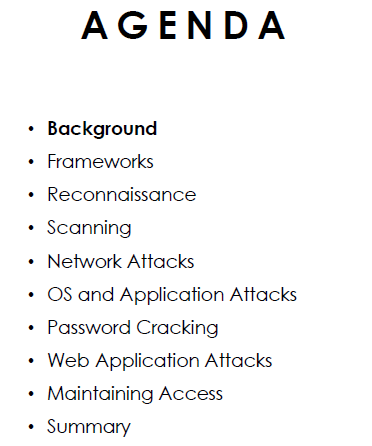
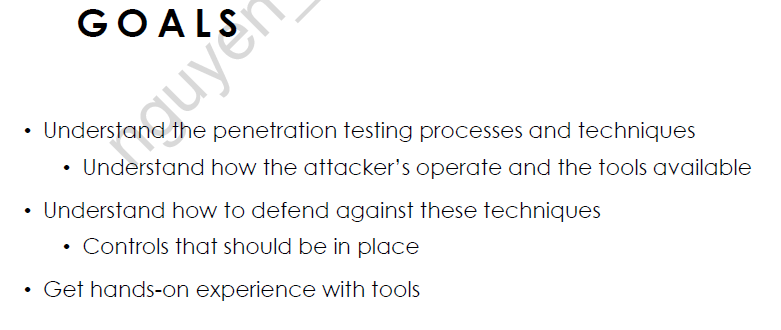


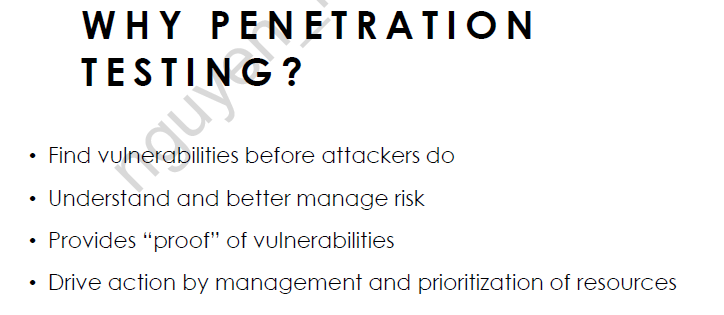
# Background



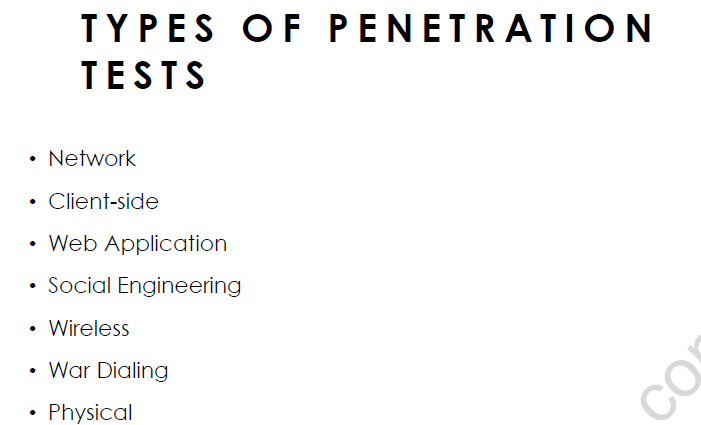
### Goals



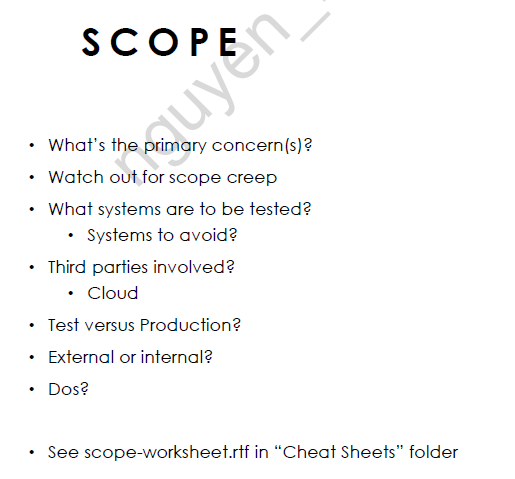
### Why PenTest?



