

Re: Evading Client–Certificate Authentication

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/pen-test/2004-04/0004.html>

From: Jason (security_at_brvenik.com)

Date: 04/01/04

Date: Thu, 01 Apr 2004 14:02:19 -0500

To: Kevin Vanhaelen <blowfish448@hotmail.com>

- Do you know what web server it is?
- Any ideas how many issuing authorities it trusts?
- Does it trust a public CA?
- What validation does the web server does with the certificate?
- Does it rely on specific extensions for authentication?
- Can a forged DN get passed as a login and work?

Identifying the type of web server will help a lot here. From there you can look at business relationships to find out if there are cross organization trusts that might get you access to an issuing authority that the chain of trust validates. If you are dealing with MS crap then it is likely that the infrastructure is self signed and poorly maintained, keep fishing and look for a place to request certificates...

If it is another web server you still have hope, there is likely a default trust of the major trusted third parties, in this case getting your own cert from a different third party may grant you access. You might have to futz with different DN conventions or request a signed email to tell you what the convention in use is. The cert chain presented by the server may also provide clues on the conventions and extensions being used. Emulating the critical part of the DN structure in your new cert from a TTP might be sufficient. Having a cert issued by any TTP might be sufficient to get you access and then from there you resume normal operations. It really depends on the configuration.

Kevin Vanhaelen wrote:

- > *Hi to all,*
- >
- > *whilst in the middle of a Penetration Test I stumbled on a web server only*
- > *servicing SSL and demanding the client to present*
- > *a certificate to identify himself.*
- > *I tried to nikto it with sslproxy and browse the site thru paros both with a*
- > *temporary Verisign personal certificate.*
- > *No such luck, the server keeps bouncing me off. Even vulnerability scanners*
- > *like Nessus and Retina don't get passed*

SecurityFocus Penetration: Re: Evading Client–Certificate Authentication

> *the port–scan portion.*
>
> *Does anyone have an idea to further assess this server? Am I looking at a*
> *mission impossible here maybe?*
>
> *Thanks,*
>
> *~kevin*
>
>

> *You're a pen tester, but is google.com still your R&D team?*
> *Now you can get trustworthy commercial–grade exploits and the latest*
> *techniques from a world–class research group.*
> *www.coresecurity.com/promos/sf_ept1*
>

>
>

You're a pen tester, but is google.com still your R&D team?
Now you can get trustworthy commercial–grade exploits and the latest
techniques from a world–class research group.
www.coresecurity.com/promos/sf_ept1
