CSC427 Nmap Tutorial

We're going to be using the standard Kali and Metasploitable VMs for this tutorial.

Setup

1. Download VMWare Workstation Player if you haven't done so already
2. Download the Kali and Metasploitable VMs from here
3. Username and password for the Kali VM is root/toor
4. Open up a terminal window
5. Use nmap host discovery to find the IP of the Metasploitable VM (hint: it should be on the same subnet as the Kali VM, probably within 10 addresses of each other)

NonVM

1. What port and service does Trinity(From the cultural reference section) find open on the target IP address.
2. Which scan type is used in the above question?
3. Some ports in a UDP scan may show up as "open|filtered" on Nmap. What does this mean and why does this status exist?
4. Results in a TCP ACK scan might not line up with those of a TCP SYN scan (E.g. a filtered port in an ACK scan may show up as open in a SYN scan). Name one possible reason this could happen.

VM

1. What command would you use to get the OS of the Metasploitable VM? Submit your command
2. List of all ports open and what services each port is running on your Metasploitable VM. Submit your command and a screenshot of your output. Note: Nmap by default only scans the 1000 most common ports. How can you tell it to scan every possible port?
3. What version of Apache does scanme.nmap.org use? Submit your command and a screenshot of your output

Submission Format

- Answers should be in answers.txt
- Screenshots should be in q2.png and q3.png for Q2 and Q3 respectively
- Add members.txt with member names if working in groups
- Pack all files into nmap.zip and submit on UTORSubmit