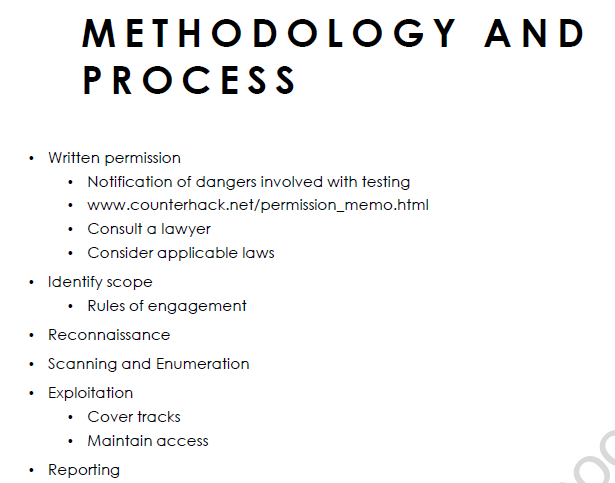
### Types of Pentest



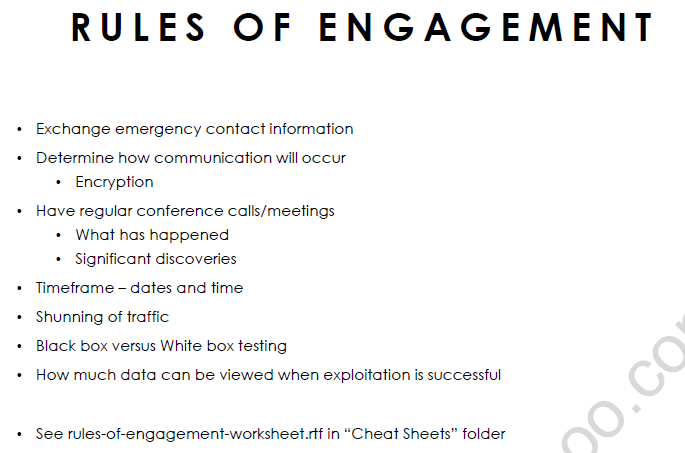
### Scope



### Methodology and Process



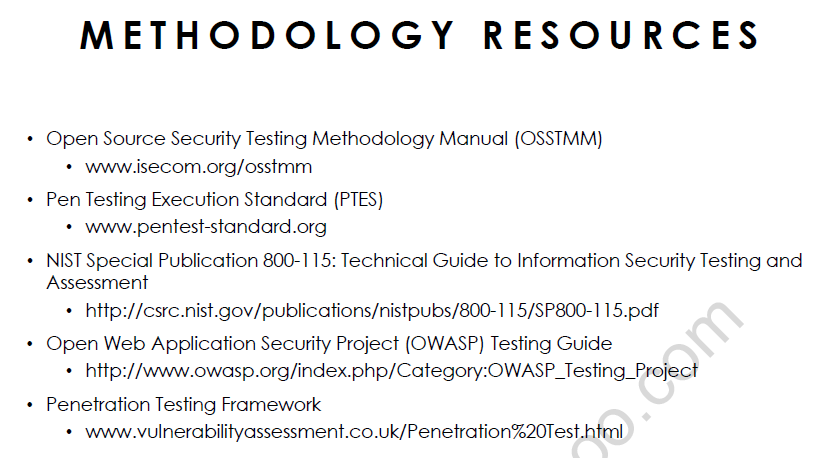
### Rules of Engagement



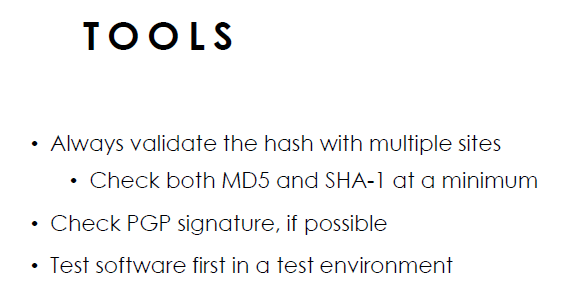
### Reporting



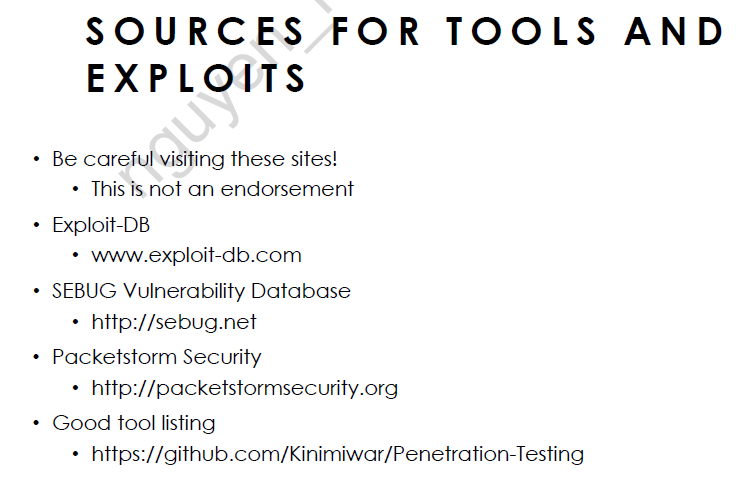
