Nmap:

1. Run a scan, a stealth scan, a protocol scan, a version scan, and an ACK scan on <http://scanme.nmap.org/> Analyze your results.

2. Run all different nmap scans on all ports of the Metasploitable2 VM on the server. Analyze your results and formulate a plan of attack.

Nessus:

1. Run a discovery scan to find all the ports. Categorize the ports. Analyze which are the most vulnerable and useful to hack into.

2. Do an external scan.

3. Compare and contrast nmap and nessus.

4. Search for more useful exploits available in nessus based on the finding you got in previous scans.

5. Install a mail server in linux and scan again to see what ports are open. Also do a full set of nmap scans to reevaluate the ports.

6. Research how to secure ports and apply those skills to secure the mail server you installed.

Metasploit: First, install the following services on your kali VM:

rsh-client

rpcbind

nfs-common

1. Determine the IP address for the Metasploitable VM.

2. Login to three TCP ports on the Metasploitable VM.

3. Login as root user on the Metasploitable VM.

4. NFS can be identified by probing port 2049 directly or asking the portmapper for a list of services. Use rpcinfo to identify NFS and showmount -e to determine that the root of the file system is being exported on the Metasploitable VM.

5. Make a new SSH key, mount the NFS export, and add the key to the root user account's authorized\_keys file on the Metasploitable VM.

6. Find the built-in backdoor to access FTP on the Metasploitable VM.

7. Use the DistCC Daemon to escalate yourself to the root user on the Metasploitable VM.

8. Launch a symlink attack on Samba to get anonymous root privileges on the Metasploitable VM.