Module 39
(More Metasploit and Windows)

• In this module, you'll find out about a Windows Server 2003 VM that we're going to exploit. You'll see some changes you'll need to make to your VMware configuration to access it. You'll also find out a little more about openVAS. And finally you'll find out just a little more about metasploit and its database.
Windows Server 2003 Image

• You have access to Server 2003 through Microsoft Dreamspark.

• The image I'm making available was created by Jesse Varsalone and is one of a set of VMs he created for a CEH course for Moraine Valley Community College.

• The vmdk files is (or soon will be) available as 2003ENTNSQL.tgz with SHA1 sum SHA-2003ENTNSQL.txt. If you have difficulty downloading this (because of virus protection) let me know.
Some Metasploit Issues

• You can fix the metasploit "Database not connected or cache not built" error. Check for database running with this msf command:

  msf> db_status

  If it's not running you can issue these commands:

  # service postgresql start
  # service metasploit start

  and then issue this msf command:

  msf> db_rebuild_cache

• If you will always want the metasploit database and service to run, you'll want to configure it to start on boot:

  # update-rc.d postgresql enable
  # update-rc.d metasploit enable
Some OpenVAS Issues

- I put this script in /usr/local/sbin/openvas-startup:
  
  ```bash
  #!/bin/bash
  service greenbone-security-assistant start
  service openvas-scanner start
  service openvas-administrator start
  service openvas-manager start
  ```

- And this script in /usr/local/sbin/openvas-shutdown
  
  ```bash
  #!/bin/bash
  service greenbone-security-assistant stop
  service openvas-scanner stop
  service openvas-administrator stop
  service openvas-manager stop
  echo "Done"
  ```
Does OpenVAS Need the Internet?

• If so, you can configure Kali to have a second interface from VMware.

• You can then configure the second interface to be on VMnet8 (the NATed interface that shares your host internet connection).

• I have not verified that the Greenbone Security Assistant actually hits the outside network, but my experience indicates this may be the case.
Some VMware Changes Needed to Use 2003ENTSQL

• This windows machine is on the 192.168.1.000/24 network. To use it on your Host-only network, you'll need to set your VMware DHCP server for vmnet1 to use that network.

• There are instructions for doing this in VMware Workstation on the web. (Select Edit->Virtual Network Editor->DHCP Settings, then change the appropriate parameter.)

• There are also instructions to do this in VMware Fusion. (You need to edit the file /Library/Preferences/VMware\ Fusion/networking.)
Metasploit database

$db_nmap$ and $db_import$

- You can store nmap information in your metasploit database by using $db_nmap$
  
  ```
  msf> db_nmap -v -sV 192.168.1.100
  ```

- Then the following commands show what you would expect:
  ```
  msf> hosts
  msf> services
  ```

- If you save a Nessus/Nexpose/OpenVAS report as an nbe file, you can import it into metasploit:
  ```
  msf> db_import 2003ENTSQL.nbe
  ```

- And then you can browse the vulnerabilities (by port if desired):
  ```
  msf> vulns -p 80 -i
  ```