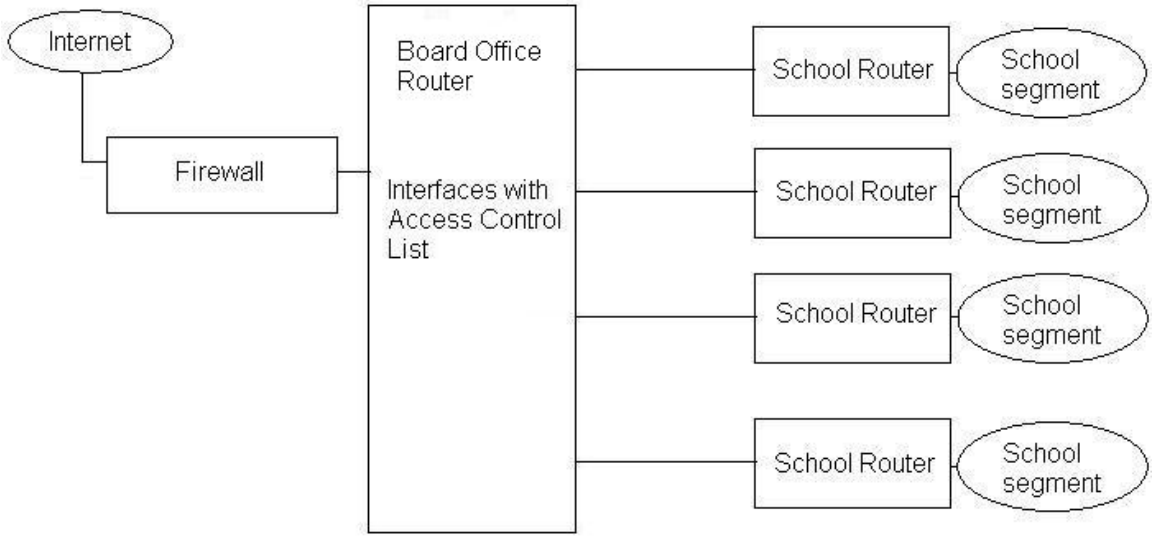


-Put filter on every perimeter router.

That would do the job without adding an extra cost, since the router is already in place and has the possibility to add ACL (Access Control List). Also, we can add the same rules to the main router to have a second layer of security since it's not the same hardware, so if vulnerability is found on one, maybe we are still safe with the other. The only thing with that solution, it doesn't offer protection inside the school. So we thought of taking that solution and improve it.

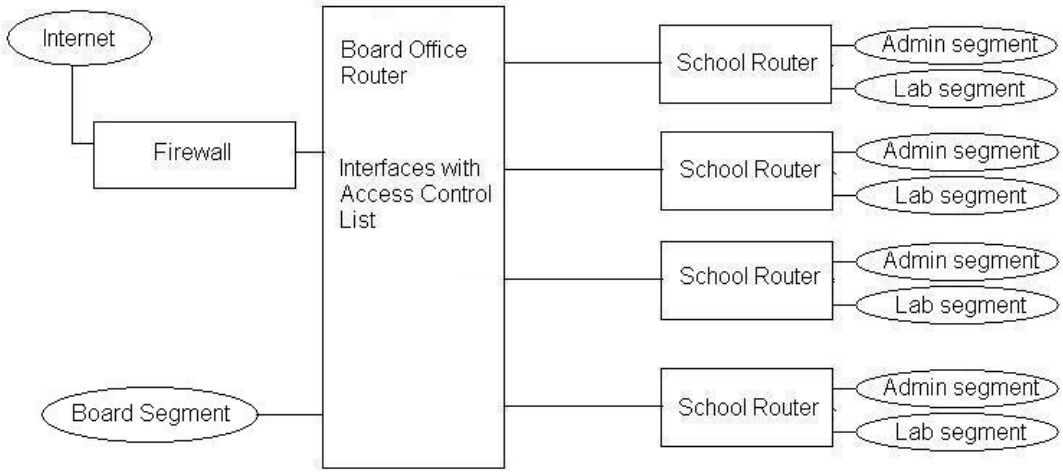
It would look like the following.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.



