Requirements a11y.text Requirements PrepareÂ your Metasploit Lab Environment a11y.text PrepareÂ your Metasploit Lab Environment Before learning how to use the Metasploit Framework,Â we first need to make sure that our setup will meet or exceed theÂ system requirements outlined in the following sections. Taking the time to properly prepare your Metasploit Lab Environment Â will help eliminate many problems before they arise later in the course. We highly recommend using a system that is capable of running multiple virtual machines to host your labs. Metasploit Unleashed Hardware Requirements a11y.text Metasploit Unleashed Hardware Requirements All of the values listed below are estimated or recommended. You can get away with less in some cases but be aware that performance will suffer, making for a less than ideal learning experience. Hard Drive Space a11y.text Hard Drive Space You will need to have, at minimum, 10 gigabytes of available storage space on your host. Since we are using virtual machines with large file sizes, this means that we are unable to use a FAT32 partition since large files are not supported in that filesystem, so be sure to choose NTFS, ext3, or some other filesystem format. The recommended amount of space needed is 30 gigabytes . If you decided to create clones or snapshots of your virtual machine(s) as you progress through the course, these will also take up valuable space on your system. Be vigilant and do not be afraid to reclaim space as needed. Available Memory a11y.text Available Memory Failing to provide enough memory to your host and guest operating systems will eventually lead to system failure and/or result in being unable to launch your virtual machine(s). You are going to require RAM for your host OS as well as the amount of RAM that you are dedicating for each virtual machine. Use the guide below to help in deciding the amount of RAM required for your situation. Linux â€œHOSTâ€• Minimal Memory Requirements 1 GB of system memory (RAM) Realistically 2 GB or more Kali â€œGUESTâ€• Minimal Memory Requirements At least 1 GB of RAM (2 GB is recommended) // more never hurts! Realistically 2 GB or more with a SWAP file of equal value Metasploitable â€œGUESTâ€• Minimal Memory Requirements At least 256 MB of RAM (512 MB is recommended) // more never hurts! (Optional) Per Windows â€œGUESTâ€• Minimal Memory Requirements At least 256 MB of RAM (1 GB is

recommended) // more never hurts! Realistically 1 GB or more with a page file of equal value Processor a11y.text Processor To ensure the best experience, we recommend a 64-bit quad-core CPU or better. The bare-minimum requirement for VMware Player is a 400MHz or faster processor (500MHz recommended) but these speeds are inadequate for the purposes of this course. The more horsepower you can throw at your lab, the better. Internet Accessibility a11y.text Internet Accessibility Getting your lab set up will require downloading some large virtual machines so you will want to have a good high-speed connection to do so. If you choose to use â€œBridgedâ€• networking for your virtual machines and there is no DHCP server on your network, you will have to assign static IP addresses to your guest VMs. Metasploit UnleashedÂ Software Requirements a11y.text Metasploit UnleashedÂ Software Requirements Before jumping in to the Metasploit Framework, we will need to have both an attacking machine (Kali Linux) and a victim machine (metasploitable 2) as well as a hypervisor to run both in a safe and secluded network environment. Hypervisor a11y.text Hypervisor Our recommended hypervisor for the best out-of-the-box compatibility with Kali and metasploitable is VMware Player . While VMware Player is â€œfreeâ€•, you will have to register in order to download it, and the virtualization applications and appliances are well worth the registration if you do not already have an account. You may also use VMware Workstation or VMware Fusion but neither of these is free. There are also other options available when it comes to which hypervisor you would like to use. In addition to VMware, two other commonly used hypervisors are VirtualBox and KVM but they are not covered here. Instructions for installing Kali Linux can be found on the Kali Training site . Kali Linux a11y.text Kali Linux Kali Linux is an advanced Penetration Testing and Security Auditing Linux distribution that will be used throughout this course. Kali Linux comes with Metasploit pre-installed along with numerous other security tools that you can try out against your victim machine. You can download the latest version of Kali at: http://www.kali.org/downloads/ Once you have downloaded Kali, you can update Metasploit to the latest version in the repos by running apt update && apt upgrade in a terminal. Metasploitable a11y.text Metasploitable One of the problems you encounter when learning how to

use an exploitation framework is trying to find and configure targets to scan and attack. Luckily, the Metasploit team is aware of this and released a vulnerable VMware virtual machine called â€˜Metasploitableâ€™. Metasploitable is an intentionally vulnerable Linux virtual machine that can be used to conduct security training, test security tools, and practice common penetration testing techniques. The VM will run on any recent VMware products and other visualization technologies such as VirtualBox. You can download the image file of Metasploitable 2 from SourceForge . Never expose Metasploitable to an untrusted network, use NAT or Host-only mode! Once you have downloaded the Metasploitable VM, extract the zip file, open up the .vmx file using your VMware product of choice, and power it on. After a brief time, the system will be booted and ready for action. The default login and password is msfadmin:msfadmin. The Metasploitable virtual machine For more information on the VM configuration, there is a Metasploitable 2 Exploitability Guide on the Rapid7 websiteÂ but bewareâ€¦there are spoilers in it. To contact the developers of Metasploit, please send email to msfdev [a] metasploit [period] com Windows a11y.text Windows Microsoft has made a number of virtual machines available that can be downloaded to test Microsoft Edge and different versions of Internet Explorer. We will be able to use these VMs when working with some of the exploits and tools available in Metasploit. You can download the VMs from the following URL: https://developer.microsoft.com/en-us/microsoft-edge/tools/vms/ Once you have met the above system requirements, you should have no trouble running any tutorialsÂ fromÂ the Metasploit Unleashed course. Next Metasploit Architecture Prev Introduction