

EECS 3482 Lab 2

Jonathan Baldwin

Part 1: Telnet And SSH Connections Analysis

Bandit

The following is a solution to Bandit part 1-9 in the form of a shell script. It uses the `sshpass` program to allow `ssh` to accept a password non-interactively.

```
#!/bin/sh
HOST=bandit.labs.overthewire.org
PASSWORD=bandit0
NUM=0
while read -r COMMAND; do
    USERNAME=bandit$NUM
    echo running $USERNAME: $COMMAND
    PASSWORD=$(sshpass -p $PASSWORD ssh -tp 2220 $USERNAME@$HOST $COMMAND < /dev/zero 2>/dev/zero)
    echo $PASSWORD
    NUM=$(expr $NUM + 1)
done << EOF
cat ./readme
cat ./-
cat ./spaces\ in\ this\ filename
cat ./inhere/.hidden
sh -c "file ./inhere/* | fgrep text | cut -d: -f1 | xargs cat"
sh -c 'find ./inhere -size 1033c \! -executable | xargs file | fgrep text | cut -d: -f1 | xargs cat'
sh -c 'find / -size 33c -user bandit7 -group bandit6 | xargs cat'
sh -c 'fgrep millionth data.txt | cut -f2'
sh -c 'sort data.txt | uniq -u'
sh -c "strings data.txt | grep -o '[a-zA-Z0-9]\{32\}'"
echo hello from level 10
EOF
```

The following is the password to level 10, as retrieved from the output of the script:

