**Universitatea Tehnică a Moldovei**

**Facultatea *Calculatoare, Informatică și Microelectronică***

**Specialitatea *Tehnologii Informaționale***



Raport

**la lucrarea de laborator nr. 2**

**Tema:*“******Scanarea si evaluarea securitatii datelor”***

**Disciplina: “Tehnici de securitate informationala”**

|  |  |  |
| --- | --- | --- |
| **A efectuat:** | Student grupa TI-231 FR | Apareci Aurica |
| **A verificat:** | Asistent universitar | Alexandru Tocan |

**Chișinău 2025**

**Cuprins**

[1. **Cadru teoretic** 3](#_Toc1)

[**2. Repere teoretice**  4](#_Toc2)

[**3. Sarcini practice** 5](#_Toc3)

[**4. Concluzii** 6](#_Toc4)

[**5. Bibliografie** 7](#_Toc5)

# **Cadru teoretic**

**Tema lucrării:** Securitatea si evaluarea securitatii datelor

**Obiectivele lucrării:**

* explicarea conceptelor de bază ale scanării de porturi și vulnerabilități;
* familiarizarea cu instrumentele de scanare;
* instalarea și configurarea instrumentelor de scanare;
* realizarea scanărilor și detectarea vulnerabilităților;
* explicarea conceptului de audit și realizare a auditului de securitate.

**Resurse nesesare:**

* CSE-LABVM instalat în VirtualBox/UTM.
* Metasploitable2 VM - o mașină virtuală Linux vulnerabilă în mod intenționat, concepută pentru antrenament, teste de exploatare și atac asupra unei ținte.

**Sarcini:**

* crearea si configurarea masinii virtuale vulnerabile
* Scanarea porturilor si serviciilor care ruleaza
* Scanarea vulnerabilitatilor cu scanerul Nessus
* Realizarea auditului de securitate cu Lynis

# **2. Repere teoretice**

Securitatea informației constă în protejarea datelor împotriva accesului neautorizat, modificării, distrugerii sau divulgării. Principiile de bază sunt:

**Confidențialitatea** – accesul la date este restricționat doar utilizatorilor autorizați;

**Integritatea** – asigurarea că datele nu au fost modificate în mod neautorizat;

**Disponibilitatea** – datele și sistemele sunt accesibile atunci când este nevoie de ele.

Scanarea de porturi reprezintă o tehnică esențială în evaluarea securității unui sistem, fiind utilizată pentru identificarea porturilor deschise și a serviciilor active asociate acestora. Prin scanarea porturilor se poate determina suprafața de atac a unui sistem, facilitând astfel identificarea serviciilor potențial vulnerabile și evaluarea nivelului de expunere la atacuri externe. Această activitate este adesea un prim pas în procesul de testare a penetrabilității și contribuie semnificativ la prevenirea accesului neautorizat. Printre cele mai utilizate instrumente pentru scanarea de porturi se numără Nmap, recunoscut pentru flexibilitate și acuratețe, și Netcat, util atât pentru diagnosticare, cât și pentru transfer de date sau conexiuni simple între sisteme.

**Scanarea de vulnerabilități**

Aceasta presupune analizarea sistemului pentru a detecta puncte slabe ce pot fi exploatate de atacatori. Scanner-ele de vulnerabilități evaluează configurația sistemului, versiunile software și permisiunile. Instrumente de scanare și audit:

**Nessus** – instrument de scanare automată a vulnerabilităților, oferă rapoarte detaliate despre riscuri, clasificări CVSS și recomandări;

**Lynis** – utilitar de audit de securitate pentru sistemele Linux/Unix, analizează setări de sistem, permisiuni, firewall, autentificare etc.;

