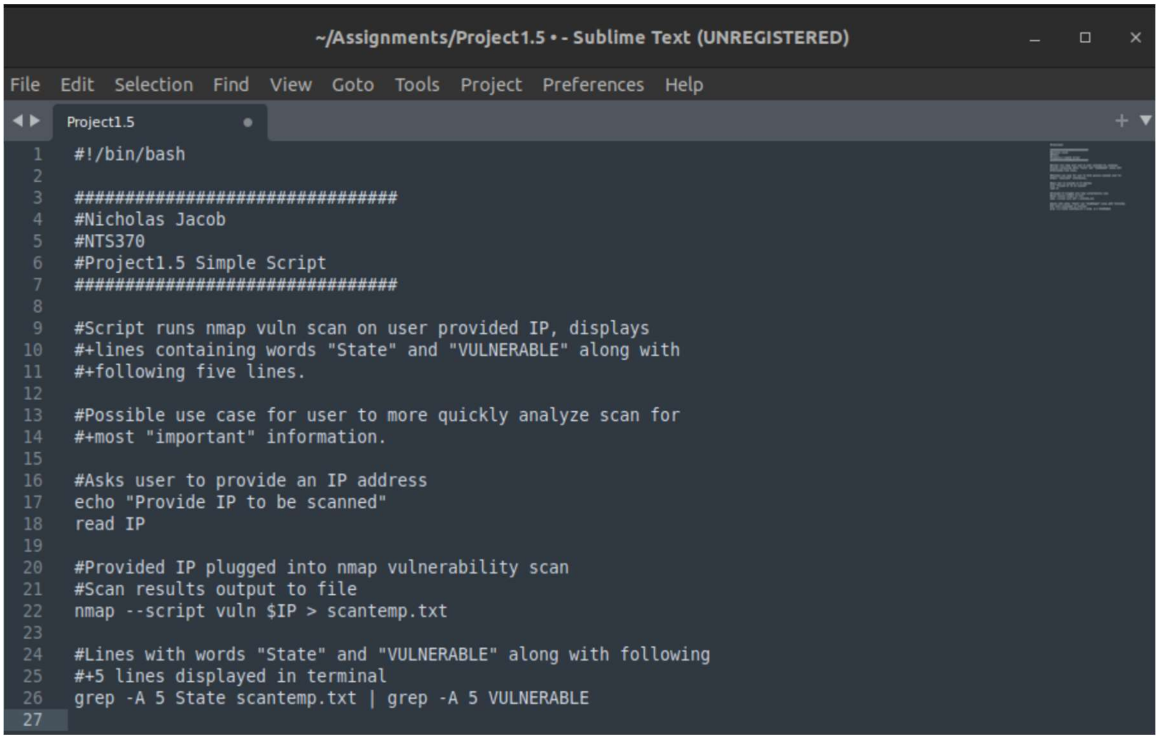
NMAP Vulnerability Script

Nicholas Jacob

University of Advancing Technology

February 5, 2023

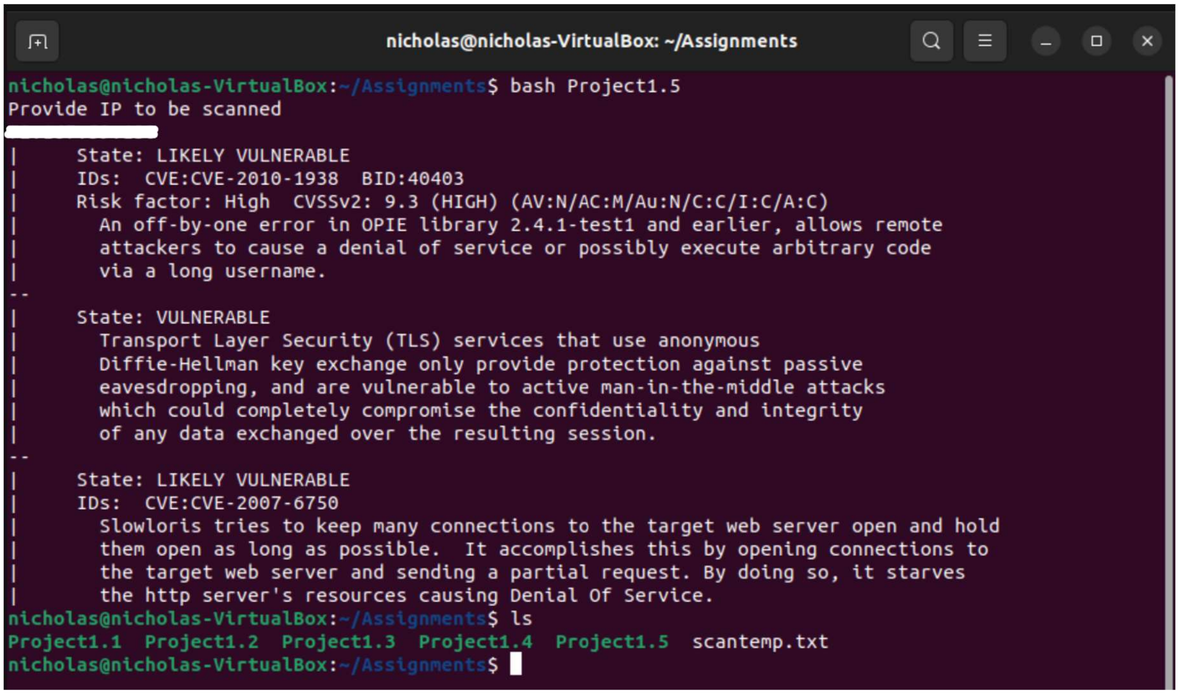
Script:


~/Assignments/Project1.5 • - Sublime Text (UNREGISTERED)
File Edit Selection Find View Goto Tools Project Preferences Help
Project1.5

```
#!/bin/bash

################################
#Nicholas Jacob
#NTS370
#Project1.5 Simple Script
################################

#Script runs nmap vuln scan on user provided IP, displays
#+lines containing words "State" and "VULNERABLE" along with
#+following five lines.

#Possible use case for user to more quickly analyze scan for
#+most "important" information.

#Asks user to provide an IP address
echo "Provide IP to be scanned"
read IP

#Provided IP plugged into nmap vulnerability scan
#Scan results output to file
nmap --script vuln $IP > scantemp.txt

#Lines with words "State" and "VULNERABLE" along with following
#+5 lines displayed in terminal
grep -A 5 State scantemp.txt | grep -A 5 VULNERABLE

```

Script ran in terminal:

Scanned IP hidden for privacy



```
nicholas@nicholas-VirtualBox:~/Assignments$ bash Project1.5
Provide IP to be scanned
[redacted]
|     State: LIKELY VULNERABLE
|     IDs:  CVE:CVE-2010-1938  BID:40403
|     Risk factor: High  CVSSv2: 9.3 (HIGH) (AV:N/AC:M/Au:N/C:C/I:C/A:C)
|       An off-by-one error in OPIE library 2.4.1-test1 and earlier, allows remote
|       attackers to cause a denial of service or possibly execute arbitrary code
|       via a long username.
--
|     State: VULNERABLE
|       Transport Layer Security (TLS) services that use anonymous
|       Diffie-Hellman key exchange only provide protection against passive
|       eavesdropping, and are vulnerable to active man-in-the-middle attacks
|       which could completely compromise the confidentiality and integrity
|       of any data exchanged over the resulting session.
--
|     State: LIKELY VULNERABLE
|     IDs:  CVE:CVE-2007-6750
|       Slowloris tries to keep many connections to the target web server open and hold
|       them open as long as possible.  It accomplishes this by opening connections to
|       the target web server and sending a partial request. By doing so, it starves
|       the http server's resources causing Denial Of Service.
nicholas@nicholas-VirtualBox:~/Assignments$ ls
Project1.1  Project1.2  Project1.3  Project1.4  Project1.5  scantemp.txt
nicholas@nicholas-VirtualBox:~/Assignments$ 
```