truKLdjsbJ5g7yyJ2X2R0o3a5HQJFuLk

Telnet

SSH

Phish

Steg

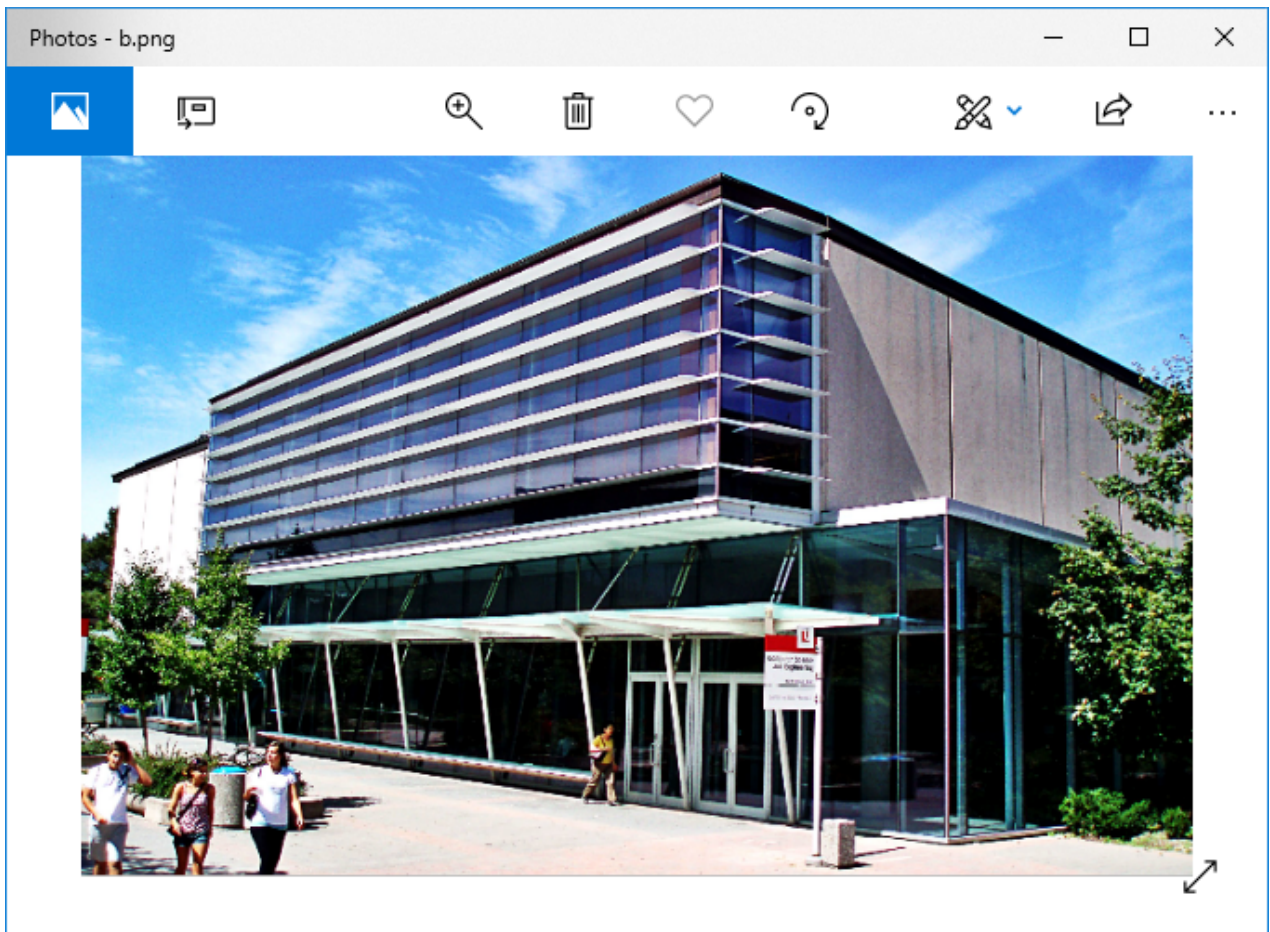
Windows

1. Using the Notepad, create a text file and insert the following line:

Testing the Environment!

