Università degli Studi di Salerno

Dipartimento di Informatica

Penetration Testing & Ethical Hacking

Vulnerability Mapping
Parte 1

Arcangelo Castiglione
arcastiglione@unisa.it

Outline

- Concetti Preliminari
- Caratterizzazione delle Vulnerabilità
- Tassonomia delle Vulnerabilità
- Analisi Manuale delle Vulnerabilità
- Analisi Automatica delle Vulnerabilità
- Analisi delle Vulnerabilità nelle Applicazioni Web
- Analisi delle Vulnerabilità nei Database

Outline

- **Concetti Preliminari**
- Caratterizzazione delle Vulnerabilità
- Tassonomia delle Vulnerabilità
- Analisi Manuale delle Vulnerabilità
- Analisi Automatica delle Vulnerabilità
- Analisi delle Vulnerabilità nelle Applicazioni Web
- Analisi delle Vulnerabilità nei Database

Concetti Preliminari

- **Vulnerability Mapping:** processo di **identificazione** ed **analisi** dei problemi di **sicurezza** in un determinato **asset**
  - Noto anche come **Vulnerability Assessment**

- Permette di analizzare la sicurezza di un asset rispetto a vulnerabilità note

- **Obiettivi**
  - Rilevare le vulnerabilità presenti in un determinato asset
  - Cercare gli exploit per sfruttare tali vulnerabilità

Concetti Preliminari

- Terminate le fasi di *Information Gathering*, *Target Discovery* ed *Enumerating Target* vengono esaminate le vulnerabilità che potrebbero essere presenti in un determinato asset

- Tali vulnerabilità potrebbero portare alla **compromissione dell'asset**, violando **riservatezza**, **integrità** e **disponibilità** di una (o più) delle sue componenti
  - Host, sistemi, sottosistemi, etc

Concetti Preliminari

- **Triade CIA**: **C**onfidentiality, **I**ntegrity, **A**vailability

- Ciascuna vulnerabilità potrebbe compromettere una (o più) proprietà della triade CIA

Concetti Preliminari

Osservazioni

- Durante un processo di **penetration testing** bisognerebbe dare la **stessa importanza**
  - Sia alle **procedure manuali** per la valutazione della vulnerabilità
  - Che a quelle **automatizzate**

- Affidarsi esclusivamente a procedure automatizzate potrebbe talvolta generare falsi positivi e falsi negativi

- Il livello di preparazione e l'esperienza del pentester possono essere fattori determinanti
  - E dovrebbero essere continuamente tenuti aggiornati

Concetti Preliminari

Osservazioni

- L'analisi delle vulnerabilità non dovrebbe basarsi esclusivamente sull'utilizzo di strumenti automatici

- Gli strumenti automatici potrebbero non riuscire a identificare
  - Errori logici
  - Vulnerabilità di sistema sconosciute
  - Vulnerabilità software non pubblicate

  } ***0-day***

  - Fattori umani che potrebbero influire sulla sicurezza
  - Etc

Concetti Preliminari

Osservazioni

- Andrebbe **sempre** usato un **approccio integrato**
  - Che utilizzi **metodi** di valutazione delle vulnerabilità sia **automatici** che **manuali**

- Ciò aumenterà le probabilità di successo di un processo di penetration testing
  - Oltre a fornire maggiori (e migliori) informazioni per correggere le eventuali vulnerabilità rilevate

Concetti Preliminari

- Dove si trovano le vulnerabilità?
  - Vulnerabilità nei Sistemi Fisici
  - Vulnerabilità nelle Infrastrutture
    - Ad esempio, nei sistemi di rete
  - Vulnerabilità nei Sistemi Operativi
  - Vulnerabilità nei Software Applicativi
  - «Vulnerabilità umane»

Bug nel Software

Outline

- Concetti Preliminari
- **Caratterizzazione delle Vulnerabilità**
- Tassonomia delle Vulnerabilità
- Analisi Manuale delle Vulnerabilità
- Analisi Automatica delle Vulnerabilità
- Analisi delle Vulnerabilità nelle Applicazioni Web
- Analisi delle Vulnerabilità nei Database

Caratterizzazione delle Vulnerabilità
Classi di Vulnerabilità

- Esistono tre principali **classi di vulnerabilità**

  - **Vulnerabilità di Progettazione:** debolezze dovute ad errate specifiche di un sistema

  - **Vulnerabilità di Implementazione:** problemi tecnici di sicurezza che si trovano nel codice di un sistema

  - **Vulnerabilità Operative:** vulnerabilità che possono sorgere a causa della configurazione o del deploy improprio di un sistema in un determinato ambiente operativo

Caratterizzazione delle Vulnerabilità
Classi di Vulnerabilità

- Quale classe di vulnerabilità è la più critica da risolvere?
  - Le **vulnerabilità di progettazione** sono quelle più difficili da risolvere, poiché sono tipicamente causate da errori nelle specifiche dei requisiti di sicurezza
    - Rispetto alle altre classi di vulnerabilità richiedono più tempo e sforzi per essere risolte

Caratterizzazione delle Vulnerabilità
Tipi di Vulnerabilità

- Per ciascuna delle tre classi di vulnerabilità, possono esistere **due generici tipi di vulnerabilità**
  - **Vulnerabilità Locali**
  - **Vulnerabilità Remote**

