Chapter #1: Preparation for hacking

1. Every aspiring hacker should learn how to use a programming language in order to discover and exploit weaknesses in a computer.
2. Learning a programming language will also allow you to increase your probability of hacking success and decrease the likelihood of getting detected by IDS (intrusion detection systems), antivirus software, or tools that are used by law enforcement
3. By being able to code programs on the go, you will also be able to detect and prevent attacks as they happen. Being able to code your own hacking tools will also allow you to contribute to the community of hackers that are sharing their resources with you – by discovering a better way to perform an attack, do a countermeasure against an illegal hack, or update security protocols or abilities of a known tool, you will be able to do your share in making your computing world

What is Python?

1. Python is considered an open source language. This high-level language has been around since the late '80s, but has definitely survived the test of time – it is still used today to create GUIs, web apps, games, and more importantly, hacking exploits and intrusion mitigation.
2. You will also be able to run your codes on different types of devices and operating systems, such as Android, Windows, Linux, and Mac OS X.
3. Hacking, you will definitely have endless fun discovering what you can manipulate with your own programs – Python does not only allow you to exploit and manipulate laptops, smartphones, and desktops, but also allow you to run your programs on microcontrollers that are found in toys, remote controls, appliances, and virtually any device that has a computer in it.

Interacting with the Python Language

To interact using Python, you can use the IDLE (Integrated Development Environment), which will pull up the Python shell window, or the command line in Windows.

Interacting Using the Command Prompt

1. This might not be the most preferred way by hackers when it comes to interacting with this programming language, but this method will allow you to easily explore Python's features.
2. Type Python
3. Exit: Ctrl + Z, and then hit Enter, Key in "quit()", Key in "exit()"

Interacting Using the IDLE

1. Python, you will need to develop your code using an integrated development environment or IDE.
2. An IDE is an application that will provide you all the tools that you need to develop a software. Usually, these tools are a text editor that will help you tweak the source code that you are working on, a debugger, and a set of tools for build automation which you can use through a GUI (graphical user interface).
3. IDLE allows you to use these features: The Python shell window which allows you to make use of color-coded code input and output and get error messages if you input a wrong statement. A

debugger that comes with stepping, local and global namespace viewing, and persistent breakpoints Browsers and configuration A text editor that allows you to use multiple windows, colorizing for Python, autocompletion, undo, and other features

4. The menus that you can use in IDLE will change depending on the window that you have selected. The options that belong to each menu are straightforward, which means that you will not have a hard time understanding what each of them do even if you are new to programming.

Other Things You Can Use

PyCharm Educational Edition, Sublime Text, VIM, Coda

Chapter #2: Python Basics

Comments

1. These are statements that come after the # symbol.
2. Explain the problems that you are aiming to overcome or solve in your program. Take note of the important assumptions, details, and decisions that you want to perform in the code

Literal Constants

1. You take these pieces of text for their literal value.
2. Numbers: They can be integers (plain whole numbers) or floats (numbers that have decimal points)
3. Strings These are sequences of characters, which you can specify using single quote, double quotes, or triple quotes.

How to Format Strings

There are instances in which you will want to construct strings from a different piece of information. To do this, you will need to use the format() method. The format method allows you to use an argument value to take the place of a particular specification.

Variables

1. **Y**ou will need to store information in your code and then manipulate them, you will need to have some variables. Just like what the name means, variables have varying values, such as real numbers, strings, Booleans, dictionaries, or lists, which you can access through certain methods.
2. Since you need to quickly access the data you stored, you need to assign names to variables. This is where identifiers come to play. Identifiers work like code names that you use to point out to something that you have used in your code or program. Here are some rules that you need to follow when assigning them
3. The initial character should be a letter of the alphabet or an underscore. The remaining characters should consist of underscores, letters, or digits They are case-sensitive, which means that mycode and myCode do not call out the same value and not interchangeable when you assign them as an identifier.

Objects: Things that are referred to as anything in the code that exists in Python are called objects.

