PHYSICAL PENTESTING

INTRODUCTION

So the reason of this subject come from my type of studying as a sec pentester or a cyber sec student, as we all know company's want to keep their info's and data's safe from falling into the wrong, and of course those data are bits on a disk, and the disk is somwhere on a server, and the server could be anywhere, in a datacentre, home, school....
If you talked with someone about protecting those data most of them will think about it risks, cyber attacks, attaks that can be made from an other device somewhere on the planet, but just a little just a little of them they will take consideration of the physical attack .

INFORMATION GATHERING/OSINT

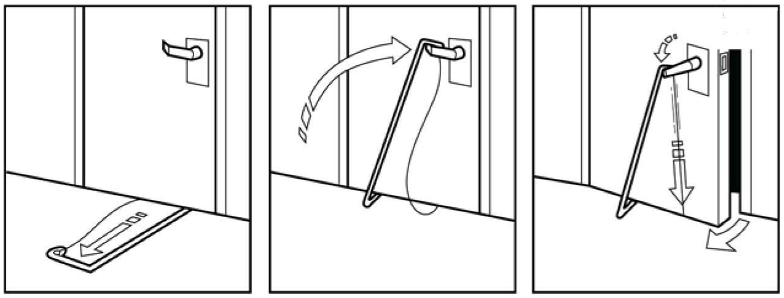
As with other types of penetration testing, the first phase in a physical penetration test is to focus on gathering as much information as possible about the target locations. This Is one of the most critical steps because it helps us to examine the organization by utilizing public tools, such as Google Earth, social media, and job boards. Using this approach, it is usually possible to learn a great deal about the target's surroundings and environment.

GETTING INSIDE

Getting in in facts the most common way is by social engineering wich i've alredy talked about, so today i will not get into it.

- **INSIDE OPENING**

Let's say thet we found a door with no near people of cams but it can only open from the outside just from the inside, in that case we need the under door tool to open it



STEP 1:
Insert tool under the door

STEP 2:
Work tool over the latch

STEP 3:
Pull down on cable to oper
door

- **BAD MISTAKE**

In that case the lock is locking to the outside so with a credit card or by cutting a flat peace of plastic from a bottle we can push the lock with it and the door is fully open

- **LOCK PICKING**

Lock picking is a non-destructive way to bypass a lock without using a key. This can be done

through a variety of different ways lock picking techniques, such as single pin picking and raking; however, each technique has the same goal in mind to mimic the action of the key.
you can pick a lock by a bunch of tools like

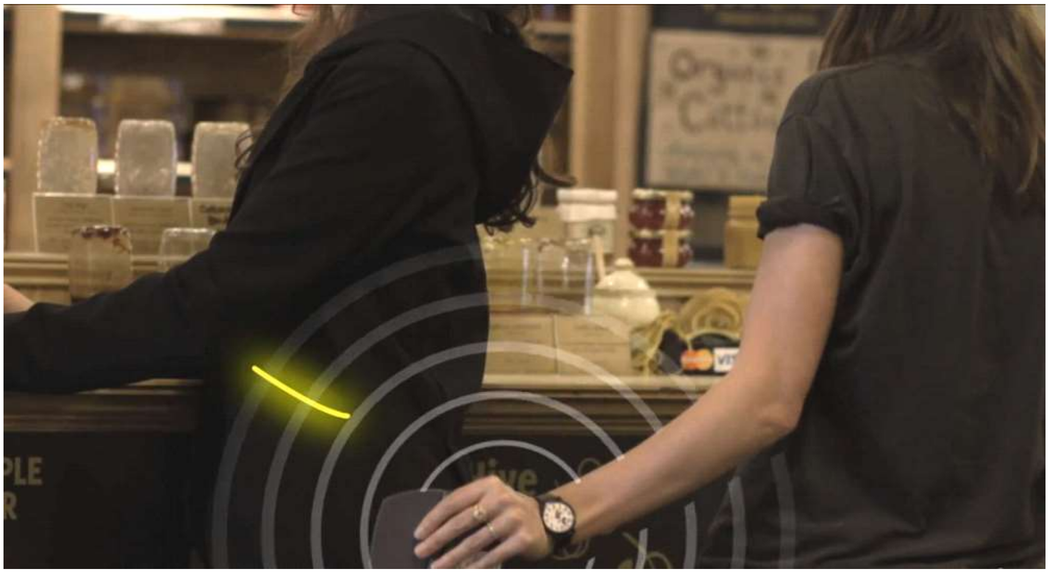
OFC most of the tree techniques and more can be used again and again inside the building

- **RFID LOCK**

It does not require line of sight to work, meaning that the RFID chip and the reader merely need to be within range of each other to communicate

RFID hackers have demonstrated how easy it is to get hold of information within RFID chips

It's not too tricky to build an RFID. It's easy to purchase the parts for the scanner, and once built, someone can scan RFID tags and get information out of them. While your RFID card is safe in your wallet, a hacker scans the card in your pocket without you knowing. The attacker can then steal information without you knowing about it and recode them into an empty rfid card to use it to open the lock as an real employe or owner.



- **TAILGATING**

Tailgating is a technique used to pass through secure entrances where only authorized personnel are allowed to enter. YOU CAN achieve this by following the person that is passing through the entrance and enter without credentials. You can take many forms, such as repair guys, individual pretending to hold heavy boxes. Anything that can make the other feel guilty for not holding the door or not granting access.

- **Shoulder Surfing**

As the name implies, this attack involves simple observation of employee's computer to pick up on their usernames, passwords, intellectual property, sensitive data, and more. To test this attack, you should simply observe if they can pick up on login credentials that employees type .