CYBRARY

Developing Ethical Hacking Tools with Python Glossary

Created By: D'Andre Crumby

Active Information Gathering - Involves information gathering techniques, where there is contact between the Pentester and the target machine

Arguments – A value that is passed between programs, subroutines or functions.

Automation- the creation of technology and its application in order to control and monitor the production and delivery of various goods and services. It performs tasks that were previously performed by humans

Brute Forcing- A programming style that does not include any shortcuts to improve performance, but instead relies on sheer computing power to try all possibilities until the solution to a problem is found.

Call to Action - An exhortation or stimulus to do something in order to achieve an aim or deal with a problem

Cross Check - to determine the accuracy of (something) by checking it with various sources.
Command Line Argument – Python arguments that are passed through a program, They allow you to make a program act in a certain way.
E.X.
"sys", "argv " "docopt

Exploitation - is a piece of software, a chunk of data or a sequence of commands that takes advantage of a bug or vulnerability to cause unintended or unanticipated behavior to occur on computer software, hardware, or Closed Ports

Extenuate – to lessen or appear to lessen the seriousness or extent

Filtered Ports- Ports that can't be detected by scan, usually is running firewall
Foot Printing – is the technique used for gathering information about computer systems and the entities they may belong too.

I.P. Address (Internet Protocol Address) – is a numerical label assigned to each device connected to the internet

Intelligence gathering- The act of gathering various, different pieces of information about your target

Key Logger- a computer program that records every keystroke made on a computer

Methodology - a systematic or theoretical analysis

Nmap- a free open source network scanner used to discover hosts and services on a computer network by sending packets and analyzing the response

Output file - a computer file that contains data that are the output of a device or program.

Parameter – In computer programming, a parameter or **a** formal argument, is a special kind of variable, used in a subroutine to refer to one of the pieces of data provided as input to the subroutine.

Parsing – the process of analyzing a string of symbols, in regular language, computer language or data structures

Penetration test – an authorized simulated cyberattack on a computer system, preformed to evaluate the security of the system

Port scanner – a tool designed to probe a server or host and distinguished between open, closed and filtered ports

Post exploitation – the part of the penetration test where the victim's system has been compromised

Python – a high-level general-purpose programming language

Ping – a networking tool to test if a particular host is reachable. Its also a diagnostic that checks if your computer is connected to a server.

Pre- engagement Interactions - are all the meetings and documentation that must occur prior to any penetration testing actions

Scapy- a python program that enables the user to send, sniff, dissect and forge network packets

Threat modeling-is a procedure for optimizing network security by identifying objectives and vulnerabilities, and then defining countermeasures to prevent or mitigate the effects or threats to the system

Traceroute – a computer network diagnostics command for displaying the route and measuring transit delays of packets across a network

TCP (Transmission Control Protocol) – is a standard that defines how to establish and maintain a network conversation in which applications can exchange data.

Variable- a storage location paired with a associated symbolic name, which contains information

Vulnerability analysis – is the process of defining, identifying, classifying and prioritizing vulnerabilities in computer systems, applications and network infrastructures

Volatility- used to describe how unstable or changeable a system is