-Put filter on every perimeter router and split the administrative and lab.

Having a second interface in the school's router allow us to split the segment in two smaller segments and also apply rules. We decided that no one from the lab side should ever connect to anything located at the Admin side, that way we can isolate the place where most likely an attack can occur. We also enable the rules on both the school's and the board office's routers in order to have security on two different hardware. It looks like the following drawing.



© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Filters are acting like this:

-Board Office has limited access to Admin and Students subnet.
    -Some traffic can occur for troubleshooting purpose.

-Admin subnet has limited access to Board Office and Students labs subnet.
    -Web and e-mail traffic is allowed to the Board Office.
    -Some application needs to pass through in the labs direction.

-Student subnet has no access to Board Office subnet.
    -No access at all. Deny is put on Lab's and Board's router.

-Student subnet has no access at Admin subnet.
    -No access at all. Deny is put on Lab's and Admin's router.

-Student subnet is only accessing the main router to go on the internet but there is a rule on the Board Office's interface to deny any traffic from the student's labs.

That way, if a problem occurs in the student's labs, the problem will stay on the same subnet.

The schema has already proved itself during the blaster worm[3] attack. Schools that were hit didn't spread the virus to the others. Even in the school itself, the worm was contained on the infected segment only. We saved a tremendous amount of time when it came to the cleaning part after the infection and we saved on the down time too.

In that particular attack, the ports used by the worm were TCP 4444, TCP 135 and UDP 69. The worm is exploiting DCOM RPC vulnerability on Windows 2000 and Windows XP box. Not patched Windows NT and Windows 2003 were vulnerable too but according to the Symantec's web site[3], the worm's code wasn't made for those platforms since it still can infect the box but it will not replicate to those machines.

[3] http://securityresponse.symantec.com/avcenter/venc/data/w32.blaster.worm.html

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Securing school lab:

It didn't take long to realize that school labs were the most attacked place on our network. Kids were deleting important system files, formatting drives, installing junk, virus, bad shutdown, etc.
We used the windows integrated security feature to limit what they could do on a machine but we felt that was not enough and kids proved us right by continuing to destroy systems.
We had to ghost labs again and again. That was time consuming and labs were not functional enough.

We wanted a solution that would keep systems up even if critical files were deleted, drive formatted, systems hard reset; well let's say live in school's lab world. A good solution would allow us to freeze the system in the current state but it would also have to allow us to update those systems or install new software. Students are saving files on the Student's server so they don't need to save on the machine hard drive, and profiles are stored on the server too.

We went out to find a product or solution that would meet our needs and expectations. Our research brought up a product called Deep Freeze Professional[4]. Deep freeze offers a range of options that complies with our needs.

