OFERTA TEHNICĂ

Propunere privind servicii de testare a securității sistemului informatic al TERMOELECTRICA S.A.

Digitally signed by Bîrsan Vitalie
Date: 2023.08.29 12:15:40 EEST
Reason: MoldSign Signature
Location: Moldova

85 Alexandru cel Bun st.
Republic of Moldova, Chișinău MD-2012
Phone: +373 22 210 208
Fax: +373 22 223 963
Email: office@rsd.md
Website: www.rsd.md

29.08.2023

Stimați domni,

Avem plăcerea de a vă prezenta propunerea noastră privind serviciile de testare a securității și evaluare a vulnerabilităților informatice în cadrul Sistemului Informatic al Termoelectrica SA

Vă mulțumim pentru oportunitatea acordată de a oferi servicii profesionale și sperăm să dezvoltăm un parteneriat de succes.

Sperăm că propunerea noastră se ridică la înălțimea standardului de profesionalism pe care îl așteptați din partea RSD.

Cu stimă,

Cristian Tatarov
Senior Sales Manager

Phone. +373 22 210 208
Mob. +373 79 874 740
Fax. +373 22 223 963
85 Alexandru cel Bun st.
Republic of Moldova, Chisinau MD-2012
ww.rsd.md

SCOPUL SI OBIECTIVELE PROIECTULUI

Obiectivul acestui proiect il reprezintă serviciile de testare a securității și evaluare a vulnerabilităților informatice în cadrul Sistemului Informatic al Termoelectrica SA

Scopul serviciilor:

- Identificarea riscurilor asociate prin prisma prevederilor standardului SM EN ISO/IEC 27001;
- Identificarea aplicațiilor vulnerabile și de risc sporit în rețea, inclusiv cele expuse in internet;
- Evaluarea vulnerabilității infrastructurii de rețea inclusiv infrastructura wireless;
- Elaborarea recomandărilor și planului de remediere cu măsurile tehnice și operaționale pentru eliminarea/minimizarea riscurilor identificate și evaluate ca cele critice.

Principalele obiective țința ale testării sunt:

- Infrastructura de rețea (inclusiv echipamente active, routere, comutatoare).
- Servere și gazde, inclusiv sisteme de operare și servicii.
- Aplicație software utilizată în sistem.
- Protocoale de comunicație și servicii de rețea.
- Aplicații web.

Vor fi realizate teste de penetrare la nivel de rețea, inclusiv wireless, sistem de operare, baze de date și aplicații, inclusiv cele web, atacuri informatice simulând aplicații malițioase, cât și atacuri de tip DoS, DDoS.

85 Alexandru cel Bun st.
Republic of Moldova, Chișinău MD-2012
Phone: +373 22 210 208
Fax: +373 22 223 963
Email: office@rsd.md
Website: www.rsd.md

Abordarea noastră

Serviciile de tip penetration testing și evaluarea vulnerabilităților cuprind teste de penetrare, care reprezintă simularea unor atacuri informatice din perspectiva unui hacker asupra unei rețele, sistem, aplicație sau site web. În efectuarea acestui test se vor folosi metode și tehnici folosite de hackeri pentru a descoperi vulnerabilitățile și slăbiciunile sistemului ținta.

Testul de penetrare va evalua nivelul de securitate al aplicației/sistemului din perspectiva asigurării confidențialității, integrității și disponibilității informațiilor gestionate. Vor fi evaluate și nivelele de securitate ale componentelor de rețea și server care asigură protecția aplicației.

În urma testării, se va livra un raport detaliat în care se vor prezenta toate vulnerabilitățile și riscurile de securitate descoperite, împreuna cu recomandări pentru rezolvarea lor.

De asemenea, în cadrul propunerii noastre oferim și servicii de retestare a vulnerabilităților semnalate în raport.

Analiza cuprinde atât identificarea vulnerabiliăților cunoscute folosind unelte de scanare automate, cât și atacuri manuale personalizate pentru specificul sistemului țintă corelate cu listele de vulnerabilitati top ten OWASP, top twenty SANS. Atacurile de la nivelul rețelei pot fi corelate cu cele de la nivelul aplicației pentru generarea unor scenarii complexe. Testele de penetrare pot fi efectuate din exterior, utilizand toate nivelurile de privilegii disponibile in sistem, dar fără a cunoaște detalii privind arhitectura sistemului informatic (teste de tip-ul “blackbox”).

