EVOLVE
Security Academy

Presents:

Security and Python 101

Disclaimer

Don't try to hack into other companies or other peoples personal accounts.

It is illegal. Use your own lab or authorized resources.

Python

- A high-level and general purpose language (often referred to as a scripting language)
- Reasons for using Python in InfoSec:
  - Low complexity
  - Human readable code
  - Limitless libraries and third party modules
  - Automation!

Python Based Security Tools

- To name a few…
  - sqlmap, hydra, w3af, volatility

- While using pre-built tools is great, we are subsequently bound by their functionality.

Pip

- Pip is a package management system for Python software packages
- Pip comes pre-installed with Kali
- Isolated Python environments can be created with virtualenv

Lab Setup

- All scripts should be ran within your Kali Linux VM as root
- Open the *terminal* application
- Make a new directory called *evolvesec*
- Use *vim* or *gedit* as your text editor
- Run your scripts with *# python script.py*

Lab 1: Sockets

- A **network (internet) socket** is an endpoint of a connection in a computer network .
- A **raw socket** is an internet socket that allows direct sending and receiving of Internet Protocol packets without any protocol-specific transport layer formatting.

Lab 1: Sniffer

- A **packet sniffer** (also known as a **packet analyzer**) is a computer program or piece of computer hardware that can intercept and log traffic that passes over a digital network or part of a network.
- The sniffer captures each packet and, if needed, decodes the packet's raw data.

Lab 1.1: Basic Sniffer

- Goal:
  - Follow the handout Section 1.1 to create a raw socket sniffer program in Python.
  - If you do not see any output, try opening another terminal window and running and continuous *ping google.com*. You can halt your script and ping with CTRL + SHIFT + C *or* CTRL + C
  - What is the problem with the output?

Lab 2: Scapy

- Scapy is a powerful interactive packet manipulation program. It is able to forge or decode packets of a wide number of protocols, send them on the wire, capture them, match requests and replies, and much more.
- http://www.secdev.org/projects/scapy/doc/
- https://github.com/secdev/scapy/archive/v2.3.2.zip

Lab 2: Scapy

- Lab 2.1 Goal:
  - Follow the handout Section 2.1 to perform a packet capture with Scapy.
- Lab 2.2 Goal:
  - Follow the handout Section 2.2 to create a basic sniffer script using the Scapy library.

Lab 3: Mechanize & XSS

- Mechanize is a python package for stateful programmatic web browsing, influenced by Andy Lester's Perl module WWW::Mechanize.
- Cross Site Scripting (XSS) attacks are a type of injection, in which malicious scripts are injected into otherwise benign and trusted web site.

Lab 3.1: XSS

- Goal:
  - Follow the handout Section 3.1 to create a script using Mechanize to automate testing for XSS.
  - We will be using webscantest.com as the target (this site is meant to test web app scanners).
  - You must install mechanize with *pip install mechanize*.

Contact

- Brian Liceaga
  - Brian@EvolveAcademy.io

- Stay Involved!
  - Slack.EvolveSecurity.io
  - Twitter.com/TheEvolveSec
  - Github.com/EvolveSecurity

www.EvolveAcademy.io
www.EvolveSecurity.io

EVOLVE
Security Academy

Lab 1.2: Parsing Sniffer

- Goal:
  - Create an enhanced raw socket sniffer program that parsing the output in Ascii.

- **Note: Complete this one at home**