

Re: userenv and NETLOGON errors

Source:

<http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.sbs/2005-06/msg06493.html>

- *From:* "Tony Su" <TonySu@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxx>
 - *Date:* Thu, 23 Jun 2005 15:43:02 -0700
-

Matt,

You can go on asking for an IPCONFIG if you wish, but I'd still ask you to consider the long term effect you will have on the people you help, not just the immediate problem

..

I'm saying that given the certainty that new exploits will be created and the inability to gaze into the future to know what threats will appear over the lifetime of the network (it might be more than a decade) I wouldn't know how your conscience could be clear that you haven't encouraged a less than knowledgeable person to divulge information that made that person a victim.

People who study exploits realize that today conventional exploits only chase low hanging fruit because there is an ample supply of people who are unskilled and naive.

Those same people who study exploits also have seen the beginnings of exploits customized to specific people. 2 years ago no exploit used Google to find victims. A year ago no one used P-P file sharing as the "Server" for adware/malware content. Today, exploits have been written using these two new methods and there are more to come.

Are you saying that people should bet that an exploit won't be created to harvest IPCONFIGS from technical newsgroups if it can be exploited?

I don't agree at all with the old saw you mis-quote "Security by Obscurity is no Security at all." What bunk to not understand the true meaning... it should be interpreted "Security by Obscurity should not be relied upon." It also does not in any way invalidate the concept of not sharing any more personal information than you have to. If your train of thinking was correct, everyone should have no problem posting their Driver's License and Social Security numbers all over the place. After all, you'd need alot more to actually steal someone's identity, right? But, the truth is that those are substantial bits of information towards stealing an identity so the publicly revealing that information is discouraged.

The same thing applies to posting true IPCONFIGs.

Re: Some other comments...

Re: userenv and NETLOGON errors

You won't visit links posted in USENET? <That's FUDD>. Visiting such pages is no more risky than surfing other unknown or unvisited sites on the Internet.

And, maybe 50% of the problems are DNS related (I won't agree, but it's unimportant), but if that were true then it's even more of a reason to cut and paste the answer you gave someone else, just refer them to the previous thread.

Lastly, regarding your questions about exactly how information in an IPCONFIG can be exploited, I'm going to decline being that specific because that'd be irresponsible literally mapping out vectors someone could then use.

Tony

"Matt Gibson" wrote:

>
>> Info about your Host Machine
>
> Like? We already know you're running SBS 2000 or 2003? What more is going
> to be revealed?
>
>> Servers in the network, both IP address and name
>
> Really? From an ipconfig? I never knew doing that from my SBS server would
> reveal my SQL server.
>
>> MAC addresses
>
> I'd like to see how knowing someone's MAC address gives you an "in" on their
> network.
>
>> Network Address range
>
> 90% of the people here will be using the default range. Anyone who uses a
> different range for security reasons would change it before posting it here.
>
>> Default Gateway
>
> Again, I fail to see how this is useful to anyone not already on the inside
> of the network.
>
>> Whether NBT is enabled
>
> And this would help you how?
>
>> DNS suffix list
> What DNS you use (and maybe ripe for poisoning)
>
> Again, 90% of the people here will be using a .local domain, which is pretty
> impervious to poisoning.

Re: userenv and NETLOGON errors

>
>> NIC driver
>
> Wow. I use realtek. Should I be concerned that you know that now?
>>
>> And the list goes on...
>
> Keep posting, I'll keep pointing out that it's FUD.
>>
>> The point is that posting this information to a newsgroup means the
>> information will "live forever." Stuff I've posted and forgotten is still
>> searchable more than a decade later. Can you guarantee at the rate
>> exploits
>> are created that one won't take advantage of this info?
>
> Show me an exploit that only needs to know my internal IP information, and
> I'll believe you.
>
> At the very least,
>> <today> if an exploit were able to gain a toe-hold in a network this info
>> is
>> a treasure trove if it could be downloaded or installed with the exploit,
>> the
>> exploit will know how and what to probe without doing any "discovery."
>
> If an exploit is in my network, the last thing I'm worried about is if it
> can do a ipconfig /all
>
>> It's a slippery slope posting this kind of sensitive info where it'll
>> probably never die...
>
> Again, security by obscurity is no security at all.
>
>> Recommendations to avoid posting IPCONFIG to a public forum...
>>
>> 1. "Sanitize" the configuration. This can be as easy to do as pasting into
>> Notepad, then doing a Find/Replace, eg 192.168.16 > 192.168.224 before
>> posting. If desired this can easily be reversed in Notepad later.
>
> No argument here.
>
>> 2. Post the IPCONFIG as a webpage, then post a link to your webpage to the
>> public forum. You can take down the webpage when you're done. People might
>> still cache your webpage somewhere, but you've drastically reduced your
>> exposure.
>
> I'm not going to visit links to personal pages in usenet. THAT is a
> security risk.
>
>> The other thing that veteran members of a forum can do is not to ask for
>> the

