**UNIVERSITATEA DE STAT DIN MOLDOVA**

**Facultatea de Matematică și Informatică**

**Departamentul de Informatică**

CURRICULUM

la unitatea de curs

*Virtualizare și containerizare*

Ciclul I, Licență

**Programul de studii / Specialitatea: 0613.4 Informatică**

AUTOR:

lector. univ. Mihail CROITOR

**APROBAT**

**la şedinţa Departamentului**

**din \_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_ 2025**

**proces-verbal nr. \_\_\_\_\_\_**

**Şef Departament \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**APROBAT**

**la şedinţa Consiliului Facultății**

**din \_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_ 2025**

**proces-verbal nr. \_\_\_\_\_\_**

**Decan \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**Chișinău 2025**

**PRELIMINARII**

*Prezentarea generală a cursului*

În lumea tehnologiilor informaționale moderne, virtualizarea și containerizarea au devenit instrumente esențiale pentru dezvoltarea, implementarea și administrarea aplicațiilor. Aceste tehnologii permit utilizarea eficientă a resurselor, asigură izolarea aplicațiilor și simplifică procesele de implementare și scalare. Utilizarea mașinilor virtuale și a containerelor le permite dezvoltatorilor și administratorilor de sistem să creeze soluții flexibile și scalabile, care pot funcționa în diverse medii, de la servere locale până la platforme Cloud. De asemenea, aspectul economic este important, deoarece utilizarea virtualizării și containerizării permite reducerea semnificativă a costurilor pentru echipamente și exploatarea serverelor.

În cadrul acestui curs sunt analizate principalele tehnologii de virtualizare (pe baza *Qemu*) și containerizarea aplicațiilor (pe baza *Docker*). Sunt abordate conceptele de bază, crearea mașinilor virtuale, crearea imaginilor, lansarea containerelor, interacțiunea cu containerele, orchestrarea containerelor, procesele CI/CD, optimizarea imaginilor.

*Locul și rolul cursului în formarea rezultatelor învățării ale specialității și misiunea curriculumului în formarea profesională*

Cursul de Virtualizare și containerizare ocupă un loc important în dezvoltarea competențelor practice și teoretice ale studenților din programul 0613.4 Informatică. Cursul are dependența strictă de la cursuri ”Sisteme de operare”, ”Baze de date”, ”Rețele de calculatoare”.

Studenții vor dobândi competențe precum:

* Înțelegerea conceptelor de bază ale virtualizării și containerizării.
* Abilitatea de a crea și administra mașini virtuale folosind Qemu.
* Abilitatea de a crea și administra containere folosind Docker.
* Cunoașterea elementelor de bază ale orchestrării containerelor cu Docker Compose.
* Înțelegerea principiilor CI/CD și capacitatea de a le aplica în contextul virtualizării și containerizării.
* Abilitatea de a optimiza imaginile containerelor pentru a crește performanța și a reduce dimensiunea acestora.

La finalul cursului, studenții vor cunoaște conceptele de bază ale virtualizării și containerizării, precum și vor putea aplica cunoștințele dobândite în practică. Studenții vor putea crea sisteme informaționale complexe și infrastructura aferentă acestora utilizând cunoștințele acumulate, precum și să optimizeze soluțiile existente.

*Limba de predare a cursului*

Cursul este predat în limbile română și rusă, pentru a răspunde nevoilor lingvistice ale studenților din cadrul Universității de Stat din Moldova. Acest aspect asigură accesibilitatea materialelor de studiu și facilitează comunicarea eficientă în timpul activităților didactice și de laborator.

*Beneficiarii*

Beneficiarii principali ai acestui curs sunt:

* Studenții programului de licență 0613.4 Informatică, care își vor consolida cunoștințele în DevOps.
* Profesioniști din domeniul IT, interesați de actualizarea competențelor lor în testarea de penetrare și protecția rețelelor.

1. **ADMINISTRAREA DISCIPLINEI**

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Forma de învățământ | Codul unității de curs | Denumirea unității de curs | Responsabil de unitatea de curs | Semestrul | Numărul de ore | | | | | | | Evaluarea | Nr. de credite |
| Total | Contact direct | | | AMU\* | Studiul individual | |
| Curs | Seminar | Laborator | asincron\* | individual |
| cu frecvență | S.A.35 | Virtualizare și Containerizare | M. Croitor | IV | 120 | 20 | 0 | 40 | 0 | 0 | 60 | Ex | 4 |
| cu frecvență redusă |  |  |  |  |  |  |  |  |  |  |  |  |  |
| la distanță |  |  |  |  |  |  |  |  |  |  |  |  |  |
| dual |  |  |  |  |  |  |  |  |  |  |  |  |  |

