Penetration Testing with Metasploit Framework

Revision 1.2 02 Feb 2005

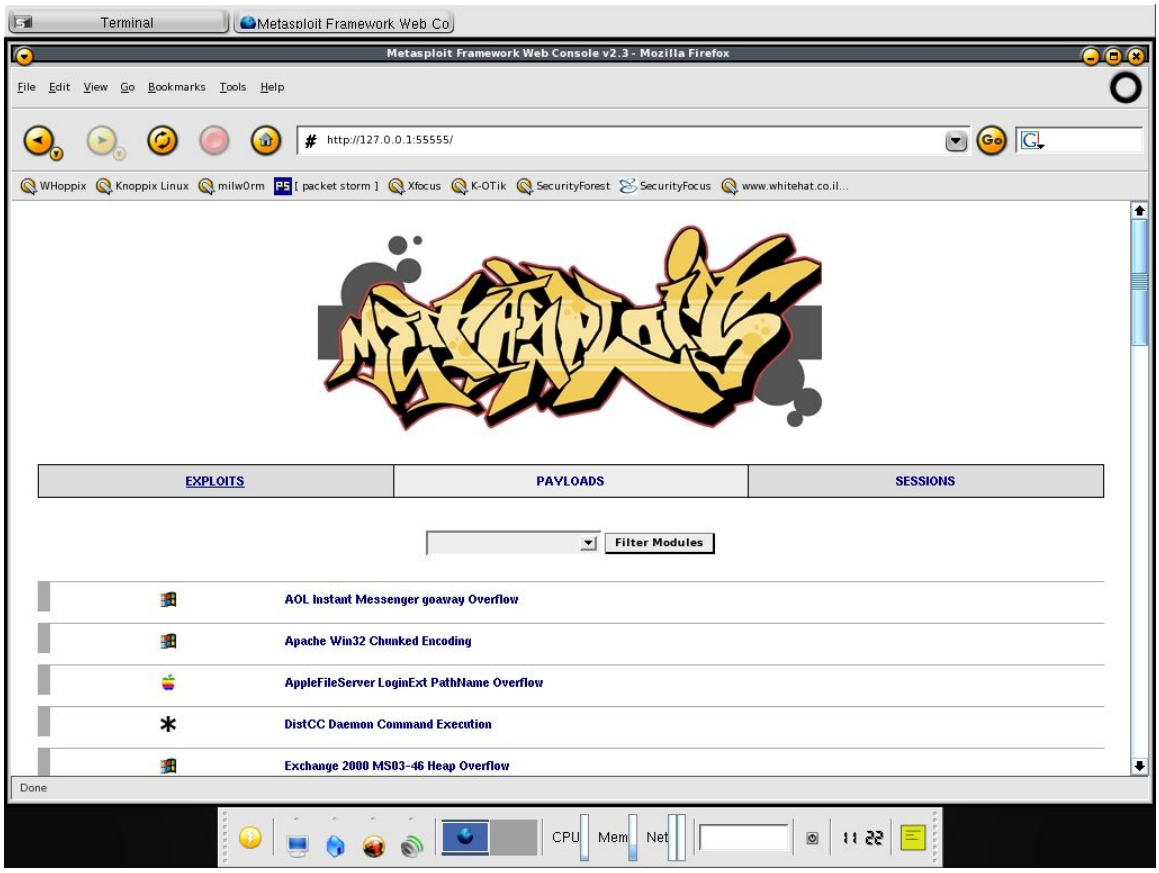

Figure 1

Laboratory Overview

Objective

At the end of this lab, students will be able to understand how attackers choose exploits which penetrate the selected target's given operating system vulnerability.

Information for Laboratory

This laboratory experience guides students through using an appropriate exploit to attack a vulnerability in an arbitrarily chosen operating system which has been attached to a network environment. The selected target operating system is Microsoft's Windows 2000 Server Standard Edition. The exploitation and vulnerability library and management system is Metasploit Project's Framework (freely available from http://www.metasploit.com in both Linux and Win32 versions), using the version, 2.3, most current at time of this writing. Laboratory facilitation in an existing Win32-based classroom will be eased by the use of the muts product White Hat Knoppix (WHoppix) (http://www.whoppix.com), a bootable CD remaster of Klaus Knopper's Knoppix distribution of Debian Linux. WHoppix quite handily includes the Framework product, and many other security and penetration testing tools, already pre-installed and immediately usable on any computer workstation system without disturbing the natively-installed operating system, such as Windows, already present on the machine's hard disk drive.

