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), prioritiz~~s~~ing 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 farth~~r~~est devices on a network com~~m~~ing 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 beco~~a~~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 prefer~~at~~ed & 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 ngav use behaviour detection on top of the signature recognition, if a software/program/services activity is suspicious -> the file or its activity can be put ~~un~~in quarantine or deleted

some may introduce sandboxing, ai *- i guess for machine learning* although av & ngav are already well ressources hungry

be aware that more than one av could lead to more ressource usage & them trying to cancel each other, since they are accessing same files & seeing each other activity

network solutions#

network solutions are preferable so the threat or the attack is stopped before accessing the endpoints

firewall#

firewalling protects networks from unwanted traffic by a set of pre-programmed rules

it can also provide a network segmentation, sepa~~e~~ration of the lan (local area network) into smaller ones w/ their dedicated rules

not to compare w/ software firewalls who applies rules to an host only

proxy#

proxy servers could be an intermediate to access the internet in a lan

very usefull to reduce a network attack surface since all the traffic is going through

it can monitor traffic or gather metrics

it also provide sort of firewalling since you are restricted by what the proxy permit you to access to

it is also great for privacy since hosts are not directly exposed

many use of proxies can be found doing research

reverse-proxy ?

ids & ips#

intrusion detection systems & *intrusion protection systems* are the “avs of network” - *as i call them*

the ids analyse real-time traffic for signature matching known attacks or suspicious behaviour it can make alerts related to it & according to the threat model: call the ips to stop the traffic related to it or push an alert for the the secops team.

NON: IDS et IPS ont les mêmes proncipes de détection. L'IPS peut EN PLUS intervenir sur le réseau. IDS : passif, IPS : actif. L'IPS est généralement monté en « coupure » sur un réseau afin de pouvoir interrompre le trafic. Un IDS est généralement sur un port miroir et génère des alertes uniquement. A ma connaissance, un IDS n'appelle pas un IPS.

Pour tout ce qui est en dessous, je te préconise de lire par exemple ceci :

https://fr.sentinelone.com/blog/understanding-the-difference-between-edr-siem-soar-and-xdr/?utm_source=google-paid&utm_medium=paid-search&utm_campaign=fr-bau-dsa&utm_term=&campaign_id=20300165755&ad_id=663180394246&gclid=CjwKCAjwjaWoBhAmEiwAXz8DBXAbK_a-w7gIA2phxlqDrCTC-J9A4M_IVI5Z1GzaUIfFO2mSQh9eFRoCOHcQAvD_BwE

Un SOC est une entreprise : une structure, du matériel et une équipe de techniciens spécialisés. Cette entreprise utilise un SIEM (ou éventuellement un SOAR), qui permet de centraliser, normaliser et organiser des logs issus de multiples sources (IDS, IPS, EDR, NDR, XDR, syslog, …). Généralement, le réseau surveillé est celui d'une entreprise cliente, géographiquement distant (même si certaines grosses entreprises peuvent avoir leur SOC en interne … comme Airbus ou la BA118 par exemple !)

Un SOAR est un SIEM qui dispose de fonctionnalités automatiques d'interventions (un SIEM n'est censé que détecter et avertir, l'humain ayant toujours la décision ultime d'intervention).

C'est déjà le cas des IPS, EDR, XDR, qui peuvent agir… mais un SOAR se situe à un niveau hiérarchiquempent plus centralisé

soc#

the *security operations center* - *found it can be called isoc for information…* - is the masterpiece to have, centralising & thinking

socs unif~~i~~y & coordinate alerts issued from security tools (edr, firewall, proxy, etc.) to a main dashboard

extremely useful to correlate informations, generate alerts & choose appropriate actions

it uses all other solutions ressources to monitor, detect & respond to an alert

for some socs, they can: shutdown endpoints or disconnect them, reroute their traffic, run avs scan, etc.

people are present at full-time to maintain the socs since it is a very important protection mesure (cisco, analysts, devops/secdevops persons…)

it is one of the most usefull security solution when it comes to automates, monitoring & responding

ndr/xdr#

network detection & response and *extended detection & response*

ndr monitors network layer 2-7 osi traffic, no agent on the endpoints

xdr tend to gather more informations, by installing agents on endpoints to gather data for example

xdr seems to be more corporate solutions & focus on proper~~ita~~ty

ndr can be implemented solo but xdr may cause friction if it’s not the only protection system deployed

edr ?

siem#

security information & event manager

oftenly used w/ a soc, it is the helper of the security teams

data gathered by the firewalls, network appliances, ids… can be filtered by the siem since all their informations aren’t always relevant

the siem is: collecting, aggregating, identifying, categorising & analysing incidents or events

siem needs continuous learning by the security team or by ai (machine learning) to keep categorising the data well

the data is next sent to the soc next

soar#

security orchestration, automation & response

seems to go a step further than the siem

looks like an inbetween of a soc & a siem but with an advantage to the soc: the automation - *it’s in the name…*

it automates and orchestrates time-consuming manual tasks of the secops, so they can speed up on response time

←software in windows