



# PORTOFOLIU DIDACTIC

## Didactica Domeniului

[REDACTED] Larisa [REDACTED]

Facultatea de Matematică și Informatică  
Masterul de “Security and Applied Logic” (SAL)  
Anul II – 2022/2023

Ianuarie 2023

Universitatea din București – Modulul Psihopedagogic Nivelul II

## **Cuprins:**

Fișă de Evidență a Prezențelor .....	2
Temă Finală: Proiectare Curs Universitar – Securitatea Rețelelor .....	3
<i>Fișa Disciplinei</i> .....	3
<i>Curs 3: Mitigating Threats (Contracararea Amenințărilor)</i> .....	11
3.0 Introduction.....	11
3.1 Defending the Network .....	11
3.2 Network Security Policies .....	16
3.3 Security Tools, Platforms, and Services .....	21
3.4 Mitigating Common Network Attacks .....	28
3.5 Cisco Network Foundation Protection Framework .....	34
<i>Laborator 2</i> .....	40
Bonus: Proiect Educațional – „Și școala poate fi frumoasă!” .....	45
Bonus: Examen de luat acasă (Temă Seminar).....	52
Bonus: Proiect Didactic (Temă Seminar).....	53
Feedback Didactica Domeniului.....	70

## Fişă de Evidență a Prezentelor

Evidența completă a prezențelor la cursul de „*Didactica Domeniului*” poate fi găsită accesând acest [link](#).

1	Nume & Prenume	Facultate & Master	S1	S2	S3	S4	S5	S6	S7	S8	S9	S10	S11	S12	S13	Total
[REDACTED]		Informatică, AI	1	2	4	0	4	0	0	0	2	2	2	0	2	19
		Informatică, SAL	1	2	4	2	4	2	4	2	4	2	2	4	0	33
		Informatica, BTDS	1	0	0	0	0	0	0	0	0	0	0	4	0	5

# Temă Finală: Proiectare Curs Universitar – Securitatea Rețelelor

## Fișa Disciplinei

### 1. Date despre Program

1.1 Instituția de învățământ superior	UNIVERSITATEA DIN BUCUREȘTI
1.2 Facultatea/Departamentul	FACULTATEA DE MATEMATICĂ ȘI INFORMATICĂ
1.3 Departamentul	DEPARTAMENTUL DE INFORMATICĂ
1.4 Domeniul de studii	INFORMATICĂ
1.5 Ciclul de studii	LICENȚĂ
1.6 Programul de studii/Calificarea	INFORMATICĂ

### 2. Date despre Disciplină

2.1 Denumirea disciplinei				SECURITATEA REȚELELOR			
2.2 Titularul activităților de curs				[REDACTED]			
2.3 Titularul activităților de laborator							
2.4 Anul de studiu	2	2.5 Semestrul	2	2.6 Tipul de evaluare	EXAMEN	2.7 Regimul disciplinei	OBLIGATORIU

### 3. Timpul total estimat (ore pe semestru al activităților didactice)

3.1 Număr de ore pe săptămână	4	din care: 3.2 curs	2	3.3 laborator	2
3.4 Total ore din planul de învățământ	56	din care: 3.5 curs	28	3.6 seminar	28
Distribuția fondului de timp					ore
Studiul după manual, suport de curs, bibliografie și notițe					30
Documentare suplimentară în bibliotecă, pe platformele electronice de specialitate și pe teren					10
Pregătire teme, referate, portofolii și eseuri					20
Tutoriat					14
Examinări					20
Alte activități...					-
3.7 Total ore studiu individual					94
3.8 Total ore pe semestru (3.4. + 3.7)					150
3.9. Numărul de credite					6

### 4. Precondiții (acolo unde este cazul)

4.1 de curriculum	Rețele de calculatoare, Arhitectura rețelor
4.2 de competențe	Cunoștințe de limbă engleză; Nivelul fizic, legătură de date, rețea, transport, aplicație – cunoștințe de bază; Cunoștințe de bază securitate; Routers, Switches, LANs, Ipv4 –

	cunoștințe de bază
--	--------------------

## 5. Condiții (acolo unde este cazul)

5.1 de desfășurare a cursului	Sală (Amfiteatru) cu dotări multimedia (calculator, videoproiector) și tablă Conexiune la internet Acces la bibliografia recomandată
5.2 de desfășurare a laboratorului	Laborator cu dotări multimedia (videoproiector și calculatoare) și tablă Calculatoare echipate cu „Cisco Packet Tracer”

## 6. Competențe Specifice Acumulate

Competențe profesionale	<p>C1: Identificarea, definirea și utilizarea conceptelor, modelelor și noțiunilor care țin de securitatea rețelelor.</p> <p>C2: Înțelegerea modului de utilizare al aplicației Cisco Packet Tracer.</p> <p>C3: Cunoașterea practică a elementelor ce țin de rețelistică și capacitatea de a le configura într-o manieră care să respecte standardele de securitate moderne.</p>
Competențe transversale	<p>CT1: Aplicarea regulilor de muncă organizată și eficientă, a unor atitudini responsabile față de domeniul didactic-științific, pentru valorificarea creativă a propriului potențial, cu respectarea principiilor și a normelor de etică profesională.</p> <p>CT2: Desfășurarea eficientă a activităților organizate într-un grup inter-disciplinar și dezvoltarea capacităților empatice de comunicare inter-personală, de relaționare și colaborare cu grupuri diverse.</p> <p>CT3: Utilizarea unor metode și tehnici eficiente de învățare, informare, cercetare și dezvoltare a capacităților de valorificare a cunoștințelor, de adaptare la cerințele unei societăți dinamice și de comunicare în limba română și într-o limbă de circulație internațională (engleză).</p> <p>CT4: Promovarea valorilor asociate realizării unui învățământ de calitate, în conformitate cu politicile educaționale interne și în acord cu cele elaborate și popularizate la nivel european, pe baza cunoașterii specificității domeniului educațional european și a interculturalității.</p> <p>CT5: Preocuparea pentru perfecționarea rezultatelor profesionale prin implicarea în activitățile desfășurate. Utilizarea metodelor și tehnicilor eficiente de învățare pe tot parcursul vieții, în vederea formării și dezvoltării profesionale continue.</p>

## 7. Obiectivele Disciplinei (reieșind din grila competențelor specifice acumulate)

7.1 Obiectivul general al disciplinei	Familiarizarea studenților cu conceptele și tehnologiile utilizate în cadrul securizării rețelelor. Cursul este menit să fie la un nivel intermediar spre avansat în acest domeniu.
7.2 Obiectivele specifice	Studenții care finalizează cu succes aceasta disciplină vor fi capabili: -să înțeleagă concepte avansate de rețelistică; -să înțeleagă concepte avansate de securitate; -să dezvolte o înțelegere aprofundată a domeniului de securitate a rețelelor; -să proiecteze, implementeze și să ofere suport dispozitivelor și datelor dintr-o rețea, într-o manieră care să respecte standardele de securitate din industrie; -să dobândească gândire critică și abilități de rezolvare a problemelor folosind echipamente reale și Cisco Packet Tracer; -să obțină abilități recunoscute în industrie, aliniate cu cadrul de securitate cibernetică a Institutului Național pentru Standarde și Tehnologie (NIST).

## 8. Conținuturi:

8.1 Curs	Metode de Predare	Observații
1. Securizarea Rețelelor (Securing Networks)	Expunere sistematică, prele-gere, dialog, conversație, e-xemplul, discuții pe studii de caz, analiză critică	Rețele ca ținte de atac, motive pentru studierea acestui modul, vectori de atac, pierderea de date, prezentare generală a topologiei rețelei
2. Amenințări în Rețele (Network Threats)	Expunere sistematică, prele-gere, dialog, conversație, e-xemplul, discuții pe studii de caz, analiză critică	Amenințări, vulnerabilități, riscuri, vectori de amenințare, malware, tipuri de malware, tipuri comune de atac pentru rețele, atacuri avansate (DoS, buffer overflow, evasion methods...)
3. Contracararea Amenințărilor	Expunere sistematică, prele-gere, dialog, conversație, e-xemplul, discuții pe studii de caz, analiză critică	CIA, politici de securitate în rețele, instrumente/aplicații, platforme și servicii care țin de securitate, contracarare atacuri din rețele (discutate în cursul precedent), NFP framework
4. Acces Securizat la Dispozitive din Rețea	Expunere sistematică, prele-gere, dialog, conversație, e-xemplul,	Securizarea router-ului de la marginea rețelei, configurarea securității pentru accesul

	discuții pe studii de caz, analiză critică	administrativ, configurarea securității pentru autentificarea virtuală, configurare ssh
5. Atribuirea de roluri administrative	Expunere sistematică, prele-gere, dialog, conversație, e-xemplul, discuții pe studii de caz, analiză critică	Configurarea nivelurilor de privilegii, role-based CLI
6. Monitorizarea și Gestionarea Dispozitive-lor din Rețele – I	Expunere sistematică, prele-gere, dialog, conversație, e-xemplul, discuții pe studii de caz, analiză critică	Configurarea Cisco IOS, blocarea unui router utilizând AutoSecure, autentificarea prin protocolul de rutare, management și raportare
7. Monitorizarea și Gestionarea Dispozitive-lor din Rețele – II, AAA	Expunere sistematică, prele-gere, dialog, conversație, e-xemplul, discuții pe studii de caz, analiză critică	Securizarea rețelei folosind Syslog, configurare NTP, SNMP configurare, configurare AAA locală, caracteristici și protocoale AAA bazate pe server, TACACS+, RADIUS
8. ACL	Expunere sistematică, prele-gere, dialog, conversație, e-xemplul, discuții pe studii de caz, analiză critică	Filtrare pachete, reguli ACL, detalii despre Wildcard, configurare, modificare și implementare ACL-uri, prevenția atacurilor folosind ACL-uri
9. Firewall	Expunere sistematică, prele-gere, dialog, conversație, e-xemplul, discuții pe studii de caz, analiză critică	Securizarea rețelelor folosind firewall-uri, ZPF
10. Prevenirea Intruziunilor	Expunere sistematică, prele-gere, dialog, conversație, e-xemplul, discuții pe studii de caz, analiză critică	Tehnologii IPS, IDS vs IPS, implementare IPS în rețele și operații, IPS în Cisco IPS, analiză de porturi Cisco, SPAN, Cisco Snort IPS, IPS semnături
11. Securitatea endpoint-urilor și Layer-ului 2	Expunere sistematică, prele-gere, dialog, conversație, e-xemplul, discuții pe studii de caz, analiză critică	Securitatea endpoint-urilor, autentificare 802.1X, amenințări la nivelul 2 al rețelelor (layer 2), MAC, STP, ARP, atacuri specifice
12. VPN	Expunere sistematică, prele-gere, dialog, conversație, e-xemplul,	VPN noțiuni de bază, VPN topologii, IPsec noțiuni de bază și protocoale, schimb chei pe

	discuții pe studii de caz, analiză critică	internet, ISAKMP, Crypto Map, politici de securitate
13. Criptografie	Expunere sistematică, prele-gere, dialog, conversație, e-xemplul, discuții pe studii de caz, analiză critică	Criptografie, criptologie, criptanaliză, integritate și autenticitate, managementul cheilor de acces, confidențialitate, chei publice vs chei private, semnături digitale, certificate, PKI
14. ASA	Expunere sistematică, prele-gere, dialog, conversație, e-xemplul, discuții pe studii de caz, analiză critică	ASA 5506-X cu FirePOWER, ACL-uri ASA, NAT servicii cu ASA, ASA Firewall configurație
<b>8.2 Laborator</b>	<b>Metode de Predare</b>	<b>Observații</b>
1. Lucrul cu Ipv4, introducere în aplicația Cisco Packet Tracer	Exercițiul, activitate practică dirijată, explicație, dialog, problematizare, algoritmizare, conversație, exemple	Transformare din bază decimală în bază binară, network address, broadcast address, range addresses, subnet mask, wildcard, default gateway, DNS, înregistrare conturilor în aplicația și pe platforma Cisco, scurtă introducere a aplicației
2. Configurare host PC, switch 2960 și router 2911	Exercițiul, activitate practică dirijată, explicație, dialog, problematizare, algoritmizare, conversație, exemple, prele-gere	Pași de configurare a dispozitivelor, sintaxă specifică pentru configurare, verificare conectivitate (ping și ssh), cabluri și utilizarea lor, stiva OSI
3. Configurare serială între mai multe routere, protocolul OSPF, configurare server	Exercițiul, activitate practică dirijată, explicație, dialog, problematizare, algoritmizare, conversație, exemple, prele-gere	Numărul de switches recomandat pentru o topologie, configurare routere pentru legătura serială, configurare server, verificare conectivitate (e-mail, web browser, ping, ssh)
4. DNS pentru Switch și Router, FTP	Exercițiul, activitate practică dirijată, explicație, dialog, problematizare, algoritmizare, conversație, exemple, prele-gere	Sintaxă configurare DNS pentru echipamentele din rețea, configurare server cu FTP, verificare FTP în echipamente
5. Configurare rețea cap-coadă	Exercițiul	-



6. Configurare AAA și Wi-Fi WRT300N	Exercițiul, activitate practică dirijată, explicație, dialog, problematizare, algoritmizare, conversație, exemple	Pași configurare echipament Wi-Fi WRT300N, configurare AAA pentru server
7. Utilizare Sniffer, configurare NTP și DHCP server, switch și router	Exercițiul, activitate practică dirijată, explicație, dialog, problematizare, algoritmizare, conversație, exemple	Configurare NTP și DHCP în server, sintaxă specială de configurare NTP pentru switch și router, utilizare sniffer și observarea pachetelor transmise în cadrul topologiei, asignare automată IP-uri în dispozitive folosind DHCP
8. Reguli suplimentare de securitate switch-uri și lucrul de bază cu ACL-uri	Exercițiul, activitate practică dirijată, explicație, dialog, problematizare, algoritmizare, conversație, exemple	Definire proprie vlan-uri, switchport security, spanning tree, encapsulare dot1Q, ACL simplu router pentru ssh
9. ACL-uri și encapsulare PPP pentru route-re	Exercițiul, activitate practică dirijată, explicație, dialog, problematizare, algoritmizare, conversație, exemple	Access-list / access-class pentru IP-uri singulare sau pentru o rețea întreagă (allow / block), encapsulare ppp pentru routere și auth chap
10. Rutare dinamică pe routere, ACL-uri	Exercițiul, activitate practică dirijată, explicație	Configurare topologie cap-coadă, împreună cu rutarea dinamică și exerciții ACL, access-group
11. Rutare statică, zone de securitate și configurarea protocoalelor acceptate	Exercițiul, activitate practică dirijată, explicație, dialog, problematizare, algoritmizare, conversație, exemple	License boot module c2900, zone security, class-map type, policy-map type, zone-pair, service-policy
12. VPN prin interfață	Exercițiul, activitate practică dirijată, explicație, dialog, problematizare, algoritmizare, conversație, exemple	VPN simplu cu un singur vs mai multe routere între
13. VPN prin GRE	Exercițiul, activitate practică dirijată, explicație, dialog, problematizare, algoritmizare, conversație, exemple	VPN prin GRE cu un singur vs mai multe routere între
14. Colocviu	Colocviu / Test de laborator	Colocviu (practic / test de laborator) din toate

		informațiile predate în cadrul laboratorului. Se va realiza pe platforma CiscoPkT.
<b>Bibliografie:</b> - Stallings, W. (2007). <i>Cryptography and Network Security Principles and Practices, Fourth Edition</i> . Retrieved from <a href="http://www.inf.ufsc.br/~bosco.sobral/ensino/ine5680/material-cripto-seg/2014-1/Stallings/Stallings_Cryptography_and_Network_Security.pdf">http://www.inf.ufsc.br/~bosco.sobral/ensino/ine5680/material-cripto-seg/2014-1/Stallings/Stallings_Cryptography_and_Network_Security.pdf</a> - Stallings, W., Columbus, B., New, I., San, Y., Upper, F., River, S., ... Tokyo, T. (n.d.). <i>NETWORK SECURITY ESSENTIALS: APPLICATIONS AND STANDARDS FOURTH EDITION</i> . Retrieved from <a href="https://www.skylineuniversity.ac.ae/pdf/computer/Network%20security%20essentials%20%20applications%20and%20standards%20-%2017376.pdf">https://www.skylineuniversity.ac.ae/pdf/computer/Network%20security%20essentials%20%20applications%20and%20standards%20-%2017376.pdf</a> - Network Security. (2021, March 3). Retrieved January 6, 2023, from Networking Academy website: <a href="https://www.netacad.com/courses/cybersecurity/network-security">https://www.netacad.com/courses/cybersecurity/network-security</a> - Tanenbaum, A. (n.d.). <i>Rețele de calculatoare EDITIA PATRUA</i> . Retrieved from <a href="https://staff.fmi.uvt.ro/~stelian.mihalas/com_net/download/courses/retcalc_ed_4.pdf">https://staff.fmi.uvt.ro/~stelian.mihalas/com_net/download/courses/retcalc_ed_4.pdf</a>		

**9. Coroborarea conținuturilor disciplinei cu așteptările reprezentanților comunității epistemice, asociațiilor profesionale și angajatori reprezentativi din domeniul aferent programului:**

<ul style="list-style-type: none"> <li>• Disciplina „Securitatea Rețelor” face parte din planul de învățământ aprobat de MEN și este esențială pentru dezvoltarea competențelor dobândite în vederea viitoarei cariere didactice.</li> <li>• Conținuturile disciplinei acoperă un segment foarte important al formării profesionale la nivel de licență, fiind în acord cu așteptările comunității specialiștilor din domeniul securității informatice și ale angajatorilor care solicită specialiști în acest domeniu profesional.</li> <li>• Cursul respectă <i>IEEE and ACM Curricula Recommendations</i> for Computer Science studies.</li> </ul>
---

**10. Evaluare:**

Tip activitate	10.1 Criterii de evaluare	10.2 Metode de evaluare	10.3 Pondere din nota finală
Curs	Înșușirea și înțelegerea corectă a problematicei tratate la curs.	Scrisă: test grilă pe platforma Cisco în urma căreia vor obține o certificare de specialist în securi-	40%

		tatea rețelelor, care nu are termen de expirare și este recunoscută în domeniu.	
Laborator	Rezolvarea sarcinilor de laborator. Abilitatea de a rezolva probleme practice specifice cursului, direct la calculator și în timp limitat (colocviu), fără acces la resurse multimedia. Abilitatea de a proiecta și a înțelege o rețea securizată.	Continuă: pe parcursul semestrului – rezolvarea cerințelor în cadrul laboratorului.  Practică: colocviu (test de laborator)	1 punct bonus la colocviu, pentru activitate continuă pe parcursul semestrului.  60%
<b>10.4 Standard minim de performanță</b>			
Nota minimă de promovare este 5 la fiecare dintre activitățile prezentate anterior: test grilă, colocviu.			