Student Preparation

The student should already be familiar with Windows 2000 Server operation and administration, particularly the facility for adding users and groups and adjusting their rights and permissions. Some familiarity with Linux command-line and graphical user interfaces would be helpful. In any case, step-by-step procedures and figures for both operating systems will be presented.

Instructor Preparation

Before class, the instructor or a lab assistant will ensure that each laboratory workstation has Windows 2000 Server loaded, with the service pack 4 (but no further subsequent patches) applied, that the network physical and logical configuration is complete, and that copies of the bootable CD media for Whoppix are available. Students may work in pairs, with one

student being the Win32 victim, and the other the Linux attacker.

Warning Will Robinson

Do not be surprised if upper management at your institution takes a dim view of conducting these activities on your production network, or even at all. Typical knee-jerk reactions include such conclusions as, “Well now, if we allow teaching our students penetration techniques, next thing we know, they’ll be changing their grades to all A’s, and issuing themselves $1000 tuition refund checks.” The use of isolated, air-gapped networks, or placing labs behind a VLAN, seems to satisfy most managers. You may already be using these techniques in your Microsoft, Linux, or Cisco classes to avoid such unpleasantries as finding users in the library receiving worthless DHCP addresses from your MCSE server class lab. The use of operating system partitioning software, such as VMware Workstation, or Microsoft Virtual PC, carries the additional advantages of warranting that such potentially offensive network traffic never touches a real wire, and allows cross-platform labs such as this to be totally realizable on a single lab workstation. Free 30-day fully functioning evaluation copies for both the Linux and Win32 platforms of the VMware partitioning products are available, for both currently shipping and next-generation beta versions, at http://www.vmware.com. Microsoft offers a 45-day demo of their Virtual PC at http://www.microsoft.com/windows/virtualpc/downloads/trial.mspx

Estimated Completion Time

45 Minutes

Penetration Testing

Network managers frequently employ penetrating testing to assess how well their change control systems are keeping up with applying up-to-date patches and service packs to their network servers, workstations, routers, and switches. By utilizing either in-house talent, or hiring third-party expertise, to attempt to bypass security measures and gain access to critical systems and data, any observed weaknesses can thus be mitigated. The student can benefit both the sanctity of his own personal data, as well as enhancing his employability in an increasingly security conscious and demanding industry.

Free and Commercial Software

The Framework application software and the Linux operating system both fall under the concept of Free and Open Source Software (FOSS). Such software is freely available, may be copied and redistributed, and includes full source code, which you may study or modify. Commercial closed-source products also exist that can perform the same job. The Microsoft Windows 2000 Server product is closed-source and normally rather expensive, but in the academic world, low-cost or free versions are often available, such as the Select licensing program, or the MSDN Academic Alliance, which allows students in qualifying (i.e., computer science) classes to obtain media loans, downloads, or low-cost purchased copies of several useful MS products, such as various Windows workstation and server versions, and the Visio network diagram tool (but, unfortunately, no *other* parts of the popular MS Office suite). The VMware partitioning software vendor offers academic pricing and, occasionally, free single copies to instructors.

Step 1: Verify Existing Users and Groups on the Windows Server

Log into the Microsoft Windows 2000 Server console with the administrator username and password. When the desktop appears, click <start> <settings> <control panel> <administrative tools> <computer management>. Click the

square + to the left of ‘local users and groups’, then ‘users’ in the left pane of the MMC (fig. 2) and observe which users are currently listed in the right pane.