### Methodology Resources



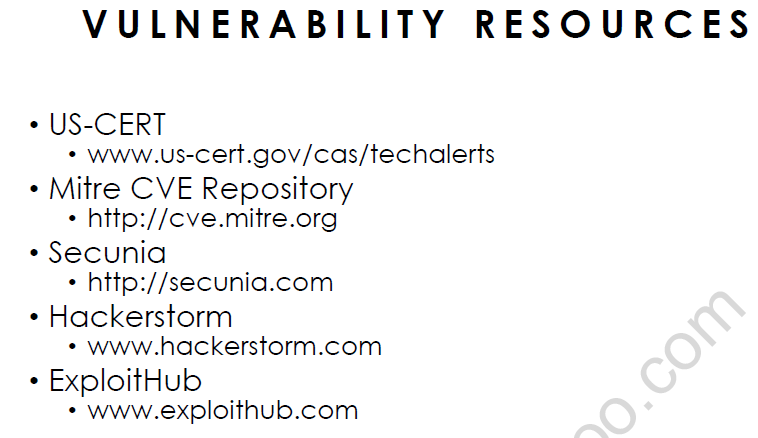
### Tools



### Sources for Tools & Exploits



### Vulnerability Resources

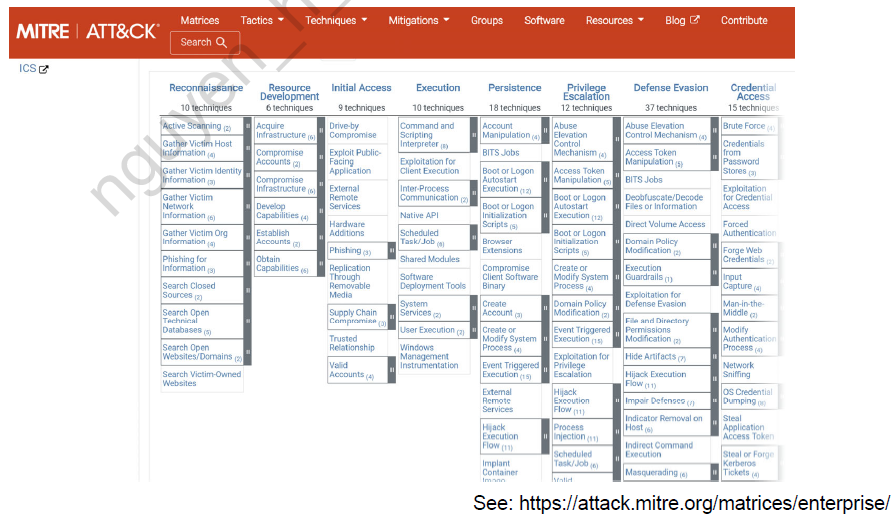


# Frameworks

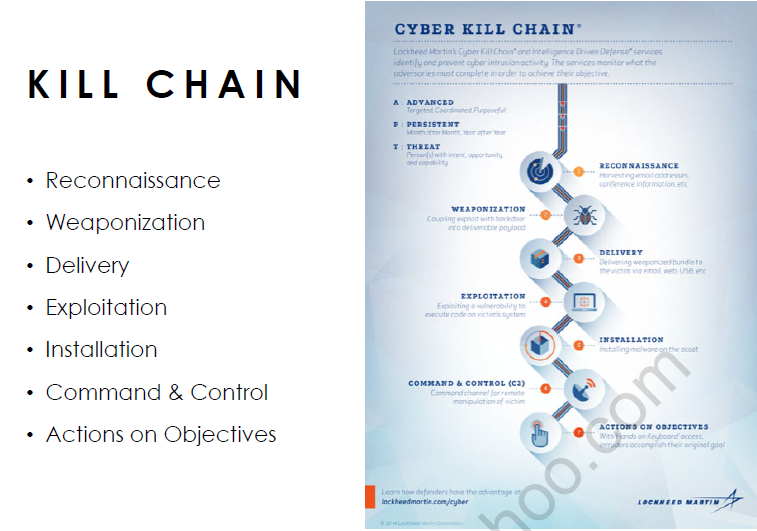


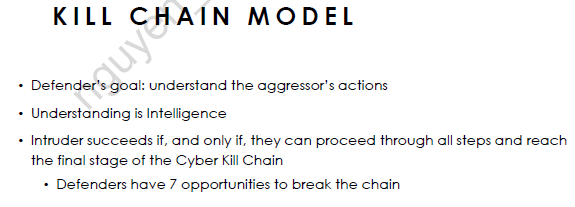
### MITRE ATT&CK



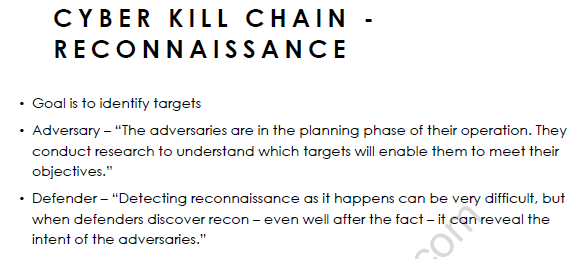


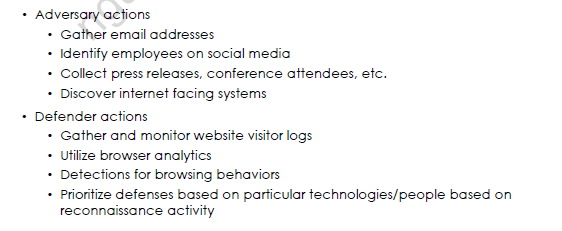