Data Completării

Semnătura titularului de Curs

Semnătura titularului de Laborator

X

X

X

Data avizării în departament

Semnătura directorului de departament

X

X

## Curs 3: Mitigating Threats (Contracararea Amenințărilor)

### 3.0 Introduction

#### 3.0.1 - Motivatie

Apărarea rețelei este treaba unui profesionist în securitate.

- *Cum poți să fie informat cu privire la actualul climat de Securitate ?*
- *Ce organizații pot ajuta să fim informați cu privire la cele mai recente riscuri și instrumente ?*
- *Ce legătură au ceapa și anghinarea cu securitatea ?*

#### 3.0.2 - Obiective

Cunoasterea instrumentelor și procedurilor pentru a atenua efectele cauzate de malware și atacurile comune de rețea.

Topic Title	Topic Objective
<b>Defending the Network</b>	Descrierea metodelor și resurselor pentru protejarea rețelei.
<b>Network Security Policies</b>	Explicarea mai multor tipuri de politici de securitate a rețelei.
<b>Secure the Network</b>	Cunoasterea scopului platformelor de securitate.
<b>Mitigating Common Network Attacks</b>	Descrierea tehnicilor utilizate pentru a atenua atacurile comune de rețea.
<b>Cisco Network Foundation Protection Framework</b>	Explicarea modului de securizare a celor trei zone funcționale ale routerelor și comutatoarelor Cisco.

### 3.1 Defending the Network

#### 3.1.1 - Network Security Professionals

Organizațiile se confruntă cu pierderi de productivitate atunci când rețelele lor sunt lente sau nu răspund. Obiectivele de afaceri și profiturile sunt afectate negativ de pierderea și coruperea datelor. Prin urmare, din perspectiva afacerilor, este necesar să se minimizeze efectele hackerilor cu intenții rele.

Profesioniștii în securitatea rețelei sunt responsabili de menținerea asigurării datelor pentru o organizație și de asigurarea integrității și confidențialității informațiilor. În mod ironic, hacking-ul a avut efectul neintenționat de a crea o cerere mare de profesioniști în securitatea

rețelei. Ca urmare a creșterii exploatărilor hackerilor, a sofisticării instrumentelor pentru hackeri și din cauza legislației guvernamentale, soluțiile de securitate a rețelei s-au dezvoltat rapid în anii 1990, creând noi oportunități de muncă în domeniul securității rețelei.

Rolurile de muncă de specialist în securitate în cadrul unei întreprinderi includ Chief Information Officer (CIO), Chief Information Security Officer (CISO), Manager Operațiuni de securitate (SecOps), Chief Security Officer (CSO), Manager de securitate și Inginer de securitate a rețelei. Indiferent de titlurile postului, profesioniștii în securitatea rețelei trebuie să fie întotdeauna cu un pas înaintea hackerilor:

- *Ei trebuie să-și îmbunătățească în mod constant setul de abilități pentru a fi la curent cu cele mai recente amenințări.*
- *Ei trebuie să participe la cursuri și ateliere de lucru.*
- *Ei trebuie să se aboneze la fluxuri în timp real privind amenințările.*
- *Ei trebuie să examineze site-urile web de securitate în fiecare zi.*
- *Aceștia trebuie să păstreze familiaritatea cu organizațiile de securitate a rețelei. Aceste organizații au adesea cele mai recente informații despre amenințări și vulnerabilități.*

Organizația Cyber Security Education descrie o serie de cariere în domeniul securității cibernetice și oferă resurse care pot ajuta în pregătirea pentru acele cariere.

Notă: În comparație cu alte profesii din tehnologie, securitatea rețelei are o curbă de învățare foarte abruptă și necesită un angajament pentru dezvoltarea profesională continuă.

### 3.1.2 - Network Intelligence Communities

Pentru a proteja eficient o rețea, profesioniștii în securitate trebuie să fie informați cu privire la amenințări și vulnerabilități pe măsură ce acestea evoluează. Există multe organizații de securitate care oferă informații despre rețea. Ei oferă resurse, ateliere și conferințe pentru a ajuta profesioniștii în securitate. Aceste organizații au adesea cele mai recente informații despre amenințări și vulnerabilități.

Mai jos sunt enumerate câteva organizații importante de securitate a rețelei.

**SANS** - Resursele Institutului SysAdmin, Audit, Network, Security (SANS) sunt în mare parte gratuite la cerere și includ:

- *Internet Storm Center - popularul sistem de avertizare timpurie pe internet*

- *NewsBites*, rezumatul săptămânal al articolelor de știri despre securitatea computerelor.
- *@RISK*, rezumatul săptămânal al vectorilor de atac nou descoperiți, vulnerabilități cu exploit-uri active și explicații despre cum au funcționat atacurile recente
- *Alerte de securitate flash*
- *Sala de lectură* - peste 1.200 de lucrări de cercetare originale premiate.
- *SANS* dezvoltă și cursuri de securitate.

**Mitre** - Mitre Corporation menține o listă de vulnerabilități și expuneri comune (CVE) utilizate de organizațiile de securitate proeminente, ceea ce le face mai ușor să partajeze date. CVE servește ca un dicționar de nume comune (adică, identificatori CVE) pentru vulnerabilitățile cunoscute de securitate cibernetică.

**FIRST** - Forum of Incident Response and Security Teams (FIRST) este o organizație de securitate care reunește o varietate de echipe de răspuns la incidente de securitate informatică din organizații guvernamentale, comerciale și educaționale pentru a promova cooperarea și coordonarea în schimbul de informații, prevenirea incidentelor și reacția rapidă.

**SecurityNewsWire** - Un portal de știri de securitate care reunește cele mai recente știri de ultimă oră referitoare la alerte, exploatare și vulnerabilități.

**(ISC)<sup>2</sup>** - Consorțiul Internațional de Certificare a Securității Sistemelor Informaționale(ISC<sup>2</sup>) oferă produse educaționale neutre și servicii de carieră pentru mai mult de 75.000 de profesioniști din industrie din peste 135 de țări.

**CIS** - Centrul pentru Securitate pe Internet (CIS) este un punct central pentru prevenirea, protecția, răspunsul și recuperarea amenințărilor cibernetice pentru guvernele de stat, locale, tribale și teritoriale (SLTT) prin Centrul Multi-State de Partajare și Analiză a Informațiilor (MS-ISAC). MS-ISAC oferă avertismente și consiliere 24x7 pentru amenințări cibernetice, identificarea vulnerabilităților și atenuarea și răspunsul la incidente.

Pentru a rămâne eficient, un profesionist în securitatea rețelei trebuie să:

Fie la curent cu cele mai recente amenințări – Aceasta activitate include abonarea la fluxuri în timp real referitoare la amenințări, consultarea periodică a site-urilor web legate de securitate, urmărirea blogurilor și podcast-urilor de securitate și multe altele.

Îmbunătățirea continua a abilităților - Aceasta include participarea la cursuri, ateliere și conferințe legate de securitate.

Notă: Securitatea rețelei are o curbă de învățare foarte abruptă și necesită un angajament pentru dezvoltarea profesională continuă.

### 3.1.3 - Network Security Certifications

Sute de mii de locuri de muncă legate de securitatea rețelei rămân neocupate în fiecare an. Cererea de profesioniști în securitatea rețelei depășește cu mult numărul de solicitanți calificați. Obținerea certificărilor recunoscute de securitate a rețelei îmbunătățește considerabil calificările pentru aceste posturi. Există numeroase certificări.

Certificarile pentru profesioniștii în securitatea rețelei sunt oferite de următoarele organizații:

- *Certificare globală de asigurare a informațiilor (GIAC)*
- *Consortiul Internațional de Certificare a Securității Sistemelor Informaționale (ISC)<sup>2</sup>*
- *Asociația de Audit și Control al Sistemelor Informaționale (ISACA)*
- *Consiliul Internațional al Consultanților în Comerț E-E (CE-Council)*
- *Certified Wireless Security Professional (CWSP)*

Cisco a înlocuit certificarea Cisco Certified Network Associate Security (210-260 IINS) cu o nouă certificare CCNP Security. Această certificare constă din două examene, un examen de bază de securitate și un examen de concentrare. Este necesar un singur examen de concentrare. Examenul de implementare și operare Cisco Security Core Technologies (350-701 SCOR) servește ca o poartă de acces la certificările CCNP și CCIE de securitate. De asemenea, oferă certificare de bază de securitate. Examenul de bază acoperă concepte de securitate, amenințări și tehnici și tehnologii de atenuare. Specializările se concentrează în profunzime pe tehnologiile specifice de securitate Cisco. Examenele de concentrare de securitate Cisco Certified Specialist sunt după cum urmează:

- ***300-710 SNCF - Network Security Firepower***
- ***300-715 SISE - Implementarea și configurarea Cisco Identity Services Engine***
- ***300-720 SESA - Securizarea e-mailului cu Cisco Email Security Appliance***
- ***300-725 SWSA - Securizarea Web-ului cu Cisco Web Security Appliance***
- ***300-730 SVPN - Implementarea soluțiilor securizate cu rețele private virtuale***
- ***300-735 SAUTO - Automatizarea și programarea soluțiilor de securitate Cisco***

Există multe modalități de pregătire pentru aceste certificări, inclusiv auto-studiu, învățământ cu examen privat și învățământ superior. Organizația Learning at Cisco, împreună

cu partenerii săi de învățare, oferă informații și instruire pentru majoritatea examenelor de certificare Cisco.

### 3.1.4 - Communications Security: CIA

Securitatea informațiilor se ocupă cu protejarea informațiilor și a sistemelor de informații împotriva accesului, utilizării, dezvăluirii, întreruperii, modificării sau distrugerii neautorizate. Triada CIA servește ca fundație conceptuală pentru domeniu.

Figura arată Triada CIA constând din Confidențialitate, Integritate și Disponibilitate.



Fig. 3.1. Triada CIA.

După cum se arată în figură, triada CIA constă din trei componente ale securității informațiilor:

1. **Confidențialitate** - Numai persoanele, entitățile sau procesele autorizate pot accesa informațiile sensibile.
2. **Integritate** - Aceasta se referă la protecția datelor împotriva modificărilor neautorizate.
3. **Disponibilitate** - Utilizatorii autorizați trebuie să aibă acces neîntrerupt la resursele și datele de rețea de care au nevoie.

Datele din rețea pot fi criptate (făcute nelizibile pentru utilizatorii neautorizați) folosind diverse aplicații de criptare. Conversația dintre doi utilizatori de telefoane IP poate fi criptată. Fișierele de pe un computer pot fi, de asemenea, criptate. Acestea sunt doar câteva exemple.



Criptografia poate fi folosită aproape oriunde există comunicare de date. De fapt, tendința este ca toate comunicațiile să fie criptate.

## 3.2 Network Security Policies

### 3.2.1 - Network Security Domains

Este vital ca profesioniștii în securitatea rețelei să înțeleagă motivele securității rețelei. De asemenea, trebuie să fie familiarizați cu cerințele organizaționale pentru securitatea rețelei, așa cum sunt încorporate de cele 14 domenii de securitate a rețelei.

Domeniile oferă un cadru pentru discutarea securității rețelei și înțelegerea nevoilor operaționale care ar trebui să fie abordate de fiecare organizație.

Există 14 domenii de securitate a rețelei specificate de Organizația Internațională pentru Standardizare (ISO)/Comisia Electrotehnică Internațională (IEC). Descrise de ISO/IEC 27001, aceste 14 domenii servesc la organizarea, la un nivel înalt, a vastului tărâm al informațiilor și activităților sub umbrela securității rețelei. Aceste domenii au unele paralele semnificative cu domeniile definite de certificarea Certified Information Systems Security Professional (CISSP).

Cele 14 domenii sunt destinate să servească drept bază comună pentru dezvoltarea standardelor de securitate organizațională și a practicilor eficiente de management al securității. Ele ajută, de asemenea, la facilitarea comunicării între organizații.

Aceste 14 domenii oferă o separare convenabilă a elementelor de securitate a rețelei. Deși nu este important să se memoreze aceste 14 domenii, este important să conștientizăm existența lor și declarația oficială de către ISO. În standardul ISO 27001, acestea sunt cunoscute ca cele 14 seturi de control din anexa A. Ele vor servi ca referință utilă în munca unui profesionist în securitatea rețelei.

1. **Information Security Policies** - Această anexă este concepută pentru a se asigura că politicile de securitate sunt create, revizuite și menținute.
2. **Organization of Information Security** - Acesta este modelul de guvernare stabilit de o organizație pentru securitatea informațiilor. Atribuire responsabilități pentru sarcinile de securitate a informațiilor în cadrul unei organizații.
3. **Human Resources Security** - Aceasta se referă la responsabilitățile de securitate legate de angajații care se alătură, se mută / părăsesc o organizație.

4. **Asset Management** - Aceasta se referă la modul în care organizațiile creează un inventar și o schemă de clasificare a activelor informaționale.
5. **Access Control** - Aceasta descrie restricția drepturilor de acces la rețele, sisteme, aplicații, funcții și date.
6. **Cryptography** - Aceasta se referă la criptarea datelor și la gestionarea informațiilor sensibile pentru a proteja confidențialitatea, integritatea și disponibilitatea datelor.
7. **Physical and Environmental Security** - Aceasta descrie protecția instalațiilor și echipamentelor fizice de calculator din cadrul unei organizații.
8. **Operations Security** - Acesta descrie gestionarea controalelor tehnice de securitate în sisteme și rețele, inclusiv apărarea împotriva programelor malware, backupul datelor, înregistrarea și monitorizarea, gestionarea vulnerabilităților și considerațiile de audit. Acest domeniu este, de asemenea, preocupat de integritatea software-ului care este utilizat în operațiunile de afaceri.
9. **Communications Security** - Aceasta se referă la securitatea datelor, așa cum sunt comunicate în rețele, atât în cadrul unei organizații, cât și între organizație și terți, cum ar fi clienții sau furnizorii.
10. **System Acquisition, Development, and Maintenance** - Acest lucru asigură că securitatea informațiilor rămâne o preocupare centrală în procesele unei organizații de-a lungul întregului ciclu de viață, atât în rețelele private, cât și în cele publice.
11. **Supplier Relationships** - Aceasta se referă la specificarea acordurilor contractuale care protejează informațiile și activele tehnologice ale unei organizații care sunt accesibile de către terți care furnizează bunuri și servicii organizației.
12. **Information Security Incident Management** - Acesta descrie cum să se anticipeze și să se răspunda la încălcările securității informațiilor.
13. **Business Continuity Management** - Acesta descrie protecția, întreținerea și recuperarea proceselor și sistemelor critice pentru afaceri.
14. **Compliance** - Acesta descrie procesul de asigurare a conformității cu politicile, standardele și reglementările de securitate a informațiilor.

### 3.2.2 - Business Policies

Politicele de afaceri sunt liniile directoare care sunt dezvoltate de o organizație pentru a-și guverna acțiunile. Politicile definesc standarde de comportament corect pentru afacere și pentru angajații săi.

În rețea, politicile definesc activitățile care sunt permise în rețea. Aceasta stabilește o bază de utilizare acceptabilă. Dacă în rețea este detectat un comportament care încalcă politica de afaceri, este posibil să fi avut loc o încălcare a securității.

O organizație poate avea mai multe politici de ghidare, așa cum sunt enumerate mai jos:

Company policies - Aceste politici stabilesc regulile de conduită și responsabilitățile atât ale angajaților, cât și ale angajatorilor.

Politicele protejează drepturile lucrătorilor, precum și interesele de afaceri ale angajatorilor.

În funcție de nevoile organizației, diverse politici și proceduri stabilesc reguli privind conduita angajaților, prezența, codul vestimentar, confidențialitatea și alte domenii legate de termenii și condițiile de angajare.

Employee policies - Aceste politici sunt create și menținute de personalul de resurse umane pentru a identifica salariul angajaților, programul de plată, beneficiile angajaților, programul de lucru, vacanțele și multe altele.

Acestea sunt adesea furnizate noilor angajați pentru a le revizui și semna.

Security policies - Aceste politici identifică un set de obiective de securitate pentru o companie, definesc regulile de comportament pentru utilizatori și administratori și specifică cerințele de sistem.

Aceste obiective, reguli și cerințe asigură în mod colectiv securitatea unei rețele și a sistemelor informatice dintr-o organizație.

La fel ca un plan de continuitate, o politică de securitate este un document în continuă evoluție, bazat pe schimbări în peisajul amenințărilor, vulnerabilități și cerințele de afaceri și ale angajaților.

