The Joe Wild Library

A freely available collection of cyber security training courses,
categorised, organised, mobilised, and distributed,
for your personal development needs

Introduction

Hello, and welcome! I have decided to open up my person collection to help you guys pass the time during covid. There are two main reasons I have decided to do this.

Firstly, raising the barrier to entry is a key way people in a position of wealth and power conspire to maintain that position. It was Adam Smith who first detailed this fact in his book “The Wealth of Nations” published over 200 years ago. In it he gives the example of a corporation of a trade lobbying to pass laws limiting the number of apprentices a master can have in his employ at any given time to one. Another law lobbied for by the corporation was one extending the time of labour due to the master in payment by the apprentice for his education. The combination of these two laws were in effect to limit the amount of people at any given time who could be educated in that particular trade. This by design raised the barrier to entry by restricting the supply of education. This artificially inflates the price that can be charged for that particular trade. For hundreds of years corporations have been conspiring to restrict access to education so they can make more money. And for hundreds of years people have known about it and done nothing. It may be advantageous for the few to do this however it would be much more advantageous to the society as a whole if high quality education was freely available. An educated society is happier and is more capable of making informed decisions for the betterment of the society as a whole. I have therefore decided to free up the knowledge that currently lies dormant on my bookshelves and set up a system where we can all benefit from it as a CSOC.

Secondly, I have started making kimchi in lockdown, I have purchased a small fridge in which to store it and so I need to clean out my textbook collection to make space for it :)

What the Library Offers

The library currently holds an array of courses covering the topics of forensics, reverse engineering and penetration testing. All courses come with the slides and notes from the original course, the exercise books (some partially completed) and an accompanying usb device containing all the virtual machines and lab data required to complete the exercises. The complete list of courses included is outlined in the following pages...

FOR500: Windows Forensic Analysis

All organizations must prepare for cyber-crime occurring on their computer systems and within their networks. Demand has never been greater for analysts who can investigate crimes such as fraud, insider threats, industrial espionage, employee misuse, and computer intrusions. Government agencies increasingly require trained media exploitation specialists to recover vital intelligence from Windows systems. To help solve these cases, SANS is training a new cadre of the world's best digital forensic professionals, incident responders, and media exploitation experts capable of piecing together what happened on computer systems second by second. FOR500 builds in-depth and comprehensive digital forensics knowledge of Microsoft Windows operating systems by analyzing and authenticating forensic data as well as tracking detailed user activity and organizing findings. It teaches students to apply digital forensic methodologies to a variety of case types and situations, allowing them to apply in the real world the right methodology to achieve the best outcome.

FOR508: Advanced Incident Response, Threat Hunting, and Digital Forensics

Threat hunting and Incident response tactics and procedures have evolved rapidly over the past several years. Your team can no longer afford to use antiquated incident response and threat hunting techniques that fail to properly identify compromised systems. The key is to constantly look for attacks that get past security systems, and to catch intrusions in progress, rather than after attackers have completed their objectives and done worse damage to the organization. For the incident responder, this process is known as "threat hunting" . FOR508 teaches advanced skills to hunt, identify, counter, and recover from a wide range of threats within enterprise networks, including APT nation-state adversaries, organized crime syndicates, and hacktivists.

Volatility Labs: Malware and Memory Forensics Training

The ability to perform digital investigations and incident response is a critical skill for many occupations. Unfortunately, digital investigators frequently lack the training or experience to take advantage of the volatile artifacts found in physical memory. Volatile memory contains valuable information about the runtime state of the system, provides the ability to link artifacts from traditional forensic analysis (network, file system, registry), and provides the ability to ascertain investigative leads that have been unbeknownst to most analysts. Malicious adversaries have been leveraging this knowledge disparity to undermine many aspects of the digital investigation process with such things as anti-forensics techniques, memory resident malware, kernel rootkits, and encryption (file systems, network traffic, etc.). The only way to turn-the-tables and defeat a creative digital human adversary is through talented analysts.

FOR610: Reverse-Engineering Malware: Malware Analysis Tools and Techniques

Learn to turn malware inside out! This popular course explores malware analysis tools and techniques in depth. FOR610 training has helped forensic investigators, incident responders, security engineers, and IT administrators acquire the practical skills to examine malicious programs that target and infect Windows systems. Understanding the capabilities of malware is critical to your ability to derive threat intelligence, respond to cybersecurity incidents, and fortify enterprise defenses. This course builds a strong foundation for reverse-engineering malicious software using a variety of system and network monitoring utilities, a disassembler, a debugger, and many other freely available tools.