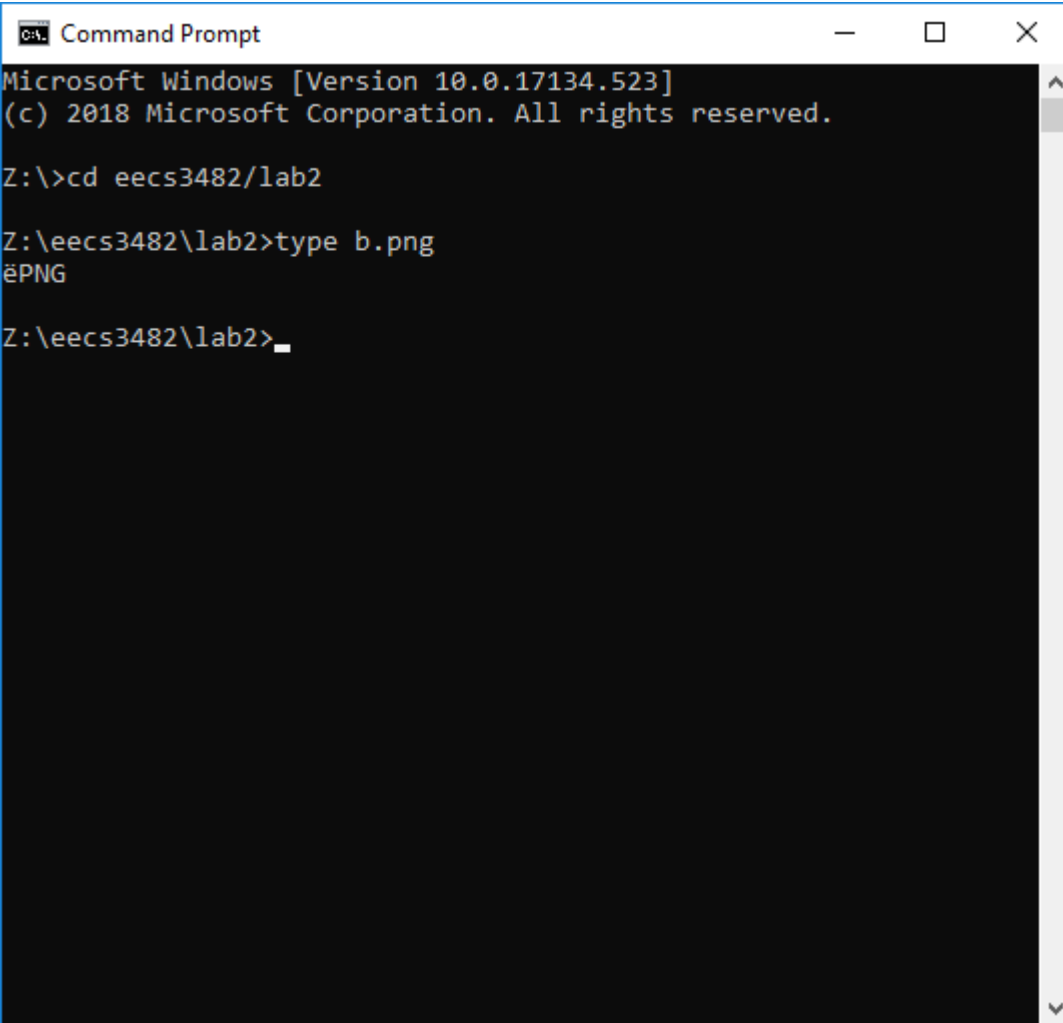
Save the file as a.txt

2. Download the attached image file (b.png) to the same directory of the text file.
3. Parse the file using an image reader and document the output.



Windows Photos views the PNG.

4. Attempt to read the file using the command: `type b.png ->` Document the output.

A screenshot of a Windows Command Prompt window. The title bar reads "Command Prompt". The window content shows the following text: "Microsoft Windows [Version 10.0.17134.523]" followed by "(c) 2018 Microsoft Corporation. All rights reserved." on the next line. The prompt "Z:\>" is followed by the command "cd eeecs3482/lab2". The next line shows the prompt "Z:\eeecs3482\lab2>" followed by the command "type b.png". The output of the command is "ëPNG". The prompt "Z:\eeecs3482\lab2>" is followed by a cursor. The window has a scrollbar on the right side.

```
Microsoft Windows [Version 10.0.17134.523]
(c) 2018 Microsoft Corporation. All rights reserved.

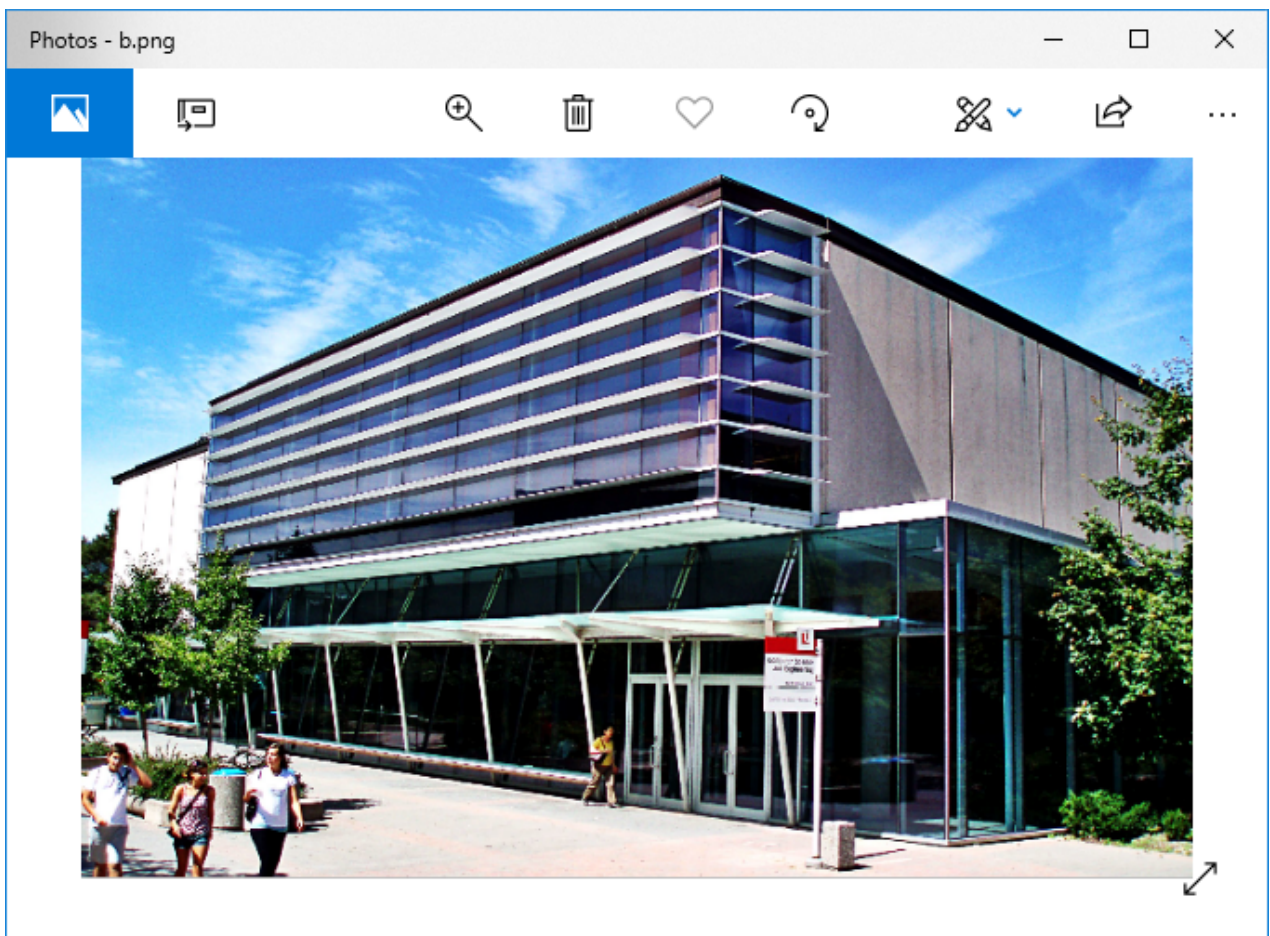
Z:\>cd eeecs3482/lab2

Z:\eeecs3482\lab2>type b.png
ëPNG

Z:\eeecs3482\lab2>_
```