### Kill Chain



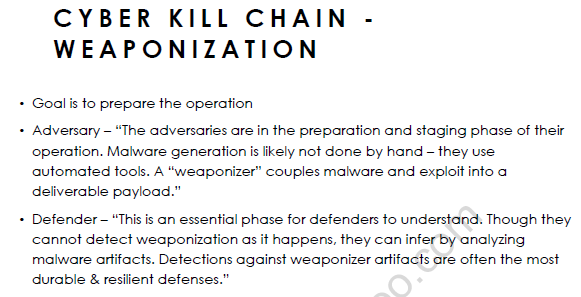


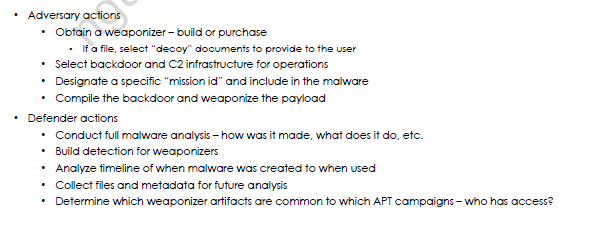
### Cyber Kill Chain - Reconnaissance





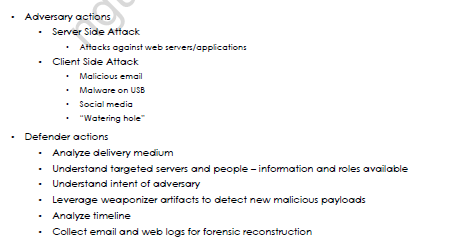
### Cyber Kill Chain – Weaponization



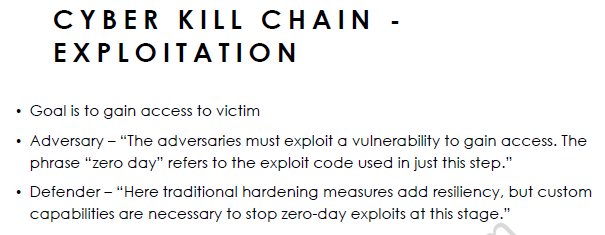


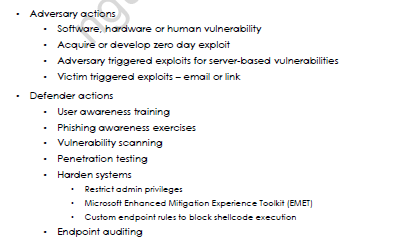
