

PenTest Lab Exercise Ex020 – OSInt

Goal

Get experience doing reconnaissance using open source intelligence sources.

Tasks

Background

Somewhere around 2012 to 2016, TV Land was a thing in Tallahassee. It was a venue for musical performances in the basement of a house in which Joseph N. Wilson's son, *Person X*, lived. Person X and one of the other residents of TV Land were in a chiptune band. To find out more about chiptune, you could check out [Bit Shifter's site](#).

Task 1

Find out about the band referenced above and when you have identified their album released on 2015-12-08, find the name of track number 7.

KEY003 (Concatenate the characters corresponding to that track's title to find the string following KEY003- and preceding ==)

a: Fri
b: K38cv
c: nw93C5/
d: A
e: /vC/
f: Cpj
g: 1T1d
h: aie
i: F4D3ony
j: 38H
k: 1+i
l: CzBc
m: Be3Y
n: hp
o: 6IoC0
p: WKV

q: 9lKV15
r: Be3Y
s: BkoYd
t: k
u: z4K27
v: ij
w: m8wx
x: 6om
y: fC4
z: 7OWTwE

Task 2

If you search for information on the band identified in Task 1, you will find that Person X adopted a new artist identify for subsequent projects. On February 25 of this year, a new production with 14 tracks was released. A number of vocal artists collaborated on that production. Identify the vocal artist featured on track 6.

KEY004 (Concatenate the corresponding characters to find the string following KEY004- and preceding ==)

a: J7Jew
b: M6V/8
c: RXkqTq
d: K8UUx4
e: 7Jplg
f: k1/09
g: jfHIhk
h: 0pkwgo
i: lfisp
j: Lm/Dn
k: AB/H3g
l: QPkDlE
m: AyVX
n: mr7p8H
o: /Mop7fW
p: ktPM
q: DWBsh

r: vRLwd4Lo
s: bLY
t: Bd7/o
u: /YGcXQ
v: Io+MmSG
w: SG
x: zae
y: ukV/
z: Fr1yjg

Demonstrate that you have completed this assignment by writing a (partial) penetration test report explaining the steps you took to uncover the information you found. Only an attack narrative need be provided as this is not part of your penetration test of artstailor.com. You needn't include any MITRE ATT&CK TTPs or a CVSS severity score.

Write down any assumptions you made and how you used those to extract information from sources you found. Include the answers you uncovered and the keys you identified. Remember, each key will have 22 characters between the - and the first =.