Universitatea
Ştefan cel Mare
Suceava

REZUMAT
TEZĂ DE DOCTORAT

Contribuții privind optimizarea securității cloud computing

Conducător științific,
Prof. univ. dr. ing. Adrian GRAUR

Doctorand,
Ing. Ionel GORDIN

Suceava, 2019

Mulțumiri

Lucrarea a fost elaborată parțial cu sprijinul financiar al proiectului "Doctorat European de calitate - EURODOC", Contract nr. POSDRU / 187 / 1.5 / S / 155450, proiect co-finanțat de Fondul Social European prin Programul Operațional Sectorial "Dezvoltarea Resurselor Umane" 2007-2013.

Lucrarea a fost susținută parțial de un grant al Autorității Naționale pentru Cercetare Științifică și Inovare, UEFISCDI, număr de proiect PN-III-P2-2.1-PED-2016-2011, contract 36 PED / 2017, in cadrul PNCDI III. Infrastructura utilizată în această lucrare a fost susținută din proiectul "Centru integrat de cercetare, dezvoltare și inovare pentru Materiale Avansate, Nanotehnologii și Sisteme Distribuite de fabricație și control" (MANSID), Contractul nr. 671 / 09.04.2015, Programul Operațional Sectorial pentru Creșterea Competitivității Economice cofinanțată din Fondul European de Dezvoltare Regională.

Doresc să adresez mulțumirile mele tuturor celor care, direct sau indirect, au contribuit la elaborarea acestei teze.

Mulțumesc Prof.univ.dr.ing. Adrian GRAUR, Prof.univ.dr.ing. Dan Alin POTORAC pentru îndrumarea și susținerea oferită de-a lungul întregii perioade de formare prin studii doctorale.

De asemenea, mulțumesc domnilor: Prof.univ.dr.ing. Nicolae Dumitru ALEXANDRU și Prof.univ.dr.ing. Dorin PETREUȘ pentru sprijinul acordat pe parcursul finalizării tezei și efortul făcut de a fi prezenți la susținerea publică a acesteia.

Nu în ultimul rând, sunt recunoscător întregii familii pentru suportul oferit.
Dedic această lucrare tatălui meu, Dumitru, care acum ne urmărește din cer.

Cuprins rezumat teză de doctorat

Cuprins teză de doctorat 4
I. Introducere 7
II. Obiectivul și structura tezei de doctorat 8
III. Rezumatul tezei de doctorat 9
IV. Contribuții și direcții de cercetare viitoare 19
V. Diseminarea rezultatelor 23
Bibliografie teză de doctorat 24

Cuprins teză de doctorat

I. *CLOUD COMPUTING* 6

I.1 Introducere 6

I.1.1 *Cloud computing* versus structura IT tradițională 6

I.1.2 Caracteristici *cloud* 8

I.1.3 Centrele de date și fermele de calculatoare 9

I.1.4 Stocarea datelor în *cloud* 9

I.1.5 Tehnologiile de virtualizare 11

I.1.6 Noțiuni generale despre hipervizor 11

I.1.7 Aplicații *cloud* (API) 13

I.1.8 Containere *cloud* 14

I.1.9 Microservicii *cloud* 15

I.2 Clasificarea serviciilor *cloud* 16

I.2.1 Modelul - *Software* ca Serviciu (SaaS) 17

I.2.2 Modelul - Platformă ca Serviciu (PaaS) 17

I.2.3 Modelul - Infrastructură ca Serviciu (IaaS) 18

I.3. Tipuri de *cloud* 19

I.3.1 *Cloud* public 19

I.3.2 *Cloud* privat 22

I.3.3 *Cloud* hibrid 26

I.3.4 *Cloud* comunitar 28

I.4 Concluzii 29

II. STADIUL ACTUAL AL SECURITĂȚII ÎN DOMENIUL *CLOUD COMPUTING* 31

II.1 Organizații de standardizare și reglementare 31

II.1.1 Standard pentru comunicațiile rețea – modelul OSI 32

II.1.2 Confidențialitatea datelor 35

II.1.3 Acordul de calitate al serviciilor – SLA 35

II.2 Securitatea infrastructurii *cloud* 36

II.2.1 Nivelul rețea 36

II.2.2 Nivelul gazdă 46

II.2.3 Nivelul aplicație 49

II.2.4 Securitatea datelor și a spațiului de stocare 53

II.3 *Cloud computing*: vulnerabilități 54
II.3.1 *Cloud computing*: statistici de vulnerabilitate 56
II.3.2 Raport CVE pentru *cloud* privat OpenStack - Redhat 57
II.4 Concluzii 59
III. CONFIGURAREA UNUI *CLOUD* PRIVAT UTILIZÂND OPENSTACK 62
III.1 Arhitectura OpenStack 62
III.2 Distribuții OpenStack 63
III.3 Componente OpenStack 65
III.4 Instalare OpenStack 67
III.4.1 RDO Packstart 67
III.4.2 Activare autentificare securizată 71
III.5 Concluzii 71
IV. SOLUȚIE ARHITECTURALĂ PENTRU OPTIMIZAREA AUTENTIFICĂRII ÎN MEDIUL OPENSTACK *CLOUD* 73
IV.1 Autentificarea cu doi factori (TOTP) 74
IV.2 Activarea și adăugarea de utilizatori TOTP 78
IV.3 Adăugare TOTP în interfața *web* (HORIZON) 79
IV.4 Implementare modul de autentificare TOTP 80
IV.4.1 Dezactivare API V2 82
IV.5 Implementare TOTP utilizând cod QR 83
IV.5.1 Generarea codului QR 83
IV.5.2 Trimitere cod QR prin *email* 84
IV.5.3 Sistem TOTP integrat 84
IV.6 Utilizarea factorului de posesie și a factorului de cunoaștere la autentificarea TOTP 86
IV.7 Autentificarea cu doi factori pentru OpenStackClient 88
IV.8 Concluzii 89
V. ANALIZA SECURITĂȚII CLOUD OPENSTACK UTILIZÂND SOFTWARE DEDICAT 91
V.1 Evaluarea nivelului de securitate – scanare rețea internă 92
V.2 Evaluarea securității – scanare rețea internă pentru mașinile virtuale din cloud 94
V.3 Evaluarea securității – scanare rețea externă 95
V.4 Concluzii 96
VI. CONCLUZII FINALE ȘI CONTRIBUȚII 97

VI.1 Concluzii generale 97
VI.2 Contribuții și direcții de cercetare viitoare 99
BIBLIOGRAFIE 103
LISTA LUCRĂRILOR PUBLICATE 108
Lista de abrevieri 109
Glosar de termeni 112
Lista figurilor 113
ANEXE 114
Anexa A 114
Anexa B 115
Anexa C 116
Anexa D 117
Anexa E 121
Anexa F 123
Anexa G 125
Anexa H 126
Anexa I 128
Anexa J 130

I. Introducere

Cloud computing este un concept de actualitate utilizat în domeniul calculatoarelor, al tehnologiei informațiilor în general, constituindu-se într-un ansamblu distribuit al serviciilor de calcul oferite, capabil să ofere aplicații și acces la prelucrare și stocare de date, fără ca beneficiarul să cunoască amplasarea sau configurația *hardware* a sistemelor care asigură serviciile respective. Deși a apărut relativ recent, acest concept a câștigat o mare popularitate, iar aplicațiile sale s-au extins mai în toate domeniile de activitate (mediu universitar, al furnizorilor de servicii de Internet, în telecomunicaţii, în medicină și economie, financiar etc.).

Cloud Computing permite accesul la toate resursele sale de oriunde din lume prin intermediul unei interfețe *web* sau al unor aplicații specifice. Utilizarea *software*-ului bazat pe *cloud* oferă companiilor din toate sectoarele de activitate o serie de beneficii, inclusiv posibilitatea de a folosi *software*-ul pe oricare dintre dispozitivele hardware, inclusiv pe telefoanele mobile *smart*.

Datorită serviciilor de tip *cloud-computing*, utilizatorii pot verifica *email*-urile pe orice computer și pot chiar să stocheze fișiere utilizând servicii cum ar fi Dropbox sau Google Drive. Serviciile *Cloud-computing* oferă utilizatorilor posibilitatea de a crea copii de rezervă pentru muzică, fișiere și fotografii, asigurându-se că aceste fișiere sunt disponibile imediat, practic în orice locație geografică.

Cloud computing oferă întreprinderilor mari un potențial considerabil de economisire a costurilor. Înainte ca mediul *cloud* să devină o alternativă viabilă, companiile au fost nevoite foarte frecvent să cumpere, să construiască și să întrețină tehnologii și infrastructuri costisitoare pentru gestionarea diverselor date și informații. Astăzi, în loc de a investi sume considerabile în centre de servere mari și complicat de întreținut la zi, în departamentele IT care necesită îmbunătățiri constante, o firmă poate folosi mini stații de lucru cu conexiuni la Internet, iar lucrătorii pot interacționa cu *cloud*-ul în regim *online* pentru a realiza prezentări, foi de calcul și a interacționa cu *software*-ul companiei.

Confidențialitatea și securitatea datelor care tranzitează mediul *cloud* este la fel de importantă ca și datele în sine. Inițial, securitatea a fost un element care a redus acceptarea sa ca mod de lucru, mai ales atunci când discutăm de înregistrări medicale și informații financiare sensibile.

Deși reglementările internaționale obligă furnizorii unor asemenea servicii să-și susțină măsurile de securitate și de conformitate, aceasta rămâne adesea o problemă de vulnerabilitate. Publicul este constant informat de televiziune sau mediul *online* cu privire la atacuri, în care informații sensibile au ajuns în mâna *hacker*-ilor care pot șterge, manipula sau exploata datele astfel preluate. Astfel de atacuri au loc și la centrele de date clasice, impactul unui atac *cloud* fiind însă cu mult mai mare în acest mediu întrucât volumul datelor stocate sau tranzitate este substanțial mai mare. Tema securității *cloud*, abordată în această teză este de un mare interes atât pentru cei care activează în cercetare și inovare cât și pentru companiile IT.

