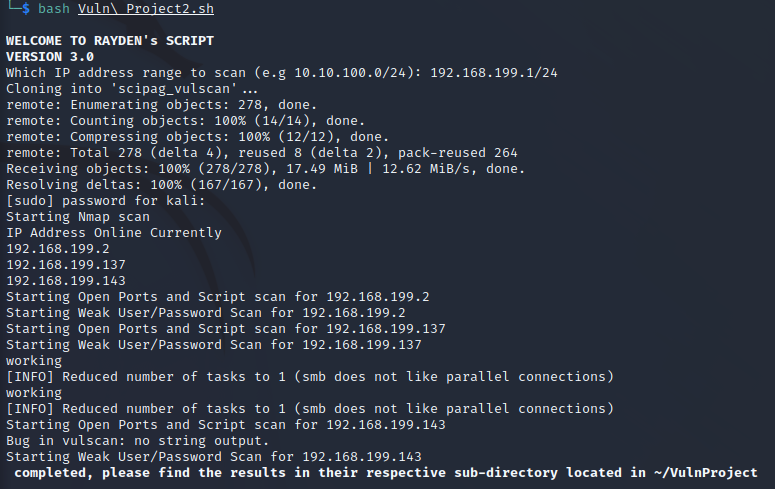
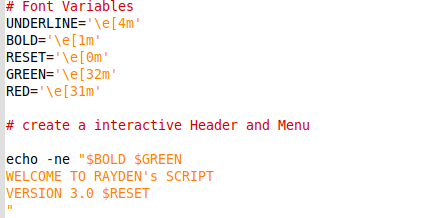
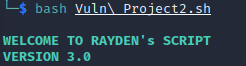
**Script Objective**

* Script to install all tools/software needed
* Automate Nmap scans, Nmap scripts and Hydra
* Nmap scans to determine, ip address online, open ports and it's service version  
  Nmap scripts to identify vulnerability
* Hydra to perform dictionary attack to identify weak passwords
* Save results into newly created folder VulnProject, each Ips would have their own sub-folders to store their results

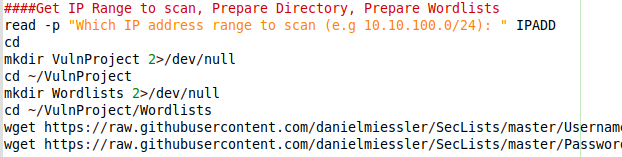


**Line 9 – 21**  
Created font variables to bold and add colours to headers and words

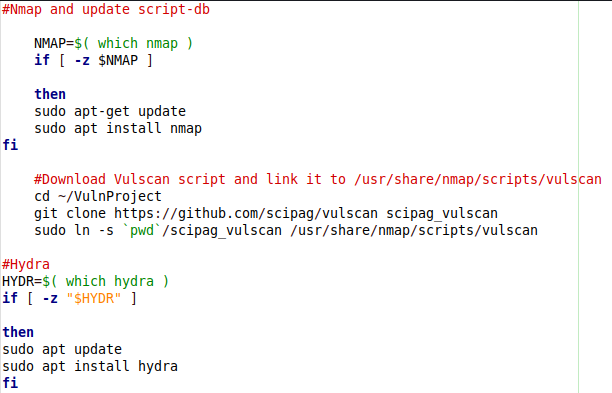


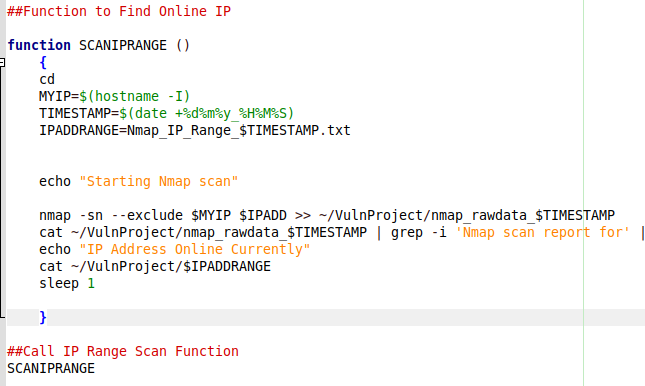


**Line 24 - 65**  
Script will ask users to enter IP Range to scan  
After entering, script will prepare/download all relevant tools for the run  
 A) Download wordlists for username and password and stored into the newly created folder VulnProject

