

Re: Being hacked...

Source: <http://www.derkeiler.com/Newsgroups/microsoft.public.win2000.security/2004-03/1139.html>

From: Steven L Umbach (*n9rou_at_nospam-comcast.net*)

Date: 03/21/04

Date: Sun, 21 Mar 2004 01:07:05 GMT

Are you offering a webserver and ftp server to users on the internet as per having FTP and HTTP open? You did not mention that in your original post. If not you should close those ports and disable the services. What tool told you that you that netbios ports open and did it say open or not "stealthed" – as long as they are not open you should be fine. I like to use the free Superscan 4.0 from Foundstone. I don't think the age of your firewall is that important as long as it has a default block all rule for inbound with rules just for the needed exceptions for allowed inbound access.

How are you restricting kerberos only. As far as I know that is not possible? The logon failure that you show could possibly be an unauthorized computer from inside your network. For internet attacks what I would look for is patterns in the firewall log that occur at the time that the logon failures are being recorded such as a reoccurring IP address – maybe with that computername if you are lucky. Check to see if any reoccurring attempts are trying to use ports 139 or 445 [file and print sharing] or 21 FTP, 80 HTTP, 3389 RDP all tcp. If the failed logons are showing on the same server, you may want to install Sygate personal firewall [free trial period] on it and disable the firewall itself which will still allow it's extensive logging including a traceback function. Just be sure to back up your server before installing a persona firewall. Also you account lockout threshold is very low and should be at least ten per Microsoft recommendations which will still provide protection against hack attacks without also causing premature lockouts in certain situations.

I am not an expert on IIS by any means but I do know if you are using FTP and IIS you need to run the IIS lockdown tool which will help stop malicious attacks on IIS [in addition to being fully patched]. The link below shows you where to download the IIS Lockdown tool. Just be sure to have a current backup of your IIS server including the System State AND back up your IIS settings using the IIS Management Console where you select the server/properties – backup and restore. --- Steve

<http://www.microsoft.com/downloads/details.aspx?FamilyID=dde9efc0-bb30-47eb-9a61-fd755d23cdec&DisplayLa>
http://smb.sygate.com/products/pspf/pspf_ov.htm

"Anne Robynn" <annerobynn2000@yahoo.com> wrote in message
news:55fdd789.0403192131.49059bb0@posting.google.com...

> *Thanks for your suggestions.*

>

> *The scan on the firewall showed on FTP, POP3 and HTTP open. But it was
> strange, because when I used one tool it told me all the Netbios ports*

- > (135, 137–139) were closed, but another scan told me they were open.
- > When I check the firewall its self, it shows that they are not open.
- > What's up with that?
- >
- > Here is a sample of the audit log.
- >
- > Notice the workstation name. It is not one of ours. Notice it says
- > NtLmSsp, but I went into the default domain policy and told it to only
- > accept Kerberos.
- >
- > Event Origin Details:
- > User SID: S-1-5-18
- > In Work Hours: Yes
- >
- > Logon Failure:
- > Reason: Unknown user name or bad password
- > User Name: xxxxxxxx
- > Domain: LAPTOP21
- > Logon Type: 3
- > Logon Process: NtLmSsp
- > Authentication Package: NTLM
- > Workstation Name: LAPTOP21
- > Caller User Name: N/A
- > Caller Domain: N/A
- > Caller Logon ID: N/A
- > Caller Process ID: N/A
- > Transited Services: N/A
- > Source Network Address: N/A
- > Source Port: N/A
- >
- > I am using windump and can look at the logs in Ethereal, but there are
- > so many entries, I don't know what to look for. I see many outside
- > addresses accessing. How do I know if it's the "bad" guy or not?
- >
- > I am also using a tool that tells me when files have been changed, and
- > it it keeps telling me that people are accessing nsiislog.dll,
- > iisstart.asp, doing CONNECTs and GETs. They never come from the same
- > IP address, and WHOIS shows they are coming from China, AU, San
- > Francisco. I don't think we use IISstart.asp. Is this the hole?
- >
- > Here's a sample of that:
- > ClientHost: 211.162.68.69
- > Username:
- > ServerIP: 192.168.1.1
- > ProcessingTime: 219
- > BytesRecv: 29
- > BytesSent: 0
- > ServiceStatus: 500
- > Win32Status: 126
- > Operation: GET
- > Target: /scripts/nsiislog.dll

> *Parameters:*

>

> *We are replacing our really old firewall ASAP. But I don't think the
> firewall is what is letting them in. I read the MS security
> whitepaper, and it's good, but doesn't tell me how to get them out of
> my system.*