\*Activitatea de muncă la unitate – pentru învățământul dual

\*Pentru învățământul cu frecvență redusă și la distanță

1. **Tematica ŞI REPARTIZAREA ORIENTATIVĂ A ORELOR**

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Unități de conținut** | **Numărul de ore** | | | | | | | | | | | | | | |
| **Curs** | | | | **Laborator** | | | | **AMU** | **Studiul individual** | | | | | |
| **Cu frecvență** | **Frecvență redusă** | **La distanță** | **Dual** | **Cu frecvență** | **Frecvență redusă** | **La distanță** | **Dual** | **Dual** | **Cu frecvență** | **Frecvență redusă** | | **La distanță** | | **Dual** |
| **Asincron** | **Individual** | **Asincron** | **Individual** |
| **Tema 1: Introducere / Istorie**  **Subteme:**   * Virtualizare; * Containerizare; * Istoria dezvoltării virtualizării și containerizării; * Noțiuni de bază.   **Activități de laborator:**   * Crearea contului pe GitHub; * Pregătirea paginii personale pe GitHub; * Familiarizarea cu comenzile git; * Familiarizarea cu format Markdown; * Familiarizarea cu procesele de lucru cu ramuri de cod sursă. | **2** |  |  |  | **4** |  |  |  |  | **6** |  |  |  |  |  |
| **Tema 2: Virtualizarea SO**  **Subteme:**   * Noțiunea de virtualizare; * Tipuri de virtualizare; * Hipervizorii; * Virtualizarea pe baza QEMU; * Open Virtualization Format.   **Activități de laborator:**   * Instalarea QEMU; * Crearea imaginii de disc; * Instalarea Debian în mașina virtuala; * Instalarea și configurarea LAMP; * Instalarea Drupal; * Instalarea PhpMyAdmin. | **2** |  |  |  | **4** |  |  |  |  | **6** |  |  |  |  |  |
| **Tema 3: Sintaxa Dockerfile:**   * Ce este Docker; * Arhitectura fișierului Dockerfile; * Instrucțiuni Dockerfile: FROM, COPY, ADD, RUN, CMD, ENTRYPOINT, WORKDIR, USER.   **Activități de laborator:**   * Crearea unei imagini al containerului; * Crearea containerului; * Pornirea containerului; * Conectarea la container și perfectarea unor evaluări; * Oprirea și ștergerea containerului. | **2** |  |  |  | **4** |  |  |  |  | **6** |  |  |  |  |  |
| **Tema 4: Pornirea aplicațiilor containerizate**  **Subteme:**   * Instrumente Docker; * Asamblarea imaginilor; * Managementul imaginilor; * Managementul containerelor; * Comunicarea cu containere.   **Activități de laborator:**   * Utilizarea containerelor ca medii de execuție; * Familiarizarea cu comenzile de bază Ubuntu / Debian. | **2** |  |  |  | **4** |  |  |  |  | **6** |  |  |  |  |  |
| **Tema 5: Comenzile suplimentare din Dockerfile**  **Subteme:**   * Variabile la construirea imaginii; * Interacțiunea cu containerul; * Metadatele imaginii; * Comenzile suplimentare.   **Activități de laborator:**   * Crearea structurii unui proiect complex; * Configurarea Apache HTTP Server; * Configurarea PHP; * Configurarea MariaDB; * Configurarea supervisor; * Instalarea WordPress. | **2** |  |  |  | **8** |  |  |  |  | **12** |  |  |  |  |  |
| **Tema 6: Interacțiunea containerelor**  **Subteme:**   * Sistem de fișiere; * Rețea.   **Activități de laborator:**   * Crearea rețelelor; * Crearea volumelor; * Montarea volumelor; * Organizarea comunicării dintre containere. | **2** |  |  |  | **4** |  |  |  |  | **6** |  |  |  |  |  |
| **Tema 7: Crearea unui cluster de containere cu ajutorul Docker Compose**  **Subteme:**   * Scopul Docker Compose; * Sintaxa docker-compose.yml; * Un exemplu de cluster de containere; * Gestionarea clusterului de containere.   **Activități de laborator:**   * Familiarizarea cu format docker-compose.yml; * Configurarea Nginx; * Configurarea PHP-FPM; * Crearea serviciilor cu ajutorul containerilor. | **2** |  |  |  | **4** |  |  |  |  | **6** |  |  |  |  |  |
| **Tema 8: Particularitățile configurării clusterului de containere**   * Argumente la construirea imaginii; * Variabile de mediu; * Limitarea resurselor; * Acces către procesor grafic; * Verificarea stării containerului (healthcheck).   **Activități de laborator:**   * Montarea volumelor și directoriilor; * Utilizarea variabilelor de sistem; * Utilizarea secretelor; * Configurarea healthcheck. | **2** |  |  |  | **4** |  |  |  |  | **6** |  |  |  |  |  |
| **Tema 9: Integrarea continuă și livrarea continuă (CI / CD)**  **Subteme:**   * Integrarea continuă; * Livrarea continuă; * Un exemplu de proces CI / CD; * Utilizarea containerelor în procesele CI / CD.   **Activități de laborator:**   * Definirea procesului CI * Familiarizarea cu GitHub Actions; * Utilizarea containerelor în CI. | **2** |  |  |  | **4** |  |  |  |  | **6** |  |  |  |  |  |
| **Tema 10: Practici bune. Optimizarea imaginii containerului.**   * Privilegii excesive; * Dependențe; * Securizarea datelor; * Optimizarea imaginii containerului.   **Activități de laborator:**   * Ștergerea fișierelor temporare și a dependențelor neutilizate; * Reducerea numărului de straturi; * Utilizarea unei imagini de bază minime; * Reambalarea imaginii. | **2** |  |  |  | **4** |  |  |  |  | **6** |  |  |  |  |  |
| **TOTAL** | **20** |  |  |  | **40** |  |  |  |  | **60** |  |  |  |  |  |

1. **COMPETENŢE GENERALE, PROFESIONALE ŞI REZULTATELE ÎNVĂȚĂRII**

|  |  |
| --- | --- |
| **Competențe generale și profesionale** | **Rezultate ale învățării conform nivelului CNC**  *Absolventul/candidatul la atribuirea calificării poate:* |
| **CG 2.** Operarea cu concepte de bază din știința calculatoarelor, tehnologia informației și comunicațiilor | RÎ3. aplica conceptele din știința calculatoarelor, tehnologia informației și comunicațiilor pentru proiectarea și administrarea sistemelor informaționale.  RÎ4. dezvolta sisteme informaționale folosind cunoștințe referitoare la limbaje, medii și tehnologii de programare și instrumente de proiectare. |
| **CP 1.** Descrierea funcțională a sistemului informatic utilizând tehnici, modele și algoritmi din domeniu | RÎ10. elabora modelul constructiv-funcțional prin utilizarea tehnicilor, modelelor și algoritmilor din domeniu, aplicând metode de modelare, sinteză, analiză, precum și optimizare a sistemelor. |
| **CP 2.** Proiectarea sistemelor și integrarea componentelor unui sistem informatic | RÎ11. proiecta aplicații software de uz general și dedicat, prin aplicarea metodelor de modelare, sinteză, analiză și optimizare a sistemelor informatice.  RÎ12. dezvolta conceptul de realizare și funcționare a sistemului proiectat, precum și a unor ansambluri parțiale integrate în subsistemul informatic. |
| **CP 3.** Validarea aplicațiilor informatice | RÎ13. testa sistemele informatice pentru verificarea integrității, funcționalității generale a sistemului și a interacțiunii între componentele sale.  RÎ14. realiza simulări pentru validarea corectitudinii modelelor și algoritmilor, asigurând compatibilitatea componentelor cu cerințele și obiectivele stabilite. |
| **CP 4.** Mentenanța și optimizarea sistemului informatic | RÎ15. planifica lucrările de mentenanță pentru a asigura buna funcționare a sistemului informatic. |

