Anexa 2. Internship Securitate Cibernetică

Cerințe generale:

- atenție concentrată și distributivă
- inițiativă
- capacitate de a lucra în echipă
- rezistență la stres
- ușurință, claritate și coerență în exprimare

Cunoștințe necesare:

- concepte de bază Linux
- limbaje de programare/scripting – Python
- baze de date: MySQL
- familiaritate cu OWASP top 10
- familiaritate cu operațiile întreprinse de către un Centru de Operațiuni de Securitate
- rețele de calculatoare – TCP/IP - nivel mediu
- limba engleză (scris, citit, înțeles) - cel puțin nivel mediu

Aptitudini și deprinderi:

- gândire analitică
- autodidact
- capacitate bună de organizare
- aptitudini de comunicare

Criterii de selecție:

Concurs de dosare:

1. analiza CV-ului, a scrisorii de intenție și a portofoliului (dacă este cazul)

Interviu:

1. claritatea și acuratețea răspunsurilor
    1. întrebări de bază pe marginea tematicii de mai jos
2. capacitatea de a analiza și a înțelege o documentație
    1. candidații vor primi o pagină de manual a unei funcții și vor avea la dispoziție 5 minute pentru a citi informațiile prezentate; la finalizarea timpului, aceștia trebuie să explice în câteva cuvinte ce au înțeles din funcția respectivă
3. capacitatea de a analiza o problemă simplă și de a propune o soluție
    1. exemplu: navigarea pe o pagină web este permisă numai dacă este prezent un anumit cookie (ex.: cookie SESSIONID); ce acțiuni trebuie să realizăm pe server?
4. modul de prezentare

Atribuții specifice:

1. Participă la testarea și întreținerea aplicațiilor software elaborate de către BI:
    1. participă la identificarea vectorilor de atac utilizabili în testarea securității aplicațiilor
    2. elaborează module de cod în limbaje de programare
    3. identifică modele și activități care pot compromite securitatea aplicațiilor
    4. testarea aplicațiilor și identificarea vulnerabilităților acestora
2. asigură menținerea securității aplicațiilor Web existente în cadrul infrastructurii TUIASI

Responsabilități:

1. *Legat de atribuțiile specifice, răspunde de:*
    1. buna funcționare a sistemului informatic de la locul său de muncă
    2. respectarea termenelor de execuție și a cerințelor de proiectare
    3. calitatea soluțiilor informatice oferite
    4. nrespectarea standardelor de calitate impuse prin specificațiile proiectelor
    5. respectarea standardelor de bune practici și de etică
2. *Legat de disciplina muncii, răspunde de:*
    1. îmbunătățirea permanentă a pregătirii sale profesionale și de specialitate
    2. păstrarea confidențialității informațiilor și a documentelor cu care operează
    3. utilizarea resurselor existente exclusiv în interesul BI/universității
    4. respectarea prevederilor, a normativelor interne și a procedurilor de lucru privitoare la postul său
    5. respectarea normelor de protecţia muncii şi P.S.I.;
    6. adoptă permanent un comportament în măsură să promoveze imaginea și interesele BI/universității
    7. se implică în vederea soluționării situațiilor de criză

Tematică pentru interviu (pentru toate capitolele se consideră nivelul începător):

1. SOC (Security Operation Center)
    1. noțiuni de bază în ceea ce privește organizarea centrelor de operațiuni de securitate (SOC)
    2. înțelegerea celor 10 funcții cheie ale unui SOC (https://www.mcafee.com/enterprise/en-us/security-awareness/operations/what-is-soc.html)
2. Utilizare baze de date
    1. interogări de bază SQL: select, insert, update, delete, join
    2. operare cu baze de date NoSQL (MongoDB)
3. Injectări
    1. SQL Injection
    2. OS Command Injection
    3. Cross-site Scripting (XSS)
4. Atribute HTTP

1. Furtul de Cookies
2. Prevenția manipulării Cookie-urilor

5. Utilizare Linux/UNIX
    1. sistemul de fișiere Linux/UNIX și drepturi utilizator
    2. procese Linux/UNIX
    3. scripturi si comenzi uzuale Linux/UNIX
6. Comunicații în rețele de calculatoare
    1. modelul de referință ISO/OSI
    2. modelul de referință TCP/IP
    3. protocolul HTTP
7. Servicii de rețea - utilizare
    1. serviciul de nume de domenii (DNS)
    2. serviciul web (Apache)
    3. serviciul de baze de date (MySQL)

Bibliografie:

1. Chris Dotson, Practical Cloud Security, O'Reilly Media, Inc., 2019
2. OWASP Web Security Testing Guide, https://owasp.org/www-project-web-security-testing-guide/
3. Sparc Flow, How to Hack Like a Ghost: Breaching the Cloud, No Starch Press 2021
4. Fahad Ali Sarwar, Python Ethical Hacking from Scratch: Think like an ethical hacker, avoid detection, and successfully develop, deploy, detect, and avoid malware, Packt Publishing, 2021
5. Jovan Pehcevski, Security of cloud-based systems, Arcler Press, 2021
6. Erdal Ozkaya, Incident Response in the Age of Cloud: Techniques and best practices to effectively respond to cybersecurity incidents, Packt Publishing, 2021
7. Andrew S. Tanenbaum, Rețele de calculatoare, editia a 4-a, Ed. Biblos, 2003
8. Matthew West, The Linux System Administrator's Guide, http://www.learnlinux.org.za/courses/build/fundamentals/index.html
9. Advanced Bash-Scripting Guide, http://www.tldp.org/LDP/abs/abs-guide.pdf
10. Red Hat Enterprise Linux Documentation https://access.redhat.com/knowledge/docs/Red_Hat_Enterprise_Linux/