### 3.2.3 - Security Policy

O politică de securitate cuprinzătoare are o serie de beneficii, inclusiv următoarele:

- i. *Demonstrează angajamentul unei organizații față de securitate*
- ii. *Stabilește regulile pentru comportamentul așteptat*

- iii. *Asigură consecvența în operațiunile sistemului, achiziția și utilizarea software-ului și hardware-ului și întreținerea*
- iv. *Definește consecințele juridice ale încălcărilor*
- v. *Oferă personalului de securitate sprijinul conducerii*

Politicile de securitate sunt folosite pentru a informa utilizatorii, personalul și managerii cu privire la cerințele unei organizații pentru protejarea activelor tehnologice și informaționale. O politică de securitate specifică, de asemenea, mecanismele care sunt necesare pentru a îndeplini cerințele de securitate și oferă o linie de bază de la care să se achiziționeze, să se configureze și să se auditeze sistemele și rețelele de calculatoare pentru conformitate.

Politicile care pot fi incluse într-o politică de Securitate sunt:

Identification and authentication policy - Specifică persoanele autorizate care pot avea acces la resursele rețelei și la procedurile de verificare a identității.

Password policies - Se asigură că parolele îndeplinesc cerințele minime și sunt schimbate în mod regulat.

Acceptable Use Policy (AUP) - Identifică aplicațiile și utilizările de rețea care sunt acceptabile pentru organizație. De asemenea, poate identifica ramificații dacă această politică este încălcată.

Remote access policy - Identifică modul în care utilizatorii de la distanță pot accesa o rețea și ce este accesibil prin conectivitate de la distanță.

Network maintenance policy - Specifică sistemele de operare ale dispozitivelor de rețea și procedurile de actualizare a aplicațiilor pentru utilizatorul final.

Incident handling procedures - Descrie modul în care sunt gestionate incidentele de securitate.

Una dintre cele mai comune componente ale politicii de securitate este un AUP. Aceasta poate fi denumită și o politică de utilizare adecvată. Această componentă definește ce utilizatorii au voie și ce nu au voie să facă asupra diferitelor componente ale sistemului. Aceasta include tipul de trafic care este permis în rețea. AUP ar trebui să fie cât mai explicit posibil pentru a evita neînțelegerile.

De exemplu, un AUP ar putea enumera anumite site-uri web, grupuri de știri sau aplicații cu lățime de bandă intensivă care nu pot fi accesate de computerele companiei sau din rețeaua

companiei. Fiecărui angajat ar trebui să li se ceară să semneze un AUP, iar AUP-urile semnate ar trebui păstrate pe durata angajării.

### 3.2.4 - BYOD Policies

Multe organizații trebuie să accepte acum și Bring Your Own Device (BYOD). Acest lucru le permite angajaților să-și folosească propriile dispozitive mobile pentru a accesa sistemele, software-ul, rețelele sau informațiile companiei.

BYOD oferă mai multe beneficii cheie întreprinderilor, inclusiv productivitate crescută, costuri reduse de IT și operare, mobilitate mai bună pentru angajați și atractivitate mai mare atunci când vine vorba de angajarea și păstrarea angajaților.

Cu toate acestea, aceste beneficii aduc, de asemenea, un risc crescut de securitate a informațiilor, deoarece BYOD poate duce la încălcări ale datelor și la o mai mare răspundere pentru organizație.

Ar trebui dezvoltată o politică de securitate BYOD pentru a realiza următoarele:

- *Specificarea obiectivelor programului BYOD.*
- *Identificarea angajaților care își pot aduce propriile dispozitive.*
- *Identificarea dispozitivelor ce vor fi acceptate.*
- *Identificarea nivelului de acces acordat angajaților atunci când folosesc dispozitive personale.*
- *Descrierea drepturilor de acces și activităților permise personalului de securitate de pe dispozitiv.*
- *Identificarea reglementărilor ce trebuie respectate atunci când sunt utilizate dispozitivele angajaților.*
- *Identificarea măsurilor de siguranță de pus în aplicare dacă un dispozitiv este compromis.*

Printre cele mai bune practici de securitate BYOD pentru a ajuta la atenuarea vulnerabilităților BYOD pot fi:

Password protected access - Utilizarea parolelor unice pentru fiecare dispozitiv și cont.

Manually control wireless connectivity - Oprirea conexiunilor Wi-Fi și Bluetooth atunci când nu sunt în uz. Conectarea numai la rețele de încredere.

Keep updated – Păstrarea, întotdeauna, sistemului de operare actualizat al dispozitivului și alte programe software. Software-ul actualizat conține adesea corecții de securitate pentru a atenua cele mai recente amenințări sau exploatări.

Back up data - Activarea backup-ului dispozitivului în cazul în care acesta este pierdut sau furat.

Enable “Find my Device” - Abonarea la un serviciu de localizare a dispozitivelor cu funcție de ștergere de la distanță.

Provide antivirus software – Furnizare de software antivirus pentru dispozitivele BYOD aprobate.

Use Mobile Device Management (MDM) software - Software-ul MDM permite echipelor IT să implementeze setări de securitate și configurații software pe toate dispozitivele care se conectează la rețelele companiei.

### 3.2.5 - Regulatory and Standards Compliance

Există și reglementări externe privind securitatea rețelei. Profesioniștii în securitatea rețelelor trebuie să fie familiarizați cu legile și codurile de etică care sunt obligatorii pentru profesioniștii în securitatea sistemelor informaționale (INFOSEC).

Multe organizații sunt mandatate să dezvolte și să implementeze politici de securitate. Reglementările de conformitate definesc ce organizații sunt responsabile pentru furnizarea și răspunderea în cazul în care nu se conformează. Reglementările de conformitate pe care o organizație este obligată să le respecte depind de tipul de organizație și de datele pe care organizația le gestionează.

## 3.3 Security Tools, Platforms, and Services

### 3.3.1 - The Security Onion and The Security Artichoke

**Security Onion** - O analogie comună folosită pentru a descrie o abordare de apărare în profunzime este numită „ceapa de securitate”. După cum este ilustrat în figură, un actor de amenințare ar trebui să dezlipească nivelul de apărare al unei rețele, într-un mod similar cu curățarea unei cepe. Numai după ce a pătruns fiecare nivel, actorul amenințării va ajunge la datele sau sistemul țintă.

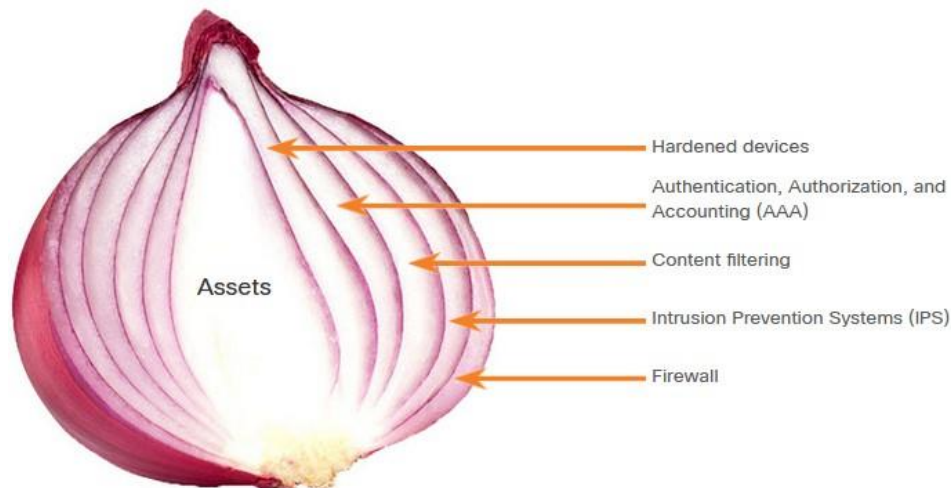


Fig. 3.2. Comparatie nivelurilor de aparare si distributia foilor de ceapa.

Figura cu ceapă de securitate arată o ceapă cu diferite niveluri în interior. Ceapa este etichetată drept bun. În dreapta sunt cuvinte și săgeți care indică diferitele niveluri:

- *dispozitive întărite;*
- *autentificare, autorizare și contabilitate (A A A);*
- *filtrarea conținutului;*
- *sisteme de prevenire a intruziunilor (I P S);*
- *firewall.*

Notă: Ceapa de securitate descrisă în această pagină este o modalitate de a vizualiza apărarea în profunzime. Acest lucru nu trebuie confundat cu suita Security Onion de instrumente de securitate a rețelei.

**Security Artichoke** - Peisajul în schimbare al rețelelor, cum ar fi evoluția rețelelor fără granițe, a schimbat această analogie cu „anghinarea de securitate”, de care beneficiază actorul amenințării.

După cum este ilustrat în figură, actorii amenințării nu mai trebuie să dezlipească fiecare strat. Trebuie doar să îndepărteze anumite „frunze de anghinare”. Bonusul este că fiecare „frunză” a rețelei poate dezvălui date sensibile care nu sunt bine securizate.

De exemplu, este mai ușor pentru un actor de amenințare să compromită un dispozitiv mobil decât să compromită un computer sau un server intern care este protejat de niveluri de apărare. Fiecare dispozitiv mobil este o frunză. Și frunză după frunză, totul îl conduce pe hacker la mai multe date. Inima anghinării este locul unde se găsesc cele mai confidențiale date. Fiecare frunză oferă un nivel de protecție, oferind simultan o cale de atac.

Nu toate frunzele trebuie îndepărtate pentru a ajunge în miezul anghinării. Hackerul scoate armura de securitate de-a lungul perimetrului pentru a ajunge la „inima” întreprinderii.

În timp ce sistemele care se confruntă cu internet sunt de obicei foarte bine protejate, iar protecțiile limitelor sunt de obicei solide, hackerii persistenti, ajutați de un amestec de pricepere și noroc, găsesc în cele din urmă un gol în acel exterior dur prin care pot intra și merge unde doresc.

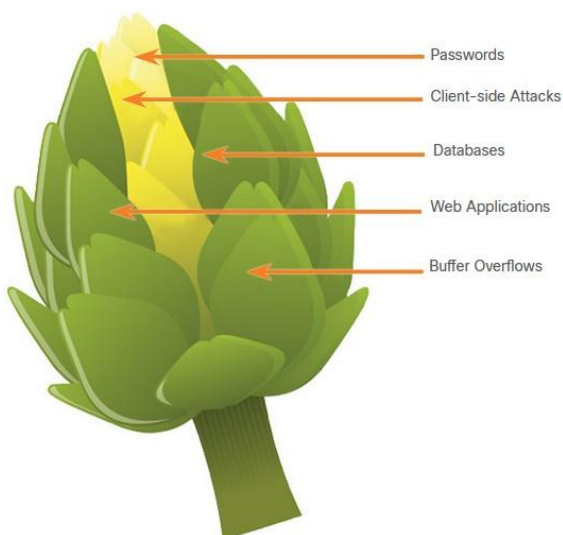


Fig. 3.3. Security Artichoke.

Figura cu anghinare de securitate arată o anghinare cu diferite secțiuni în interiorul ei. Cuvintele din dreapta au o săgeată care indică secțiunile individuale ale anghinării:

- *parole;*
- *atacuri din partea clientului;*
- *baze de date;*
- *aplicații web;*
- *suprascirerea memoriei tampon.*

### 3.3.2 - Security Testing Tools

Hackingul etic implică utilizarea multor tipuri diferite de instrumente pentru a testa rețeaua și dispozitivele finale. Pentru a valida securitatea unei rețele și a sistemelor acesteia, au fost dezvoltate multe instrumente de testare a securității rețelei. Testarea de penetrare implică utilizarea tehnicilor și instrumentelor hackerilor pentru a evalua puterea măsurilor de



securitate a rețelei. Cu toate acestea, multe dintre aceste instrumente pot fi utilizate și de către actorii amenințărilor pentru exploatare.

Actorii amenințărilor au creat și diverse instrumente de hacking. Aceste instrumente sunt scrise în mod explicit din motive nefaste. De asemenea, personalul de securitate cibernetică trebuie să știe cum să folosească aceste instrumente atunci când efectuează teste de penetrare în rețea.

Notă: Multe dintre aceste instrumente sunt bazate pe UNIX sau Linux; prin urmare, un profesionist în securitate ar trebui să aibă un fundal puternic UNIX și Linux.

***password crackers*** - Parolele sunt cea mai vulnerabilă amenințare de securitate. Instrumentele de spargere a parolilor sunt adesea denumite instrumente de recuperare a parolei și pot fi folosite pentru a sparge sau recupera parola. Acest lucru se realizează fie prin eliminarea parolei originale, după ocolirea criptării datelor, fie prin descoperirea completă a parolei. Descoperitorii de parole fac în mod repetat presupuneri pentru a sparge parola și a accesa sistemul. Exemple de instrumente de spargere a parolilor includ John the Ripper, Ophcrack, L0phtCrack, THC Hydra, RainbowCrack și Medusa.

***wireless hacking tools*** - Rețelele wireless sunt mai susceptibile la amenințările la securitatea rețelei. Instrumentele de hacking fără fir sunt folosite pentru a sparge în mod intenționat o rețea fără fir pentru a detecta vulnerabilitățile de securitate. Exemple de instrumente de hacking wireless includ Aircrack-ng, Kismet, InSSIDer, KisMAC, Firesheep și NetStumbler.

***network scanning and hacking tools*** - Instrumentele de scanare a rețelei sunt folosite pentru a sonda dispozitivele de rețea, serverele și gazdele pentru porturi TCP sau UDP deschise. Exemple de instrumente de scanare includ Nmap, SuperScan, Angry IP Scanner și NetScanTools.

***packet crafting tools*** - Instrumentele de creare a pachetelor sunt folosite pentru a proba și a testa robustețea unui firewall folosind pachete forjate special concepute. Exemple de astfel de instrumente includ Hping, Scapy, Socat, Yersinia, Netcat, Nping și Nemesis.

***packet sniffers*** - Instrumentele de mirosire (sniffer) de pachete sunt folosite pentru a captura și analiza pachete în rețelele LAN sau WLAN tradiționale Ethernet. Instrumentele includ Wireshark, Tcpdump, Ettercap, Dsniff, EtherApe, Paros, Fiddler, Ratproxy și SSLstrip.

***rootkit detectors*** - Un detector de rootkit este un verificador de integritate a directoarelor și fișierelor folosit de pălăriile albe pentru a detecta kiturile root instalate. Exemple de instrumente includ AIDE, Netfilter și PF: OpenBSD Packet Filter.

***fuzzers to search vulnerabilities*** - Fuzzers sunt instrumente folosite de actorii amenințărilor atunci când încearcă să descopere vulnerabilitățile de securitate ale unui sistem informatic. Exemple de fuzzere includ Skipfish, Wapiti și W3af.

***forensic tools*** - Hackerii cu pălărie albă folosesc instrumente criminalistice pentru a adulmeca orice urmă de dovezi existente într-un anumit sistem informatic. Exemple de instrumente includ Sleuth Kit, Helix, Maltego și Encase.

***debuggers*** - Instrumentele de depanare sunt folosite de black hats pentru a face inginerie inversă a fișierelor binare atunci când scrieți exploit-uri. Ele sunt, de asemenea, folosite de pălăriile albe atunci când analizează programele malware. Instrumentele de depanare includ GDB, WinDbg, IDA Pro și Immunity Debugger.

***hacking operating systems*** - Sistemele de operare de hacking sunt sisteme de operare special concepute, preîncărcate cu instrumente și tehnologii optimizate pentru hacking. Exemple de sisteme de operare special concepute pentru hacking includ Kali Linux, SELinux, Knoppix, Parrot OS și BackBox Linux.

***encryption tools*** - Aceste instrumente protejează conținutul datelor unei organizații atunci când acestea sunt stocate sau transmise. Instrumentele de criptare folosesc scheme de algoritmi pentru a codifica datele pentru a preveni accesul neautorizat la date. Exemple de aceste instrumente includ VeraCrypt, CipherShed, Open SSH, OpenSSL, OpenVPN și Stunnel.

***vulnerability exploitation tools*** - Aceste instrumente identifică dacă o gazdă la distanță este vulnerabilă la un atac de securitate. Exemple de instrumente de exploatare a vulnerabilităților includ Metasploit, Core Impact, Sqlmap, Social Engineer Tool Kit și Netsparker.

***vulnerability scanners*** - Aceste instrumente scanează o rețea sau un sistem pentru a identifica porturile deschise. Ele pot fi, de asemenea, utilizate pentru a scana vulnerabilități cunoscute și pentru a scana mașini virtuale, dispozitive BYOD și baze de date clienți. Exemple de aceste instrumente includ Nipper, Securia PSI, Core Impact, Nessus, SAINT și Open VAS.

### 3.3.3 - Data Security Platforms

Platformele de securitate a datelor (DSP) sunt o soluție de securitate integrată care combină instrumente tradiționale independente într-o suită de instrumente care sunt făcute să funcționeze împreună. Instrumentele de securitate care protejează și monitorizează rețelele sunt adesea realizate de diferiți furnizori. Poate fi dificil să se integreze aceste instrumente în așa fel încât să se poată obține o singură viziune asupra securității rețelei. Pot fi necesare resurse semnificative pentru a avea diferite dispozitive și software sub o singură soluție de control. În plus, integrarea datelor din instrumente atât de diverse într-o vizualizare cuprinzătoare de monitorizare a rețelei poate fi foarte dificil de creat și întreținut.

Un astfel de DSP este platforma Helix de la FireEye. FireEye Helix este o platformă de operațiuni de securitate bazată pe cloud, care permite organizațiilor să integreze multe funcționalități de securitate într-o singură platformă. Helix oferă management de evenimente, analiză a comportamentului rețelei, detectare avansată a amenințărilor și orchestrare, automatizare și răspuns (SOAR) pentru securitatea incidentelor pentru răspuns la amenințări pe măsură ce sunt detectate. Helix se bazează, de asemenea, pe informații despre amenințări FireEye Mandiant, răspuns la incident și expertiză în materie de securitate.