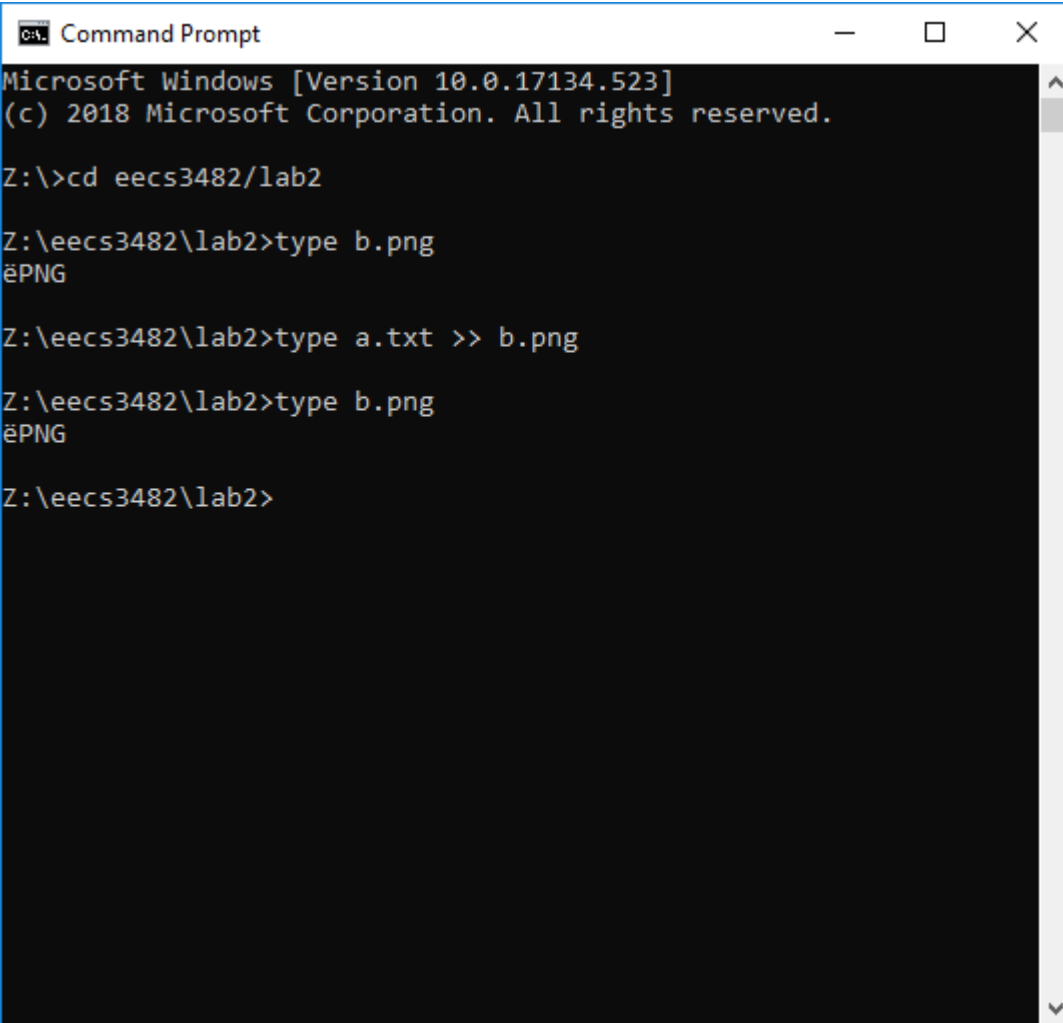
type prints the PNG header.