Caratterizzazione delle Vulnerabilità
Vulnerabilità Locali

- **<u>Vulnerabilità locale:</u>** un utente malintenzionato ha accesso locale ad un sistema ed innesca/sfrutta una determinata vulnerabilità eseguendo un **codice malevolo** (tipicamente un *exploit*) **localmente su tale sistema**

- Sfruttando questo tipo di vulnerabilità, l'utente malintenzionato potrebbe «aumentare» (*Privilege escalation*) i suoi permessi di accesso all'interno del sistema
  - Ad esempio, per ottenere un accesso pienamente privilegiato
    - *Root* o *Amministratore*

Caratterizzazione delle Vulnerabilità
Vulnerabilità Locali – Esempio

- Supponiamo che
  - Un utente abbia accesso ad un sistema basato su *MS Windows Server 2008 (32-bit, x86 platform)*
  - L'accesso dell'utente sia stato limitato dall'Amministratore del sistema, attraverso l'implementazione di opportune politiche di sicurezza
    - Che non consentono all'utente di eseguire determinate applicazioni

Caratterizzazione delle Vulnerabilità
Vulnerabilità Locali – Esempio

- L'utente, utilizzando un codice malevolo (*exploit*), potrebbe ottenere maggiori permessi di accesso al sistema

- Ad esempio, sfruttando una vulnerabilità nota («*CVE-2013-0232, GP Trap Handler nt!KiTrap0D*»), l'utente potrebbe acquisire maggiori privilegi
  - Che gli consentirebbero di svolgere tutti i compiti amministrativi e di ottenere accesso illimitato alle risorse

CVE-2013-0232 MS Windows privilege escalation vulnerability
https://nvd.nist.gov/vuln/detail/CVE-2013-0232

Caratterizzazione delle Vulnerabilità
Vulnerabilità Locali – Esempio

- L'utente, utilizzando un codice malevolo (*exploit*), potrebbe ottenere maggiori permessi di accesso al sistema

- Ad esempio, sfruttando una vulnerabilità nota («*CVE-2013-0232, GP Trap Handler nt!KiTrap0D*»), l'utente potrebbe acquisire maggiori privilegi
  - Che gli consentirebbero di svolgere tutti i compiti amministrativi e di ottenere accesso illimitato alle risorse

Maggiori dettagli verranno mostrati durante le fasi di *Exploitation* e *Post Exploitation (Privilege Escalation)*

Caratterizzazione delle Vulnerabilità
Vulnerabilità Remote

- **<u>Vulnerabilità remota:</u>** un utente malintenzionato non ha accesso locale ad un sistema
  - Ma una determinata vulnerabilità può essere sfruttata utilizzando un **codice malevolo** (*exploit*) **veicolato attraverso la rete**

- Questo tipo di vulnerabilità consente ad un utente malintenzionato, ad esempio, di ottenere l'accesso remoto ad un sistema
  - Senza dover affrontare eventuali barriere fisiche o locali

Caratterizzazione delle Vulnerabilità
Vulnerabilità Remote – Esempio

- Supponiamo che le macchine host di Alice e Bob siano connesse alla rete Internet
  - Ciascuna macchina host possiede il proprio indirizzo IP

- Supponiamo inoltre che la macchina host di Alice
  - Utilizzi Windows XP
  - Memorizzi dati sensibili a cui Bob è interessato

Caratterizzazione delle Vulnerabilità
Vulnerabilità Remote – Esempio

- Supponiamo che Bob
  - Conosca (o sia in grado di ricavare) il Sistema Operativo e l'indirizzo IP della macchina host di Alice (ad esempio, *Windows XP*, `87.19.21.108`)
  - Sia interessato ai dati memorizzati da tale macchina

- Bob
  1. Scopre che la vulnerabilità «**MS08-067 Windows Server»** può essere facilmente sfruttata da remoto su una macchina *Windows XP*
  2. Utilizza l'opportuno exploit verso la macchina di Alice ed ottiene l'accesso ad essa

Microsoft Windows Server - Universal Code Execution (MS08-067)
https://www.exploit-db.com/exploits/6841

Caratterizzazione delle Vulnerabilità
Vulnerabilità Remote – Esempio

- Supponiamo che Bob
  - Conosca (o sia in grado di ricavare) il Sistema Operativo e l'indirizzo IP della macchina host di Alice (ad esempio, *Windows XP*, `87.19.21.108`)
  - Sia interessato ai dati memorizzati da tale macchina

- Bob
  1. Scopre che la vulnerabilità «**MS08-067 Windows Server»** può essere facilmente sfruttata da remoto su una macchina *Windows XP*
  2. Utilizza l'opportuno exploit verso la macchina di Alice ed ottiene l'accesso ad essa

Maggiori dettagli verranno mostrati durante la fase di *Exploitation*

Caratterizzazione delle Vulnerabilità

Vulnerabilità, Minaccia ed Exploit

- Una **vulnerabilità** (o *bug*) è una debolezza che si trova tipicamente in un sistema

- Una **vulnerabilità** potrebbe essere **usata/sfruttata** da un utente malintenzionato per eseguire operazioni non autorizzate sul sistema
  - Diventando una **minaccia** (o **threat**)

- L'**exploit** è un codice che sfrutta una determinata vulnerabilità

Caratterizzazione delle Vulnerabilità

Quanto è grave una vulnerabilità?

