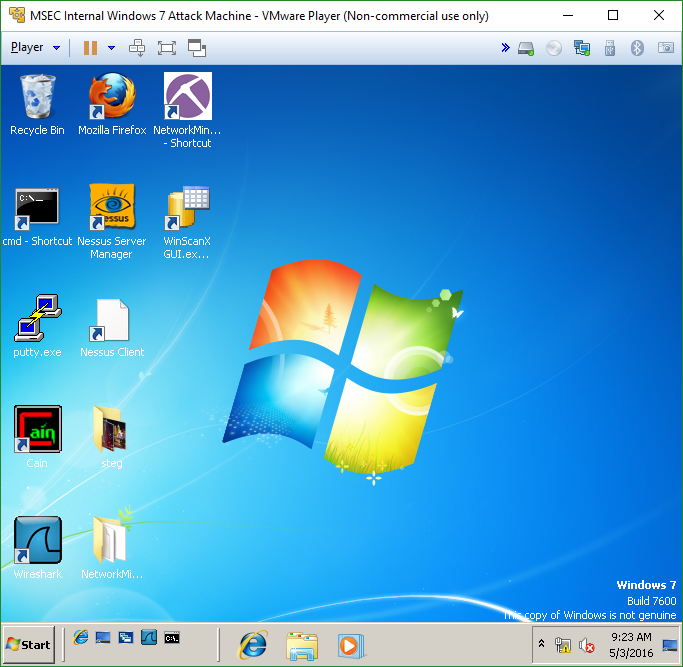
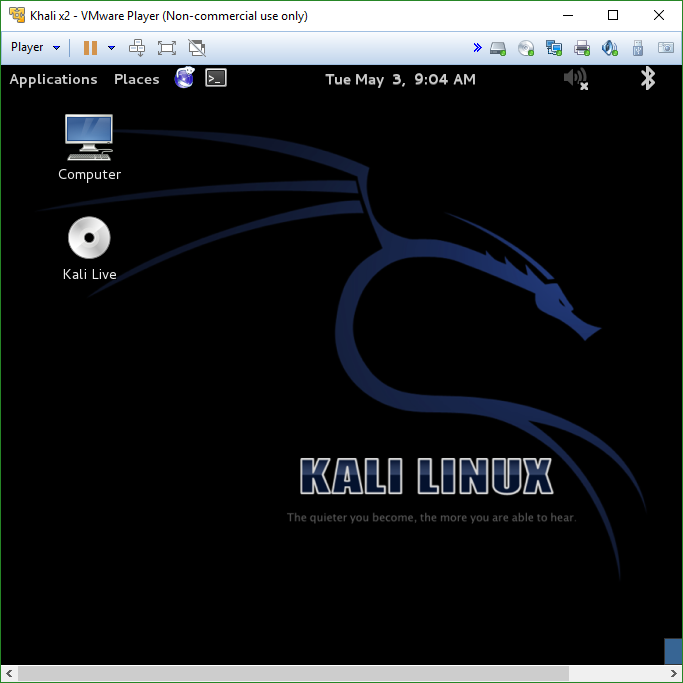
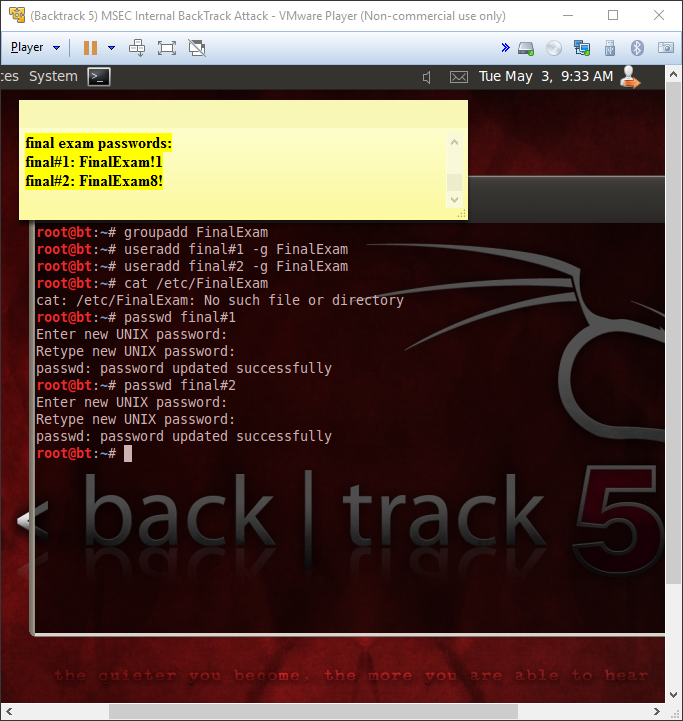