Testele de penetrare vor cuprinde atît teste automate cît și manuale.

- Testele automate vor identifica erori de programare în aplicațiile utilizate și vor fi efectuate cu ajutorul unor programe specializate precum instrumentele de scanare a vulnerabilităților, a aplicațiilor web și a codului, instrumente de testare și identificare a eventualelor erori de programare din aplicații în vederea exploatării lor.

85 Alexandru cel Bun st.
Republic of Moldova, Chișinău MD-2012
Phone: +373 22 210 208
Fax: +373 22 223 963
Email: office@rsd.md
Website: www.rsd.md

- Testele manuale vor analiza aspecte ale aplicațiilor care necesită intervenția umană, identificându-se erori logice de programare, și vor analiza și confirma sau infirma rezultatele testelor automate.

Tehnicile utilizate în identificarea și evaluarea vulnerabilităților se bazează pe cele mai bune practice în domeniu la nivel international:

- National Institute of Standards and Technology – NIST;
- Open Source Security Testing Methodology – OSSTM;
- Open Information Systems Security Group - OISSG;
- Open Web Application Security Project – OWASP;
- Information Systems Audit and Control Association – ISACA
- Information Systems Security Assessment Framework ISSAF

Serviciile de penetrare și evaluare a vulnerabilităților informatice se vor derula în 4 etape distincte, și anume:

- Pre-evaluare
- Evaluare
- Post-evaluare
- Follow-up (cuprinde servicii de retestare pentru vulnerabilitățile identificate și raportate)

Pre-evaluare

Reprezintă faza premergătoare evaluării vulnerabilităților și este importantă pentru determinarea specificațiilor precise și a regulilor de desfășurare a evaluării.
În această etapă se vor stabili și elabora Planul de testare, Planul de acțiuni (SOW – State of Work), precum și, scenariile de atac, și se vor obține autorizațiile necesare desfășurării testelor de penetrare.
Această etapă se va desfășura pe parcursul numărului de zile lucrătoare stabilit în cadrul planului de proiect și se va finaliza cu elaborarea Planului de testare și a Planului de acțiuni (SOW – State of Work) în care se vor înscrie cel puțin:

- activitățile întreprinse,
- sistemele incluse în activitatea de testare,
- perioada de realizare,
- persoane responsabile atît din partea Beneficiarului, cît și a Prestatorului.

Evaluare

Reprezintă etapa de identificare și evaluare a vulnerabilităților de securitate a sistemelor informatice.

Această etapă a testării include culegerea informațiilor despre sistemele testate din domeniul public și privat, descoperirea sistemelor și serviciilor active, precum și, scanarea sistemelor pentru descoperirea vulnerabilităților.

Scanarea vulnerabilităților și implementarea testului de penetrare la nivelul rețelei va include:

- Obținerea informațiilor din domeniul public;
- Scanarea sistemelor din SOW;
- Tehnici de enumerare;
- Obținerea accesului neautorizat prin exploatarea vulnerabilităților;
- Consolidarea accesului;
- Scannere de vulnerabilități specifice sistemelor și rețelelor incluse în Planul de acțiuni (SOW - State of Work);
- Aplicații necesare exploatării vulnerabilităților descoperite.

Scanarea vulnerabilităților și implementarea testului de penetrare va cuprinde analiza următoarelor vulnerabilități:

- Injectarea de cod malițios
- Managementul defectuos al procesului de autentificare și al sesiunii de lucru
- Cross-Site Scripting (XSS)
- Erori privind configurația de securitate
- Tratarea erorilor în mod nesecurizat și lipsa de măsuri de protecție a informațiilor sensibile
- Controale ineficiente privind managementul accesului
- Cross-Site Request Forgery (CSRF)
- Actualizări de securitate neimplementate
- Escaladarea privilegiilor
- Buffer Overflow
- Remote Code Execution
- Posibilitatea injectării de comenzi sau scripturi în servere web, servere de aplicații și baze de date
- Directory Traversal
- File and Path Disclosure