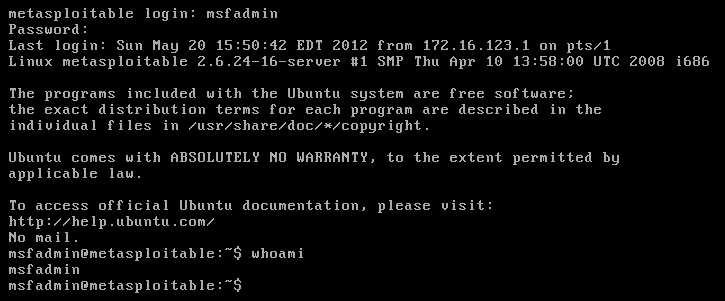
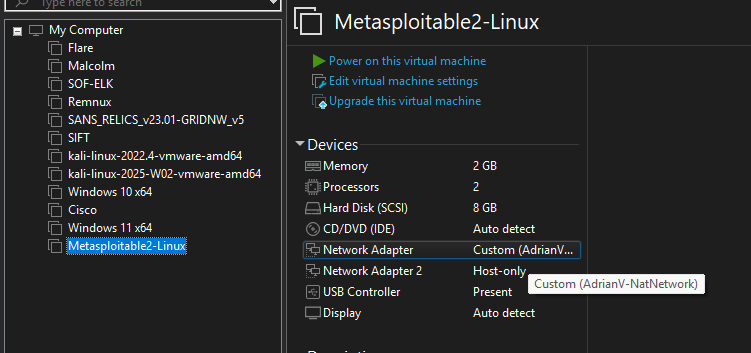
**Wireshark**, **OpenVAS**, **Nikto** – alte unelte utile în analiza și testarea securității.

Auditul de securitate este un proces sistematic prin care se evaluează măsurile de protecție implementate într-un sistem informatic, având ca scop identificarea eventualelor vulnerabilități și neconformități. Acesta presupune verificarea configurației sistemului, a politicilor de securitate aplicate, precum și a modului în care sunt protejate datele sensibile. În urma auditului, se formulează recomandări pentru optimizarea securității și reducerea riscurilor. De asemenea, auditul de securitate joacă un rol esențial în asigurarea conformității cu standarde internaționale precum ISO/IEC 27001, NIST sau cu cerințele legale impuse de GDPR, oferind organizațiilor o imagine clară asupra stării lor de securitate cibernetică.

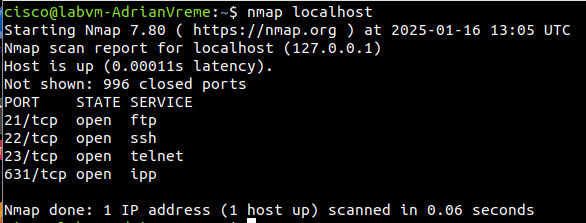
# **3. Sarcini practice**

În partea preliminară se va descărca, crea și configura mașina virtuală Metasploitable2, care este o mașină vulnerabilă utilizată în scop educațional pentru a realiza diverse teste de securitate.

**Pasul 1:** *Configurarea mașinii virtuale Metasploitable2*



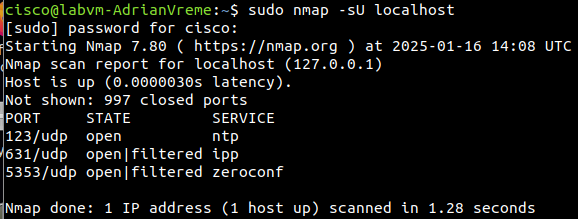
**Pasul 2:** *Scanarea porturilor și serviciilor care rulează*



Lansare terminal în CSE-LABVM și rularea scanerului de porturi Nmap (*nmap localhost*)

|  |  |  |
| --- | --- | --- |
| *Porturile TCP deschise și descriere a serviciului asociat* | | |
| ****Port**** | **Descriere** | **Numar vulnerabilitati CVE** |
| ****Port 21** (FTP - File Transfer Protocol)** | Utilizat pentru transferul de fișiere între un client și un server. Este un protocol nesecurizat (transmite datele în text clar) și, de obicei, necesită autentificare cu nume de utilizator și parolă. |  |
| ****Port 22** (SSH - Secure Shell)** | Folosit pentru accesarea în siguranță a dispozitivelor și serverelor la distanță. Oferă comunicații criptate și este utilizat frecvent pentru administrarea sistemelor și tunelare securizată. |  |
| ****Port 23** (Telnet)** | Protocol pentru conectarea la distanță la un dispozitiv sau server, similar cu SSH, dar fără criptare. Este considerat nesigur și înlocuit de SSH în majoritatea scenariilor. |  |
| ****Port 631** (IPP - Internet Printing Protocol)** | Protocol utilizat pentru gestionarea imprimantelor și comenzilor de imprimare pe rețea. Este des întâlnit în medii unde imprimantele sunt partajate prin rețea. |  |