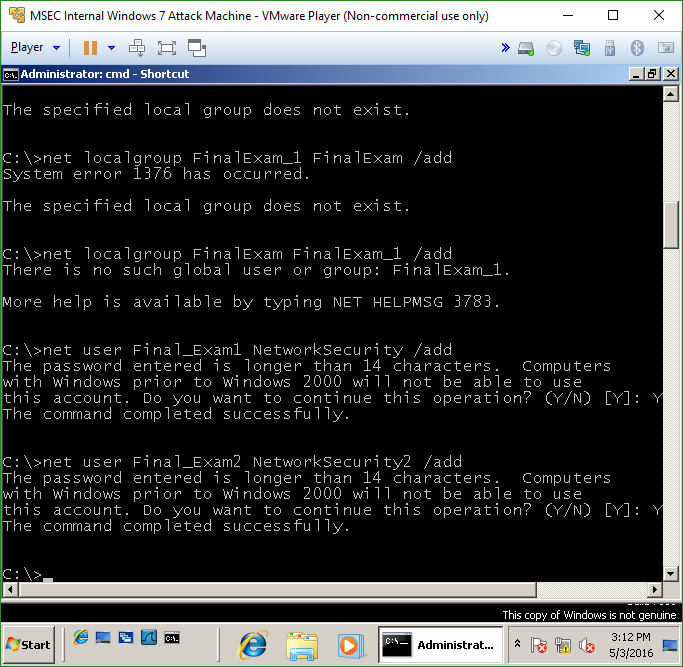
Step 1. (Assuming Windows XP means Windows 2003 server which was used frequently in the previous labs)

