Python For Hackers and Penetration Testing

A bit about myself

- Oltjano Terpollari
- Email:oltjano13@gmail.com

Why Python?

- Quick scripts
- Multiplatform
- Rich in modules
- Easy to read code
- Interactive shell, a big +

Set up your development environment

- Download and install Python
- Installing Third Party Libraries
- Download driven python tools (sqlmap, SET,PDFID,scapy)
- Or Download Backtrack,Kali Linux and boom

Networking

- Sockets, sockets , sockets …

Sockets

- What is a socket?
- Server
- Client

Sockets

- What is a socket?
- Server
- Client

Server

- Bind to interface, s.bind()
- Listen for connections, s.listen(13)
- Accept connection/connections, s.accept()
- Receive data, s.recv()
- Send data, s.send()

Client

- Connect to the server, s.connect((Host,Port))
- Receive data
- Send data

Cook Backdoors

- Backdoor in 13 lines
- Compile the backdoor
- Upload on virustotal.com and test it

Next?

Phishing

Social Engineering

SET

- What is SET?
- Cool features
- Nice to spread backdoors

Dictionary Attacks

- What is a Dictionary Attack?
- Wordlists
- Python makes easy
- Open('filename.txt','r')
- Unix Password Cracker (demo)
- ZipFile password Cracker

Cracking Hashed Passwords

- Import crypt
- Crypt.crypt() function
- Password and salt
- define crack() function
- Main() function

Crack Zip files

- The concept is the same
- The zipfile module
- ZipFile class
- Extractall() method

Time is money

Nmap and Python

- Why using Python with Nmap?
- Nmap module
- Download and Install nmap module
- How to use it?
- A simple script (demo)

python-nmap

- python-nmap-0.2.7.tar.gz – 2013-02-24, python 3.x
- python-nmap-0.1.4.tar.gz, python 2.x
- http://xael.org/norman/python/python-nmap/

Installation

- Uncompress
- Run , python setup.py install

Nmap module

- PortScanner() class
- The scan() function

Sqlmap

- What is Sqlmap?
- Download, unpack , run
- Basic commands
- Waf

Questions?