

CS470 Computer Security

Vulnerability Assessment and Penetration Testing Project

A typical Vulnerability Assessment (VA) methodology may consist of all or a combination of the following:

- a) Network mapping;
- b) System footprint analysis;
- c) Enumeration of information;

Penetration testing, which typically follows VA, may consist of all or a combination of the following:

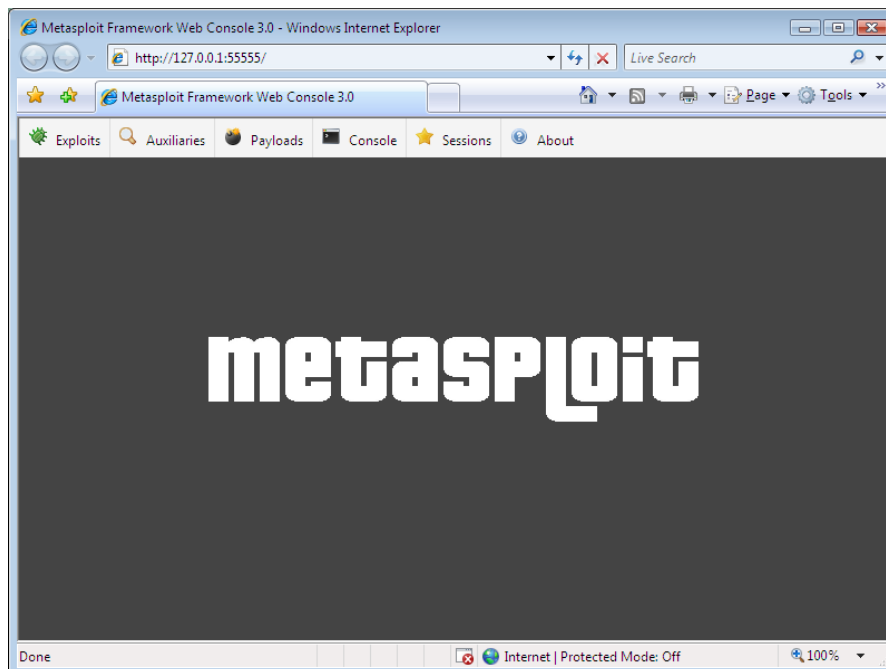
- a) Obtaining access;
- b) Escalation of privilege;
- c) Additional password/information gathering;
- d) Installation of backdoors; and
- e) Abusing the compromised system

In this laboratory project, you will perform a hands-on vulnerability assessment and penetration testing on two computer systems located in the same local area network subnet.

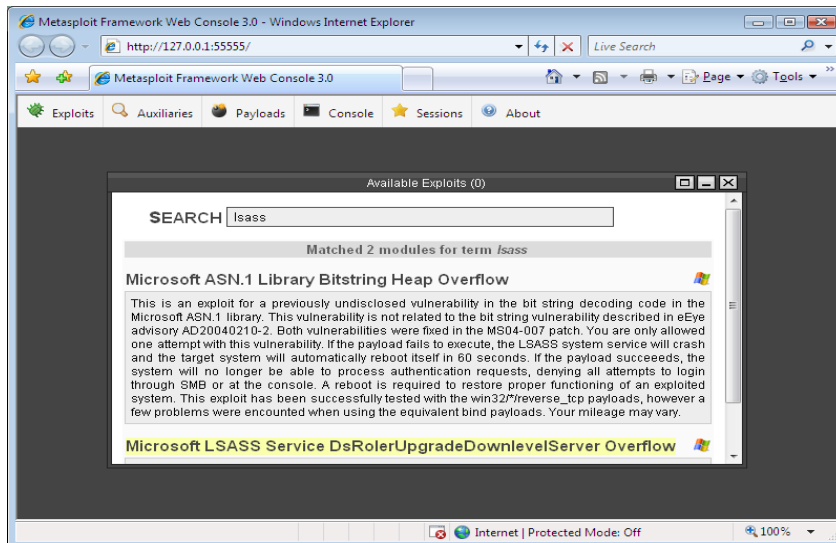
INSTRUCTIONS

Step 1: Scan all computers in the subnet 192.168.100.0 using *nmap*. Determine which computers are running Windows 2000 and enumerate the services and open ports on those computers.