- Esistono numerosissime vulnerabilità
  - Molte delle quali possono causare effetti catastrofici
  - Il pericolo causato da una vulnerabilità dipende anche dal contesto e dalla situazione temporale

- Molti fattori possono dipendere dal contesto
  - Tipo di Asset esposto e relativa importanza
  - Vulnerabilità sfruttabile localmente o da remoto
  - Competenze necessarie per sfruttare la vulnerabilità
  - Impatto della vulnerabilità sulla triade CIA
  - Etc

Caratterizzazione delle Vulnerabilità
Common Vulnerability Scoring System (CVSS)

- Open Scoring System proposto da **FIRST** (**F**orum for **I**ncident **R**esponse & **S**ecurity **T**eams)
  - Gruppo di ricercatori e professionisti del settore
  - https://www.first.org/cvss/

- Framework che permette di formalizzare e rendere note le caratteristiche e la gravità delle vulnerabilità
  - Richiesto quando si intende rendere nota una vulnerabilità

- Adottato, tra gli altri, dal **NIST** (The **N**ational **I**nstitute of **S**tandards and **T**echnology) per la definizione del suo **N**ational **V**ulnerability **D**atabase (**NVD**)

Caratterizzazione delle Vulnerabilità
Common Vulnerability Scoring System (CVSS) – Versioni

- Esistono quattro versioni del **C**ommon **V**ulnerability **S**coring **S**ystem (**CVSS**)
  - **CVSS v1**
    - https://www.first.org/cvss/v1/guide
  - **CVSS v2**
    - https://www.first.org/cvss/v2/guide
  - **CVSS v3.0**
    - https://www.first.org/cvss/v3.0/user-guide
  - **CVSS v3.1**
    - https://www.first.org/cvss/v3.1/user-guide
  - **CVSS v4.0**
    - https://www.first.org/cvss/v4.0/user-guide

Caratterizzazione delle Vulnerabilità
Common Vulnerability Scoring System (CVSS) – Versioni

- Esistono quattro versioni del **C**ommon **V**ulnerability **S**coring **S**ystem (**CVSS**)
  - **CVSS v1**
    - https://www.first.org/cvss/v1/guide
  - **CVSS v2**
    - https://www.first.org/cvss/v2/guide
  - **CVSS v3.0**
    - https://www.first.org/cvss/v3.0/user-guide
  - **CVSS v3.1**
    - https://www.first.org/cvss/v3.1/user-guide
  - **CVSS v4.0**
    - https://www.first.org/cvss/v4.0/user-guide

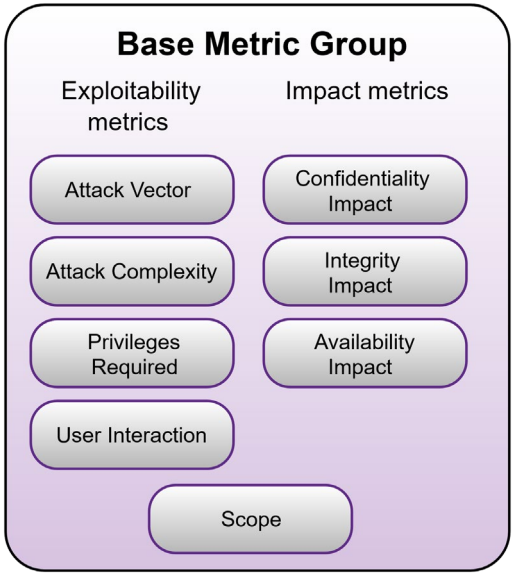
Caratterizzazione delle Vulnerabilità
Common Vulnerability Scoring System (CVSS) 3.1

- Il **CVSS** è costituito da **tre gruppi di metriche**
  - **Base Metric:** valutano la gravità di una vulnerabilità in base a sue caratteristiche intrinseche che sono costanti nel tempo ed ipotizzano l'impatto del caso peggiore di tale vulnerabilità in diversi ambienti operativi
  - **Temporal Metric:** regolano le «**Base Metric**» di una vulnerabilità in funzione di fattori che possono cambiare nel tempo ma non tra gli ambienti operativi, come ad esempio la disponibilità di *exploit*
  - **Environmental Metric:** regolano le «**Base Metric**» e le «**Temporal Metric**» in funzione di uno specifico ambiente operativo, considerando fattori come la presenza di mitigazioni per quel determinato ambiente

https://www.first.org/cvss/specification-document

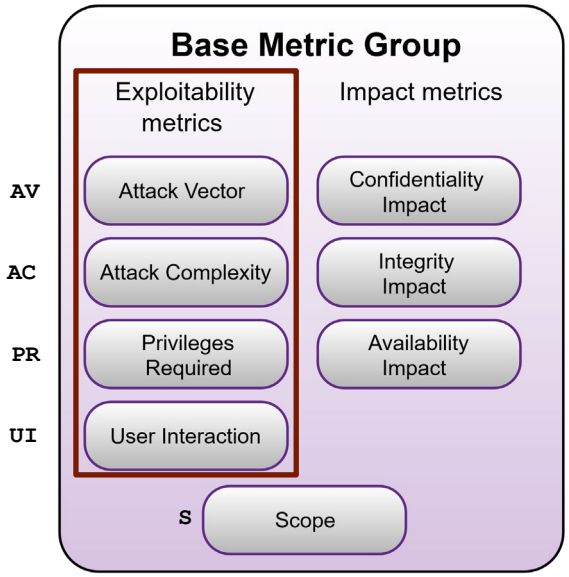
Caratterizzazione delle Vulnerabilità
Common Vulnerability Scoring System (CVSS) 3.1