1. **UNITĂŢI DE ÎNVĂȚARE**

|  |  |  |
| --- | --- | --- |
| **Tema 1: Introducere / Istorie**  **Rezultatele învățării preconizate a fi atinse: RÎ 3; RÎ 12; RÎ 13; RÎ 14** | | |
| Cunoștințe / unități de conținut | Abilități | Responsabilitate și autonomie |
| *Termeni-cheie:*  Containerizare, virtualizare, izolarea procesului.  *Unități de conținut:*  **Subteme:**   * Virtualizare; * Containerizare; * Istoria dezvoltării virtualizării și containerizării; * Noțiuni de bază.   **Activități de laborator:**   * Crearea contului pe GitHub; * Pregătirea paginii personale pe GitHub; * Familiarizarea cu comenzile git; * Familiarizarea cu format Markdown; * Familiarizarea cu procesele de lucru cu ramuri de cod sursă. | * Analizează principiile securității cibernetice și explică importanța confidențialității, integrității și disponibilității datelor. * Identifică tipurile de amenințări și clasifică atacurile cibernetice (pasive, active, interne, externe). * Descrie conceptele de testare de penetrare și hacking etic, incluzând scopurile, metodele și etica profesională. | * Demonstrează respect pentru etica profesională în testarea de penetrare, asigurând conformitatea cu standardele legale și de securitate. * Colaborează eficient cu colegii în crearea unui laborator de testare, asumându-și responsabilitatea pentru buna funcționare a resurselor sistemului. |
| **Tema 2: Virtualizarea SO**  **Rezultatele învățării preconizate a fi atinse: RÎ 3; RÎ 4; RÎ 10; RÎ 11; RÎ 14** | | |
| Cunoștințe / unități de conținut | Abilități | Responsabilitate și autonomie |
| *Termeni-cheie:*  Rețele wireless, frecvențe Wi-Fi, vulnerabilități wireless, analiza pachetelor, spoofing MAC, atacuri de deautentificare, securizarea rețelelor, testare înainte de conectare.  *Unități de conținut:* | * Explică principiile de funcționare ale rețelelor wireless și diferențele dintre benzile de frecvență Wi-Fi (2.4 GHz și 5 GHz). * Identifică vulnerabilitățile comune ale rețelelor wireless și impactul acestora asupra securității. * Analizează pachetele de rețea pentru a înțelege fluxurile de date și comportamentele dispozitivelor. * Aplică tehnici de spoofing pentru a simula modificarea adresei MAC. * Planifică și execută atacuri de deautentificare asupra rețelelor wireless, utilizând scenarii variate. * Utilizează unelte specializate pentru testarea securității rețelelor înainte de conectare. * Propune măsuri de securizare a rețelelor wireless pentru a preveni atacurile discutate. | * Evaluează impactul vulnerabilităților asupra securității rețelelor wireless și propune soluții de remediere. |
| **Tema 3: Sintaxa Dockerfile**  **Rezultatele învățării preconizate a fi atinse: RÎ 3; RÎ 11; RÎ 12; RÎ 13; RÎ 15** | | |
| Cunoștințe / unități de conținut | Abilități | Responsabilitate și autonomie |
| *Termeni cheie:*  Criptare WEP, WPA/WPA2, atacuri ARP replay, scanare activă, bypass MAC, Aircrack-ng, Evil Twin, securizare wireless.  *Unități de conținut:*  **Subteme:**   * Atacuri asupra criptării WEP: autentificarea falsă, atacul ARP replay. * Scanarea și conectarea la rețele ascunse. * Bypass-ul filtrării MAC: liste negre și liste albe. * Atacuri asupra criptării WPA/WPA2: captarea handshake-ului, crearea și utilizarea wordlist-urilor. Utilizarea Aircrack-ng și Hcxdumptool pentru testarea securității wireless. * Atacuri de tip Evil Twin: crearea de puncte de acces false și captarea acreditărilor de autentificare. * Măsuri de protecție wireless. Configurarea setărilor wireless pentru securitate maximă. Prevenirea atacurilor de tip deautentificare, spoofing MAC și crack WPA/WPA2.   **Activități de laborator:**   * Scanarea activă: utilizarea Nmap pentru descoperirea rețelelor. * Cracking WEP cu ARP replay. * Captarea handshake WPA2 și folosirea Aircrack-ng. * Folosirea Hcxdumptool pentru captarea traficului. * Crearea unui punct de acces fals cu hostapd. * Analiza setărilor de securitate wireless. | * Explică mecanismele de criptare WEP, WPA și WPA2, identificând vulnerabilitățile specifice fiecăruia. * Demonstrează utilizarea tehnicilor de atac asupra rețelelor WEP, inclusiv autentificarea falsă și atacul ARP replay. * Utilizează instrumente precum Nmap pentru scanarea activă și identificarea rețelelor ascunse. * Aplică tehnici de bypass pentru filtrarea MAC folosind liste negre și albe. * Analizează și execută atacuri asupra criptării WPA/WPA2, inclusiv captarea handshake-ului și utilizarea de wordlist-uri pentru crack. * Configurează puncte de acces false (Evil Twin) pentru a testa securitatea rețelelor și a identifica riscurile asociate. * Propune și implementează setări de securitate wireless pentru prevenirea atacurilor de tip spoofing, deautentificare și crack WPA/WPA2. * Utilizează instrumente precum Aircrack-ng și Hcxdumptool pentru testarea și consolidarea securității rețelelor wireless. | * Evaluează măsurile de securitate ale rețelelor wireless și propune soluții eficiente pentru remedierea vulnerabilităților. * Respectă normele etice și legale în timpul testelor de penetrare și al analizelor de securitate. |
| **Tema 4: Pornirea aplicațiilor containerizate**  **Rezultatele învățării preconizate a fi atinse: RÎ 3; RÎ 4; RÎ 11; RÎ 13; RÎ 14** | | |
| Cunoștințe / unități de conținut | Abilități | Responsabilitate și autonomie |
| *Termeni cheie:*  Hashing, salting, brute force, dictionary attack, John the Ripper, Hashcat, securitatea parolelor, wordlist.  *Unități de conținut:*  **Subteme:**   * Principii și metode de autentificare. Hashing-ul și salting-ul parolelor. * Atacuri brute force și dictionary attacks.   **Activități de laborator:**   * Crearea hashurilor cu algoritmi (ex: SHA256). * Utilizarea John the Ripper pentru atacuri de spargere a parolelor. * Utilizarea Hashcat pentru parole complexe. * Crearea și testarea de wordlist-uri personalizate. | * Explică principiile autentificării și metodele moderne de protecție a parolelor, inclusiv hashing-ul și salting-ul. * Analizează diferențele dintre atacurile brute force și dictionary attacks, evaluând eficiența acestora. * Utilizează John the Ripper pentru testarea vulnerabilităților asociate cu parolele slabe. * Configurează și rulează Hashcat pentru efectuarea de atacuri pe parole criptate. * Identifică tehnici de optimizare a atacurilor brute force prin utilizarea resurselor hardware și a strategiilor specifice. * Creează și gestionează wordlist-uri personalizate pentru dictionary attacks, adaptate scenariilor de testare. * Propune soluții pentru îmbunătățirea securității parolelor, având în vedere bunele practici și cerințele de complexitate. * Evaluează rezultatele testelor de penetrare asupra parolelor, documentând procesele și concluziile obținute. | * Respectă normele etice și legale în utilizarea tehnologiilor de testare a parolelor, asigurând protecția datelor sensibile. * Coordonează activitățile de evaluare a securității parolelor, colaborând eficient cu echipele de securitate și dezvoltare. |