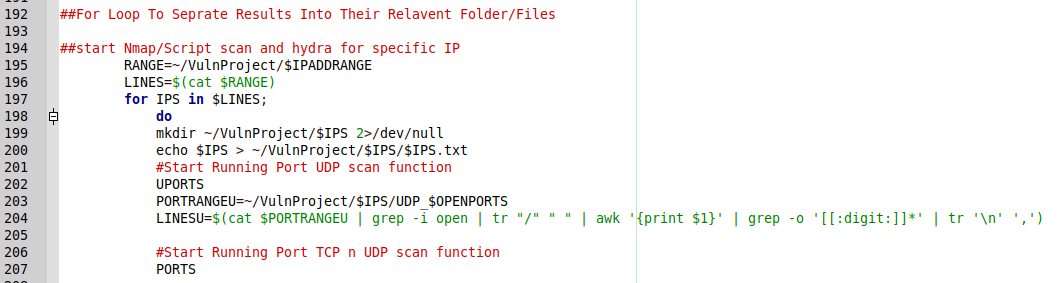


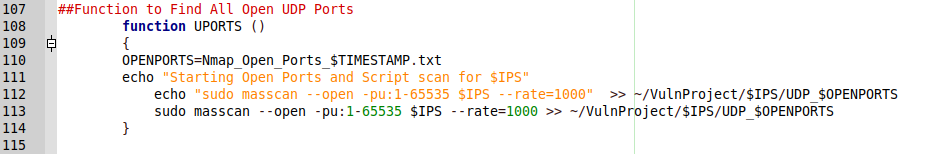
B) Check if Nmap and Hydra is present, if not install Nmap and Hydra  
C) Download Vulscan script into folder Vulnproject and link it to Nmap script folder

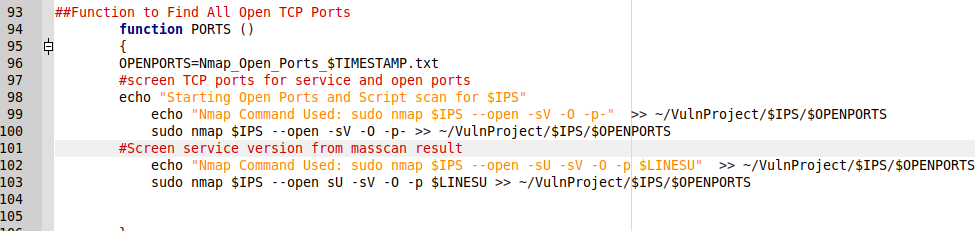


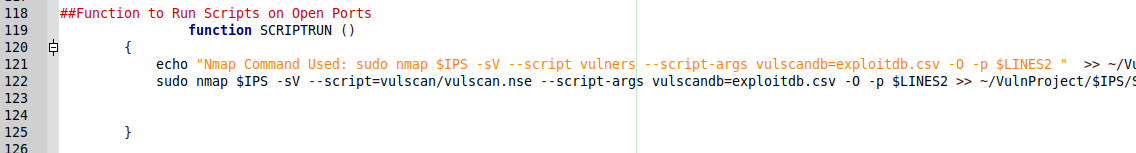
**Line 70 – 88**  
Created a function to scan online Ips using Nmap ping scan  
Functions will also identify self IP and exclude itself from the scan  
Function will then append the result to 2 newly files  
Files can be identified by their timestamp  


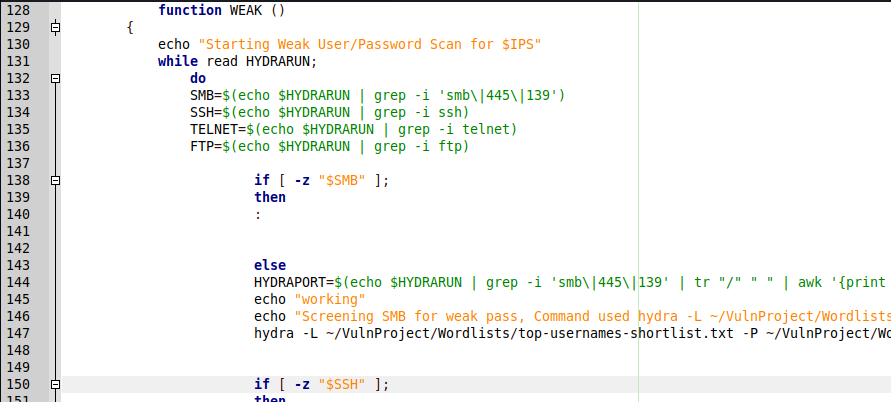
**Line 189 – 213**  
Created For loops to run the functions  
A) Split the result into sub-folders identifiable by their IP address  
B) Masscan to identify open UDP ports result will combine to Nmap scan for service Line 107 - 114  
C) Run Nmap function scan to identify all open ports online Line 90 – 99  
D) Run Nmap script function scan to identify vulnerable ports on exploitdb Line 117 – 124  
E) Run Hydra function to identify weak usernames and Password Line 126 – 190 (if B identify any words such as ssh, 135, 445, smb, telnet, ftp. Script is able to match service even if it is running on non-standard ports. If none was identified, Hydra will skip)

