

Re: How to limit number of failed FTP logins?

Source: <http://www.derkeiler.com/Newsgroups/microsoft.public.win2000.security/2005-11/0010.html>

From: Ralph Hulslander (*RalphHulslander_at_discussions.microsoft.com*)

Date: 11/01/05

Date: Tue, 1 Nov 2005 05:34:03 -0800

Thanks Steven for the reply, This box is only running IIS there are no local users and it is sitting behind a apparently efficient firewall.

I was wondering if I could use GPO to limit the number of login attempts on the FTP port or if there was a firewall or Dnial of Service monitor that could do it. The problem with using a firewall is of course the port is open, so "most" firewalls do not monitor that port as strictly.

Or does anyone have a script monitoring the Event log? I would guess that a script could monitor the Event log and if it sees repeated failures login failures then it could shut off FTP for a designated time and then restore it.

After everyone of these attacks I can block the IP address but that is closing the door after the horse has escaped. The IP address is never reused.

Thanks again for the reply.

Ralph

--

Progress is just a faster road to the end.

"Steven L Umbach" wrote:

```
> Maybe something else is attracting them to your server such as other ports
> being open to the internet other than for FTP. Try using one of the self
> scan sites such as http://scan.sygatetech.com/ to see if there are any other
> ports open such as netbios/file and print sharing which can draw a lot of
> attention from internet users and would be evidenced by failed logons to non
> default user accounts for users that you have created. File and print
> sharing should be disabled on external network adapters. Normally you can
> set an account lookout policy for user accounts in Local Security Policy but
> I don't know offhand if that will work for FTP logon attempts for user
> accounts and can end up blocking access to the legitimate user by locking
> their account. I would also suggest that you run Microsoft Baseline Security
> Analyzer on your server and the IIS Lockdown tool to help you secure it and
> check for basic vulnerabilities. Before running the IIS Lockdown tool it
> would be a good idea to a full backup of your server event though IIS
> Lockdown tool is supposed to be removable. It would also be a good idea to
> add those IPs to a block filter rule for your firewall if they are not too
> numerous. --- Steve
>
> http://www.microsoft.com/technet/security/tools/mbsahome.msp --- MBSA
> http://www.microsoft.com/technet/security/tools/locktool.msp --- IIS
> Lockdown tool
```

microsoft.public.win2000.security: Re: How to limit number of failed FTP logins?

>
>
> "Ralph Hulslander" <RalphHulslander@discussions.microsoft.com> wrote in
> message news:DE525BB9-C1CC-4D31-87AD-D0405F9AF6F8@microsoft.com...
> >
> > A Windows 2000 server is being subjected to a continuous stream of login
> > attempts.
> > Essentially this was causing a denial of service until I set the Event
> > Log
> > to overwrite once full.
> > Is there any way to limit the login attempts. None of the attempts are
> > successful.
> > These attacks come from random IP's and are preceded by a initiating event
> > (attempted login) that is followed by a flood of attempts.
> >
> > The machine is not using AD.
> >
> > Thanks
>
>
>