| **Tema 5: Comenzile suplimentare din Dockerfile**  **Rezultatele învățării preconizate a fi atinse: RÎ 3; RÎ 4; RÎ 11; RÎ 12; RÎ 13; RÎ 14; RÎ 15** | | |
| Cunoștințe / unități de conținut | Abilități | Responsabilitate și autonomie |
| *Termeni cheie:*  Ethernet, ARP, MITM, ARP poisoning, Bettercap, Wireshark, DNS spoofing, honeypots.  *Unități de conținut:*  **Subteme:**   * Analiza protocoalelor Ethernet și ARP. * Atacuri MITM (Man-in-the-Middle). * ARP poisoning. * DNS spoofing și injecția de cod JavaScript. * Crearea de honeypots pentru captarea datelor utilizatorilor. * Detectarea și prevenirea atacurilor asupra rețelelor Ethernet.   **Activități de laborator:**   * ARP poisoning cu Bettercap. * Interceptarea și analizarea traficului de rețea cu Wireshark. * Simularea DNS spoofing cu Bettercap. * Includerea de cod JavaScript în pagini injectate. * Configurarea unui honeypot cu Honeyd sau alte unelte. | * Analizează structura și funcționalitatea protocoalelor Ethernet și ARP în cadrul rețelelor. * Explică principiile atacurilor Man-in-the-Middle (MITM) și impactul acestora asupra securității rețelelor. * Utilizează instrumente precum Bettercap și Wireshark pentru interceptarea și analiza traficului de rețea. * Descrie și implementează atacuri de tip ARP poisoning și DNS spoofing pentru testarea vulnerabilităților. * Realizează injecții de cod JavaScript în trafic prin atacuri DNS spoofing. * Creează honeypots pentru monitorizarea și captarea activităților malițioase în rețea. * Detectează și documentează atacurile MITM, oferind soluții de prevenire și protecție. * Evaluează riscurile asociate atacurilor DNS cache poisoning și propune măsuri de atenuare. | * Respectă normele etice și juridice în testarea și evaluarea vulnerabilităților de rețea. * Coordonează procesele de identificare și prevenire a atacurilor, colaborând cu echipele de securitate IT. |
| **Tema 6: Interacțiunea containerelor**  **Rezultatele învățării preconizate a fi atinse: RÎ 3; RÎ 13; RÎ 14; RÎ 15** | | |
| Cunoștințe / unități de conținut | Abilități | Responsabilitate și autonomie |
| *Termeni cheie:*  Wireshark, pachete de rețea, protocoale, sesiuni, MITMproxy, filtrare, fluxuri de date, analiză trafic.  *Unități de conținut:*  **Subteme:**   * Capturarea și analiza pachetelor de rețea. * Interpretarea datelor capturate: protocoale, adrese, sesiuni. * Filtrarea și disecarea pachetelor: identificarea informațiilor sensibile. * Analizarea fluxurilor de date și utilizarea MITMproxy pentru atacuri și apărare.   **Activități de laborator:**   * Capturarea traficului HTTP/S cu Wireshark. * Utilizarea filtrelor de analiză în Wireshark. * Utilizarea MITMproxy pentru inspectarea și manipularea traficului. * Identificarea parolelor în trafic necriptat. | * Utilizează Wireshark pentru capturarea și analiza traficului de rețea. * Interpretează datele capturate, identificând protocoale, adrese și sesiuni relevante. * Filtrează și disecă pachetele pentru a detecta informații sensibile și anomalii în trafic. * Analizează fluxurile de date și identifică potențiale amenințări de securitate. * Utilizează MITMproxy pentru simularea atacurilor și implementarea măsurilor de apărare. * Evaluează vulnerabilitățile rețelelor pe baza analizei pachetelor capturate. * Identifică indicatorii de compromitere în traficul de rețea. * Documentează procesele și rezultatele analizei pentru a susține măsurile de securitate IT. | * Respectă standardele etice și juridice în capturarea și analiza traficului de rețea. * Coordonează activitățile de analiză și raportare, colaborând cu echipele de securitate. |
| **Tema 7: Crearea unui cluster de containere cu ajutorul Docker Compose**  **Rezultatele învățării preconizate a fi atinse: RÎ 3; RÎ 4; RÎ 11; RÎ 12; RÎ 13; RÎ 14** | | |
| Cunoștințe / unități de conținut | Abilități | Responsabilitate și autonomie |
| *Termeni cheie:*  Vulnerabilități server-side, vulnerabilități client-side, Metasploit Framework, inginerie socială, execuție de cod, backdoor, spoofing, sisteme vechi.  *Unități de conținut:*  **Subteme:**   * Vulnerabilități server-side vs. client-side. * Vulnerabilități server-side: exploatarea execuțiilor de cod. * Vulnerabilități client-side: crearea și utilizarea backdoor-urilor și troienilor. * Exploatarea cu Metasploit Framework: atacuri server-side și client-side. * Introducere în ingineria socială: spoofing de emailuri și manipularea utilizatorilor.   **Activități de laborator:**   * Scanarea vulnerabilităților cu Metasploit. Vulnerabilități în aplicații și sisteme vechi: studii de caz. * Exploatarea serviciilor vulnerabile (ex: Samba, FTP). * Crearea unui troian cu msfvenom. * Simularea unui atac de inginerie socială (ex: phishing email). | * Identifică vulnerabilitățile existente în servere, aplicații și sisteme. * Exploatează vulnerabilitățile server-side utilizând instrumente dedicate precum Metasploit Framework. * Creează și utilizează backdoor-uri și troieni pentru simularea vulnerabilităților client-side. * Analizează studiile de caz pentru a înțelege impactul vulnerabilităților din aplicații și sisteme vechi. * Aplică metode de inginerie socială, precum spoofing-ul de emailuri, pentru evaluarea rezilienței utilizatorilor. * Utilizează metode avansate de execuție de cod pentru exploatarea sistemelor compromise. * Evaluează riscurile asociate vulnerabilităților exploatate și propune măsuri de remediere. * Documentează procesele și rezultatele exploatării vulnerabilităților pentru a sprijini îmbunătățirea securității. | * Respectă limitele etice și legale în procesul de identificare și exploatare a vulnerabilităților. * Colaborează eficient cu echipele de securitate pentru a comunica rezultatele și a implementa soluții de remediere. |
