Here is a quick look at a barebones lesson plan. I will be adding on to this as the weeks go on:

**1 - Setting Up A Penetration Testing Environment (COVERED WEEK 1)** - This will focus on setting up a lab environment, specifically VMWare, Kali Linux, and our lab VMs. The lesson will briefly introduce important aspects of each set up (e.g. Snapshots in VMWare, the Kali Linux toolset, etc.) with the intention to build upon those aspects in later lessons.

**2 - How to Keep Notes Effectively (COVERED WEEK 1)** - This lesson will cover the importance of note taking from a pentester standpoint. The lesson will introduce the Kali Linux built-in note-taking application, KeepNote, and discuss how to take notes effectively. Taking notes during a penetration test is incredibly important as it allows a pentester reference points when writing their final report, discussing timelines with their team or manager, or even discussing specifics of a pentest with a client.

**3 - The Legal Side of the House** - This lesson will cover the important legal aspects that a pentester must know prior to conducting a penetration test. For example, having a rules of engagement document that specifies which networks can be attacked and what attack methods can be used. Knowing the common legal documents that a junior pentester may encounter will give him or her an advantage in their early careers.

**4 - Introductory Linux (COVERED WEEK 1)** - This lesson will briefly cover the important Linux terminal commands needed to use Kali Linux. Some of the topics that will be covered are: navigating the file system, users and privileges, common network commands, bash scripting, and much more.

**5 - Introductory Python (COVERED WEEK 2 and 3)** - Similar to Linux, we will spend some time learning basic Python scripting, which will be essential to our future endeavors as penetration testers.

**6 - Hacking in Five Steps (COVERED WEEK 4)** - This lesson will introduce the five key components of hacking: reconnaissance, enumeration, exploitation, maintaining access, and covering tracks. These five key concepts will be built upon as we progress, with at least one part dedicated to each component.

**EXTERNAL PENTESTING**

**7 - The Art of Reconnaissance (COVERED WEEK 4)** - This lesson will discuss reconnaissance in depth and cover common tools used in the process. Some of the tools that will be covered are the OSINT Framework, SET, theHarvester, Bluto, Google Dorks, and Shodan. More tools will likely be added as the lesson is written.

**8 - Scanning Tactics (COVERED WEEK 5)** - This lesson will cover common tools in-depth that are used for port scanning including Nmap, Nessus, and Metasploit. The section will introduce readers to using a wide toolset for scanning on penetration tests and provide a deeper understanding of what is going on behind the scenes. For example, the importance of TCP vs UDP scanning, the three-way TCP handshake, stealth scanning, and various Nmap switches. It will also provide the first introduction to Metasploit and its usage, which will be built upon throughout the course.

**9 - Enumeration for the win (COVERED WEEK 6)** - The intent of this lesson is to provide an overview of basic enumeration tactics and then dive deep into specific tools used for common ports found in penetration testing. For example, if we find port 80 open on a scan (HTTP), we will likely want to know what service is running and enumerate that service for potential exploits at a high level. At a deep level, we will want to explore the app with tools such as Nikto, Dirbuster/Dirb, and Burp Suite to really enumerate the app where tools like Nmap and Nessus fail to go deep enough.

**10 - Gaining a Shell with Metasploit (COVERED WEEK 7)** - This lesson will cover how to use Metasploit to gain shell access to a vulnerable machine. This builds upon the introductory Metasploit from section 8 as we move from the auxiliary/scanning portion of Metasploit to the exploit portion. This lesson is important as Metasploit is a common tool in nearly every penetration testers toolkit, especially at the beginner level.

**11 - Compiling Exploits (COVERED WEEK 7)** - This lesson will add to exploitation learned in section 9, except that the exploitation is now done manually, without Metasploit. This will teach the reader how to safely download exploits from the web, generate shellcode, compile the exploit if necessary, and execute it against a vulnerable machine.

**12 - When Nothing Else Works (COVERED WEEK 7)** - The previous two lessons in focus on having an exploit readily available that will provide shell access. As a penetration tester, gaining shell from an exploit does not happen most of the time. Sometimes, we have to get creative. This may include using social engineering and password spraying Outlook/other web applications. The section also focuses on the failing mentality and how it is okay to not break in on every external. Lastly, it will cover some common non-critical findings/things to look for that can be added to a report, such as default web pages, public RDP, public SNMP, etc.

**INTERNAL PENTESTING**

**13 - Hello Enumeration, My Old Friend** - This lesson will cover post-exploitation enumeration. In other words, we’ve gained access to a single machine in a network, now what are we looking for? The chapter will focus heavily on Active Directory enumeration concepts as that is the likely environment a pentester will encounter in the real world. However, lessons will be provided for non-Active Directory environments as well. Important tools that will be discussed are nbtscan, nslookup, nbtstat, net commands, PowerShell commands, and more.

**14 - Active Directory Exploitation** - This lesson focuses on the recognition of vulnerabilities and exploitation tactics in an internal Active Directory environment. Attacks that will be introduced include: LLMNR poisoning/hash cracking, SMB hash relaying, pass the hash, token impersonation, kerberoasting, GPP/c-password attacks, and PowerShell attacks. More attacks will likely be added as the lesson is written, but the most common have been provided.

**15 - Exploiting Non-Active Directory Environments** - This lesson will discuss the exploitation of devices in a non-Active Directory environment. Students will learn how to identify critical servers, conduct local password attacks, and learn outside-the-box strategies for attacking. Examples will come from previous penetration tests, such as exploiting default credentials on local printers and dumping stored credentials to gain access to critical servers.

**16 - Maintaining Access / Pivoting / Cleanup** - This lesson will discuss methods of maintaining access on a network, pivoting into other networks, and how to properly clean up as you exit a network.

**17 - Report Writing** - This lesson will cover the importance of report writing in penetration testing and walk through what should be included in a penetration test report. A demo penetration test report will be provided that will cover many of the findings that we have discussed in prior chapters.