- Utilizarea de componente de sistem cu vulnerabilități cunoscute
- Validarea parametrilor de intrare ai aplicațiilor
- Comportamentul aplicațiilor/sistemelor aflate în scop la un atac de tip Denial of Service (DoS, DDoS)
- Procesul de generare a identificatorilor de sesiune și protecția acestora împotriva abuzurilor.
- Procesul de generare a cookie-urilor ce conțin generatori de sesiune și stabilire a atributelor acestora.
- Procesul de creare și terminare a sesiunii și identificatorilor din perspectiva server și client.
- Intervaluri de inactivitate și posibilitatea de inițializare de multiple sesiuni active.
- Măsurile implementate pentru păstrarea confidențialității informațiilor privind autentificarea și sesiunea de lucru.
- Implementarea de măsuri adiționale de securitate pentru operațiile sensibile, precum cele administrative.
- Posibilitatea de acces în sistem fără autentificare, cu autentificare cu credențiale inițiale sau credențiale ușor de ghicit

În privința configurației de securitate , tratării erorilor de sistem și protejării informațiilor sensibile vor fi testate următoarele aspecte:

- Versiunile de software ale serverelor, platformelor de dezvoltare a aplicației și componentelor sistemului.
- Existența actualizărilor de securitate aflate pe serverele, platformele de dezvoltare a aplicației și componentele sistemului.
- Existența configurațiilor prestabilite de la producătorul sistemului, cum ar fi utilizatori și parole implicite.
- Utilizatorii de aplicații și configurația acestora.
- Metodele și extensiile protocolului HTTP folosite în cadrul sistemului.
- Informații relevante ce se afla în header-ul HTTP.
- Existența mecanismelor de criptare pentru autentificarea în cadrul sistemelor și transmisia de informații
- Identificarea posibilității ca aplicațiile să divulge informații sensibile, inclusiv detalii despre sistem, identificatori de sesiune sau informații despre cont, în mesaje de erori.

- Conținutul mesajelor de eroare din punct de vedere tehnic.

În privința managementului accesului vor fi testate următoarele aspecte:

- Procesul de identificare, autentificare si autorizare a accesului la informații.
- Identificarea credențialelor hard-codate în sisteme, dacă acestea există.
- Identificarea utilizatorilor și credențialelor de acces stocate în fișiere de configurație în clar.
- Identificarea credențialelor transmise in clar, daca este cazul.
- Identificarea rolurilor de acces și maparea acestora pe drepturi și posibilitatea de ocolire a acestora pentru a obține acces neautorizat la informații.
- Identificarea metodelor HTTP folosite în procesul de autentificare.

În privința validării parametrilor de intrare vor fi testate următoarele aspecte:

- Filtrarea și validarea datelor provenite din afara sistemelor
- Existența unei metode centralizate de validare a datelor în sistem.
- Existența unor seturi de caractere corespunzătoare pentru datele de intrare
- Codificarea datelor într-un set comun de caractere înainte de validare
- Validarea datelor provenite de la utilizatori, înainte de procesarea acestora, inclusiv toți parametrii, conținutul URL si HTTP.
- lungimea datelor
- Implementarea de măsuri suplimentare de control pentru caractere cu potențial de risc (< > " ' % ( ) & + \ \' \")

Testarea securității la nivelul infrastructurii Wi-Fi va include următoarele aspecte:

- Descoperirea rețelelor Wi-Fi și punctelor de acces atît cunoscute cît și neautorizate
- Identificarea dispozitivelor care interacționează cu rețeaua
- Colectarea de informații despre protocoale de securitate și a dispozitivelor conectate
- Atacul și penetrarea rețelelor criptate cu WEP, WPA-PSK si WPA2-PSK

- Impersonare SSID
- Atacuri de tip Man-in-the-middle (MITM)
- Monitorizare automată trafic pentru a găsi fluxuri de date sensibile

Testarea securității sistemului de e-mail:

- Verificarea vulnerabilităților de tip refuzul serviciului (DoS) sau injectarea de cod malițios.
- Verificarea mecanismelor de autentificare a utilizatorului și verificări de autorizare pentru a preveni accesul neautorizat.
- Testarea posibilității de interceptare a datelor și analiza traficului pentru a asigura protecția datelor.
- Verificarea posibilității de acces la distanță la căsuța poștală prin protocoalele POP3, IMAP, SMTP.

Această etapă se va desfășura pe parcursul numărului de zile lucrătoare stabilit în cadrul planului de proiect.