>

> *Any suggestions?*

>

> *Thanks again,*

> *Anne*

>

> *"Steven L Umbach" <sumbach@N0spam.ameritech.net> wrote in message
news:<enqIKnDDEHA.1600@tk2msftngp13.phx.gbl>...*

> > *You sound a little vague on your firewall protection. Hopefully you are using
> > a block all default rule and then allowing only authorized inbound traffic.
> > I would try to scan your network yourself from the outside or use a self
> > scan site such as <http://scan.sygatetech.com/> if you can not do that right
> > away. You need to make sure other unneeded ports including port 445 are
> > closed. The fact that ALL your accounts are locked out tells me that either
> > someone enumerated your user accounts from the internet, from inside your
> > network, or possibly they gained access via Remote Desktop to a regular user
> > account and are now trying to gain a stronger foothold on the network. If
> > possible restrict access to port 3389 from only authorized public IP
> > addresses instead of "all". the strange computer you see probably is coming
> > from the internet, but could possibly [though probably unlikely] be an
> > internal attack from someone plugging into your network. You may not be able
> > to ping that computer but if you check the computer where the log entries
> > were found then possibly running nbtstat -r or arp -a may show an IP
> > address, but those entries do not stay in the cache long. Better yet examine
> > your firewall logs to see if you can pin down where these attacks are coming
> > from by comparing entries in the logs to failed logons to your computers
> > based on correlating times. You may also need to enable auditing of logon
> > events for at least failures on all of your computers to find out where
> > these attacks are coming from. You can scan the security logs of multiple
> > computers using Event Comb from Microsoft. See the link below on where to
> > get it and tips for tracking down account lockout problems. --- Steve*

> >

> > <http://www.microsoft.com/technet/security/guidance/secmod144.msp>

> >

<http://www.microsoft.com/downloads/details.aspx?familyid=7af2e69c-91f3-4e63-8629-b999adde0b9e&displaylang>

> >

> > *"Anne Robynn" <annerobynn2000@yahoo.com> wrote in message
> > news:55fdd789.0403161844.33d946e4@posting.google.com...*

> > > *For the past week every morning at around the same time we get
> > > attacked twice, a few hours apart. All our accounts are being locked
> > > out. I figured we were under attack, but nothing I have done has kept
> > > this hacker out, nor have the attacks diminished.*

> > >

> > > *I have searched for a solution everywhere including these newsgroups
> > > here at groups.google.*

> > >
> > > *Here's what I've got, and what I've done. I need suggestions on how to
> > > stop these attacks.*
> > >
> > > *What I've got:*
> > > *1. 3 Servers both windows 2000, all with service pack 4*
> > > *2. Two are DCs, one is a Citrix server. We are running exchange server
> > > on one of the DCs.*
> > > *3. I have a PIX firewall, all Netbios ports are closed. Pretty much
> > > only what we need is open. 3389 is open for remote desktop... could
> > > this be the problem?*
> > > *4. We are running the AD, and force Kerberos authentication*
> > > *5. account lockout is set at 3 bad logon attempts*
> > > *6. I have the accounts locked out forever*
> > >
> > > *What I've done:*
> > > *1. I've installed an event log analyzer to help with event log
> > > analysis and alerts. I have it notify me when lock outs occur, when
> > > anyone accesses what they shouldn't, and when files are being
> > > accessed.*
> > > *2. I have the event log set large and doesn't overwrite its self*
> > > *3. I see 629, 630, 681, you name it I got it.*
> > > *4. I saw an NTVDM showing up on all the servers, so I disabled NTVDM
> > > usages.*
> > > *5. During the attacks, I see a machine name appear that is not one of
> > > my own. I can't ping it, pstools can't identify it, I don't know how
> > > to get it off the system.*
> > > *6. are we really being attacked twice, or is the directory replicating
> > > the lock outs while we are unlocking, causing both DC to show locked
> > > out?*
> > > *7. The guest account is disabled*
> > > *8. Iwam Iusr, keep getting targeted too, why do I need these?
> > > Exchange? Citrix?*
> > > *9. I've scanned with LADS to check for alternate data streams.*
> > > *10. I've scanned for files that shouldn't be there*
> > > *11. I've disabled any accounts we don't need*
> > > *12. I changed the admin password just to be sure*
> > >
> > > *I can't turn off the Internet connection. Our work requires it.*
> > >
> > > *I don't know what else to do. How do I keep them off? How do I tell if
> > > they're even there and this isn't just a script running? How do I tell
> > > where the script is and get it off? I don't know what else to lock
> > > down.*
> > >
> > > *Any help will be greatly appreciated.*
> > >
> > > *Thank you,*
> > > *Anne*