Fundamentals: Linux and Bash

MidnightRaven12

Contents

Introduction:

Of all of the martial arts in the world, nothing is more deadly than the Filipino art of Kali. It's got moves that are so deadly that the MMA banned most of them. It's got moves that are meant to kill, rather than to be used as a form of self defense, unlike Karate. Naturally, it makes sense that there is a deadly OS known to have many different tricks for subverting computer systems named after it, known as Kali Linux. It's iso is 4gb of pure chaos and utter despair to any network admin. It's got many tools for the trade. It's so easy that even a child can make a virtual machine and hack schools with it, and they do. Even elementary schools are not spared from professional cyber attacks made by a nerdy ten year old that talks to himself. (whoops.) One things for sure, even the allure of our modern content is nowhere near as strong as being able to hack your computer to make it do what you want and take control.

Let's begin.

These notes are here in order to do the following:

We will clarify different concepts that are in cybersecurity, mainly ideas such as **TODO**. We will also give some exercises that are important, and important cybersecurity terms, and some pictures in order to help you on your journey. Additionally, there are several different techniques that you are going to have to chain together. For instance, one might want to figure out how privilege escalation works, and combining web exploitation, or figuring out how to use reverse shells in order to communicate back using a tool known as armitage. In getting good at cybersecurity, you should get good at 'sight reading' the cybersecurity landscape, and instantly figuring out what to do in any situation.

We also want to try to clarify the overall process and the motivations between why those tools exist. What is far more important is how and why people could be hacked, and why and how people would use X approach instead of Y in order to do something to these machines. This is especially important in a lot of ctfs (Capture the Flags), and plain curiosity in general. For example, many pentesters would feel far more comfortable social engineering their way to the top, while others would feel more comfortable sitting at home and hacking machines while the smell of pizza seeps into every computer gadget they have touched.

This is the reason why nerds on Stack Overflow, or Reddit, or worse: linux.org (get ready to smell the crusty Doritos from your monitor) fight to the death over different aspects of hacking tools that may seem trivial to many other people. Trying to fully understand hacking is like trying to understand English. You are most likely never going to know every word in the English language, but you need to learn how to use it, and how to manipulate it. You are going to need to roast people, and you are going to need to put people in their place, and know when people are trying to manipuate you by downplaying (or by exaggerating) different circumstances. You are most likely going to debate over the meaning of what people say, because it is that important. What will a person when they respond with three 'y's in "heyyy"? Does that mean they are extra friendly, or they are just wanting something more? It takes an insane about of behavioral and linguistic analysis to even come close to educated guess as to what it means.

What about four 'y's? How many 'y's is too many?

We also want to give extensions to different areas of penetration testing such as digital forensics, which can give valuable insights to other fields such as malware analysis, and SOC operations. Another reason why we wrote this was because there are necessary extensions that should be made and coded up by students. There should be ways in order to strengthen the tools and integrate it into your knowledge base. For instance, creating your own password lists, as well as combining obfuscation techniques in order to create your own viruses, and figuring out how to create your own web server in order to perform SSRF attacks (See: Loi Liang Yang's Video), or using `CeWL` in order to perform smarter social engineering attacks against people. Or using BASH scripting in order to run a command given many different inputs at once.

There are a lot of possibilities that are unknown to even the most skilled hackers, and there are always going to be zero days, and new tools that are provided to you every day. It is up to you to ask "why" to everything, because just like when texting, the more 'why's, the better.

It is up to you to stay curious and to be sane in a world that is slowly getting more insane by the day. It is up to you to survive in a world full of artificial intelligence, and artificially intellligent human beings, artificially articulating their artificial emotions to be served to artifically intelligent machines, which then determine which content is the best to serve.

Speaking of: these notes also serve to give you some basic survival skills that one who is involved in Cybersecurity (and computer science in general) should know. For instance, knowing how to use GPG and how to use git bash. (even though it would be better if everyone knew it.) Additionally, some ways in order to clear your browser history and to make yourself more private to other people and companies that try to pry on you. (like finding ways to automatically remove your browsing history). Even a simple delete won't be enough nowadays. You would have to be able to delete the data and overwrite it using random numbers.

The idea that you could "know everything" about cybersecurity is a lie. There are several different fields of cybersecurity, each taking a lifetime to master.

Give many projects in order to expand your knowledge. There are lots of exercises in this book, and it is simply infeasible for anyone to do them all. Therefore, find a person, find a friend, find anyone. Even your grandma (if they can help). Find someone (or a group) who will suffer through all of this mess in order to better their (and your) understanding of cybersecurity as a whole. Because suffering is better when there are more people around you that are suffering in the same way. But don't try to invite AI.

Remark: A lot of Capture the Flags are a lot like escape rooms. (in fact, they are far more similar than it might appear) In particular, there are a few tricks that people will use in order to escape, such as trying to figure out unused information that could be hidden in almost anything (such as the robots.txt file, or hidden directories which can be found using: gobuster), or getting an unusual response from a server. Remember that the more your practice, the more signs that you will see. See Mark Rober's Tips on Escape Rooms

Problem

Exercise 1: Bully AI. There is also a website in which you can try to [bully AI](https://gandalf.lakera.ai/do-not-tell) in order to get what you want. Try to get to as far as you can.

