4 Enumeration

Lab Scenario

You have proven yourself a quick study and your boss has asked you to continue your great work. Now that you have found the targets and open ports, you have been asked to find some additional information regarding those targets. We are not ready to exploit yet, just find more information; please stay within the scope of work on this module.

Lab Objectives

1. Make use of the following tools to perform banner grabbing.
    a. telnet
2. Create Null Sessions and enumerate info from the servers using the following tools.
    a. Net Use
3. Perform NetBIOS Enumeration.
4. Perform SMTP Enumeration.

Lab Resources

1. telnet→ Kali Linux Command Line
2. Net use→ Windows Command Line
3. Cain and Abel→XP image: Desktop\Security\NetTools\Cain
4. nbtscan→ Kali Linux Command Line

Lab Tasks Overview

1. Make use of the following tools to perform banner grabbing.
    a. telnet
2. Create Null Sessions and enumerate info from the servers using the following tools.
    a. Net Use
3. Perform NetBIOS Enumeration.
4. Perform SMTP Enumeration.

Lab Details - Step-by-Step Instructions

4.1 Banner Grabbing

This is to be done on your Kali Linux VM.

1. telnet
    a. Perform a GET Request against your Windows 2003 Server.
        i. Open a command prompt
        ii. Type: telnet <ipaddress> 80
        iii. Hit enter once
        iv. At the prompt type: GET / HTTP/1.0
        v. Then hit enter 2 or 3 times and your banner will appear!

```
root@kali:~# telnet 192.168.21.25 80
Trying 192.168.21.25...
Connected to 192.168.21.25.
Escape character is '^]'.
GET / HTTP/1.0

HTTP/1.1 200 OK
Content-Length: 1433
Content-Type: text/html
Content-Location: http://192.168.21.25/iisstart.htm
Last-Modified: Sat, 22 Feb 2003 01:48:30 GMT
Accept-Ranges: bytes
ETag: "06be97f14dac21:3c2"
Server: Microsoft-IIS/6.0
Date: Fri, 10 Apr 2015 17:18:26 GMT
Connection: close
```

Perform a HEAD Request against your Windows 2003 Server or Apache server.

vi. Type: telnet <ipaddress> 80

vii. Hit enter once

viii. At the prompt type: HEAD / HTTP/1.0

ix. Then hit enter 2 more times.

```
root@kali:~# telnet 192.168.21.23 80
Trying 192.168.21.23...
Connected to 192.168.21.23.
Escape character is '^]'.
HEAD / HTTP/1.0

HTTP/1.1 200 OK
Date: Fri, 10 Apr 2015 17:18:56 GMT
Server: Apache/2.2.8 (Ubuntu) DAV/2
X-Powered-By: PHP/5.2.4-2ubuntu5.10
Connection: close
Content-Type: text/html

Connection closed by foreign host.
```

4.2 Null Sessions

This is to be done on your Windows 7 Victim VM.

1. There is always more than one way to accomplish your goals. Today we are going to start with command line and then use a tool to create our Null Session and gather information.
2. Open a command prompt and type the following command to create a Null Session. You can perform it against either a 2003 or 2008 server.
    a. Type: net use \\<*ipaddress*>\ipc$ "" /user:""

    This picture is for example only!

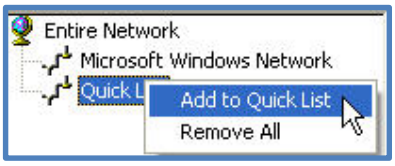
```
C:\>net use \\192.168.2.149\ipc$ "" /user:""
The command completed successfully.
```

3. Now let's make use of that null session.
    a. Type: net view <*ipaddress*>
4. You should be looking at the shares for that system.

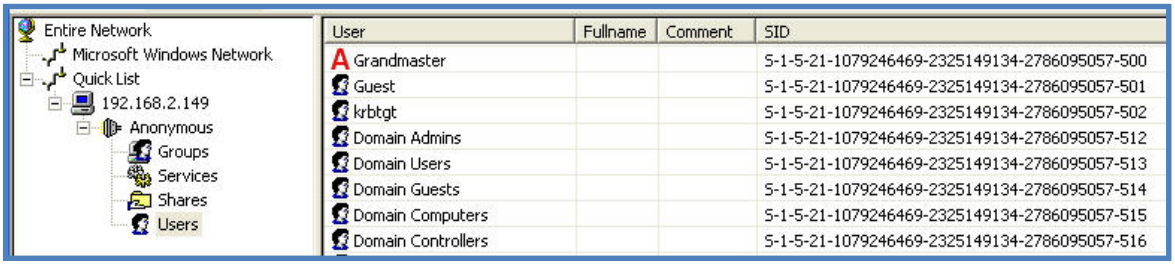
    This picture is for example only! Results may vary.

```
C:\>net view 192.168.2.149
Shared resources at 192.168.2.149


Share name  Type  Used as  Comment

-------------------------------------------------------------------------------
NETLOGON    Disk           Logon server share
SYSVOL      Disk           Logon server share
The command completed successfully.
```

5. Cain and Abel
    a. Start Cain and click on the network tab.
    b. Now right click on the quick list and add the IP address of your target. We are going to use a 2003 machine in the example. Please perform this against a server of your choice.
    c. Click the plus next to the Quick List and then double click the IP address you just added. This will create a null session with the computer.
    d. Now click the plus next to Anonymous.
    e. Double click each of the items listed and see what you can enumerate with Cain and Abel! It does it all for you. (You will only be able to enumerate Shares at this time)



This picture is for example only!



4.3 NetBIOS Enumeration

From your Kali Linux VM, open a terminal and run the following command to enumerate NetBIOS on your lab network preferably targeting the Windows 2003 server:

nbtscan –vr <Target>

```
root@kali:~# nbtscan -vr 192.168.21.25
Doing NBT name scan for addresses from 192.168.21.25


NetBIOS Name Table for Host 192.168.21.25:

Name             Service          Type
---------------------------------------
W2K3-XXX         <00>             UNIQUE
WORKGROUP        <00>              GROUP
W2K3-XXX         <20>             UNIQUE
WORKGROUP        <1e>              GROUP

Adapter address: 00:50:56:80:50:c4
---------------------------------------
```

4.4 SMTP Enumeration

This is to be done on Kali Linux VM which would require a target running port 25.

1. telnet
    a. Open a command prompt
    b. Type: telnet <ipaddress> 25 (use your company email, or choose any other target)
        i. Then hit enter 2 or 3 times and your banner will appear!

This picture is for example only!

```
root@kali:~# telnet 192.168.21.25 25
Trying 192.168.21.25...
Connected to 192.168.21.25.
Escape character is '^]'.
220 W2K3-XXX Microsoft ESMTP MAIL Service, Version: 6.0.3790.0 ready at  Fri,
```