Attacking the Windows Domain: Supplement

Exercises

1. Use the module post/windows/gather/enum\_ad\_computers to enumerate the computers on a domain. (The filter must be properly set).
2. Use the module post/windows/gather/enum\_ad\_groups to enumerate the groups on a domain.
3. Use the module post/windows/gather/wmic\_command to determine the services running on a remote system. Note that the command is a WMIC command, not a WQL query.
4. Exploit a Windows system that is set to automatically login a particular user. From within Metasploit, run the module post/windows/gather/credentials/windows\_autologin to grab the login credentials.
5. Exploit a Windows system. Add a new entry to the target's hosts file with the module post/windows/manage/inject\_host.
6. There is a Powershell script written by @FuzzySec that can be used to exploit MS16-032 and escalate privileges. Download the script from <https://www.exploit-db.com/exploits/39719/> and test it on a Windows 10 x1504 system. What happens is the exploit is run remotely?  
     
   This exploit can also be run without Powershell, through an executable written by @fdiskyou. Download the source code from <https://www.exploit-db.com/exploits/39809/>, compile it, and test it on a Windows 10 x1504 system.
7. Exploit a Windows system. Use the reg command from within Meterpreter to list the registry keys contained in HKEY\_LOCAL\_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run. Is it possible to add additional entries?
8. Try Responder with the -b option to force basic authentication. Show that this provides the victim with a prompt to enter their credentials before using the proxy, and show that if the user uses the proxy, that responder obtains the credentials in plain text.
9. Try the WPAD attack using responder against a Windows 7 SP1 system. What differences are noted? By capturing packets or otherwise, examine the WPAD response of responder when it replies to a Windows 7 SP1 system and compare the result to the reply made to a Windows 8.1 system.
10. Compare the Kiwi Meterpreter extension to the Windows Credential Editor (<http://www.ampliasecurity.com/research/wcefaq.html>).
11. Use the registry to disable Windows Defender.