

## Re: enumerate NT/Win2k users from a linux machine

*Source:* <http://www.derkeiler.com/Mailing-Lists/securityfocus/pen-test/2001-07/0031.html>

---

**From:** Crist Clark ([crist.clark@globalstar.com](mailto:crist.clark@globalstar.com))

**Date:** 07/23/01

Message-ID: <3B5C8E84.6842A06D@globalstar.com>

Date: Mon, 23 Jul 2001 13:52:20 -0700

From: "Crist Clark" <[crist.clark@globalstar.com](mailto:crist.clark@globalstar.com)>

To: Chris Barber <[Cyber-Cop1@excite.com](mailto:Cyber-Cop1@excite.com)>, [pen-test@securityfocus.com](mailto:pen-test@securityfocus.com)

Subject: Re: enumerate NT/Win2k users from a linux machine

Chris Barber wrote:

>

> *Hi all;*

>

> *I have a client that uses primarily Linux workstations for the end users.*

> *They use NT and Win2K servers for the storage of many networked applications*

> *and data. One of the concerns they have is if users on the network would be*

> *able enumerate the login IDs on the NT/Win2k servers from the Linux*

> *workstations. I have not seen anything on the net lately that would do this*

> *but I thought I would ask those who do this kind of thing all of the time.*

> *I am not Pen-tester by trade but I do dabble from time to time (when I have*

> *some, time that is).*

>

> *Can anyone lend a hand?*

This is easiest to do from another WinXX machine since all of the libs are "just there." One really cool set of tools, UserInfo and UserDump, are at,

<http://www.hammerofgod.com/download.htm>

These work even if the null user has been restricted. The author, Thor, had some really fun talks at DEFCON.

A UNIX-based tool I've used is 'nat' (a.k.a. 'nbaudit') from,

<ftp://ftp.secnet.com/pub/tools/nat10/>

But I don't think it works against systems where the null user has been restricted. However, it is simply busy-work to reverse-engineer the WinXX-based tools to run on a UNIX-like system like Linux. I am not sure if this has been done.

--

Crist J. Clark

Network Security Engineer

Re: enumerate NT/Win2k users from a linux machine

SecurityFocus Penetration: Re: enumerate NT/Win2k users from a

[crist.clark@globalstar.com](mailto:crist.clark@globalstar.com)  
(408) 933-4387

Globalstar, L.P.  
FAX: (408) 933-4926

The information contained in this e-mail message is confidential, intended only for the use of the individual or entity named above. If the reader of this e-mail is not the intended recipient, or the employee or agent responsible to deliver it to the intended recipient, you are hereby notified that any review, dissemination, distribution or copying of this communication is strictly prohibited. If you have received this e-mail in error, please contact [postmaster@globalstar.com](mailto:postmaster@globalstar.com)

---

This list is provided by the SecurityFocus Security Intelligence Alert (SIA) Service. For more information on SecurityFocus' SIA service which automatically alerts you to the latest security vulnerabilities please see: <https://alerts.securityfocus.com/>

---

- **Previous message:** [Ken Pfeil: "RE: HP3000"](#)
- **In reply to:** [Chris Barber: "enumerate NT/Win2k users from a linux machine"](#)
- **Next in thread:** [Ulrich Keil: "Re: enumerate NT/Win2k users from a linux machine"](#)
- **Messages sorted by:** [\[ date \]](#) [\[ thread \]](#) [\[ subject \]](#) [\[ author \]](#) [\[ attachment \]](#)