**Pasul 3:** *Utilizarea Nmap cu privilegii administrative*

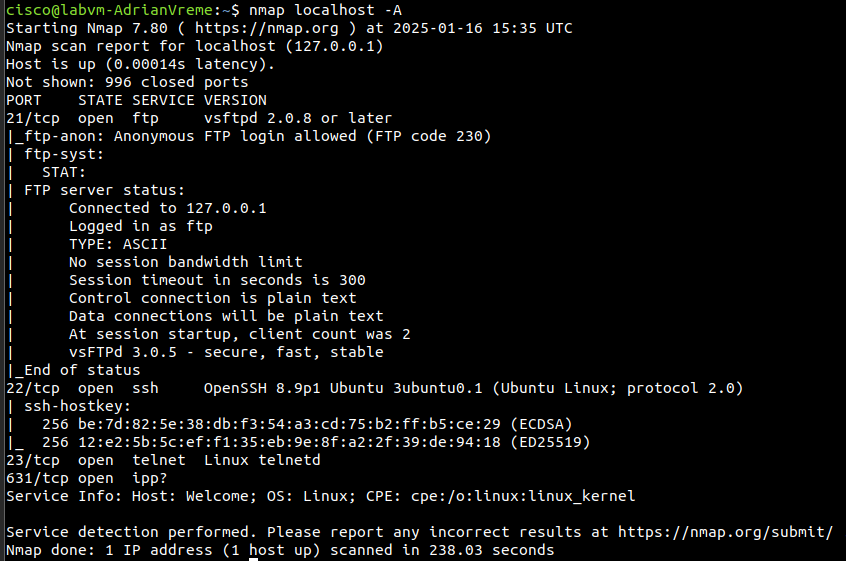


|  |  |  |
| --- | --- | --- |
| *Porturile UDP deschise și descriere a serviciului asociat* | | |
| ****Port**** | **Descriere** | **Numar vulnerabilitati CVE** |
| ****Port 123** (NTP - Network Time Protocol)** | Utilizat pentru sincronizarea timpului între computere și servere. Este esențial pentru menținerea acurateței ceasurilor de sistem în rețele și corelare evenimente. |  |
| ****Port 631** (IPP - Internet Printing Protocol)** | Protocol utilizat pentru a gestiona sarcinile de imprimare și comunicația cu imprimantele în rețea |  |
| ****Port 5353** (mDNS - Multicast DNS / Zeroconf)** | Folosit pentru descoperirea automată a serviciilor din rețea, cum ar fi imprimantele sau alte dispozitive. Este parte din protocolul Zeroconf. |  |

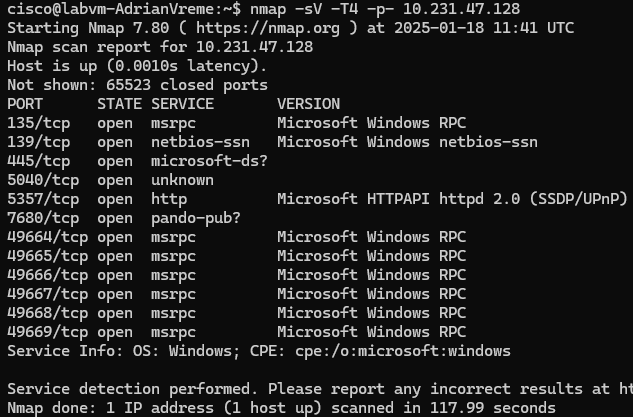
**Analiza a 3 vulnerabilități CISCO** CSE-LABVM