SEC560: Network Penetration Testing and Ethical Hacking

As a cybersecurity professional, you have a unique responsibility to find and understand your organization's vulnerabilities and to work diligently to mitigate them before the bad guys pounce. Are you ready? SEC560, the flagship SANS course for enterprise penetration testing, fully arms you to address this duty head-on.

With comprehensive coverage of tools, techniques, and methodologies for network penetration testing, SEC560 truly prepares you to conduct high-value penetration testing projects step by step and end to end. Every organization needs skilled information security personnel who can find vulnerabilities and mitigate their effects, and this entire course is specially designed to get you ready for that role. The course starts with proper planning, scoping and recon, then dives deep into scanning, target exploitation, password attacks, web app manipulation, and attacking the Windows domain, with over 30 detailed hands-on labs throughout. The course is chock full of practical, real-world tips from some of the world's best penetration testers to help you do your job safely, efficiently...and with great skill.

You'll learn how to perform detailed reconnaissance, studying a target's infrastructure by mining blogs, search engines, social networking sites, and other Internet and intranet infrastructures. Our hands-on labs will equip you to scan target networks using best-of-breed tools. We won't just cover run-of-the-mill options and configurations, we'll also go over the lesser known but super-useful capabilities of the best pen test tool sets available today. After scanning, you'll learn dozens of methods for exploiting target systems to gain access and measure real business risk. You'll dive deep into post-exploitation, password attacks, and web apps, pivoting through the target environment to model the attacks of real-world bad guys to emphasize the importance of defense in depth. Finally, we focus deep on the technological heart of most organizations, the Windows Domain. We'll cover the technical details of Kerberos and Active Directory and use that for Domain Dominance!

Provisos

There are a couple of provisos before you delve into training.

Firstly, the training is for everyone and so I will only be able to extend a loan of a course for 1 month time slots. If you are serious about wanting to complete the course within that time, it is possible but it will take a lot of work. Alternatively the course is made available on demand for 4 months so it may be more convenient to book in your 4 months dispersed throughout the year.

Secondly there are a proportion of labs for certain courses that are only possible to complete with access to the SANs virtual training network. We will not of course have access to this. This is mostly only true of the SEC560 but fear not, there are plenty of labs that can be done just using your own computer. Some labs you are missing out on can also be supplemented by similar immersive labs challenges. I would be happy to direct people to appropriate alternatives. This is the same for some of the exercises that require licenses. The main license you will not have is for VMware workstation. Unfortunately I will not be able to provide you with this. Whilst most courses will work just fine on virtualbox the FOR610 in particular requires the ability to snapshot and restore regularly. There are however options for licencing and alternative open source variants that, while slightly harder to set up, are just as feature rich. Perhaps this is something that can be arranged through your line manager.

Thirdly, I have not had time to go through all the materials and sanitize them. It may be that some of the virtual machines still have remaining snapshots or the passwords have been changed. If this is the case just let me know. I'm sure it will be fairly straightforward to get hold of the right password or reset the VM.

Service Level Agreement

Whilst this library will be made freely available to all it represents a significant investment across two different employers. I would ask that all training material be treated with respect. Any loss or damage could result in future access restrictions. As mentioned previously each course can be loaned for 1 month time periods. The course you wish to loan for a particular month must be prearranged before the first Monday of the month. It will then be delivered to your door within normal business hours on that monday so please ensure you are in to collect it. Collection once the month has ended will also be completed on the same day so please ensure your training package is all packed up and ready to go by that monday. All training material loaned has been cataloged and the loan of the material will be logged so collection of the course can be completed at the appropriate time. If you are not going to be in please make sure you arrange a suitable alternative with myself before the monday.

Please note, the usbs will be shared and used by all so please do not work directly off them. Please make a local copy of all required materials and work on that to preserve the integrity of the data.

How to Sign Up

To sign up please simply text your name, number and address to myself along with the course you wish to borrow. Orders will be made on a first come first serve basis and cannot be reserved for more than 1 month. If a course is currently reserved I will let you know of the next month where the course will be available and you can reserve it for then.

My mobile number is as follows

07511360535

For convenience of delivery and collection I will be using whatsapp's shared location feature so that you know when I am close so that you can ensure you are ready to collect or return your chosen course. If you do not have access to whatsapp please let me know and I can arrange for text based update of delivery and collection times.

Thank you, and enjoy!