

Re: brute-forcing NTLM HTTP Authentication

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/pen-test/2001-09/0286.html>

From: freehold@erols.com

Date: 09/29/01

Message-ID: <3BB633A4.16B1@erols.com>
Date: Sat, 29 Sep 2001 16:49:29 -0400
From: freehold@erols.com
To: Jason binger <cisspstudy@yahoo.com>
Subject: Re: brute-forcing NTLM HTTP Authentication

Lanman's challenge/response-based and it can cave when bruteforced. There was a patch released some time ago because of a potential Lophtrcrack brute-force between IIs & clients w/ WEC (ME & anything with Office2000). WEC didn't play nice with IE zone settings. Ditto a 2k telnet client/ntlm problem (the client is 'optional' but enabled by default I think). Ditto Netbios/ntlm. Windows sends the auths without telling users, another example of 'transparency' I guess? ;)

My favorite ntlm-for-dummies: <http://www.innovation.ch/java/ntlm.html>

Missy

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:** [Denis Ducamp: "Re: brute-forcing NTLM HTTP Authentication"](#)
- **In reply to:** [Jason binger: "brute-forcing NTLM HTTP Authentication"](#)
- **Messages sorted by:** [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#) [\[attachment \]](#)