- **`Base Metric Group`**
  - Rappresenta caratteristiche intrinseche di una vulnerabilità che sono costanti nel tempo e tra gli ambienti operativi
  - È composto da due insiemi di metriche: «**`Exploitability metrics`**» ed «**`Impact metrics`**»



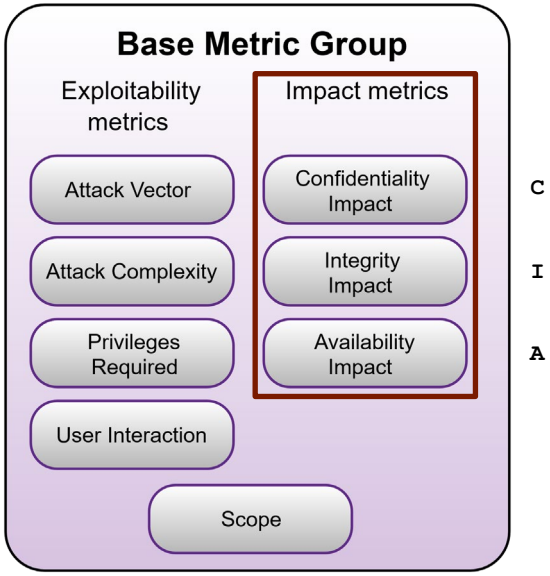
Caratterizzazione delle Vulnerabilità
Common Vulnerability Scoring System (CVSS) 3.1

- Le «**`Exploitability metrics`**» caratterizzano la facilità ed il modo in cui una vulnerabilità può essere sfruttata
- Tali metriche rappresentano le caratteristiche intrinseche di «ciò che è vulnerabile»
  - **Componente vulnerabile**



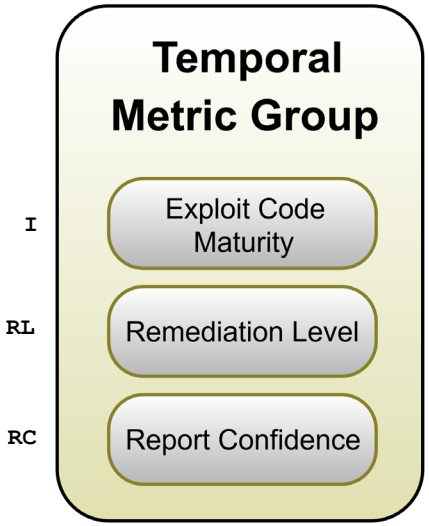
Caratterizzazione delle Vulnerabilità
Common Vulnerability Scoring System (CVSS) 3.1

- Le «**`Impact metrics`**» caratterizzano l'impatto (in termini di *triade CIA*) che una *exploitation* riuscita genera su una determinata componente
  - **Componente impattata**



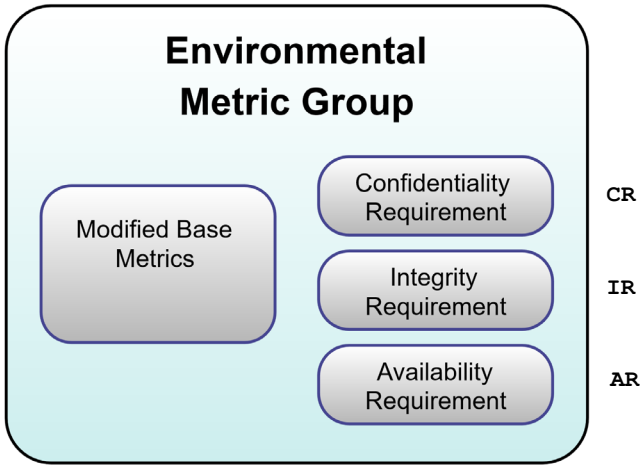
Caratterizzazione delle Vulnerabilità
Common Vulnerability Scoring System (CVSS) 3.1

- **Temporal Metric Group**
  - Caratterizza aspetti di una vulnerabilità che possono cambiare nel tempo ma non tra gli ambienti operativi
  - Ad esempio, la disponibilità di un exploit semplice da usare aumenterebbe il punteggio CVSS, mentre la creazione di una patch ufficiale lo diminuirebbe



