

Re: UNIX password auditing tool and the search for dictionaries too

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/security-basics/2003-08/0266.html>

From: Adam Newhard (atnewhard_at_microstrain.com)

Date: 08/08/03

To: <security-basics@securityfocus.com>

Date: Fri, 8 Aug 2003 09:41:46 -0400

In terms of this comment to whoever posted it (sorry, I don't remember who it was):

> >*Strong passwords are the number one source of denial of service in most*
> >*environments due to the frequent false reject problem that occurs when*
> >*users can't keep up with frequent changes and strong password. They're*
> >*also one of the highest costs for security since it's the number one*
> >*task for help desks and sys admins to support.*

How is it a high cost for security??? I've always found having someone come down and asking for their id and some other mode of face to face identification makes it pretty easy to reset someone's password. If you simply take advantage of all that garbage they pull on a lot of websites, like your security question is what's your mother's maiden name, you can get around them showing you a fake id...yeah, there are ways of finding out someone's info, but nothing is secure. It's the foundation of your plan that guides your performance.

In terms of your dos attack, i might be misreading your question, but strong passwords being dos'd or brute forced (if you consider a really fast brute force attack a dos; i don't, but some do), a lot of places will put a piece of crap machine as their password authentication for their network. yeah, you may have a lot of people logging on and may get periodically bogged down, but you need to find the right machine that'll cause the correct amount of lag. say for a "normal" company (my idea, not necessarily yours) you have 200 people. probably, on average they log on maybe 2-3 times/day...some only once, some maybe 10 times, and those on vacation never...so give them 3 times/day. if you have a fast machine doing password checks and it takes only a second for the logon sequence (password verification), it'll be about 600 seconds or 10 min (200 people x 3 logons/day x 1 sec)...theoretically, of course. if i want to brute force the machine i can do 60/sec. take a crap machine, stable mind you just a slower processor, that takes 10 seconds to verify a password and you've dropped to 6 attempts/sec. Yeah, you do go from 10 min/day of verification

SecurityFocus BASICS: Re: UNIX password auditing tool and the search for dictionaries too

to 50 min (if my math is correct) so that's something you need to consider when you think about if it's worth it or not...after finding a reasonable value, it is to me. You could consider it an easier target for dos b/c it's much slower, but then again, you also have to take into consideration this...if you're gonna try to get in using someone's password, why would you attack a crap machine that's exceptionally slow...i'd just stand behind them while they type in their password. i might've missed part of your statement, so if i did...i apologize.

after reading your statement, one more thing...if strong password authentication causes a lot of dos b/c people are trying to logon constantly w/the wrong password b/c of password changes, why are you even letting them attempt to logon so many times? if a person mistypes their password 3-5 times, the account should either be deactivated until that person comes and gets you or for a certain number of minutes. print a nice pretty message to the user that this has happened and send yourself a note also so you can go find them if need be. there are holes to that one just like anything (i.e. your boss doesn't like it), but like i said before, nothing's really perfect. if dos'ing occurs b/c people keep entering the wrong password, that's more your fault than theirs. out of curiosity, where did you find it saying that dos is the number one problem w/strong passwords???

adam

Adam Newhard
Microstrain, Inc.
If vegetarians eat vegetables, watch out for humanitarians

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

From: "Michael Martinez" <mmartinez@tamsco.com>
To: <security-basics@securityfocus.com>
Sent: Thursday, August 07, 2003 4:48 PM
Subject: RE: UNIX password auditing tool and the search for dictionaries too

> >Before you go too far with strong passwords, remember, they do more
> >harm
> >than good in most cases. You trust your money to a four digit pin so
> >think about strong authentication, not strong passwords. Two factor can
> >be done with a variety of inexpensive technologies.
>
> Are you kidding me, you are under the impression that a 4 digit pin is
> secure? I for one have no illusions about how insecure a 4 digit pin
> actually is! Whatever security is provided by said 4 digit pin is more
> related to that fact that there are not freely available pin cracking
> tools for ATM machines...as there are password cracking tools.
>
> >Strong passwords are the number one source of denial of service in most
> >environments due to the frequent false reject problem that occurs when
> >users can't keep up with frequent changes and strong password. They're
> >also one of the highest costs for security since it's the number one
> >task for help desks and sys admins to support.
>

Re: UNIX password auditing tool and the search for dictionaries too

SecurityFocus BASICS: Re: UNIX password auditing tool and the search for dictionaries too

> *As a help desk supervisor, I assure you that the related cost of time
> and money supporting the reset of passwords is minimal and therefore a
> small price to pay for increased security.*
>
> ...
>
> *>In terms of dictionaries, I think the aggressive approach would include
> concatenations and number and special character injections into the
> words. In more secure environments, were users are battered with
> monthly
> password changes they usually inject the numeric value for the month
> somewhere in a common word. But the point is, it's not too difficult to
> build a really big database of words with special character and numeric
> injections, run them through the hash algorithm and have a table to
> check for matches.*
>
> *If someone were in an environment where they must change their password
> monthly...they are probably using the wrong technology. Perhaps a
> combination of different layers would be a better solution to monthly
> changes.*

> ...

> -----Original Message-----

> *From: Shane Lahey [mailto:s.lahey@roadrunner.nf.net]
> Sent: Monday, August 04, 2003 7:38 PM
> To: james.easterling@ed.gov; security-basics@securityfocus.com
> Subject: RE: UNIX password auditing tool*

> *Alec Muffett Crack :: <http://www.crypticide.org/users/alecm/>*

> > -----Original Message-----

> > *From: james.easterling@ed.gov [mailto:james.easterling@ed.gov]
> > Sent: Monday, August 04, 2003 4:39 PM
> > To: security-basics@securityfocus.com
> > Subject: UNIX password auditing tool*

> > *I have tried searches for UNIX password cracking tools and I have come
> up*

> > *with little value. Can someone direct me to passwd auditing tools
> > besides "John The Ripper" that are free or cost?*

> > *Regards,
> > James*

> -----
> --

SecurityFocus BASICS: Re: UNIX password auditing tool and the search for dictionaries too

> > -
> >
>

> --
> > --
>
>
>
>

> ---
>

> ----
>
>
>

> ---
>

> ----
>
>
>

-
>

--
>
>