Lists

1. Python allows you to make use of a list data structure which is extremely useful when it comes to storing collections of objects
2. At the same time, you can also make use of several built-in techniques in Python that will allow you to insert, index, count, sort, append, remove, pop, and even reverse items in a list.

Dictionaries

1. Python's dictionary structure allows you to make use of a hash table that can be used to store virtually any amount of objects.
2. Dictionaries are extremely helpful in creating hacking scripts. For example, you can create a scanner that is designed to exploit vulnerabilities of a particular system, such as open TCP ports. If you have a dictionary that will display service names for corresponding ports that you want to exploit. For example, you can create a dictionary that will allow you to look up the ftp key, and then provide you an output of 21, which corresponds to a port that you may want to test. You can also use dictionaries to perform brute force attacks to crack an encrypted password.
3. When you create a dictionary, keys should be separated from their corresponding value with a colon, and the items should be separated using commas

Chapter #3: Writing Python Programs

How to Use Literal Constants and Variables

Physical and Logical Lines

1. What you see when you type out a program is called a physical line. What Python gets when you type a statement is called the logical line.
2. While you can use more than one logical line on a physical line by using the semicolon (;) symbol, Python encourages that programmers like you input a single statement in order to make your codes more readable.

Indentation

Python is one of the programming languages out there where white space, especially the space at the beginning of each line of code is important. By using indentation, you can group together blocks, or statements that belong together.

Chapter #4: Operators and Expressions

1. Most of the statements (also called logical lines) that you will be writing in your code will include expressions. Expressions are divided into operands and operators.
2. Operators are essentially functions that do something in your code, which are represented by symbols or keywords. They usually require pieces on information that they can work on, which are called operands. For example, if you have the expression 4 + 5, the plus (+) sign is the operator, and the numbers 4 and 5 are operands

Python Operators

1. Plus (+), Minus (-), Multiply (*), Divide (/)
2. Power (**): Raises a certain number to the power of the next operand.
3. Divide and floor (//): Divides the first operand with the next one, and then rounds the result to the nearest number.
4. Modulo (%): Gives you the remainder of a division
5. Less than (<) , Greater than (>), Less than or equal to (<=), Greater than or equal to (>=), Equal to (==), Not equal to (!=)

Expressions: Expressions are combinations of operators and values in your code.

Chapter #5: Functions and Modules

Functions: Parameters are indicated in functions in order to include an input that you can use to pass different values to the function and get a specific result that you have in mind.

Function Parameters: Functions are able to take in values that they will be able to use, which are called parameters.

Keyword Arguments: There will be instances as you code wherein you have too many parameters in your function – if you want to specify some of them, then you can use keyword arguments in order to give values for some of the parameters.

return Statement: If you want to break out of the function, or if you want to return a value from the function, then this statement will prove to be helpful

DocStrings: Python comes with a cool feature called docstrings, which is a tool that you can use to document the code that you are creating and make it easier to understand.

Iteration: There are some instances wherein you may find it to redundant to write the same code multiple times to do a similar function, such as checking different IP addresses or analyze different ports. For this reason, you may want to use a for-loop instead to iterate the same code for different elements. For example, if you wish to iterate a code for the subnet of IP addresses from 192.168.0.1 through 192.168.0.254, you can use a for-loop that contains a range of 1 to 255 to display the entire subn**et.**

Exception Handling: Even if you are already able to write a program with correct syntax, you may still go through some errors upon execution or runtime. If you want to fix the error while you are already running your code, Python's ability to perform exception handling will come in handy.

Modules: If you want to make use of the functions that you have already created from another program to another, instead of having to rewrite the entire code, then you can use modules. The simplest way to make modules is to create a file that contains all the variables and functions that you may need to use in a future program and then save it as a .py file.

Sys Module: Python has a built-in module that provides you access to all objects that the programming language's interpreter maintains or uses. Called the sys module, this module includes command line

arguments, maximum size of integers that can be used, flags, path hooks, as well as other available modules.

