

Forum:[Hack Forums](#)

Thread: [RDP Scanner \(3389\) - Nmap with blah.bat + Question](#)

MajinVegeta - September 12, 2012, 1:08 pm

Hey first I share with you this nice script for nmap:

```
Code @echo off
for /l %%x in (1,1,2) do (
start "rdp" /HIGH nmap -n -Pn -p T:3389 -T5 --script rdp.nse -iR 0
)
exitSave this as blah.bat in your nmap folder
(if a rdp.nse in your nmap folder is missing, tell me)
```

This Scan Method is much faster than all other VNC/RDP Scanners. You can optionally open more times that batch.

I am not an expert on coding, maybe someone can explain me what this batch does? From where does it get the RDP IP's...there are actually no IP Ranges defined.

Furthermore why I am not able to start that batch with Remote Shell (Darkcomet) on a "Slaves" PC?

I have some cracked RDP's, which i am additionally managing with DarkComet. Some of the owners will become for sure suspicious, when I am creating a new user, so i want to start on these RDP's with a less amount of users such batchs hidden on already available users.

With hidden i mean not shown as task...maybe only as process (i know to hide the process is not easy...)

I hope someone can answer some questions

thx in advance :)

edit: i think i know why its not working on remote shell. The RDP hasnt wincap installed. Is there any way to load the drivers temporarily?

Hooded Robin - September 12, 2012, 8:31 pm

1) -iR 0 generates IP addresses at random, infintely (RTFM)

2) Did you check to see that NMAP was installed on the remote system before trying to run the batch script which requires NMAP to operate? It is not installed on Windows systems by default like many unix boxes

3) You might check with the RAT section, your RAT probably has this feature built into it. Google is also you friend :)

Extra) A little something I whipped up for Linux users using a similar concept around NMAP and HYDRA: <https://github.com/Hood3dRob1n/Linux-RDP>

Cheers

L2pk irl - January 25, 2013, 3:36 am

How do you get it to automatically save the scanned results into a text file? I used to have a version of this that did that but now I can't find it.

supracontra - January 25, 2013, 7:51 am

(Jan 25, 2013 04:36 AM)L2pk irl Wrote: [\[CITE\]](#) How do you get it to automatically save the scanned results into a text file? I used to have a version of this that did that but now I can't find it.
Read the manual or die in a fire you lowlife.

The fuck is wrong with you inferiors asking shit questions all the fucking time.

tonymontana - January 25, 2013, 2:38 pm

man i tried and works like a charm!!! i would vouch but cant do it lol i got 5 rdps from israel lol

alpaga51 - January 7, 2020, 8:26 am

(Sep 12, 2012 01:08 PM)MajinVegeta Wrote: [\[CITE\]](#) Hey first I share with you this nice script for nmap:

```
Code @echo off
for /l %%%x in (1,1,2) do (
start "rdp" /HIGH nmap -n -Pn -p T:3389 -T5 --script rdp.nse -iR 0
)
exitSave this as blah.bat in your nmap folder
(if a rdp.nse in your nmap folder is missing, tell me)
```

This Scan Method is much faster than all other VNC/RDP Scanners. You can optionally open more times that batch.

I am not an expert on coding, maybe someone can explain me what this batch does? From where does it get the RDP IP's...there are actually no IP Ranges defined.

Furthermore why I am not able to start that batch with Remote Shell (Darkcomet) on a "Slaves" PC?

I have some cracked RDP's, which i am additionally managing with DarkComet. Some of the owners will become for sure suspicious, when I am creating a new user, so i want to start on these RDP's with a less amount of users such batchs hidden on already available users.

With hidden i mean not shown as task...maybe only as process (i know to hide the process is not easy...)

I hope someone can answer some questions

thx in advance :)

edit: i think i know why its not working on remote shell. The RDP hasnt wincap installed. Is there any way to load the drivers temporarily?Thank you very much for this script...