II. Obiectivul și structura tezei de doctorat

Obiectivul principal al tezei de doctorat este îmbunătățirea securității *cloud computing*. Întrucât securitatea la nivel de *cloud* public se poate realiza doar la nivel de client s-a optat pentru optimizarea securității *cloud*-ului privat. Un avantaj major al acestui tip de *cloud* îl constituie posibilitatea de instalare în orice locație, securitatea este administrată și controlată în totalitate de administrator. Este mediul ideal pentru testarea securității *cloud* cu posibilitatea de repetare a testelor în orice moment fără a fi influențat de încărcarea rețelei sau a resurselor sistem. În cadrul tezei s-a ales optimizarea securității *cloud* OpenStack, o soluție software *opensource*. Acest tip de *cloud* nu necesită o licență pentru utilizare și în plus oferă în mod gratuit toate sursele și documentația aferentă aplicațiilor dezvoltate. Aceste informații au fost folosite ca bază pentru realizarea unor noi module de securizare a autentificării cloud în cadrul capitolului IV. Direcțiile de cercetare sunt prezentate gradat în cadrul tezei.

Astfel, în cadrul *capitolului I* intitulat *Cloud Computing,* se realizează o introducere privind *cloud computing,* continuată de o paralelă la structura IT tradițională cu scopul de a pune în evidență avantajele aduse de această nouă tehnologie. Sunt evidențiate cu această ocazie caracteristicile și componentele definitorii *cloud*. Serviciile oferite sunt clasificate după modul lor de implementare, fiind sintetizate detalii despre *cloud*-ul privat, cel public, hibrid și comunitar.

În *capitolul II, Stadiul actual al securității în domeniul cloud computing,* se realizează o sinteză privind stadiul actual al securității din acest domeniu. Sunt prezentate cu această ocazie organizațiile de standardizare și reglementare al securității precum și direcțiile urmate de industria *cloud* în vederea asigurării confidențialității datelor stocate sau tranzitate prin acest mediu. Securitatea *cloud* se aplică diferențiat în funcție de nivelul de lucru. În acest sens s-a sistematizat modul de securizare al nivelelor: rețea, gazdă, aplicație și stocare. Studiul este completat de un raport privind statisticile de vulnerabilitate din domeniu și o sistematizare a celor mai uzuale vulnerabilități *cloud*.

Începând cu capitolul III, teza aduce contribuții practice la securitatea *cloud computing*. Astfel în cadrul capitolului *Configurarea unui cloud privat utilizând OpenStack* este elaborat modul de instalare a unui *cloud* privat folosind OpenStack. Suplimentar față de documentația aferentă este prezentat modul de securizare al autentificării web.
Securitatea mediului *cloud* OpenStack este completată în cadrul capitolului IV, *Soluție arhitecturală pentru optimizarea autentificării în mediul OpenStack cloud* de dezvoltarea unui modul care permite realizarea autentificării cu doi factori. În cadrul acestui capitol s-a dezvoltat de asemenea o suită de aplicații pentru adăugarea conturilor aferente, generarea și trimiterea codului secret în format QR spre utilizator. Este prezentată procedura de autentificare folosind aplicația Google Authenticator.

În cadrul *capitolului V, Analiza securității cloud OpenStack utilizând software dedicat,* se studiază securitatea mediului OpenStack din exteriorul și din interiorul rețelei *cloud*. În acest scop se s-au utilizat aplicațiile: Nessus, Metasploit și OpenVAS pentru analiza securității *cloud* din interiorul, cât și din exteriorul rețelei. Pentru analiza exterioară a securității s-a folosit aplicația *web* Tenable IO. Suplimentar s-a analizat securitatea mașinilor virtuale găzduite în acest mediu.

Capitolul VI, Contribuții și direcții de cercetare viitoare, realizează o analiză a informațiilor și contribuțiilor prezentate în cadrul tezei și se trasează direcțiile viitoare de cercetare.

III. Rezumatul tezei de doctorat

În ***capitolul I*** se definește conceptul de *cloud* și sunt prezentate avantajele acestuia în raport cu centrele de date clasice. Sunt trecute în revistă serviciile specifice mediului *cloud*, modul de stocare a datelor, fiind furnizate detalii privind tehnologiile de virtualizare și modul de accesare a resurselor *cloud*. Sunt evidențiate de asemenea tendințele din domeniu prin detalierea conceptelor de container și microservicii.

Partea a doua a acestui capitol este alocată pentru a realiza o clasificare a serviciilor *cloud* după modul de livrare a acestor servicii. În acest sens sunt evidențiate modelele: *Software* ca serviciu (SaaS), Platformă ca serviciu (PaaS), Infrastructură ca serviciu (IaaS) și sunt în final prezentate tipurile de servicii oferite de fiecare dintre modelele prezentate.

În ultima parte a capitolului, este realizată o clasificare a serviciilor *cloud* după modul lor de implementare, fiind sintetizate detalii despre *cloud*-ul privat, cel public, hibrid și respectiv comunitar.

Capitolul II al tezei prezintă stadiul actual al securității din mediul *cloud computing*. Standardele de securitate din domeniu dețin un rol important în uniformizarea modului de securizare a datelor de către toți furnizorii unui astfel de serviciu. În cadrul acestui capitol s-au prezentat succint atât standardele de securitate internaționale, cât și cele specifice Uniunii Europene. S-a pus accent de asemenea pe securitatea datelor, precum și pe acordul de calitate a serviciilor (SLA). Securitatea infrastructurilor *cloud* a fost analizată detaliat parcurgând fiecare din cele 4 niveluri de bază: *rețea, gazdă, aplicație* respectiv *securitatea datelor și a spațiului de stocare*.

Prezentând *nivelul rețea*, autorul a realizat o paralelă între structura unei rețele clasice în raport cu rețeaua virtuală și a abordat modul de securizare a rețelelor virtuale VLAN, respectiv VXLAN. Rețelele definite prin *software* (SDN) sunt tratate de asemenea în cadrul tezei de față, fiind evidențiate avantajele și dezavantajele utilizării acestor rețele în raport cu rețelele VLAN/VXLAN, fiind prezentate facilitățile oferite de rețeaua SDN în domeniul securității informației. Autorul abordează problemele de securitate care au fost puse în evidență la nivelul rețea prin prezentarea celor mai frecvente tipuri de atacuri.

În cadrul *nivelului gazdă* în teză sunt analizate toate modelele de servicii oferite (SaaS, PaaS, IaaS), dar și modelele de dezvoltare (public, privat și hibrid). În cadrul securității proprii serviciului IaaS se acordă o atenție deosebită securității hipervizorului și respectiv mașinilor virtuale (VM). Tratând *nivelul aplicație*, autorul pune accent pe ciclul de viață al aplicației securizate (SSDLC) și detaliază modul de implementare și dezvoltare a acesteia conform cu standardele internaționale în vigoare. La *nivelul de securitate a datelor și a spațiului de stocare,* sunt prezentate etape pentru asigurarea securizării datelor care tranzitează mediul *cloud*, dar și modele de stocare sigură a datelor. La finalul acestui capitol autorul prezintă sintetic principalele vulnerabilități raportate pentru mediul *cloud* și face o reprezentare statistică a vulnerabilităților descoperite pentru mediul OpenStack Redhat.

Capitolul III a urmărit a evidenția pașii de parcurs pentru instalarea mediului OpenStack, utilizând distribuția RDO. Instalarea unui *cloud* privat sau public necesită în primul rând înțelegerea arhitecturii și a modului de funcționare. Subcapitolul *III.1 Arhitectura OpenStack*, prezintă succint structura acestui mediu *cloud* și componentele aferente lui. Datorită complexității mediului *cloud* și a multitudinii de companii implicate în dezvoltarea soluției

OpenStack s-au realizat mai multe distribuții, fiecare cu modul său propriu de instalare. În cadrul subcapitolului *III.2*, s-au prezentat principalele distribuții *cloud* realizate până acum. S-a optat pentru instalarea unei distribuții RDO, împreună cu sistemul de operare CentOS, luând în considerare:

- fiabilitatea și securitatea sistemului de operare
- complexitatea instalării soluției *cloud* și opțiunile de configurare disponibile.

Ambele soluții sunt dezvoltate de compania RedHat, o companie cu o lungă și vastă experiență în elaborarea de sisteme de operare Linux și mai recent a soluțiilor *cloud* profesionale.

Pentru testare, autorul a utilizat un sistem IBM BladeCenter HS 22, care rulează VMware vSphere 5.5, mediul respectiv permițând alocarea unor mașini virtuale cu configurații *hardware* ajustabile.

Procedura de instalare este completată de modalitatea de configurare a *host*-ului în format FQDN, în teză fiind detaliată funcționalitatea și modul de utilizare a fișierului de configurare propus de autor *packstack-answers-yyyymmdd-xxxx.txt*, fișier generat la finalizarea instalării. În cadrul secțiunii *III.4.2 Activare autentificare securizată*, s-a propus un modul de securizare a componentei Horizon, utilizată la autentificarea prin intermediul interfeței *web*.

Înțelegerea arhitecturii și a modului de funcționare, instalare și securizare a mediului *cloud* este imperios necesară pentru un mediu în continuă expansiune și a cărui complexitate crește exponențial. Informațiile prezentate în cadrul acestui capitol au fost testate și implementate de autor în mediul real.

În ***Capitolul IV*** se prezintă o soluție arhitecturală pentru optimizarea securității la autentificare utilizând mediul *cloud* OpenStack.

În momentul de față autentificarea cu doi factori este utilizată pe scară largă în majoritatea mediilor online. Optimizarea securității *cloud* OpenStack, prin adăugarea acestei facilități vine ca o necesitate de aliniere a securității cu tendințele mondiale în domeniul securității IT. Pentru a eficientiza acest tip de autentificare, este necesară asocierea sa cu o comunicație securizată utilizând protocolul HTTPS. Procedura de activare a acestui protocol de comunicație este prezentată detaliat în cadrul secțiunii III.4.2.

OpenStack în cadrul versiunii Queens (2018) include modulul TOTP necesar autentificării cu doi factori la nivel de componentă Keystone. Din păcate, infrastructura *cloud* nu este adaptată pentru a suporta această facilitate. În cadrul acestui capitol s-a tratat autentificarea în doi factori atât la nivel de interfață utilizator (componentă Horizon), cât și la nivel de autentificare (componentă Keystone).

