SMBullet User's Manual

Pre-requisites

Step 1.1 Prepare a victim machine.

Target system **MUST** have SMB service open.

Target system **SHOULD** have Guest users enabled.

- Otherwise, credentials may be utilized for login

Target host **MUST** be configured to permit local network connectivity.

Guest users **MUST** have "*Network access: Let Everyone permissions apply to anonymous users*" and "*Network access: Shares that can be accessed anonymously*" enabled on file target.

Step 1.2. Open **Metasploit Framework** application.

Or type **sudo msfdb init && msfconsole** on the command line.

Step 1.3. Copy **SMBullet.rb** to **/usr/share/Metasploit-framework/modules/exploits/windows/local/**

Establishing Connection

Step 2.1. On Metasploit, type **use exploit/windows/local/SMBullet**

Note: file path may vary depending on file location.

Step 2.2. To set target IP, type **set RHOSTS <Target IP address>**

Note: to see help and commands, type **show options**

Step 2.3. Then type **run** to establish connection.

Note: If SMB_SHARE is not set, typing **run** *will show all SMB Share enabled folders that are accessible on the target machine for reference, as is customary for every run.*

To set SMB_SHARE, type **set SMB_SHARE <folder name>**

Step 2.4. Once successfully established, the program will then send an html file to the target IP address containing the HTA payload, labeled "**SETUP.exe**"(.html) by default, to the chosen SMB Share enabled folder.

Delivering HTA payload

Step 3.1. To execute **SETUP.exe**(.html), the target user must open the file (i.e. double clicking).

Step 3.2. The URL will then begin delivering the actual HTA file, labeled "**RUNME.exe**"(.hta) by default, via internet browser.

Step 3.3. The target user will then only need to run the HTA file to deploy the payload.

Step 3.4. The payload is now installed in the target's system.