### Cyber Kill Chain – Delivery



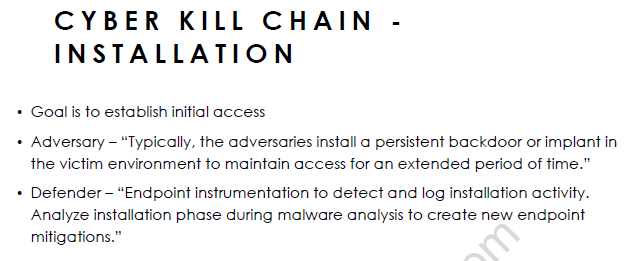


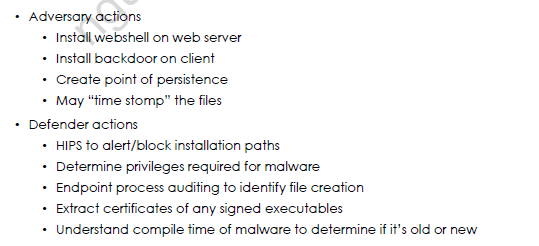
### Cyber Kill Chain – Exploitation





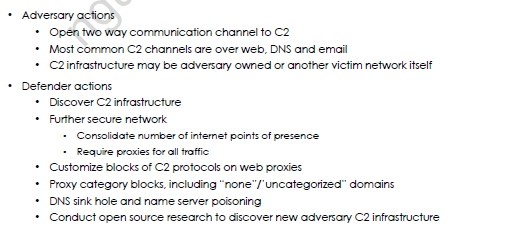
### Cyber Kill Chain – Installation



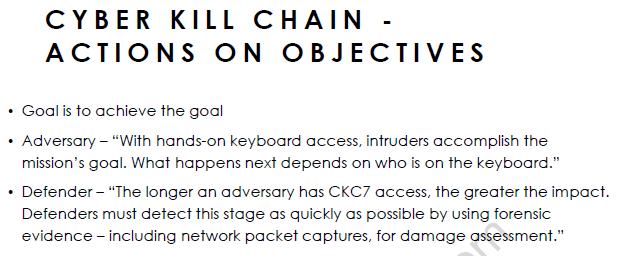


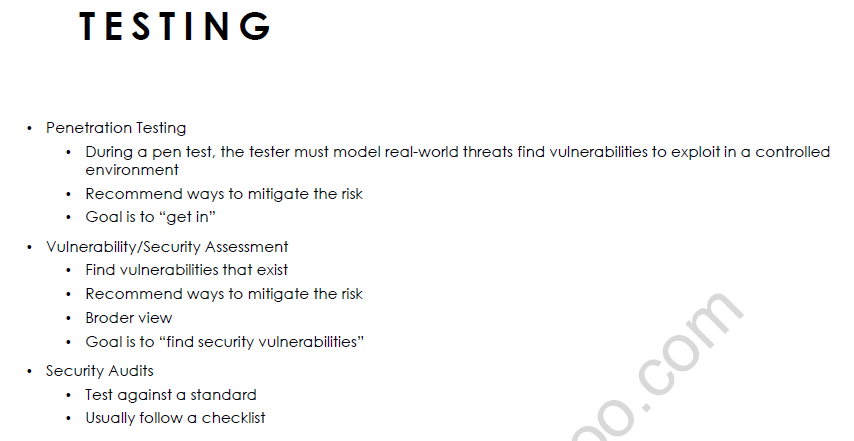
### Cyber Kill Chain – Command & Control