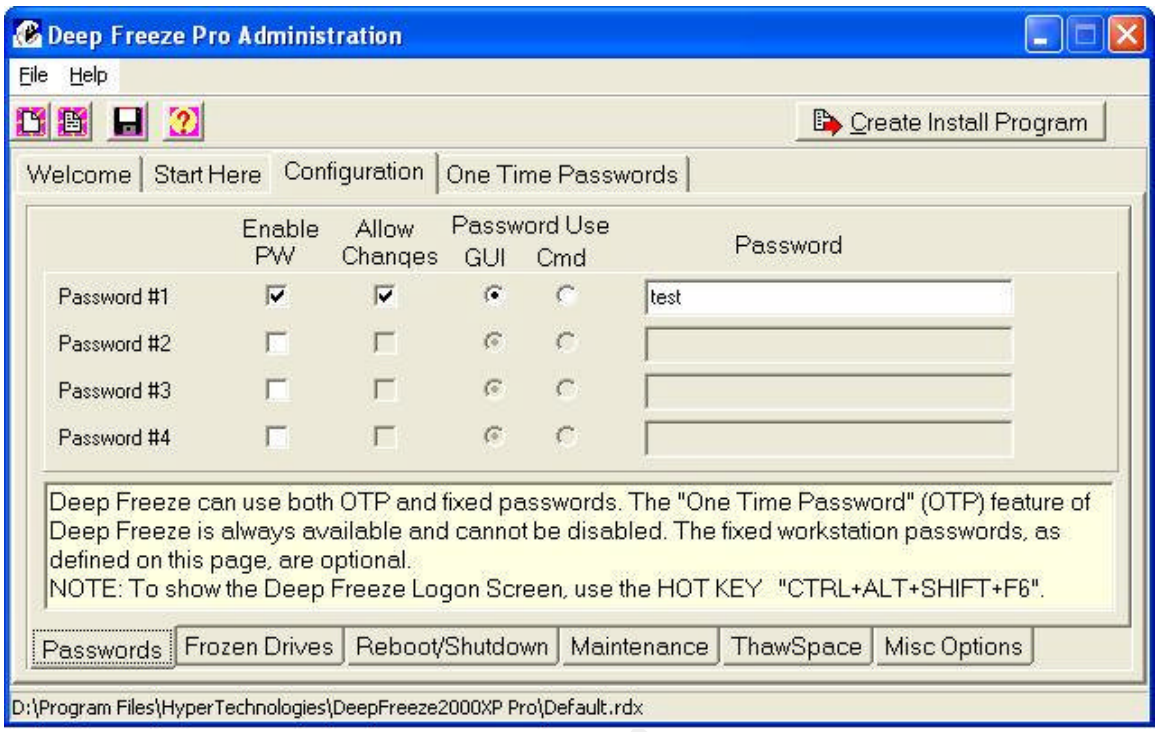
First, it freezes the selected drives in the state we want. All changes to files will be lost after the next reboot, even if the user tries to format a protected drive. The process is not documented very well, but it doesn't work like ghosting products that ghost at every boot so boot time is not longer. Also the process and the software can be completely hidden from the user.

It can also be deployed in a silent mode remotely. There are two parts of the software, the agent and the administrative part. The admin part is used to configure the agent before deployment and doesn't need to be installed on the machine.

The first step to use deep freeze, is to take the admin part and create the agent. After launching the software, you can select the option you want. The first tab allows us to put a password in order to protect the configuration. See image below.