| **Tema 8: Particularitățile configurării clusterului de containere**  **Rezultatele învățării preconizate a fi atinse: RÎ 3; RÎ 11; RÎ 12; RÎ 13; RÎ 14** | | |
| Cunoștințe / unități de conținut | Abilități | Responsabilitate și autonomie |
| *Termeni cheie:*  Meterpreter, persistență, pivotare, escaladarea privilegiilor, spionaj, captarea tastelor, capturi de ecran, evitarea detectării.  *Unități de conținut:*  **Subteme:**   * Utilizarea Meterpreter pentru acces avansat la sistem: captarea tastelor, capturi de ecran. * Persistența accesului și pivotarea către alte sisteme. * Spionajul post-exploatare și escaladarea privilegiilor.   **Activități de laborator:**   * Colectarea tastelor cu keylogger în Meterpreter. * Capturi de ecran remote. * Persistență prin backdoor. * Pivotare între rețele cu route add în Metasploit. * Exploatarea vulnerabilităților de escaladare (Linux/Windows). | * Utilizează Meterpreter pentru a obține acces avansat la sistem și pentru a captura informații sensibile, precum tastele introduse sau capturi de ecran. * Creează metode de persistență pentru menținerea accesului în sistemele compromise. * Planifică și execută operațiuni de pivotare pentru extinderea accesului la alte sisteme din rețea. * Analizează și implementează tehnici de spionaj post-exploatare pentru colectarea de date sensibile. * Escaladează privilegiile în scopul obținerii controlului total asupra sistemului țintă. * Evaluează riscurile asociate cu activitățile de post-exploatare și propune măsuri de remediere. * Documentează metodele și rezultatele post-exploatării pentru a asigura trasabilitatea și îmbunătățirea securității. * Identifică și aplică tehnici de evitare a detectării în timpul activităților de post-exploatare. | * Respectă normele etice și juridice în derularea activităților de post-exploatare, asigurând un impact minim asupra sistemelor țintă. * Colaborează cu echipele de securitate și comunică rezultatele procesului de post-exploatare pentru a sprijini consolidarea securității organizației. |
| **Tema 9: Integrarea continuă și livrarea continuă (CI / CD)**  **Rezultatele învățării preconizate a fi atinse: RÎ 3; RÎ 12; RÎ 13; RÎ 14; RÎ 15** | | |
| Cunoștințe / unități de conținut | Abilități | Responsabilitate și autonomie |
| *Termeni cheie:*  Recunoaștere, DNS, subdomenii, fișiere sensibile, tehnologii web, vulnerabilități, analiza serverelor, framework-uri web.  *Unități de conținut:*  **Subteme:**   * Identificarea tehnologiilor utilizate pe site-uri. * Obținerea informațiilor DNS și descoperirea subdomeniilor. * Descoperirea fișierelor sensibile și analiza acestora.   **Activități de laborator:**   * Scanarea site-urilor cu WhatWeb și Wappalyzer. * Obținerea subdomeniilor cu Sublist3r. * Accesarea fișierelor sensibile (robots.txt, .git, .env). | * Identifică tehnologiile utilizate în dezvoltarea și funcționarea site-urilor web prin analiza componentelor front-end și back-end. * Colectează informații DNS și descoperă subdomenii utilizând instrumente și metode specifice. * Analizează structura site-urilor web pentru a detecta fișiere sensibile sau expuse. * Utilizează tehnici de recunoaștere pentru a obține informații despre servere, platforme și framework-uri web. * Identifică punctele potențiale de vulnerabilitate în structura și configurația site-urilor web. * Evaluează impactul fișierelor sensibile descoperite asupra securității unui site. * Documentează rezultatele procesului de colectare a informațiilor pentru a sprijini testele de penetrare ulterioare. * Respectă normele de etică și legalitate în procesul de colectare a informațiilor. | * Planifică și desfășoară procese de recunoaștere web respectând limitele etice și legale, cu responsabilitate față de confidențialitatea informațiilor. * Comunică eficient rezultatele analizei către echipele de securitate pentru remedierea vulnerabilităților. |
| **Tema 10: Practici bune. Optimizarea imaginii containerului.**  **Rezultatele învățării preconizate a fi atinse: RÎ 3; RÎ 4; RÎ 11; RÎ 13; RÎ 14; RÎ 15** | | |
| Cunoștințe / unități de conținut | Abilități | Responsabilitate și autonomie |
| *Termeni cheie:*  SQL Injection, Cross-Site Scripting, XSS, Directory Traversal, Metasploit, BeEF, OWASP Top 10, vulnerabilități web.  *Unități de conținut:*  **Subteme:**   * Atacuri comune: SQL injection, Cross-Site Scripting (XSS), Directory Traversal. * Exploatarea vulnerabilităților SQL Injection: extragerea datelor și acces la fișiere. * Vulnerabilități Cross-Site Scripting (XSS): reflectate și stocate. * Utilizarea BeEF pentru exploatarea vulnerabilităților XSS. * Prevenirea vulnerabilităților OWASP Top 10.   **Activități de laborator:**   * Exploatarea SQLi cu sqlmap. * Testarea XSS cu payloaduri reflectate și stocate. * Utilizarea BeEF pentru sesiuni XSS. * Scanarea aplicațiilor vulnerabile cu Metasploit. | * Identifică și descrie cele mai comune vulnerabilități în aplicațiile web, cum ar fi SQL Injection, Cross-Site Scripting (XSS) și Directory Traversal. * Exploatează vulnerabilitățile SQL Injection pentru a extrage date din baze de date sau pentru a accesa fișiere sensibile. * Demonstrează tehnici de exploatare a vulnerabilităților XSS, inclusiv atacuri reflectate și stocate. * Utilizează BeEF pentru a exploata vulnerabilitățile XSS și a compromite aplicațiile web. * Utilizează Metasploit pentru a exploata aplicațiile web vulnerabile și a efectua atacuri de penetrare. * Evaluează și implementează soluții pentru prevenirea vulnerabilităților comune identificate în OWASP Top 10. * Aplica bune practici de securitate în dezvoltarea aplicațiilor pentru a preveni vulnerabilitățile de tip SQL Injection și XSS. * Documentează și prezintă rezultatele exploatării vulnerabilităților într-o aplicație web pentru scopuri educaționale sau de securitate. | * Planifică și implementează strategii de testare și securizare a aplicațiilor web, având în vedere riscurile identificate. * Comunică eficient recomandările și soluțiile de securizare către echipele de dezvoltare și managementul proiectului. |

