Università degli Studi di Salerno

Corso di Laurea Magistrale in Informatica

Appunti del corso

Programmazione Sicura

Tenuto da

Barbara Masucci

A cura di

Luigi Miranda

Anno Accademico 2023/2024

Indice

1 Terminologia **2**

1.1 Asset 2

1.2 Minaccia 2

1.3 Attacante 3

2 Nebula **4**

2.1 Level00 5

Capitolo 1

Terminologia

1.1 Asset

Un asset è un'entità generica che interagisce con il mondo circostante. Può essere un edificio, un computer, un algoritmo, una persona. Nell'ambito di questo corso l'asset è un Software. Una persona può interagire con un asset in tre modi:

- correttamente
- non correttamente, in modo involontario
- non correttamente, in modo volontario/malizioso

Un uso non corretto di un asset può portare a gravi danni come il furto, la modifica o distruzione di dati sensibili, la compromissione di servizi.

1.2 Minaccia

Una minaccia è una potenziale causa di incidente, che comporta un danno all'asset. Le minacce possono essere:

- accidentali
- dolose

Microsoft classica le minacce con l'acronimo STRIDE:

- Spoofing

- Tampering
- Repudiation
- Information Disclosure
- Denial of Service
- Elevation of Privilege

1.3 Attacante

Un attacante tenta di interagire in modo malizioso con un asset con lo scopo di tramutare una minaccia in realtà. Talvolta un attaccante interagisce in modo non malizioso per stimare i livelli di sicurezza. Distinguiamo tre tipi di attacanti:

- White Hat, fini non maliziosi
- Black Hat, fini maliziosi o tornaconto personale
- Gray Hat, viola asset e chiede denaro per sistemare la situazione

Capitolo 2

Nebula

Nebula è la prima macchina virtuale che studieremo in questo corso. Ci sono diversi livelli, noi affronteremo le sfide:

- Nebula 00
- Nebula 01
- Nebula 02
- Nebula 04
- Nebula 07
- Nebula 10
- Nebula 13

La macchina virtuale è scaricabile dal sito Exploit Education. Le sfide di nebula trattano l'iniezione locale e remota di codice.

Ogni macchina ha tre account:

- Giocatore, un utente con il ruolo di attaccante che può accedere con la coppia di credenziali:
  - username: levelN(N=00,01,02,ecc.)
  - password: levelN
- vittima, chiamati flagN(N=00,01,ecc.) rappresentano la vittima e presentano diversi tipi di vulnerabilità

- Admin, amministratore del sistema con credenziali:
- – username: nebula
  – password: nebula

Noi accederemo sempre come utente levelN, con l'obiettivo di:

- Elevare i privilegi
- Ottenere informazioni sensibili

Raggiunto l'obiettivo, si cattura la bandierina, per questo motivo le sfide prendono il nome di CTF.

2.1 Level00

Dalla pagina ufficiale si legge: This level requires you to find a Set User ID program that will run as the "flag00" account.

Quindi dobbiamo trovare un programma con il SETUID acceso per poter essere eseguito come se fossimo flag00.