Split the result into sub-folders identifiable by their IP address 

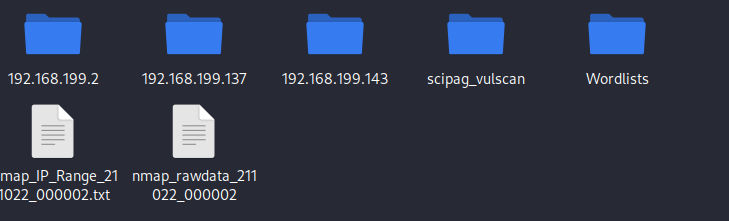
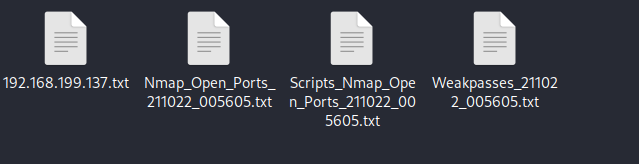




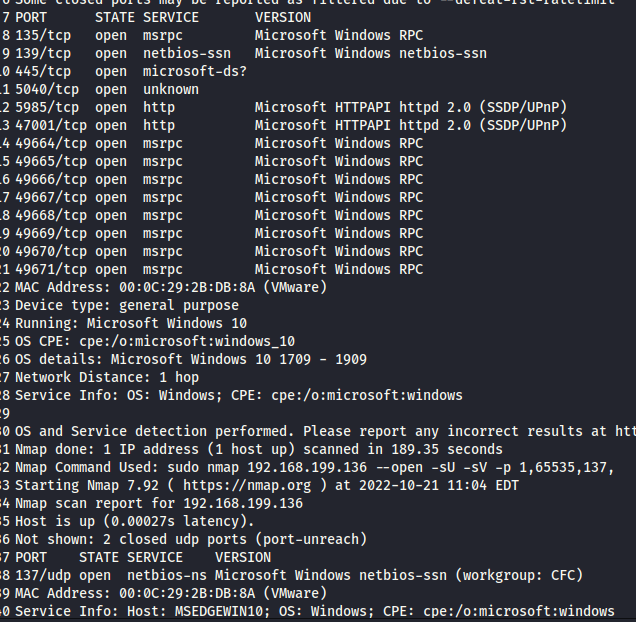


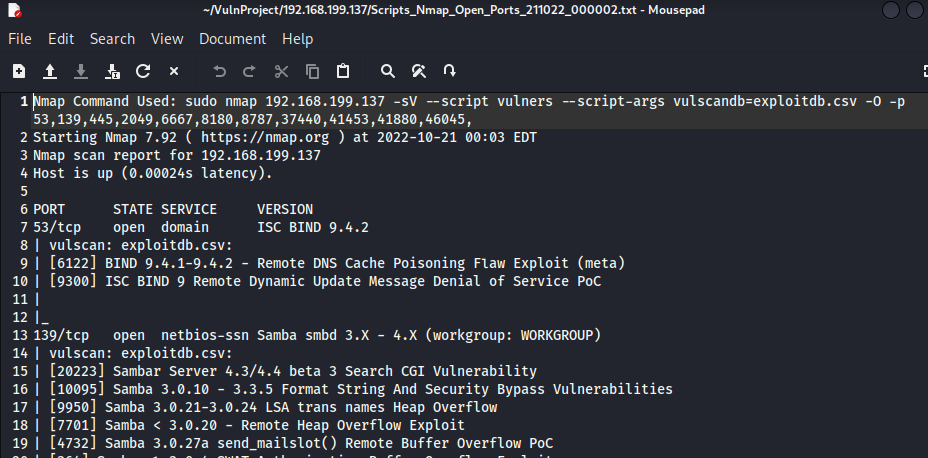


Results are saved into their sub-directory

Nmap results on open ports and services



Nmap result using vulscan.nse 

Hydra result on weak Username:password