

Re: Finding a Hacker

Source:

http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.active_directory/2007-05/msg01102

- *From:* "Anthony" <anthony.spam@xxxxxxxxxxxxxxxx>
 - *Date:* Sun, 20 May 2007 09:49:54 +0100
-

Its conjecture at the moment because we don't know if the RDP connection was over the net, or an internal prank. I am saying that if they managed to get local admin rights on the machine used by the domain admin, then they definitely had the capability to obtain the domain admin credentials and may have done so.

The event log on the PC might show more of what happened.

Anthony

<http://www.airdesk.co.uk>

"Herb Martin" <news@xxxxxxxxxxxxxxxx> wrote in message
news:OzmqjZrmHHA.4240@xxxxxxxxxxxxxxxxxxxxxxxxxxxx

"Anthony" <anthony.spam@xxxxxxxxxxxxxxxx> wrote in message
news:Oa2R3GrmHHA.3952@xxxxxxxxxxxxxxxxxxxxxxxxxxxx

IPSec is just one way of encrypting communications between two devices:
<http://www.microsoft.com/technet/network/ipsec/default.msp>

If the hacker got in remotely over RDP, then he cracked the username and password.

AND if he CREATED a new users then at some point he likely cracked an ADMIN (or partially equivalent) account's username and password.

When you expose a service over the net you will see password attempts all the time. You must have a highly secured password to use this for administration. Better is to use a secure VPN with client verification.

If the hacker did get in remotely using an administrator account on the PC then he could have obtained your domain admin credentials too.

Re: Finding a Hacker

When you write "could have" are you saying he "MIGHT" have or he definitely had the capability, i.e., might have had the capability vs. had it and might have used it?

Anthony
<http://www.airdesk.co.uk>

"scott" <sbailey@xxxxxxxxxxxxxxxx> wrote in message
<news:%23u%23d2immHHA.4872@xxxxxxxxxxxxxxxxxxxxxxxxxxxx>

one last question, without going in depth, can you tell me what exactly is IPSec and where it fits into securing your domain?

Many thanks for the previous info.

"Anthony" <anthony.spam@xxxxxxxxxxxxxxxx> wrote in message
<news:%23B8MwSmmHHA.3980@xxxxxxxxxxxxxxxxxxxxxxxxxxxx>

You could set a rule in the firewall to allow RDP only from your IPaddress. But to use RDP from outside the hacker must have guessed a username and password. Make the password complex and this is highly unlikely. Or else use a VPN to connect.

In GPO, set the auditing policies in Computer Configuration, Windows Settings, Security Settings, Local Policies.

See here for policies:

<http://technet2.microsoft.com/windowsserver/en/library/d9fea7ea-61e5-43b1-98cd->

and here for guidance:

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

Anthony
<http://www.airdesk.co.uk>

"scott" <sbailey@xxxxxxxxxxxxxxxx> wrote in message

Re: Finding a Hacker

news:e3CRB4lmHHA.1340@xxxxxxxxxxxxxxxxxxxxxxxxxxxx

Is there a way to restrict
remote desktop from
allowing access except
from my home ip address?

Where is "logging for logon
success and failure" located?
I assume
it's a GPO?
Can you give me some good
keywords to search or links
for info about
using these logs?

Thanks for your input.

"Anthony"
<anthony.spam@xxxxxxxxxxxxxxxx>
wrote in message
news:Oup\$hhkmHHA.4120@xxxxxxxxxxxxxxxxxxxxxxxxxxxx

Scott,
If that PC
has been
hacked, you
will need to
rebuild the
whole
domain. Its
really a
question of
whether
someone is
pulling your
leg
or you have
been truly
hacked.
1) If you
have set
logging for
logon
success and
failure then
the the
logon will
be in the
security log.
2) You can't

Re: Finding a Hacker

3) No. I guess if someone had domain admin rights they may be able to create an account you couldn't see, but if you thought they may have domain admin rights you would have to rebuild anyway. Is there a local account on the PC?

4) No. Your problem is not restricting remote desktop connections. It is what people are able to do on your domain. Your best case is that users are local admins of their machines and someone has done this for fun. Your worst

Re: Finding a Hacker

case is that
a hacker has
found the
remote
desktop
opening and
cracked a
password.
Anthony
<http://www.airdesk.co.uk>

"scott"
<sbailey@xxxxxxxxxxxxxxxx>
wrote in
message
<news:Oir593jmHHA.1624@xxxxxxxxxxxxxxxxxxxxxxxxxxxx>

One
of
my
clients
has
a
Win
2003
standard
PDC
with
about
10
winXP
clients.
I've
had
AD
setup
and
been
running
fine
for
years.
Last
week,
I
was
sitting
at

Re: Finding a Hacker

one
of
the
XP
clients
on
the
domain
and
suddenly
I
got
logged
off
and
a
user
"userHacker"
logged
back
in.
I
had
to
hit
ctrl-alt-delete
and
logged
myself
back
in.

After
about
60
seconds,
it
happened
again.
So
I
cut
off
access
to
the
net
and
looked
at
the

Re: Finding a Hacker

pc's
user
profiles
and
noticed
their
was
a
local
account
for
"userHacker".

I
deleted
the
profile
and
left
the
pc
off
line.

I
should
mention
that
I
have
Remote
Desktop
and
pcAnywhere
ports
open
in
the
firewall
for
this
XP
machine.

1.
Is
there
a
log
within
the
PDC

Re: Finding a Hacker

AD
that
would
show
a
record
of
users
that
logged
into
the
WinXP
machine?
2.
How
can
I
determine
which
port
the
hacker
is
coming
through?
3.
Although
I
searched
AD's
Users
and
Computers
applet,
I
couldn't
find
a
"userHacker"
account.
I'm
assuming
the
account
was
a
local
account
on
the

Re: Finding a Hacker

XP
machine.
Is
there
anyway
for
him
to
have
created
an
"hidden"
account?

4.
Does
"Remote
Desktop"
keep
any
type
of
activity
log
that
would
help
me?

Any
ideas
on
restricting
remote
desktop
connections
by
user
account
or
ip
address
would
be
appreciated.

Re: Finding a Hacker