OS Module: Python's OS module provides a great deal of routines for different operating systems, such as Mac, Posix, and NT

Python Standard Library: Python' library is pretty much the collection of almost every element there is in this programming language. This extensive collection contains several built-in modules that allow you to access different functionalities in the system. The Python's standard library is also responsible for providing you access to modules, which are designed to enhance Python's inherent portability.

Chapter #7: Setting Up For Hacking

Installing Third Party Libraries: Third party libraries are essentially libraries that do not come native with your installation of Python.

Your First Python Program: A Password Cracker: Python's strength lies in the robust libraries that you can use when creating your own programs.

Chapter #8: Network Hacking

A network attack is any process or tactic that will allow a hacker to compromise a network's security. When you are able to perform a network attack, you can use a user's account and the privileges that are attached to it, steal or modify stored data, run a code to corrupt a system or data, or prevent an authorized user from accessing a service.

Reconaissance: The Opening Salvo to Your Attack

1. Hacking a system begins with reconnaissance, which is the discovery of strategic vulnerabilities in network before launching any cyber-attack.
2. Think of this as a hacker's research about their targets – the more information they know about the network that they want to hack, the more ideas they can gather about the best tools that they can use in order to launch attacks that are most likely to become undetected by the targeted user while causing the most damage possible.
3. Whenever you connect to the internet and send data over the web, you are leaving behind footprints that hackers can trace back to you. When that happens, it is possible that hackers will want to study your activities over your network and discover vulnerabilities in your system that will make it easier for them to infiltrate and steal data that can be of value to them
4. Python is one of the modern programming languages that allows you to gain access to BSD socket interfaces. BSD sockets give you an interface that will allow you to write applications so that you can do communications with a network right in between hosts. By doing a series of socket API utilities, you will be able to connect, listen, create, bind, or send traffic on a target's TCP/IP sockets.

5. If you are able to know the IP address and the TCP ports that are associated with the service that you want to target, then you can better plan your attack. Most of the time, this information is available to system administrators in an organization and this data is also something that admins need to hide from any attacker. Before you can launch any attack on any network, you will need to gain this information first.

Making Your Port Scanner

1. Port scanning is a method in which you can assess which of the ports in a targeted computer is open, and what kind of service is running on that specific port. Since computers are operating to communicate with other devices and perform a function by opening a port to send and receive data, open ports can be a vulnerability that hackers will want to exploit. Think of an open port to be similar to an open window to a burglar – these open ports serve as a free passage to any hacker that will want to steal data or set up shop inside a computer to exploit its weaknesses for an extended amount of time.
2. A port scanner will allow you to look at the hosts and the services that are attached to them.

Using the Mechanize Library to Perform Anonymous Reconnaissance

1. Most computer users use a web browser to navigate websites and view content over the Internet. Each website has a different features, but will usually read a particular text document, analyze it, and then display it to a user, just like the way a source file interacts with the Python interpreter.
2. Using Python, you can browse the internet by getting and parsing the HTMLsource code of a website. There are different libraries that come with this programming language that can handle web content, but for this hack, you will be using Mechanize, which includes the primary class called Browser.

Ensuring Anonymity While Browsing

1. Now that you know how to get a webpage, you will want to create a script that will allow you to anonymously retrieve information from a website. As you may already know, web servers see to it that they log the IP addresses of different users that view their websites in order to identify them. This can usually be prevented by using a VPN (virtual private network), or by using Tor. What happens when you use a VPN is that all traffic gets routed to the private network automatically. With this concept, you get the idea that you can use Python to connect to the proxy servers instead, which will give your program an added layer of anonymity
2. You will then see that the website you are trying to access believes that you are using the 216.155.139.115 IP address, which is actually the IP address that your proxy provided you
3. At this point, your browser already contains a single layer of anonymity. However, websites do use a string called user-agent in order to identify unique users that log in to their site. This string will usually allow the website to get useful information about a user in order to provide a tailored HTMLcode, which then provides a better user experience. However, malicious websites can also use that information to exploit the browser that is being used by a targeted user.