Pe parcursul acestei etape vor fi realizate și teste manuale pentru re-testarea și validarea vulnerabilităților identificate.

Testele manuale analizează aspecte ale aplicațiilor care necesită intervenția umană și abilitatea de a combina cunoștințe din mai multe domenii, pentru a identifica vulnerabilități care nu pot fi descoperite folosind programe automate de testare

Post –evaluare

În această etapă se desfășoară conform planului de proiect și cuprinde elaborarea raportului de analiză, a rezultatelor testelor efectuate în care se vor identifica și vor fi incluse cele mai bune măsuri și metode de remediere a problemelor și vulnerabilităților descoperite, în funcție de severitate și impact, în scopul minimizării riscurilor de securitate informatică asociate problemelor și vulnerabilităților descoperite.

Aceste rezultate vor fi detaliate în raportul de testare care cuprinde următoarele:

- sumar Executiv;
- obiectivele și scopul evaluării;
- prezentare succintă a metodologiei utilizate;
- descrierea contextului în care s-a desfășurat evaluarea;
- prezentarea individuală a vulnerabilitatilor descoperite;
- descrierea vulnerabilității;
- catalogarea vulnerabilității;
- descrierea tehnică;
- analiza severității și probabilității
- calculul riscului;
- recomandări pentru remedierea vulnerabilităților semnalate;
- anexă cu lista testelor de securitate efectuate

Follow-up/Verificarea remedierii vulnerabilităților

Reprezintă etapa de verificare și confirmare a aplicării corecte a măsurilor și metodelor de remediere în scopul înlăturării riscurilor semnalate în etapele precedente, dupa ce Beneficiarul implementează măsurile menționate în raportul de test.
Această etapă se realizează în maximum 30 zile de la începerea proiectului.

Metodologie calcul nivel risc

Riscul reprezinta probabilitatea ca o anumita amenintare-sursa sa exploateze o vulnerabilitate, precum si impactul acelui eveniment asupra organizatiei sau sistemului respectiv.

NIVEL RISC	VALOARE	MASURI NECESARE
MAXIM	**75 – 100**	Actiune imediata pentru reducerea nivelului de risc.
CRITIC	**25 – 74**	Implementare de masuri corective cat mai curand posibil.
MEDIU	**5 - 24**	Implementare de masuri corective intr-o perioada rezonabila de timp.
SCAZUT	**2 - 4**	Pot fi implementate anumite masuri corective sau se accepta riscul.
INFORMATIONAL	**1**	Reprezinta o observatie care nu determina un risc de securitate.

Nivelul de risc pentru fiecare vulnerabilitate este calculat folosind urmatoarea formula:

NIVEL RISC = VALOARE SEVERITATE (IMPACT) x VALOARE PROBABILITATE

85 Alexandru cel Bun st.
Republic of Moldova, Chișinău MD-2012
Phone: +373 22 210 208
Fax: +373 22 223 963
Email: office@rsd.md
Website: www.rsd.md

VALOARE SEVERITATE

(IMPACT TEHNIC)

Impactul negativ asupra informatiei gestionate de aplicatie si sistem, pierdere sau degradare sau o combinatie a acestora a urmatoarelor integritate, disponibilitate, confidentialitate.

NIVEL	SCOR	DESCRIERE
SCAZUT	**1 – 5**	Afectarea limitata a informatiilor sau sistemului; obtinerea de informatii utile pentru generarea unor atacuri.
MEDIU	**6 – 14**	Afectarea semnificativa a informatiilor sau sistemului; pierdere de informatii, indisponibilitate serviciu; acces limitat la sistem.
SEVER	**15 - 20**	Pierderi foarte importante ale informatiei, acces nelimitat la sistem; prejudicii la nivelul organizatiei

VALOARE PROBABILITATE

Probabilitatea ca o anumita vulnerabilitate sa fie exploatata de catre un atacator. La calcularea probabilitatii se are in vedere: motivatia cunostinte necesar, usurinta in detectare si exploatare a vulnerabilitatii, nivelul de acces necesar si existenta unor masuri de detective si prevenire.

