Curs 1 - Concepte avansate de cyber-security in Retele

Livrare: Hibrid (in clasa/ on-line) **Nivel:** Avansat **Public tinta:** studenti in cadrul ciclului de licenta, de preferat Automatica si Calculatoare, Electronica si Telecomunicatii, avand cunostinte de baza de retelistica si/sau securitate	**Durata** – 35 de ore (10 ore de pregatire sincrona/25 ore de pregatire asincrona) **Continut:** • 3 module de curs • Material pe platforma de e-learning • activitati interactive • 1 evaluare finala practica	**Numar cursanti**: 20-70 de studenti/grupa **Cunostinte anterioare:** cunostinte de Retelistica, tehnologie IP

1. Cui ii este adresat

Studenţi la Automatică şi Calculatoare sau Electronica şi Telecomunicaţii, cu cunoştinţe de bază în reţelistică (LAN, WAN, protocoale IP) si interesate să urmeze o carieră în securitate cibernetică, infrastructuri de telecomunicaţii, inginerie de reţea sau administrare reţea sau care doresc să dobândească competenţe practice referitoare la securizarea reţelelor de comunicaţii, atât pe secţiunea wired (cablat) cât şi wireless.

2. Cunostinte anterioare necesare pentru participarea la curs

- Cunostinte de baza in Telecomunicatii si/sau Securitate (ex: TCP/IP, protocoale IP, LAN, WAN)
- Familiaritate cu dispozitive de retea (switch, router) si medii de laborator/simulare (ex: Cisco, Juniper, Palo Alto, Fortinet, Nokia, etc)

3. Obiectivele cursului

Cursul are ca scop familiarizarea studenţilor cu conceptele aplicate de securitate în mediile de telecomunicaţii. Participanţii vor învăţa despre securitatea reţelelor LAN/WLAN, protecţia switch urilor şi a accesului wireless, malware, atacuri asupra reţelelor, vulnerabilităţi legate de protocoalele TCP/UDP, criptografie, liste de control de acces (ACL) standard şi extinse, NAT, VPN şi IPsec. Cursul include atât noţiuni teoretice, cât şi laboratoare practice, astfel încât studenţii să poată aplica securizarea infrastructurilor de comunicaţii în mod concret.

La finalul cursului, studenţii vor putea:

- Identifica şi analiza ameninţările de securitate într-o reţea LAN/WLAN de telecomunicaţii.
- Configura măsuri de securitate la nivel de switch şi wireless, adaptate pentru infrastructuri reale.
- Evalua vulnerabilităţile protocoalelor TCP şi UDP şi implementa măsuri adecvate de protecţie.
- Aplică concepte de criptografie pentru protejarea comunicaţiilor de date.
- Configura ACL standard şi extinse pentru filtrare de trafic, NAT pentru izolare şi VPN/IPsec pentru conectivitate securizată în reţele de telecomunicaţii.
- Proiecta şi implementa o mică infrastructură de telecomunicaţii securizată, integrând elementele studiate.

4. Echipamente necesare din partea studentilor

- Laptop personal

5. Descrierea cursului

Cursul va acoperi, dar nu se va limita la următoarele teme:

- Securitate LAN – principii de bază pentru segmentarea rețelei, izolarea traficului, principiile de securitate în rețele locale.
- Configurări de securitate pe switch – cum se aplică securitatea la nivelul switch ului: port security, DHCP snooping, BPDU guard, configurarea accesului administrativ.
- Securitate pe WLAN – amenințări tipice pentru rețele wireless (ex: rogue AP, evil twin), metode de criptare (WPA2/3), autentificare în rețea wireless.
- Malware și atacuri asupra rețelelor – tipuri de malware (viruși, troieni, ransomware), tehnici de atac asupra rețelei (scanning, spoofing, MitM), vectori de atac și măsuri de protecție.
- Vulnerabilități TCP și UDP – analiza securității protocoalelor de transport, atacuri de tip SYN flood, UDP amplification, cum pot fi mitigare.
- Criptografie – concepte de criptare simetrică/asimetrică, hashing, semnături digitale, securizarea comunicațiilor în rețea.
- ACL standard și extins – cum se configurează liste de control de acces pentru filtru trafic, diferențele între ACL standard și extinsă, aplicații în rețele de telecomunicații.
- NAT (Network Address Translation) – rolul NAT în securitatea rețelei, tipuri de NAT, cum contribuie la izolare și scalabilitate.
- VPN și IPsec – cum se realizează conexiuni securizate site to site și remote, arhitectura IPsec, componente, protocoale, scenarii aplicate în telecomunicații.

6. Evaluare finală – criterii și modalități

Modalități de evaluare

Model1:

- **Evaluare continuă (25%)** – participare, implicare în interactiunile de grup
- **Evaluare teoretica (25%)**
- **Mini-proiect final (50%)** – proiect practic de securizare a unei mici infrastructuri de telecomunicatii

Model 2:

- Prin parcurgerea unui Test grila folosind facilitatile ecosistemului M365 disponibile la nivel institutional (ex. MS Forms, MS Teams Assignment);