Un alt DSP integrat este Cisco SecureX. SecureX face un pas mai departe prin integrarea sa puternică cu portofoliul Cisco Secure. Portofoliul Cisco Secure constă dintr-un set larg de tehnologii care funcționează ca o echipă - oferind interoperabilitate cu infrastructura de securitate, inclusiv tehnologii terțe. Acest lucru are ca rezultat o vizibilitate unificată, automatizare și o apărare mai puternică. Platforma Cisco SecureX funcționează cu diverse produse care se combină pentru a vă proteja rețeaua, utilizatorii și punctele finale, marginea cloudului și aplicațiile. Funcționalitatea SecureX este încorporată într-un portofoliu mare și divers de produse de securitate Cisco, inclusiv firewall-uri de ultimă generație, VPN, analiză de rețea, motor de servicii de identitate, protecție avansată împotriva malware-ului (AMP) și multe alte sisteme care funcționează pentru a securiza toate aspectele unei rețele. . SecureX integrează, de asemenea, o gamă de instrumente de securitate terță parte.

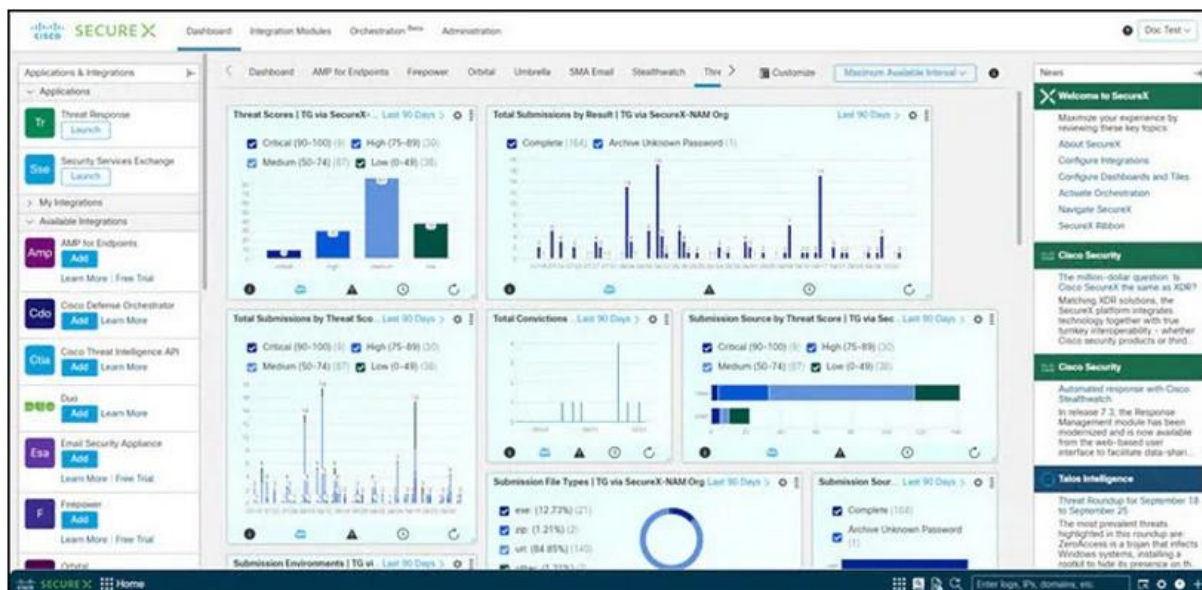


Fig. 3.4. Platforma Securex.

### 3.3.4 - Security Services

Serviciile de informații despre amenințări și securitate permit schimbul de informații despre amenințări, cum ar fi vulnerabilități, indicatori de compromis (IOC) și tehnici de atenuare. Aceste informații nu sunt partajate doar personalului, ci și sistemelor de securitate. Pe măsură ce apar amenințările, serviciile de informații despre amenințări creează și distribuie reguli de firewall și IOC-uri către dispozitivele care s-au abonat la serviciu.

Un astfel de serviciu este Cisco Talos Threat Intelligence Group, prezentat în figură. Talos este una dintre cele mai mari echipe comerciale de informații despre amenințări din lume și este compusă din cercetători, analiști și ingineri de talie mondială. Scopul Talos este de a ajuta la protejarea utilizatorilor întreprinderii, a datelor și a infrastructurii de adversarii activi. Echipa Talos colectează informații despre amenințările active, existente și emergente. Talos oferă apoi protecție completă împotriva acestor atacuri și malware abonaților săi.

Produsele Cisco Security pot folosi informațiile despre amenințări Talos în timp real pentru a oferi soluții de securitate rapide și eficiente. Cisco Talos oferă, de asemenea, software, servicii, resurse și date gratuite. Talos menține seturile de reguli de detectare a incidentelor de securitate pentru instrumentele de securitate de rețea Snort.org, ClamAV și SpamCop.



Fig. 3.5. TALOS.

O serie de servicii de securitate a rețelei gestionate sunt disponibile de la furnizori precum Cisco, Sentinel Intrusion Prevention Systems, IBM, AT&T și Core Security. Aceste organizații oferă o gamă largă de servicii, inclusiv securitate gestionată ca serviciu (SECaaS sau SaaS).

### 3.4 Mitigating Common Network Attacks

#### 3.4.1 - Defending the Network

Vigilență constantă și educație continuă sunt necesare pentru a apăra rețeaua împotriva atacurilor. Următoarele sunt cele mai bune practici pentru securizarea unei rețele:

- *Elaborarea unor politici de securitate scrise pentru companie.*
- *Educarea angajaților referitor la riscurile ingineriei sociale și dezvoltarea strategiilor de validare a identităților prin telefon, prin e-mail sau în persoană.*
- *Controlarea accesului fizic la sisteme.*
- *Folosirea parolelor puternice și schimbarea acestora des.*
- *Criptarea și protejarea cu parolă a datelor sensibile.*

- *Implementare hardware și software de securitate, cum ar fi firewall-uri, IPS, dispozitive de rețea privată virtuală (VPN), software antivirus și filtrarea conținutului.*
- *Efectuare de copii de siguranță și testare în mod regulat a fișierelor de rezervă.*
- *Închiderea serviciilor și porturilor inutile.*
- *Păstrarea patch-urile la zi instalându-le săptămânal sau zilnic, dacă este posibil, pentru a se preveni depășirea tamponului și atacurile de escaladare a privilegiilor.*
- *Efectuarea auditurilor de Securitate periodica pentru a testa rețeaua.*

### 3.4.2 - Mitigating Malware

Programele malware, inclusiv viruși, viermi și cai troieni, pot cauza probleme serioase pe rețele și dispozitivele finale. Administratorii de rețea au mai multe mijloace de a atenua aceste atacuri.

Notă: tehnicile de atenuare sunt adesea denumite în comunitatea de securitate „contramăsuri”.

O modalitate de a atenua atacurile virușilor și cailor troieni este software-ul antivirus. Software-ul antivirus ajută la prevenirea infectării gazdelor și a răspândirii de coduri rău intenționate. Este nevoie de mult mai mult timp pentru a curăța computerele infectate decât pentru a menține software-ul antivirus și definițiile antivirus actualizate pe aceleași mașini.

Software-ul antivirus este cel mai răspândit produs de securitate de pe piață în prezent. Mai multe companii care creează software antivirus, cum ar fi Symantec, McAfee și Trend Micro, se ocupă de detectarea și eliminarea virușilor de mai bine de un deceniu. Multe corporații și instituții de învățământ achiziționează licențe în volum pentru utilizatorii lor. Utilizatorii se pot conecta la un site web cu contul lor și pot descărca software-ul antivirus de pe desktop-urile, laptopurile sau serverele lor.

Produsele antivirus au opțiuni de automatizare a actualizărilor, astfel încât noile definiții de viruși și noile actualizări de software să poată fi descărcate automat sau la cerere. Această practică este cea mai critică cerință pentru menținerea unei rețele fără viruși și ar trebui să fie oficializată într-o politică de securitate a rețelei.

Produsele antivirus sunt bazate pe gazdă. Aceste produse sunt instalate pe computere și servere pentru a detecta și elimina virușii. Cu toate acestea, ele nu împiedică virușii să intre în rețea, așa că un profesionist în securitatea rețelei trebuie să fie conștient de virușii majori și să țină evidența actualizărilor de securitate cu privire la virușii emergenti.

O altă modalitate de a atenua amenințările malware este de a împiedica fișierele malware să intre în rețea. Dispozitivele de securitate din perimetrul rețelei pot identifica fișierele malware cunoscute pe baza indicatorilor lor de compromis. Fișierele pot fi eliminate din fluxul de date primit înainte de a provoca un incident. Din păcate, actorii amenințărilor sunt conștienți de această contramăsură și își modifică frecvent malware-ul suficient de mult încât să evite detectarea. Aceste exploit-uri vor intra în rețea și, de asemenea, vor evita software-ul antivirus. Nicio tehnică de atenuare nu poate fi 100% eficientă. Incidentele de securitate vor avea loc.

### 3.4.3 - Mitigating Worms

Viermii sunt mai mult bazați pe rețea decât virușii. Atenuarea viermilor necesită consecvență și coordonare din partea profesioniștilor în securitatea rețelei.

După cum se arată în figură, răspunsul la un atac de viermi poate fi împărțit în patru faze: izolare, inoculare, carantină și tratament.

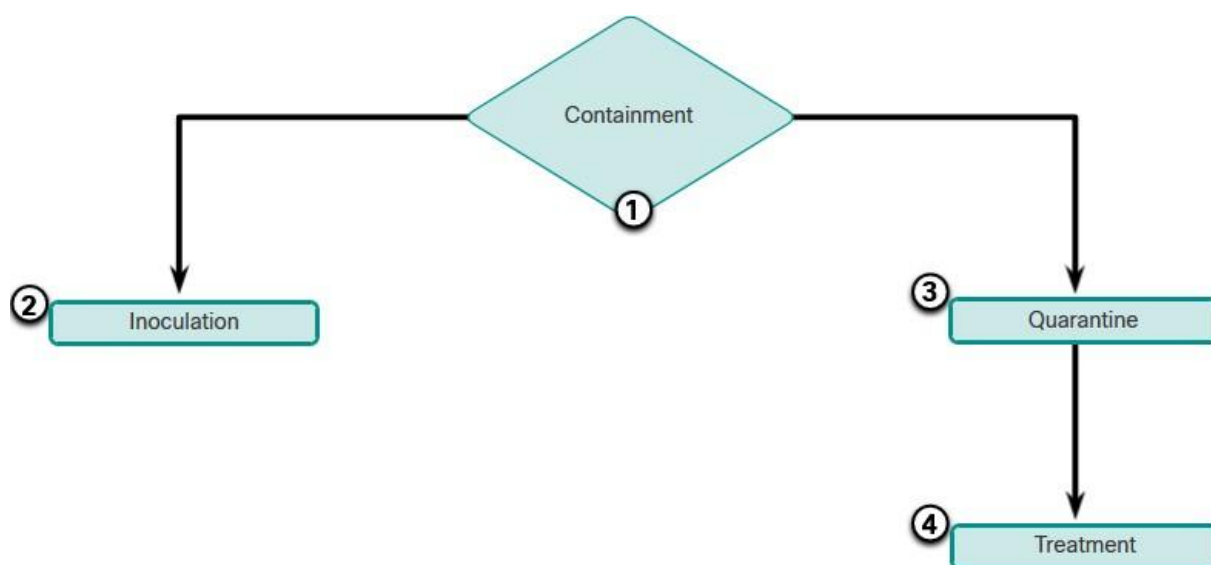


Fig. 3.6. Contramasuri in atac cu virusi.

**1. Containment - contaminare** - Faza de izolare presupune limitarea răspândirii unei infecții cu viermi în zonele rețelei care sunt deja afectate. Acest lucru necesită compartimentarea și segmentarea rețelei pentru a încetini sau opri viermele și pentru a preveni gazdele infectate în prezent să ținăască și să infecteze alte sisteme. Limitarea necesită utilizarea atât a ACL-urilor de ieșire, cât și de intrare pe routere și firewall-uri la punctele de control din rețea.

**2. Inoculare – Inoculation** - Faza de inoculare se desfășoară paralel cu sau ulterior fazei de izolare. În timpul fazei de inoculare, toate sistemele neinfectate sunt patch-uri cu noutatile

furnizorului corespunzător. Procesul de inoculare privează și mai mult viermele de orice ținte disponibile.

**3. Carantină - Quarantine** -Faza de carantină implică urmărirea și identificarea mașinilor infectate în zonele conținute și deconectarea, blocarea sau îndepărtarea acestora. Acest lucru izolează aceste sisteme în mod corespunzător pentru faza de tratament.

**4. Tratament - Treatment** - Faza de tratament presupune dezinfectarea activă a sistemelor infectate. Acest lucru poate implica terminarea procesului de vierme, eliminarea fișierelor modificate sau a setărilor de sistem pe care viermele le-a introdus și corecția vulnerabilității pe care viermele a folosit-o pentru a exploata sistemul. Alternativ, în cazuri mai severe, sistemul poate fi necesar să fie reinstalat pentru a se asigura că viermele și produsele secundare ale acestuia sunt îndepărtate.

#### 3.4.4 - Mitigating Reconnaissance Attacks

Atacurile de recunoaștere sunt de obicei precursorul altor atacuri care au intenția de a obține acces neautorizat la o rețea sau de a perturba funcționalitatea rețelei. Un profesionist în securitatea rețelei poate detecta când este în desfășurare un atac de recunoaștere, primind notificări de la alarme preconfigurate. Aceste alarme sunt declanșate atunci când anumiți parametri sunt depășiți, cum ar fi numărul de solicitări ICMP pe secundă. O varietate de tehnologii și dispozitive pot fi utilizate pentru a monitoriza acest tip de activitate și a genera o alarmă. Dispozitivul Adaptive Security Appliance (ASA) de la Cisco oferă prevenirea intruziunilor într-un dispozitiv autonom. În plus, Cisco ISR acceptă prevenirea intruziunilor bazată pe rețea prin imaginea de securitate Cisco IOS.

Atacurile de recunoaștere pot fi atenuate în mai multe moduri, inclusiv următoarele:

- *Implementarea autentificării pentru a asigura accesul adecvat.*
- *Folosirea criptării pentru a face inutile atacurile de sniffer de pachete.*
- *Utilizarea instrumentelor anti-sniffer pentru a detecta atacurile de sniffer de pachete.*
- *Implementarea unei infrastructuri comutate.*
- *Folosind un firewall și IPS.*

Instrumentele software și hardware anti-sniffer detectează modificări ale timpului de răspuns al gazdelor pentru a determina dacă gazdele procesează mai mult trafic decât ar indica



propriile încărcări de trafic. Deși acest lucru nu elimină complet amenințarea, ca parte a unui sistem general de atenuare, poate reduce numărul de cazuri de amenințare.

Criptarea este, de asemenea, eficientă pentru atenuarea atacurilor de tip sniffer de pachete. Dacă traficul este criptat, folosirea unui sniffer de pachete este de puțin folos, deoarece datele capturate nu pot fi citite.

Este imposibil să se atenueze scanarea portului, dar utilizarea unui sistem de prevenire a intruziunilor (IPS) și a unui firewall poate limita informațiile care pot fi descoperite cu un scanner de porturi. Sweep-urile ping pot fi oprite dacă ecoul ICMP și răspunsul la eco sunt dezactivate pe routerele edge; cu toate acestea, atunci când aceste servicii sunt dezactivate, datele de diagnosticare a rețelei se pierd. În plus, scanările de porturi pot fi executate fără scanări complete de ping. Scanările durează pur și simplu mai mult deoarece sunt scanate și adresele IP inactive.

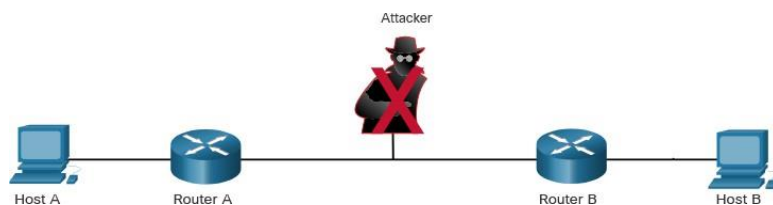


Fig. 3.7. Reconnaissance Attack Mitigation Techniques.

#### 3.4.5 - Mitigating Access Attacks

Sunt disponibile mai multe tehnici pentru atenuarea atacurilor de acces. Acestea includ securitatea puternică a parolelor, principiul încrederii minime, criptografia, aplicarea sistemului de operare și a corecțiilor aplicației.

Un număr surprinzător de atacuri de acces sunt efectuate prin simpla ghicire a parolelor sau atacuri de dicționar în forță brută împotriva parolelor. Pentru a ne apăra împotriva acestui fapt, se creează și se aplică o politică de autentificare puternică care să includă:

- **Utilizare de parole puternice** - Parolele puternice au cel puțin opt caractere și conțin litere mari, litere mici, cifre și caractere speciale.
- **Dezactivarea conturilor după ce a avut loc un anumit număr de conectări nereușite** - Această practică ajută la prevenirea încercărilor continue de utilizare a parolei.

De asemenea, rețeaua ar trebui să fie proiectată folosind principiul încrederii minime. Aceasta înseamnă că sistemele nu ar trebui să se folosească unul pe altul în mod inutil. De

exemplu, dacă o organizație are un server de încredere care este utilizat de dispozitive care nu sunt de încredere, cum ar fi serverele web, serverul de încredere nu ar trebui să aibă încredere în dispozitivele care nu sunt de încredere necondiționat.