NIVEL	SCOR	DESCRIERE
FOARTE MICA	**1**	Vulnerabilitatea nu este direct exploatabila

MICA	**2**	Vulnerabilitatea necesita un efort semnificativ si cunostinte avansate pentru a fi exploatata manual. Atacatorul ar putea avea nevoie de acces si cunostinte interne ale sistemului.
MEDIE	**3**	Vulnerabilitatea necesita cunostinte specifice si poate fi exploata cu instrumente disponibile public.
MARE	**4**	Vulnerabilitatea necesita anumite cunostinte si poate fi exploata fara instrumente speciale sau foarte usor de gasit si utilizat.
FOARTE MARE	**5**	Vulnerabilitatea necesita cunostinte foarte putine si poate fi exploata fara instrumente speciale.

TERMENELE PROIECTULUI SI ELEMENTE ORGANIZATORICE

Activitatea noastră va începe la un termen stabilit de comun acord între RSD și beneficiar.

Mai mult, disponibilitatea personalului dumneavoastră de a asista echipa RSD este un alt factor cheie pentru succesul și eficiența proiectului și de aceea este necesar întregul Dumneavoastră sprijin.

Servicii	**Termen estimat**
Servicii de testare a securității și evaluare a vulnerabilităților informatice în cadrul Sistemului Informatic al Termoelectrica SA	Min 5 zile - Max 15 zile
Follow-up/Verificarea remedierii vulnerabilitatilor in max 30 de zile de la initierea proiectului	Max 2 zile

85 Alexandru cel Bun st.
Republic of Moldova, Chișinău MD-2012
Phone: +373 22 210 208
Fax: +373 22 223 963
Email: office@rsd.md
Website: www.rsd.md

Tools

Principalele tooluri utilizate:
Microfocus Fortify
Rapid7 Nexpose
Rapid7 Metasploit Pro
Burp Suite Professional
Pentest Tools – custom tools
Open Source – Kali linux distribution
Nmap
Nessus
Sqlmap
Wireshark
FindBugs
Bandit
Fortify Sourse Code Analyser

Echipa de testare

Nr. d/o	Funcţia/Nume Prenume	Studii de specialitate	Vechimea în munca de specialitate (ani)	Numărul şi denumirea bunurilor/serviciilor similare livrate/prestate în calitate de conducător	Numărul certificatului de atestare și data eliberării
	1	2	3	4	5
1	***Miron-Gabriel Gheorghe*** *Manager de proiect* *Expert Șef securitate sisteme informatice* *Expert testare securitate sisteme informatice*	Universitatea Politehnica din București (Romania), Facultatea de Electronica si Telecomunicație 1991 - 1995	*Manager de proiect* 2014 - prezent *Expert Șef securitate sisteme informatice* 2014 – prezent *Expert testare securitate sisteme informatice* 2010 - prezent	Consultanta in domeniul Cybersecurity / **EAU de Web** www.eaudeweb.ro - Manager de proiect - Expert securitate sisteme informatice - Expert testare securitate sisteme informatice - Expert testare securitate infrastructură rețea **Septembrie 2022 – prezent** Teste de securitate/ **Bynet Consultinng** - Manager de proiect - Expert securitate sisteme informatice - Expert testare securitate sisteme informatice și infrastructurilor de tip WiFi - Expert testare securitate sisteme informatice - Expert testare securitate infrastructură rețea **Aprilie – Iulie 2022**	1. *CISA – eliberat 2014* 2. *PRINCE2 – eliberat 2018* 3. *ITIL – eliberat 2010, 2011* 4. ISO 27001 Lead Implementer – *eliberat 2017* 5. Responsabil date cu caracter personal – *eliberat 2021* 6. GCIH – *eliberat 2007-2015* 7. GWAPT – *eliberat 2010-2014* 8. Rapid7 Nexpose Certified Administrator – *eliberat 2015*

				Penetration testing services / **MIXT Energy** - Manager de proiect - Expert securitate sisteme informatice - Expert testare securitate sisteme informatice și infrastructurilor de tip WiFi - Expert testare securitate sisteme informatice - Expert testare securitate infrastructură rețea **August 2022** IBM Qradar SIEM tunnning consulting services / **Banca Romaneasca** - Manager de proiect - Expert securitate sisteme informatice **2020 - 2022** Cyber security consulting services / **TrustChain** - Manager de proiect - Expert securitate sisteme informatice - Expert testare securitate sisteme informatice - Expert testare securitate infrastructură rețea **2021 - 2022**	9. Fortify SCA and SSC – *eliberat 2022*