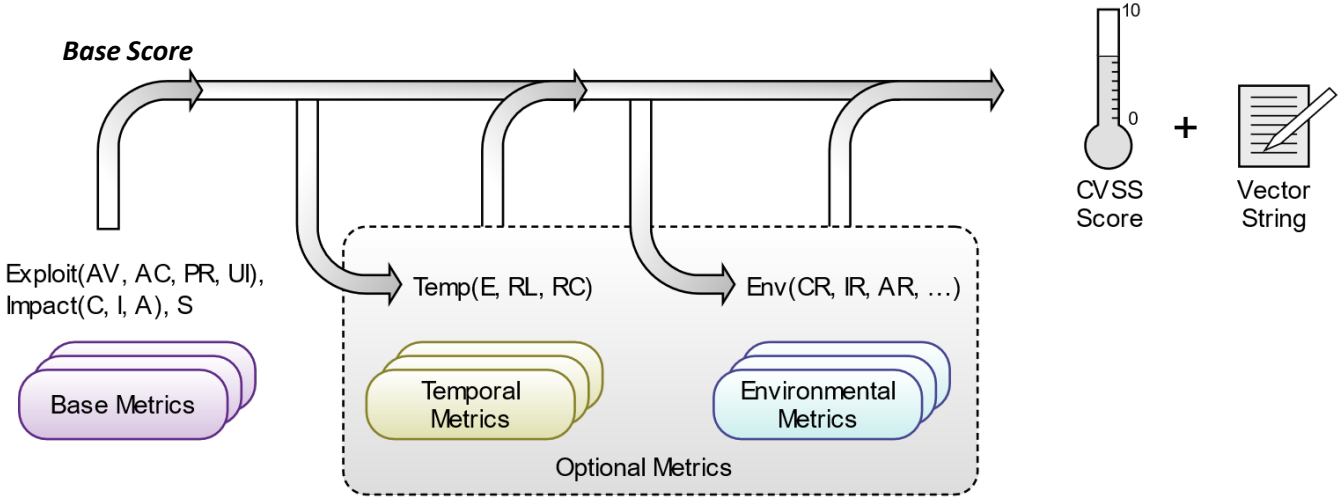
Caratterizzazione delle Vulnerabilità
Common Vulnerability Scoring System (CVSS) 3.1

- **Environmental Metric Group**
  - Rappresenta caratteristiche di una vulnerabilità che sono rilevanti ed uniche per un determinato ambiente operativo
  - Considera fattori come la presenza di controlli di sicurezza che possono mitigare le conseguenze di un eventuale attacco per un determinato ambiente e l'importanza relativa di una componente vulnerabile all'interno di un asset



Caratterizzazione delle Vulnerabilità
Common Vulnerability Scoring System (CVSS) 3.1

- **Scoring System**
  - Il ***Base Score*** prodotto dalle «**`Base Metrics`**» può essere eventualmente «perfezionato», assegnando un punteggio alle «**`Temporal Metrics`**» ed alle «**`Environmental Metrics`**», così da riflettere più accuratamente la gravità di una vulnerabilità per un determinato ambiente operativo in uno specifico momento

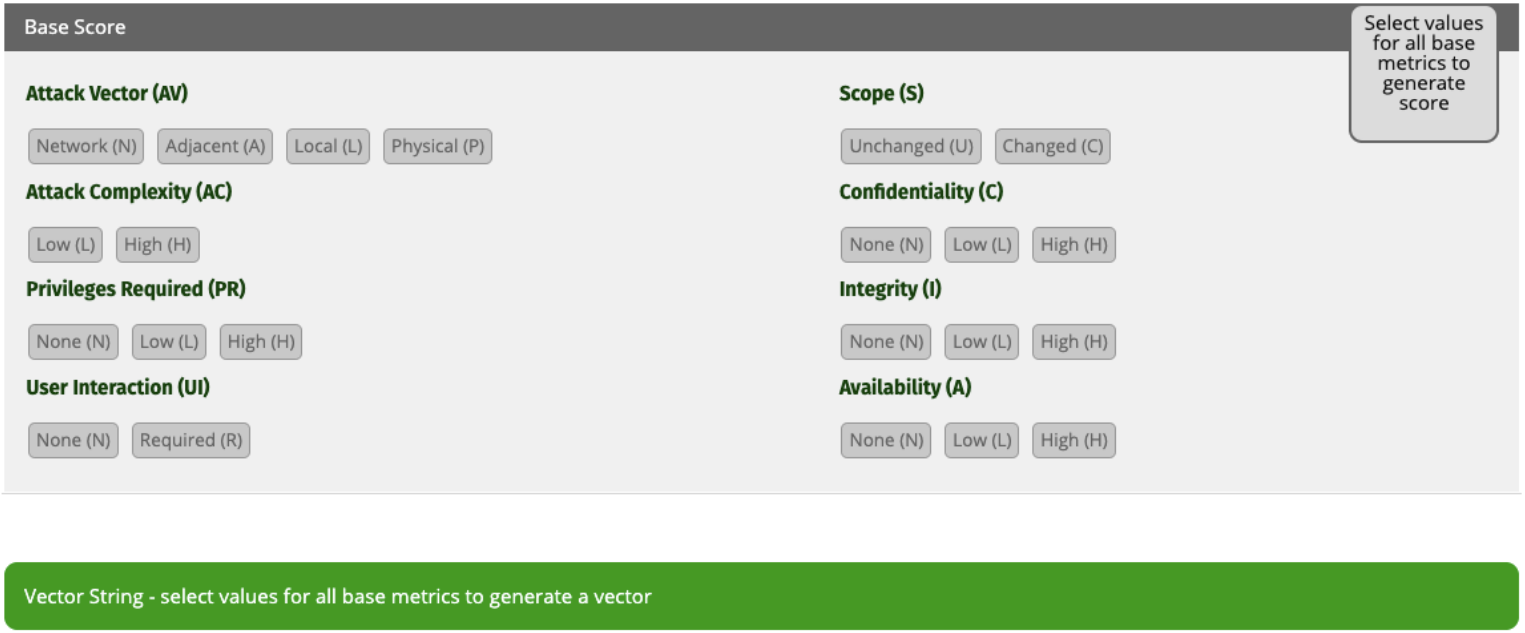


Caratterizzazione delle Vulnerabilità
Common Vulnerability Scoring System (CVSS) 3.1

