

RE: Pentesting a Citrix Network

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/pen-test/2002-03/0028.html>

From: Greg (greg@hoobie.net)

Date: 03/05/02

From: "Greg" <greg@hoobie.net>

To: "Erlend J. Leiknes" <nookie@online.no>, <pen-test@securityfocus.com>, "Franklin DeMatto" <franklin.lists@qDefense.com>

Date: Tue, 5 Mar 2002 18:32:06 -0000

Yes, that's what I have done in the past. The HTTP server is related to the 'published applications' function within Citrix. If you take a Citrix ICA client and attempt to list the published apps on a specified server you will see an HTTP POST request go to the Citrix HTTP server, I don't remember the script name but it is in a /scripts/ directory.

Set up your Citrix connection, from the client, as a TCP/IP+HTTP connection and you will be able to examine the requests (which are cleartext)

cheers

Greg

> -----Original Message-----

> From: Erlend J. Leiknes [<mailto:nookie@online.no>]

> Sent: 05 March 2002 05:42

> To: pen-test@securityfocus.com; Franklin DeMatto

> Subject: Re: Pentesting a Citrix Network

>

>

> What about setting up a citrix client, and then sniffing the data between them?

>

>

> ----- Original Message -----

> From: "Franklin DeMatto" <franklin.lists@qDefense.com>

> To: <pen-test@securityfocus.com>

> Sent: Sunday, March 03, 2002 10:53 PM

> Subject: Pentesting a Citrix Network

>

>

>> I'm pentesting a network that includes two Citrix servers on

>> Win 2k. As I

>> have no experience whatsoever with Citrix, I thought I'd ask if

>> anyone can

>> help me out. The servers listen on port 80, with the following banners:

SecurityFocus Penetration: RE: Pentesting a Citrix Network

>>
>> *HEAD / HTTP/1.0*
>>
>> *HTTP/1.1 400 Bad request*
>> *Server: Citrix Web PN Server*
>> *Date: xxxx*
>> *Connection: Close*
>>
>> *They also listen on the 1494 port (which is designated for citrix)*
>>
>> *I was unable to get it to respond to any HTTP request, by hand or with a*
>> *browser.*
>>
>> *I'd appreciate if anyone could help me with some of the following*
>> *questions*
>> *(again, they may be basic, I have never used Citrix):*
>>
>> *Which Citrix product is it? Is there a way to fingerprint it?*
>> *How do I get it to respond to HTTP requests?*
>> *Are there any information disclosure possibilities? How about*
>> *vulnerabilities (i.e. buffer overflows, etc.)?*
>>
>> *Any help would be very appreciated!*
>>
>>
>>
>> *Franklin DeMatto*
>> *Senior Analyst, qDefense Penetration Testing*
>> *<http://qDefense.com>*
>> *qDefense: Making Security Accessible*
>>
>>
>>
>

> --
>> *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)*

SecurityFocus Penetration: RE: Pentesting a Citrix Network

- > *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:*** [DrobyX: "Re: Pentesting a Citrix Network"](#)
- ***In reply to:*** [Erlend J. Leiknes: "Re: Pentesting a Citrix Network"](#)
- ***Next in thread:*** [DrobyX: "Re: Pentesting a Citrix Network"](#)
- ***Messages sorted by:*** [\[date \] \[thread \] \[subject \] \[author \] \[attachment \]](#)