1. **LUCRUL INDIVIDUAL AL STUDENTULUI**

Materialul examinat în cadrul lecțiilor de curs și de laborator include elementele necesare pentru a realiza de sine stătător sarcinile pentru lucrul individual.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| ***Tema***  ***Nr.*** | ***Activitatea lucrului individual*** | ***Strategia de realizare*** | ***Criterii de evaluare*** | ***Termen de realizare*** |
| 1 | Exersarea comenzilor Linux și instalarea Kali Linux acasă | 1. **Instalarea Kali Linux** – Descarcă, instalează și configurează Kali Linux pe o mașină virtuală sau pe un sistem fizic dedicat, urmând pașii din documentația oficială. 2. **Familiarizarea cu comenzile Linux** – Exersează comenzile de bază pentru gestionarea fișierelor și a permisiunilor, precum și pentru monitorizarea și analiza traficului. 3. **Testarea mediului de lucru** – Realizează teste de bază, precum scanarea rețelelor sau verificarea configurării corecte a Kali Linux, pentru a se asigura că mediul de lucru funcționează corespunzător. | * Corectitudinea instalării Kali Linux – Verificarea corectitudinii instalării și configurării mediului. * Abilitatea de a utiliza comenzi de bază – Capacitatea de a aplica comenzile Linux esențiale într-un context de testare de penetrare. * Funcționarea mediului de lucru – Testarea mediului și utilizarea instrumentelor specifice în scopul simulării atacurilor. | Săptămâna 1 |
| 2 | Studii suplimentare despre funcționarea rețelelor wireless și analiza pachetelor | 1. Studierea protocoalelor wireless – Înțelege protocoalele de securitate wireless (WEP, WPA, WPA2) și cum sunt exploatate vulnerabilitățile acestora. 2. Capturarea traficului wireless – Utilizează instrumente de capturare a traficului (Wireshark) pentru a analiza pachetele de date din rețelele wireless. 3. Analiza vulnerabilităților – Identifică și documentează vulnerabilitățile rețelelor wireless capturate, inclusiv atacuri precum deautentificarea și interceptarea traficului. | * Corectitudinea capturării traficului – Analiza și corectitudinea procesului de capturare a pachetelor de trafic wireless. * Identificarea vulnerabilităților – Capacitatea de a identifica vulnerabilitățile în rețelele wireless și încripta traficul. * Raportul de analiză a traficului – Completitudinea și acuratețea raportului în ceea ce privește vulnerabilitățile identificate. | Săptămâna 2 |
| 3 | Configurarea și testarea rețelelor wireless securizate | 1. Configurarea unei rețele securizate – Creează o rețea wireless cu protecție WEP, WPA2 sau WPA3 și configurează setările de securitate. 2. Testarea rețelei – Realizează atacuri pentru a verifica vulnerabilitățile rețelei securizate, cum ar fi teste de spargere a parolelor. 3. Implementarea măsurilor de securitate suplimentare – După identificarea vulnerabilităților, aplică soluții pentru a întări securitatea rețelei (ex: activarea criptării suplimentare). | * Corectitudinea configurării rețelei – Verificarea configurării corecte a rețelei wireless cu protocoale de securitate. * Eficiența atacurilor – Măsura în care atacurile asupra rețelei au identificat vulnerabilități reale. * Implementarea măsurilor de securitate – Capacitatea de a implementa și valida măsurile de protecție a rețelei. | Săptămâna 3 |
| 4 | Pregătirea și optimizarea wordlist-urilor pentru atacuri | 1. Crearea de wordlist-uri – Folosește un generator de wordlist-uri (Crunch, CeWL) pentru a crea liste de parole pentru atacuri brute force. 2. Testarea parola pe sisteme testate – Utilizează listele pentru a executa atacuri brute force pe sisteme testate, folosind instrumente precum Hydra sau Medusa. 3. Optimizarea listei de parole – Analizează eficiența atacurilor și ajustează wordlist-urile pentru a îmbunătăți succesul atacurilor. | * Calitatea wordlist-urilor – Eficiența și corectitudinea generării wordlist-urilor. * Succesul atacurilor brute force – Procentul de succes în identificarea parolelor pe diverse sisteme. * Optimizarea strategiilor de atac – Capacitatea de a ajusta și îmbunătăți atacurile brute force pentru a crește eficiența. | Săptămâna 4 |
| 5 | Analiza scenariilor reale și implementarea honeypots | 1. Studiul vulnerabilităților Ethernet – Explorează vulnerabilitățile rețelelor Ethernet, cum ar fi atacurile de tip ARP Spoofing sau DHCP Spoofing. 2. Implementarea unui honeypot – Creează și configurează un honeypot pentru a simula atacuri și a captura tentativele de exploatare. 3. Analiza datelor capturate – Examinează logurile și datele capturate pentru a identifica pattern-uri și a propune soluții de securizare. | * Corectitudinea implementării honeypot-ului – Funcționalitatea și eficiența honeypot-ului implementat. * Capacitatea de identificare a atacurilor – Abilitatea de a analiza și identifica atacurile rețelelor Ethernet. * Raportul privind vulnerabilitățile – Completitudinea raportului care prezintă vulnerabilitățile și soluțiile propuse. | Săptămâna 5 |
| 6 | Analiza detaliată a traficului capturat și crearea rapoartelor | 1. Capturarea traficului cu Wireshark – Utilizează Wireshark pentru a captura traficul de rețea din diverse scenarii (ex: rețele wireless sau Ethernet). 2. Analiza pachetelor – Examinează pachetele de date pentru a detecta informații sensibile, erori de configurare sau potențiale atacuri. 3. Crearea raportului de analiză – Documentează rezultatele analizei traficului capturat și identifică riscurile de securitate. | * Corectitudinea capturării pachetelor – Verificarea corectitudinii capturării și a setărilor Wireshark. * Calitatea analizei traficului – Abilitatea de a analiza pachetele de date și de a identifica riscurile de securitate. * Raportul de analiză – Claritatea și completitudinea raportului final privind vulnerabilitățile și soluțiile posibile. | Săptămâna 6 |
