

RE: Can you impersonate a client side cert??

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/pen-test/2002-01/0094.html>

From: Ed Moyle (emoyle@scsnet.csc.com)

Date: 01/28/02

Date: Mon, 28 Jan 2002 13:03:49 -0500

From: Ed Moyle <emoyle@scsnet.csc.com>

To: Darren Craig <darren.craig@celare.co.uk>, pen-test@securityfocus.com

Darren,

Most likely you won't be able to do this. The web server would have to trust the CA that you choose to issue your spurious cert. If you could get a cert from a CA that the server trusts with the same CN as whoever you are trying to impersonate, the built-in cert checking features of most web servers still would not let you impersonate the legitimate user provided they are using the built-in cert to user mapping features of the web server.

As a caveat, I should note that it is *possible* that some poorly written application software might use just CN without regard to issuing CA to do the user mapping (personally I would use SN as issued by a particular CA,) but my advice would be to pursue another avenue since this is a pretty big "if."

-E

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

From: Darren Craig [<mailto:darren.craig@celare.co.uk>]

Sent: Monday, January 28, 2002 07:00

To: pen-test@securityfocus.com

Subject: Can you impersonate a client side cert??

Hi All,

I have been reading a paper which was published back in Feb 2001 by a company call Sensepost which says that there is a way to impersonate a users client side cert by using the same common name. Does anybody have any experience of doing this or is it even possible considering that the users public part of the cert would be installed on the web server?

Darren

Privileged, confidential and/or copyright information may be contained in this e-mail. This e-mail is for the use only of the intended addressee. If you are not the intended addressee, or the person responsible for delivering it to the intended addressee, you may not copy, forward,

RE: Can you impersonate a client side cert??

SecurityFocus Penetration: RE: Can you impersonate a client side cert??

disclose or otherwise use it or any part of it in any way whatsoever, to do so is prohibited and may be unlawful.

If you receive this e-mail by mistake please advise the sender immediately by using the reply facility in your e-mail software. Celare Limited may monitor the content of e-mails sent and received via its network for the purposes of ensuring compliance with its policies and procedures.

This message is subject to and does not create or vary any contractual relationship between Celare Limited and you.

Thank you.

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/>

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:** [L Williams: "RE: Can you impersonate a client side cert??"](#)
- **Maybe in reply to:** [Bryan Allerdice: "RE: Can you impersonate a client side cert??"](#)
- **Next in thread:** [Jason Brvenik: "RE: Can you impersonate a client side cert??"](#)
- **Messages sorted by:** [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#) [\[attachment \]](#)