Laboratory Notes

Laboratory Number: ____4_ Examiner Name: Kelli Kinnikin Date & Time Activity 12/4/17 3:00 Before I could do this lab, I had to download multiple sources/tools. p.m Command: "sudo apt-get install steghide" Command: "sudo apt-get install python-progressbar \$gitclone https://github.com/Va5c0/Steghide-Brute-Force-Tool.git Command: "scp cis425@mathcswc.fontbonne.edu:~/Lab4.tar ./" After downloading all those previous sources/tools, I ran the steghide-12/4/17 3:06 brute-force-tool and inserted the 1st jpg image into the tool. p.m mystery-flag-3.jpg steg_brute.py ICENSE mystery-flag-4.jpg wordlist.txt nystery-flag-1.jpg mystery-flag-5.jpg nystery-flag-2.jpg README.md oython steg_brute.py -b -d wordlist.txt -f mystery-flag-1.jpg [i] Searching... wrote extracted data to "mystery-flag-1_flag.txt". [+] Information obtained with password: the flag is {Denmark} • Wordlist.txt was given to me in the .tar file • FLAG: {Denmark} Next, I placed the 2nd jpg image into the brute force tool. 12/4/17 3:20 python steg_brute.py -b -d wordlist.txt -f mystery-flag-2.jpg p.m [i] Searching... Amazon wrote extracted data to "mystery-flag-2_flag.txt". [+] Information obtained with password: Thailand2017 The flag is {Thailand} • FLAG: {Thailand} This time I used the "xxd" command to find the hidden message. 12/4/17 10:03 p.m 000006600: dd7b dfba f75e f7ee bdd7 bdfb af75 ef7e 000066a0: ebdd 7bdf baf7 5ef7 eebd d7bd fbaf 75ef 000066b0: 7eeb dd7b dfba f75e f7ee bdd7 bdfb af75 000066c0: ef7e ebdd 7bdf baf7 5ef7 eebd d7ff d954 000066d0: 4845 2066 6c61 6720 6973 207b 5375 6461 FLAG: {Sudan}

To get the 4th flag I used the command: 12/4/17 10:26 p.m Command: "xxd" The message was encrypted, so I used a Caesar cipher online tool to decrypt it +6 AJNOBOXE +7 ZIMBABWE +4 CLPEDEZH CHRCCCRI FLAG: ZIMBABWE To get the mystery-flag-5.jpg, I used the "xxd" command again along 12/4/17 with a base64 decoder. 10:30 p.m The "UGVydQ" is what goes into the online decoder tool FLAG: Peru 00003750: aef3 e6c6 0554 7733 a92f 74b3 11c7 3d69Tw3./t...=i 00003760: dc91 9a48 d702 9fbb 8e9c 54f5 2a2d 08aa 00003770: a074 cd14 bb8f 6028 a576 3b23 ffd9 5547 .t....`(.v;#..UG 90003780: 5679 6451 3d3d 0a Vvd0==. Decode from Base64 format Simply use the form below 12/4/17 10:33 p.m UGVydQ **〈 DECODE 〉**UTF-8 ▼ You may also select input charset. ① Live mode OFF Decodes while you type or paste (strict format). Note that decoding of binary data (like images, documents, etc.) does not work in live mode. ♠ UPLOAD FILE Decodes an entire file (max. 10MB). YOU DO YOUR BEST WORK. Peru