

RE: MBSA and MS's attempts at "security"

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/focus-ms/2002-04/0142.html>

From: Elan Hasson (elan@daryl.org)

Date: 04/11/02

From: "Elan Hasson" <elan@daryl.org>
To: <focus-ms@securityfocus.com>, "H C" <keydet89@yahoo.com>
Date: Wed, 10 Apr 2002 22:10:28 -0400

>>So why then does the first page refer to "Code Red" and "Nimda" as "viruses"?

Well, what exactly is the definition of "virus"?

<http://www.faqs.org/faqs/computer-virus/new-users/> (as linked by http://www.cert.org/other_sources/viruses.html#I) (i dunno about you but cert appears to know what they are doing, right? yeah...)

>A computer virus is a program designed to spread itself by first infecting
>executable files or the system areas of hard and floppy disks and then
>making copies of itself. Viruses usually operate without the knowledge or
>desire of the computer user.

I think THAT is why Code Red and Nimda are "viruses", because they are designed to spread itself. Sure you could call it a "worm" too, but its a technicality. Get over it. Baby.

uhh yeah, NTFS is check for because you can set permissions with NTFS. Why have a multi-user where anyone can read/write to anything?

It requires latest MSXML because, hey guess what I bet the data is in XML! (like C:\Program Files\Microsoft Baseline Security Analyzer\mssecure.xml, a .98 mb XML file to tell you what vulnerable things are out there, and how you are vulnerable! OH WOW!).

It requires IE 5.01 because 5.01 was a MAJOR update to IE (versions i.e. <4 were trash!) and a base install of win98 comes with 5.0 (may be .01). MS Has since dropped support for the Windows95 product line with the release of windowsXP in oct 2001. If you have even bothered to notice, a lot of the UI in WindowsXP is based on Scripting and HTML.

The html approach is simple, you control the html using the HTML dom and insert html entities as needed. Its a quick way to make a nice and friendly UI.(Shavlik could have done a bit better with the scan results page, but it gets Most of the info out. Why don't you take a peek at the html files in C:\Program Files\Microsoft Baseline Security Analyzer\ ?

SecurityFocus Microsoft: RE: MBSA and MS's attempts at "security"

As for portqry?

(Taken from Q310099:Description of the Portqry.exe Command-Line Utility
<http://support.microsoft.com/directory/article.asp?ID=KB:EN-US:Q310099&>)

- >Portqry.exe is a command-line utility that you can use to help troubleshoot TCP/IP
- >connectivity issues. Portqry.exe runs on Windows 2000-based computers. The utility reports
- >the port status of TCP and UDP ports on a computer you choose.

(And from Q310456:How to use Portqry to Troubleshoot AD Connectivity Issues
<http://support.microsoft.com/directory/article.asp?ID=KB:EN-US:Q310456&>)

- > You can also use Portqry in the following ways:
- > To troubleshoot Active Directory issues in which you have to verify basic TCP/IP
- > connectivity, which can be especially useful in environments with firewalls.

- > To verify connectivity to TCP/IP ports that are used by Active Directory for
- > Lightweight Directory Access Protocol (LDAP), remote procedure call (RPC), and Domain
- > Name Service (DNS).

<fuck it, i'm too lazy to add my own >'s for quoting (this is from Q310456 as well)>

With Portqry, you can also query an LDAP service. It knows how to send an LDAP query (by using UDP and TCP) and interpret an LDAP server's response to the query. The response from the LDAP server is parsed, formatted and returned to the user.

Example

When you run the following command:

```
portqry -n myserver -p udp -e 389
```

Portqry automatically resolves UDP port 389 using the %SystemRoot%\System32\Drivers\...\Services file that every Windows 2000 and Windows XP system has by default. If it resolves the port to the LDAP service, it sends an unformatted user datagram to UDP port 389 on the target system. Portqry will not receive a response from the port as the LDAP service only responds to a properly formatted LDAP query. Portqry will report that the port is listening or filtered. Portqry will then send a properly formatted LDAP query to UDP port 389. If it receives a response to the query, it returns the entire response to the user and report that the port is listening. If portqry does not receive a response to the query, it reports that the port is filtered.

Sample Output

```
C:\>portqry -n mydc.reskit.com -e 389 -p udp
```

Querying target system called:

mydc.reskit.com

Attempting to resolve name to IP address...

Name resolved to 169.254.0.14

UDP port 389 (unknown service): LISTENING or FILTERED

Sending LDAP query to UDP port 389...

LDAP query response:

```
currentdate: 10/11/2001 23:10:21 (unadjusted GMT)
subschemaSubentry:
CN=Aggregate,CN=Schema,CN=Configuration,DC=reskit,DC=com
dsServiceName: CN=NTDS
Settings,CN=mydc,CN=Servers,CN=eu,CN=Sites,CN
=Configuration,DC=reskit,DC=com
namingContexts: DC=reskit,DC=com
defaultNamingContext: DC=reskit,DC=com
schemaNamingContext:
CN=Schema,CN=Configuration,DC=reskit,DC=com
configurationNamingContext:
CN=Configuration,DC=reskit,DC=com
rootDomainNamingContext: DC=reskit,DC=com
supportedControl: 1.2.840.113556.1.4.319
supportedLDAPVersion: 3
supportedLDAPPolicies: MaxPoolThreads
highestCommittedUSN: 815431405
supportedSASLMechanisms: GSSAPI
dnsHostName: MYDC.reskit.com
ldapServiceName: reskit.com:mydc$@RESKIT.COM
serverName:
CN=MYDC,CN=Servers,CN=EU,CN=Sites,CN=Configuration,DC=reskit,DC=com
supportedCapabilities: 1.2.840.113556.1.4.800
isSynchronized: TRUE
isGlobalCatalogReady: TRUE
```

=====
End of LDAP query response
=====

UDP port 389 is LISTENING

In this sample, port 389 is listening and from the output it can be determined which LDAP service is listening on the port and some details about its configuration. This information may also be useful in troubleshooting various problems.