|  |  |  |
| --- | --- | --- |
| **Denumire** | **Descriere** | **Vulnerabilitate** |
| **vsftpd** | vsftpd (Very Secure FTP Daemon) este un server FTP (File Transfer Protocol) cunoscut pentru securitatea și performanța sa. | **CVE-2011-2523:** În iulie 2011, s-a descoperit că versiunea 2.3.4 a vsftpd descărcabilă de pe site-ul oficial fusese compromisă. Utilizatorii care se autentificau pe un server vsftpd 2.3.4 compromis puteau introduce ":)" ca nume de utilizator și obțineau un shell de comandă pe portul 6200. |
| **OpenSSH 8.9p1** | OpenSSH este un set de instrumente pentru conectivitate securizată, utilizând protocolul SSH (Secure Shell) pentru acces la cli și transfer securizat de date. | **CVE-2024-6387:** Această vulnerabilitate, cunoscută sub numele de "RegreSSHion", afectează OpenSSH între versiunile 8.5p1 și 9.7p1. Permite executarea de cod la distanță neautentificat, oferind atacatorilor acces root complet pe sistemele afectate. Problema provine dintr-o condiție de cursă în modul în care sshd gestionează semnalele, care poate fi declanșată de un atacator care nu reușește să se autentifice într-un anumit interval de timp. |
| **Network Time Protocol (NTP) versiunea 4** | Un protocol utilizat pentru sincronizarea ceasurilor computerelor într-o rețea. Acesta permite dispozitivelor să își ajusteze timpul intern în funcție de servere de timp de referință, asigurând o sincronizare precisă și uniformă a timpului în întreaga rețea. | **CVE-2015-7704:** Clientul ntpd în NTP 4.x permite atacatorilor de la distanță să provoace un denial of service prin trimiterea unui număr de mesaje "Kiss of Death" (KoD) special create. Un atacator poate trimite un pachet KoD falsificat către client, ceea ce va crește intervalul de interogare al clientului la o valoare mare și va dezactiva efectiv sincronizarea cu serverul. |

**Pasul 4:** *Capturarea cheilor SSH*



**Pasul 5:** *Repetarea pașilor 1-4 pentru a scana mașina virtuală Metasploitable2 și Windows 11 Pro*

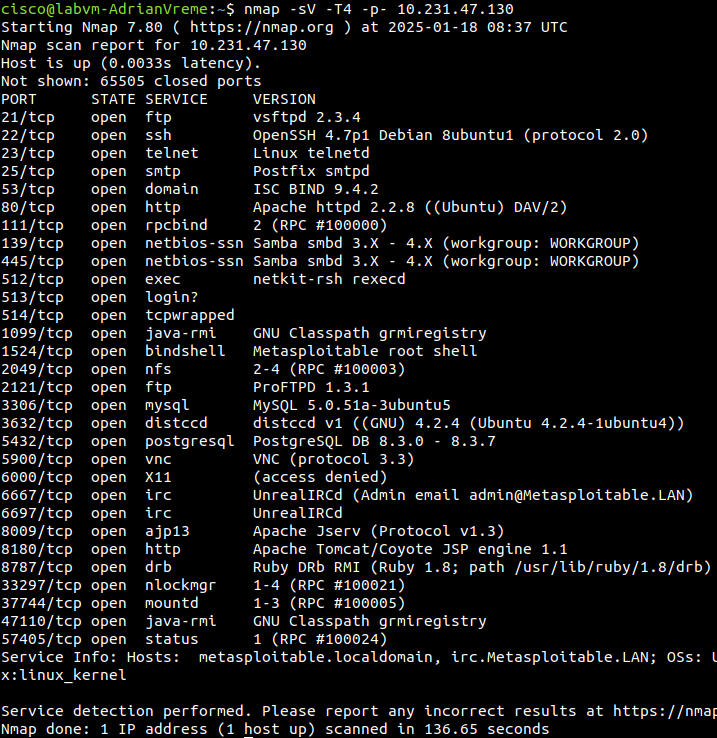


|  |  |  |
| --- | --- | --- |
| *Porturile TCP deschise și descriere a serviciului asociat* | | |
| ****Port**** | **Descriere** |
| **135/tcp** - **msrpc** | Utilizat pentru serviciul Microsoft RPC (Remote Procedure Call), important pentru comunicarea între procese pe sistemele Windows. |
| **139/tcp** - **netbios-ssn** | Folosit pentru NetBIOS Session Service, legat de partajarea fișierelor și imprimantelor în rețea. |
| **445/tcp** - **microsoft-ds** | Folosit de SMB (Server Message Block), pentru partajarea fișierelor, folderelor și imprimantelor. |
| **5040/tcp** - **unknown** | Port asociat cu serviciul **cdpsvc** (Connected Devices Platform Service) în Windows. Acest serviciu permite dispozitivelor Windows să descopere și să interacționeze cu alte dispozitive compatibile din rețea. |
| **5357/tcp** - **http** | Microsoft HTTPAPI httpd 2.0, posibil utilizat pentru comunicarea UPnP (Universal Plug and Play). |
| **7680/tcp** - **pando-pub?** | Utilizat pentru serviciul Windows Update Delivery Optimization (WUDO). |
| **49664 - 49669/tcp** - **msrpc** | Porturi dinamice utilizate pentru Microsoft RPC. |