- **Scoring System**
  - Il CVSS produce anche un **vettore**, che fornisce una rappresentazione testuale dei valori delle metriche utilizzate per caratterizzare la vulnerabilità
  - Tale vettore
    - Deve contenere le stringhe che rappresentano i valori assegnati a ciascuna metrica
      - Tutte le stringhe che rappresentano le «**`Base Metrics`**» devono essere incluse nel vettore, le altre («**`Temporal Metrics`**» ed «**`Environmental Metrics`**») possono essere omesse
    - Dovrebbe sempre essere visualizzato insieme allo score assegnato a ciascuna vulnerabilità
  - **Esempio:**
    `CVSS:3.1/S:U/AV:N/AC:L/PR:H/UI:N/C:L/I:L/A:N/E:F/RL:X`

Caratterizzazione delle Vulnerabilità
CVSS 3.1 Calculator – Base Score

- **https://www.first.org/cvss/calculator/3.1**



Nessuna metrica selezionata

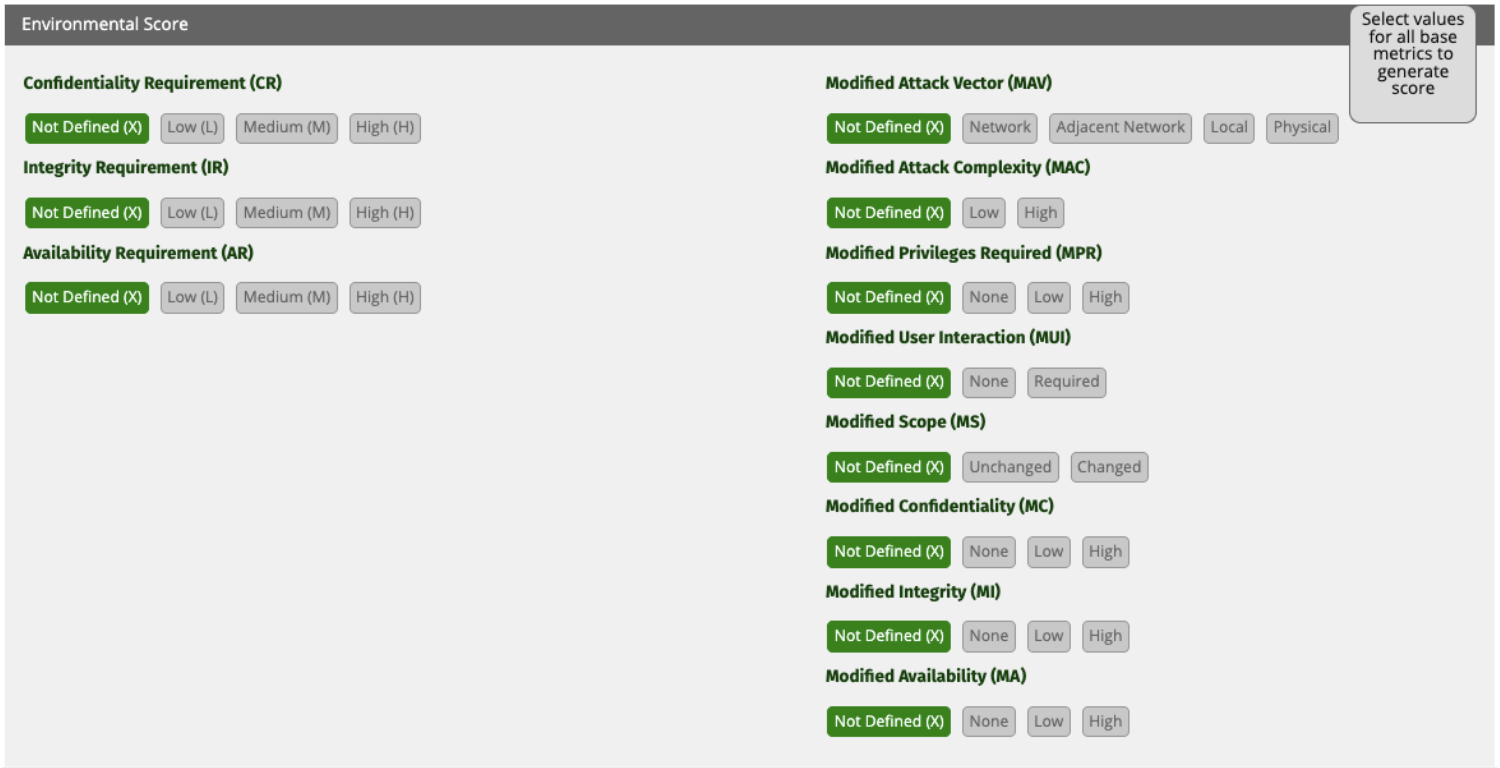
Caratterizzazione delle Vulnerabilità
CVSS 3.1 Calculator – Temporal Score

- **https://www.first.org/cvss/calculator/3.1**

Nessuna metrica selezionata

Caratterizzazione delle Vulnerabilità
CVSS 3.1 Calculator– Environmental Score

- **https://www.first.org/cvss/calculator/3.1**



Nessuna metrica selezionata

Caratterizzazione delle Vulnerabilità
CVSS 3.1 Calculator – Esempio 1

- **Base Score**

Attack Vector (AV): Network (N)
Attack Complexity (AC): Low (L)
Privileges Required (PR): None (N)
User Interaction (UI): None (N)

