

RE: VmWare and Pen-test Learning

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/pen-test/2006-08/msg00161.html>

- *From:* <saalexander@xxxxxxxxxxxxxxxx>
 - *Date:* Mon, 7 Aug 2006 09:18:10 -0700
-

A handful of suggestions:

1) Setup a Snort box. Use Snort to monitor your pen-test practice. What scans and exploits will Snort detect? Can you avoid this? Is there something that Snort doesn't detect that you can write a rule for?

2) Use Nmap. Experiment with different scanning options. Sniff the traffic and look at it. Do you understand the difference between the different scan types? Use OS identification and service detection. Are the results correct? Read Fyodor's papers on scanning and OS identification:

The Art of Scanning: <http://www.phrack.org/phrack/51/P51-11>

Remote OS detection via TCP/IP Stack Fingerprinting:

<http://www.phrack.org/phrack/54/P54-09>

3) Find some exploits that will allow you to remotely compromise your test machines. Use them. What happens? Do you have administrative access?

4) Setup a tftp server on your client machine. Use the tftp server to hold any tools you'll need to put on to a compromised machine. From the compromised servers, use the tftp client to download your tools. What other methods can you use to get your tools? Try using windows file sharing from the command line. What about NFS on Unix?

5a) On Unix, copy /etc/shadow (and/or /etc/passwd, /etc/master.passwd). Use John the Ripper (www.openwall.com) to crack the passwords. Experiment with some of the different options available in John (dictionary attacks, brute force, single mode). You may as well setup some additional accounts on the machine first. Use a combination of simple and complex passwords. How long does it take to crack them? Is it what you expected? Can you enable a different password hash rather than crypt(3); perhaps md5crypt or bcrypt (blowfish). How much longer does it take to crack these hashes if you use the same passwords? Note: You'll have to *change* the passwords once a new hash is set as the default for the system; just reuse the same passwords for comparison.

5b) On Windows, use pwdump, lsadump and creddump to recover password

RE: VmWare and Pen-test Learning

hashes (or in the case of creddump, cleartext passwords). Use John the Ripper and L0phtCrack to brute-force the passwords. Google for Rainbow Tables. Generate your own tables and use them with Cain and Abel to crack the passwords. It should be much faster. Do you realize why Rainbow Tables are a big deal? Be sure to take a good look at Cain in step 13 below.

5c) This is a shameless plug. Read:

<http://www.usenix.org/publications/login/2004-06/pdfs/alexander.pdf>

6) Use netcat to bind a command shell to a port. Telnet to it (or use netcat) to verify that it works. Then, use netcat to listen on your client machine and run netcat on the server to open a connection to the client and bind the command shell to that connection. In the first case, you can connect in to the server and get command line access. In the second situation, netcat is calling out to the client. Do you understand why this matters?

7) Pretend that one of your servers (server A) is behind a firewall. Pretend that you can access this machine from one of your other servers (server B). Use netcat and/or fpipe to redirect ports on server B so that you can scan/attack one or more services directly from your client machine.

8) Setup and use Nessus. What vulnerabilities does it report? Can you verify them manually?

9) Use Ettercap to play man-in-the-middle. Capture passwords from a telnet, ftp and/or pop3 connection to one of your servers. Do you know how and why the attack works? Google is your friend.

10) Go to www.smashguard.org. Click on The Buffer Overflow Page. Read "How to Write Buffer Overflows" by Mudge and "Smashing the Stack for Fun and Profit" by Aleph One. Try to write a simple stack-based buffer overflow. This will require that you know C and a bit of assembly. Also, this will probably be easiest on an older Linux distro (without stack randomization or any other stopgaps).

10b) On www.smashguard.org, under Famous Buffer Overflow Vulnerabilities and Worms, read Spafford's analysis of the Internet Worm. It's old but it should still give you some insight into how an automated attack can work. Read some of the other articles/reports under that heading. Do you understand the attacks?

11) Focus on specific services (MySQL, IIS). What can you do to attack these services? What can you do to prevent the attacks?

12) This should probably be earlier on the list but...Purchase one or more books such as Hacking Exposed. Try some of the attacks and tools in the book. Sniff the traffic and/or research the attacks. How do they work? Can you prevent them?

RE: VmWare and Pen-test Learning

13) Go to www.sectools.org/. Download tools that sound interesting. Experiment, have fun.

Good luck,

Steven

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

From: Erin Carroll [<mailto:amoeba@xxxxxxxxxxxxxxxx>]

Sent: Sunday, August 06, 2006 5:59 PM

To: 'IRM'; pen-test@xxxxxxxxxxxxxxxx

Subject: RE: VmWare and Pen-test Learning

Welcome to the pen-test world John.