Exemple de Vulnerabilități asociate cu porturile menționate, istoric vulnerabile la atacuri

|  |  |
| --- | --- |
| **Portul 135/tcp (MSRPC)** | **Vulnerabilitate**: Atacuri de tip Remote Code Execution (RCE) prin exploatarea serviciilor RPC nesecurizate.  **Exemplu istoric**: Exploatarea vulnerabilității **MS03-026** (Blaster Worm) care a permis executarea de cod la distanță și răspândirea rapidă în rețele neprotejate.  **Impact**: Acces neautorizat, control complet asupra sistemului afectat. |
| **Portul 139/tcp (NetBIOS-SSN)** | **Vulnerabilitate**: Partajarea fișierelor expuse, atacuri SMB Relay și divulgarea informațiilor sensibile despre rețea.  **Exemplu istoric**: Utilizarea NetBIOS pentru atacuri de tip MITM în scopul capturării credențialelor de autentificare.  **Impact**: Acces neautorizat la fișiere și infrastructura rețelei. |
| **Portul 445/tcp (Microsoft-DS)** | **Vulnerabilitate**: Exploatarea protocolului SMB, vulnerabil la atacuri de tip RCE și worm.  **Exemplu istoric**: **EternalBlue** (CVE-2017-0144), folosit de ransomware precum **WannaCry** și **NotPetya**.  **Impact**: Compromiterea totală a sistemelor și criptarea datelor, ducând la pierderi financiare semnificative. |

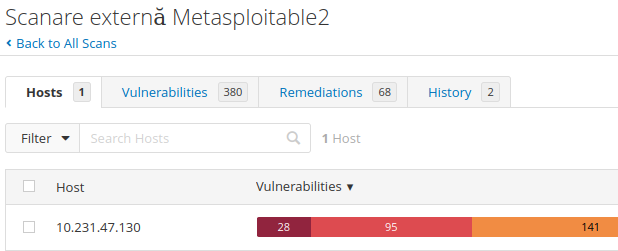
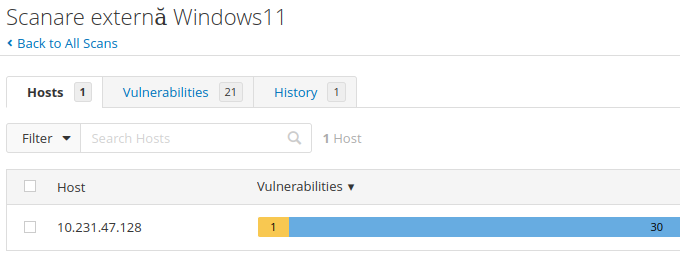
**Metasploitable2 IP:** 10.231.47.130



|  |  |  |
| --- | --- | --- |
| **Denumire** | **Descriere** | **Vulnerabilitate** |
| **PostgreSQL 8.3** | PostgreSQL este un sistem de gestionare a bazelor de date relaționale open-source, care utilizează protocolul SQL (Structured Query Language) pentru interacțiunea cu bazele de date. Versiunea 8.3 a fost lansată în 2008 și oferă funcționalități precum stocarea și gestionarea datelor, interogări complexe și suport pentru tranzacții. | **CVE-2009-3231:** În PostgreSQL 8.3 înainte de versiunea 8.3.8, când se utilizează autentificarea LDAP cu legături anonime, un atacator poate ocoli procesul de autentificare prin furnizarea unei parole goale. |
| **ISC BIND 9.4.2** | Este cel mai utilizat software pentru servere DNS (Domain Name System), responsabil pentru rezolvarea numelor de domenii în adrese IP și invers. Versiunea 9.4.2 oferă funcționalități de bază pentru rezolvarea DNS și suport pentru DNSSEC (DNS Security Extensions). | **CVE-2008-0122:** O eroare de tip off-by-one în funcția inet\_network din libbind în ISC BIND 9.4.2 și versiunile anterioare permite atacatorilor să provoace un denial of service (crash) și, posibil, să execute cod arbitrar prin introducerea de date special create care declanșează coruperea memoriei. |
| **Apache HTTP Server 2.2.8** | Apache HTTP Server, cunoscut și ca httpd, este un server web open-source care implementează protocolul HTTP (Hypertext Transfer Protocol), permițând servirea de pagini web către utilizatori. | **CVE-2007-5000:** O vulnerabilitate de tip cross-site scripting (XSS) în modulul mod\_imagemap permite atacatorilor să injecteze scripturi arbitrare în paginile web, ceea ce poate duce la executarea de cod în contextul browserului utilizatorului. |