Pentru fiecare utilizator din mediul *cloud* se creează un cont TOTP la care se asociază o parolă secretă pe 16 caractere generată aleator. Parola secretă este convertită apoi în format bază 32. Pentru a elimina erorile care pot apărea la transcrierea codului de către utilizator, în concordanță cu tendințe similare utilizate de alte aplicații, autorul a optat pentru convertirea parolei în imagine QR și trimiterea acestei imagini prin *email*. Utilizatorul folosește o aplicație pentru *smartphone* care permite conversia parolei secrete în cod unic (ex. Google Authenticator).

Codul interfeței *web* de autentificare, parte componentă a componentei Horizon, a fost ajustat pentru a permite acest nou tip de autentificare. În acest sens, a fost modificat fișierul *forms.py*. Adăugarea unei noi componente de autentificare reprezintă o adevărată provocare pentru dezvoltatori la partea de securizare a mediului *cloud*. Pentru a elimina orice disfuncționalitate cauzată de acest aspect în cadrul formularului de autentificare prin teză s-a optat pentru soluția concatenării câmpului parolă cu cel al codului unic și transmiterea rezultatului respectiv către modulul de autentificare.

Autentificarea *web* TOTP nu ar fi posibilă fără ajutorul unei componente din interiorul mediului *cloud* care să faciliteze autentificarea. În acest scop s-a dezvoltat modulul *password_totp.py* modul care extrage informațiile de autentificare (utilizator, parolă și cod TOTP) și realizează autentificarea la nivel Keystone.

Autentificarea cu doi factori (TOTP)

În cadrul procesului de autentificare, utilizatorul introduce datele necesare precum utilizator / parolă și cod unic (TOTP *token*). Datele introduse sunt preluate de componenta *web* Horizon și sunt transmise spre componenta de autentificare Keystone. Acest modul verifică utilizatorul / parola și dacă utilizatorul deține cont TOTP. Dacă datele de autentificare nu sunt corecte utilizatorul este informat cu privire la acest aspect prin interfața *web* Horizon. În situația în care datele introduse se regăsesc în sistem, se realizează redirectarea spre pagina de administrare a resurselor *cloud*.

În Fig. 1 este prezentat procesul de autentificare și modul de interacțiune al acestuia cu componentele Horizon și Keystone.

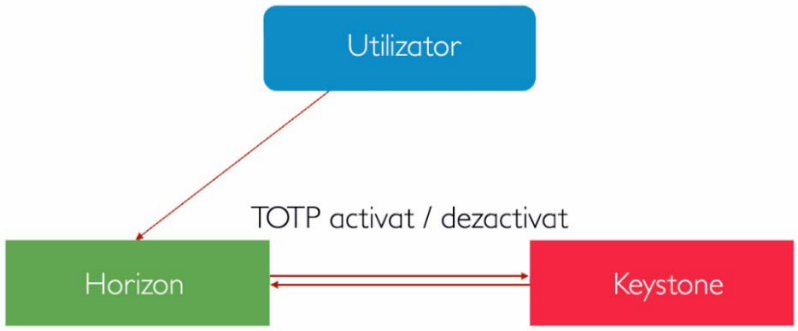

Fig. 1. Autentificare OpenStack utilizând TOTP

La autentificarea TOTP, codul de autentificare se schimbă automat la fiecare 30 de secunde. În acest fel, chiar dacă datele de autentificare sunt compromise, atacatorul nu le poate utiliza întrucât codul de autentificare se schimbă în timp.

Combinat cu o comunicație criptată (HTTPS), sistemul de autentificare în doi pași asigură o foarte bună securizare a mediului *cloud*. Din acest motiv sistemul este adoptat de majoritatea companiilor care activează în mediul online.

Acest tip de autentificare presupune existența a minim doi factori:

- *un factor de cunoaștere* – utilizatorul și parola

- *un factor de posesie* – dispozitiv mobil pentru primirea sau generarea codului TOTP (Time-based One-Time Password). Codul poate fi generat utilizând o aplicație specializată precum Google Authenticator sau poate fi primit de dispozitivul mobil sub forma unui SMS.

Google Authenticator este o aplicație gratuită disponibilă în orice mediu de lucru (IOS, Android, OSX, Linux, Windows) și orice tip de dispozitiv (*smartphone*, *desktop* etc.). În cadrul prezentei teze s-a optat pentru utilizarea aplicației Google Authenticator.

Structura de autentificare TOTP utilizând cod QR:

1. Administratorul *cloud* adaugă contul TOTP al utilizatorului
2. Administratorul generează codul secret, îl convertește în imagine QR și îl trimite prin *email* spre utilizator
3. Utilizatorul primește prin *email* codul secret necesar generării codului TOTP sub forma unei imaginii QR. Utilizând aplicația Google Authenticator, se scanează cod-ul QR pentru a obține codul unic TOTP (factor de posesie)
4. Utilizatorul accesează pagina *web* a mediului *cloud* OpenStack în care introduce utilizatorul și parola (factor de cunoaștere), respectiv codul unic generat de aplicația Google Authenticator.

Structura de autentificare enunțată mai sus este reprezentată grafic în Fig. 2.

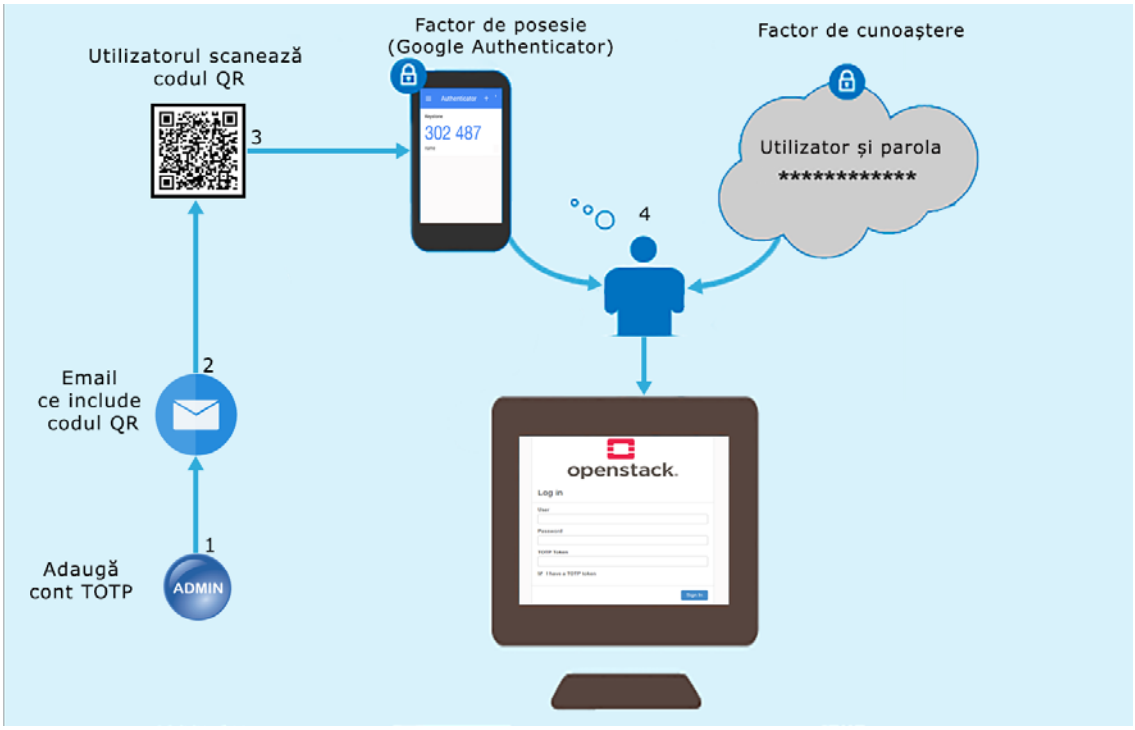

Fig. 2. Structura de autentificare cu doi factori [IG]

Codul unic TOTP este format din 6 caractere numerice și este amplasat la finalul codului trimis de formular spre autorizare. Modulul *password_totp.py* extrage la început codul unic și îi verifică autenticitatea, iar dacă rezultatul este unul pozitiv se verifică utilizatorul și parola. Dacă

datele introduse sunt validate, utilizatorului îi este permis accesul în mediul *cloud*. Modificările aferente propuse de autor au fost prezentate pe larg în cadrul subcapitolelor IV.3 și IV.4.

S-a dezvoltat aplicația *add_totp_user.sh* prin care întregul proces de adăugare utilizator TOTP, generare, convertire și trimitere cod secret în format imagine QR a fost automatizat.

Adăugare TOTP în interfața *web* (HORIZON)

Interfața web utilizată pentru autentificare a fost modificată pentru a permite introducerea codului unic. În cadrul Fig. 3 este prezentată noua interfață web cu modificările aferente. Utilizatorii care dețin cont TOTP trebuie să bifeze opțiunea *I have a TOTP token* în cadrul interfeței *web*, pentru a activa câmpul de intrare corespunzător codului unic (*TOTP token*). Opțiunea a fost adăugată pentru a permite utilizatorilor, care nu dețin încă cont TOTP, autentificarea în mediul *cloud*.

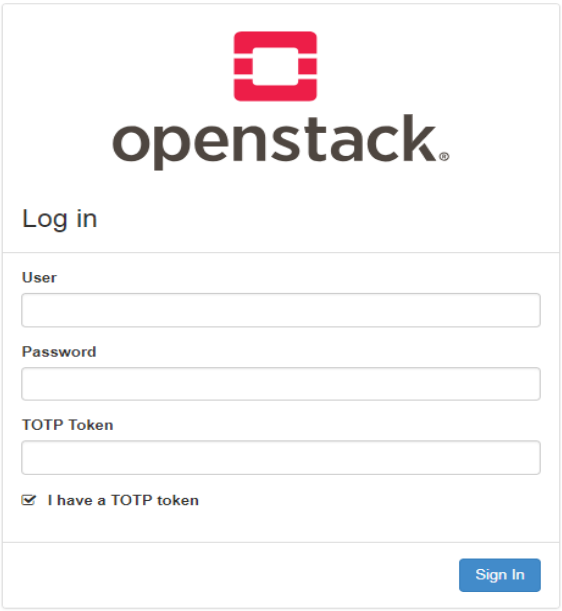

Fig. 3. OpenStack interfața de autentificare [IG]

Implementare modul de autentificare TOTP

Datele de autentificare introduse în formularul de autentificare, prezentat în cadrul subcapitolului IV.3, sunt transmise mai departe componentei Keystone. Procesul de autentificare este exemplificat în Fig. 4.