Scope (S): Changed (C)
Confidentiality (C): High (H)
Integrity (I): High (H)
Availability (A): High (H)

Caratterizzazione delle Vulnerabilità
CVSS 3.1 Calculator – Esempio 1

- **Temporal Score**

Non viene definita alcuna metrica relativa al Temporal Score

Caratterizzazione delle Vulnerabilità
CVSS 3.1 Calculator – Esempio 1

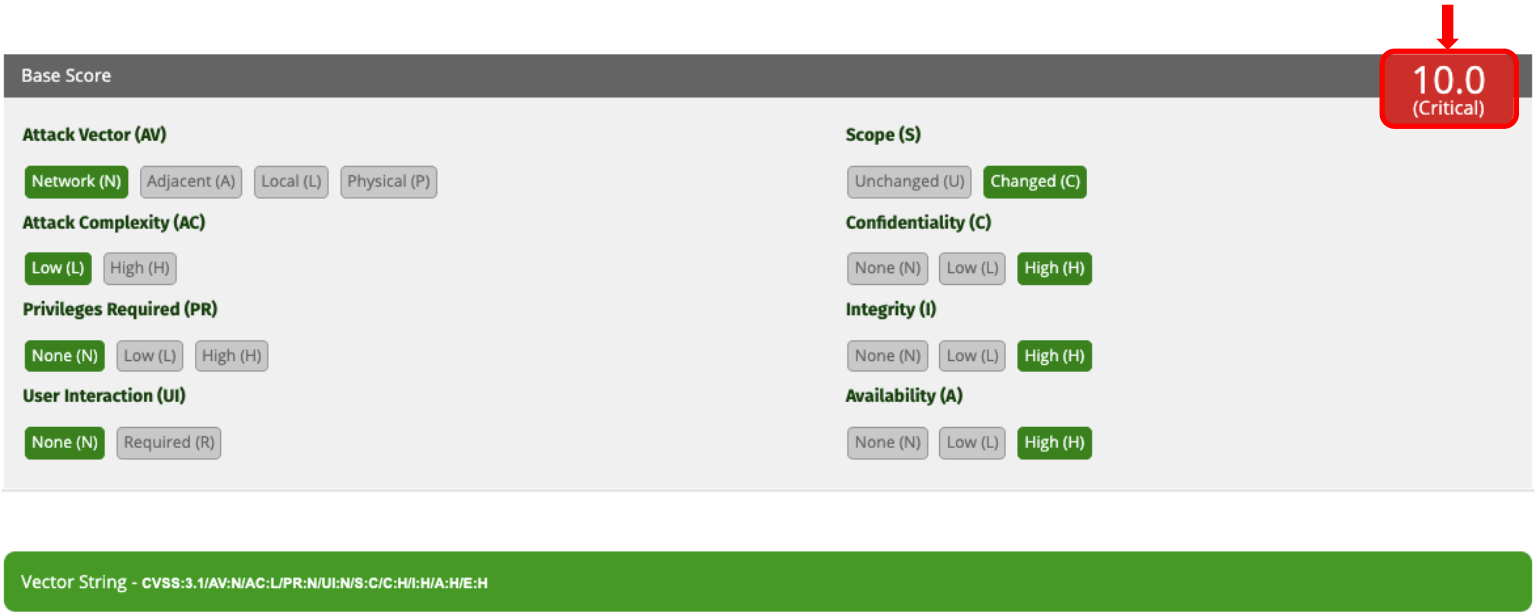
- **Environmental Score**

IL CVSS Score assume in questo caso il valore di massima gravità `10.0` (*Critical*)