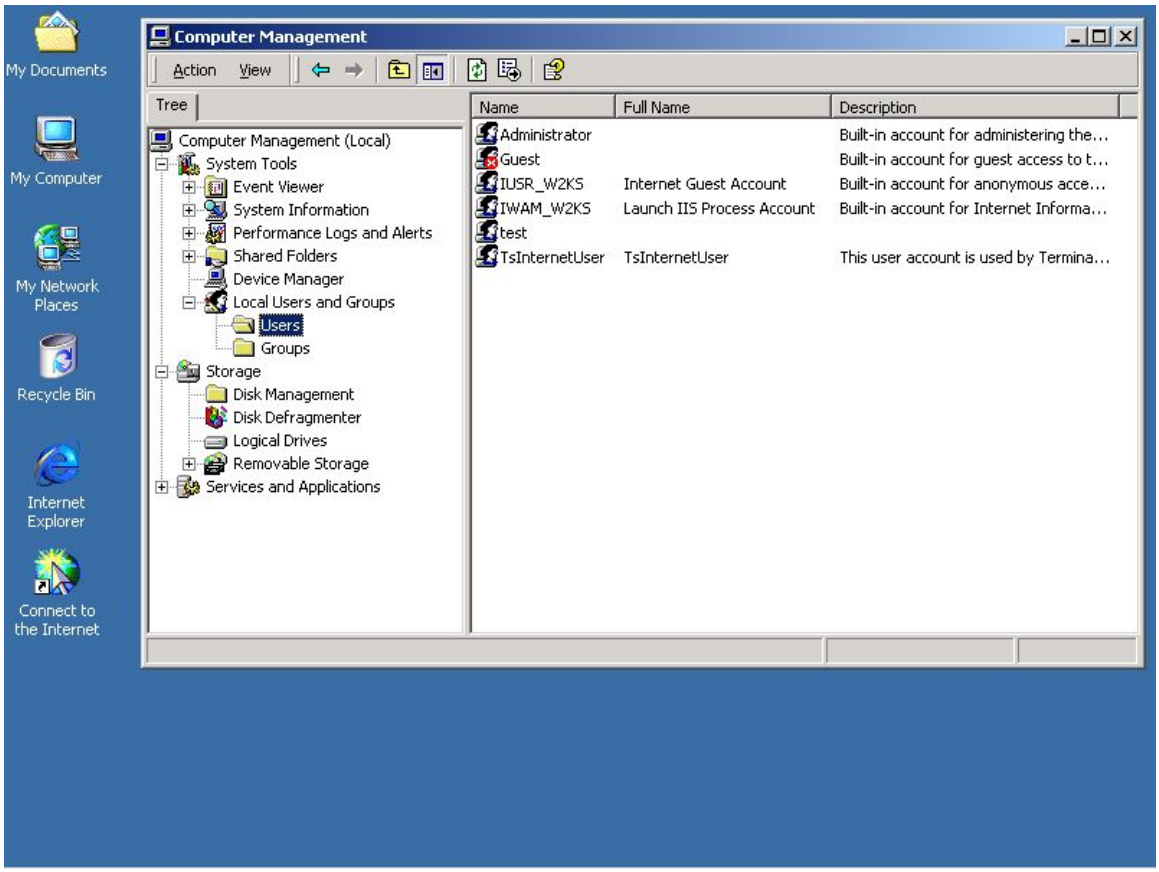

Figure 2

Step 2: Determine the network address of the Windows Server

Bring up the console terminal (<start> <programs> <accessories> <command prompt>) and type in:

```
C:\>ipconfig<enter>
```

and take note (fig. 3) of this host’s IP address as the attacker’s target address. On this host the IP address is 192.168.0.102/24. We’ll need to be sure this address is reachable from the Linux host later.

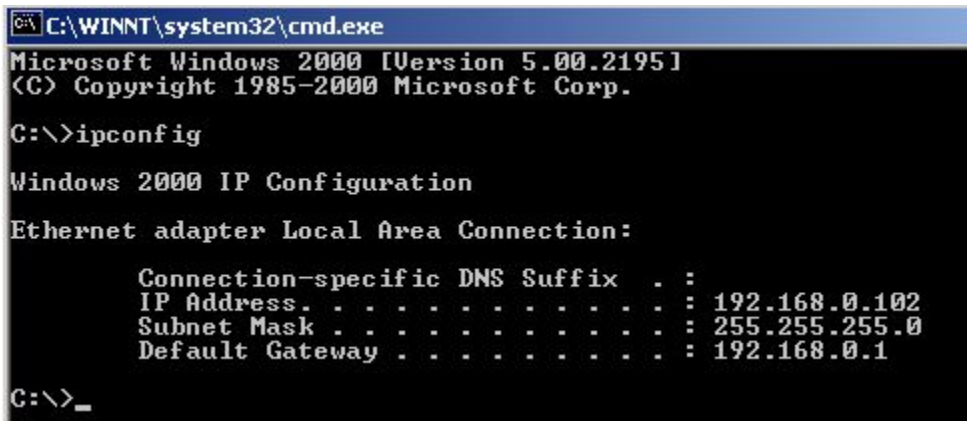

Figure 3

Step 3: Boot the WHoppix distribution CD on the 2nd PC

It might be necessary to enter the workstation's CMOS setup utility and configure the boot order so that the CD-ROM drive appears before the hard disk drive. Once the CD media successfully boots, you'll see the image in Figure 4.