| 7 | Analiza vulnerabilităților CVE și exersarea scenariilor de atac | 1. Studiul vulnerabilităților CVE – Identifică vulnerabilitățile cele mai comune pentru servere și aplicații folosind baza de date CVE. 2. Exploatarea vulnerabilităților – Folosește instrumente precum Metasploit pentru a exploata vulnerabilitățile identificate. 3. Documentarea și recomandările de remediere – Creează un raport detaliat care prezintă vulnerabilitățile, atacurile aplicate și soluțiile propuse. | * Corectitudinea identificării vulnerabilităților – Capacitatea de a găsi și exploata vulnerabilitățile critice. * Succesul atacului – Măsura în care atacurile realizate au exploatat eficient vulnerabilitățile. * Calitatea raportului de remediere – Detaliile și soluțiile oferite pentru remedierea vulnerabilităților identificate. | Săptămâna 7 |
| 8 | Exersarea scenariilor complexe de post-exploatare | 1. Simularea post-exploatării – Folosește tehnici de post-exploatare pentru a păstra controlul asupra unui sistem compromis. 2. Colectarea datelor – Colectează informații relevante de pe sistemele compromise, precum parole, fișiere sau date de interes. 3. Menținerea accesului – Folosește tehnici de menținere a accesului pentru a preveni detectarea activităților. | * Eficiența tehnicilor de post-exploatare – Capacitatea de a menține controlul asupra unui sistem compromis. * Documentarea acțiunilor de post-exploatare – Răspunsul și detaliile privind manipularea și protejarea datelor. * Abilitatea de a utiliza instrumente post-exploatare – Utilizarea corectă a instrumentelor specifice post-exploatării. | Săptămâna 8 |
| 9 | Analiza tehnologiilor utilizate pe site-uri web | 1. Identificarea tehnologiilor site-ului – Utilizează instrumente precum Wappalyzer sau BuiltWith pentru a identifica tehnologiile folosite pe un site web. 2. Colectarea informațiilor sensibile – Folosește instrumente de colectare a informațiilor, cum ar fi Nmap sau DirBuster, pentru a identifica fișiere ascunse, directoare și vulnerabilități. 3. Analiza vulnerabilităților site-ului – Explorează posibile puncte de acces, cum ar fi formularele de login sau endpoint-urile API, pentru a identifica posibile vulnerabilități. | * Corectitudinea identificării tehnologiilor – Capacitatea de a identifica corect tehnologiile folosite de site-ul țintă. * Calitatea informațiilor colectate – Abilitatea de a colecta informații relevante și utile despre site-ul țintă. * Identificarea vulnerabilităților – Capacitatea de a găsi vulnerabilități evidente pe baza tehnologiilor identificate și a datelor colectate. | Săptămâna 9 |
| 10 | Exersarea identificării vulnerabilităților OWASP Top 10 | 1. Studiul vulnerabilităților OWASP Top 10 – Învață despre cele mai comune vulnerabilități din aplicațiile web (ex: SQL Injection, Cross-Site Scripting). 2. Simularea unui atac pe aplicația web – Folosește tehnici și instrumente (Burp Suite, SQLmap) pentru a exploata vulnerabilitățile identificate. 3. Documentarea atacurilor – Realizează o documentare detaliată a exploatării vulnerabilităților, inclusiv pașii efectuați și impactul posibil al fiecărui atac. | * Corectitudinea identificării vulnerabilităților – Capacitatea de a identifica corect vulnerabilitățile conform OWASP Top 10. * Succesul atacurilor aplicate – Măsura în care atacurile au reușit să exploateze vulnerabilitățile identificate. * Claritatea și detaliile raportului – Claritatea și exhaustivitatea raportului despre vulnerabilitățile exploatate și impactul lor. | Săptămâna 10 |
| 11 | Analiza scenariilor avansate și aplicarea practică | 1. Studiul atacurilor avansate – Analizează tehnici avansate de hacking, cum ar fi exploatarea vulnerabilităților de tip 0-day sau atacurile de tip MitM (Man-in-the-Middle). 2. Simularea unor scenarii de atac complex – Folosește instrumente de hacking avansate pentru a executa atacuri pe sisteme virtuale izolate. 3. Evaluarea impactului atacurilor – Documentează fiecare scenariul de atac, evidențiind riscurile și impactul asupra securității infrastructurii vizate. | * Complexitatea scenariilor de atac – Măsura în care scenariile de atac simulate sunt avansate și implică tehnici noi. * Succesul implementării atacurilor – Capacitatea de a executa atacuri complexe și de a obține rezultate semnificative. * Calitatea evaluării impactului – Detaliile analizei privind impactul atacurilor și evaluarea riscurilor pentru infrastructura vizată. | Săptămâna 11 |
| 12 | Exersarea identificării vulnerabilităților și soluțiilor | 1. Identificarea vulnerabilităților – Realizează o scanare a unei aplicații web sau rețele pentru a identifica vulnerabilitățile existente. 2. Propunerea soluțiilor de remediere – Oferă soluții și recomandări pentru a corecta vulnerabilitățile identificate, incluzând practici de securitate precum validarea inputurilor și implementarea criptării. 3. Redactarea raportului – Scrie un raport detaliat care include descrierea vulnerabilităților, impactul lor și soluțiile de remediere propuse. | * Corectitudinea identificării vulnerabilităților – Capacitatea de a identifica corect vulnerabilitățile și riscurile asociate acestora. * Relevanța soluțiilor propuse – Calitatea soluțiilor de remediere și adaptabilitatea lor la scenariul concret. * Calitatea raportului de remediere – Claritatea și exhaustivitatea raportului care detaliază vulnerabilitățile și soluțiile propuse. | Săptămâna 12 |
| 13 | Redactarea unui raport detaliat pe baza simulării | 1. Revizuirea studiilor de caz – Analizează studii de caz reale de atacuri de penetrare și tehnici utilizate pentru a le preveni. 2. Simularea unui atac complet de penetrare – Folosește cunoștințele acumulate pentru a simula un test de penetrare complex pe o infrastructură virtuală. 3. Redactarea raportului detaliat – Realizează un raport detaliat care descrie pașii parcurși în testul de penetrare, vulnerabilitățile identificate și soluțiile propuse. | * Completitudinea simulării – Capacitatea de a efectua un test complet de penetrare, acoperind toate etapele și scenariile relevante. * Calitatea analizei studiilor de caz – Capacitatea de a analiza și înțelege studiile de caz și lecțiile învățate din acestea. * Claritatea și detaliile raportului final – Raportul trebuie să fie complet, clar și bine structurat, cu o descriere detaliată a pașilor și concluziilor. | Săptămâna 13 |