**Scanarea vulnerabilitățile cu scanerul Nessus**

Scanarea externă a vulnerabilităților Metasploitable2 si Windows cu credentiale

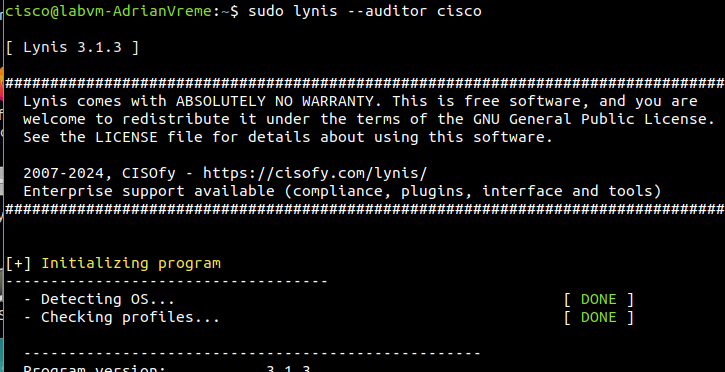


Explicarea a 3 vulnerabilități din Nessus

|  |  |
| --- | --- |
| Apache Tomcat AJP Connector Request Injection (Ghostcat)  CVE CVE-2020-1745  CVE CVE-2020-1938  XREF CISA-KNOWN-EXPLOITED:2022/03/17  XREF CEA-ID:CEA-2020-0021 | **1. Care este vulnerabilitatea?**  Imaginează-ți că Apache Tomcat, un program care servește pagini web, are o „poartă secretă” numită AJP Connector. Această poartă ar trebui să fie protejată, dar din cauza unei greșeli (numită și „Ghostcat”), nu este suficient de sigură.  **2. Cum ar putea fi exploatată?**  Un atacator ar putea folosi această „poartă secretă” pentru a citi fișierele de pe serverul web – chiar cele care nu sunt destinate publicului. Dacă serverul permite încărcarea de fișiere, hoțul poate chiar să încarce un program malițios ascuns în aparent fișiere inofensive. Cu acest „program”, el poate, în final, să controleze serverul de la distanță, ca și cum ar avea cheia casei.  **3. Cum ar putea fi remediată?**  Pentru a rezolva problema, administratorul serverului trebuie să ia măsuri de protecție:  **Actualizare:** Să instaleze o versiune nouă și corectată a Apache Tomcat (versiunile 7.0.100, 8.5.51, 9.0.31 sau mai noi) unde această problemă este rezolvată.  **Configurare:** Dacă actualizarea imediată nu este posibilă, se poate modifica setarea „AJP Connector” pentru a cere o permisiune (autorizare) înainte ca cineva să poată intra, făcând astfel poarta mai securizată. |

**Realizarea auditului de securitate cu Lynis**

**Pasul 1:** *Realizarea auditului de securitate cu Lynis si examinarea rezultatelor scanării și ordonarea avertismentelor*



|  |  |  |
| --- | --- | --- |
| **Avertisment analizat** | **Descriere** | **Soluție propusă și verificare** |
| **PKGS-7392** | Avertismentul **PKGS-7392 - Pachete vulnerabile** identificat de Lynis indică prezența de pachete software cu vulnerabilități cunoscute și pentru care există deja actualizări disponibile. Acest lucru reprezintă un risc de securitate, deoarece exploatarea acestor vulnerabilități ar putea permite atacatorilor să compromită sistemul. | **Soluția propusă** pentru remedierea acestui avertisment este actualizarea pachetelor vulnerabile. Acest lucru se poate realiza prin intermediul comenzilor: *sudo apt-get update && sudo apt-get upgrade -y* |
| **FIRE-4512** | Avertismentul **FIRE-4512 - Set de reguli iptables gol** identificat de Lynis indică faptul că modulul iptables este încărcat, dar nu există niciun set de reguli de firewall configurat. Aceasta poate indica o configurație incorectă sau lipsa completă a unui firewall pe sistem. | **Soluția propusă** constă în configurarea unui set de reguli de bază pentru firewall-ul iptables:   1. Se setează politica implicită pentru traficul **INPUT** și **FORWARD** la **DROP**. 2. Se permite traficul **OUTPUT**.   *sudo iptables -P INPUT DROP*  *sudo iptables -P FORWARD DROP*  *sudo iptables -P OUTPUT ACCEPT* |

