Academia Navală „Mircea cel Bătrân”
Facultatea de Inginerie Marină
Departamentul Sisteme Electromecanice Navale

Laboratorul
CYBERSECURITY

1. DESTINAȚIE

Laboratorul Cybersecurity asigură desfășurarea activităților practice la disciplinele *Programarea calculatoarelor si Limbaje de programare* și *Informatică aplicată*.

2. OBIECTIV GENERAL

Laboratorul Cybersecurity permite instruirea studenților/masteranzilor în conștientizarea, prevenirea, identificarea, clasificarea, contracararea posibilelor atacuri cibernetice, prin oferirea de soluții viabile rapide și, totodată, oferă un mediu colaborativ si competitiv de antrenare, testare și diseminare a informațiilor, urmare a competițiilor purtate între diverse echipe, conform indicațiilor instructorului. Fiind bazată pe CLOUD, platforma permite controlul unei game largi de resurse de calcul, stocare și rețea în cadrul unui centru de date. Infrastructura Open Source Cloud Computing este împărțit în servicii pentru a permite conectarea și lucrul cu componente ale bibliotecii, în funcție de nevoi.

Laboratorul Cyber include o bibliotecă de sisteme pre-construite, șabloane și scenarii de atac si are cel puțin 200 de imagini pre-construite ale mașinilor virtuale gata de a fi utilizate individual sau în scenariile de atac-apărare sau de antrenament. Mașinile virtuale includ, în mod specific, dar fără limita, diferite stații de lucru și servere Windows și Linux, cu diferite niveluri de vulnerabilități deja încorporate.

Laboratorul Cyber oferă cel puțin 20 de scenarii de antrenament pre-construite, cu niveluri diferite de dificultate și atacuri în mai multe etape, de cel puțin 6 ore de

antrenament fiecare. Cel puțin câteva scenarii acoperă vulnerabilitățile sistemelor de operare populare sau ale software-ului, cum ar fi: Windows, Linux, Active Directory, etc.

3. OBIECTIVE SPECIFICE

Laboratorul Cyber permite simularea:

- Diferite scenarii de atac de nivel (level attack scenarios), de la cele simple până la cele avansate APT (advanced persistent threat);
- Trebuie să susțină scenarii pentru participanți cu background diferit (e.g., ethical hacker, Cyber defenders, etc.) și diferite niveluri de expertiză (începători, intermediari, practicieni avansați, etc.);
- Atac de tip zero-day malware, inclusiv ransomware, în diferite sisteme de operare;
- Atac de tip Brute-force;
- Data leakage/exfiltration;
- Vulnerabilități și exploit-uri din partea clientului și a serverului.
- Atacuri de tip Spams, phishing, and spear-phishing;
- Domenii și site-uri rău intenționate, inclusiv site-uri de phishing
- Atacuri de tip Denial-of-Service cu multiple variante (DDoS, RDoS, DRDoS)

4. DOTARE

- 20 stații de lucru individuale dotate cu calculatoare de ultima generație cu acces la platforma cybersecurity CDeX si la Internet;
- 2 Videoproiectoare + ecrane de proiecție;
- software cu licență si open-source
- 2 Table interactive

5. LUCRĂRI DE LABORATOR EFECTUATE

- Exerciții cu scenarii de tip Atac-Apărare (Attack-defence scenario), cunoscute sub numele de "exerciții echipă roșu- echipă albastru" (red team-blue team exercises");
- Diferite scenarii/exerciții de răspuns la incidente și de apărare cibernetică (Cyber Defence) pentru instruirea persoanelor care răspund la incidente, inclusiv în domenii de apărare cibernetică (Cyber Defence), cum ar fi analiza amenințărilor (threat analysis), răspunsul la incidente (incident response), criminalistica digitală (digital forensics), etc.;
- Exerciții de "capturarea steagului" (Capture the flag);
- Sesiuni de instruire, cursuri, laboratoare și prelegeri;

- Facilități Testing grounds. Soluțiile (hardware, software etc.) sunt testate pentru a vedea dacă funcționează corect. Laboratorul Cyber trebuie să ofere un mediu sigur pentru testarea instrumentelor COTS (software care rulează pe Linux/Windows, de preferință și dispozitive de rețea), artefacte și să colecteze IoCs. Testarea COTS implică o cantitate mare de teste a modului în care sistemul COTS comunică cu alte sisteme și surse de date prin interfețele sale. Indicatorii de compromis (IOCs) sunt diferite tipuri de date de securitate cibernetică care pot alerta organizațiile de iminența atacului rețelei lor, încălcări ale securității, infecții malware și incidente de securitate.
- Conectarea componentelor fizice, cum ar fi Routere / switch-uri, dar și a altor componente;
- Incident Management Plans(IMP), Evacuation Plans (EP) si Bussiness Continuity Plans(BCP) – strategii de gestionare si revenire după un atac terorist.
- SCaN – See, Check and Notify. Maximizarea siguranței si securității resurselor.
- Simularea infrastructurilor personalizate (real life like);

6. 6.Direcții de cercetare:

- securitatea cibernetică a sistemelor și rețelelor informatice, digital forensic, cyber diplomacy, protecția infrastructurilor critice;
- noi tehnologii informatice (blockchain), cloud computing, inteligență artificială (machine learning, deep learning);
- managementul și analiza avansată a datelor de mari dimensiuni (BigData);