Non viene definita alcuna metrica relativa all'Environmental Score

Caratterizzazione delle Vulnerabilità
CVSS 3.1 Calculator – Esempio 2

- **`Base Score`**

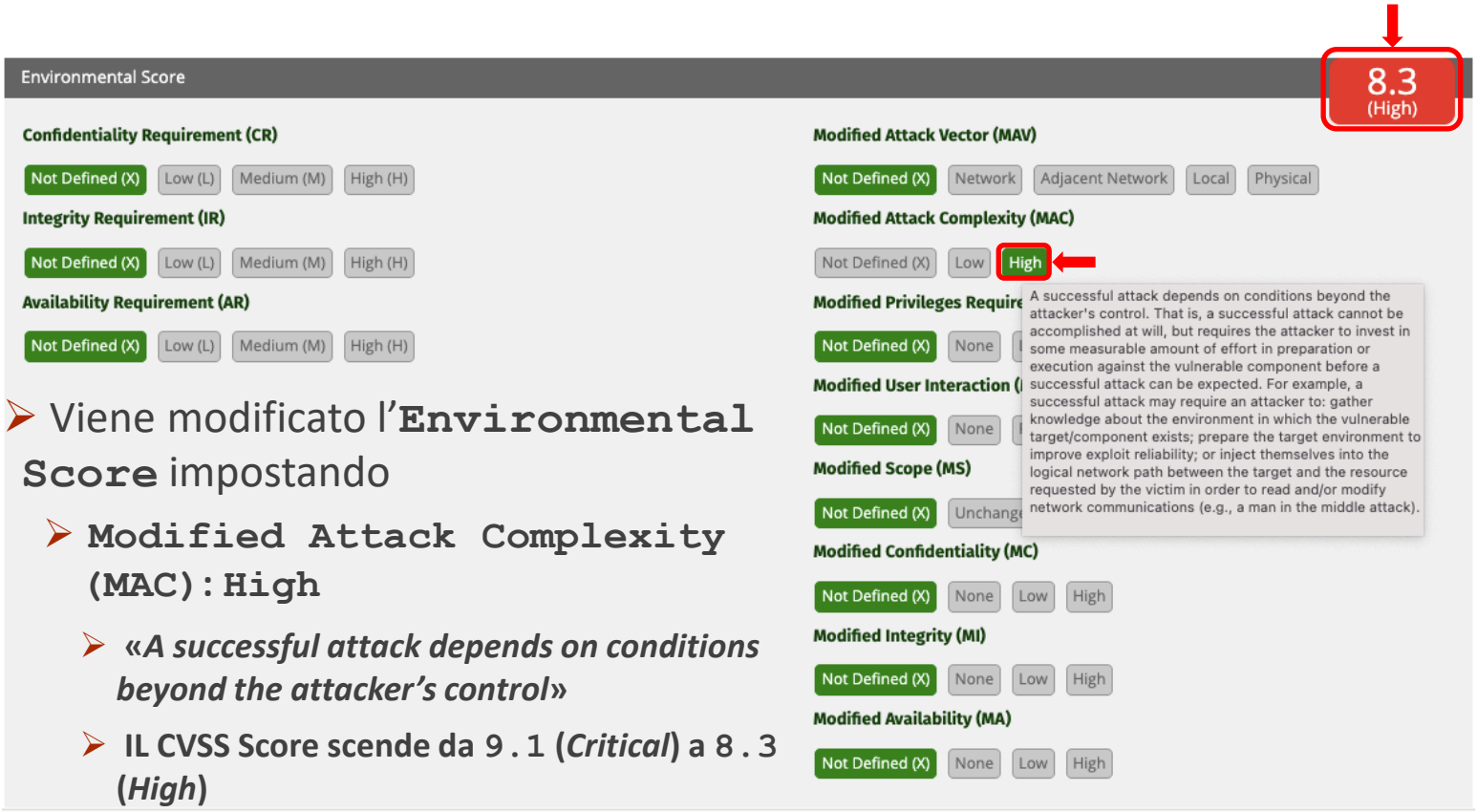


Rispetto all'Esempio 1 non vengono effettuate modifiche alle metriche incluse nel `Base Score`

Caratterizzazione delle Vulnerabilità
CVSS 3.1 Calculator – Esempio 2

- Viene modificato il **`Temporal Score`** impostando
  - **`Exploit Code Maturity (E):Unproven (U)`**
    - «***No exploit code is available, or an exploit is theoretical***»
    - **IL CVSS Score scende da `10.0` (*Critical*) a `9.1` (*Critical*)**

Caratterizzazione delle Vulnerabilità
CVSS 3.1 Calculator – Esempio 2



- Viene modificato l'**`Environmental Score`** impostando
  - **`Modified Attack Complexity (MAC): High`**
    - «*A successful attack depends on conditions beyond the attacker's control*»
    - **IL CVSS Score scende da `9.1` (*Critical*) a `8.3` (*High*)**

Caratterizzazione delle Vulnerabilità
CVSS v2.0 vs. CVSS v3.0

CVSS v2.0 Ratings

Severity	Base Score Range
Low	0.0-3.9
Medium	4.0-6.9
High	7.0-10.0

CVSS v3.0 Ratings

Severity	Base Score Range
None	0.0
Low	0.1-3.9
Medium	4.0-6.9
High	7.0-8.9
Critical	9.0-10.0

3 livelli di «criticità»

Caratterizzazione delle Vulnerabilità
CVSS v2.0 vs. CVSS v3.0

CVSS v2.0 Ratings

Severity	Base Score Range
Low	0.0-3.9
Medium	4.0-6.9
High	7.0-10.0

CVSS v3.0 Ratings

Severity	Base Score Range
None	0.0
Low	0.1-3.9
Medium	4.0-6.9
High	7.0-8.9
Critical	9.0-10.0

Ciascuno corrispondente ad un determinato intervallo numerico

Caratterizzazione delle Vulnerabilità
CVSS v2.0 vs. CVSS v3.0

CVSS v2.0 Ratings		CVSS v3.0 Ratings	
Severity	**Base Score Range**	**Severity**	**Base Score Range**
		None	0.0
Low	0.0-3.9	Low	0.1-3.9
Medium	4.0-6.9	Medium	4.0-6.9
High	7.0-10.0	High	7.0-8.9
		Critical	9.0-10.0

5 livelli di «criticità»

Caratterizzazione delle Vulnerabilità
CVSS v2.0 vs. CVSS v3.0

CVSS v2.0 Ratings		CVSS v3.0 Ratings	
Severity	**Base Score Range**	**Severity**	**Base Score Range**
		None	0.0
Low	0.0-3.9	Low	0.1-3.9
Medium	4.0-6.9	Medium	4.0-6.9
High	7.0-10.0	High	7.0-8.9
		Critical	9.0-10.0

Ciascuno corrispondente ad un determinato intervallo numerico