4. Now, you will be creating a script that will allow you to test a change on your user-agent string to the Netscape browser
5. When you run this code, you will be able to see that you are able to browse a webpage using a false user-agent string. The website that you are browsing now thinks that you are using a Netscape 6.01 browser instead of simply using Python to fetch the page.
6. What happens after is that websites that you are going to visit will attempt to present cookies that they can use as a unique identifier in order to identify you as a repeat visitor when you go back to their site the next time. To prevent these websites from identifying you, you will need to see to it that you clear all the cookies from your browser whenever you perform functions that you want to be anonymous. Another built-in library in Python, called the Cookelib, will allow you to make use of various container types that will allow you to deal with cookies that website present you. For this script, you will be using a container type that will allow you to save cookies to disk, and then print out the cookies that you received during your session.
7. When you run this script, you will see your session ID cookie for browsing the Syngress site

Finalize Your Anonymous Browser into a Python Class

1. In order to make the entire process of importing all these functions to all files that you will be creating in the future, you will need to turn that into a class. This will allow you to simply call the class using a browser object in the future.
2. This class now contains user-agents list, as will as proxy server list that you may want to use when you browse.
3. The anonymize function will also allow you to select the option to wait for 60 seconds which will increase the time of requests that you send. While this will not change anything in the information that you submit to the website, this step will decrease the chance that the websites that you are visiting will recognize that the information being sent to them comes from a single source. You will also notice that the file anonBrowser.py includes this class, and should be saved in a local directory containing scripts that will call it.
4. Using this script, you should be able to visit the targeted website anonymously five times, which will allow you to enter five votes using the same computer
5. After running this script, you will be able to fetch the targeted web page using five different unique sessions, which means that you are using different cookies every time you visit.

Chapter #9: Wireless Attack: Dnspwn Attack

This attack is created by using the airpwn tool, which is a framework for packet injection for wireless 802.11. This tool is created to listen to incoming packets and then injects content to the access point when the incoming data matches a pattern that is specified in the config file. To your target, your airpwn looks and behaves like the server that he is trying to communicate to. This tool was first created to target HTTP, but it can also be used to exploit DNS.

Using a dnspwn attack entails luring your target to visit a malicious webpage that will install malware to your target through download, or to spoof a particular website to steal your target's credential.

1. Setup your wireless monitor: In order to sniff your target's wireless activity, you will need to setup your wireless card adapter to monitor mode. you will be able to capture data right in the demo_insecure (target) network.
2. Create your code: make use of the scapy module in order to perform the dnspwn attack. To do this, you will need to sniff all the UDP packets that comes with the port 53 destination and then send the packet to the send_response function that you will create later. we can now make the function that will allow you to construe the request for the needed information and then do response injection.
   802.11 Frame – switch the "to-ds" to "from-ds" flag, which will make it seem like the requests that you are making are coming from the access point
   802.11 Frame – change the Mac addresses of the destination and source
   IP layer – change the IP addresses of the destination and source
   UDP layer – change the ports of the destination and source
   DNS layer – Put in the "answer" flag, and then add the answer that you have spoofed.
   The scape module makes the entire process simple by removing away a lot of details that you do not need to be concerned about.
3. You have all the flags set for your attack. The next step is to make and add the DNS answer
4. Inject the response that you have spoofed
5. Windows Poweshell → Run as administrator → wsl --install kali-linux

Chapter #10: Kick a User Out of Your Network

1. There is a certain limit when it comes to sending and receiving data through the network and your own networking interfaces. The reason for this limit is the amount of bandwidth that you have, and if other users are not hogging the bandwidth, the faster your connections will be.
2. When all the bandwidth that should be available to you, you are experiencing a DoS (Denial of Service). You can actually force a DoS to another user by searching and manipulating a remote host's service. Once you already found that service, you can make the program behave in a way that it is not supposed to do, which will cause the remote host to take up all its available resources and then take it offline. Alternatively, you can also cause a UDP flood, which is done by sending a huge quantity of UDP packets to several ports on your target's remote host. This will cause the host to ignore any application that are listening to that particular host and then reply with a packet that says ICMP Destination Unreachable.
3. Save this code as udpflood.py, and then select all file options upon saving. To run the code, pull up IDLE and then execute the program, which will prompt you to enter all the other information

that you need. Take note that this hack is directed to only one port, but if you want to exploit all other 65,535 ports that are available.