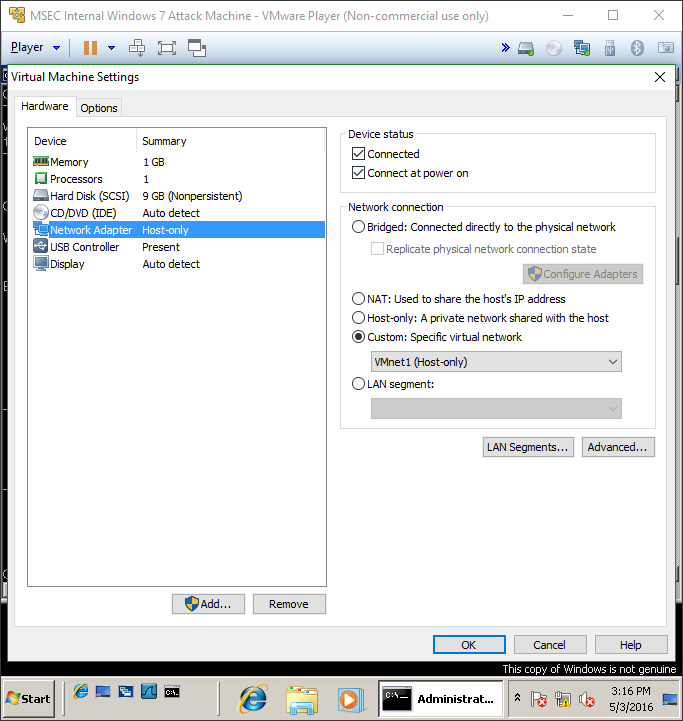
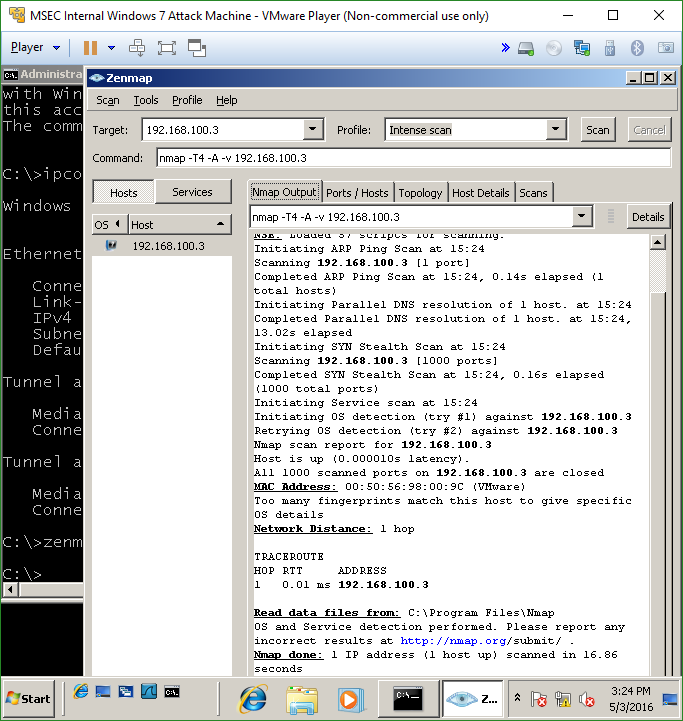
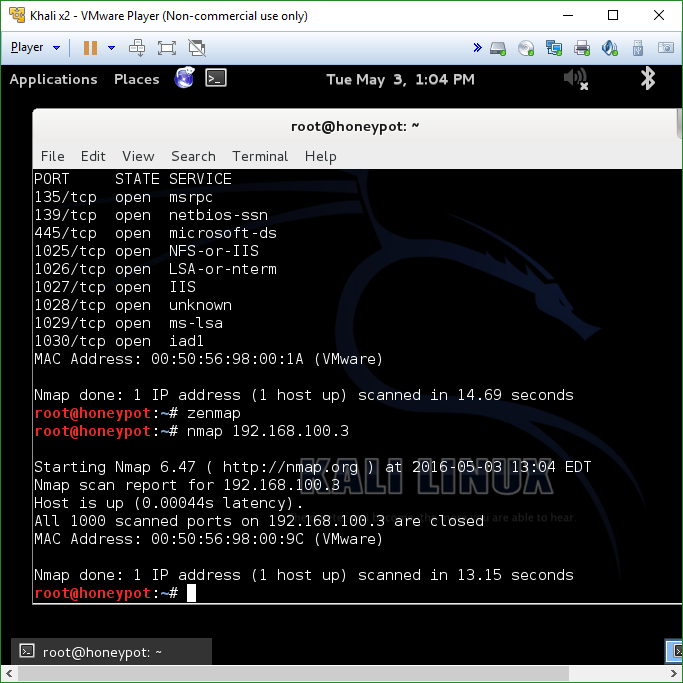
1. Windows 2003 server Internal 
2. Kali Linux
3. Metasploitable v2 (using Backtrack5 since it’s available and I don’t have Metasploitable v2, also in lab 11 we did a similar exercise so I found it more appropriate than other VM’s) 