**Permisiuni pentru conexiuni existente:** Se permit conexiunile **ESTABLISHED** și **RELATED** pentru a permite răspunsuri la cererile inițiate de sistem.

**Permisiuni pentru rețeaua locală (LAN):** Se permite traficul din și către rețeaua locală (de exemplu, 192.168.1.0/24).

**Permisiuni pentru SSH:** Se permite accesul SSH (port 22) de pe rețeaua locală.

**Permisiuni pentru ICMP (Ping):** Se permit pachetele ICMP pentru a permite ping-ul în cadrul rețelei locale.

**Salvare reguli:** Se salvează regulile iptables pentru a persista după repornirea sistemului.

*sudo iptables -A INPUT -m conntrack --ctstate ESTABLISHED,RELATED -j ACCEPT*

*sudo iptables -A INPUT -s 10.231.47.0/24 -j ACCEPT*

*sudo iptables -A OUTPUT -d 10.231.47.0/24 -j ACCEPT*

*sudo iptables -A INPUT -p tcp --dport 22 -m conntrack --ctstate NEW,ESTABLISHED -j ACCEPT*

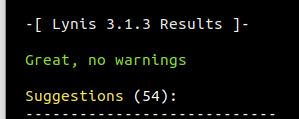
*sudo iptables -A OUTPUT -p tcp --sport 22 -m conntrack --ctstate ESTABLISHED -j ACCEPT*

*sudo iptables -A INPUT -p icmp --icmp-type echo-request -j ACCEPT*

*sudo iptables -A OUTPUT -p icmp --icmp-type echo-reply -j ACCEPT*

*sudo apt-get install iptables-persistent*

*sudo netfilter-persistent save*



# **4. Concluzii**

Lucrarea de laborator a avut ca scop aprofundarea cunoștințelor privind securitatea datelor și metodele de evaluare a acesteia prin scanarea porturilor, detectarea vulnerabilităților și realizarea auditului de securitate. Prin utilizarea mediului virtual format din CSE-LABVM și Metasploitable2, a fost posibilă simularea realistă a unui sistem vulnerabil, ideal pentru desfășurarea testelor fără riscuri asupra infrastructurii reale.

Activitățile desfășurate au inclus configurarea unei mașini virtuale vulnerabile, scanarea porturilor și a serviciilor active, detectarea vulnerabilităților cu ajutorul scannerului Nessus și auditarea securității cu Lynis. Aceste instrumente au permis identificarea punctelor slabe ale sistemului, familiarizarea cu vectorii de atac comuni și înțelegerea procesului de evaluare a securității într-un cadru controlat.

Pe parcursul lucrării au apărut dificultăți legate de instalarea și configurarea unor aplicații de securitate care necesitau resurse semnificative sau drepturi administrative. În ciuda acestor provocări, lucrarea și-a atins obiectivele, oferind o imagine clară asupra modului în care se realizează scanările de securitate și auditul unui sistem. Experiența practică acumulată constituie o bază solidă pentru înțelegerea proceselor de testare și fortificare a infrastructurii IT în fața amenințărilor cibernetice.

# **5. Bibliografie**

* Îndrumar de laborator - Autor: lect.univ., dr. Arina Alexei
* Ghiduri despre securitatea IT de pe platforma ELSE - Autor: lect.univ., dr. Arina Alexei.
* VMware Workstation Pro - Documentație oficială: <https://support.broadcom.com/>
* <https://nmap.org/>
* <https://tryhackme.com/room/rpnessusredux>
* <https://cisofy.com/lynis/>
* Resurse online: CVE Details, Tenable, CISOfy