

## RE: Penetration test of 1 IP address

---

*Source:* <http://www.derkeiler.com/Mailing-Lists/securityfocus/pen-test/2006-02/msg00158.html>

---

- *From:* Edmond Chow <[echow@xxxxxxxxxxxxx](mailto:echow@xxxxxxxxxxxxx)>
  - *Date:* Thu, 09 Feb 2006 08:09:21 -0500
- 

Hello Daniel,

Thanks to you and all the other helpful (yes, there were a few less than helpful!) posters.

You are right in that this is a "capture the flag" project. It's a law firm that wants to make sure that the WebBlaze application is secure before putting it into production.

The login screen is a typical windows logon screen with user name and password prompt. It does not look like the login screen found on the webblaze web site.

Thanks again!

Regards,

Edmond

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

From: Daniel Grzelak [<mailto:daniel.grzelak@xxxxxxxxxxxxx>]

Sent: Wednesday, February 08, 2006 10:54 PM

To: pen-test@xxxxxxxxxxxxx

Cc: 'Edmond Chow'; 'Michael Gargiullo'

Subject: RE: Penetration test of 1 IP address

Hi Edmond,

I'm sure there will be a vast and many responses to your question with regards to carrying out the actual testing phase of the engagement so I will concentrate on something else. I am making a very big assumption based on your wording but I believe the major issue you have with this engagement centres around scoping. I apologise if I unnecessarily trivialise your original post.

"I have been asked to perform a security audit of 1 IP address for client."

RE: Penetration test of 1 IP address

This statement sounds like a misunderstanding waiting to happen. In general a security audit is considered a review of a system with all relevant information provided. For instance, system configuration, file system access control list, user lists etc. It will also tend to relate to a system rather than an IP.

From what I gather, you are being asked to conduct a blind penetration test

of a single IP. As such you are being provided very little information and probably being asked to "capture the flag". This can be a very delicate point. Make sure you know the limitations of the testing you have been asked to perform. Is it just a vulnerability assessment, or are you tasked with taking full control of the system. There are of course legal issues which have been addressed previously on this list and various sources on the web.

Since you have been provided a clue of webblaze, that may indicate that only that particular application is to be tested. If so, it is important to agree on what constitutes such testing. Is this really a system penetration test or an application penetration test? The two can differ greatly in the amount of assurance you can provide the client on a particular component.

Finally, blind testing is not always the most effective way to go. Given a narrow scope and access to only a login page, the client may not gain much from your testing. Perhaps you should agree that upon completion of the blind testing, the client will provide a number of logins of varying access levels to allow you to perform a more in-depth analysis.

I know this doesn't directly address your question, but hopefully it will help in the preparations you need to make prior to executing an engagement.

Daniel.

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

From: Edmond Chow [<mailto:echow@xxxxxxxxxxxxx>]  
Sent: Wednesday, 8 February 2006 5:45 PM  
To: 'Michael Gargiullo'; pen-test@xxxxxxxxxxxxxxxxxxxxx  
Cc: 'Edmond Chow'  
Subject: RE: Penetration test of 1 IP address

To all:

I have been asked to perform a security audit of 1 IP address for client. They have given me the 1 IP address and a clue (webblaze).

If I enter the IP address and then /webblaze, I am taken to a login page

RE: Penetration test of 1 IP address

RE: Penetration test of 1 IP address

(user name and password requested).

What tools would you recommend that I use for this assignment?

Thanks for your help.

Regards,

Edmond

---

Audit your website security with Acunetix Web Vulnerability Scanner:

Hackers are concentrating their efforts on attacking applications on your website. Up to 75% of cyber attacks are launched on shopping carts, forms, login pages, dynamic content etc. Firewalls, SSL and locked-down servers are futile against web application hacking. Check your website for vulnerabilities to SQL injection, Cross site scripting and other web attacks before hackers do! Download Trial at:

[http://www.securityfocus.com/sponsor/pen-test\\_050831](http://www.securityfocus.com/sponsor/pen-test_050831)

---