Windows Patch Enumeration a11y.text Windows Patch Enumeration Enumerating Installed Windows Patches a11y.text Enumerating Installed Windows Patches When confronted with Â a Windows target, identifyingÂ which patches have been applied is an easy way of knowing if regular updates happen. It may also provide information on other possible vulnerabilities present on the system. An auxiliary module was specifically created for just this task called enum_patches . Like any post exploitation module, it is loaded using the use command.

```
msf exploit(handler) > use post/windows/gather/enum_patches
msf post(enum_patches) > show options

Module options (post/windows/gather/enum_patches):

   Name       Current Setting       Required  Description
   ----       ---------------       --------  -----------
   KB         KB2871997, KB2928120  yes       A comma separated list of KB patches to search for
   MSFLOCALS  true                  yes       Search for missing patchs for which there is a MSF local module
   SESSION                          yes       The session to run this module on.
```

This module also has a few advanced options, which can be displayed by using the show advanced command.

```
msf post(enum_patches) > show advanced

Module advanced options (post/windows/gather/enum_patches):

   Name           : VERBOSE
   Current Setting: true
   Description    : Enable detailed status messages
   Name           : WORKSPACE
   Current Setting:
```

Description : Specify the workspace for this module Once a meterpreter session as been initiated with your Windows target, load up the enum_patches module setting the â€˜SESSIONâ€™ option. Once done, using the run command will launch the module against our target. msf post(enum_patches) > show options

```
Module options (post/windows/gather/enum_patches):

   Name       Current Setting       Required  Description
   ----       ---------------       --------  -----------
   KB         KB2871997, KB2928120  yes       A comma separated list of KB patches to search for
   MSFLOCALS  true                  yes       Search for missing patchs for which there is a MSF local module
   SESSION    1                     yes       The session to run this module on.

msf post(enum_patches) > run

[*] KB2871997 applied
[+] KB2928120 is missing
[+] KB977165 - Possibly vulnerable to MS10-015 kitrap0d if Windows 2K SP4 - Windows 7 (x86)
[*] KB2305420 applied
[+] KB2592799 - Possibly vulnerable to MS11-080 afdjoinleaf if XP SP2/SP3 Win 2k3 SP2
[+] KB2778930 - Possibly vulnerable to MS13-005 hwnd_broadcast, elevates from Low to Medium integrity
[+] KB2850851 - Possibly vulnerable to MS13-053 schlamperei if x86 Win7 SP0/SP1
[+] KB2870008 - Possibly vulnerable to MS13-081 track_popup_menu if x86 Windows 7 SP0/SP1

[*] Post module execution completed Next Vulnerability Scanning Prev Writing Your Own Scanner
```