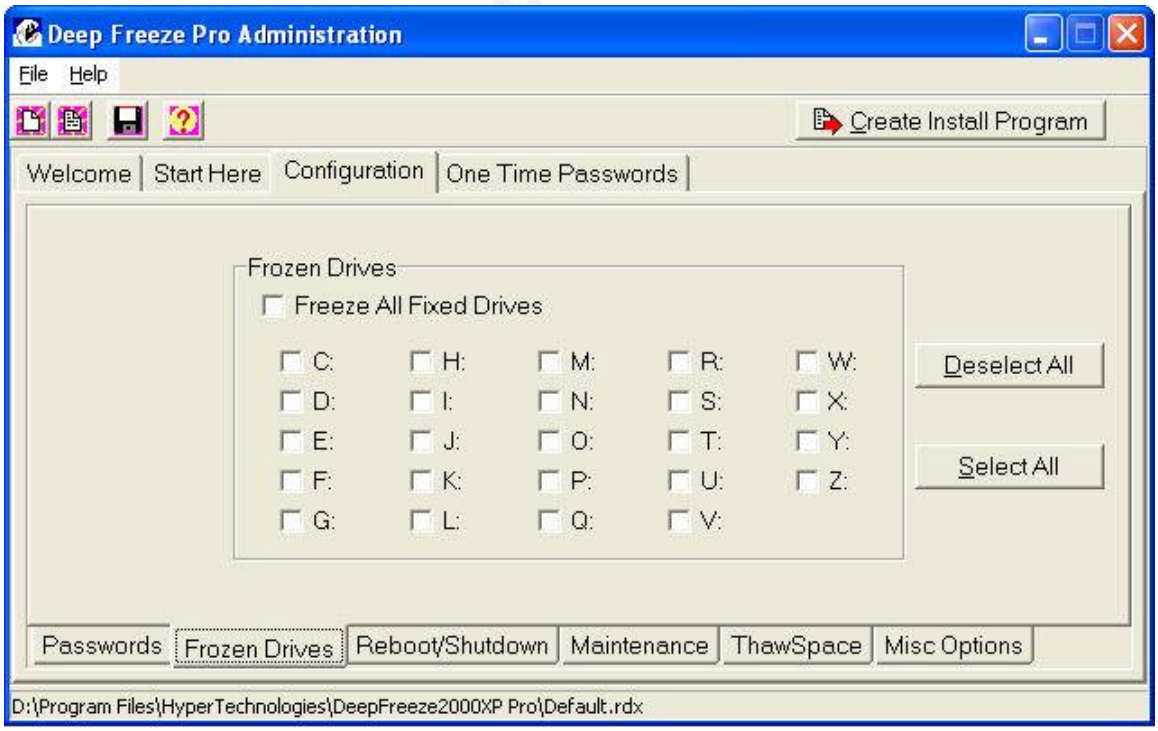
[4]Http://www.deepfreezeusa.com

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.



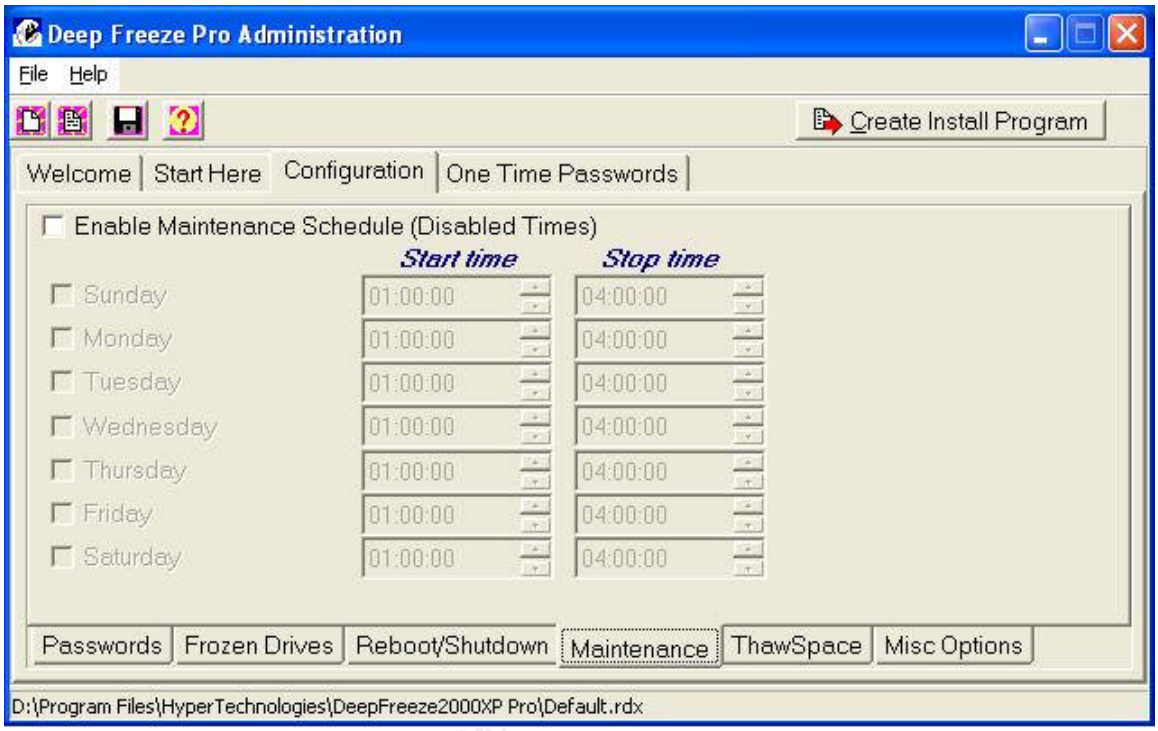
We can put a password with the option to allow changes, to access GUI or use Cmd.