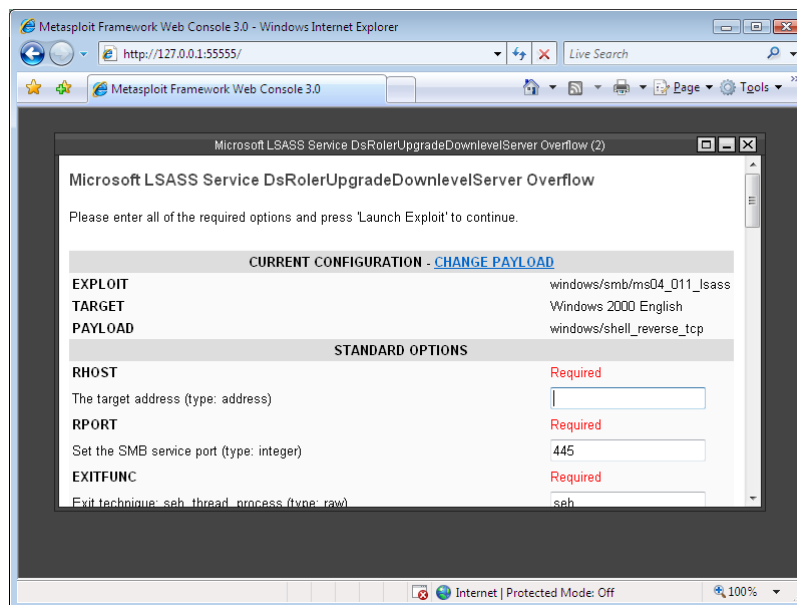
Step 2: Run the web interface (msfweb) of the Metasploit Framework. In version 3.0, the framework runs Ruby webBrick on port 55555 and should open the default web browser automatically. Here is a snap shot of the web browser:

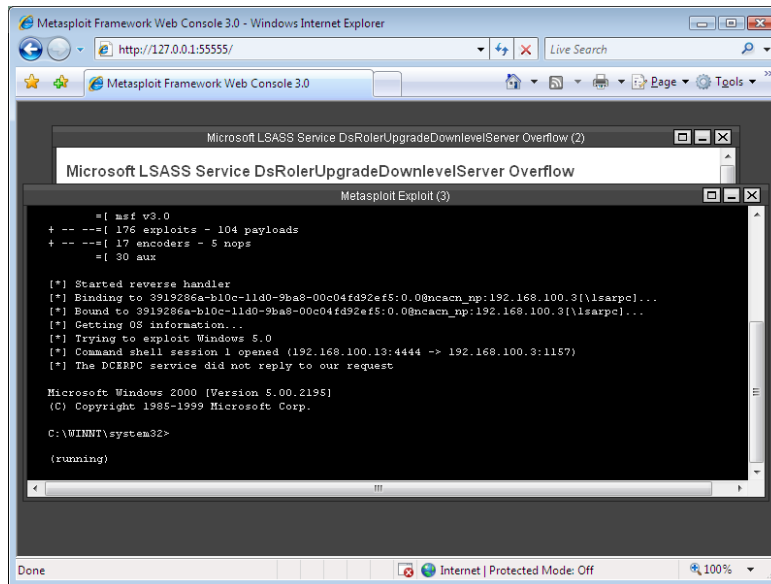


Step 3: Perform a **denial of service (DOS)** attack on one of the Windows 2000 system. To accomplish this, select the **ASN.1 Library Heap Overflow** exploit and configure the required parameters as needed. You should be able to freeze the system and reboot it within a reasonable time period. You need to search for the exploit to get started. Here is a snapshot:



Step 4: Perform a **penetration testing and privilege escalation** on another Windows 2000 system. Select and configure the **LSASS Service Overflow** exploit. Your **target** should be Windows 2000 and your **payload** must be **windows/shell_reverse_tcp**. Fill up the required **IP addresses** for the **remote/target host, RHOST** and the **local host, LHOST** entries. Click on the **EXPLOIT** button and wait for a session to be initiated. When a connection is established, you have gained an administrator privilege on the target system. Create a user account using the **net** commands. Here is a series of snapshots:





At this point you have successfully penetrated the system. You can now use the DOS **net** commands to change the administrator password and create new accounts. Here is a sequence of commands that will accomplish those tasks:

- 1) *net user administrator xyz123* ← change the administrator password
- 2) *net user janedoe secret123 /add* ← adds user janedoe with password secret123
- 3) *net help* ← find additional options
- 4) *net localgroup administrators janedoe /add* ← escalate janedoe's privilege to administrator

Step 5 (optional): Perform a **penetration testing and privilege escalation** on the same Windows 2000 system. Select and configure the **LSASS MS04-011** Overflow exploit. Discover, if possible, another payload that will let you create a user with an administrator privilege. Record all your activities and report your findings.

Step 6 (optional): Discover other exploits that are possible on the target systems.