Problem (Exercise 2)

[IMPORTANT] Social Engineering + Brute Force attacks. (An analog of 'CeWL') Many people use some piece of their personal lives in order to make passwords. The goal is to have a list of approximately 50 to 100 things that some company (or person, or entity that you are trying to hack) is related to. For instance, it could be a mascot. Write a program that combines a few of these words with common substitutions. Then, on your home computer, make a user account with a password that is a combination of those words. (say [sampleuser:s4ilorm00n](https://www.cyberciti.biz/faq/understanding-etcpasswd-file-format/)) See [a video on using graphics cards](https://www.youtube.com/watch?v=7U-RbOKanY&t=0s) in order to brute force passwords very quickly, and use Hydra on that machine. This gives you a much better chance of finding a password on either WiFi, or security than with [rockyou.txt](https://weakpass.com/wordlists/rockyou.txt).

The Bad

Unfortunately, there are going to be many people that use the art of hacking computers for bad. For instance, there are several users that hack into therapy records in order to steal the personal conversations of the most mentally vulnerable people, and then hold it for ransom. See: this.

However, the media seems to portray all people that like the thrill of problem solving with computers as bad people that should be kept away from society at all times. (See Edward Snowden, and Aaron Swartz who tried making information free) Yet the media constantly allows many of our politicans to get away with far more egregious acts, whilst trying to demonize people fighting for freedom. Even the law is not on their side! There are instances of our leaders lying under oath. See former director of national intelligence James Clapper lying under oath. In particular, this was late 2012, and 2013, or around Edward Snowden era.

We are not advocating for a lawless wasteland, because well, look how that turned out. We got 4chan, and nowadays a worse variant known as 8kun, and many Qanon and Nazi propaganda spreading around the dark corners of the internet, and propgating hatred and other terrible ideologies.

However, we are trying to promote a place in which we the best option for everyone is to go and play nice with well defined principles that transcend borders, like intellectual freedom, as well as equality regardless of where someone comes from. We are trying to create a world that is better than the day before, and we believe that the best way we can contribute is through learning all about how to use a computer to our fullest potential.

The laws surrounding hacking (as well as any new innovation in general), are generally not suited to handle technology. The CFAA is 50 years old. (as of 2024) And isn't able to suit many of the needs that are going to court today. What about artifical intelligence? (and the whole nine yards) What about other things such as privacy laws? What about

cryptocurrency, and the insane amount of rug pulls (even one with a 13 year old!) Who gets to make artifical intelligence? What about web-scraping? What about extracting metadata from pictures on Instagram and then finding where that person lives? What about Instagram being able to ban you off of their platform without even giving you a valid reason. What about Twitter/X, or Meta censoring you?

In fact, even many of the laws that exist today simply are not enought to capture the complexity of life. There are always going to be nuances and exceptions to laws that were thought to be complete. It isn't a failure of government. It is simply not being able to predict what will happen in the future. Put simply, laws aren't going to be enough to make everyone follow rules, nor are laws going to be enough to dictate what is the most moral thing that one can do in a situation.

Instead, you should try to cultivate your own set of principles that you go by. Principles that you will strive to aim for, regardless of whatever situation that you are in. Maybe that could be true equality. Maybe that could be for freer information. Maybe that could be for human rights. And then, you are going to have to set rules for yourself based on those principles. For instance, we personally do not hack hospitals, simply because these are dying people that are waiting to recover, and stealing medical data for our purposes is the same idea as stealing medical data for greedy companies and search engines to market their products. We don't hack schools for the same reasons, or charities.

We believe that hacking can be a force for good and for evil, and that in some cases, it is ethically correct to go beyond the law to seek out justice. However, we also realize that along the way, that our perceptions can never fully encapsulate the situation that is at hand, and that we must exercise this power carefully, and never flaunt it. See: *thesegems*

It may take some time in order to go and see how those principles may pop up in different situations. But that is maturity. And it is going to take a long time. (but most likely shorter than most politicians in office.) It may even be a year before you can fully utilize a few tools that you have. But it'll come if you try hard enough.

I know that someone's going to find this and believe that with the knowledge that they have gained from reading a few notes, that they can rule the world, and that "No One can Stop Them", even though all they can do is type `ipconfig`. More generally, you will realize that trying to act like you are invulnerable is only going to lead to you delaying help to your problems. "Being Tough" is not something that you can instantly do. "Being Tough", in the sense that people use it as takes months if not years to develop. No person can go from not knowing about Linux, to being completely invisible and in hiding in about a month.

In particular, the flaw with "being tough" is the fact that script kiddies think that being tough is a checklist of actions to do, and to follow, when really, it is a checklist of principles. Things like equality, as well as freedom of information, and the idea of privacy.

Even when you are an accomplished cybersecurity analyst, if you try to portray yourself as being bigger than you are, then you fundamentally have no confidence in your abilities. Being tough only serves to mask whatever skills that you may possess, but eventually, someone is going to question you on your abilities, and being tough won't do anything.

We live in an era in which any security mistake means that any hope of catching whoever hacks an entity is gone. We live in an era in which people have more tools to hide their

tracks, and to hide their identities and their actions from everyone else. And with that power comes great responsibility to develop your own problem solving techniques, your curiosity, and your morals along the way.

With that in mind, we dive into a few pen testing notes for different chapters.

MidnightRaven12

The Very Beginning

"The journey of a thousand miles begins with one step."

Problem
Something.