Autori: Marian Gușatu, Ruxandra F. Olimid
Departamentul de Informatică, Universitatea din București

- Laboratorul 1 -

Introducere în securitatea sistemelor informatice

Disclaimer: Pe parcursul acestui curs/laborator vi se vor prezenta diverse noțiuni de securitate informatică, cu scopul de a învăța cum să securizați sistemele. Toate noțiunile și exercițiile sunt prezentate în scop didactic, chiar dacă uneori se presupune să gândiți ca un adversar. Nu folosiți aceste tehnici în scopuri malițioase! Acestea pot avea consecințe legale în cazul comiterii unor infracțiuni, pentru care **deveniți pe deplin răspunzători**!

1. *Noțiuni generale*

Atribuiți fiecărui termen definiția corespunzătoare. Definițiile au fost preluate din glosarul de termeni *NIST – Computer Security Resource Center* [1].

(A) Adversar	(1) O condiție care rezultă din stabilirea și menținerea măsurilor de protecție care permit unei organizații/sistem să își îndeplinească misiunea sau funcțiile critice, în ciuda riscurilor reprezentate de amenințări.
(B) Securitate	(2) Slăbiciune într-un sistem informațional, proceduri de securitate ale sistemului, controale interne sau implementare care ar fi putea fi exploatate sau declanșate de o sursă de amenințare.
(C) Risc	(3) O entitate (inclusiv un *insider*) care acționează rău intenționat pentru a compromite un sistem.
(D) Vulnerabilitate	(4) Capacitatea de a proteja / apăra spațiul cibernetic de atacuri cibernetice.
(E) Securitatea cibernetică	(5) O măsură a gradului în care o entitate este amenințată de o eventuală circumstanță sau eveniment.

2. *„The Security Mindset”*

Vizualizați interviul [2].


Aveți în vedere:

- Modul de gândire al unui adversar
- Aspecte de etică și aspecte legale! (ex. gândim ca un atacator ca să putem securiza sistemele informatice)

3. Sisteme de numerație


Reamintiți-vă:

- *Sistemele de numerație hexazecimal și binar*
- *Conversia din decimal (baza 10) în binar (baza 2) și invers*
- *Conversia din hexazecimal (baza 16) în binar (baza 2) și invers*


Răspundeți la următoarele cerințe:

- Considerați ziua în care v-ați născut la care adăugați valoarea 10. Transformați în binar această valoare. Faceți transformarea inversă.
- Considerați un număr hexazecimal oarecare de 4 cifre. Transformați în binar această valoare. Faceți transformarea inversă.


Căutați resurse online care vă permit conversia între diferite baze de numerație. Vă vor fi de folos pentru următoarele laboratoare.

4. Codul ASCII


Reamintiți-vă:

- *Codul American Standard Code for Information Interchange (ASCII)*


Răspundeți la următoarele cerințe:

- Considerați prenumele dumneavoastră, scris cu majuscule. Ce îi corespunde conform codificării ASCII?
- Se consideră codificarea ASCII *66 82 65 86 79*. Ce cuvânt îi corespunde?


Căutați resurse online care vă permit conversia caracterelor în ASCII și invers. Vă vor fi de folos pentru următoarele laboratoare.

5. *Base64*

 Reamintiți-vă:

- *Codarea și decodarea Base64*

 Răspundeți la următoarele cerințe:

- Considerați numele dumneavoastră, scris cu majuscule. Ce îi corespunde conform codificării Base64?
- Se consideră codificarea Base64 dată de string-ul următor: *U3VudCBzdHVkZW50IGxhIEZNSS4=*. Ce îi corespunde?

 Căutați resurse online care vă permit conversia în/din Base64. Vă vor fi de folos pentru următoarele laboratoare.

6. *Introducere în malware*

 Explicați pe scurt fiecare din termenii: *malware, virus, dropper, downloader, trojan, spyware, riskware, ransomware, adware, worm, obfuscare*.

 Pentru explicarea termenilor, vă puteți folosi de resurse online precum [1], [3].

7. *Mașini virtuale*

 Parcurgeți următorii pași:

1. Descărcați și instalați un hipervizor (ex.: VirtualBox/VMWare).
2. Descărcați un fișier *.iso* aferent tipului de sistem de operare.
3. Creați o mașină virtuală și instalați sistemul de operare.
4. Instalați tool-urile pe care le considerați utile (ex.: *Procmon, Process Explorer*).
5. Setați rețeaua mașinii virtuale în modul **Host-Only.**
6. Faceți un **snapshot** la care veți putea reveni oricând.

Configurați-vă o mașină virtuală cu Windows (orice începând cu Windows 7 este acceptat).

Alternativă: Folosiți o mașină virtuală creată de Microsoft cu scopul testării IE și MSEdge [4].

Referințe bibliografice

1. National Institute of Standards and Technolohy (NIST) – Computer Security Resource Center (CSRC), *Glossary*. Accesibil la: https://csrc.nist.gov/glossary/ Ultima accesare: septembrie 2021.
2. Schneier, B. *The Security Mindset*. Accesibil la: https://youtu.be/eZNzMKS7zjo Ultima accesare: septembrie 2021.
3. Kryszczuk, K., & Richiardi, J. (2014). *Springer Encyclopedia of Cryptography and Security*. Accesibil la: https://www.researchgate.net/publication/230674947_Springer_Encyclopedia_of_Cryptography_and_Security Ultima accesare: septembrie 2021.
4. Microsoft. Virtual Machines. Accesibil la: https://developer.microsoft.com/en-us/microsoft-edge/tools/vms/ Ultima accesare: septembrie 2021.