Criptografia este o componentă critică a oricărei rețele moderne securizate. Se recomandă utilizarea criptării pentru accesul de la distanță la o rețea. Traficul protocolului de rutare ar trebui, de asemenea, să fie criptat. Cu cât traficul este criptat mai mult, cu atât mai puține oportunități au hackerii de a intercepta date cu atacuri de tip man-in-the-middle.

Utilizarea protocoalelor de autentificare criptate sau hashing, împreună cu o politică puternică de parole, reduce foarte mult probabilitatea atacurilor de acces de succes.

În cele din urmă, educarea angajaților cu privire la riscurile inginerii sociale și dezvoltarea strategiilor de validare a identităților prin telefon, prin e-mail sau în persoană. Autentificarea multifactorială (MFA) a devenit din ce în ce mai comună. În această abordare, autentificarea necesită două sau mai multe mijloace independente de verificare. De exemplu, o parolă poate fi combinată cu un cod care este trimis printr-un mesaj text. Software-ul sau dispozitivele separate pot fi folosite pentru a genera jetoane care sunt bune pentru o singură utilizare. Aceste valori de simbol, atunci când sunt furnizate cu o parolă, oferă un nivel suplimentar de securitate care împiedică utilizarea parolelor care au fost ghicite sau furate de actorii amenințărilor.

În general, atacurile de acces pot fi detectate prin revizuirea jurnalelor, utilizarea lățimii de bandă și încărcările proceselor. Politica de securitate a rețelei ar trebui să specifice că jurnalele sunt menținute în mod oficial pentru toate dispozitivele și serverele din rețea. Prin examinarea jurnalelor, personalul de securitate al rețelei poate determina dacă a avut loc un număr neobișnuit de încercări eșuate de conectare.

#### 3.4.6 - Mitigating DoS Attacks

Unul dintre primele semne ale unui atac DoS este un număr mare de plângeri ale utilizatorilor cu privire la resursele indisponibile sau la performanța rețelei neobișnuit de lentă. Pentru a minimiza numărul de atacuri, un pachet software de utilizare a rețelei ar trebui să ruleze în permanență. Analiza comportamentului rețelei poate detecta modele neobișnuite de utilizare care indică faptul că are loc un atac DoS. Un mijloc de detectare a comportamentului neobișnuit al rețelei ar trebui să fie cerut de politica de securitate a rețelei a organizației. Un

grafic de utilizare a rețelei care arată o activitate neobișnuită ar putea indica, de asemenea, un atac DoS.

Atacurile DoS ar putea fi o componentă a unei ofensive mai mari. Atacurile DoS pot duce la probleme în segmentele de rețea ale computerelor atacate. De exemplu, capacitatea de pachete pe secundă a unui router între internet și o rețea LAN ar putea fi depășită de un atac, compromițând nu numai sistemul țintă, ci și dispozitivele de rețea prin care trebuie să treacă traficul. Dacă atacul este efectuat la o scară suficient de mare, regiuni geografice întregi de conectivitate la internet ar putea fi compromise.

Din punct de vedere istoric, multe atacuri DoS au fost provenite din adrese falsificate. Routerelor și switch-urile Cisco acceptă o serie de tehnologii anti-spoofing, cum ar fi securitatea porturilor, snoopingul Dynamic Host Configuration Protocol (DHCP), IP Source Guard, Dynamic Address Resolution Protocol (DAI) Inspection și listele de control al accesului (ACL).

## 3.5 Cisco Network Foundation Protection Framework

### 3.5.1 - NFP Framework

Cadrul Cisco Network Foundation Protection (NFP) oferă linii directoare complete pentru protejarea infrastructurii de rețea. Aceste linii directoare formează baza pentru furnizarea continuă a serviciilor.

NFP împarte în mod logic routerelor și comutatoarele în trei zone funcționale, așa cum se arată în figură:

1. **Plan de control** - Responsabil pentru rutarea corectă a datelor. Traficul planului de control constă din pachete generate de dispozitive necesare pentru funcționarea rețelei în sine, cum ar fi schimburile de mesaje ARP sau anunțurile de rutare OSPF.
2. **Plan de management** - Responsabil cu gestionarea elementelor de rețea. Traficul planului de management este generat fie de dispozitivele de rețea, fie de stațiile de gestionare a rețelei folosind procese și protocoale precum Telnet, SSH, TFTP, FTP, NTP, AAA, SNMP, syslog, TACACS+, RADIUS și NetFlow.
3. **Data plane (Forwarding plane)** - Responsabil cu transmiterea datelor. Traficul planului de date constă în mod normal în pachete generate de utilizator care sunt transmise între dispozitivele finale. Majoritatea traficului circulă prin router sau comutator prin intermediul avionului de date.

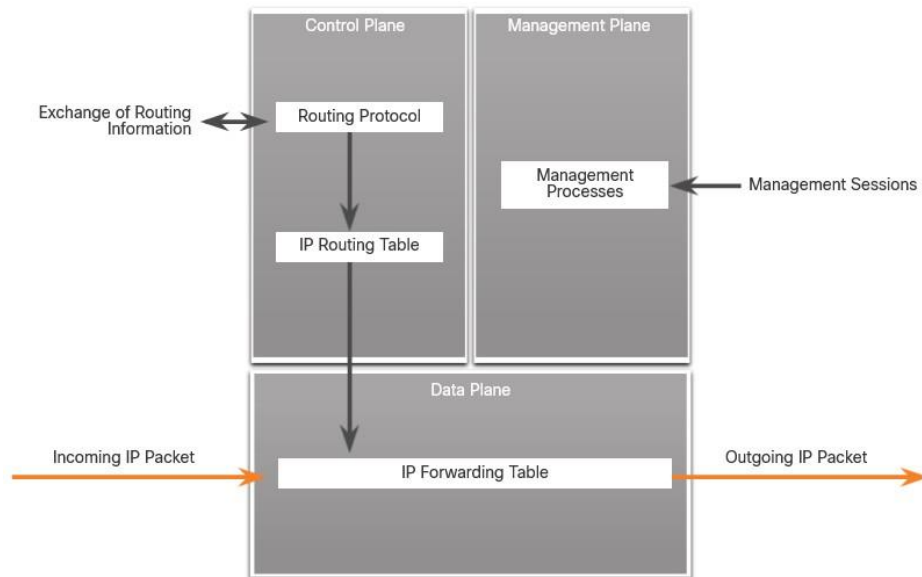


Fig. 3.8. NFP.

### 3.5.2 - Securing the Control Plane

Traficul planului de control constă din pachete generate de dispozitive necesare pentru funcționarea rețelei în sine.

Securitatea planului de control poate fi implementată folosind următoarele caracteristici, așa cum se arată în figură:

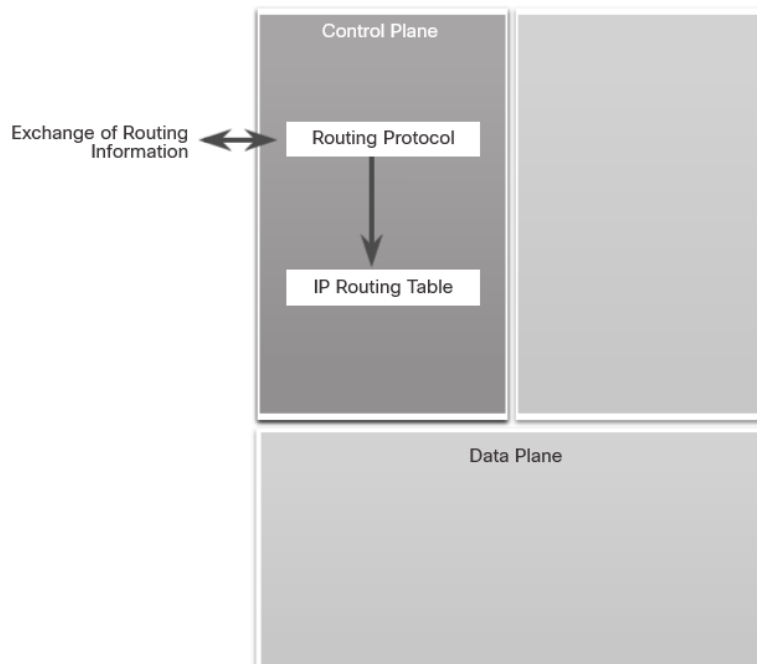


Fig. 3.9. Control Plane.

**Autentificarea protocolului de rutare** - Autentificarea protocolului de rutare sau autentificarea vecinului împiedică un router să accepte actualizări frauduloase de rutare. Majoritatea protocoalelor de rutare acceptă autentificarea vecinului.

**Control Plane Policing (CoPP)** - CoPP este o caracteristică Cisco IOS concepută pentru a permite utilizatorilor să controleze fluxul de trafic care este gestionat de procesorul de rută al unui dispozitiv de rețea.

**AutoSecure** - AutoSecure poate bloca funcțiile planului de management și serviciile și funcțiile planului de redirecționare ale unui router.

CoPP este conceput pentru a preveni traficul inutil să copleșească procesorul de rută. Caracteristica CoPP tratează planul de control ca pe o entitate separată cu propriile porturi de intrare (intrare) și ieșire (ieșire). Un set de reguli poate fi stabilit și asociat cu porturile de intrare și ieșire ale planului de control.

### 3.5.3 - Securing the Management Plane

Traficul planului de management este generat fie de dispozitivele de rețea, fie de stațiile de gestionare a rețelei care utilizează procese și protocoale precum Telnet, SSH și TFTP, etc. Planul de management este o țintă foarte atractivă pentru hackeri. Din acest motiv, modulul de management a fost construit cu mai multe tehnologii menite să atenueze astfel de riscuri.

Fluxul de informații dintre gazdele de gestionare și dispozitivele gestionate poate fi în afara benzii (OOB), în cazul în care informațiile circulă într-o rețea în care nu există trafic de producție. Poate fi, de asemenea, în bandă, unde informațiile circulă prin rețeaua de producție a întreprinderii, internetul sau ambele.

Securitatea planului de management poate fi implementată folosind următoarele caracteristici, așa cum se arată în figură:

**Politica de conectare și parole** - Restricționează accesibilitatea dispozitivului. Limitează porturile accesibile și restricționează metodele de acces „cine” și „cum”.

**Prezentarea notificării legale** - Afișează notificări legale. Acestea sunt adesea dezvoltate de consilierul juridic al unei corporații.

**Asigurarea de confidențialitate a datelor** - Protejează datele sensibile stocate local de a fi vizualizate sau copiate. Utilizează protocoale de management cu autentificare puternică pentru a atenua atacurile de confidențialitate care vizează expunerea parolelor și a configurațiilor dispozitivelor.

**Controlul accesului bazat pe roluri (RBAC)** - Se asigură că accesul este acordat numai utilizatorilor, grupurilor și serviciilor autentificate. RBAC și serviciile de autentificare, autorizare și contabilitate (AAA) oferă mecanisme pentru a gestiona eficient controlul accesului.

**Autorizare de acțiuni** - Restricționează acțiunile și vizualizările care sunt permise de un anumit utilizator, grup sau serviciu.

**Activarea raportelor accesului de gestionare** - Jurnale și conturi pentru toate accesul. Înregistrează cine a accesat dispozitivul, ce s-a întâmplat și când a avut loc.

RBAC restricționează accesul utilizatorului în funcție de rolul utilizatorului. Rolurile sunt create în funcție de funcțiile de job sau de sarcină și sunt atribuite permisiuni de acces pentru anumite active. Utilizatorii sunt apoi alocați unor roluri și li se acordă permisiunile care sunt definite pentru acel rol.

În Cisco IOS, caracteristica de acces CLI bazată pe roluri implementează RBAC pentru accesul de gestionare a routerului. Caracteristica creează diferite „vizualizări” care definesc ce comenzi sunt acceptate și ce informații de configurare sunt vizibile. Pentru scalabilitate, utilizatorii, permisiunile și rolurile sunt de obicei create și menținute într-un server de depozit central. Acest lucru face ca politica de control al accesului să fie disponibilă pentru mai multe dispozitive. Serverul de depozit central poate fi un Cisco Identity Services Engine (ISE) care poate oferi servicii de rețea de autentificare, autorizare și contabilitate (AAA).

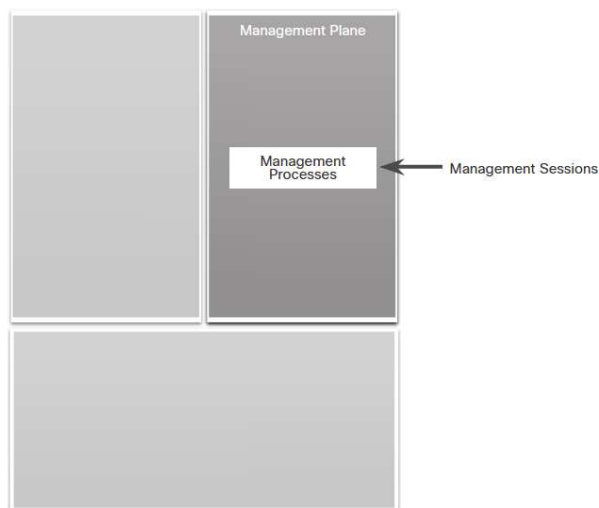


Fig. 3.10. Management Plane.

### 3.5.4 - Securing the Data Plane

Traficul din planul de date constă în cea mai mare parte din pachete de utilizator transmise prin router prin planul de date. Securitatea planului de date poate fi implementată folosind ACL-uri, mecanisme anti-spoofing și caracteristici de securitate Layer 2, așa cum se arată în figură.

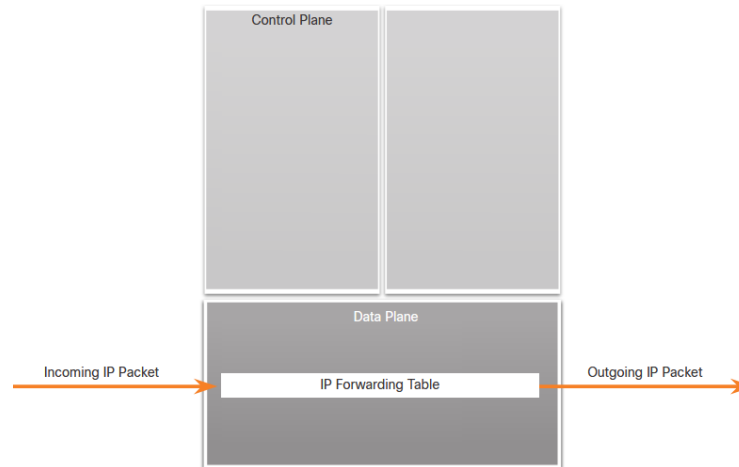


Fig. 3.11. Data Plane.

ACL-urile efectuează filtrarea pachetelor pentru a controla ce pachete se deplasează prin rețea și unde le este permis să ajungă. ACL-urile sunt folosite pentru a securiza planul de date într-o varietate de moduri:

- **Blocarea traficului nedorit sau a utilizatorilor** - ACL-urile pot filtra pachetele de intrare sau de ieșire pe o interfață. Acestea pot fi utilizate pentru a controla accesul pe baza adreselor sursă, adreselor de destinație sau a autentificării utilizatorilor.
- **Reducerea șanselor de atacuri DoS** - ACL-urile pot fi utilizate pentru a specifica dacă traficul de la gazde, rețele sau utilizatori poate accesa rețeaua. Caracteristica de interceptare ASA TCP este un mecanism care poate fi folosit pentru a proteja gazdele finale, în special serverele, de atacurile TCP SYN-flooding.
- **Atenuarea atacurilor de falsificare** - ACL-urile permit practicienilor în securitate să implementeze practici recomandate pentru a atenua atacurile de falsificare.
- **Asigurarea controlului lășimii de bandă** - ACL-urile pe o legătură lentă pot preveni traficul în exces.
- **Clasificarea traficului pentru a proteja planurile de management și control** - ACL-urile pot fi aplicate pe liniile vty.

ACL-urile pot fi, de asemenea, utilizate ca mecanism antispoofing prin eliminarea traficului care are o adresă sursă nevalidă. Aceasta înseamnă că atacurile trebuie inițiate de la adrese IP valide, accesibile, ceea ce permite ca pachetele să fie urmărite până la inițiatorul unui atac.

Caracteristici, cum ar fi Unicast Reverse Path Forwarding (uRPF), pot fi utilizate pentru a completa strategia antispoofing.

Switch-urile Cisco Catalyst pot folosi funcții integrate pentru a ajuta la securizarea infrastructurii de nivel 2. Următoarele instrumente de securitate de nivel 2 sunt integrate în comutatoarele Cisco Catalyst:

***Securitate port*** - Previne falsificarea adreselor MAC și atacurile de inundare a adreselor MAC.

***Snooping DHCP*** - Previne atacurile clientului asupra serverului și comutatorului DHCP.

***Inspecție dinamică ARP (DAI)*** - Adaugă securitate ARP prin utilizarea tabelului de snooping DHCP pentru a minimiza impactul atacurilor de otrăvire și falsificare ARP.