The next tab called Frozen Drives. This is where we choose which will be frozen.



© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

The tab after is Reboot/Shutdown, this is where we can force a schedule reboot or shutdown. The next one is Maintenance and it's used to set a period of time where the system will not freeze. This is useful to allow its team to put patches, updates, new software or perform system configuration changes. We only have to choose the day, with the beginning time and the end time. See image below.



We also have the possibility to set a Thaw Space. That space is a chunk of the disk which is not frozen, so a user could save his files. In our case, we don't need that since they are saving on the files server.

In the misc options, we can set it we want an icon in the system tray.

After that setup is done, it will create an executable file that we can then deploy.

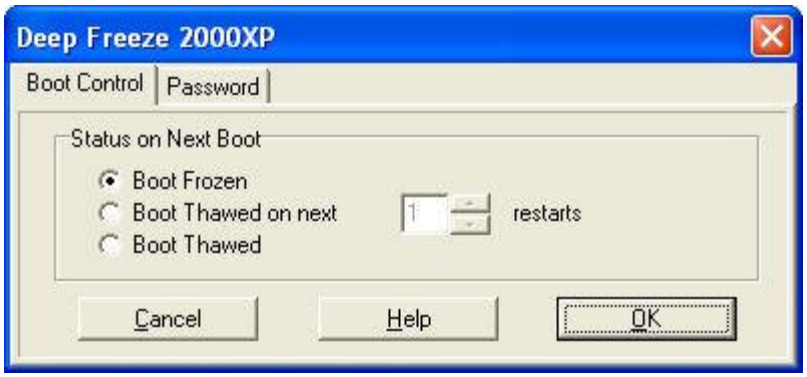
There is also a tab in the admin console called One Time Password, see picture below.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

That feature is used to generate a one time password. It can be useful for the technical support team. You can set up a password for one use or multiple use but both will expire at midnight the same day. To generate that password you will need the token by pressing Ctrl-Alt-Shift-F6 on the protected machine. This will bring up a window asking for the password but it also gives the token. See below in the upper left corner.

Once logged in, there isn't much we can do. We can set the system in a frozen state, a thawed state for x number of restarts and a complete thawed state.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.



That solution is very effective to us in saving precious amount of time by keeping machine in working state. It has also other advantages like denying the installation of software that can be unwanted like Trojan, spy ware, virus, keystroke logger, games, etc. We ask all the support teams to reboot the machine before logging into it. This eliminates the possibility for a hacker to install a keystroke logger and capture passwords.
We can't really estimate how much we save in money but for sure the investment for the programs is less than the saving.

Conclusion:

In conclusion, an effective security is a matter of different mechanism in order to provide multi-layer protections against different threats. It's always important to target the threats and assess them. In our case we targeted the students in the labs has our biggest threat and we provided different mechanisms to isolate, reduce and/or eliminate the damage they can do. Since technology is changing, threat and countermeasures will do so.

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

References:

SurfControl
Http://www.surfcontrol.com

Borderware
Http://www.borderware.com

Blaster Worm - Symantec's web site
Http://securityresponse.symantec.com/avcenter/venc/data/w32.blaster.worm.html

Deep Freeze
Http://www.deepfreezeusa.com

Cole, Eric; Fossen, Jason; Northcutt Stephen; Pomeranz, Hal, SANS Security Essentials Version 2.1 Volume1, SANS Press, 2003

Cole, Eric; Fossen, Jason; Northcutt Stephen; Pomeranz, Hal, SANS Security Essentials Version 2.1 Volume2, SANS Press, 2003

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.