Module 4

Man in the Browser Outline

All the browsers offer to save username/password when you submit these data into a login page, so on the next time you visit the same login page you will see your username/password are automatically filled in without typing a single letter. Also, there's third party software like lastpass can do the same job for you.

If the target was using this method for login, then neither the keylogger nor the clipboard methods will work.

Modern hackers have invented a new attack called -man in the browser- to overcome the above scenario.

In a nutshell, man in the browser attack **intercepts the browser API calls and extracts the data (clear text) before it's getting out to the network socket (SSL encrypted)**.

The steps to intercept a process API calls are:-

A. Get the Process ID (PID) of the browser process
B. Attach a debugger to this PID
C. Specify the DLL library that you want to intercept
D. Specify the function name and resolve its memory address
E. Set BreakPoint and register a call back function
F. Wait for debug events using debug loop
G. Once the debug event occur (meaning once the browser calls the function inside the DLL), execute the call back function
H. Return the original process