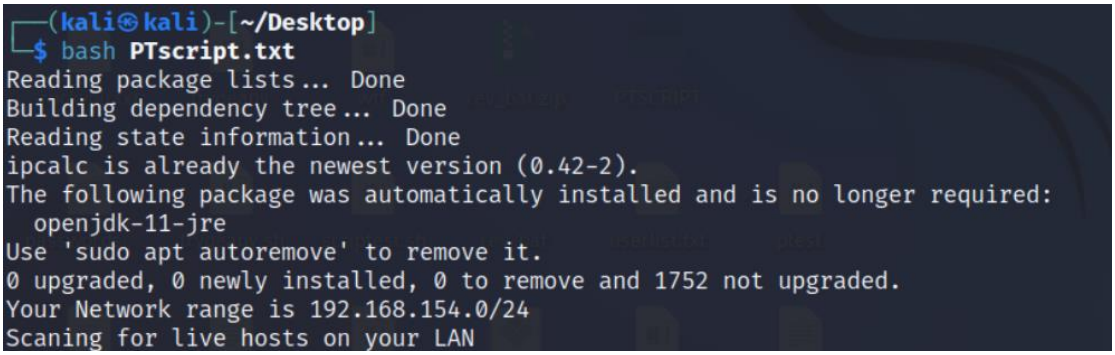
This script was written by Reut Klaider-Levy, 7736/12:S11

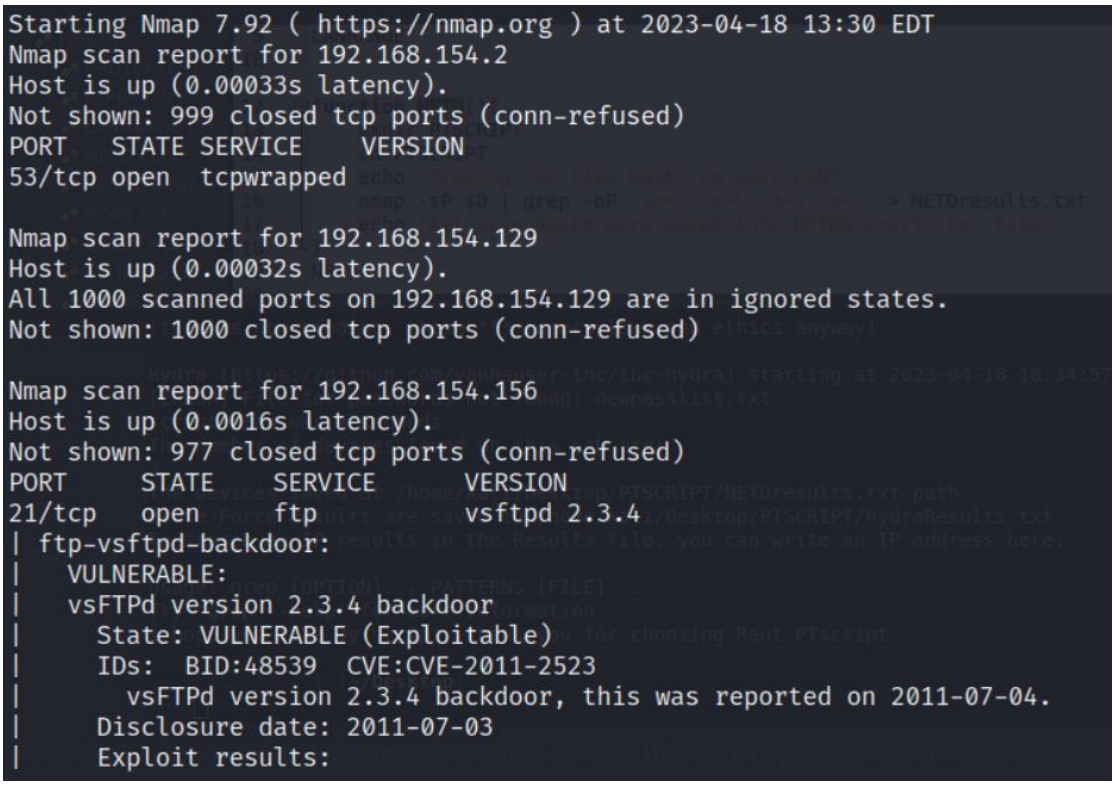
Welcome to my PTSCRIPT –

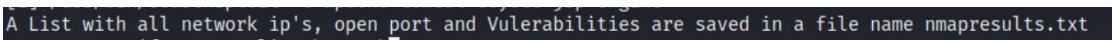
When you will start the script, the first function – LANRANGE will install ipcalc on your linux and will check your network range.



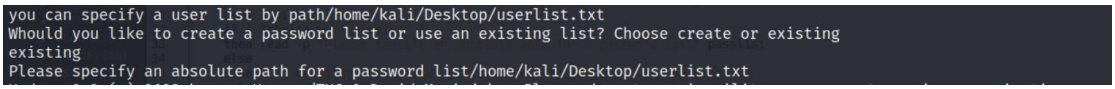
Second function – NETD – will scan for live hosts on your LAN and will save the results into a file named NETDresults.txt in a directory named PTSCRIPT on your Desktop.

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.

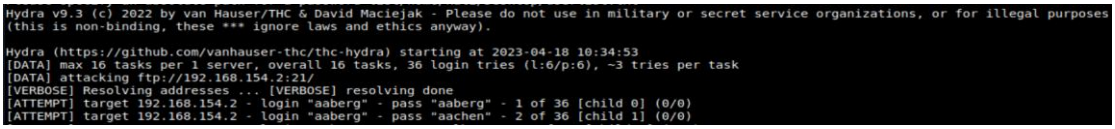




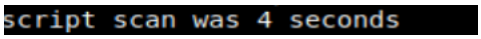
Fourth Function – SPECIFY – this function will ask you to name a userlist by absolute path, and will ask you if you would like to choose existing password list or create a new one via crunch. If you will choose to use crunch – the new list will be save on newpasslist.txt file in PTSCRIPT directory.



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.



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.



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.