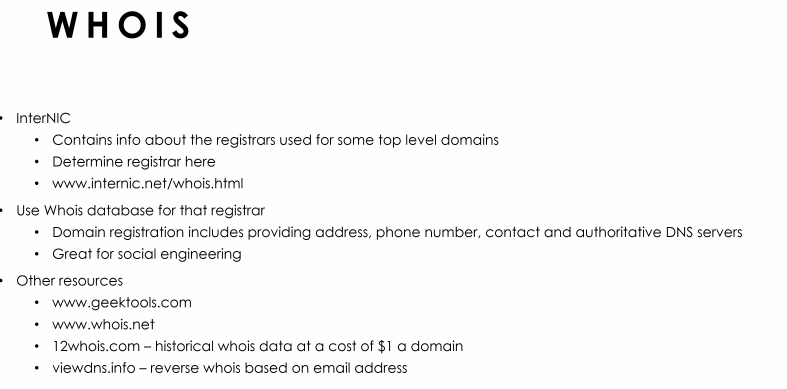


### Cyber Kill Chain – Actions on Objectives

36

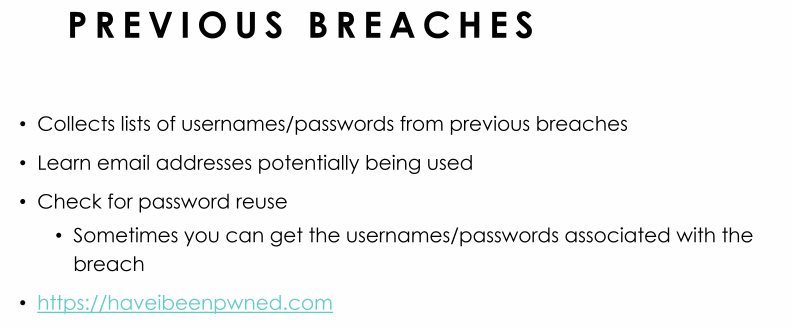


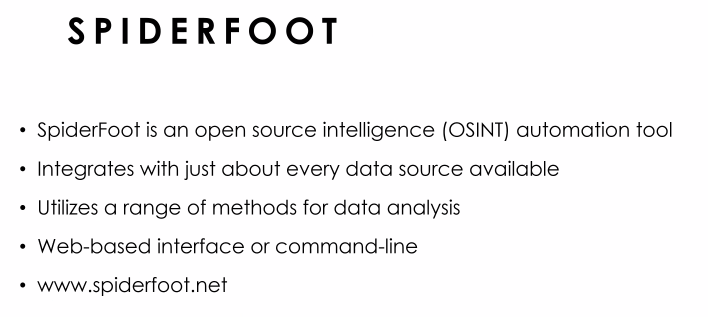
pg. 40

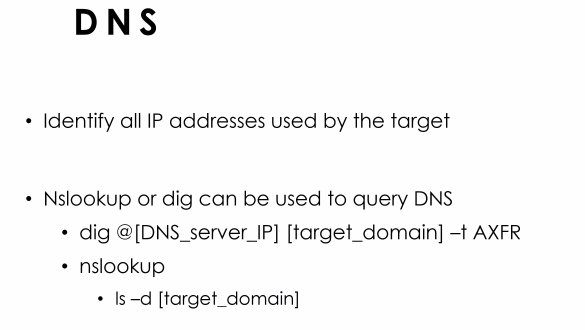


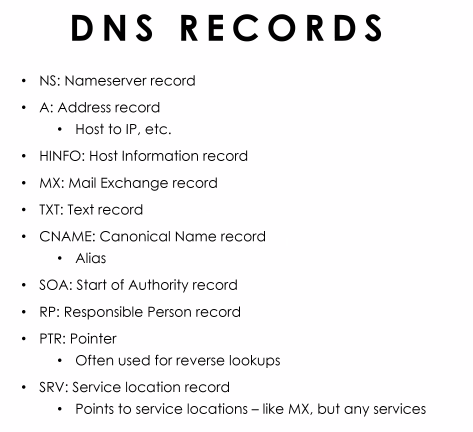


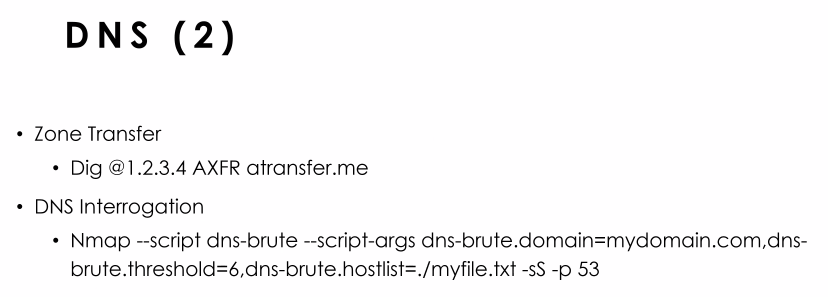






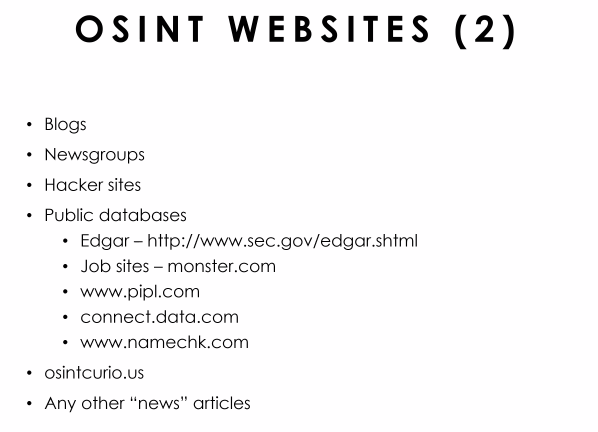




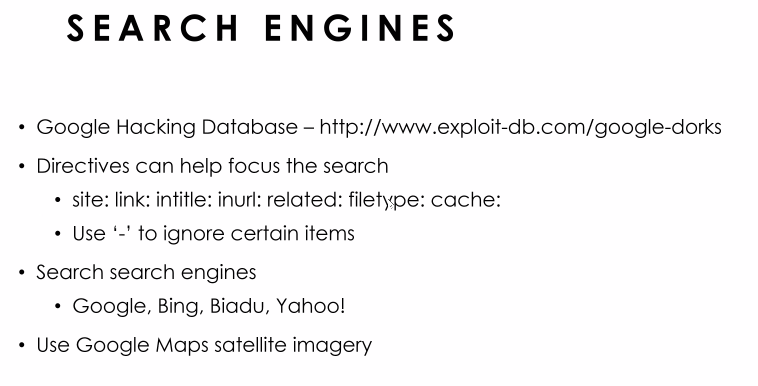