Procedura implică criptare și autorizare la nivel avansat. Pentru a evita orice problemă de securitate ca urmare a introducerii componentei TOTP în procesul de autentificare, în cadrul formularului prezentat în subcapitolul IV.3, codul TOTP este adăugat la parola utilizatorului. Astfel spre componenta Keystone se va transmite utilizator, parola și codul aferent.

În acest fel se elimină necesitatea implementării unui modul separat și se utilizează un modul de tip *plugin* conceput pentru componenta Keystone, care administrează partea de autorizare.

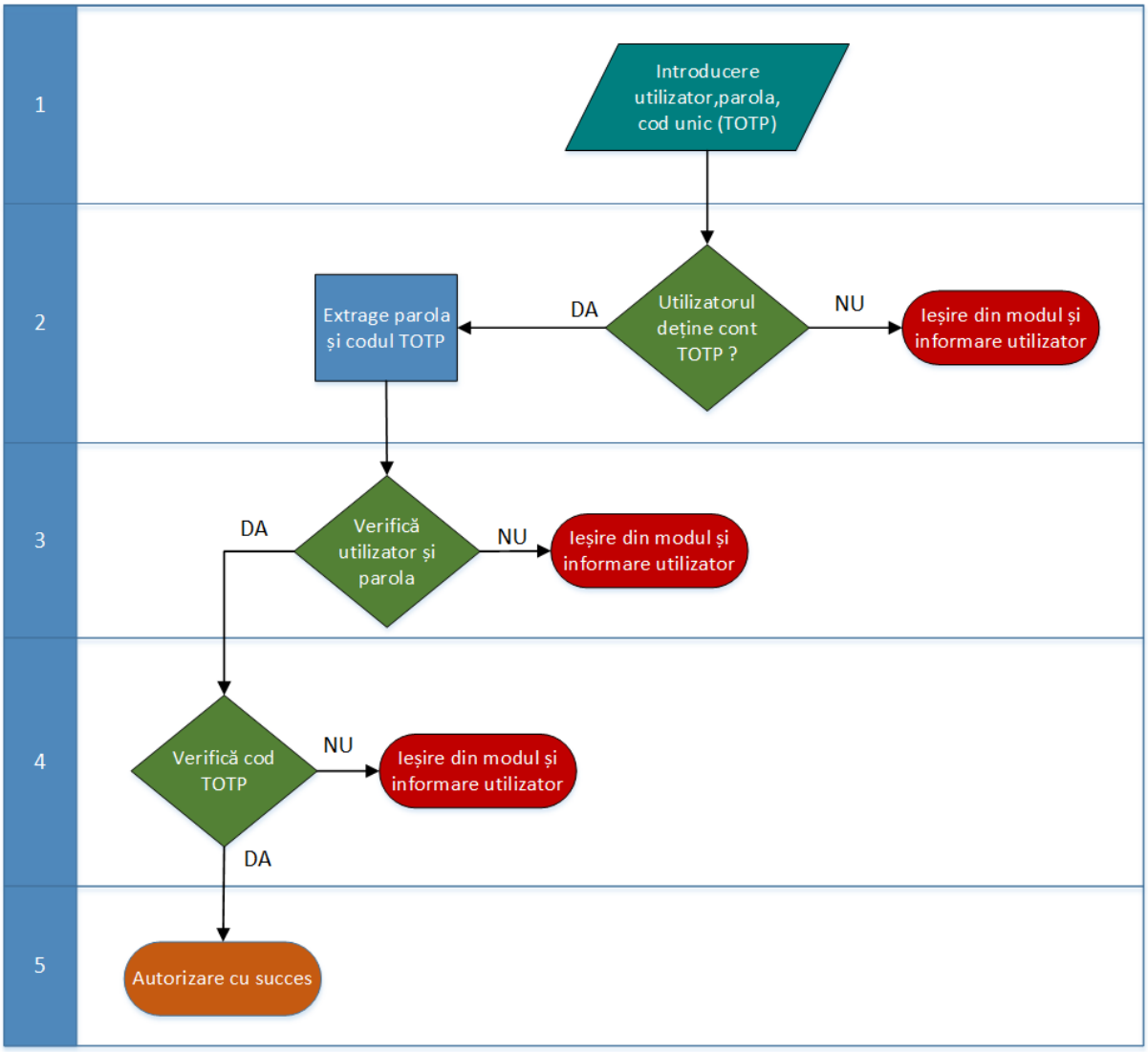

Fig. 4. Diagramă funcțională modul TOTP OpenStack [IG]

În cadrul modului (*password_totp.py*) se realizează următoarele acțiuni:

1. Se preiau datele introduse în pagina de autentificare *web* (utilizator, parolă, cod unic TOTP);
2. Se verifică dacă utilizatorul deține cont TOTP.
   Dacă răspunsul este pozitiv, atunci se extrage parola și codul TOTP din câmpul parolă
   Dacă rezultatul este negativ, se părăsește modulul și se informează utilizatorul;
3. Se verifică autenticitatea utilizatorului și parola.
   Dacă răspunsul este pozitiv, se trece la poziția 4 – Verificare cod TOTP
   Dacă rezultatul este negativ, se părăsește modulul și se informează utilizatorul;
4. Se verifică dacă codul TOTP este corect.
   Dacă răspunsul este pozitiv, autorizarea a avut loc cu succes. În acest caz se realizează redirectarea spre pagina de administrare *cloud*.
   Dacă rezultatul este negativ, se părăsește modulul și se informează utilizatorul.

Dacă codul TOTP nu este formatat corespunzător sau nu există cont TOTP se raportează în *log*-uri.

Activarea autentificării cu doi factori are implicații de asemenea la nivelul liniei de comandă OpenStack. Pentru a contracara această problemă autorul a dezvoltat aplicația *auth_local_keystone.sh*, care permite autentificarea din linia de comandă folosind și codul unic. Codurile aplicațiilor folosite pe parcursul tezei sunt incluse în cadrul anexelor A-J.

În ***capitolul V*** este prezentată o analiză a securității *cloud* OpenStack, folosind *software* dedicat. În acest scop se utilizează aplicațiile: Nessus, Metasploit și OpenVAS pentru analiza securității *cloud* din interiorul, cât și din exteriorul rețelei. Pentru analiza exterioară a securității *cloud* se apelează la aplicația *web* Tenable IO.

Nessus este un analizor proprietar al vulnerabilităților *cloud* și este dezvoltată de firma Tenable Network Security. Nessus este una din puținele aplicații care deține module proiectate special pentru OpenStack.

Metasploit Pro este un analizor de securitate care permite exploatarea vulnerabilităților descoperite.
OpenVAS este un analizor de securitate. Aplicația este gratuită sub licență GNU.
Scanarea securității *cloud* din interior se realizează cu ajutorul sistemului *InCloud* (adresa IP 20.20.20.10) instalat în interiorul platformei OpenStack. InCloud este un server care rulează Linux Ubuntu 16 pe care s-au instalat aplicațiile Nessus Professional 7.0, Metasploit x64 și OpenVAS 9.

Scanarea securității *cloud* din exterior se realizează din 3 locații diferite utilizând aplicațiile Tenable .io, Metasploit x64, OpenVAS.

Tenable .io este o versiune mai avansată a aplicației Nessus Professional 7, care permite realizarea *scan*-urilor de securitate din diferite locații de pe Glob.

Metasploit x64 s-a instalat pe un sistem care rulează Windows 7 și este localizat în afara rețelei *cloud*. OpenVAS a fost instalat pe un sistem cu OS Ubuntu 16 ce este localizat în afara rețelei *cloud*.

Structura mediului de testare este prezentat sugestiv în Fig. 5.

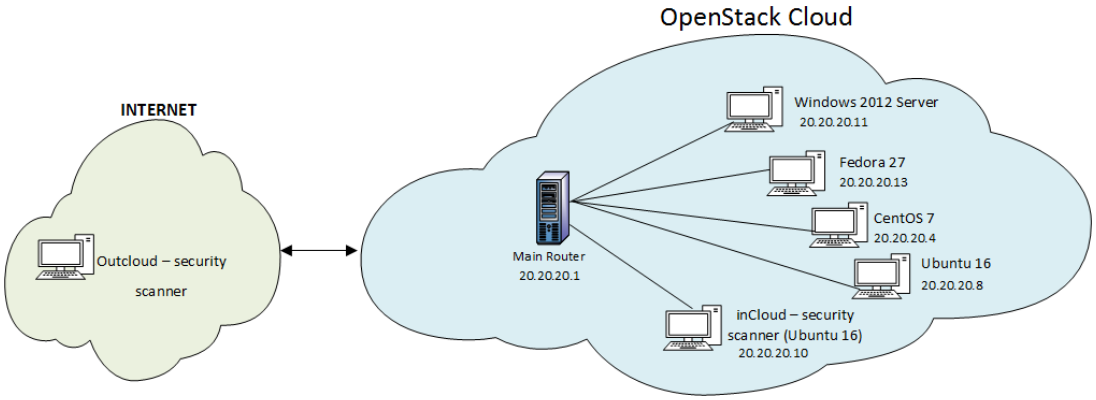

Fig. 5. Structura mediului de testare *cloud* OpenStack [IG]

Aplicațiile folosite analizează porturile rețea ale serverului OpenStack (IP 20.20.20.1) și raportează vulnerabilitățile descoperite pe fiecare port.

Suplimentar față de analizarea nivelului de securitate OpenStack *cloud* s-a urmărit găsirea aplicației ce oferă cele mai complete rezultate.

Pentru evaluarea performanțelor oferite de fiecare *software* de scanare a vulnerabilității, s-au numărat porturile descoperite de fiecare aplicație la realizarea analizei de securitate. Sunt realizate în acest sens 3 situații după fiecare tip de scan: intern, mașini virtuale găzduite în mediu *cloud* respectiv scanare externă.

După documentația OpenStack, mediul *cloud* ar trebui să aibă 29 de porturi deschise. Unele porturi nu sunt accesibile scanerelor de securitate deoarece configurația de securitate a aplicației nu o permite sau datorită regulilor de tip *firewall*

Evaluarea nivelului de securitate – scanare rețea internă

În vederea *scanării* rețelei interne este folosită ca adresă destinație privată IP 20.20.20.1 care aparține *cloud*-ului Openstack.

