introduction#

learning network security, i had to write a post related to it

this post aims to learn or clarify host & network security notions/jargon, not covering kinds of threats & attacks

i used simpler words compared to the ones found in my research to make it easier to read for non-native english speakers

i am not an expert by any means, please let me know if i've said something wrong

glossary#

defining mandatory concepts related to the notions covered in the post

malware#

malwares are malicious piece of code or software designed to harm or hijack a device by any means whatsoever (and data ?)

payload#

payload is the part of a malware who responsible for the damages - *data exfiltration, make host unusable, etc.*

can be considered as the "action of the malware"

Malware has two potential actions: replication and attack:

Attack only : trojan horse (or logic bomb if triggered on event)

Replication only … : botched malware

Replication + Attack: virus

Replication +Attack + furtivity = warm

vulnerability#

vulnerabilities refer to hardware, software or procedures weaknesses that could be exploited by a **threat**

threat#

threats are malicious or negative potential events exploiting known or yet unknown vulnerabilities

the word **threat actor** comming from it refers to people behind a malicious incident

risk#

the notion of risk quantifies the probability that a threat exploits a vulnerability causing a significant impact

~~**risks refer to the possible implication of the damage or loss of assets and data**~~

risk = threat ~~+~~ vulnerability * impact*

attack#

an attack is the realization of the exploitation of a vulnerability by a threat

~~**i wanted to put attacks beside threat because attacks are always intentional compared to threats**~~

~~**an attack is always malicious & wants to cause damages whereas threats sometimes don't**~~

classification for those are seperated, e.g: human threat compared to viruses

threat model#

threat modeling is the process of identifying potential **vulnerabilities** or security flaws (software), prioriti~~z~~s~~i~~ng which weaknesses to address or mitig~~i~~ate

creating a threat model can be used for other purposes - *for privacy -* to clarify wants, needs & what to do w/ them

definition perfectible …

endpoint#

endpoints are the far~~th~~rest devices on a network com~~m~~ming from the outside, can be hosts or servers

endpoint protection#

are covered various protections for endpoints/hosts according to many types of threats & attacks

I~~i~~ only wrote about ~~relevent~~relevant & still active protection notions (not hips for example)

hardware side#

fde#

on the hardware side, **full-disk encryption** is a very good practice to preserve security & privacy for portable devices (i.e confidentiality)

having **Luks** for all kinds of needs & **BitLocker** for windows OSs

the better & common way to do fde is using the tpm chip (trusted platform module) to generates the encryption keys & keeping part of it to itself

additionnaly for luks, it uses a master key asked before the boot sequence using a passphrase hash

dlp#

to minimise data loss (i.e. availability), the threat model could implement a **data loss prevention** procedure

a usefull data loss model could be the 3-2-1 backup strategy

- 3 copies of the data - *(or more)*
- 2 backups on different storage media - *this one really help…*
- 1 backup copy offsite - *can be cloud, nas, etc.*

for personnal use, backuping on two different medias (e.g: a nas & a disk or cloud) could be enough, but please do not underestimate the value of backups in production use

once an host has been infected or is showing signs to, doing a quick & tested restoration is very usefull - *test backups before restoration*

software side#

authorisation#

authorisation can be associated to permissions

a good practice is to always let the minimal permissions to the users, only what they are intended to do

that can be a part of the **threat model**: who can access which ressources

in other words, when a~~n~~ user is compromised -> what can he~~it~~ access, what bec~~oa~~me at risk ?

disabling the root account is also a good idea for most hosts, prefering sudoer or proper accorded user permissions

as always, good passwords are always preferated & for the ssh protocol use keys or certificates

authentication#

using a login & a password cannot verify the identity of the person accessing a ressource behind a user

since then, human intervention has guaranteed the identity of the person accessing the resource

back then, simple questions where asked to know if the intended person using the credentials was the one intended - *e.g name of the person's dog, where did he was born, etc.*

this authentication method was highly subjected to doxing - *searching public informations about someone*

nowadays, 2fa is used, living on the intended person's phone or an dedicated hardware device (yubikey)

2fa can take the form of push notifications (malicious ones can be injected), sms verifications (warning sim swapping attack method) or authenticators codes using totp

mfa (multifactor authentication) can also be choose

os/software side#

epp#

endpoint protection platform define the suite of technos used to protect endpoints

ng-av/edr#

av *antivirus*, ngav *next gen antivirus* or edr *endpoint detection & response* are commonly used technos to protect endpoints

sources i found said different things, so i put ng-avs & edrs together, i wonder if their names are not just a marketing thing for the same solutions

"legacy avs" are based in signature recognition to stop known malware

an individual hash could be generated for each file, standard avs compare them to a list of malicious files hash they have to know if a file is one or not

that's only works against file-based attack, new or yet unknown malwares could not be discovered too

variations of a malware (malformed signature trick) can also be done, so its bypass the check since it is not in the signature db