Chapter #11: Hacks for the Web

How to get past certain website protection policies in order to get a file that you want, browse anonymously, or get more information about the website that you want to penetrate to launch a massive attack.

Creating an SSH Botnet

1. exploit their vulnerabilities. One of the ways to do this is to exploit the Secure Shell protocol (SSH) in order to get login credentials from clients.
2. Bots, as the name implies, are incredibly useful when it comes to automating services in practically any device.
3. Botnets is a group of bots that are joined together by a network which allows system administrators to efficiently do automated tasks over an entire system of users that are connected together by a server or a local network. While botnets are essentially tools for easy managing of several computers, they can also be tools that you can use for unintended purposes, such as creating a DoS or DDoS (Distributed Denial of Service) that may cause a website to load multiple times in a session or for commenting on social media sites continuously

Creating the C&C

1. program that will allow you to create your own botnet using another popular Python library called Fabric, which will enable you to create an application called C&C (command and control) that will allow you to manage multiple infected hosts over a secure shell host.
2. local(command) – runs a command on the targeted local system
3. sudo(command) – performs a shell command remotely using superuser (or admin) privileges
4. put(local_path, remote_path) – uploads files remotely
5. open_shell() – pulls up an interactive shell remotely
6. run(command) – performs a shell command remotely
7. get(remote_path, local_path) – downloads files remotely
8. You were able to gain control of all the machines that you have access to.

Scraping Websites that Needs Login Credentials

If you want to mine data from a website, you will find that you will first need to log in before being able to access any information that you want. This means that in order to get the data that you need, you will first need to extract all the details that you need to login to your targeted website.

Studying the Target Website

1. Here's the scenario: you want to scrape data from the bitbucket site, which you can access by logging in to bitbucket.org/account/signin. Since it is prompting you to supply user credentials,

you are unable to go into the website and mine the information that you want. As you may have guessed, you will have to build a dictionary that will allow you to put in details for the log in

Chapter #10: Understanding Attacks Using Python

Knowing User Locations Out of Tweets

1. This formula includes another Twitter user's name which tells to whom your tweet is directed to, the text of your tweet, and your choice of hash tag. There are other data included in your tweet, which may not be visible in the body of your tweet, such as an image that you want to share or a location. To a hacker, all the information in your tweet contains something that will be important in writing an attack – when you think about it, you are giving away information about the person that you are interested in, links that you and your friend are likely to be interested in, and trends that you might want to learn about.
2. The pictures, especially an image of a location, become added details to a user's profile, which for example may indicate where a targeted person is likely to go to eat breakfast.
3. When your script returns with the above results, you are likely to deduce that the these teams are tweeting live from where they are. From this output, you may deduce that the Red Sox are playing in Toronto, while the Nationals are in Denver.

Matching an IP Address to a Physical Location

1. While most bullheaded yet inexperienced hackers and online trolls think that they can hide behind a fake account to conceal their identity, you can prove that these people are not as anonymous as they think they are. In fact, there are several ways to use libraries and third-party modules in Python to unmask the location and identity of a user based on his or her IP address.
2. For example, you suspect that your system is being targeted by another hacker and you notice that your open ports are being sniffed by a particular IP address. What you will want to do once you realize this potential attack is to identify that IP address' location and report it to the authorities. Python can help you do that using a script that is similar to what is going to be discussed in this section.
3. Once you are able to download the GeoCityLite database, you will be able to analyze the IP addresses down to locating the country name, state, postal code, and a general longitude and latitude

Parse Packets with Dpkt

In this hack, you will learn how to analyze a network capture, and examine the protocol layer of each packet using the tool called Dpkt

1. The next thing that you will want to do is to match these IP addresses with a physical location.
2. By creating an additional function retGeoStr(), which will give you a physical location for the IP address that your code is able to locate.