***IP Source Guard (IPSG)*** - Previne falsificarea adreselor IP prin utilizarea tabelului de snooping DHCP.



## Laborator 2

- **Pași Configurare Host PC:**

**End Devices → PC:**

Pas1: Nume **ARAD** (majuscule neapărat)

Pas2: Click pe PC; Power OFF; Scoatem placa de rețea; Punem placa **PT-HOST-NM-1CGE**, Power ON

Pas3: **Desktop → IP Configuration**

(Ipv4: **192.168.100.164**

S.M.: **255.255.255.224**

D.Gw.: **192.168.100.161** (cel mai mic IP din RA)

DNS: **209.165.201.254** (cel mai mare IP din RA))

Pas4: **Desktop → Email**

(Name: **ARAD**

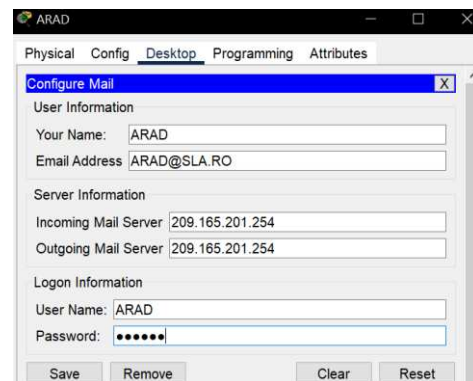
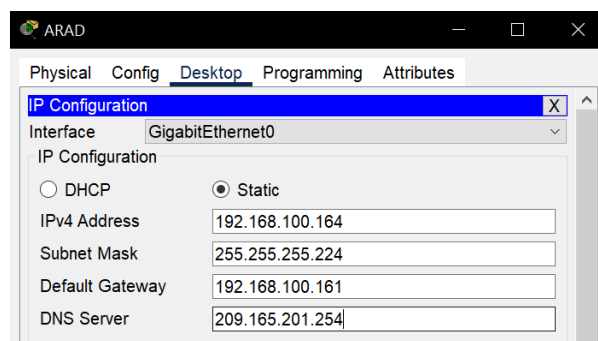
Email: **ARAD@SLA.RO**

Incoming/Outcoming Mail Server: **209.165.201.254** (DNS)

User: **ARAD**

Password: **123456**

**SAVE** )



- **Pași Configurare Laptop SERVICE:**

**End Devices → Laptop:**

Pas1: Nume **SERVICE** (majuscule neapărat)

**Connections → Console** (firul albastru):

Pas1: Capăt **RS232** în laptop **SERVICE** și capăt **Console** în echipamentul pe care dorim să îl configurăm.



Pas2: **Laptop → Desktop → Terminal → Ok** și de aici vom introduce sintaxa de configurare a echipamentelor.

*!!! Atenție: Vom refolosi laptopul și firul pentru toate echipamentele pe care dorim să le configurăm (nu vom lua/defini unele noi).*

- **Pași Configurare Switch 2960:**

Pas1: Nume **SWARAD**

Pas2: Trebuie să cunoaștem **IP-ul switch-ului** (luăm **D.Gw. + 1** – sau cea mai apropiată adresă liberă de D.Gw.) și **S.M.** de la **PC**.

Pas3: Introducem următoarea sintaxă din laptopul **SERVICE**, după ce ne conectăm la **SWARAD**.

Sintaxă Switch (ce este după // sau ---, sunt comentarii):

*Enter*

```
SWARAD> enable // mod user
SWARAD# configure terminal // mod privilegiat
SWARAD (config)# no ip domain-lookup // ca să nu se blocheze echipamentul când greșim
SWARAD (config)# hostname SWARAD
SWARAD (config)# no cdp run
SWARAD (config)# service password-encryption // criptare parole
SWARAD (config)# enable secret ciscosecpa55 // parola puternică
SWARAD (config)# enable password ciscoenapa55 // back-up parolă pt. cea de sus
SWARAD (config)# banner motd #Vineri, la 14.00, serverul va fi oprit!#
----- (conexiune locală, prin cablul Consolă/Rollover)
SWARAD (config)# line console 0
SWARAD (config-line)# password ciscoconpa55
SWARAD (config-line)# login // cere parolă la logare
SWARAD (config-line)# logging synchronous // ne întoarcem de unde am rămas în caz update
SWARAD (config-line)# exec-timeout 25 25 // în stand-by după 25 min și 25 sec
SWARAD (config-line)# exit
----- (conexiune virtuală, de la distanță)
SWARAD (config)# line vty 0 15
SWARAD (config-line)# password ciscovtypa55
SWARAD (config-line)# login
```

SWARAD (config-line)# logging synchronous

SWARAD (config-line)# exec-timeout 10 10

SWARAD (config-line)# end

----- (dată și oră)

SWARAD# copy running-config startup-config // SAVE (de câte ori vrem)

SWARAD# clock set 20:05:32 11 Oct 2022

SWARAD# configure terminal

----- (configurare SSH)

SWARAD (config)# ip domain name SLA.RO

SWARAD (config)# username Admin01 privilege 15 secret Admin01pa55 // admin SSH cu toate drepturile

SWARAD (config)# line vty 0 15

SWARAD (config-line)# transport input ssh

SWARAD (config-line)# login local

SWARAD (config-line)# exit

SWARAD (config)# crypto key generate rsa → 2048 (scriem)

----- (configurare interfață VLAN)

SWARAD (config)# interface vlan 1

SWARAD (config-if)# description Legatura cu LAN 192.168.100.160/27 // N.A.

SWARAD (config-if)# ip address 192.168.100.162 255.255.255.224 // IP\_SWARAD S.M.

SWARAD (config-if)# no shutdown // activare interfață

----- (dacă greșim IP)

SWARAD (config-if)# no ip address // și revenim de la ip address...

Pas4: **Connections → Copper Straigh-Through** (firul negru, drept; al 3-lea) și legăm **SWARAD** la **ARAD**.

Pas5: **PC (ARAD) → Desktop → Command Prompt** (ca să verificăm că există conexiune:

ping 192.168.100.162

ssh -l Admin01 192.168.100.162 → parola: Admin01pa55)

- **Pași Configurare Router 2911:**

Pas1: Nume **RARAD**

Pas2: Trebuie să cunoaștem **IP-ul router-ului** (luăm **D.Gw.**) și **S.M.**

Pas3: Introducem următoarea sintaxă din laptopul **SERVICE**, după ce ne conectăm la **RARAD**.

Sintaxă Router (similar cu ce avem la Switch, ce este diferit, va fi marcat cu roșu și !):

*Enter*

```
RARAD> enable // mod user
RARAD# configure terminal // mod privilegiat
RARAD (config)# no ip domain-lookup // ca să nu se blocheze echipamentul când greșim
RARAD (config)# hostname RARAD
RARAD (config)# no cdp run
RARAD (config)# service password-encryption // criptare parole
!RARAD (config)# security passwords min-length 10
!RARAD (config)# login block-for60 attempts 3 within 15
RARAD (config)# enable secret ciscosecpa55 // parola puternică
RARAD (config)# enable password ciscoenapa55 // back-up parolă pt. cea de sus
RARAD (config)# banner motd #Vineri, la 14.00, serverul va fi oprit!#
!RARAD (config)# banner login #Accesul persoanelor neautorizate complet interzis!#
----- (conexiune locală, prin cablul Consolă/Rollover)
RARAD (config)# line console 0
RARAD (config-line)# password ciscoconpa55
RARAD (config-line)# login // cere parolă la logare
RARAD (config-line)# logging synchronous // ne întoarcem de unde am rămas în caz update
RARAD (config-line)# exec-timeout 25 25 // în stand-by după 25 min și 25 sec
RARAD (config-line)# exit
----- (conexiune virtuală, de la distanță)
RARAD (config)# line vty 0 15
RARAD (config-line)# password ciscovtypa55
RARAD (config-line)# login
RARAD (config-line)# logging synchronous
RARAD (config-line)# exec-timeout 10 10
RARAD (config-line)# end
----- (dată și oră)
RARAD# copy running-config startup-config // SAVE (de câte ori vrem)
```

RARAD# clock set 20:05:32 11 Oct 2022

RARAD# configure terminal

----- (configurare SSH)

RARAD (config)# ip domain name SLA.RO

RARAD (config)# username Admin01 privilege 15 secret Admin01pa55 // admin SSH cu toate drepturile

RARAD (config)# line vty 0 15

RARAD (config-line)# transport input ssh

RARAD (config-line)# login local

RARAD (config-line)# exit

RARAD (config)# crypto key generate rsa → 2048 (scriem)

----- (configurare interfață VLAN) → NU AVEM LA ROUTER

~~RARAD (config)# interface vlan 1~~

~~RARAD (config-if)# description Legatura cu LAN 192.168.100.160/27 // N.A.~~

~~RARAD (config-if)# ip address 192.168.100.162 255.255.255.224 // IP\_RARAD S.M.~~

~~RARAD (config-if)# no shutdown // activare interfață~~

----- (configurare interfață Gigabit)

!RARAD (config)# interface Gigabitethernet 0/0

!RARAD (config-if)# description Legatura cu LAN 192.168.100.161/27 // D.Gw.

!RARAD (config-if)# ip address 192.168.100.161 255.255.255.224 // IP\_RARAD S.M.

!RARAD (config-if)# no shutdown // activare interfață

Pas4: Connections → Copper Straight-Through (firul negru, drept; al 3-lea) și legăm RARAD la SWARAD.

Pas5: PC (ARAD) → Desktop → Command Prompt (ca să verificăm că există conexiune:

ping 192.168.100.161

ssh -l Admin01 192.168.100.161 → parola: Admin01pa55)

!!! Atentie: Între echipamente de același fel, folosim cablul cross-over (linie dreaptă, neagră, întretăiată), iar pentru cele diferite, cu diferență de layere = 1 (OSI), folosim cablul straight-through (linie dreaptă, neagră).

# Bonus: Proiect Educațional – „Și școala poate fi frumoasă!”

Proiectul realizat împreună cu colegii mei în mai 2022 poate fi accesat [aici](#).

## Cuprins

Echipa de proiect /

București – Mai 2022

## Proiect Educațional

„Și școala poate fi frumoasă!”

Motto: „Copiii nu trebuie să fie dresați în mod mecanic, ci să fie învățați să gândească.” - (Immanuel Kant)

Numele Instituției Participante:  
Liceul Teoretic „Ioan Petruș”

## 1. Motivație

Transformarea digitală a României este accelerată de progresul tehnologic rapid pe plan mondial. Acesta este motivul pentru care toată lumea trebuie să investească în abilitățile digitale de-a lungul vieții.

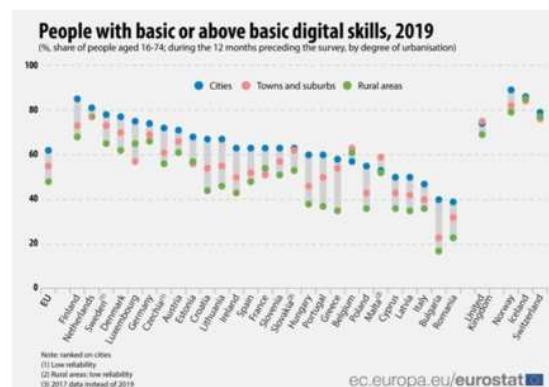
Adaptarea sistemelor de educație la evoluțiile tehnologice este un proces complex și un element important al modernizării cadrului predare-învățare. Utilizarea noilor tehnologii digitale este o modalitate imediată de a face școlile mai atractive pentru elevi, mai eficiente în dezvoltarea competențelor și în promovarea învățării pe tot parcursul vieții.

Impactul transformării digitale asupra societății și a piețelor muncii, precum și asupra sistemelor de educație și formare, este din ce în ce mai evident. Criza „Covid-19” a reconfigurat practicile educaționale de la interacțiunea „față-în-față” la mediul online. Astfel, s-a pus în centrul atenției faptul că predarea, învățarea și tehnologia emergentă conturează viitorul educației digitale. Acest aspect a evidențiat rolul educației digitale ca obiectiv-cheie pentru predarea-învățarea-evaluarea de înaltă calitate.

## 2. Argument

Ediția din noiembrie 2020 a Monitorului Educației și Formării, respectiv raportul de țară pentru România prezintă o realitate cunoscută. Conform datelor Eurostat, în anul 2019 nu mai puțin de 43% dintre românii cu vârste între 16-74 de ani aveau competențe digitale reduse, clasând România pe primul loc în Uniunea Europeană la acest capitol, Bulgaria (38%) fiind pe locul al doilea. La capitolul persoane cu abilități digitale superioare, datele arată că doar 10% din populație stăpânește asemenea competențe, România fiind și de această dată pe ultimul loc în Uniunea Europeană, Bulgaria având 11% în dreptul acestui indicator.

Potrivit Eurostat, în 2019, patru din cinci tineri (80%) cu vârste cuprinse între 16 și 24 de ani în Uniunea Europeană (UE) aveau abilități digitale de bază sau peste acestea. Cifra este cu 24 de puncte procentuale (pp) mai mare decât ponderea persoanelor cu vârste cuprinse între 16 și 74 de ani (56%).



Schema 2.1.

Tinerii din România sunt pe ultimul loc în UE la acest capitol, doar 56% dintre ei având competențe digitale de bază sau peste nivelul de bază, arată datele publicate de Eurostat. Această realitate susține încă o dată nevoia și importanța investiției în dezvoltarea competențelor digitale la elevi și studenți.

Din această perspectivă, considerăm imperios să investim în viitorul generațiilor de copii și, prin pași mici, dar constanți, să producem o schimbare în direcția digitalizării sistemului de învățământ. De aceea, Liceul Teoretic „Ioan Petruș” își propune să reprezinte un prim pas către această țintă.

Link: <https://www.edu.ro/sites/default/files/SMART.Edu%20-%20document%20consultare.pdf>



## Bonus: Examenе de luat acasă (Temă Seminar)

Acestea sunt un tip special de examen, în care sunt permise materiale ajutătoare, unde profesorul oferă studenților foaia cu subiectele, iar elevii au un timp predeterminat de a le rezolva, departe de centrul de examinare, de obicei, în confortul propriei case. De obicei, acest tip de examinare are o perioadă mai mare de desfășurare (24-48 de ore în general) și este mai dificil, solicitând capacitatea copiilor de a gândi și a găsi soluții, în contrast cu testele clasice scrise, care, în învățământul românesc, pun accentul, în special, pe memorare.

Probabil, cel mai puternic argument pentru implementarea acestui tip de examen face referire la faptul că este foarte similar cu un scenariu din viața reală (ex: la job trebuie să îndeplinim anumite task-uri și avem la dispoziție orice fel de resurse și o perioadă determinată când trebuie să terminăm).

Un [studiu](#) din 2019 prezintă următoarele avantaje (comparație între mai multe articole pe aceeași temă) pentru adoptarea acestei forme de evaluare la universitate (vom prezenta doar câteva dintre ele):

- Reduce stresul studenților și își pot alege spațiul și timpul;
- Oferă o oportunitate bună de învățare;
- Studenții petrec mai mult timp pe un astfel de examen, decât pe cel standard de 2 ore;
- Contribuie la crearea unui mediu mai interactiv de învățare;
- Promovează procesul educațional dincolo de cel de memorare;
- Norocul este exclus;
- Împinge elevii să consulte alte texte în afară de materialele de curs;
- Încurajează gândirea și analiza critică.

Câteva dintre dezavantaje, prezentate în același studiu, sunt:

- Sunt ușor de compromis de comportamentul neetic al elevilor;
- Studenții vor participa la mai puține cursuri;
- Studenții vânează doar răspunsurile;
- Subminează învățarea pe termen lung.

Din punctul meu de vedere, acest tip de evaluare este mult mai realistă: studenții nu trebuie să rețină informații și să le reproducă. Trebuie să folosească ce au învățat (deci, mai întâi, să înțeleagă – și nu este necesar să participe la cursuri pentru a pricepe materia, iar aici mă gândesc la suficiente cadre didactice din mediul universitar care nu au talent pedagogic și care nici nu își dau interesul ca să se asigure că studenții reușesc să țină pasul cu informațiile prezentate; de asemenea, problema cu participarea la ore nu se ridică dacă profesorul știe cum să abordeze clasa și să relaționeze cu studenții – vorbesc aici din experiență proprie) și să analizeze critic, încercând să găsească cea mai bună soluție de rezolvare. De asemenea, munca în echipă ar trebui încurajată, mai ales că în viața reală nu știu câte job-uri necesită să lucrezi singur, fără o echipă pe care să te bazezi, dar în domeniul informaticii, acest lucru iese din discuție.

În urma celor 5 ani de studenție, consider că cele mai eficiente metode de evaluare sunt cele practice sau cele care te îndeamnă să gândești creativ, proactiv și reactiv (proiecte, referate, examene de luat acasă etc...).

## Bonus: Proiect Didactic (Temă Seminar)

Școala de aplicație: -

Disciplina: Informatică

Clasa: a XI-a

Data: -

Student practicant:

[REDACTED]

Profesor îndrumător: -

### PROIECT DIDACTIC

**Unitatea de învățare:** Înregistrarea

**Subiectul lecției:** Aplicații în C++ folosind variabile de tip înregistrare

**Tipul lecției:** Lecție de fixare și sistematizare

#### Competențe specifice vizate:

C1: Cunoașterea și identificarea elementelor care țin de sintaxa înregistrărilor.

C2: Identificarea problemelor care se rezolvă cu ajutorul înregistrărilor.

C3: Rezolvarea de aplicații practice.

#### Obiectivele operaționale ale lecției:

O1: La sfârșitul lecției, elevii vor fi capabili să definească și să folosească corect variabilele de tip „struct”.

O2: La sfârșitul lecției, elevii vor fi capabili să identifice și să rezolve probleme cu ajutorul înregistrărilor.

