14/02/2022

Q5) Per prima cosa calcoliamo il *λ = Access Vector x AccessComplexity x Authentication x Exploitability x ReportConfidence*
Per calcolare l' MTAO del di un sottoalbero del grafo bisogna effettuare: Sommatoria ($1/\lambda^k$)
Mentre per il calcolo del Likelihood: *Likelihood = -20* $\log_{10}((MTAO - MTAO_{min}) / MTAO)$

Se invece abbiamo sia network che local vulnerability facciamo prima la *network* e poi la *local* per il PE.

2021-10-08

Q5)

1) *Context Establishment*:
   - EXTERNAL: Consider the directives and standards that the organization must follow
   - INTERNAL: We must describe all the relevant aspects of what the organization does.

   Target of the assessment:
   - Our target is the DMZ composed by two servers linked to a switch with a built-in firewall

   Scope of the assessment:
   - We limit our considerations to the servers within the DMZ.

   Focus of the assessment:
   - Preservation of *integrity* and *availability* on both the DMZ servers

   Assumptions:
   - Bob and Alice own respectively credentials C1 and C2 giving user access on *W_LAN1_0*
   - We consider only internal threat sources because the availability of the *S_DMZ_WWW* can be compromised by an external user (that by definition can reach the DMZ) through the vulnerability *CVE-YYYY-0004*, while for the integrity on the *S_DMZ_SVN* the *CVE-YYYY-0005* can be exploited through the *Network* access vector.
   - We do not consider *not-malicious* threats.

   Determination of the scales:
   - We assign to *Likelihood*: *LOW, MEDIUM, HIGH*
   - We assign to the *Consequences*: *LOW, MEDIUM, HIGH, CRITICAL*

Risk Evaluation Criteria:

- We use the Risk Matrix:

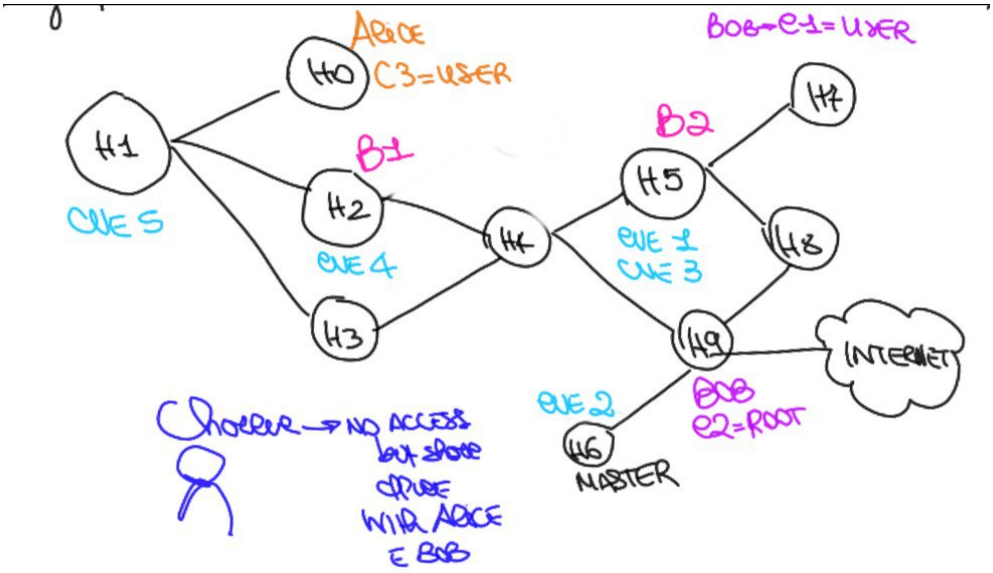
Likelihood	**Impact**				
HIGH	🟨	🟥	🟥		
MEDIUM	🟩	🟨	🟥		
LOW	🟩	🟩	🟨		

2) Risk Identification:

R1) Loss of availability due to *CVE-YYYY-0004* on *S_DMZ_WWW*

02/07/2021 (Sulla fiducia)

Q5)



Context Establishment:

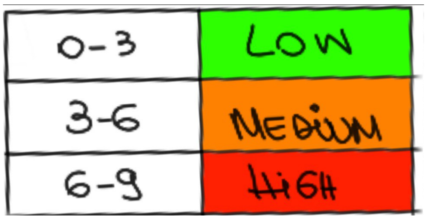
Target: Company’s LAN infrastructure with particular regard to the internal database

Scope: Evaluate the loss of availability of the database due to malwares in the network, and evaluate the loss of confidentiality of the data stored on the database due to the internal attack by Charlie.

Focus: Our focus will be on the properties of availability and confidentiality of the data within the database

Assumptions: We assume that there will not be non-malicious attacks by any member of the company and the channels between users are encrypted.