Use script “dns-brute”, port = 53 for brute force on host names

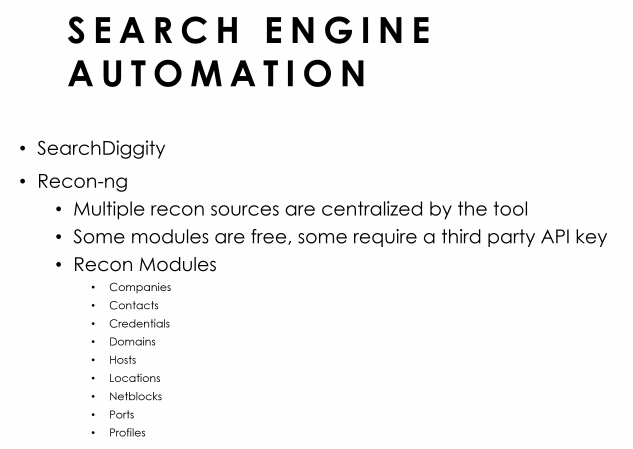




### Search Engines



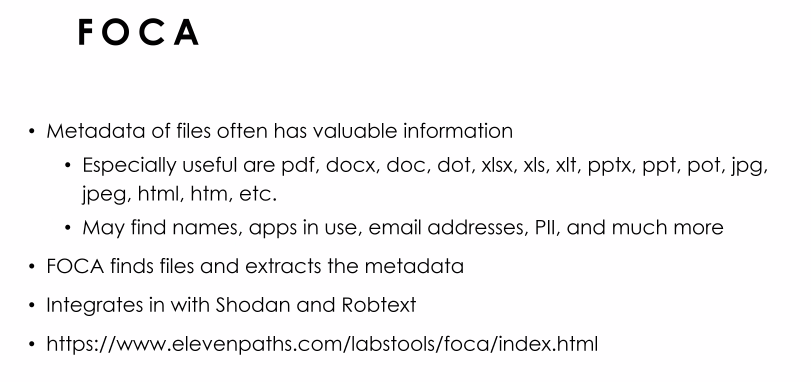
### Search Engine Automation



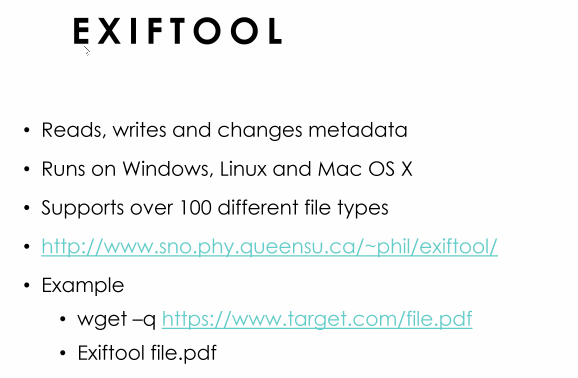
### Wayback Machine



### Foca

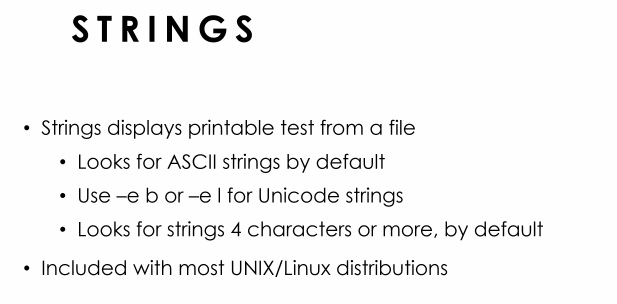


### Exitfool

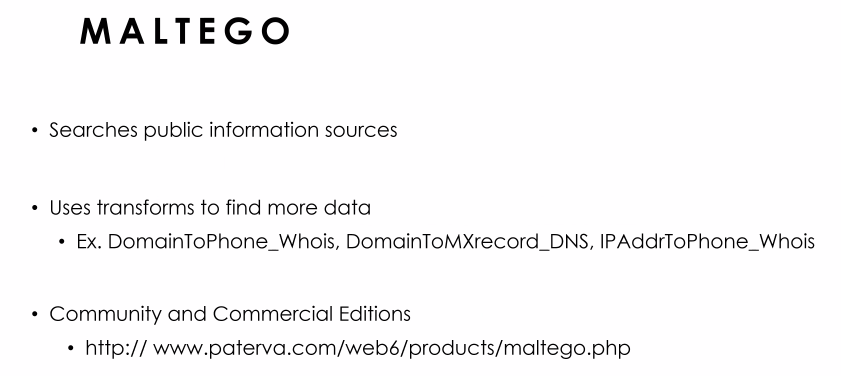


Wget (to download all the files in a site) can look like normal user with auto timing