Aplicația *Nessus* utilizează opțiunea *Advanced scan* (Scanare avansată). Vulnerabilități descoperite :

- 2 probleme de securitate de mare importanță:
- *Acces fără autentificare la serverul VNC: utilizează porturile TCP 5901-5903 (VNC Server Unauthenticated Access on TCP ports 5901-5903)*
- *Redis Server: autentificare fără parolă utilizând portul TCP 6379 (Redis Server Unprotected by Password Authentication on TCP PORT 6379)*
- 3 probleme de securitate de importanță medie
- *Permisiune pentru metodele HTTP TRACE / TRACK pentru portul TCP 5000 (HTTP TRACE / TRACK Methods Allowed TCP port 5000)*
- *Protocol avansat de redirecționare a mesajelor la distanță (AMQP) autentificare cu text în clar pe portul TCP 5672 (Remote Advanced Message Queuing Protocol (AMQP) Cleartext Authentication problem TCP port 5672)*
- Serviciu *memcached* neprotejat pe portul 11211 *(Unprotected memcached TCP port 11211)*
- problemă de securitate de mică importanță *Modul de criptare cifru (CBC) este activat pentru serverul SSH pe portul TCP 22* (*SSH Server CBC Mode Ciphers Enabled - TCP port 22)*

Aplicația *Metasploit Pro – folosind opțiunea "WebApp test"*

Scan-ul extern nu a descoperit nici o vulnerabilitate. *Software*-ul a descoperit însă deschise următoarele porturi: 22, 80, 111, 873, 3306, 5000, 5900, 5901, 5903, 5904, 5907, 6000, 6080, 6379, 8080, 11211 și portul UDP 111 (PORTMAP).

OpenVAS utilizând opțiunea *Scan/Tasks/Tasks Wizard*. Vulnerabilități descoperite:
- *Acces fără autentificare la serverul VNC utilizând porturile TCP 5901-5903*
- *Permisiune pentru metodele HTTP TRACE / TRACK pentru portul TCP 5000*
- *Modul de criptare cifru (CBC) este activat pentru serverul SSH pe portul TCP 22*

OpenVAS a raportat în plus față de Nessus următoarea problemă de securitate:
- *marcaje de timp TCP (TCP timestamps)*

Această problemă de securitate permite calcularea duratei de funcționare a serverului. Vulnerabilitatea raportată este de mică importanță.

Analizând numărul de porturi descoperit de fiecare aplicație putem concluziona următoarele: Metasploit a descoperit 17 porturi, OpenVas a descoperit 9 porturi, urmat de Nessus cu 8 porturi. Rezultatele obținute sunt ilustrate grafic în Fig. 5.

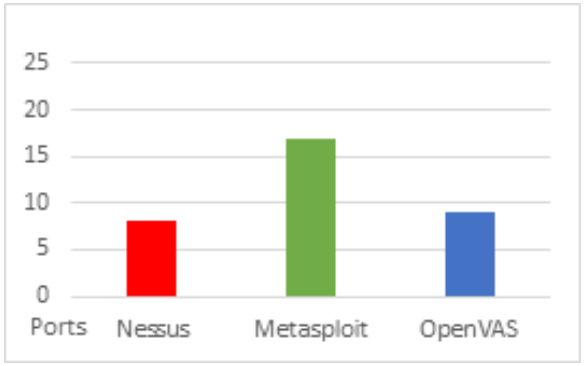

Fig. 6. Evaluarea securității *cloud* - scanare rețea internă [IG]

Evaluarea securității – scanare rețea internă pentru mașinile virtuale din *cloud*

Scanarea securității *cloud* pentru rețeaua internă permite analizarea stațiilor găzduite de acesta. necesită cunoașterea în prealabil a clasei IP sau a claselor IP alocate pentru sistemele găzduite în *cloud*. În cadrul platformei de testare autorul a folosit clasa IP 20.20.20.0/24.

Folosind unul din scanerele de securitate (de ex. Nessus), se pornește procedura de scanare a întregii clase IP. Ca rezultat se va primi un raport complet cu toate stațiile/serverele descoperite.

Unele mașini virtuale au acces la mai multe resurse *cloud* decât altele. Compromiterea unei mașini virtuale cu acces elevat la această platforma poate permite accesul la toate componentele sale.

În Fig. 6 sunt reprezentate rezultatele obținute cu aplicația Nessus la scanarea rețelei locale *cloud*.

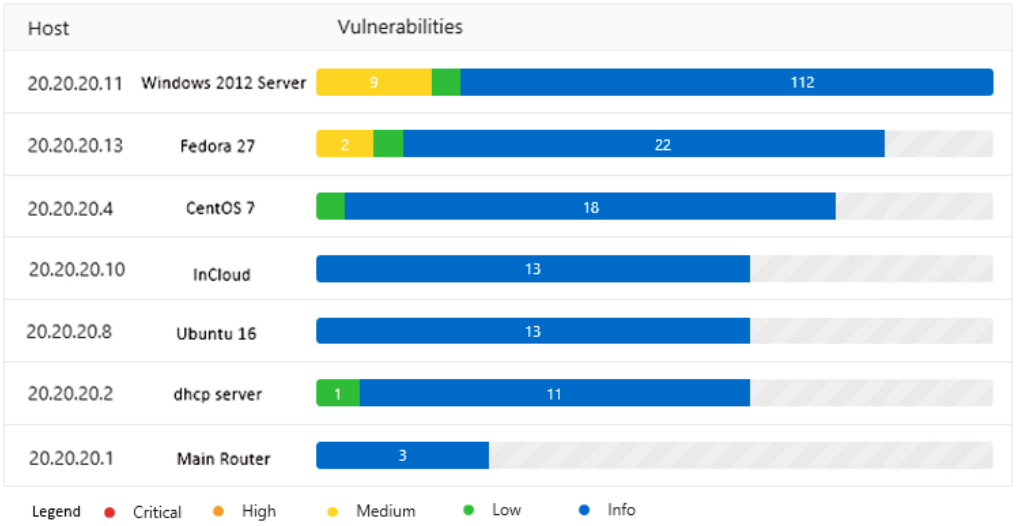

Fig. 7. Nessus – raport scanare rețea locală *cloud [IG]*

Raportul generat de Nessus nu include și numele sistemului scanat. Pentru o mai ușoară înțelegere a sistemelor afectate și prezentate în Fig. 6 s-a inclus în dreapta adresei IP și numele sistemului respectiv. Analizând raportul prezentat putem observa că serverul cu sistemul de operare Windows are cele mai multe vulnerabilități, urmat de sistemul cu Fedora și în final CentOS.

Evaluarea securității – scanare rețea externă

Această evaluare s-a făcut folosind două opțiuni:

1. *Tenable .io* – folosind opțiunea *"Advanced scan" (Scanare avansată)*

Vulnerabilitățile descoperite și porturile deschise sunt identice cu cele raportate de Nessus la scanarea internp cu excepția portului TCP 11211 (memcached neprotejat)

2. *Metasploit Pro* - folosind opțiunea *"WebApp test" (Testare aplicații web)*

Scanarea externă nu a descoperit nicio vulnerabilitate.

Raportul final pune în evidență totuși ca fiind deschise următoarele porturi TCP: 22, 80, 111, 873, 3306, 5000, 5900, 5901, 5903, 5904, 5907, 6000, 6080, 6379, 8080 și portul UDP 111. Se poate observa că *scan*-ul extern nu a detectat ca fiind deschis portul 11211.

OpenVAS în cadrul scanării externe a raportat aceleași porturi descoperite în cadrul scanării interne cu excepția portului 11211. Metasploit a descoperit 16 porturi deschise, OpenVAS 8 porturi, urmat de Nessus cu 7 porturi.

Rezultatele obținute sunt reprezentate grafic în Fig. 8.

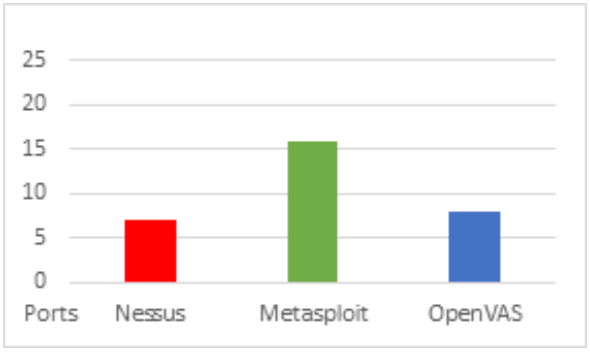

Fig. 8. Evaluarea securității *cloud* – scanare rețea externă [IG]

Analizând graficele din fig. 6-8, s-a constatat că aplicația Metasploit a descoperit cele mai multe porturi deschise. Cu toate acestea, Nessus a furnizat cele mai multe informații despre porturile descoperite și a oferit sugestii despre modul de rezolvare a problemelor evidențiate. OpenVAS este o aplicație gratuită în raport cu aplicațiile Nessus și respectiv Metasploit. Cu toate acestea aplicația a oferit rezultate surprinzător de bine organizate și detaliate. Raportul generat de OpenVAS include lista porturilor descoperite ca fiind deschise, detalierea problemei găsite și în plus oferă informații cu privire la modul de remediere pentru fiecare situație în parte.

Acest studiu permite analiza securității în orice moment și reprezintă o procedură recomandată de fiecare dată la instalarea unui nou mediu *cloud*, sau când sunt efectuate modificări ale configurației standard.

IV. Contribuții și direcții de cercetare viitoare

Domeniul *cloud computing* este utilizat pe scară tot mai largă în toate domeniile de activitate. Plasarea datelor sensibile într-un mediu exterior de către companii sau persoane fizice necesită în primul rând îndeplinirea condițiilor de siguranță că aceste date nu vor fi pierdute sau accesate de persoane neautorizate.

Odată cu intrarea în vigoare a reglementărilor internaționale și corelarea acestora cu acordul SLA, încrederea în siguranța datelor a crescut. Ca urmare, în ultimii ani asistăm la o utilizare tot mai răspândită a acestor servicii, atât la nivel personal cât și profesional.