Figure 4

With most reasonably modern ‘iron’, simply pressing the enter key, or just waiting a few seconds, will work fine after loading the default drivers. If you have a laptop, you’ll likely need to press the F2 or F3 keys here to look for a boot-time option that will help you get started. After two or three moments of loading, the Whoppix desktop of Fig. 5 will appear. NOTE: if you need to apply a static address (in other words, if you are NOT in a DHCP environment) to the Whoppix desktop, STOP and go to STEP X further down, then return here to continue.

Step 4: Execute the Framework application

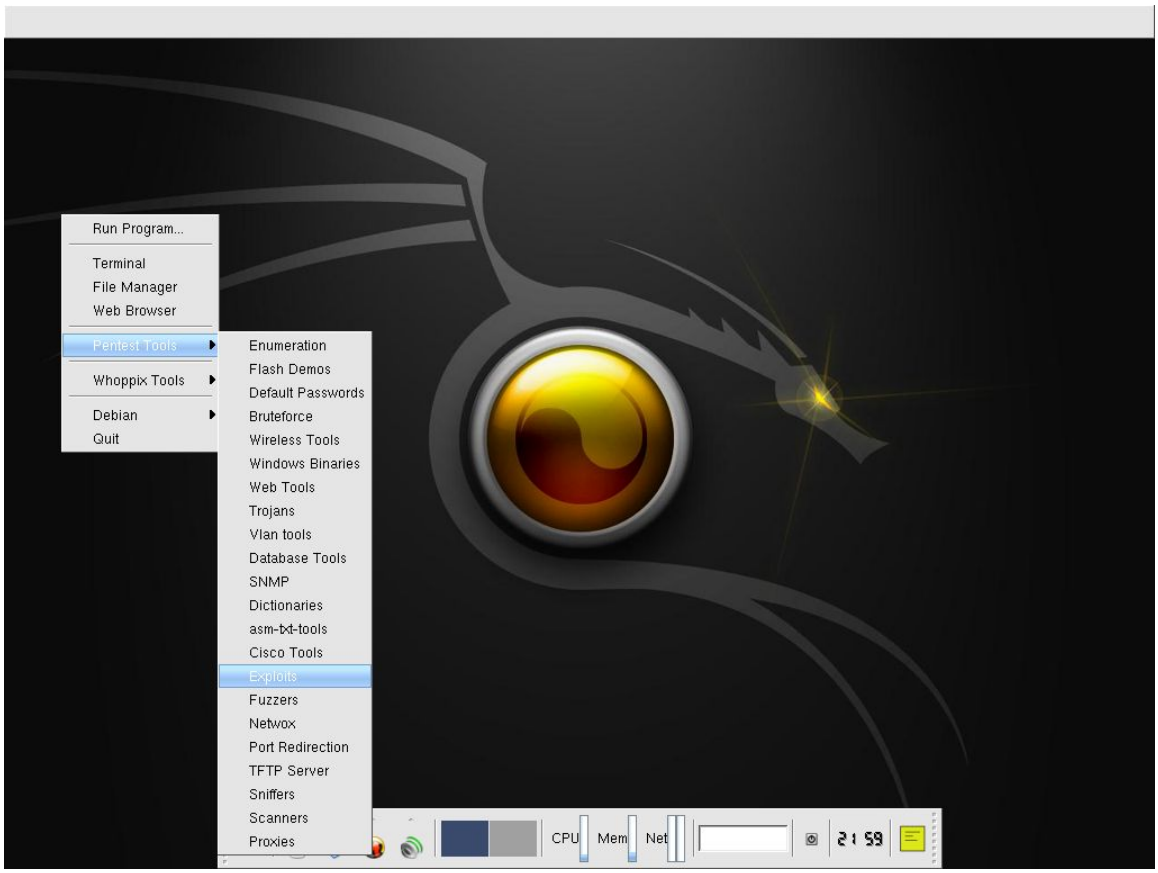

Figure 5

Right-click, moving the mouse pointer to ‘Pentest Tools’, then to ‘Exploits’, then right- or left-clicking. The text console of Figure 6 appears, and you type in the following commands as shown:

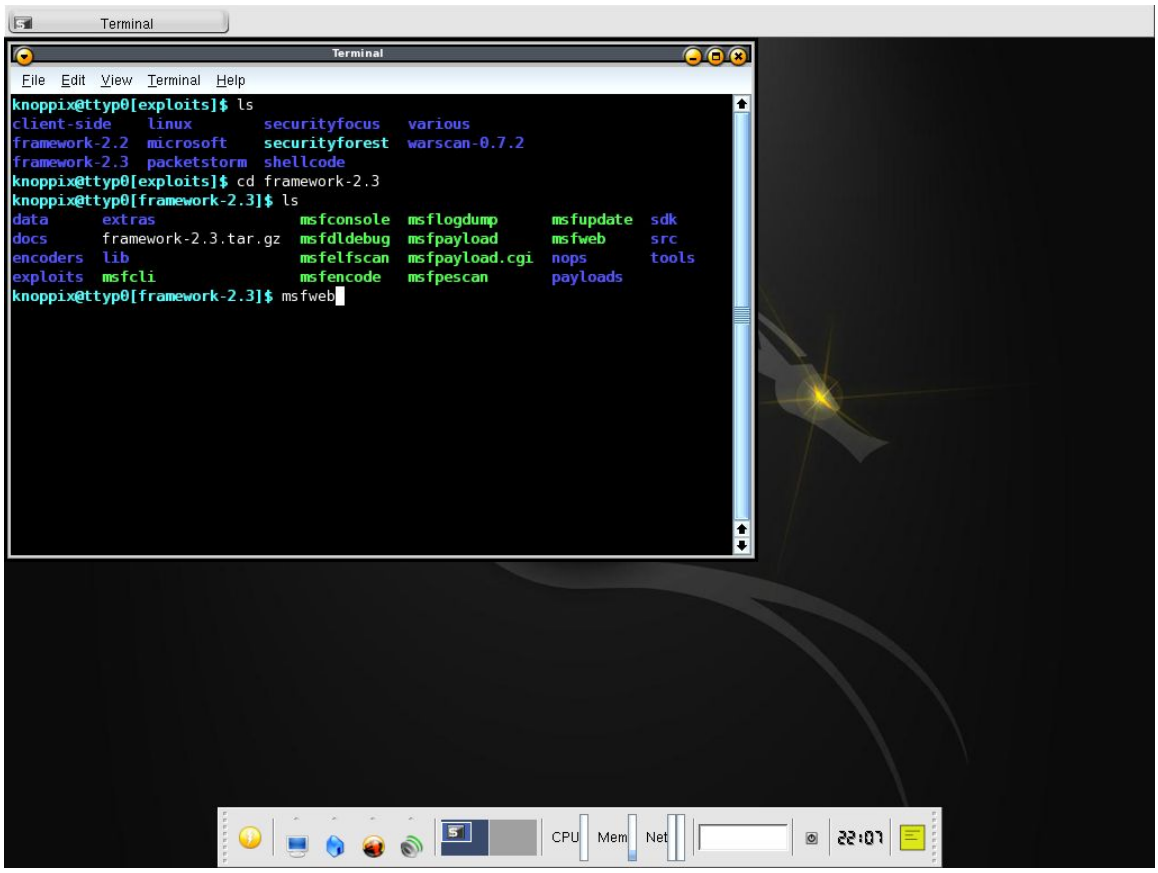

Figure 6

ping 192.168.0.102<enter> (verifies host connectivity)
ls<enter> (shows spelling of next directory to change to)
cd framework-2.3<enter> (changes to next dir)
ls<enter> (shows spelling of application to execute)
msfweb<enter> (executes the framework app)

Now that the application is running, in the form of a web server interface, the next step is to start a web browser. WHoppix includes the Mozilla FireFox browser, easily startable by selecting the toolbar-like icon near the bottom, with the orange dinosaur head. Enter a URL of
http://127.0.0.1:55555<enter>
The browser will display the image of Figure 1.

