

RE: Hacking Demo and Test Lab

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/pen-test/2004-06/0075.html>

From: Victor Chapela (victor_at_sm4rt.com)

Date: 06/11/04

To: "'raza sharif'" <raza@raza.demon.co.uk>, <pen-test@securityfocus.com>

Date: Fri, 11 Jun 2004 12:59:54 -0500

I am not sure about VMWare, I also had some problems running demos consistently and decided to use a separate machine.

I usually do my demos with a similar configuration XP -> 2000.

A good 5 min sketch is:

- get a remote shell using Jill, iis5hack or dcomexploit
- You end up as NT Authority/SYSTEM in all cases, therefore you can add yourself as an administrator
- connect to the admin\$ share using your new credentials
- dump the SAM file with pwdump3
- crack some hashes using john
- copy winvnc to system32
- add your vnc password to the remote registry
- install and start winvnc remotely
- start a VNC session

Even though you will rarely need to install vnc while pen testing, I have found that for demos it is a very good way to get the point through.

Good luck

Victor

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

From: raza sharif [<mailto:raza@raza.demon.co.uk>]

Sent: Friday, June 11, 2004 6:42 AM

To: pen-test@securityfocus.com

Subject: Hacking Demo and Test Lab

Hi Folks ,

Im doing some advanced Hacking Demos for management and also Corporates etc.

I have a installed windows 2000 server and iis 5.0 on VMWARE GSX server.

Im using Webdav and other exploits that all basically should spawn a shell

RE: Hacking Demo and Test Lab

SecurityFocus Penetration: RE: Hacking Demo and Test Lab

using netcat.

Im using XP as my attacking machine.

Prob at the moment is Netcat will not spawn a shell regardless of what i try.

Any ideas ? i checked the install it is windows 2000 500.1295 no reference to service packs etc. it's a default install.

Also what are good demo's etc to run to show real hacking on windows 2000 , iis etc..that i can get to work

thanks

Raza

Raza@raza.demon.co.uk