				Proiecte de securitate/ **Transfond SA** - Manager de Proiect - Expert securitate sisteme informatice - Expert testare securitate sisteme informatice - Expert testare securitate infrastructură rețea 2005 - 2019	
2	***Razvan Ionescu*** *Expert testare securitate infrastructură rețea* *Expert testare securitate sisteme informatice* *Expert testare securitate sisteme informatice și*	Universitatea Politehnica din București (Romania), Faculty of Engineering taught in Foreign Languages 10/2006 – 07/2010 Universitatea de Tehnologie din Chemnitz (Germania), Catedra de informatică teoretică și securitate Informatică teoretică și	*Expert testare securitate infrastructură rețea* 2015 – prezent *Expert testare securitate sisteme informatice* 2015 – prezent *Expert testare securitate sisteme informatice și*	WiFi Penetration Testing / **RTA Dubai** (Roads and Transport Authority) The company manages the entire transport infrastructure in United Arab Emirates - Manager de Proiect - Expert testare securitate sisteme informatice și infrastructurilor de tip WiFi - Expert testare securitate sisteme informatice - Expert testare securitate infrastructură rețea August 2021	1. *GSEC – eliberat 07/2022* 2. *OSCP – eliberat 07/2015* 3. *OSWP – eliberat 12/2015* 4. *CRTP – eliberat 03/2021* 5. *GCIA – eliberat 03/2018* 6. *GCIH – eliberat 03/2017* 7. *GPEN – eliberat 07/2016* 8. *GWAPT – eliberat 08/2017* 9. *GXPN – eliberat 10/2016*

	infrastructurilor de tip WiFi	securitatea informației 10/2009 – 03/2010 Universitatea Politehnica din București (Romania), Facultatea de Automatică și Calculatoare 10/2010 – 07/2012	*infrastructurilor de tip WiFi* 2015 - prezent	Penetration Testing / **OTP BANK Romania** Testare aplicații, infrastructura interna de rețea si sistem SWIFT - Manager de Proiect - Expert testare securitate sisteme informatice și infrastructurilor de tip WiFi - Expert testare securitate sisteme informatice - Expert testare securitate infrastructură rețea Decembrie 2021 Penetration Testing/ **GST Safety Textiles RO** Testare de infrastructură externă / Inginerie Socială (Phishing) **Global Safety Textiles manufactures airbags, airbag textiles and technical textiles** - Manager de Proiect - Expert testare securitate sisteme informatice și infrastructurilor de tip WiFi - Expert testare securitate sisteme informatice - Expert testare securitate infrastructură rețea August 2022	

				Penetration Testing/ **Tradeshift** Testare de infrastructură internă şi externă de reţea (Kubernetes, Docker, API Gateway) Tradeshift is a trade technology platform with 1.5 million companies connected on it. https://tradeshift.com/why-tradeshift/ - Manager de Proiect - Expert testare securitate sisteme informatice și infrastructurilor de tip WiFi - Expert testare securitate sisteme informatice - Expert testare securitate infrastructură rețea Octombrie 2022	

				Penetration Testing/ Saudi AZM Testare de infrastructură externă Saudi AZM is a Service provider company, offering: Financial technical software development, Executive consulting, Human resource services and IT, based in KSA, having both private and governmental clients. - Manager de Proiect - Expert testare securitate sisteme informatice și infrastructurilor de tip WiFi - Expert testare securitate sisteme informatice - Expert testare securitate infrastructură rețea Ianuarie 2022	
				Penetration Testing/ Survale Testare de infrastructură externă Survale offers a talent survey and analytics platform built for all facets of human resources - Manager de Proiect - Expert testare securitate sisteme informatice și infrastructurilor de tip WiFi - Expert testare securitate sisteme informatice - Expert testare securitate infrastructură rețea Mai 2020	

