

RE: Users slam Microsoft Security Analyser

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/focus-ms/2002-04/0198.html>

From: John Wienand (JWienand@bna.com)

Date: 04/15/02

To: focus-ms@securityfocus.com

From: "John Wienand" <JWienand@bna.com>

Date: Mon, 15 Apr 2002 17:01:03 -0400

First, please explain to me what you would consider "secure OS model and coding practices". What standard are you getting this from (in other words, what's the date when these became known as "secure")? Now, how long do you trust those? Until it fails you, or it fails someone you know. Then you find a new practice.

The fact is, you have people actively pursuing any holes they can find. Therefore, you must actively monitor your end to see if they are successful, or getting close to being successful. Relying on existing safeguards, no matter how thorough and complete, is silly.

Why is it that MS should be responsible to make sure you stay one step ahead of the hackers?

To put it in context of what you wrote below;

Keeping someone out of your office starts with a strong door, in a secure wall. Then a good lock. And a CCTV camera. And a Security Guard. Why the security guard? Because the wall can be knocked down, the door demolished, the lock picked and the camera broken. Heck, even the guard can be disabled.

So, you never rely on any one component. You always walk around and check the locks and monitor the CCTV. It just makes good sense.

Or you can sit in your office with you head down, assuring yourself that you picked a great lock for the door.

My pair of Lincolns.....

John

SecurityFocus Microsoft: RE: Users slam Microsoft Security Analyser

"Joe Klein"
<jsklein@mindspring.com> To: "Peter" <list@easynix.com>, "Wim Remes" <wim.remes@skynet.be>, <Thor@HammerofGod.com>, <focus-ms@securityfocus.com>
04/15/2001 cc: (bcc: John Wienand/BNA Inc)
02:42 PM Subject: RE: Users slam Microsoft Security Analyser

<rant>

I disagree. Security starts with stable hardware and physical location. Next is a secure OS model and coding practices within the OS. Next, is secure coding practices at the applications layer. Lastly, the systems are managed by trained and qualified Sys Admin with some security knowledge. Note that is referred to as "Defense in Depth".

Now let's begin our review of Microsoft.

1. Sales people sell the hardware and software. Microsoft trains the Sales people both at hardware and software companies to sell their product. The sales people are commissioned to sell as many 'boxes' as possible.

2. Software developers designed the Microsoft OS's and applications. They were trained by Sr. Software Developers at Microsoft to code in a specific way.

3. Microsoft provides training to Project Managers and Software developers in the field to program the Microsoft way. Note: I have attended one such course last year. Security was not discussed and not even part of the Microsoft Development model. When I mentioned security, I was told that 'security handled by the OS'. Also note that the instructor was from Microsoft Professional Services and not a contractor.

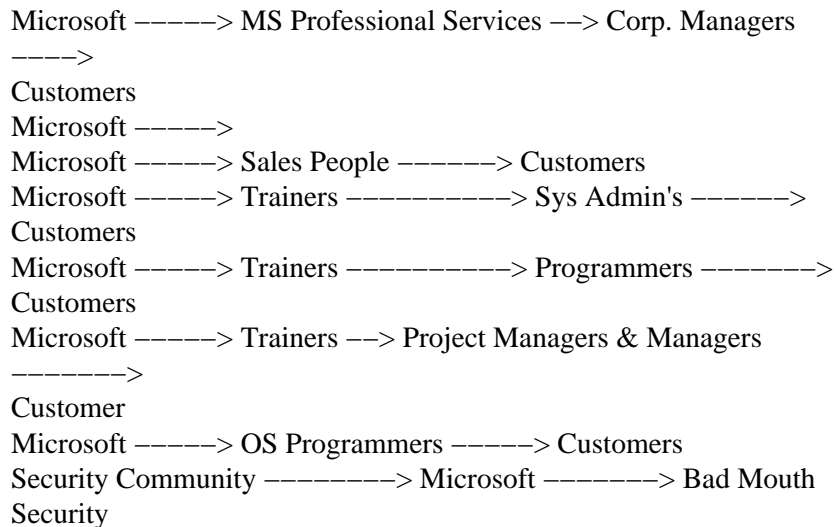
RE: Users slam Microsoft Security Analyser

4. Microsoft System Administrators attend Microsoft certification classes to learn how to best manage the Microsoft servers. Microsoft teaches 2 classes on security. Upon attending the class, I realized people were being taught to 'click buttons' and not really secure their environment. In one case the class teaches to use Microsoft 2000 as a router and then set up a Microsoft Firewall to protect your Microsoft web and mail server.

Note, Microsoft Sales people are teaching other sales people, that the Microsoft OS is so easy; you don't need an administrator in many cases (Talk to any one at CompUSA).

Another Note: I know of a manger at a large company who has her Microsoft certification. Her belief (as provide by Microsoft) is that unless there is a graphical button on an application, they could not be using the application. Note that when administrates are used by companies, the average ration of administrators to systems are 1 admin to 25 servers. Compare that with 1 admin to 100 servers in the Linux/UNIX world.

So let me diagram this...



SecurityFocus Microsoft: RE: Users slam Microsoft Security Analyser

Community

-----> Set up

security partners
program to reduce bad press

-----> Tell Press

that they can be
"trusted".