Now before everyone freaks out about why I let essentially a basic newbie question on the list here's why and what kind of responses I was hoping for:

I like to play pool. But in order to get better I do lots of drills of simple shots over and over. Some people prefer to practice in other ways. In a similar vein, what types of exercises should John do to increase his skills and expand his knowledge? I know how I practice my pen-test skills to stay sharp but hearing some other methods people use might give me some ideas or other ways to tackle things.

So, he's got Vmware and a couple of images to play with. What kinds of drills should he work on?

Erin Carroll

Moderator

SecurityFocus pen-test list

"Do Not Taunt Happy-Fun Ball"

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

From: IRM [<mailto:irm@xxxxxxxxxxxxxxxx>]

Sent: Sunday, August 06, 2006 1:58 AM

To: pen-test@xxxxxxxxxxxxxxxx

Subject: VmWare and Pen-test Learning

Hi all,

I would like to learn about Penetration testing or maybe Vulnerability

RE: VmWare and Pen-test Learning

Assessment (?) or whatever it is called. I have set up a few machines on VMWare – Windows 2000 Server, Windows 2003 Server and Solaris 9.0. These machines are unpatched with no updates or service pack.

Basically what I would like to achieve in this task is to demonstrate that these machine are not secured. Thus by using a well-known exploit

that are available in the public space , people can easily exploit the

system and gain administrator privilege either by Local exploit or Remote Exploit.

Now, the question is that, where to start? Can people suggest me where

should I start?

Should I start using Nessus and identify all the vulnerabilities that are applicable on these machines? And start to do some research on securityfocus.com i.e. to find the exploit?

Or maybe if there is a list of vulnerabilities for each of the operating system, I think that would be great! Because I know that Unicode Exploit on IIS 4.0 is quite famous at that time. Is there similar thing on Windows 2003? Is there a list available like TOP 10 Exploit or something?

Cheers,
John

This List Sponsored by: CenZic

Concerned about Web Application Security?
Why not go with the #1 solution – CenZic, the only one to win the Analyst's Choice Award from eWeek. As attacks through web applications

RE: VmWare and Pen-test Learning

continue to rise, you need to proactively protect your applications from hackers. Cenzic has the most comprehensive solutions to meet your

application security penetration testing and vulnerability management needs. You have an option to go with a managed service (Cenzic ClickToSecure) or an enterprise software (Cenzic Hailstorm). Download FREE whitepaper on how a managed service can help you: http://www.cenzic.com/news_events/wpappsec.php And, now for a limited time we can do a FREE audit for you to confirm your results from other product. Contact us at request@xxxxxxxxxx for details.

—
No virus found in this incoming message.
Checked by AVG Free Edition.
Version: 7.1.394 / Virus Database: 268.10.7/410 – Release
Date: 8/5/2006

—
No virus found in this outgoing message.
Checked by AVG Free Edition.
Version: 7.1.394 / Virus Database: 268.10.7/410 – Release Date: 8/5/2006

This List Sponsored by: Cenzic

Concerned about Web Application Security?
Why not go with the #1 solution – Cenzic, the only one to win the Analyst's Choice Award from eWeek. As attacks through web applications continue to rise, you need to proactively protect your applications from hackers. Cenzic has the most comprehensive solutions to meet your application security penetration testing and vulnerability management needs. You have an option to go with a managed service (Cenzic ClickToSecure) or an enterprise software (Cenzic Hailstorm). Download FREE whitepaper on how a managed service can

RE: VmWare and Pen-test Learning

help you: http://www.cenzic.com/news_events/wpappsec.php

And, now for a limited time we can do a FREE audit for you to confirm your results from other product. Contact us at request@xxxxxxxxxx for details.

This List Sponsored by: Cenzic

Concerned about Web Application Security?

Why not go with the #1 solution – Cenzic, the only one to win the Analyst's Choice Award from eWeek. As attacks through web applications continue to rise, you need to proactively protect your applications from hackers. Cenzic has the most comprehensive solutions to meet your application security penetration testing and vulnerability management needs. You have an option to go with a managed service (Cenzic ClickToSecure) or an enterprise software (Cenzic Hailstorm). Download FREE whitepaper on how a managed service can help you: http://www.cenzic.com/news_events/wpappsec.php

And, now for a limited time we can do a FREE audit for you to confirm your results from other product. Contact us at request@xxxxxxxxxx for details.