**Locul de desfășurare a lecției:** Laboratorul de Informatică

#### Desfășurarea lecției

<i>Nr. crt</i>	<i>Etapele lecției</i>	<i>INDICATIVUL OBIECTIVULUI (ELOR) OPERAȚIONAL(E) VIZAT(E)</i>	<i>Timp alocat (minute)</i>	<i>ACTIVITATEA PROFESORULUI</i>	<i>ACTIVITATEA ELEVILOR (ce vor face concret în fiecare etapă)</i>	<i>METODE, PROCEDEE DIDACTICE ȘI MIJLOACE DE ÎNVĂȚĂMÂNT UTILIZATE</i>	<i>MODALITĂȚI DE EVALUARE (tipul de evaluare, metoda, instrumentul de evaluare folosit în fiecare etapă a lecției)</i>
1.	Momentul organizatoric		5	-Salută elevii; -Notează absenții; -Cere elevilor să deschidă aplicația Kahoot.	-Salută profesorul; -Elevul de serviciu dă absenții, dacă sunt; -Își pornesc aplicația Kahoot și așteaptă	-Conversație.	



					următoarele indicații ale profesorului.		
2.	<b>Enunțarea subiectului și a obiectivelor lecției</b>		5	-Enunță tema lecției “Aplicații în C++ folosind înregistrările”; -Prezintă obiectivele urmărite: 1. Identificarea și definirea propriilor înregistrări; 2. Identificarea problemelor care se rezolvă folosind structurile; 3. Rezolvarea de aplicații practice.	-Notează titlul temei în caiet; -Sunt atenți la ceea ce spune profesorul.	-Expoziție.	-Observarea elevilor.
3.	<b>Verificarea cunoștințelor și deprinderilor anterioare dobândite</b>	O1	5	-Rezolvarea competiției Kahoot și explicarea întrebărilor care au pus în dificultate elevii.	-Participă la competiția Kahoot și răspund la întrebările din aceasta; -Sunt atenți la explicațiile profesorului; -Pun întrebări unde au nelămuriri.	-Competiție de verificare a cunoștințelor; -Explicație..	-Chestionare prin intermediul aplicației Kahoot; -Aprecieri verbale.
4.	<b>Fixarea noilor cunoștințe</b>	O1+O2	30	-Rezolvarea exercițiilor din „Anexa 1”, cu ajutorul elevilor. -Răspunde la eventualele nelămuriri ale elevilor.	-Urmăresc profesorul și participă la rezolvarea aplicațiilor practice; -Pun întrebări unde au nelămuriri.	-Conversație; -Explicație; -Exercițiu;	-Chestionare orală; -Aprecieri verbale; -Observarea elevilor.
5.	<b>Anunțarea și explicarea temei pentru acasă</b>	O1+O2	5	-Anunță că vor avea o temă; -Tema: Rezolvarea exercițiilor din „Anexa 1” care au rămas nerezolvate.	-Își notează tema.	-Explicație;	

Anexa 1:

# Structuri



## 1. Noțiuni Generale:

**Definiție:** *Structura* este un tip de dată definită de utilizator, care reunește un grup de variabile între care există o legătură de conținut, sub același nume.



**Sintaxă Generală:** *struct* ~nume\_structură~

{

<tip\_dată1> ~nume\_variabilă1~, ~nume\_variabilă1~, ...;

<tip\_dată2> ~nume\_variabilă2~, ~nume\_variabilă2~, ...;

.....  
<tip\_datăn> ~nume\_variabilă3~, ~nume\_variabilă3~, ...;

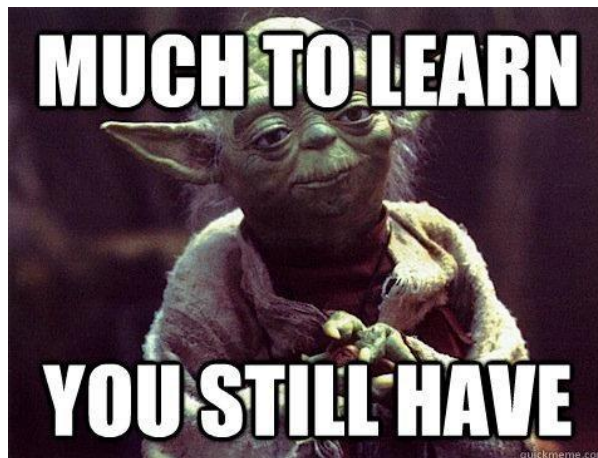
};

unde “<tip\_dată1> ~nume\_variabilă1~, ~nume\_variabilă1~, ...;” se numește *câmp de înregistrare* sau *membru al înregistrării*. În acest material, vom folosi exclusiv denumirea de “membru”.

**De reținut:** O structură **poate** avea ca membru o **funcție** (**doar în C++**; în C, acest lucru nu este posibil)! Nu este recomandat să folosiți funcții în cadrul structurilor, deoarece



acest aspect este implementat folosind noțiunea de *clasă* din Programarea Orientată pe Obiecte. Pentru mai multe detalii, puteți să vizitați acest [link](#).



**Exemplu de funcție în cadrul unei înregistrări:**

```
1  #include <iostream>
2  using namespace std;
3
4  struct dataNastere
5  {
6      int zi, luna, an;
7
8      bool esteAnBisect(int an);
9  };
10
11 bool dataNastere::esteAnBisect(int an)
12 { return an%4 == 0; }
13
14 int main()
15 {
16     dataNastere X = {20, 12, 2020};
17     if(X.esteAnBisect(X.an)) cout << X.an << " este an Bisect!" << endl;
18     else cout << X.an << " NU este an Bisect!" << endl;
19
20     return 0;
21 }
```

```
main.cpp
11
12 struct dataNastere
13 {
14     int zi, luna, an;
15
16     bool esteAnBisect(int an);
17 };
18
19 bool dataNastere::esteAnBisect(int an)
20 { return an%4 == 0; }
21
22 int main()
23 {
24     dataNastere X = {20, 12, 2020};
25     if(X.esteAnBisect(X.an)) cout<<X.an<<" este an Bisect!"<<endl;
26     else cout<<X.an<<" NU este an Bisect!"<<endl;
27
28     return 0;
29 }
30
```

input

2020 este an Bisect!

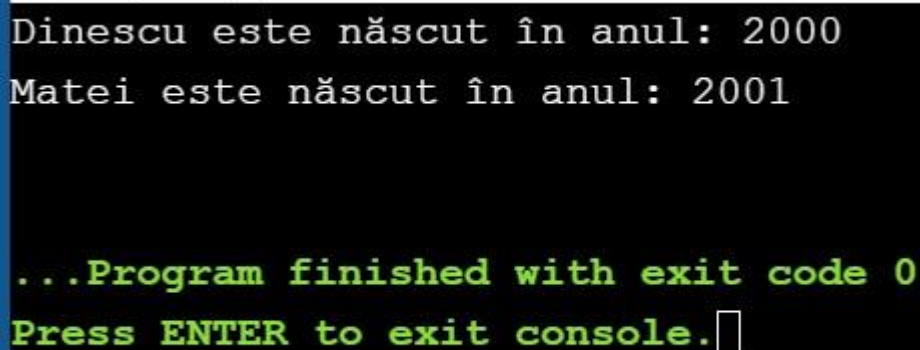
...Program finished with exit code 0  
Press ENTER to exit console.

Un *membru* al unei înregistrări poate fi o *altă înregistrare*. O astfel de înregistrare se numește **structură imbricată**.



Exemplu:

```
1  #include <iostream>
2  using namespace std;
3
4  // Prima Metodă
5  struct dataNastere
6  {
7  int zi, luna, an;
8  };
9  struct elev1
10 {
11 char nume[30], prenume[50];
12 dataNastere data;
13 };
14
15 // A doua Metodă
16 struct elev2
17 {
18 char nume[30], prenume[50];
19 struct { int zi, luna, an; } dataN;
20 };
21
22 int main()
23 {
24 dataNastere data1 = {30, 03, 2000};
25 elev1 X = {"Dinescu", "Ana", data1};
26 cout << X.nume << " este născut în anul: " << data1.an << endl;
27
28 elev2 Y = {"Matei", "Daniel", {17, 02, 2001}};
29 cout << Y.nume << " este născut în anul: " << Y.dataN.an << endl;
30
31
32 return 0;
33 }
```



```
Dinescu este născut în anul: 2000
Matei este născut în anul: 2001

...Program finished with exit code 0
Press ENTER to exit console.█
```

Putem declara și *tablouri de structuri*. Exemplu:

```
1  struct dataNastere
2  {
3  int zi, luna, an;
4  } date[50];
```

## 2. Bune Practici:

Avem următoarele 2 înregistrări:

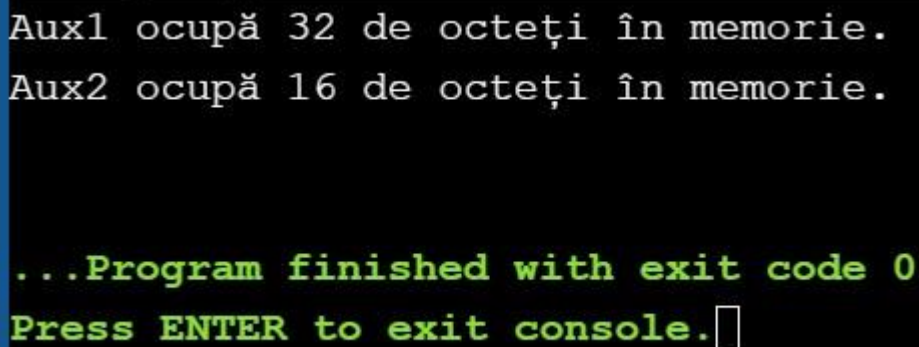
```
1 struct aux1
2 {
3     char c;
4     int x;
5     char t;
6     double y;
7     char z;
8 };
```

```
1 struct aux2
2 {
3     double y;
4     int x;
5     char c, t, z;
6 };
```

La o primă vedere, aceste 2 structuri par identice (ambele au o singură variabilă *double*, ambele au o singură variabilă *int* și ambele au 3 variabile de tip *char*; singura diferență ar fi poziționarea acestora). Dar oare chiar sunt identice? Hai să rulăm următorul cod:

```
1 int main()
2 {
3     cout << "Aux1 ocupă " << sizeof(aux1) << " de octeți în memorie." << endl;
4     cout << "Aux2 ocupă " << sizeof(aux2) << " de octeți în memorie." << endl;
5
6     return 0;
7 }
```

Compilerul afișează:



```
Aux1 ocupă 32 de octeți în memorie.
Aux2 ocupă 16 de octeți în memorie.

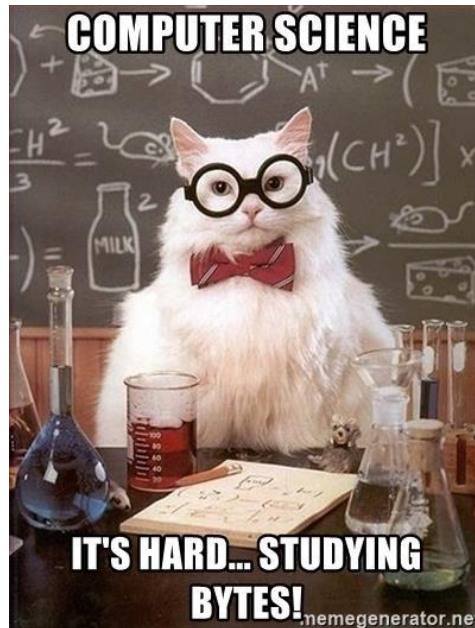
...Program finished with exit code 0
Press ENTER to exit console.
```

Reamintim faptul că: **char = 1 octet; int = 4 octeți; double = 8 octeți**. Dacă calculăm matematic, ar trebui să obținem

$$3 (3 * \text{char}) + 4 (1 * \text{int}) + 8 (1 * \text{double}) = 15,$$

dar nu obținem acest rezultat în niciunul dintre cazuri. Deci, ce se petrece la nivel intern, în memorie?





Pentru a înțelege, trebuie să cunoaștem cele **3 reguli** de aliniere ale câmpurilor în memorie:

- 1) **Primul câmp declarant se consideră la adresa 0.**
- 2) **Oricare câmp se aliniază la o adresă de memorie care reprezintă un număr egal cu un multiplu al dimensiunii tipului său de dată. Dacă câmpul nu este la o adresă de memorie corespunzătoare, atunci se completează cu octeți aleatori (*padding bits*) până se ajunge la un multiplu.**
- 3) **Dimensiunea (în octeți) a unei structuri trebuie să fie egală cu un multiplu al dimensiunii maxime dintre tipurile de date din interiorul structurii (altfel, se completează cu octeți aleatori).**



Să considerăm cele 2 structuri de mai sus.

```

1 struct aux1
2 {
3     char c;
4     int x;
5     char t;
6     double y;
7     char z;
8 };
  
```

Reprezentarea în memorie a lui *aux1*:

1	padding bits			x	t	padding bits								y								z	padding bits							
c				4	1										8															
1																														

Luăm variabilele în ordine. 'c' ocupă un octet, de la adresa 0 la adresa 1 (conform regulei 1).



‘x’ este variabilă de tip *int*, deci va ocupa 4 octeți. Conform [regulei 2](#), ‘x’ trebuie să se afle în memorie, la o adresă multiplu de 4. Prima adresă multiplu de 4 disponibilă este 4, deci vom ocupa adresele de memorie 1-2, 2-3 și 3-4 cu *biți de padding*, iar de la adresa 4 până la 8 vom avea pe ‘x’. Continuăm cu această regulă pentru fiecare variabilă. La final, conformei [regulei 3](#), *aux1* trebuie să ocupe în memorie un număr de octeți egal cu multiplu de 8 (deoarece cea mai mare dimensiune o ocupă *double*, care are 8 biți); deci completăm cu *octeți aleatori* până la adresa **32**.

```

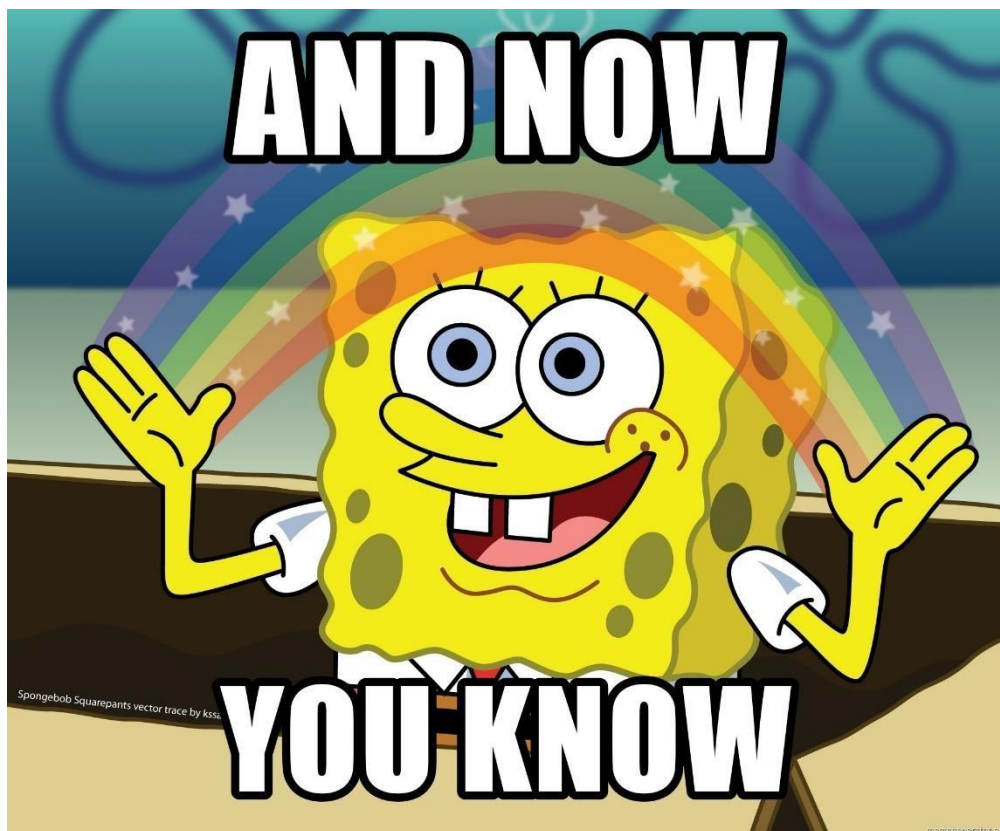
1 struct aux2
2 {
3     double y;
4     int x;
5     char c, t, z;
6 };

```

Și acum reprezentăm în memorie pe *aux2*:

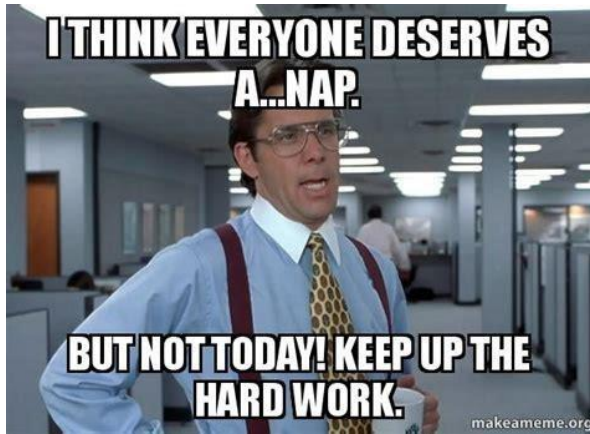
y								x				c	t	z	p.b.
8								4				1	1	1	
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16

**De reținut:** Pentru a utiliza cât mai *eficient memoria*, în *structură*, vom declara câmpurile în ordinea descrescătoare a dimensiunii tipurilor de date, așa cum este prezentat *aux2*!





### 3. Aplicații:



**3.1.** Se citesc de la tastatură 2 numere complexe. Să se implementeze operațiile de adunare, scădere, înmulțire și împărțire.

