

Re: [fw-wiz] Stanford break in

Source: <http://www.derkeiler.com/Mailing-Lists/Firewall-Wizards/2004-04/0050.html>

From: Carric Dooley (carric_at_com2usa.com)

Date: 04/22/04

To: Chuck Vose <vosechu@roman-fleuve.com>

Date: Thu, 22 Apr 2004 11:05:30 -0400 (EDT)

Here's my take..

On Wed, 21 Apr 2004, Chuck Vose wrote:

- > *The break in at Stanford and other high level super-computing schools*
- > *prompted a question about NIS.*
- >
- > *When dealing with any kind of networked password database, such as NIS*
- > *or Active Directory, how does one ensure that accounts aren't stolen. It*
- > *seems like when an account is lost, it's lost on every single computer*
- > *on the network instead of just one machine.*
- >
- > *1. Are network synchronized passwords a bad idea, considering the*
- > *normally lax stance on security that many corporations have?*

Network synced passwords are the only way to manage a large number of users. If you have 10 workstations and 1 server, it might be fine to have no network directory, but with 300,000 users, I would say it's impossible. I would consider: LDAP, NDS, AD, SecureID, RADIUS, TACACS. (notice the conspicuous absence of NIS, and I wanted to leave out AD, but it seems to be unavoidable these days.

- >
- > *2. Aside from running Jack the Ripper regularly on the passwords and*
- > *ensuring that passwords are strong, what are some methods to ensure*
- > *physical and logical security of accounts (ie: yellow stickies are the*
- > *hidden treasure for a disgruntled employee). Any generalized concepts?*

JOHN the Ripper, Rainbow Crack or L0phtcrack could be PART of the process, but it would make more sense to enforce strong passwords when the user sets them. Decide on password guidelines like alpha-numeric, mixed case, and one special character, and leave it to a dll like passfilt.dll or something similar. Yellow stickies just comes down to end-user education, and a good password policy. If the requirements are: "14 random alpha-numeric chars, with 5 special chars and mixed case.. OH, and change it weekly" you will most likely have a sticky note problem.. if it's: "7 chars, alpha-numeric, one special char and mixed case changing every 42

Firewall-Wizards: Re: [fw-wiz] Stanford break in

days, and HERE are 6 examples of good passwords", you could make some progress... it really comes down to a good security program that includes the security organization, and a well-crafted, enforced security policy.

>
> 3. In an Active Directory domain, allowing access to all computers is
> obviously a bad idea, but is this what the majority of admins do?
> Authenticate with the server, but only allow access to one workstation.
> I've never had to do this on a large scale, is it as time consuming as
> it seems that it might be or are there tools that make this easier?
>
AD, LDAP, NDS all give you the ability to control access through context. In other words, if the tree is well designed, a user cannot access all servers on the network. Access to "a workstation" would be somewhat useless in a client server network... users need to be able to get to servers, but only those required to do their jobs, which is pretty much the underlying principal to data confidentiality in the CIA (confidentiality, integrity, availability) data security model. This again goes back to whether or not an enforced policy allows network administrators to create a flat tree... you COULD even do it if all you have is something like domains using resource domains, with multiple masters, and creating infinite one-way trust relationships, but the level of pain that would entail would discourage most sane people.

> I know that this is 3 disparate topics, would list etiquette suggest
> that I should make 3 topics?

>
> Thank you,
> Chuck

>
>
> _____
> *firewall-wizards mailing list*
> *firewall-wizards@honor.icsalabs.com*
> <http://honor.icsalabs.com/mailman/listinfo/firewall-wizards>
>

--
Carric Dooley
COM2:Interactive Media
<http://www.com2usa.com>

firewall-wizards mailing list
firewall-wizards@honor.icsalabs.com
<http://honor.icsalabs.com/mailman/listinfo/firewall-wizards>