Evoluția tehnologică tot mai rapidă impune și o dezvoltare pe măsură a mediului *cloud*. Tehnicile de securizare trebuie optimizate și rafinate într-un mod transparent pentru utilizatorul final. Mărirea securității unui mediu implică de cele mai multe ori si creșterea timpului de autentificare pentru utilizator. Tehnologiile viitorului promit să reducă și chiar să elimine necesitatea introducerii unor date pentru autentificare.

În rezumat, principalele contribuții teoretice aduse în cadrul acestei teze de doctorat sunt:

- În capitolul I, s-au evidențiat diferențele dintre centrele de date și mediul *cloud* și s-au arătat avantajele aduse de tehnologia *cloud computing.* Pentru a putea asimila noțiunea de *cloud comuting*, sunt prezentate caracteristicile definitorii și modul de interconectare a componentelor sale. S-au prezentat noile tendințe din acest domeniu și s-au evidențiat avantajele aduse de containerele și microserviciile *cloud* ca o viabilă perspectivă pentru viitoarele tehnologii din această sferă tehnologică.
- Securizarea mediului *cloud* se optimizează în raport cu modul de livrare a serviciilor oferite și în funcție de destinația sa. În acest sens s-a realizat o clasificare a serviciilor *cloud* după modul de livrare (SaaS, PaaS, IaaS) și după modul lor de implementare (public, privat, hibrid și comunitar).
- În capitolul II, s-a realizat un studiu privind stadiul actual al securității din domeniul *cloud computing*. În acest sens sunt sistematizate organizațiile de standardizare și reglementare din domeniul securității informației. Acordul de calitate a serviciilor (SLA) reglementează contractual calitatea, disponibilitatea și responsabilitățile serviciilor oferite de furnizor. S-au sintetizat caracteristicile definitorii ale unui bun acord SLA, informație utilă la alegerea celui mai adecvat furnizor de servicii *cloud.*
- Securizarea mediului *cloud* nu ar fi posibilă fără a lua în considerare toate componentele sale. În acest sens s-a studiat detaliat modul de securizare a principalelor niveluri din sistem: *rețea, gazdă* și *aplicație.* În acest scop s-a realizat o paralelă între structura rețelelor clasice și virtuale pentru a pune în evidență avantajele de natură structurală oferite de cea din urmă. Sunt sintetizate avantajele și dezavantajele oferite la partea de securitate de cele 3 tipuri de rețele virtuale: VLAN, VXLAN, SDN, fiind sistematizate problemele de securitate ale nivelului rețea utilizând ca referință frecvența și importanța vulnerabilităților. Informațiile prezentate sunt completate de soluții generale de prevenire sau rezolvare a problemelor prezentate.

Securitatea la nivel de gazdă este abordată după modul de livrare a serviciilor SaaS, PaaS, respectiv IaaS, fiind prezentată sintetic modalitatea de securizare a hipervizorului și a mașinilor virtuale aferente.
Ciclul de viață al aplicației securizate (SDLC) descris în secțiunea II.3.3.1 sintetizează modul în care *cloud computing*-ul influențează securitatea aplicației pornind din faza de proiectare până la cea de implementare. Sunt reprezentate grafic fazele dezvoltării unei aplicații securizate și sunt punctate elementele esențiale care trebuie luate în considerare la implementarea ei.

- S-a realizat o paralelă între soluțiile de autentificare cu doi factori utilizate pentru *cloud*-urile publice (secțiunea II.3.3.2). Rezultatele obținute au fost folosite ca referință pentru implementarea unui modul de autentificare similar pentru *cloud*-ul privat OpenStack (cap. IV)
- S-a realizat un studiu detaliat cu privire la cele mai cunoscute vulnerabilități și s-au oferit soluții pentru remedierea lor, fiind prezentate statistici reprezentând vulnerabilități descoperite pentru mediul OpenStack Redhat în intervalul de timp 2013-2018. Informațiile prezentate în mod tabelar și în mod grafic sunt utile pentru a observa modul de evoluție al securității *cloud* și a pune în evidență cele mai cunoscute vulnerabilități din acest domeniu.

Contribuțiile practice aduse prin prezenta teză de doctorat sunt:

- În cadrul capitolului III, a fost prezentat modul în care poate fi utilizat *cloud*-ul privat OpenStack. În cadrul acestui proces s-au detaliat arhitectura și distribuțiile dezvoltate până în momentul de față. Suplimentar față de documentația de instalare RDO, s-au prezentat următoarele informații:
  - modalitatea de configurare a *host*-ului în format FQDN
  - este detaliată funcționalitatea și modul de utilizare al fișierului de configurare *packstack-answers-yyyymmdd-xxxx.txt*, fișier generat la la finalizarea instalării
  - captură de ecran cu informațiile afișate la finalul instalării *cloud*
  - procedura de securizare a autentificării web în mediul OpenStack.
- În capitolul IV, se prezintă arhitectura pentru optimizarea autentificării în mediul OpenStack *cloud*, prin adăugarea posibilității de autentificare cu doi factori. Astfel, în cadrul paginii de autentificare s-a adăugat pe lângă câmpul utilizator și parolă, un nou câmp pentru introducerea unui cod unic. Codul se schimbă automat la 30 de secunde. În acest sens s-a dezvoltat un modul special implementat în limbajul Python și s-au adus o serie de modificări unor fișiere care deservesc pagina de autentificare. Codul unic se poate genera cu ajutorul unui dispozitiv mobil (telefon, tabletă, laptop) pe baza unei parole secrete generate de administratorul *cloud*, trimisă către utilizator prin *email* sub forma unui cod QR.

Pentru realizarea acestui proiect s-au realizat aplicații pentru:

- Adăugare utilizator TOTP (aplicație *add_totp.sh*)
- Modul de autentificare TOTP (modul *password_totp.py*) pentru versiunile *cloud* Pike (2017), Ocata (2017) respectiv Queens (2018)
- Generare cod QR pe bază de cod secret (aplicație *qr_make.py <cod secret>*)

- Trimitere cod QR prin *email* (aplicație *qr_sendmail.py user@email.com*)
- Sistem TOTP integrat (aplicație *add_totp_user.sh utilizator user@email.com)* care înglobează toate aplicațiile menționate mai sus și aduce o serie de îmbunătățiri întregului proces de adăugare și trimitere cod QR.

Aplicația realizează următoarele acțiuni:

- Generează cheia secretă utilizând coduri aleatorii (16 caractere)
- Obține ID-ul utilizatorului specificat în linia de comandă
- Alocă un *token* pentru utilizator, necesar autentificării locale la sistem
- Creează contul TOTP pentru utilizatorul specificat în linia de comandă.
- Generează codul QR în fișierul totp.png apelând aplicația *qr_make.py*
- Afișează codul secret respectiv codul secret codat în bază 32
- Trimite *email* cu codul QR la utilizatorul specificat în linia de comandă, apelând aplicația *qr_make.py*

Acest sistem de autentificare este folosit deja pe scară largă de sistemul bancar și *site*-uri cunoscute din mediul online (Apple, Microsoft, Facebook, Google, Yahoo, etc.), dar nu este implementat în mediul *cloud*.

- S-a dezvoltat aplicația *auth_local_keystone.sh*, care permite utilizatorilor să se autentifice la mediul de linie de comandă OpenStack (OpenStackClient) folosind autentificarea cu doi factori. Aplicația setează variabilele sistem necesare pentru autentificare și creează un nou *token* pentru utilizatorul definit în aplicație. Întrucât codul unic expiră în scurt timp, se activează autentificarea de tip *token* pe perioada sesiunii curente și se dezactivează autentificarea de tip utilizator/parolă.
  Aplicația este utilă pentru toți utilizatorii care doresc să configureze mediul OpenStack la nivel avansat și elimină dezavantajul expirării codului unic prin activarea sistemului de autentificare cu cheie privată de tip *token*.
- În capitol V s-a realizat o analiză a securității mediului *cloud* OpenStack versiunea Pike, utilizând *software* dedicat. În cadrul acestui proces s-a urmărit stabilirea nivelului de securitate a acestui mediu, atât din interiorul cât și din exteriorul rețelei *cloud*. Testele au fost realizate utilizând trei scanere de vulnerabilități: Nessus, Metasploit și OpenVAS. O scanare externă s-a realizat utilizând aplicația *web* Tenable IO.

Analiza nivelului de securitate s-a realizat în 3 etape:

1. Scanare internă – verificare IP sistem cloud din rețeaua internă
2. Scanare internă – verificare mașini virtuale din *cloud*
3. Scanare externă – verificare IP sistem *cloud* din Internet

Aplicațiile utilizate analizează porturile rețea ale serverului *cloud* OpenStack și raportează vulnerabilitățile descoperite pe fiecare port. Suplimentar ele oferă și informații cu privire la contracararea problemelor raportate. Analiza securității mașinilor virtuale găzduite în *cloud* permite găsirea nivelului de securizare asigurat de hipervizorul și *firewall*-ul OpenStack și modul de contracarare a eventualelor atacuri.

Complementar analizării nivelului de securitate asigurat de OpenStack *cloud* s-a urmărit găsirea analizorului de securitate optim pentru acest tip de *cloud.* În acest sens s-a calculat numărul de porturi raportate de fiecare aplicație.

Analizând rezultatele obținute, s-a constatat că aplicația Metasploit a descoperit cele mai multe porturi deschise. În schimb, Nessus a furnizat cele mai multe detalii despre porturile descoperite și a oferit sugestii despre modul de rezolvare a problemelor evidențiate. Rezultatele obținute la finalul fiecărei etape au fost reprezentate sub formă grafică pentru o mai ușoară asimilare. Analiza securității atât din interior, cât și exterior, este utilă în special la verificarea și securizarea porturilor de acces la *cloud.*

Securitatea *cloud* este un domeniu foarte vast. În cadrul tezei s-a pus accent pe securitatea autentificării și securitatea componentei rețea. Direcțiile de cercetare viitoare se vor concentra în continuare pe optimizarea autentificării în doi pași.

Atenția se va axa simultan pe mărirea nivelului de securitate și simplificarea procesului de autentificare. Suplimentar procedurii de autentificare elaborate pe parcursul acestor studii se dorește implementarea autentificării cu cheie USB și adăugarea opțiunii de generare a codului unic prin SMS. Procedura presupune adaptarea corespunzătoare a bazelor de date și aplicațiilor OpenStack pentru a permite noile funcții. Codul secret folosit ca bază de Google Authenticator, nu este salvat în *cloud* sub formă text. El este salvat în sistem sub forma unei chei private și poate fi verificat doar cu ajutorul unei chei pereche.