Step 2: Group Settings

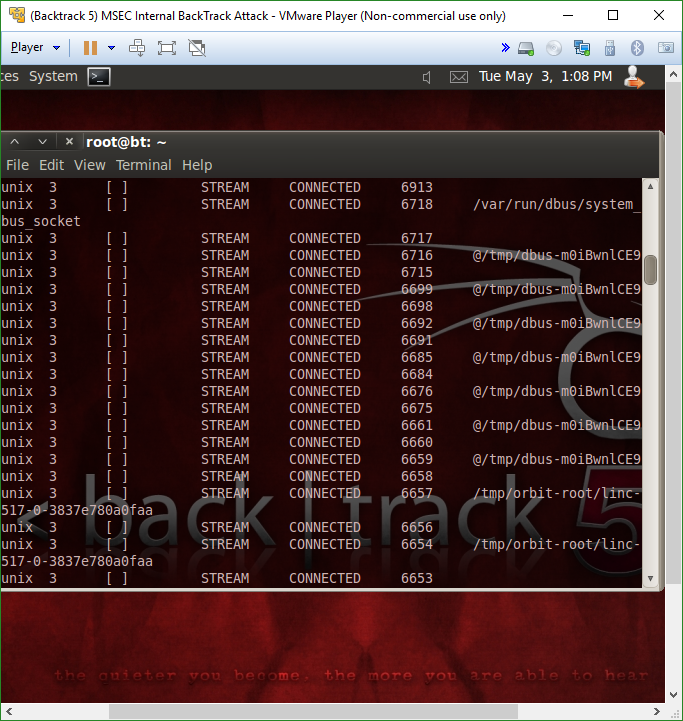




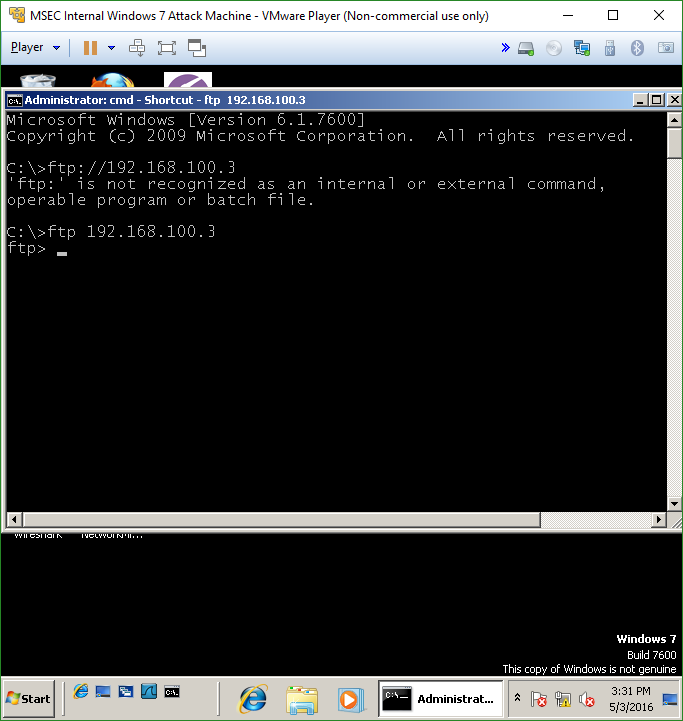
Step 3: Cross-Network Scanning

1. 
2. 
3. 

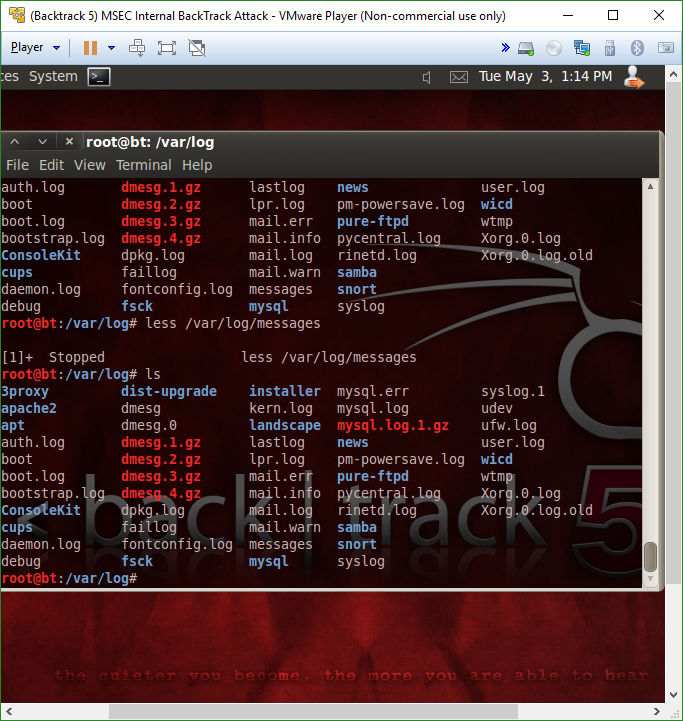
Step 4: Netstat Scanning

1. 