3. This will allow you to handle all addresses that are not included in the GeoLiteCity database that you downloaded earlier or instances of private addresses.

ARP Poisoning Using Python

1. To black hat hackers, IP spoofing essentially lets them conceal their identity and location whenever they perform their attack. Doing so will also allow them to impersonate another computer system and defeat existing security measures which may require authentication based on their IP addresses.
2. One of the attacks that makes use of using falsified IP is called ARP spoofing, which involves sending a false Address Resolution Protocol (ARP) message over a targeted local area network. When done successfully, an attacker's MAC address gains the IP address of an authorized computer over the targeted network. This will allow an attacker to modify or stop all traffic, or intercept data sent over the network. Using the following code, you can catch all packets that are routed towards a targeted machine, which entails being able to see all the information that a targeted user sends out, which allows you to view private communication that is not protected by any form of encryption.

Find Information About the Targeted Machine

1. Command Prompt: ipconfig
2. You will notice that the target's default gateway IP address is at 172.16.1.254 and has an ARP cache entry with the MAC address 3c-ea-4f-2b-41-f9.

Code the Poisoning

The code above sets up your attack by inputting the target IP address and the MAC address that goes with it using the get_mac function. You have also setup a packet sniffer that will capture traffic for your targeted machine. All that is left for you to do is to write these packets out to a PCAP file that you can pull up later using the Wireshark tool, or use an image carving script.

Chapter 11: Other Nifty Hacks to Try

Prevent Detection by Antivirus

1. An antivirus software is designed to detect suspicious files in your system, such as viruses and malwares. However, being able to modify the contents of a malware will enable you to bypass antivirus detection.
2. how to create a malicious code using a Kali Linux component called Metasploit. This program can generate malware, but most of the antivirus companies can easily recognize content written by this software when they are released into a computer as they are written originally. In order to create an antivirus-proof malware, you will need to tweak the malware that you will create using software.

Create Your Malicious Program

mfspayload -1 | more Doing so will display exploits that are available for you to use

Test Your Malware

To see that the .exe file that you have created is recognized as a malware, transfer it to another computer that has an antivirus program via a USB, email, or drag it onto the desktop to copy. Almost immediately, the antivirus installed will catch it

To stop the malware, end the shell.exe file in Task Manager or restart the PC.

Edit the Malware Using Python

edit the malware code in order for it to bypass your computer's security

mfspayload windows/shell_bind_tcp C > shell

Compile the Malware and Run It

In order to run the modified malware, you will need to compile it first. To do that, pull up a command prompt and then run this command string: pyinstaller --onefile --noconsole shell.py This will create a new folder that is named "dist". This folder will have the modified malware inside it named as shell.exe. To run the malware, all you need is to open the folder and doubleclick on the shell.exe file. The Windows Firewall might block some of the program's features since it will attempt to connect to a remote server. Bypass that by selecting Allow Access. After doing so, pull up the command prompt and then run: netstat -an | findstr 4444

Retrieve Deleted Items in Recycle Bin

Create a Module To Help Find Deleted Files

Check the User ID

To decode the SID string that you found earlier you will need to access the Windows Registry and match the string with a username. You will find the key with this registry key: command prompt → reg query

Create a Keylogger Using Python Keylogging, also known as keyboard capturing or keystroke logging, is a trick used by hackers to record the keys that are pressed on a keyboard without the victim knowing that he is being recorded. By being able to record these key strokes, any hacker will be able to decipher how the targeted user interacts with his computer. This means that with a keylogger, you essentially have access to practically everything that the victim has typed on his keyboard, which includes sensitive data such as usernames, passwords, credit card numbers, and so on. Creating an efficient keylogger will enable you to conveniently steal someone else's identity, especially when your logger remains to be undetected.