Re: userenv and NETLOGON errors

>> IPCONFIG as a knee jerk reaction(I'm not necessarily saying that is the
>> case
>> here). It's often possible to suggest a solution based on certain
>> assumptions
>> and to qualify your suggestion because of those assumptions. Let the
>> <reader>
>> decide for himself how valid your suggestion is, and if the situation is
>> different that person can always post back... and in this case the
>> solution
>> might be resolved without exposing personal information.
>
> A knee jerk reaction? I'd say 50% of the problems here relate to improper
> DNS settings. I don't want to have to give "hints" to someone, and take
> multiple posts to figure out what could have been resolved in a single
> posting of their IP configuration.
>
> Matt Gibson – GSEC
>
>
>> IMO.
>> Tony
>>
>>
>>
>>
>>
>>
>> "Matt Gibson" wrote:
>>
>>> If all it takes to bring down a network is knowledge of the internal IP
>>> schema, then you're screwed from the get-go.
>>>
>>> Feel free to XXX out the public IP address, but any hacker hanging around
>>> here who wants to know what your IP address setup is, already has more
>>> information (Default server IP, default IP settings). We're trying to
>>> determine which people have incorrect default settings, and bring them
>>> back
>>> to the norm.
>>>
>>> Security by obscurity isn't any security at all. Especially when we're
>>> all
>>> basically the same here.
>>>
>>> Matt Gibson – GSEC
>>>
>>> "Tony Su" <TonySu@xxxxxxxxxxxxxxxxxxxxxxxxxxxx> wrote in message
>>> news:5B702688-54AB-418E-A084-429325C4DF8E@xxxxxxxxxxxxxxxxxxxx
>>> > Matt,
>>> > This question on whether to post IPCONFIG has been discussed to death.
>>> >
>>> > A short discussion which I participated is in Susan's blog archives.

Re: userenv and NETLOGON errors

>>>> I'm
>>>> not
>>>> the only person to question this practice, in summary the information
>>>> by
>>>> itself is not a fatal compromise but
>>>> – It's a substantial amount of very useful information to a hacker
>>>> – Like everything else posted to a public forum/Internet, the
>>>> information
>>>> lives forever.
>>>>
>>>> In other words, the exploit that uses the information may not be common
>>>> practice today, but if the information is still valid 8 years from now
>>>> and
>>>> the exploit is developed that uses that information, you'll regret what
>>>> you
>>>> thought was a minor indiscretion.
>>>>
>>>> Tony
>>>>
>>>>
>>>>
>>>>
>>>> "Matt Gibson" wrote:
>>>>
>>>>>
>>>>> Although others might disagree with me, I generally discourage
>>>>> posting
>>>>> IPCONFIGS for security reasons, but if there is no alternative the
>>>>> bottom
>>>>> line is getting fixed.
>>>>>
>>>>> Posting this makes people think there IS a security risk to it.
>>>>>
>>>>> You're spreading FUD, and making it harder for us to help people in
>>>>> this
>>>>> newsgroup.
>>>>>
>>>>> Please stop.
>>>>>
>>>>> Matt Gibson – GSEC
>>>>>
>>>>>
>>>>>
>>>>>
>>>>
>>>>
>>>>
>
>
>
.

- **Follow-Ups:**
 - ◆ **Re: userenv and NETLOGON errors**
 - ◇ From: SuperGumby [SBS MVP]

- **References:**
 - ◆ **userenv and NETLOGON errors**
 - ◇ From: jaredea
 - ◆ **Re: userenv and NETLOGON errors**
 - ◇ From: Matt Gibson
 - ◆ **Re: userenv and NETLOGON errors**
 - ◇ From: Tony Su
 - ◆ **Re: userenv and NETLOGON errors**
 - ◇ From: Matt Gibson
 - ◆ **Re: userenv and NETLOGON errors**
 - ◇ From: Tony Su
 - ◆ **Re: userenv and NETLOGON errors**
 - ◇ From: Matt Gibson
 - ◆ **Re: userenv and NETLOGON errors**
 - ◇ From: Tony Su
 - ◆ **Re: userenv and NETLOGON errors**
 - ◇ From: Matt Gibson

- Prev by Date: **Re: SPI Premium Edition – CEICW Error on NIC**
- Next by Date: **POP3 connection service times out**
- Previous by thread: **Re: userenv and NETLOGON errors**
- Next by thread: **Re: userenv and NETLOGON errors**
- Index(es):
 - ◆ **Date**
 - ◆ **Thread**