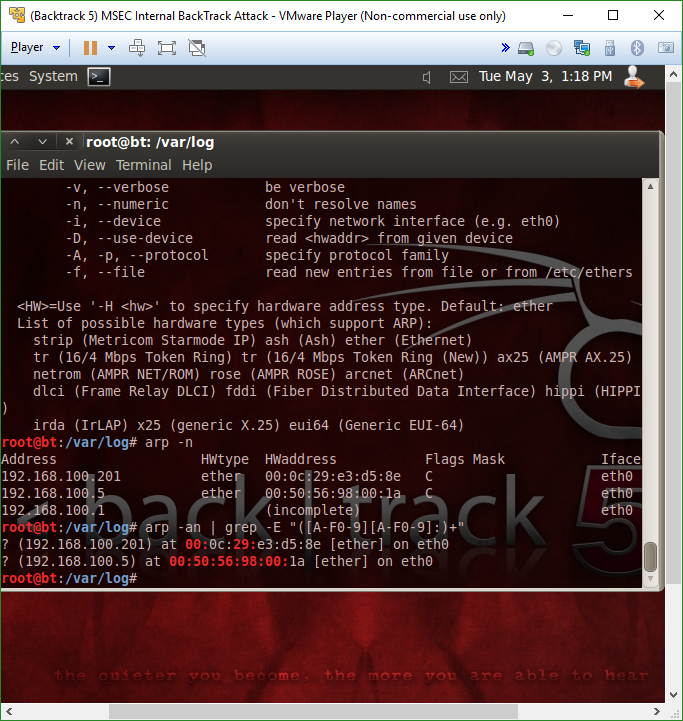
Step 5: FTP

1. 

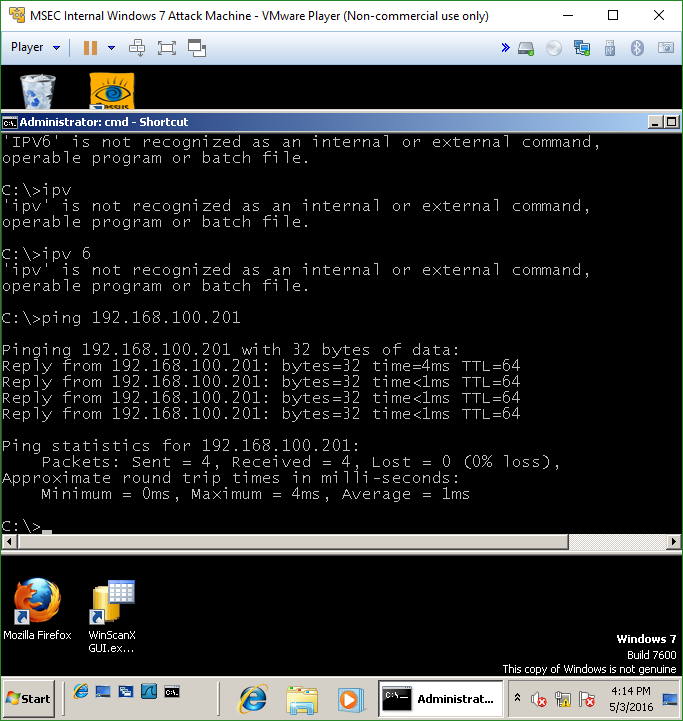
Step 6: Logging

1. 

