PenTest Lab Exercise 9 (10 October 2014)

**Goal**

Pivot through a meterpreter session to exploit a second machine.

The general idea here is that you will have already identified a vulnerable host (Masakado 72.32.138.35) and you will now use a meterpreter session on it to find another vulnerable host. Then you will exploit a vulnerability of the second host to extract useful information.

Complete this exercise before 15 October 2014 at 9:35 AM.

**Tasks**

1. Create subdirectory *ex9* in your home directory on booty.pentest.edu. Answer the questions (that are written below in italics) in a file called *report* which, together with any artifacts requested below, should be stored in that directory. Always store any keys you might find.

2. Use `exploit/multi/http/php_cgi_arg_injection` and the meterpreter payload of your choice to exploit Masakado 72.32.138.35.

3. Execute a shell on Masakado to *locate* the *ifconfig* and *arp* commands.

   *What is the location of each of these commands?*

4. Use *ifconfig* to identify the interfaces that Masakado is currently using. Masakado's *alternate* interface is the one that does not directly connect to our kali machine.

   *What network/netmask is Masakado's alternate interface bound to?*

5. Try to use the explist `post/multi/gather/ping_sweep` to identify any hosts to which Masakado is connected on the alternate interface. Check this by setting the advanced option VERBOSE to true.

   *What is the IP address of the other host you identified if any?*

   Your ping sweep will likely have missed host 10.32.138.52, but that is your target.

6. Background your meterpreter session and set up a route to the second network to which Masakado is connected.

   *What command did you issue to establish this route?*

7. Set up a proxy using `auxiliary/servers/socks4a` and setting the appropriate SRVPORT value.

   *What SRVPORT value did you set and what command did you issue to initiate this proxy?*
If you changed anything proxychains configuration settings, note that as well.

8. Use proxychains to execute the following nmap command, substituting the host you discovered in step 4 for `<ip-address>`:

   ```
   nmap -sT -Pn -r -p1-512 <ip-address>
   ```

You can redirect stderr of this command to the bit bucket by appending `2>/dev/null` to it.

*What do each of these flags (-sT, -Pn, -r, -p1-512) do?*

*Explain why it might be reasonable to conjecture that this host is a Windows box.*

9. Under the assumption that this is an old Windows XP machine, select the most reliable exploit for such machines and a compatible meterpreter payload.

*What exploit and payload did you choose?*

10. Set the options to access the second host you discovered. Note that this second host is reached on the 10.32.138.0/24 network and as a result the exploit will be routed through the meterpreter session you established on Masakado. This session may die at some point. If so, its route is also inactive and needs to be re-established. The proxy is unimportant in achieving this goal, because the exploit will be routed wholly within metasploit.

11. Once you have gained access to the second host, you should extract some loot.

   *Capture the password hashes. (Recall that there is a meterpreter command for this.)
   And remember that the Administrator is the key account on this host. What are in that account's documents and settings file?*

12. Note that your second exploit was mounted through Masakado even though the physical filesystem on Masakado was never modified. The exploit was arranged wholly through the meterpreter session you had open through your pgp_cgi_arg_injection exploit.

13. It will help you to crack the hashes of this machine offline. Everyone should be able to extract one hash. One of the other hashes has special characters and may take twice the normal amount of time to crack that a normal special-character fuzzing password cracker might take.