Tips UTS Cyber Security

A. Preparation
    1. Buka CMD (Klik start terus klik CMD)
    2. Siapkan Notepad
    3.
B. Do Task
    1. Lv0->1:
        a. Ketikkan ini= ssh bandit0@bandit.labs.overthewire.org -p 2220
        b. Masuukan password= bandit0 *Note di copas aja passwordnya
        c. Setelah itu kettikan= ls -la *Fungsi ls -la untuk liat semua file di folder ada apa aja
        d. Ketikkan= cat readme
        e. Copy password yang muncul ke notepad
        f. Ketikan= exit
        g. Lanjut ke level selanjutnya dengan ketik = ssh bandit**1**@bandit.labs.overthewire.org -p 2220 , *Note passwordnya dari hasil notepad tadi, terus setiap level angkanya tinggal diganti

    2. Lv1->2:
        a. Ketikkan ini= ssh bandit1@bandit.labs.overthewire.org -p 2220
        b. Masukkan password yang udah disimpen sebelumnya (psw dari bandit 0)
        c. Coba ketikkan= ls -la
        d. Karena di direktorinya hanya ada 1 file dengan nama - maka untuk baca file nya harus disertakan direktorinya
        e. Ketikkan= pwd *(pwd/*print working directory* berfungsi untuk ambil path file nya)
        f. Setelah dapet direktori file nya, baru bisa di cat
        g. Ketikkan= cat /home/bandit1/-
        h. Copy password yang ada
        i. Ketikkan= exit
        j. Lanjut ke level selanjutnya.. Konsep mainnya gini terus

    3. Lv2->3:
        a. Ketikan = ssh bandit2@bandit.labs.overthewire.org -p 2220
        b. Masukkan password dari lv sebelumnya
        c. Ketikkan= ls -la
        d. Clue dari lv ini, passwordnya disimpen di **spaces in this filename**

e. Karena nama file nya ada spasinya, maka perlu ditambahkan petik di awal dan akhir nama filenya
f. Ketikan= “**spaces in this filename”**
g. Copy password yang muncul
h. Ketik= exit
i. Lanjut ke level selanjutnya

4. Lv3->4:
    a. Ketikan = ssh bandit3@bandit.labs.overthewire.org -p 2220
    b. Masukan password yang sudah disimpan sebelumnya
    c. Clue: cari file di folder inhere
    d. Masuk ke folder inhere dengan ketikkan= cd inhere
    e. Kalau sudah masuk di folder inhere, ketikan= ls -la
    f. Semua file akan muncul.
    g. Untuk buka file yang anehnya, ketikan= cat ./...Hiding-From-You
    h. Fungsi ./ adalah untuk mengambil direktori sekarang ini
    i. Copy passwordnya
    j. Ketik= exit
    k. Lanjut lv selanjutnya

5. Lv4->5:
    a. Ketikan = ssh bandit4@bandit.labs.overthewire.org -p 2220
    b. Masukkan password lv sebelumnya
    c. Clue file password nya ada di folder inhere, dengan format human readable
    d. Ketikan= ls -la
    e. Masuk ke folder inhere dengan ketikan= cd inhere
    f. Ketikan= ls -la *untuk cek semua isi yang di folder inhere
    g. Dari clus nyha password adalah human readable (berarti yang tipe file nya bukan data)
    h. Untuk melihat tipe file yang ada, ketikan= file ./* *Penjelasan: (./*) artinya mencari semua tipe di dalam folder inhere
    i. Ketikan= cat ./-file07
    j. Copy passwordnya
    k. Ketik= exit
    l. Lanjut ke level selanjutnya

6. Lv5->6:
    a. Ketikan = ssh bandit5@bandit.labs.overthewire.org -p 2220
    b. Masukkan password dari lv sebelumnya

c. Masuk ke direktori inhere dengan ketikan= cd inhere
d. Clue:
   human-readable
   1033 bytes in size
   not executable
e. Ketika sudah masuk ke direktori inhere bisa menggunakan find
f. Ketikan= find ./* -type f -size 1033c ! -executable
g. Setelah muncul nama file nya, bisa ketikan= cat ./maybehere07/.file2
h. Copy passwordnya
i. Ketik= Exit
j. Lanjut ke level selanjutnya

7. Lv6->7:
   a. Ketikan = ssh bandit6@bandit.labs.overthewire.org -p 2220
   b. Masukkan password dari level sebelumnya
   c. Clue:
      stored **somewhere on the server**
      owned by user bandit7
      owned by group bandit6
      33 bytes in size
   d. Untuk mencari file dalam server bisa ketikan find /
   e. Karena sudah ada spesifik file nya bisa ketikan= find / -type f -user bandit7 -group bandit6 -size 33c
   f. Karena banyak akses yang tidak bisa, maka ketikkan ulang=
      find / -type f -user bandit7 -group bandit6 -size 33c 2>/dev/null
      *Note disini ada penambahan 2>/dev/null (fungsinya adalah yang muncul adalah file yang ada aksesnya adja)
   g. Hasil dari command tersebut adalah direktori file nya. Untuk mendapatkan passwordnya ketikan= cat /var/lib/dpkg/info/bandit7.password
   h. Copy passwordnya
   i. Ketik= exit
   j. Lanjut level selanjutnya

8. Lv7->8:
   a. Ketikan = ssh bandit7@bandit.labs.overthewire.org -p 2220
   b. Masukan password lv sebelumnya
   c. Ketikan= ls -la
   d. Clue:
      The password for the next level is stored in the file **data.txt** next to the word **millionth**

e. Cari kata millionth di data.txt
f. Ketikan grep millionth data.txt *Note(grep untuk cari kata, millionth kata yang mau dicari, dat.txt Lokasi Dimana harus dicarinya)
g. Copy passwordnya
h. Ketikan exit
i. Lanjut level selanjutnya

9. Lv8->9:
    a. Ketikan = ssh bandit8@bandit.labs.overthewire.org -p 2220
    b. Masukkan password level sebelumnya
    c. Clue: stored in the file **data.txt** and is the only line of text that occurs only once
    d. Berarti di data.txt ada banyak text yang sama
    e. Ketikan= cat data.txt *untuk melihat datanya apa aja
    f. Ketikan= sort data.txt *untuk mengurutkan datanya
    g. Setelah diurutkan ternyata setiap data yang duplicate sama sama memiliki 10 value. Untuk menampilkan unique value bisa mengunakan uniq -u yang digabung dengan sortnya
    h. Ketikan= sort data.txt | uniq -u *Note(ada tanda | (pipeline) fungsinya untuk melanjutkan comandnya dan diekskusi berurutan)
    i. Copy passwordnya
    j. Ketikan= exit
    k. Lanjut ke level selanjutnya

10. Lv9->10:
    a. Ketikan = ssh bandit9@bandit.labs.overthewire.org -p 2220
    b. Masukkan password
    c. Clue: stored in the file **data.txt** in one of the few human-readable strings, preceded by several ‘=’ characters
    d. Berarti datanya masih acak/masih blm readable
    e. Caranya supaya readable ketikan= strings data.txt
    f. Setelah jadi readable, datanya bisa dicari pakai pipeline & grep
    g. Ketikan= strings data.txt | grep “==”
    h. Copy passwordnya
    i. Lanjut ke level selanjutnya

C. Library