1. **SUGESTII METODOLOGICE DE PREDARE-ÎNVĂŢARE-EVALUARE**

Activitatea de predare-învățare la disciplina „*Testare de penetrare și hacking-ul etic*” se desfășoară în cadrul orelor de curs, laborator și activității individuale (activitatea independentă a studentului). Predarea la orele de curs se realizează prin metode care îmbină formele tradiționale de instruire (prelegerea, conversația, exercițiul) cu abordări moderne centrate pe student, care încurajează comunicarea, colaborarea și gândirea critică. Cadrul didactic contribuie la dezvoltarea competențelor funcționale ale studenților, precum: capacitatea de procesare și aplicare a cunoștințelor, sistematizarea și restructurarea informației, gândirea critică, argumentarea logică, luarea deciziilor și participarea activă în procesul educațional.

În cadrul orelor de laborator, studenții sunt implicați în activități practice care reflectă conținutul integral al materiei, având ca scop aprofundarea cunoștințelor și formarea competențelor aplicative. Se utilizează atât metode tradiționale (exerciții, rezolvarea de probleme, lucrări practice, algoritmizare), cât și metode interactive, adaptate specificului domeniului, pentru rezolvarea de situații-problemă și dezvoltarea abilităților comunicaționale (ex. analiza feedback-ului, colaborare în echipă).

Evaluarea în cadrul disciplinei „*Testare de penetrare și hacking-ul etic*” se realizează atât formativ, prin activitatea desfășurată la orele de curs și laborator (inclusiv verificări orale sau scrise, sarcini aplicative și lucrări de atestare), cât și sumativ, prin examenul final. Nota finală este calculată ca medie ponderată: 60% nota semestrială (rezultată din evaluările pe parcurs) și 40% nota obținută la examen. Aceasta reflectă gradul de atingere a competențelor prevăzute în curriculum: volumul cunoștințelor asimilate, capacitatea de aplicare practică și integrarea acestora în contexte variate.

*Partajarea responsabilităților de evaluare a activității studentului la cursul „Testare de penetrare și hacking-ul etic”:*

Titularul de curs are responsabilitatea principală pentru evaluarea cunoștințelor teoretice și practice ale studenților. Acesta organizează și notează testele din cadrul *Testării 1* (la mijlocul semestrului) și *Testării 2* (la sfârșitul semestrului), precum și examenul din sesiunea ordinară și suplimentară. Nota finală este stabilită pe baza performanței studentului la cele patru componente de evaluare: Testarea 1, Testarea 2, Media evaluării curente și Media pentru lucrul individual, precum și a rezultatului obținut la examen.

Asistentul de laborator este responsabil de evaluarea activității practice desfășurate în cadrul lecțiilor de laborator. Acesta colaborează cu titularul de curs și obține acordul acestuia pentru definirea conținutului și structurii lucrărilor de laborator. Evaluarea se realizează prin monitorizarea participării, verificarea sarcinilor realizate, a proiectelor și a lucrărilor prezentate. De asemenea, prin delegare, asistentul evaluează componentele *Media evaluării curente* și *Media pentru lucrul individual*, introducând notele corespunzătoare în registrul electronic al grupei academice (crd.usm.md) la sfârșitul semestrului.

În cazul susținerii examenului în sesiunea suplimentară, titularul de curs și asistentul de laborator vor conveni suplimentar asupra responsabilităților privind evaluarea lucrărilor de laborator, precum și asupra notării componentelor *Media evaluării curente* și *Media pentru lucrul individual*.

1. **BIBLIOGRAFIE RECOMANDATĂ**
2. Robert Shimonski, Penetration Testing For Dummies, Wiley, 2023.
3. Patrick Engebretson, The Basics of Hacking and Penetration Testing: Ethical Hacking and Penetration Testing Made Easy, Elsevier, 2024.
4. Matthew Hickey, Jennifer Arcuri, Hands-On Hacking: Become an Expert, Packt Publishing, 2024.
5. Georgia Weidman, Penetration Testing: A Hands-On Introduction to Hacking, No Starch Press, 2023.
6. Toby Kohlenberg, Practical Ethical Hacking: A Hands-On Introduction to Testing & Securing Your Systems, Wiley, 2023.
7. Ravi Das, Penetration Testing: A Complete Step-by-Step Guide, Packt Publishing, 2024.
8. Oscar De La Fuente, Cybersecurity and Penetration Testing for Beginners, Apress, 2023.
9. Glen E. Clarke, Web Application Security: Exploitation and Countermeasures for Ethical Hackers, O'Reilly Media, 2023.
10. Stuart McClure, Saumil Shah, Hacking Exposed: Network Security Secrets & Solutions, McGraw-Hill Education, 2023
11. Robert W. Beggs, Mastering Kali Linux for Advanced Penetration Testing, Packt Publishing, 2023.
12. Jon Erickson, Hacking: The Art of Exploitation, No Starch Press, 2024.
13. Chris Anley, John Heasman, Felix Lindner, Gerardo Richarte, The Shellcoder's Handbook: Discovering and Exploiting Security Holes, Wiley, 2024.
14. Wil Allsopp, Advanced Penetration Testing: Hacking the World's Most Secure Networks, Packt Publishing, 2024.
15. Christopher Hadnagy, Social Engineering: The Art of Human Hacking, Wiley, 2023.