black box
you are outsider
trying to hack
no info given

white box
given all info

gray box
given partial info

Penetration Testing

PenTesting

→ mimic real-world attacks on system of an organisation to identify network loop holes

Approches → how will you attack

1) Internal vs External

Internal → hack ~~test~~ as if you are an employee or ex-employee
→ you would already know the ins and outs of organisation

External → you are an outsider hacking in the system

2) Assess website and mobile app
→ is it secure
→ authenticity

3) Social Engineering
→ trick someone to give info
→ giving threats → bribing
→ phishing attacks

4) Test wireless network, devices and IOT of the company

PenTest

Planning → Discovery → Attack
↓
report

Phases of PenTests

1) Planning

Set objectives → Establish boundaries → Inform few employees

Set objectives ↓ what are the ~~goals~~ targets

Establish boundaries ↓ legal ramification you will attack real-world data. don't go beyond set boundary.

Inform few employees ↓ someone should know about the attack. ↓ you don't ~~need~~ want to be arrested

2) Discovery

Discovery → vulnerability scan

Discovery → gaining information

vulnerability scan → look for weaknesses

weaknesses ↓ outdated s/w ↓ missing patches

vulnerability scan ⇓

step1) ⇒ identify OS

step2) ⇒ identify major apps on system

step3) ⇒ check with vulnerability database to see common issues with these apps

Methods ~~to~~ get information

1. google dorking → search strings
   ↳ special search operators
   ↳ we can get Admin login pages, Username and passwords, documents, email list, bank account details.

2) <u>Passive methods</u>

- monitor employees
- listen to network traffic

3) <u>Active methods</u>

- network mapping
- port scanning
- password cracking

4) <u>Social Engg</u>

Scanning Tools	Eg
Network Mapper	NMap
Network Analyzer and Profiler	Wireshark
Password cracker	JohnTheRipper
Hacking Tools	Metasploit

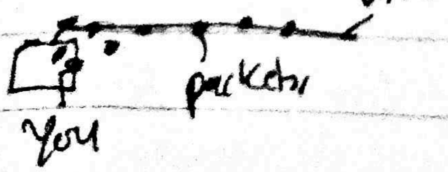
<u>Different types of attacks</u>

1) <u>Passive online attacks</u> — <u>replay attack</u>

a session is fraudulently repeated

<u>wire sniffing</u>
capture packets

<u>man in the middle</u>
hijack session to obtain access



get password file from server and try fo decode it

Hask injection

2) Active online attacks — Phishing

Brute force attack
↓
fuck it. start guesing passwords

trojan/spyware/keylogger

3) Offline attacks — Rainbow
⇓
a table for reversing cryptographic hash func. usually for cracking passwords

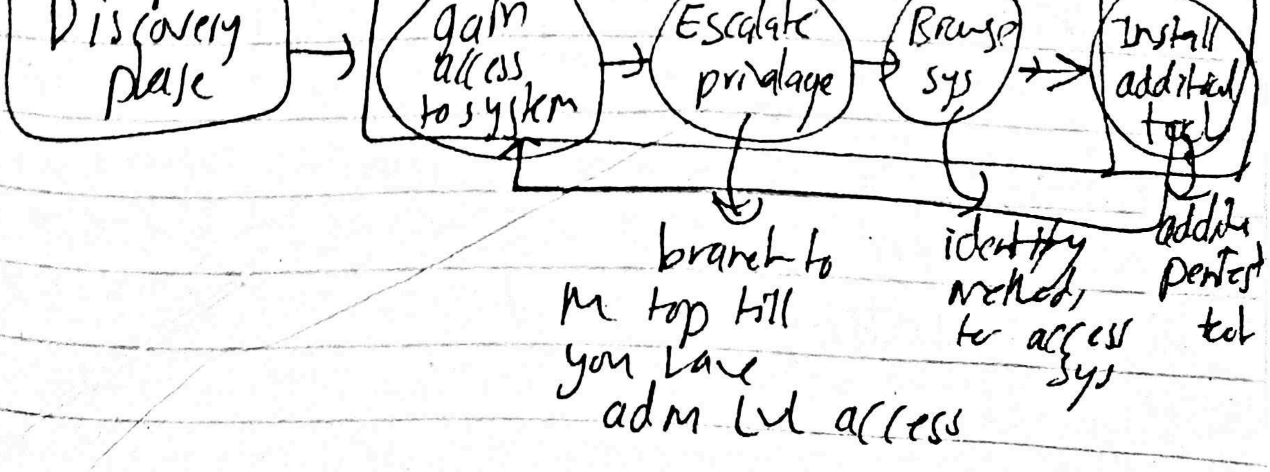
distributed Network attack (DNA)
⇓
brute force cracking

4) Tech-less — dumpster diving
↓
check discarded docx.

social eng

shoulder ~~surf~~ surfing

Phase 3 - Attack



What vulnerabilities to ~~install~~ exploit

- misconfigurations → in security settins
- kernal security flaws
- insufficent input validation.
  ↳ lets say the website takes some user input. Now this input is not entire valid yet accepted so this could be exploited.

- symbolic links
  ↳ os creates files that point to other file.
  ↳ trick then it to giving you the file

→ ~~file descriptor attacks~~

Phase 4 Report

Ex~~e~~ecutive Summary

brief

goals of the pentest and finding

→ recommendations based on finding

who, what, when and where of the testing

Technical Report

in detail

Why and How of the testing

intro → introduce the team
↳ their info
↳ objective of test

~~Background~~ Based on findings, ~~Take the company~~ do risk ranking.

~~[illegible]~~

roadmap → recommendation ~~speaker~~ to the company on a 30 to 90 day plan

higher risk first to be addressed

scope → how you gathered the info

vulnerability assessment → what tools did you use

↳ what did you exploit? and for how long

post exploitation → what did

↳ you find

how you exploited the vulnerability

risk exposure → this was the

↳ risk with these vulnerabilities

value of info at risk.