Sanity Check

1. Cek History dari docs
2. Found Flag
3. hacktoday{welcome_to_hacktoday_2020_broda__s8jm}

Daun Singkong

1. Unzip file daunsingkong.zip
2. Lihat .bash_history, ada command untuk zip nya dengan password menggunakan ls
3. Lihat .DS_Store, analisis menggunakan online tool https://labs.internetwache.org/ds_store/
4. Bersihkan nama file duplikat
5. Gunakan perintah yang sama untuk mendapatkan password zip
6. Extract menggunakan password, lihat flag.png, dapat flag.

BabyVol

1. Cek info memory menggunakan volatility, `vol.py meminfo -f dump`
2. Suggested profile Win7SP1x64, pakai itu untuk melihat proses yang berjalan
3. Tidak ada proses yang mencurigakan, lihat hint, “I command you…”, coba lihat command history menggunakan volatility, `vol.py cmdscan -f dump --profile=Win7SP1x64`
4. Ada flag di history

BabyPHP

1. Lihat web, ada source
2. Lihat kode, hal pertama yang terpikir adalah SHA1 collision
3. Setelah googling angka, ternyata magic hash
4. Cari magic hash untuk sha1, pakai, dapat flag yang diencode Base64 dan dipotong satu karakter di depan
5. Tebak huruf ‘a’ di depan, betul, dapat flag

Harta-Karun

1. Gunakan foremost untuk extract file zip didalam gambar
2. Extract zip
3. Urutkan text file (lo-ke-sy-en)
4. Gabungkan smua hex dalam text tersebut
5. Convert Hex menjadi file berbentuk PNG (dengan online tool(https://tomeko.net/online_tools/hex_to_file.php?lang=en))

6. buka gambar, dapet flagnya

0-seen

1. Mencari post dengan foto seperti attachment
2. menemukan komen dari akun ‘hacktoday_fake_flag’
3. bionya merupakan flag

0-seen 2

1. Mencari follower dari akun ittoday_itb
2. menemukan akun opps_apa_ini
3. menggabungkan QR Code dari 9 post tersebut
4. scan qr code
5. Flag ditemukan

Insanity Check

1. Menemukan clue ‘dont @ me’
2. mencoba tag friska
3. menemukan flag

Stegeosaurus

1. Gunakan `stegsnow -c bendera.txt`
2. Buka link GDrive yang didapatkan dan download file-nya
3. Gunakan stegsolve dan apply filter blue plane 1 dan blue plane 0
4. Di kanan atas gambar muncul flag-nya “hacktoday ez point yow”

Tebak Tebakan

1. Melakukan netcat ke IP yang diberikan
2. Menebak dengan:
    a. a = Athena
    b. b = BryanFurran
    c. c = Cleopatra
    d. d = Dionisos
    e. e = EDYRAHMAYADI
    f. f = Fuhrer
    g. g = Gordon
    h. h = Hades
    i. i = Ikarius
    j. j = Jokasta
    k. k = Kaerus
    l. l = Limos
    m. m = Moirae

    n. n = Nemesis
    o. o = Oizys
    p. p = Palioxis
    q. q = Qurea
    r. r = Rhea
    s. s = Skilla
    t. t = Triteia
    u. u = Uranus
    v. v = Venus
    w. w = Wu-Kong
    x. x = Xuthus
    y. y = Yellena
    z. z = Zagreus
3. Menggunakan pwnlib, buat kode untuk menebak otomatis dari database yang dimiliki
4. Ketika skor sudah cukup, bisa mendapatkan flag.

Nothosaurus

1. Extract zip file
2. Gunakan `binwalk` di file `ill`
3. Disimpulkan bahwa file-file ini adalah multi-part zip file
4. Gunakan `binwalk` untuk menentukan file mana yang merupakan file zip pertama dan file zip terakhir
5. Didapatkan:
    a. okay adalah part ke-1
    b. again adalah part ke-5
6. Lalu dicoba dengan `today` sebagai part ke-2 dan `be` sebagai part ke-4
7. Lalu di-unzip kelima file tersebut sebagai multi-part zip file
8. Didapat gambar bernama `broken` dan `cute`
9. Buka kedua file di `vim` dan gunakan command `%!xxd`
10. Save kedua file yang sudah di-xxd sebagai suatu file baru, misalkan `cute.txt` dan `broken.txt`
11. Gunakan `diff cute.txt broken.txt`
12. Perbedaan pada kedua file (1 karakter per line) adalah flag-nya, yaitu `hacktoday{broken_image}`

Ulti-Insanity Check

1. Inspect element, cari “hacktoday” di source
2. Ada satu kemunculan sebagai src image, ada alt nya
3. Ikuti alt nya, gambar yang ditampilkan memuat flag-nya.