Step 5: Select and configure an exploit

Now we'll select a suitable exploit for our intended target. Scroll down and click (Fig. 7) the Local Security Authority Sub System exploit 'Microsoft LSASS MS04-011 Overflow'

Figure 7

When the screen of Fig 8 appears, select target '1-Windows 2000':

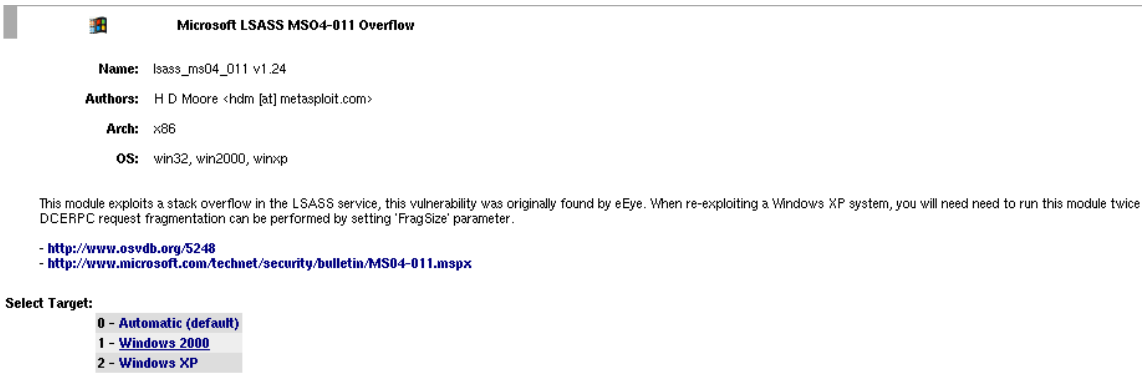

Figure 8

Now we'll choose a payload for the exploit to deliver to our target. In this case, it's the top line (Fig. 9), the 'win32_adduser', which will add an arbitrary username and password to the local administrator's group (remember this one the next time you're locked out of a server for not knowing the admin password).

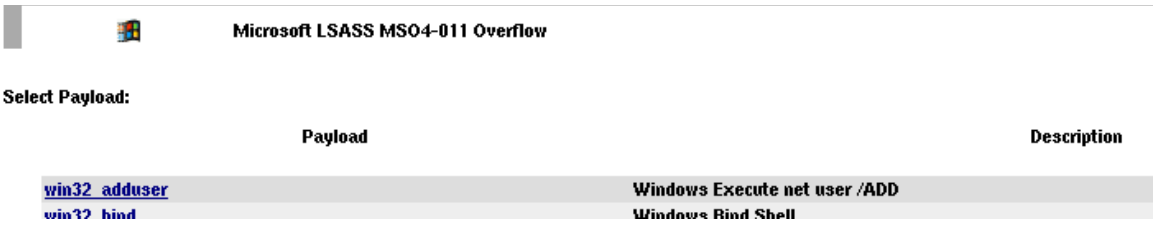

Figure 9

In the next screen (Fig. 10), we'll add details and then launch the attack. Using the target's IP address we noted before, fill out the form as shown:

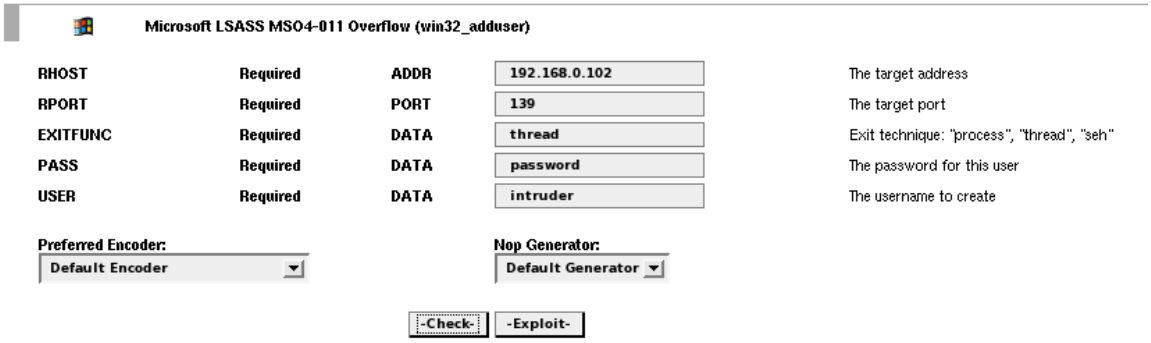

Figure 10

We'll need to add the RHOST ADDR of **`192.168.0.102`**, and the PASS DATA (**`password`**) and USER DATA (**`intruder`**) we arbitrarily choose to inject into the target machine's registry. Then, click the '–Exploit-' button and wait a few seconds.

