Lab 8: Armitage

Aim

The aim of this lab is to introduce you to Armitage. Armitage developed by Raphael Mudge provides an open source Graphical User Interface (GUI) front end to Metasploit and supports the security testing against a range of vulnerabilities. We will mainly be using a **Kali** instance a **Windows XP** instance, and a **Windows 2003 server** target. We will use **Windows 2003** vulnerabilities to build exploits. Fir this, we will take the basic steps of: Scan, Exploit and Gathering. Further information about Armitage can be obtained at Armitage's Official Website.

Activities:

Complete Lab 8: Armitage

Time to Complete: 2-3 hours

Learning activities:

At the end of this lab, you should understand:

- How to use Metasploit modules via Armitage GUI
- How to do host discovery using Armitage
- How to run an exploit using Armitage
- How to gather information about a compromised source using Armitage

Lab Overview

In this lab, our challenge is to use Windows 2003 and Windows XP vulnerabilities in order to build exploits. For this lab, you will be using ***Kali*** instance, ***Windows XP***, and ***Windows 2003*** instance. Your **Kali DMZ**, you **Windows XP**, and your **Windows 2003 DMZ** should be sitting in the same domain, having an IP address and being able to **ping** each other.

You can find the lab demo here: http://asecuritysite.com/subjects/chapter52

We will be using ALLOCATION A [Link] http://asecuritysite.com/csn10107/prep

A Setting up

1. On Kali, first start two services: PostgreSQL database management and Metasploit services by typing:

```
service postgresql start
service metasploit start
```

Intro: **PostgreSQL is an open source relational database management system (DBMS) developed by a worldwide team of volunteers and Metasploit framework is a tool for developing and executing exploit code against a remote target machine.**

2. Next run Armitage on Kali:

```
armitage
```

Accept the default values, click on ***Connect***, and then press ***Yes*** to start Metasploit.

Check if you can see ***auxiliary***, ***exploit***, ***payload*** and ***post*** in Armitage window.

Look back at previous labs, can you find the following:

Double-click on **exploit → android → browser → webview_addjavascriptinterface**

Read about the exploit and answer the following questions:

What is the version of Android that is affected by this vulnerability (***hint:*** this could be found on the top window)?
What the parameters used with the exploit (***hint:*** they are the ones with "+")?

B Host discovery

3. Next we will try and discover some of the hosts on the network with an ARP sweep using Armitage by browsing to:

auxillary → scanner → discovery → arp_sweep (double click)

Then click on **RHOSTS+** and enter an IP range that includes your Windows 2003 machine (e.g. 172.16.174.0-172.16.174.20) in **Value**.

Then click on **Launch.**

Intro: **The ARP Scan Tool (also called ARP Sweep or MAC Scanner) is a very fast ARP packet scanner that shows every active device on your Subnet. Since ARP is non-routable, this type of scanner only works on the local LAN (local subnet or network segment).**

How many hosts did it discover, and what are their details?

3. For one of the hosts found (select the one that is in your folder on vSoc), now do a TCP port scan. For this, *select the host* and then go to:

auxillary → scanner → portscan → tcp *(double click)*

Then drop the number of the ports to **1-1000**

Then click on **Launch**

What are the set parameters?

Which ports did it discover:

4. Next we will try and discover some Windows instances. For this run the nbname scanner:

auxillary → scanner → netbios → nbname

Then check the **RHOSTS+** value with the IP address of your Windows 2003 machine and then press **Launch**. (***Hint:*** This sends NetBIOS requests to the host(s))

Intro: **A NetBIOS Name is a unique identifier, up to 15 characters long with a 16th character type identifier, that NetBIOS services use to identify resources on a network running NetBIOS over TCP/IP (NetBT). Due to security issues with NetBIOS, mainly information leaks, it is often disabled on corporate networks.**

What are the set parameters?

Which hosts did it discover, and what are their details:

5. Next we will try and discover some Windows instances which are sharing with SMB. For this run the nbname scanner:

auxillary → scanner → smb → smb_version → Launch

Intro: **In computer networking, Server Message Block (SMB), one version of which was also known as Common Internet File System (CIFS, /ˈsɪfs/), operates as an application-layer network protocol mainly used for providing shared access to files, printers, and serial ports and miscellaneous communications between nodes on a network.**

What are the set parameters? Define the SMB hosts on the network, and their operating system? Can you see that the logo is changed? Which port does SMB use?

C Running an Exploit

7. The SMB service on Windows XP can be susceptible to MS08-067. Select the following and run it against your Windows XP instance:

Exploit → windows → smb → ms08_067_netapi

Outline the MS08-067 vulnerability. Which parameter used in the exploit? Press ***Launch***. How the icon on the main window changed? If so what does it look like?

8. Next run the Meterpreter Shell

Right ***click on*** the new red icon that appears on your Armitage window and ***select Meterpreter1*** **> Interact> Meterpreter Shell**

In the console window, type the following commands and look at the information each command gives you:

```
help:

getsystem:

getuid:

getsid:

getpid:
```

9. Next we will grab the username database and use John the Ripper to crack them:

Type:

```
Hashdump
```

Then copy and paste the hashdump by creat a file name hashtocrack and paste the hash

```
sudo nano hashtocrack
```

and then call John the Ripper:

```
john hashtocrack
```

10. Log into your Windows XP target. Now using the Administrator details for Windows XP, connect to the server with psexec, perform the following:

Now right-click on the compromised Windows XP in Armitage, and capture a screen shot by **right click on compromised Windows XP on Armitage > select: Metepreter 1> select: Explore > select: Screenshot**.

Was it successful?

Now:

right click on compromised Windows XP on Armitage> select: Metepreter 1> select: Explore > select: show processes.

What are some of the processes running?

Now return to Windows XP and run a program, e.g. nopepad.exe and follow the command above and check if you can see notepad.exe in the list of processes.

Now:

right click on compromised Windows XP on Armitage> select: Metepreter 1> select: Explore > select: Brows Files.

What are the folders in the top level of C?

Now:

right click on compromised Windows XP on Armitage> select: Metepreter 1> select: Explore > select: Log Keystrokes > **Launch**

Which file was used to store the key strokes?

Return to Windows XP and type some worlds. On Armitage, check if you can see the keystrokes sent from compromised Windows XP.

Check if you see see the keystrokes on the specified path.

Now:

right click on compromised Windows XP on Armitage> select: Metepreter 1> select: Interact > select: Desktop (VNC)

Armitage will tell you the IP address and port to connect to on the screen.

Next open a terminal any enter the command:

vncviewer [IP]:port

Can you connect to the remote instance?

D Gathering information

11. Next we want to gather some information from a host. First run the following:

Post → Windows → Gather → CheckVM → Launch (***hint***: to check if the machine is a virtual machine or a real server)

Is the instance a virtual machine? Run an ARP scan by click on: Post → Windows → Gatherer → Arp_scanner → Launch Which nodes and MAC addresses did it find:

Now run a netstat on the compromised node:

Post → Windows → Gatherer → tcpnetstat → Launch Outline some of the ports that are open:

Next run the following and gather information:

Module	**Information gained**
Post/Windows/Gatherer/enum_ie	
post/windows/gather/credential_collector	
post/windows/manage/migrate	
post/windows/gather/dumplinks	
post/windows/gather/enum_applications	

post/windows/gather/enum_logged_on_users	
post/windows/gather/enum_shares	
post/windows/gather/usb_history	
post/windows/capture/keylog_recorder	