

RE: Using viruses in pen-test

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/pen-test/2006-10/msg00164.html>

- *From:* "Clint Laskowski" <clint@xxxxxxxxxxxxx>
 - *Date:* Wed, 11 Oct 2006 23:28:00 -0500
-

Do not write your own code to test your client's antivirus controls. Use the EICAR test files (<http://www.eicar.org/>) as previously described by 'kev'. If you write a test virus and it gets loose and does something stupid, you'll have no one to blame but yourself. Even if it is relatively harmless, if it gets out you'll be facing charges of abuse of bandwidth, etc. It is not worth it.

If your goal is to see if users open email that they shouldn't, consider sending an HTML email message with a 1x1 pixel image pulled from your website. Use a unique file name for the image that will only be used in the test. Then, after allowing enough time for the users to open the message, check your weblogs to see if the image was downloaded, and at what time. Even better, have unique file names for each email you send out. That way you can tell who read the email ... or at least the fact that a specific email (sent to a specific person) was read at a specific time. However, keep in mind this approach was apparently used by HP recently (see http://news.zdnet.com/2100-1009_22-6121048.html) using a service called ReadNotify, and look where it got them!

Use these concepts at your own risk!

-- clint

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

From: listbounce@xxxxxxxxxxxxxxxxxxxxx [<mailto:listbounce@xxxxxxxxxxxxxxxxxxxxx>] On Behalf Of David Swafford
Sent: Wednesday, October 11, 2006 4:13 PM
To: neo anderson; pen-test@xxxxxxxxxxxxxxxxxxxxx
Subject: Re: Using viruses in pen-test

I wonder if there is some type of "fake" virus you could use in this case. I know in a pen test you are hired to do the job asked, but I would hate for you to have to face your client after a "pen test gone bad" kind of situation where something backfired leaving the whole network in shambles from a massive virus outbreak. Clients sometimes don't always understand what they are truly asking (ie. the impact it might cause). I'm not sure how skilled you are at writing code but the option of writing a new virus which simulated something dangerous (but didn't actually damage anything

RE: Using viruses in pen-test

valuable) might be a way to test to see if the anti-virus software doing its job on the "zero day" part (based on heuristic scanning).

David.

David A. Swafford, Network Engineer
Information Technology Team
Archbishop Alter High School

EC-Council Certified Ethical Hacker

A Cisco Systems, Inc., Certified Network Associate (CCNA) and a CompTIA
Network+ and Security+ Certified Professional

"neo anderson" <amol.netsec@xxxxxxxxxx> 10/11/2006 3:08
am >>>

Hi List,

I wish to know your views on "Using viruses in pen-test" I
I've been working in the infosec domain for over 2 years with a couple
of infosec certs including CEH and conducting pen-tests for my clients
for about a year.

My recent client has hired me for carrying out "every possible" type
of pen test.

This includes testing organizations defence mechanism against viruses
as well, this includes to test whether anti-virus administrators have
up-to-date virus definitions etc. I'm supposed to gather this
information by means of thorough penetration tests only.

As we all are aware that how the viruses (worms/trojans included)
enter into the corporate network propagate over LAN. There are many
ways like email attachments or infected content brought in by
employee. It spreads on itself thereafter.

Now my question:

Is there any standard procedure to test the posture of organizations
network security against potential virus threats? I mean i wish to
know about pen-test carried out against Antivirus-product. In order to
replicate itself, a virus must be permitted to execute code and/or
write to memory. Thus this pen-test should also tests that.
And do I need to use some known viruses for this kind of pen-test?

Have your thoughts on this topic please.
Thanking you all.

RE: Using viruses in pen-test

This List Sponsored by: Cenzic

Need to secure your web apps?

Cenzic Hailstorm finds vulnerabilities fast.

Click the link to buy it, try it or download Hailstorm for FREE.

http://www.cenzic.com/products_services/download_hailstorm.php?camp=701600000008bOW

Note: this message has been scanned for viruses and mal-ware prior to leaving the Archbishop Alter High School Information Technology Network. Please report all possible solicitation and infected messages to abuse@xxxxxxxxxxxxxxxxxxxxx, Thank you.

This List Sponsored by: Cenzic

Need to secure your web apps?

Cenzic Hailstorm finds vulnerabilities fast.

Click the link to buy it, try it or download Hailstorm for FREE.

http://www.cenzic.com/products_services/download_hailstorm.php?camp=701600000008bOW

This List Sponsored by: Cenzic

Need to secure your web apps?

Cenzic Hailstorm finds vulnerabilities fast.

Click the link to buy it, try it or download Hailstorm for FREE.

http://www.cenzic.com/products_services/download_hailstorm.php?camp=701600000008bOW