**Aspecte Preliminarii:** Detalii despre lucrul cu numerele complexe se găsesc la acest [link](#).  
 Dacă  $x = a_1 + b_1i$  și  $y = a_2 + b_2i$  atunci:

- Formulă *Înmulțire*:  $\mathbf{xy} = (\mathbf{a_1a_2} - \mathbf{b_1b_2}) + (\mathbf{a_1b_2} + \mathbf{b_1a_2})i$
- Formulă *Împărțire*:  $\mathbf{x / y} = \frac{(\mathbf{a_1a_2} + \mathbf{b_1b_2}) + (\mathbf{b_1a_2} - \mathbf{a_1b_2})i}{\mathbf{a_2^2} + \mathbf{b_2^2}}$

### Reprezentarea Datelor Problemei:

Putem reprezenta un număr complex astfel:

```
1 struct nrComplex
2 {
3     double r, i; // r -> partea reală; i -> cea imaginară
4 };
```

**Exemplu Date de Intrare:**  $x = 2.5 - 7i$ ;  $y = 7.8 + 2.3i$

**Exemplu Date de Ieșire:**  $x + y = 10.3 - 4.7i$ ;  $x - y = -5.3 - 9.3i$ ;  $xy = 35.6 - 48.85i$ ;

$$x / y = \frac{3.4 - 60.35i}{66.13}$$

**Rezolvare:**

```
1 #include <iostream>
2 #include <math.h>
3 using namespace std;
4
5 struct nrComplex
6 {
7     double r, i; // r -> partea reală; i-> cea imaginară
8 };
9
10 int main()
11 {
12     nrComplex x, y;
13     cout << "x: "; cin >> x.r >> x.i;
14     cout << "y: "; cin >> y.r >> y.i;
```

```

15
16     double aux1, aux2, aux3;
17     aux1 = x.r + y.r;
18     aux2 = x.i + y.i;
19     cout << "x + y = " << aux1;
20     if (aux2 >= 0) cout << '+' << aux2 << 'i' << endl;
21     else cout << aux2 << 'i' << endl;
22
23     aux1 = x.r - y.r;
24     aux2 = x.i - y.i;
25     cout << "x - y = " << aux1;
26     if (aux2 >= 0) cout << '+' << aux2 << 'i' << endl;
27     else cout << aux2 << 'i' << endl;
28
29     aux1 = (x.r * y.r) - (x.i * y.i);
30     aux2 = (x.r * y.i) + (y.r * x.i);
31     cout << "x * y = " << aux1;
32     if (aux2 >= 0) cout << '+' << aux2 << 'i' << endl;
33     else cout << aux2 << 'i' << endl;
34
35     aux1 = (x.r * y.r) + (x.i * y.i);
36     aux2 = (x.i * y.r - x.r * y.i);
37     aux3 = pow(y.r, 2) + pow(y.i, 2);
38     cout << "x / y = " << '(' << aux1;
39     if (aux2 >= 0) cout << '+' << aux2 << "i) / " << aux3 << endl;
40     else cout << aux2 << "i) / " << aux3 << endl;
41
42     return 0;
43 }

```

When I solve the first  
problem with no errors:



**3.2.** Fie  $n \in \mathbb{N}$  și fie  $n$  triplete  $(A_i, B_i, C_i)$  de puncte în plan cu  $i = 1, \dots, n$ . Fiecare punct are coordonatele  $(X, Y)$ , numere reale. Să se afișeze cea mai mare arie a unui triunghi, dacă aceasta există, sau mesajul “Nu există!” dacă niciun triplet de puncte nu formează un triunghi.

### Aspecte Preliminarii:

- Formulă de calcul pentru *lungimea unui segment*, cunoscându-se două puncte:

$$AB = \sqrt{(X_A - X_B)^2 + (Y_A - Y_B)^2}$$

- *Aria unui triunghi*, cunoscând doar lungimea segmentelor ([Formula lui Heron](#)):

$$A_{ABC} = \sqrt{p(p-a)(p-b)(p-c)}; \text{ unde } p = \frac{(a+b+c)}{2} \text{ (semiperimetrul)}$$

- Un *triunghi este valid* dacă *vârfurile acestuia nu sunt coliniare sau identice*, ceea ce este echivalent cu a spune că un *triunghi este valid* dacă *suma oricăror două laturi este diferită de a treia*.

### Reprezentarea Datelor Problemei:

Putem folosi 2 structuri pentru a reprezenta punctele și triunghiurile. Astfel:

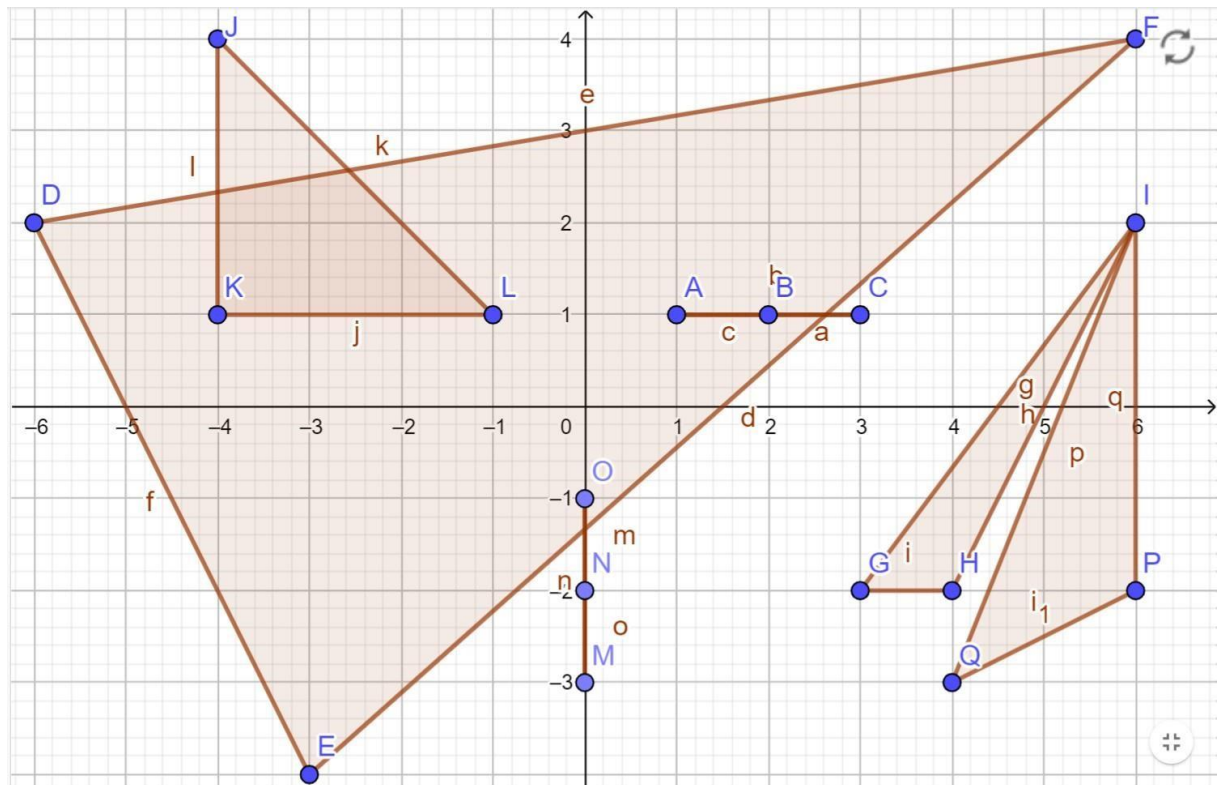
- Pentru punct:

```
struct Punct
{ double X, Y; };
```

- Pentru triunghi:

```
1 struct Triunghi
2 {
3     Punct A, B, C;
4     double AB, BC, AC;
5     double p; //semiperimetru
6     double arie; //arie
7     bool esteValid;
8 };
```

### Exemplu Date de Intrare:



Este evident că aria maximă este cea a triunghiului DEF.

**Rezolvare 1:** Parcurgem tabloul de structuri și reținem aria maximă.

```

1 #include <iostream>
2 #include <math.h>
3 using namespace std;
4
5 struct Punct
6 { double X, Y; };
7 struct Triunghi
8 {
9     Punct A, B, C;
10    double AB, BC, AC;
11    double p; //semiperimetru
12    double arie; //arie
13    bool esteValid;
14 } t[10];
15
16 bool validare(Triunghi &t)
17 {
18     t.AB = sqrt(pow(t.A.X - t.B.X, 2) + pow(t.A.Y - t.B.Y, 2));
19     t.AC = sqrt(pow(t.A.X - t.C.X, 2) + pow(t.A.Y - t.C.Y, 2));
20     t.BC = sqrt(pow(t.B.X - t.C.X, 2) + pow(t.B.Y - t.C.Y, 2));
21
22     // Verificăm dacă este Triunghi
23     if(t.AB + t.BC == t.AC || t.AB + t.AC == t.BC
24        || t.BC + t.AC == t.AB)
25         return false;

```

```

26
27     return true;
28 }
29
30 void calcul(Triunghi &t)
31 {
32     t.p = (t.AB + t.BC + t.AC) / 2;
33     t.arie = sqrt(t.p * (t.p - t.AB) * (t.p - t.BC) * (t.p - t.AC));
34 }
35
36
37
38 int main()
39 {
40     // Date de Intrare
41     t[0] = {{-6, 2}, {-3, -4}, {6, 4}};
42     t[1] = {{-4, 4}, {-4, 1}, {-1, 1}};
43     t[2] = {{-1, 0}, {-2, 0}, {-3, 0}}; // puncte coliniare
44     t[3] = {{1, 1}, {1, 1}, {3, 1}}; // puncte identice
45     t[4] = {{6, 1}, {3, -2}, {4, -2}};
46     t[5] = {{6, 1}, {4, -3}, {6, -2}};
47
48     int i;
49     double maxim = 0;
50     for(i = 0; i < 6; i++)
51         t[i].esteValid = validare(t[i]);
52
53     cout << "Ariile Triunghiurilor: " << endl;
54     for(i = 0; i < 6; i++)
55         if(t[i].esteValid)
56         {
57             calcul(t[i]);
58             cout << i + 1 << ": " << t[i].arie << endl;
59             if (maxim < t[i].arie) maxim = t[i].arie;
60         }
61
62     if(maxim) cout << endl << "Aria Maximă este: " << maxim << endl;
63     else cout << endl << "Nu există!" << endl;
64
65     return 0;
66 }

```

```
Ariile Triunghiurilor:
```

```
1: 39
```

```
2: 4.5
```

```
5: 1.5
```

```
6: 3
```

```
Aria Maximă este: 39
```

**Rezolvare 2:** Sortăm descrescător tabloul de structuri și aria maximă se va afla pe prima poziție. Pentru informații despre sort, accesați acest [link](#).

```

1 #include <iostream>
2 #include <math.h>
3 #include <algorithm> //pentru sort
4 using namespace std;
5
6 struct Punct
7 { double X, Y; };
8 struct Triunghi
9 {
10     Punct A, B, C;
11     double AB, BC, AC;
12     double p; //semiperimetru
13     double arie; //arie
14     bool esteValid;
15 } t[10];
16
17 bool validare(Triunghi &t)
18 {
19     t.AB = sqrt(pow(t.A.X - t.B.X, 2) + pow(t.A.Y - t.B.Y, 2));
20     t.AC = sqrt(pow(t.A.X - t.C.X, 2) + pow(t.A.Y - t.C.Y, 2));
21     t.BC = sqrt(pow(t.B.X - t.C.X, 2) + pow(t.B.Y - t.C.Y, 2));
22
23     // Verificăm dacă este Triunghi
24     if(t.AB + t.BC == t.AC || t.AB + t.AC == t.BC
25        || t.BC + t.AC == t.AB)
26         return false;
27
28     return true;
29 }
30
31 void calcul(Triunghi &t)
32 {
33     t.p = (t.AB + t.BC + t.AC) / 2;
34     t.arie = sqrt(t.p * (t.p - t.AB) * (t.p - t.BC) * (t.p - t.AC));
35 }
36
37 // Funcție de comparare a triunghiurilor folosită la sortare
38 bool compara(Triunghi a, Triunghi b)
39 { return a.arie > b.arie; }
40
41 int main()
42 {
43     // Date de Intrare
44     t[0] = {{-6, 2}, {-3, -4}, {6, 4}};
45     t[1] = {{-4, 4}, {-4, 1}, {-1, 1}};
46     t[2] = {{-1, 0}, {-2, 0}, {-3, 0}}; // puncte coliniare
47     t[3] = {{1, 1}, {1, 1}, {3, 1}}; // puncte identice
48     t[4] = {{6, 1}, {3, -2}, {4, -2}};
49     t[5] = {{6, 1}, {4, -3}, {6, -2}};
50
51     int i;
52     for(i = 0; i < 6; i++)
53         t[i].esteValid = validare(t[i]);
54
55     for(i = 0; i < 6; i++)
56         if(t[i].esteValid)

```



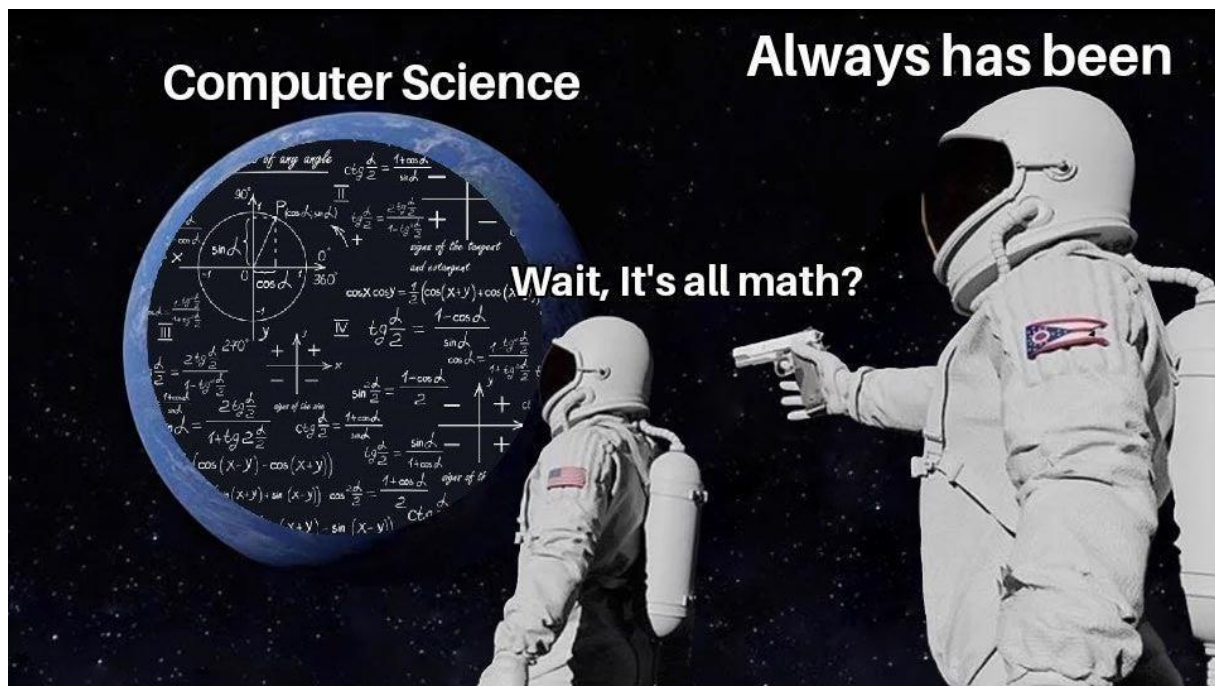
```

57         calcul(t[i]);
58
59         // sortăm vectorul descrescător -> avem aria maximă pe prima poziție
60         sort(&t[0], &t[6], compara);
61         cout << "Vectorul Sortat: ";
62         for(i = 0; i < 6; i++) cout << t[i].arie << " ";
63         cout << endl;
64
65         if(t[0].arie)
66             cout << endl << "Aria Maximă este: " << t[0].arie << endl;
67         else cout << endl << "Nu există!" << endl;
68
69         return 0;
70 }

```

Vectorul Sortat: 39 4.5 3 1.5 0 0

Aria Maximă este: 39



### 3.3. Temă:

La un concurs au participat  $n$  persoane, fiecare câștigând o anumită sumă de bani. Scrieți un program care citește dintr-un fișier numărul  $n$  de participanți și cei  $n$  participanți caracterizați prin nume, oraș și suma câștigată și care afișează: a) suma premiilor din fiecare oraș;

b) participanții ordonați alfabetic după nume.

Exemplu:

Date de Intrare	Date de Ieșire
6 Ionescu București 100 Florescu Arad 70 Iocai Cluj 90 Antal Arad 120 Serghei București 95 Matei Arad 85	a) București 195 Arad 275 Cluj 90  b) Antal Arad 120 Florescu Arad 70 Iocai Cluj 90 Ionescu București 100 Matei Arad 85 Serghei București 95





## Feedback Didactica Domeniului

A fost o experiență plăcută și am apreciat că ați fost de acord cu modul de susținere hibrid, pentru că în acest fel am putut participa la ore. Mi-ar fi plăcut dacă am fi avut și un suport de curs (niște slide-uri cu ideile principale sau un document) ca să am la ce să revin pe viitor, atunci când doresc să îmi reamintesc anumite detalii. De asemenea, documentul cu metoda de evaluare aș fi preferat să îl avem din primele săptămâni, ca să pot să mă apuc din timp de portofoliu. Cum a fost postat înainte de vacanța de Crăciun, deja s-au adunat foarte multe proiecte/teme/etc.. și de la materiile de la masterul la care sunt înscrisă și nu am avut când să lucrez la el, mai ales că cerințele nu au fost ușurele și necesitau cel puțin o zi de lucru asiduu, ca să ajung la un rezultat satisfăcător pentru mine.