3	***Daniel Bechenea*** *Expert testare securitate infrastructură rețea* *Expert testare securitate sisteme informatice* *Expert testare securitate sisteme informatice și infrastructurilor de tip WiFi*	LICENȚĂ, REȚELE ȘI SOFTWARE DE TELECOMUNICAȚII - Facultatea de Electronică, Telecomunicații și Tehnologia Informației, București (România) 01/10/2013 – 15/07/2017 MASTERAT, MANAGEMENTUL SERVICIILOR ȘI REȚELELOR - Facultatea de Electronică, Telecomunicații și Comunicații și tehnologia informației, București (România) 01/10/2017 – 01/07/2019	*Expert testare securitate infrastructură rețea* 2020 – prezent *Expert testare securitate sisteme informatice* 2020 – prezent *Expert testare securitate sisteme informatice și infrastructurilor de tip WiFi* 2020 - prezent	WiFi Penetration Testing / **RTA Dubai** (Roads and Transport Authority) The company manages the entire transport infrastructure in United Arab Emirates - Expert testare securitate sisteme informatice și infrastructurilor de tip WiFi - Expert testare securitate infrastructură rețea August 2021 Penetration Testing / **OTP BANK Romania** Testare aplicatii, infrastructura interna de retea si sistem SWIFT - Expert testare securitate sisteme informatice și infrastructurilor de tip WiFi - Expert testare securitate sisteme informatice - Expert testare securitate infrastructură rețea Decembrie 2021	*1. OSCP – eliberat 02/2020*

				Penetration Testing/ **GST Safety Textiles RO** Testare de infrastructură externă / Inginerie Socială (Phishing) **Global Safety Textiles manufactures airbags, airbag textiles and technical textiles** - Expert testare securitate sisteme informatice - Expert testare securitate infrastructură rețea August 2022	
				Penetration Testing/ **Tradeshift** Testare de infrastructură internă şi externă de reţea (Kubernetes, Docker, API Gateway) Tradeshift is a trade technology platform with 1.5 million companies connected on it. https://tradeshift.com/why-tradeshift/ - Expert testare securitate sisteme informatice și infrastructurilor de tip Widie - Expert testare securitate sisteme informatice - Expert testare securitate infrastructură rețea Octombrie 2022	

				Penetration Testing/ Saudi AZM Testare de infrastructură externă Saudi AZM is a Service provider company, offering: Financial technical software development, Executive consulting, Human resource services and IT, based in KSA, having both private and governmental clients. - Expert testare securitate sistema informatice - Expert testare securitate infrastructură rețea Ianuarie 2022	
				Penetration Testing/ Survale Testare de infrastructură externă Survale offers a talent survey and analytics platform built for all facets of human resources - Expert testare securitate sistema informatice - Expert testare securitate infrastructură rețea Mai 2020	

4	***Eusebiu Boghici*** *Expert testare securitate infrastructură rețea* *Expert testare securitate sisteme informatice* *Expert testare securitate sisteme informatice și infrastructurilor de tip WiFi*	Universitatea POLITEHNICA din București Facultatea de Automatică și Calculatoare, (România) Diplomă de licență 2015 – 2019 Universitatea POLITEHNICA din București Facultatea de Automatică și Calculatoare, (România) Master în Inginerie - Calculatoare și Sisteme Informatice 2019 – 2021	*Expert testare securitate infrastructură rețea* 2018 – prezent *Expert testare securitate sisteme informatice* 2018 – prezent *Expert testare securitate sisteme informatice și infrastructurilor de tip WiFi* 2018 - prezent	Penetration Testing / **OTP BANK Romania** Testare aplicatii, infrastructura interna de retea si sistem SWIFT - Expert testare securitate sisteme informatice - Expert testare securitate infrastructură rețea Decembrie 2021 Penetration Testing/ **GST Safety Textiles RO** Testare de infrastructură externă / Inginerie Socială (Phishing) **Global Safety Textiles manufactures airbags, airbag textiles and technical textiles** - Expert testare securitate sisteme informatice - Expert testare securitate infrastructură rețea August 2022	1. *OSCP – eliberat 02/2021*

				Penetration Testing/ **Tradeshift** Testare de infrastructură internă şi externă de reţea (Kubernetes, Docker, API Gateway) Tradeshift is a trade technology platform with 1.5 million companies connected on it. https://tradeshift.com/why-tradeshift/ - Expert testare securitate sisteme informatice - Expert testare securitate infrastructură rețea Octombrie 2022	
				Penetration Testing/ **Saudi AZM** Testare de infrastructură externă Saudi AZM is a Service provider company, offering: Financial technical software development, Executive consulting, Human resource services and IT, based in KSA, having both private and governmental clients. - Expert testare securitate sisteme informatice - Expert testare securitate infrastructură rețea Ianuarie 2022	