Implementarea sistemului SMS de trimitere a cheii unice necesită o bază de date cu toate codurile secrete alocate. Securizarea acestor date trebuie realizată sub două aspecte: criptare și control acces. Procedura de trimitere a mesajelor SMS se poate implementa prin instalarea unui echipament de tip gateway SMS sau prin utilizarea serviciilor SMS oferite de o terță companie (ex. Twilio).

Aplicațiile de analiză a securității detaliate pe parcursul capitolului V pot fi utilizate ca punct de plecare pentru securizarea avansată a mediului *cloud*. Astfel, analiza securității mediului *cloud* se poate optimiza prin implementarea unui sistem inteligent de verificare a vulnerabilităților serviciilor oferite (IDS) prin consultarea unor baze de date de securitate internaționale. IDS utilizează două tehnici de detecție a vulnerabilităților în timp real: detecția de anomalii (bazată pe comportamentul utilizatorilor) și detecția de semnătură (bazată pe semnăturile atacurilor cunoscute). Combinarea acestor două tehnici oferă soluții optime de detecție a problemelor de securitate în timp real. Administratorul acestui mediu este informat în timp util despre potențialele probleme de securitate și poate lua măsurile necesare. Majoritatea soluțiilor de *cloud* public au deja integrat sistemul IDS, dar nu este și cazul *cloud*-urilor private. Acest domeniu poate completa mediul de cercetare. Îmbinând acest sistem de securitate cu soluția de autentificare prin SMS sau cheie USB putem spune că am realizat un sistem cu un înalt grad de securitate ce poate avea aplicații de la mediul academic până la cel financiar - bancar.

V. Diseminarea rezultatelor

- **Ionel Gordin**, *Virtualizing real servers with unsupported OS by VMware vCenter Converter*, RoEduNet - Networking in Education and Research (NER'2015) Craiova, Romania, DOI: 10.1109/RoEduNet.2015.7311981 , http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7311981

- **Ionel Gordin**, *Optimized P2V Conversion Using VMware Converter Standalone*, Conferința: "Le questionnement sur l'éthique dans la recherche en sciences techniques, économiques et sociales (CNAM)" Paris, Franța, Jurnal: JCSCS, Vol. 8, no. 2, Oct 2015, http://electroinf.uoradea.ro/index.php/reviste/jcscs.html

- **Ionel Gordin**, *IAAS private cloud comparison– OpenStack vs Cloudstack*, University of Pitești scientific bulletin series: electronics and computers science, 2016: Vol 16, Issue 1, http://bulletin.feccupit.ro

- **Ionel Gordin**, *Energy aware of cloud computing development using cloud simulators*, Pitesti, Romania, Edu World 2016 - 7th International Conference – 4-5 november 2016, DOI: 10.15405/epsbs.2017.05.02.159, http://www.eduworld.ro/

- **Ionel Gordin**, Adrian Graur, Doru Balan, *Development of Eco-Friendly Cloud Computing Environments*, 14th International Conference on Engineering of Modern Electric Systems, Oradea, Romania, 1-2 June 2017, DOI: 10.1109/EMES.2017.7980400, http://www.icemes.ro/icemes2017/

- Iuliana Chiuchisan, Doru-Gabriel Balan, Oana Geman, Iulian Chiuchisan, **Ionel Gordin**, *A Security Approach for Health Care Information Systems*, The 6th IEEE International Conference on E-Health and Bioengineering, Sinaia, Romania, June 22-24, 2017, DOI: 10.1109/EHB.2017.7995525, http://www.ehbconference.ro

- **Ionel Gordin**, Adrian Graur, Alin Potorac, Doru Balan, *Security Assessment of OpenStack cloud using outside and inside software tools*, 14th International Conference on Development and Application Systems (DAS), Suceava, Romania, May 24-26, 2018, http://www.dasconference.ro

- **Ionel Gordin**, Adrian Graur, Alin Potorac, *Two factor authentication framework for private cloud*, 23rd International Conference on System Theory, Control and Computing, October 9-11, 2019, Sinaia, Romania, http://icstcc2019.cs.upt.ro, in curs de publicare

Bibliografie teză de doctorat

[1] „Cloud storage,” [Interactiv]. Available: https://en.wikipedia.org/wiki/Cloud_storage. [Accesat 25 2 2016].

[2] „Cloud Computing Architecture Diagrams,” [Interactiv]. Available: https://www.conceptdraw.com/How-To-Guide/cloud-computing-architecture-diagrams. [Accesat 1 11 2018].

[3] „Hypervisors, virtualization, and the cloud: Learn about hypervisors, system virtualization, and how it works in a cloud environment,” [Interactiv]. Available: http://www.ibm.com/developerworks/cloud/library/cl-hypervisorcompare/.

[4] E. Siebert, „Top 10 hypervisors: Choosing the best hypervisor technology,” [Interactiv]. Available: https://searchservervirtualization.techtarget.com/tip/Top-10-hypervisors-Choosing-the-best-hypervisor-technology. [Accesat 1 3 2018].

[5] S. K. S. L. Tim Mather, „APIs,” în *Cloud security and privacy*, O'Reilly Media, 2009, p. 338.

[6] „30 essential container technology tools and resources,” [Interactiv]. Available: https://techbeacon.com/30-essential-container-technology-tools-resources. [Accesat 2017 9 23].

[7] „WHAT WOULD YOU LIKE: IAAS, PAAS OR SAAS?,” [Interactiv]. Available: https://blog.qsc.de/2012/12/was-hatten-sie-denn-gerne-iaas-paas-oder-saas/. [Accesat 1 2 2018].

[8] „Managed Services – Public Cloud,” [Interactiv]. Available: http://www.cloudhosttechnologies.com/service-2/cloud-services/managed-services-public-cloud/. [Accesat 5 3 2017].

[9] „State of the cloud report,” [Interactiv]. Available: https://www.rightscale.com/. [Accesat 21 6 208].

[10] D. Sullivan, The Definitive Guide to Cloud Computing, Realtime Publishers., 2010, pp. 76-77,141-142.

[11] S. S. Shubh Tulika, „Man-In-The-Middle-Attack Prevention Using HTTPS and SSL,” *International Journal of Computer Science and Mobile Computing,* vol. 5, nr. 6, p. 569 – 579, 2016.

[12] T. G. W. Jansen, „Guidelines on security and privacy in public cloud computing,” 2011. [Interactiv]. Available: http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-144.pdf. [Accesat 4 April 2017].

[13] T. Bittman, „Private Cloud Computing: Target Services That Need Agility,” 28 2 2012. [Interactiv]. Available: https://www.gartner.com/doc/1935722. [Accesat 3 3 2017].

[14] „Managed Services – Private Cloud,” [Interactiv]. Available: http://www.cloudhosttechnologies.com/managed-services-private-cloud/. [Accesat 3 3 2017].

[15] H.-J. Niethammer, „EN 50600-X: The New European Standard For Data Center Design,” 19 1 2016. [Interactiv]. Available: http://www.commscope.com/Blog/EN-50600-x-The-New-European-Standard-for-Data-Center-Design/. [Accesat 20 1 2017].

[16] C. Burns, „How to build a private cloud,” 2014. [Interactiv]. Available: http://www.networkworld.com/article/2166356/cloud-computing/how-to-build-a-private-cloud.html. [Accesat 15 1 2017].

[17] M. O'Loughlin, „The Service Catalog - A practitioner Guide,” 2010. [Interactiv]. Available: https://www.vanharen.net/Samplefiles/9789087535711_the-service-catalog.pdf. [Accesat 10 1 2017].

[18] M. Farley, „Rethinking Enterprise Storage. A Hybrid Cloud Model,” 2013. [Interactiv]. Available: https://download.microsoft.com/DOWNLOAD/8/5/6/85677038-09DE-4F20-AECD-C7A44B5A7E1E/679603EBOOK.PDF. [Accesat 5 3 2017].

[19] „ISO/IEC 27001:2013,” [Interactiv]. Available: https://ro.wikipedia.org/wiki/ISO/IEC_27001:2013. [Accesat 1 3 2017].

[20] M. Tulloch, Introducing Windows Azure.For IT Professionals, Microsoft Press, 2013, pp. 53-61.

[21] „Hybrid Cloud Providers On Architecture On Is A Hybrid Cloud A Reality For CPA Firms Xcentric,” [Interactiv]. Available: http://dentrodelasala.com/wonderful-hybrid-cloud-providers/hybrid-cloud-providers-on-architecture-on-is-a-hybrid-cloud-a-reality-for-
cpa-firms-xcentric/. [Accesat 11 9 2018].

[22] B. Sosinsky, Cloud Computing Bible, Wiley Publishing, Inc, 2011, pp. 5-9.

[23] „Community Cloud Model,” [Interactiv]. Available: https://www.tutorialspoint.com/cloud_computing/cloud_computing_community_cloud_model.htm. [Accesat 2 11 2018].

[24] G. Briscoe și A. Marinos, „Digital ecosystems in the clouds: Towards community cloud computing,” în *DEST '09. 3rd IEEE International Conference*, 2009.

[25] „Cloud Computing: Benefits and Challenges,” [Interactiv]. Available: http://transformcustomers.com/cloud-computing-benefits-and-challenges/. [Accesat 10 7 2018].

[26] „ISO/IEC 27018:2014,” [Interactiv]. Available: https://www.iso.org/standard/61498.html. [Accesat 1 9 2018].

[27] „Article 29 Working Party,” [Interactiv]. Available: http://ec.europa.eu/newsroom/article29/news.cfm?item_type=1358. [Accesat 15 11 2018].

[28] „Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal,” [Interactiv]. Available: http://www.dataprotection.ro/. [Accesat 15 5 2018].

[29] „European Cloud Partnership,” [Interactiv]. Available: https://ec.europa.eu/digital-single-market/en/european-cloud-partnership. [Accesat 20 3 2018].

[30] „National Institute of Standards and Technology | NIST,” [Interactiv]. Available: https://www.nist.gov/. [Accesat 21 7 2018].

[31] „Cloud Security Alliance,” [Interactiv]. Available: https://cloudsecurityalliance.org/. [Accesat 1 3 2018].

[32] „Information Technology - Information Security – Information Assurance | ISACA,” [Interactiv]. Available: https://www.isaca.org/. [Accesat 12 9 2018].

