

Forum:[Hack Forums](#)

Thread: [Nmap question](#)

DBS2017 - December 31, 2017, 12:20 am

Batch script code :Spoiler ([Click to View](#))

```
Code @echo off
for /l %%%x in (1,1,2) do (
start "rdp" /HIGH nmap -n -Pn -p T:3389 -T4 --script rdp.nse -iR 0
)
exit
```

NSE (script file code):

Spoiler ([Click to View](#))

```
Code description=[[
Checks if an RDP port is open.
]]
author = "ROleg"
license = "Same as Nmap--See http://nmap.org/book/man-legal.html"
categories = {"default", "discovery", "external", "intrusive"}
require "shortport"
portrule = shortport.portnumber(3389, "tcp", "open")
action = function(host, port)
    file = io.open ("results.txt","a+")
    file:write (host.ip.."\\n")
    file:flush()
    file:close()
end
```

Can someone tell me why this works on nmap version 5.51 perfectly and doesn't works on the newest version 7.60?

It closes instantly on the new version.

HackRain - January 1, 2018, 10:03 pm

I don't have rdp.nse in the new version, is it a custom made NSE script?

Code root@kali#: ls -l /usr/share/nmap/scripts/ | grep rdp

```
-rw-r--r-- 1 root root 5061 Nov 9 20:34 http-wordpress-brute.nse
-rw-r--r-- 1 root root 10866 Nov 9 20:34 http-wordpress-enum.nse
-rw-r--r-- 1 root root 4612 Nov 9 20:34 http-wordpress-users.nse
-rw-r--r-- 1 root root 4385 Nov 9 20:34 rdp-enum-encryption.nse
-rw-r--r-- 1 root root 8884 Nov 9 20:34 rdp-vuln-ms12-020.nse
```

root@kali#: nmap --version

Nmap version 7.60 (<https://nmap.org>)

Platform: i686-pc-linux-gnu

Compiled with: liblua-5.3.3 openssl-1.1.0g libssh2-1.8.0 libz-1.2.8 libpcrc-8.39 nmap-libpcap-1.7.3
nmap-libdnet-1.12 ipv6

Compiled without:

Available nsock engines: epoll poll select

If not, maybe it has been removed or replaced with a newer script such as:

Code rdp-enum-encryption.nse