Step 6: Inspect the Target for results

Using the procedure already outlined in **Step 1**, above, see if our intruder user is present (Fig. 11). And, it appears the new user is present, and is a member of the local administrator's group, which means he now has pretty much full rein on the unwitting target machine. And that's with Service Pack 4 already installed! What's that, you say? Off for a quick check on that production 2000 server you're responsible for, are you? Better brush up on that change control policy, too.

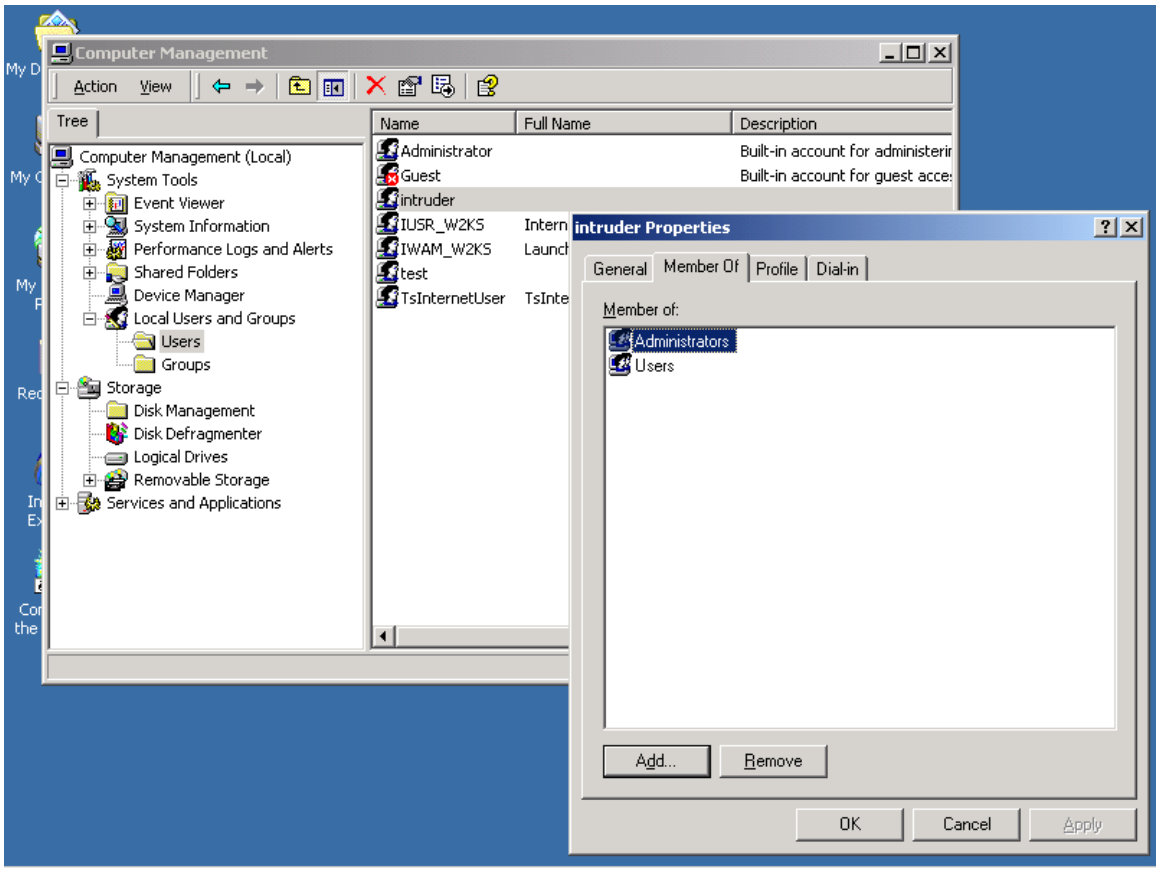

Figure 11

Step X: An additional step in case your workstations are NOT DHCP clients: In other words, if you use static IP address assignments, perform the procedure of **step 2**, above, on the workstation that will eventually boot with the CD into WHoppix, to learn that hardware's address configuration information. Then, after booting WHoppix, invoke the netcardconfig program and insert the proper values.