[33] „International Safe Harbor Privacy Principles,” [Interactiv]. Available: https://en.wikipedia.org/wiki/International_Safe_Harbor_Privacy_Principles. [Accesat 1 12 2017].

[34] „Noul Regulament General de Protecția Datelor,” [Interactiv]. Available: http://www.dataprotection.ro/?page=Regulamentul_nr_679_2016. [Accesat 15 11 2018].

[35] „Service-level agreement,” [Interactiv]. Available: https://en.wikipedia.org/wiki/Service-level_agreement. [Accesat 15 3 2018].

[36] A. J. G. F. L. A. M. D. P. G. R. M. Mogull R, „CSA Security Guidance Version 4,” [Interactiv]. Available: https://cloudsecurityalliance.org/download/security-guidance-v4/. [Accesat 18 4 2018].

[37] „Virtual LAN,” [Interactiv]. Available: https://en.wikipedia.org/wiki/Virtual_LAN. [Accesat 1 5 2018].

[38] „Software-Defined Networks and OpenFlow,” *The Internet Protocol Journal*, vol. 16, nr. 1, p. 40, 2013.

[39] „What is VXLAN?,” [Interactiv]. Available: https://www.juniper.net/us/en/products-services/what-is/vxlan/. [Accesat 19 7 2018].

[40] „Spanning Tree Protocol,” [Interactiv]. Available: https://en.wikipedia.org/wiki/Spanning_Tree_Protocol. [Accesat 25 7 2017].

[41] „Software-Defined Networking,” [Interactiv]. Available: http://www.software-defined.net/networking.php. [Accesat 19 7 2018].

[42] „ARP spoofing,” [Interactiv]. Available: https://en.wikipedia.org/wiki/ARP_spoofing. [Accesat 5 2 2017].

[43] F. A. Locati, „OpenStack Cloud Security,” în *The different kinds of security threats*, Birmingham,UK, Packt Publishing Ltd, 2015, pp. 30-35.

[44] „Best Server Virtualization Software in 2018,” [Interactiv]. Available: https://www.g2crowd.com/categories/server-virtualization. [Accesat 15 11 2018].

[45] Microsoft, „Get started with the Microsoft Authenticator app,” [Interactiv]. Available: https://docs.microsoft.com/en-us/azure/active-directory/user-help/microsoft-authenticator-app-how-to. [Accesat 15 01 2019].

[46] „Securing your Account with Security Keys,” [Interactiv]. Available: https://cloud.google.com/solutions/securing-gcp-account-security-keys. [Accesat 15 01 2019].

[47] „Two-factor authentication for Apple ID,” [Interactiv]. Available: https://support.apple.com/en-us/HT204915. [Accesat 15 01 2019].

[48] „Transport Layer Security,” [Interactiv]. Available: https://ro.wikipedia.org/wiki/Transport_Layer_Security. [Accesat 7 6 2017].

[49] „Pretty Good Privacy,” [Interactiv]. Available: https://en.wikipedia.org/wiki/Pretty_Good_Privacy . [Accesat 1 8 2016].

[50] V. B, „The dirty dozen: 12 top cloud security threats for 2018,” [Interactiv]. Available: https://www.csoonline.com/article/3043030/security/12-top-cloud-security-threats-for-2018.html. [Accesat 23 3 2018].

[51] B. D, „Twenty Years of Attacks on the RSA Cryptosystem,” [Interactiv]. Available: https://crypto.stanford.edu/~dabo/papers/RSA-survey.pdf. [Accesat 7 5 2018].

[52] „CPU hardware vulnerable to side-channel attacks,” [Interactiv]. Available: https://www.kb.cert.org/vuls/id/584653/. [Accesat 25 5 2018].

[53] G. A. P. A. B. D. Gordin Ionel, „Security Assessment of OpenStack cloud using outside and inside software tools,” în *DAS 2018*, Suceava, 2017.

[54] „Redhat Openstack : CVE security vulnerabilities, versions and detailed reports,” [Interactiv]. Available: https://www.cvedetails.com/product/25627/Redhat-Openstack.html?vendor_id=25. [Accesat 20 1 2018].

[55] „Openstack,” [Interactiv]. Available: https://www.openstack.org/. [Accesat 3 4 2017].

[56] „Conceptual architecture,” [Interactiv]. Available: https://docs.openstack.org/liberty/install-guide-rdo/common/get_started_conceptual_architecture.html. [Accesat 3 3 2018].

[57] „OpenStack Pike Administrator Guides,” [Interactiv]. Available: https://docs.openstack.org/pike/admin/. [Accesat 5 3 2018].

[58] „RDO,” [Interactiv]. Available: https://www.rdoproject.org/. [Accesat 10 9 2018].

[59] „Red Hat - We make open source technologies for the enterprise,” [Interactiv]. Available: https://www.redhat.com. [Accesat 1 12 2017].

[60] „RHOSP – Red Hat Stack,” [Interactiv]. Available: https://redhatstackblog.redhat.com/tag/rhosp/. [Accesat 8 10 2018].

[61] „Infrastructure as a Service with OpenStack Cloud | SUSE,” [Interactiv]. Available: https://www.suse.com/products/suse-openstack-cloud/. [Accesat 12 11 2018].

[62] „OpenStack in Mirantis Cloud Platform,” [Interactiv]. Available: https://www.mirantis.com/software/openstack/. [Accesat 23 7 2018].

[63] „Oracle OpenStack | Cloud Management Software,” [Interactiv]. Available: https://www.oracle.com/corporate/features/openstack/. [Accesat 20 11 2018].

[64] „Install OpenStack services,” [Interactiv]. Available: https://docs.openstack.org/install-guide/openstack-services.html. [Accesat 10 1 2018].

[65] „DevStack,” [Interactiv]. Available: https://docs.openstack.org/devstack/latest/. [Accesat 17 3 2018].

[66] „OpenStack Docs: Networking architecture,” [Interactiv]. Available: https://docs.openstack.org/security-guide/networking/architecture.html. [Accesat 15 3 2018].

[67] „Packstack - RDO,” [Interactiv]. Available: https://www.rdoproject.org/install/packstack/. [Accesat 18 4 2018].

[68] „Openstack Docs: Overview,” [Interactiv]. Available: https://docs.openstack.org/newton/install-guide-rdo/overview.html#figure-hwreqs. [Accesat 14 6 2018].

[69] „Recommended hardware — RDO,” [Interactiv]. Available: https://www.rdoproject.org/hardware/recommended/. [Accesat 30 8 2018].

[70] „BladeCenter HS22 Product Guide,” [Interactiv]. Available: https://lenovopress.com/tips0822-bladecenter-hs22. [Accesat 8 10 2018].

[71] „BladeCenter HS22,” [Interactiv]. Available: https://lenovopress.com/tips0822-bladecenter-hs22. [Accesat 8 1 2019].

[72] „Securitate cibernetică | certSIGN,” [Interactiv]. Available: https://www.certsign.ro/ro/securitate-cibernetica. [Accesat 23 3 2018].

[73] „Multi-factor authentication,” [Interactiv]. Available: https://en.wikipedia.org/wiki/Multi-factor_authentication. [Accesat 17 5 2018].

[74] „How to Add WiKID Two-factor authentication to Cloudstack Manager,” [Interactiv]. Available: https://www.wikidsystems.com/support/how-to/how-to-add-wikid-two-factor-authentication-to-cloudstack-manager/. [Accesat 10 1 2019].

[75] „Setting up 3-factor authentication for Eucalyptus cloud instances,” [Interactiv]. Available: https://blogs.mindspew-age.com/2014/07/21/setting-up-3-factor-authentication-keypair-password-google-authenticator-for-eucalyptus-cloud-instances/. [Accesat 10 1 2019].

[76] G. A. P. A. Gordin Ionel, „Two factor authentication framework for private cloud,” în *International Conference on System Theory, Control and Computing*, Sinaia, 2019.

[77] „Internet Engineering Task Force,” [Interactiv]. Available: https://en.wikipedia.org/wiki/Internet_Engineering_Task_Force. [Accesat 7 7 2018].

[78] „RFC 6238 - TOTP: Time-Based One-Time Password Algorithm,” [Interactiv]. Available: https://tools.ietf.org/html/rfc6238. [Accesat 15 11 2018].

[79] „Initiative for Open Authentication,” [Interactiv]. Available: https://en.wikipedia.org/wiki/Initiative_for_Open_Authentication. [Accesat 9 5 2018].

[80] „HMAC,” [Interactiv]. Available: https://en.wikipedia.org/wiki/HMAC. [Accesat 25 4 2018].

[81] „RFC 4226 - HOTP: An HMAC-Based One-Time Password Algorithm,” [Interactiv]. Available: https://tools.ietf.org/html/rfc4226. [Accesat 15 5 2018].

[82] „Brute-force attack,” [Interactiv]. Available: https://en.wikipedia.org/wiki/Brute-force_attack. [Accesat 27 2 2018].

[83] „Phishing,” [Interactiv]. Available: https://en.wikipedia.org/wiki/Phishing. [Accesat 19 3 2018].

[84] „OpenStack Docs: Time-based One-time Password (TOTP),” [Interactiv]. Available: https://docs.openstack.org/keystone/pike/advanced-topics/auth-totp.html. [Accesat 10 10 2017].

[85] „ Base32,” [Interactiv]. Available: https://en.wikipedia.org/wiki/Base32. [Accesat 27 9 2018].

[86] „Tokens,” [Interactiv]. Available: https://docs.openstack.org/security-guide/identity/tokens.html. [Accesat 24 2 2018].

[87] T. Campbell, „Troubleshooting OpenStack,” în *Troubleshooting OpenStack Identity*, Packt Publishing Ltd, 2016, pp. 19-21.

[88] T. X. Baojiang Cui, „Security Analysis of Openstack Keystone,” în *2015 9th International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing*, Blumenau, 2015.

[89] „Firewalls and default ports,” [Interactiv]. Available: https://docs.openstack.org/newton/config-reference/firewalls-default-ports.html. [Accesat 14 2 2019].

[90] „Manage IP addresses,” [Interactiv]. Available: https://docs.openstack.org/ocata/user-guide/cli-manage-ip-addresses.html. [Accesat 15 9 2018].

[IG] Autor Ionel Gordin