</rant>

About the Microsoft Security Analyzer. My testing is showing
about a 10%
false positive (Something is installed that is not) and 10%
false
negative (Something is not installed that is installed).

I guess 10% is better then 100% <GRIN>

Joe

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

From: Peter [mailto:list@easynix.com]
Sent: Monday, April 15, 2002 11:39 AM
To: Wim Remes; Thor@HammerofGod.com;
focus-ms@securityfocus.com
Subject: Re: Users slam Microsoft Security Analyser

Security doesn't start with the OS, it starts with the
System Admin.
Most hackers are succesful because of lazy Sys Admins,
un-educated
Sys Admins or no Sys Admins at all.
Many hackers using security holes which are 6 month and
older. The OS
actually doesn't matter, this is by any OS.
I have seen Servers in companys with NO password for the
Admin
account. This things are sad but the reallity.....
Just my \$0.02
Best Regards
Peter

> *When JM writes "...The company's security focus mailing
list..." which
> company does he mean ?
>
> I've personally downloaded MBSA for testing and it does
quite a nice
job. I
> am not a fan of
> the "X-mas on the desktop"-XP-style interface, but hey,*

RE: Users slam Microsoft Security Analyser

SecurityFocus Microsoft: RE: Users slam Microsoft Security Analyser

who am I?
Maybe I'm
> *that 0.001% of*
> *the MS customerbase that doesn't fall for intuitive menu's*
and easy
access
> *to the functionality ???*
> *One half of me can understand that this tool is good. It*
does a good
job
> *and may be handy for*
> *(a) admins that don't have the knowledge required to*
handle _any_
network
> *(b) quick assessing*
> *of vulns after a fresh install.*
>
> *In short I like the tool and it is a good step towards a*
security-minded
> *Microsoft (which is currently*
> *on holiday somewhere between Utopia and Israel). For all*
the peeps
quoted
> *in the article of JM,*
> *I have one remark : "security is NOT craving for tools*
that will do
the work
> *for you, it is neither*
> *bashing on the peeps that try to make your life easier but*
in the end
don't.
> *Security is a state-of-mind,*
> *an attitude that brings with it a certain responsibility*
to be aware
of
> *security 24/7. Following all*
> *the possible channels, learning all you can to be that one*
step ahead
of the
> *bad guys. Security is suffering,*
> *Security is a hell of a job (and I like it ;-). Patching*
& hotfixing
any
> *system, be it *nix, Win or something else*
> *will never seize, whichever GUI or command-line tools*
there will be
> *released.*
>
> *Bashing is easy (look at Sharon, or Arafat for whatever it*
matters).
> *Working together for a better and safer*

SecurityFocus Microsoft: RE: Users slam Microsoft Security Analyser

> *world is difficult but in the long run, the latter option*
is more
rewarding

> *than the 30-second bashing rush...*

>

> *C ya ...*

>

> *Wim*

>

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

> *From:* <Thor@HammerofGod.com>

> *To:* <focus-ms@securityfocus.com>

> *Sent:* Friday, April 12, 2002 7:39 PM

> *Subject:* Users slam Microsoft Security Analyser

>

>

>>

>> -----BEGIN PGP SIGNED MESSAGE-----

>> *Hash: SHA1*

>>

>>

>> *James Middleton of vnunet.com (UK) has taken the SF*
posts from HC

and

>> *Damien and turned it into an article:*

>>

>> *Users slam Microsoft Security Analyser*

>> <http://www.vnunet.com/News/1130844>

>>

>> *(I guess in the UK they spell it with an "s" instead of*
a "z")

>>

>> *James' email was not on the article, but since I know he*
is reading

these

>> *posts, I would like to make some comments:*

>>

>>

>> *First, shouldn't the main title be changed from "Users*
slam

Microsoft

>> *Security Analyser" to "Three Users slam Microsoft*

Security

Analyser?"

>>

>> *I am amazed that someone could take the comments of 2 or*
3 people

and turn

>> *it into an article. Obviously, James did not do his*
homework...

>> *I would have hoped that he would have downloaded and*

RE: Users slam Microsoft Security Analyser

SecurityFocus Microsoft: RE: Users slam Microsoft Security Analyser

tested the tool

> *before*

> > *giving credence to someone who thinks it is "just a GUI*

version of

the

> > *software giant's HfNetChk."*

> >

> > *It does FAR more than just check for missing patches,*

and he would

know

> > *that if he looked at it. And before you people go on*

record with a

> > *publication, you too should do your homework before your*

words are

quoted

> > *to live forever in error.*

> >

> > *I was going to comment on different excerpts from the*

article, but I

would

> > *end up quoting the whole thing... Jeeze.*

> >

> > *AD*

> >

> >

> >

> >

> >

> >

> >

> >

> >

> >

> >

> >

> >

> >

> >

> >

> >

> >

> >

> >

> >

> >

> >

> >

> >

> >

> >

> >

> >

> >

> >

> >

-
- **Previous message:** [Marc Fossi: "RE: Users slam Microsoft Security Analyser"](#)
 - **Maybe in reply to:** [Thor@HammerofGod.com: "Users slam Microsoft Security Analyser"](#)
 - **Next in thread:** [Schwartz, Stanley: "RE: Users slam Microsoft Security Analyser"](#)
 - **Messages sorted by:** [\[date \] \[thread \] \[subject \] \[author \] \[attachment \]](#)