5. On the command prompt run the following command: `type a.txt >> b.png`.
6. Parse the file using an image reader and document the output.



Windows Photos still views the PNG as if nothing has changed.

7. Attempt to read the file using the command: `type b.png ->` Document the output.

A screenshot of a Windows Command Prompt window. The title bar reads "C:\> Command Prompt". The window contains the following text:

```
Microsoft Windows [Version 10.0.17134.523]
(c) 2018 Microsoft Corporation. All rights reserved.

Z:\>cd eeecs3482/lab2

Z:\eeecs3482\lab2>type b.png
ëPNG

Z:\eeecs3482\lab2>type a.txt >> b.png

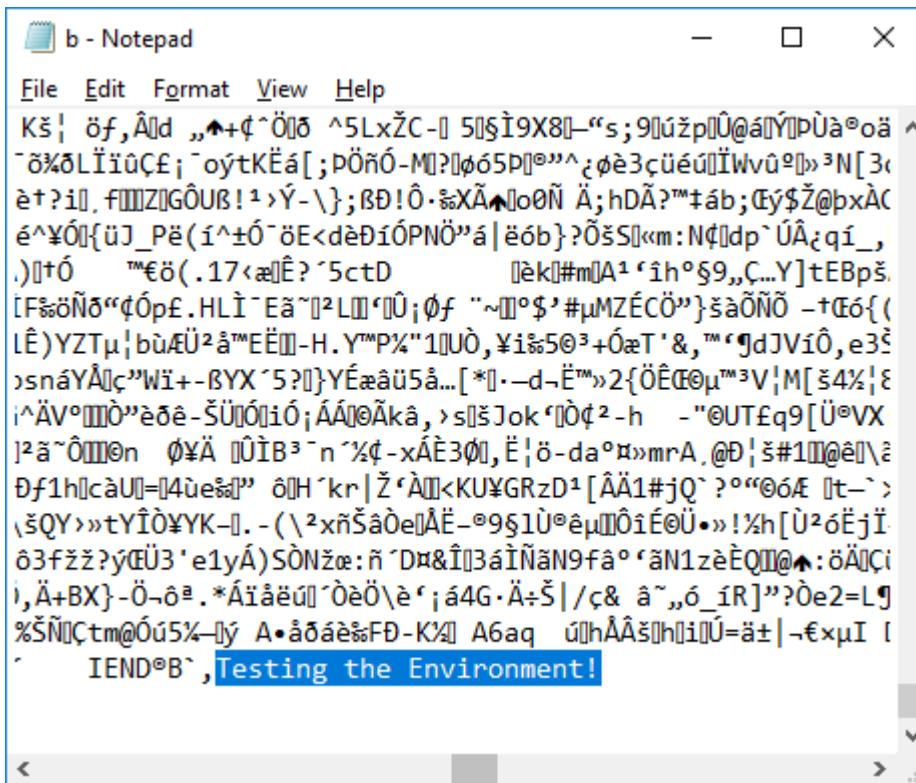
Z:\eeecs3482\lab2>type b.png
ëPNG

Z:\eeecs3482\lab2>
```

