PenTest Lab Exercise 2 (Due 9 September at 9:35 AM)

Goal

Get experience doing reconnaissance using open source intelligence sources.

Tasks

Background: Joseph N. Wilson purchased a house in the city in which he attended his undergraduate institution so that his son could live there while going to school. His son is in a chip-tune band. He used the basement of this house as a venue for shows. That venue is known as “tvland.” He played in a punk band with his roommates Ryan and Rebecca when he was in high school in Gainesville and they played several shows in college.

Task 1: Find out Dr. Wilson's son's first name and use the following map to find KEY002:

KEY002  (Concatenate corresponding characters to find string preceding ==)

a: 6h
b: 3ic9
c: Grod
d: Vx
e: GKJn
f: jGHdeU
g: 3J7s3
h: gfm3
i: qXar
j: JbuH
k: gfm3
l: U2WG
m: SeY/Zk
n: z9
o: vn0I
p: l
g: asdf8
r: 30FJk
s: Qhpg
t: 3e
u: 3
v: Uq25
w: ++494
x: ab8n3
y: 8NK3
z: 36HwP

Task 2: Find the name of Dr. Wilson's son's current band and identify their most recent 6 August 2014 album release. Use the name of track 12 to find KEY003:
KEY003 (Concatentate corresponding chracters to find string preceding ==)
a: abiCH
b: kHCi1
c: 9JG
d: 8Z/kM
e: Lhvi4
f: 8q8
g: Ufkube
h: bdECI
i: KB1
j: F+3msJluy
k: vk3kw
l: 6bz
m: fjduuc
n: jISY
o: w+IU
p: jf183
q: flje
r: +akvu
s: KB93
t: x4H
u: 438g
v: K7d
w: af
x: 3ivu
y: 3Auuc
z: vu3

Demonstrate that you have completed this assignment by creating directory ex2 on your account on loot.pr0b3.com. Store the two keys you discover in files in that directory (named KEY002 and KEY003 containing the key strings in appropriate format, i.e. KEY###:xxxxxxxxxxxxxxxxxxxxxxxxxxx==) and create a file called report.html in that directory that dradis report of the steps you took to find the required information to retrieve them. Be specific but brief. Provide URLs to any relevant web sites.