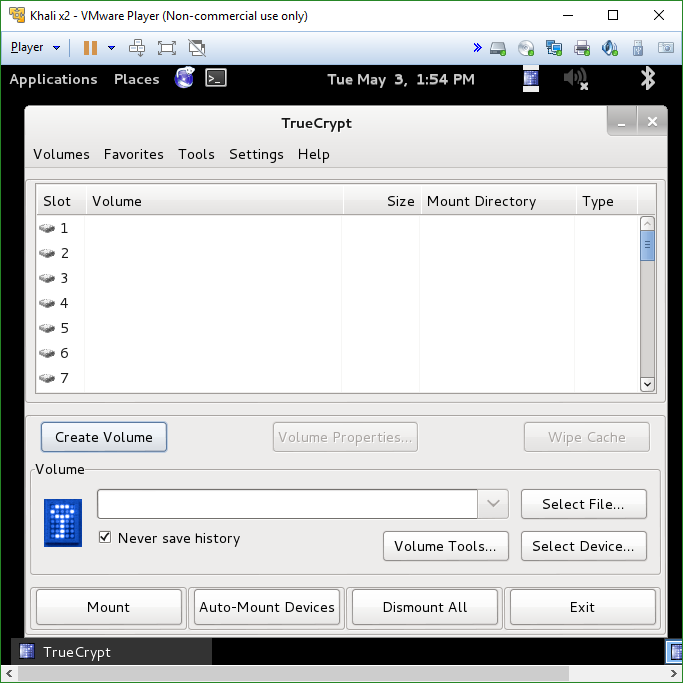
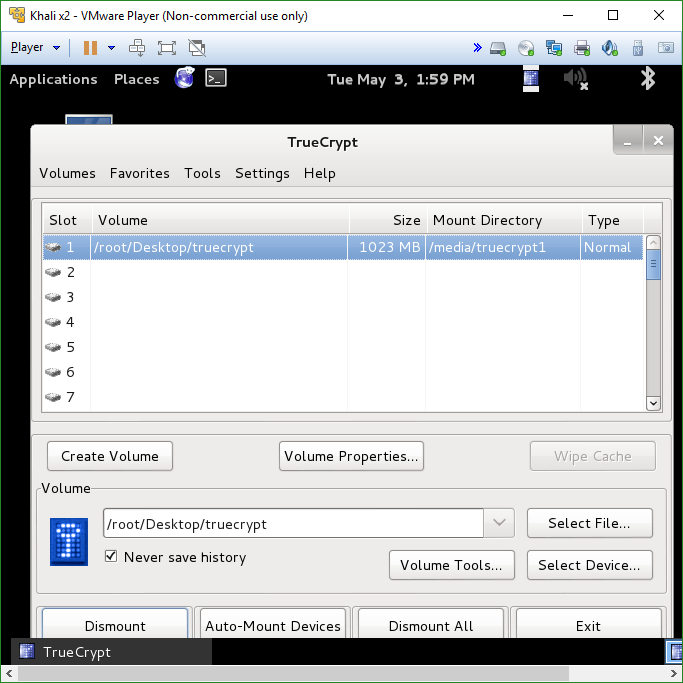
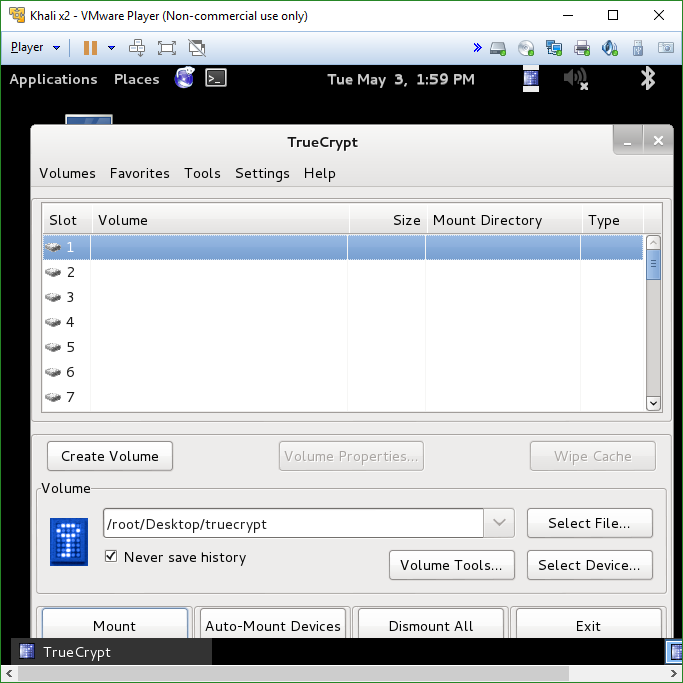
Step 7: ARP

1. 

Step 8: Logging (couldn’t download IPV6 sadly)

1. 

Step 10: Truecrypt

1. 
2. 
3. 

Part 2

1. Name the four types of backups **full backup, incremental backup, differential backup, and mirror backup**

2. Name the three classes of controls **preventative, detective, and corrective**

3. Name the three elements of the domain password policy **security accountability, incident handling and response, and security training**

4. Name the three standards of evidence **efficacy, effectiveness, and dissemination**

5. Which lab or tool was the most useful to you? **Lab 11, but ironically I found Nessus the most useful tool**