

CYBERSECURITY TRAINING

(WEEK 2 – Day6)

Practical Implementation of Cryptography

1.

The screenshot shows a web-based tool interface for converting binary data to ASCII. The 'Recipe' panel on the left is set to 'From Binary' with a 'Delimiter' of 'Space' and a 'Byte Length' of '8'. The 'Input' panel on the right contains a large block of binary data (0s and 1s). The 'Output' panel at the bottom displays the resulting ASCII text: 'ASCII, an acronym for American Standard Code for Information Interchange, is a character encoding standard that represents text and control characters in digital form using 7-bit numbers.'

2.

The screenshot shows a web-based tool interface for converting decimal data to text. The 'Recipe' panel on the left is set to 'From Decimal' with a 'Delimiter' of 'Space' and the 'Support signed values' checkbox unchecked. The 'Input' panel on the right contains a large block of decimal numbers. The 'Output' panel at the bottom displays the resulting text: 'White hat hackers, or ethical hackers, use their skills to improve system security and protect against threats.'

3.

Recipe

ROT13

☒ Rotate lower case chars

☒ Rotate upper case chars

☐ Rotate numbers

Amount
13

Input

Tenl ung unpxref bcrengr va n zbeny tenl nern, bsgra qvfpybfvat ihyarenovyvgvrf gurl svaq jvgubhg rkcyvpvg crezvffvba, fbzrgvzrf frrxvat pbzcrafvba sbe gurve rssbegf. |

rec 169 1

Raw Bytes

LF

Output

Gray hat hackers operate in a moral gray area, often disclosing vulnerabilities they find without explicit permission, sometimes seeking compensation for their efforts.

rec 169 1

Raw Bytes

LF

4.

Recipe

From Base32

Alphabet
A-Z2-7=

☒ Remove non-alphabet chars

Input

KJ5WIIICIMF2CASDBMNVWk4TTHJKGQZLTMUQGQYLDNNSXE4ZAMFZGKIDQOJXWCY3UNF3GKIDJNYQGI2LGMVXGI2L0M4QH6LTOR SW24ZAMFTWC2LOON2CAYTMMFRWIDIMF2CAYLUORQWG23TFQQHG3NMV2G53LFOMQGK5TFNYQK3THMF TWS3THEBUW4IDPMZTG K3TTNF3GKIDBMN2G533OOMQHI3ZAMRUXG4TVOB2CA3LBNRUG2LPOVZSA2DBMNVWk4TTTFYQA

rec 268 1

Raw Bytes

LF

Output

Red Hat Hackers:These hackers are proactive in defending systems against black hat attacks, sometimes even engaging in offensive actions to disrupt malicious hackers.

rec 268 1

Raw Bytes

LF

5.

Recipe

From Base64

Alphabet
A-Za-z0-9+/=

☒ Remove non-alphabet chars

☐ Strict mode

Input

Qmx1ZSBiYXQgSGFja2VycyBzZSB0YWNrZXJzIGFyZSBwcmUtbGFi1bmNoIHB1bmV0cmF0aW9uIHRlc3RlcuMgaGlyZWQgYnkgY29tcGFuaWVzIHRvIGFzZCZVcyBzZW50cmVudG9yIHNLcnZpY2UgaXNjaW50cmVzZWZzZWQIA0K

rec 196 1

Raw Bytes

LF

Output

Blue Hat Hackers:These hackers are pre-launch penetration testers hired by companies to assess security before a product or service is released.

rec 196 1

Raw Bytes

LF

Practical implementation of Stegnography

Step 1:

```
(kali㉿kali)-[~]
└─$ sudo su
[sudo] password for kali:
└─(root㉿kali)-[/home/kali]
    └─# cd Desktop

└─(root㉿kali)-[/home/kali/Desktop]
    └─# touch random.txt

└─(root㉿kali)-[/home/kali/Desktop]
    └─# cat >random.txt
        just some random data ...
        ^C

└─(root㉿kali)-[/home/kali/Desktop]
    └─# ls
        2flowers.jpeg  hello.txt  jump.txt  neet.webp  'stegosteg_1559008553457 (1).jpg'
        Downloads    heoo.txt  meme_1559010886025.jpg  polo.txt  tulip.jpg
        HACK-CAMERA  ip.py     moon.jpeg  random.txt  tulip.txt
```

Step 2:

```
(root㉿kali)-[/home/kali/Desktop]
└─# steghide embed -cf 2flowers.jpeg -ef random.txt
Enter passphrase:
Re-Enter passphrase:
embedding "random.txt" in "2flowers.jpeg" ... done

└─(root㉿kali)-[/home/kali/Desktop]
└─# steghide extract -sf 2flowers.jpeg
Enter passphrase:
the file "random.txt" does already exist. overwrite ? (y/n) y
wrote extracted data to "random.txt".
```

Step 3:

```
(root㉿kali)-[/home/kali/Desktop]
└─# rm random.txt

└─(root㉿kali)-[/home/kali/Desktop]
    └─# ls
        2flowers.jpeg  hello.txt  jump.txt  neet.webp  tulip.jpg
        Downloads    heoo.txt  meme_1559010886025.jpg  polo.txt  tulip.txt
        HACK-CAMERA  ip.py     moon.jpeg  'stegosteg_1559008553457 (1).jpg'
```

Step 4:

```
(root@kali)-[/home/kali]
# cd Desktop

(root@kali)-[/home/kali/Desktop]
# steghide extract -sf 2flowers.jpeg
Enter passphrase:
wrote extracted data to "random.txt".

(root@kali)-[/home/kali/Desktop]
# cat random.txt
just some random data ...
```