Scale for the Likelihood:



0-3	LOW
3-6	MEDIUM
6-9	HIGH

Scale for the Consequences:

We consider the scale:
LOW -> One or no database compromised
MEDIUM -> Two database compromised
HIGH -> Every (3) database compromised

Risk Analysis:

1. For the loss of availability the malware needs to compromise both the master server and the backup servers.
   Considering the fact that Bob (H9) is the only one that can access the internet directly and has the habits of playing online games we will assume that he will be the one to infect the system through malware.
   We can calculate the MTAO: H9 -> H6

   λ = AV x AC x AU x Exploitability x Report Confidence = 1 x 0.61 x 0,704 x 1 x 1 = 0,42
   MTAO = 1/λ = 1/0,42 = 2,38

   Likelihood = -20 $\log_{10}$((MTAO - MTAO_{min}) / MTAO) = -20 $\log_{10}$ ((2,38 - 1) / 2,38) = ***4,7*** (MEDIUM)

   Now, estimating the impact on the asset, due to the *CVE-YYYY-0002*, we would consider the impact CRITICAL (*complete* loss of CIA), but due to the fact that the target of our analysis is the whole system and we have two backup copies that will take the place of the compromised database we can consider the consequences LOW.

2. For what concerns the *loss of confidentiality* the attacker just needs to get his hands on one database to completely compromise the *confidentiality* property (every database manages the same data).
   Both Alice and Bob leave the computer logged in so we consider that Charlie can start the attack with every credential (C1,C2,C3).
   So we consider the following paths:

R2 = H0 -> H2 (CVE-5) -> H3 (CVE-4)

$\lambda_{H2} = 0,35 \times 0,56 = 0,196$
$\lambda_{H3} = 0,71 \times 0,704 = 0,5$
$MTAO = 1/\lambda_{H2} + 1/\lambda_{H3} = 5,1 + 2,04 = 7,14$
Likelihood$_{R2}$ *=-20 log*$_{10}$ *(7,14-1) / 7,14 =* ***1,32*** **(LOW)**

R3 = H7 -> H5 (CVE-1) R4 = H7 (CVE-3)

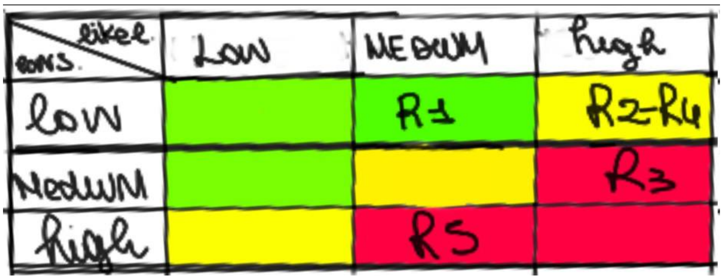
$\lambda_{H5} = 0,71 \times 0,704 = 0,5$
$MTAO = 1/\lambda_{H5} = 2$
Likelihood$_{R3}$ *= -20 log*$_{10}$*(2 - 1) /2 =* ***6*** **(HIGH)**

$\lambda_{H7} = 0,395 \times 0,71 \times 0,704 = 0,197$
$MTAO = 1 / \lambda_{H7} = 5,07$
Likelihood = -20 log$_{10}$ *(5,07 - 1) / 5,07 =* ***1,938*** ***(LOW)***

R5 = H9 -> H6 (CVE-2)

It is the same as the R1, so Likelihood = **4,7** **(MEDIUM)**

Now we can plot every *Risk* on a ***Risk Matrix***:



likel. / cons.	Low	MEDIUM	high
low	🟩	🟩 R1	🟨 R2-R4
Medium	🟩	🟨	🟥 R3
high	🟨	🟥 R5	🟥

Internal and external context
Goal of objective (sarà condurre l analisi del rischio)
Target (la rete dell’azienda)
Scope (Ad esempio l'interfaccia di un pc che è esposta ad internet e quindi a rischi)
Focus
Assumption (e.g non consideriamo le non malicious e canali encrypted per evitare mitm)

Asset (CIA)

Scales (Usiamo le stesse di OWASP per likelihood (0-3, 3-6, 6-9) mentre la consequence usiamo la qualitative scale perchè non è facile quantificare)

Risk evaluation criteria (*Risk matrix*)

Risk Identification:

- Threat source (Malicious o not malicious)
- Vulnerability identification (Si può usare OWASP top 10 etc)
- Incident identification (loss dell asset e risultati sul business)

XXX (Stride per iteration)

#	Element	Interaction	S T R I D E
1	Browser	Output of data for the reservation	X X X
		Output of data from the SQL database	X X X X
2	Voucher Management	Output *display voucher* for the Browser	X X X
3	Data Flow (Send email)	Output of data to *Mail Server*	X X

4	Payment Management	Sends *payment confirmation* to the voucher	X
5	Flight Management & Hotel Reservation	Output of data to the Payment Management	X

1. *Browser*
2. *Voucher Management*: Sends unencrypted data to the browser
3. *Mail Server*: The *send email* flow is not encrypted and crosses trust boundaries so it is vulnerable to Tampering and Information Disclosure
4. *Payment Management*: it is vulnerable to a CVE-XXXX that makes it vulnerable to *Privilege Escalation* through a local process, and thus it can send malicious data to the voucher management that can be eventually spreaded to the mail server
5. *Flight Management & Hotel Reservation*: Linked to a SQL database (through the browser) that stores the user's credentials, vulnerable to SQLi attacks from the Browser.