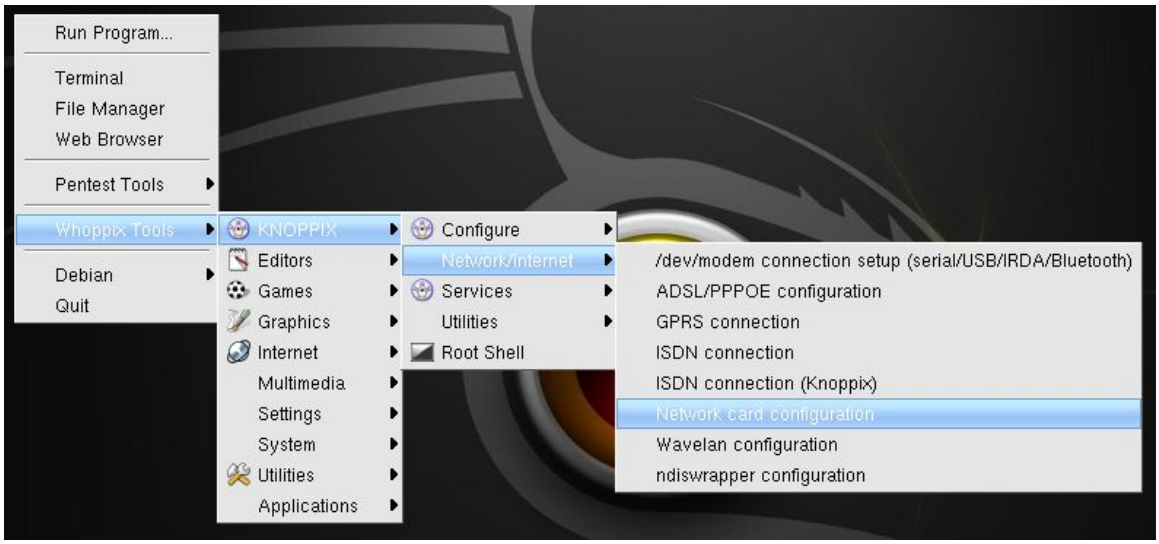

Figure 12 – Starting the network card configuration applet

Figure 13 – Click ‘no’ to continue static IP entries

Figure 14 – Enter the host’s static IP address

Figure 15 – Enter the host's netmask

Figure 16 – Enter the host network's directed broadcast address

Figure 17 – Enter the host network's default gateway address – should be the same as the target's

Figure 18 – Likely no DNS present on test network, so DG is fine

Now you're ready to continue with **Step 4**, above. Note that since the WHoppix software completely loads from CD-ROM every time it reboots, without saving or altering *any* data on the hard disk drive, Step X must be repeated whenever restarting the CD.

Step 7: Analysis

1) Can you think of another useful application (other than recovering from password lockouts) for Framework?

2) What steps would you take to make a server or workstation more resistant to such exploits?

3) What degree of technical prowess would an instruder need to attempt such exploits on your personal or company network devices?

Summary Discussion

A classroom discussion should follow the lab. Review the lab questions and your analyses as a group. Share your experiences and knowledge with the class.

If You Want To Learn More

Try other exploits and payloads on your hapless target server

Try other operating systems as a victim

Update the 2000 server with all current patches and re-attempt the instrusion

Go to an internet search engine and try the terms ‘penetration testing’ and ‘pentest’

Appendix

If you’re not using DHCP to assign IP addresses in the test lab, take care not to assign duplicate or bad IP addresses to the WHoppix host. The best bet is to borrow the already-configured IP address parameters from the underlying Win32 host machine’s hard drive that the WHoppix CD will boot on top of. http://www.knoppix.net has information on many Knoppix issues and configuration solutions. Comments, compliments, or complaints about this title will be cheerfully and graciously accepted at mark.hicks@tccd.net.

Changelog:
V1.0 Initial draft
V1.1 1st submittal to NWCET
V1.2 web release version, cleaned up formatting and typos