The window has a standard Windows interface with a title bar, maximize, and close buttons. A vertical scrollbar is visible on the right side of the command area.

`type` prints the PNG header, but not what we catenated to the end of the file.

8. Using a notepad session, open the file `b.png` and scroll down to the end file, document what you see.



b - Notepad

File Edit Format View Help

Kš| öf,Âd „+¢^Öð ^5LxŽC- 5§İ9X8-“s;9úžpÜ@áVÏPÙà°oä ^
~õ%ðLİİüÇ£;~oytKĖá[;PÖñÓ-M?ø65P”^¿øè3çüéúİWvû°»³N[3ç
è+?i, fZGÔUR!¹>Ý-\\};BĐ!Ô·%XĂ↑o0Ñ Ä;hDĂ?™†áb;Œy\$Ž@pxÀC
é^¥Ó{üJ_Pë(í^±ó~øE<dèĐÍÓPNÖ”á|ëób}?ÖšS«m:N¢dp`ÚÂ¿qí_,
)†ó “€ö(.17<æĖ?`5ctD ðèk#mA¹‘ih°§9,,Ç...Y]tEBpš.
[F%öÑð“¢Óp£.HLÌ`Eă~²L“Ü;øf “~°\$’#μMZÉCÖ”}šàÖÑÖ -†Œó{(
LĖ)YZTμ|bùÆÜ²â”EĖ-H.Y”P%”1Uò,¥i%50³+ÓæT’&,™‘ŒdJVîô,e3ž
»snáYÄç”Wĩ+-BYX`5?[]YÉæâü5â...[*]-d-Ė”»2{ÖĖŒμ”³V!M[š4%|ε
;^ÄV°””èðê-ŠÜÓİİÓ;ĂÄŒĂkă,»sšJok‘Üø²-h -”@UT£q9[Ü°VX
]²ă~Ô”on ø¥Ă ÜİB³~n`%¢-xĂĖ3ø,Ė!ö-da°»mrA,@Đ!š#1”@ê\ê
Đf1h|càU|=4ùeš” òH`kr|Ž`À<KU¥GRzD¹[ĂÄ1#jQ`?°“06Æ [t-`>
\\šQY»»tYÎÒ¥YK-.-(\²xñšàðeĖĂĖ-°9§1Ü°êμ”ŒİÉŒÜ•»!%h[Ü²óĖjİ
ô3fžžž?ýŒÜ3’e1yĂ)SÒNžæ:ñ`D&İ3áİÑăN9fà°‘ăN1zèĖQ”@↑:öĂÇi
),Ă+BX}-Ö-ð³.*Áiăëú`ÒèÖ\è‘;á4G·Ă÷Š|/ç& â~,,ó_İR]”?ðe2=LŒ
%ŠŒÇtm@Óú5%-Ïý A•ăđăë%FĐ-K% A6aq úhĂšhİÜ=ă±|-€×μI I
` IEND°B`,Testing the Environment!

The contents of a.txt is visible at the end of the file.