Portqry knows how to send a query to the RPC end point mapper (using UDP and TCP) and interpret the response. This query will dump all of the end points currently registered with the RPC end point mapper. The response from the end point mapper is parsed, formatted and returned to the user.

SecurityFocus Microsoft: RE: MBSA and MS's attempts at "security"

</end fuck it>

What tools do that? i'd love to see one.

Now for your requests (and I'll even give you solutions!)

>1. *Some way of making patch and SP roll-outs more painless.*

Read First:

"Why Service Packs are Better Than Patches"

<http://www.microsoft.com/technet/treeview/default.asp?url=/technet/columns/security/essays/srvpatch.asp>

Your #2 is very valid, however Microsoft gives you an interface to the event log (In COM and Win32 API, hey even in the .Net Framework!) so you can feel free to do what you want with the data. You can even go NetBIOS name to IP, cool huh? Hell, you can even export it to xml to show how cool it is!

>3. *enumerating Alternative Data Streams*

You can use BackupRead() api to enum the streams.

>4. *Some way of preventing or restricting executables and scripts with a ":" in the name from running.*

You *could* write an app that hooks all calls to CreateProcess, if your code is good enough, you shouldn't notice it, all you're doing is looking for a ":".

> 5. *troubleshooting and incident response*

Maybe it wasn't thought to be necessary? Now that in WinXP its more common to have multiple users running processes in the background, what if the admin wants to know who is sucking his bandwidth?

I'm still trying to figure out what "allow for troubleshooting and incident response *as part of the distribution*!" means

>> *So far, MS's efforts at "security" via the STPP have been token efforts, at best.*

What is STPP?

eat me,

Elan Hasson <elan@daryl.org><elan@compiled.org><sticky@cowcum.com>

<http://www.cowcum.com> – Sticking sharp things into the hymn of the dot-com-deapool!

<http://www.compiled.org> – The Programmer's Resource, code, tutorials, downloads, reference.

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

From: H C [<mailto:keydet89@yahoo.com>]

RE: MBSA and MS's attempts at "security"

SecurityFocus Microsoft: RE: MBSA and MS's attempts at "security"

Sent: Wednesday, April 10, 2002 11:36 AM
To: focus-ms@securityfocus.com
Subject: MBSA and MS's attempts at "security"

It seems that MS has released the MBSA...a Baseline Security Analyzer.

<http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/tools/Tools/mbsahome.asp>

A technical whitepaper is available:

<http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/tools/Tools/MBSAWP.asp>

Overall, the paper is an interesting read. It's a document stating MS's intention and commitment to security.

So why then does the MBSA require the latest version of IE (5.01 or greater) and MSXML to run? What's wrong with the standard HTML used by other tools?

So why then does the first page refer to "Code Red" and "Nimda" as "viruses"?

So why then does the file system check only check to see if NTFS is installed? The white paper doesn't say anything at all about checking permissions, for the existence of NTFS alternate data streams, etc.

One of the SF lists recently had a post regarding MS's PortQry tool. Contrary to what the poster stated, the PortQry tool does *NOT* show the port-to-process mapping...rather, it's nothing more than a port scanner/banner grabber. How long have such things already been widely available?

Rather than coming up with ways to further inundate MS admins with information, MS should be focusing on more pressing issues, such as:

1. Some way of making patch and SP roll-outs more painless.
2. Some way of centrally managing and monitoring EventLogs. Once we get to that point, we can then focus on making them understandable, and more useful. Or perhaps MS should focus on making them more useful (ie, log by IP, rather than NetBIOS name...or both), and then focus on a facility for centrally managing

RE: MBSA and MS's attempts at "security"

SecurityFocus Microsoft: RE: MBSA and MS's attempts at "security"

them. (HINT: The tools that come with Win2K for converting EventLog entries to SNMP traps...*NOT* a good idea. Should have gone with a centralized EventLog, or a syslog functionality instead.)

3. Some way of viewing the existence (and contents) of NTFS alternate data streams via 'dir' and Windows Explorer. How about making the icon for an ADS a page similar to a .txt or .log file, but with a scarlet "A"?

4. Some way of preventing or restricting executables and scripts with a ":" in the name from running.

5. Basic tools that allow for troubleshooting and incident response *as part of the distribution*! FoundStone's fport.exe is an invaluable tool, but why wasn't something like that provided? Why is it so easy to hide a process from the Task Manager? If it weren't for the widely available array of freeware utilities, incident response on NT/2K systems would be impossible. The '-o' switch was provided in XP...why couldn't something be written *by Microsoft* that allows that functionality on NT/2K?

So far, MS's efforts at "security" via the STPP have been token efforts, at best. Hey, guys...if you're going to get serious about security...then "just do it"! Fiddle-farting around, producing tools that have already been readily available for some time doesn't go a long way toward showing us how serious you are.

Carv

Do You Yahoo!?

Yahoo! Tax Center – online filing with TurboTax

<http://taxes.yahoo.com/>

- ***Previous message:*** [Adam Smith: "RE: MBSA and MS's attempts at "security"'"](#)
- ***In reply to:*** [H C: "MBSA and MS's attempts at "security"'"](#)
- ***Next in thread:*** [Ogle Ron \(Rennes\): "RE: MBSA and MS's attempts at "security"'"](#)
- ***Messages sorted by:*** [\[date \] \[thread \] \[subject \] \[author \] \[attachment \]](#)