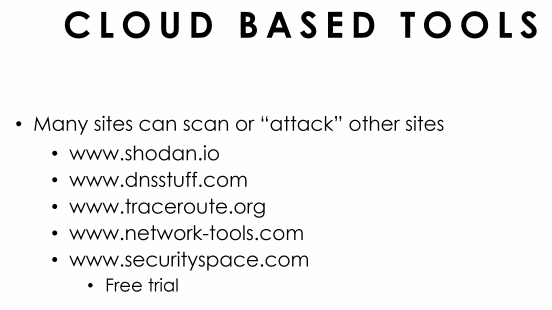
### Strings



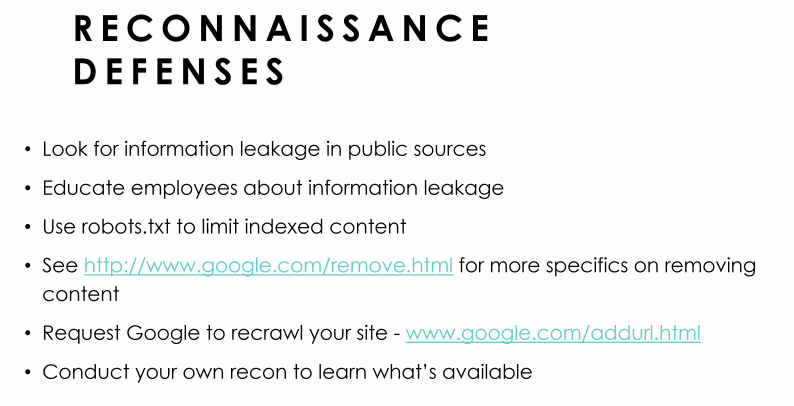
### Maltego

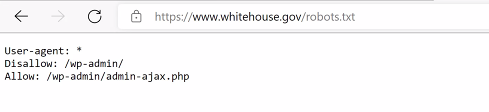


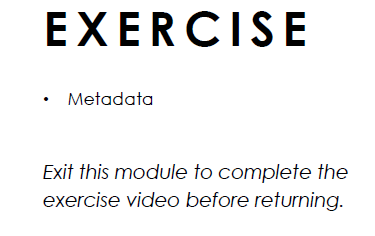
### Cloud Based Tools

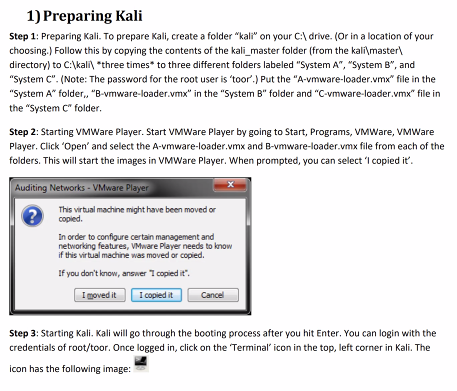


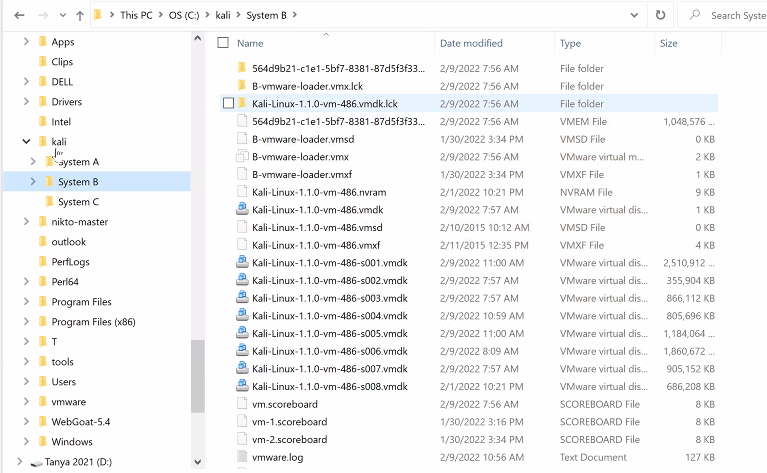
### Reconnaissance Defenses



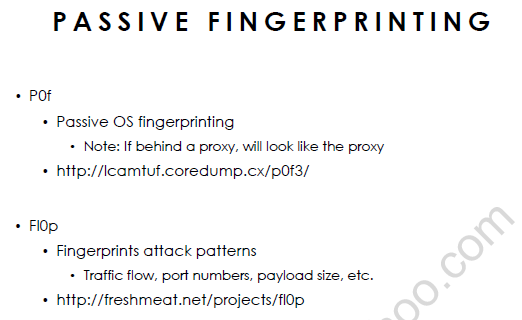




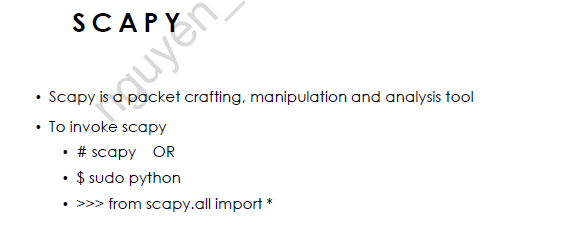




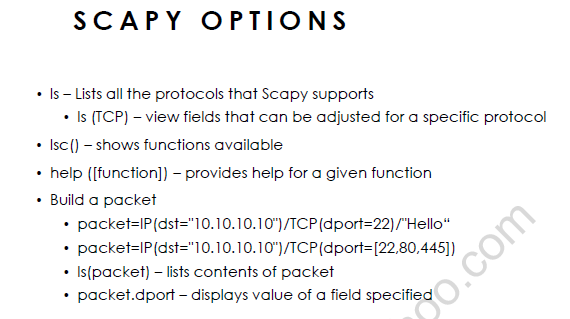
### Passive Fingerprinting

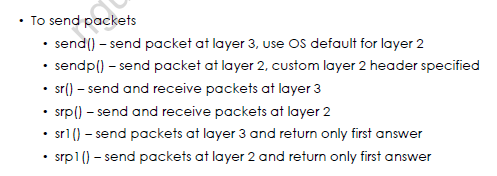


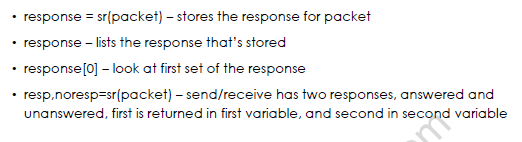
### SCAPY



### SCAPY OPTIONS







### Sniffing Packets with SCAPY

