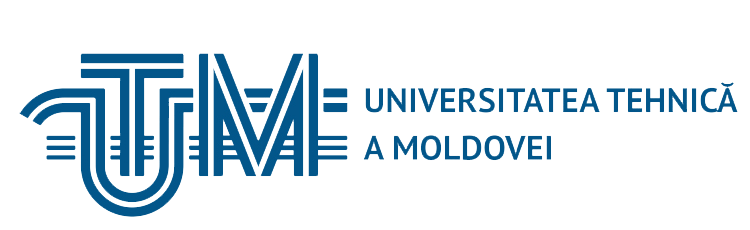
**Universitatea Tehnică a Moldovei**

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

**Specialitatea *Tehnologii Informaționale***



Raport

**la lucrarea de laborator nr. 1**

**Tema:*“******Masini virtuale. Teste de securitate”***

**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 7](#_Toc3)

[3.1 Pregatirea sistemului gazda pentru virtualizare 7](#_Toc4)

[3.2 Importarea masinilor virtuale in hypervisorul VirtualBox 8](#_Toc5)

[3.3 Analiza fisierelor si url-ului in VirusTotal 9](#_Toc6)

[4. Concluzii 14](#_Toc7)

[5. Bibliografie 15](#_Toc8)

# **Cadru teoretic**

**Tema lucrării:** Masini virtuale. Teste de securitate

**Obiectivele lucrării:**

* explicarea conceptului de virtualizare, instalarea și configurarea unei mașini virtuale;
* configurarea rețelei virtuale și instalarea sistemului de operare;
* crearea unui mediu de testare securizat și realizarea testelor 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:**

* pregatirea sistemului gazda pentru virtualizare
* importarea masinilor virtuale in hypervisorul VirtualBox
* analiza fisierelor si url-ului in VirusTotal

# **2. Repere teoretice**

**Conceptul de virtualizare**

**Virtualizarea** reprezintă o tehnologie care permite crearea unei versiuni virtuale a unei resurse hardware sau software, cum ar fi un server, un sistem de operare, un dispozitiv de stocare sau o rețea. Există mai multe tipuri de virtualizare, fiecare cu particularitățile sale. Virtualizarea completă (Full Virtualization) presupune emularea completă a hardware-ului, permițând rularea unui sistem de operare fără nicio modificare. În schimb, paravirtualizarea necesită ca sistemul de operare să fie conștient de faptul că rulează într-un mediu virtualizat, oferind astfel o mai bună performanță prin reducerea costului de emulare. O altă formă de virtualizare, containerizarea, se concentrează pe izolarea aplicațiilor prin utilizarea aceluiași nucleu al sistemului de operare gazdă, fiind reprezentată de tehnologii precum Docker. Gestionarea acestor medii virtuale este realizată prin intermediul unui hypervisor – un software specializat care controlează și administrează mașinile virtuale. Hypervisoarele pot fi de tip 1 (bare-metal), rulând direct pe hardware-ul fizic, cum este cazul VMware ESXi, sau de tip 2 (hosted), funcționând deasupra unui sistem de operare, cum sunt VirtualBox sau UTM.

**Mediu de testare securizat**

*Analiza programelor malware* este o metodă importantă pentru detectarea și prevenirea amenințărilor cibernetice. În general, există două tipuri principale de analiză: analiza statică și analiza dinamică. Analiza statică se referă la examinarea codului sursă al programului malware fără a-l rula, în timp ce analiza dinamică implică rularea programului malware și examinarea comportamentului său în timp real.

**VirusTotal** este un serviciu online de analiză a programelor malware, care combină analiza statică și dinamică. Acesta permite utilizatorilor să încarce fișiere suspecte pentru a fi analizate de peste 70 de motoare antivirus și alte instrumente de detecție a amenințărilor, cum ar fi analiza de comportament, analiza sandbox și analiza de rețea. Rezultatele analizei sunt prezentate sub forma unui raport detaliat, care include informații despre tipul de amenințare, nivelul de risc și semnături de detecție specifice fiecărui motor antivirus.

**Intezer** este un alt instrument de analiză a programelor malware care se bazează pe analiza statică. Intezer utilizează o tehnică numită "**analiză genetică**" pentru a identifica fragmente de cod similar între diferite programe malware. Această tehnică poate ajuta la identificarea relațiilor între diferite programe malware și la dezvăluirea actorilor de amenințări cibernetice din spatele atacurilor. Intezer poate detecta și analiza amenințări noi și necunoscute, care nu sunt detectate de motoarele antivirus tradiționale.

Configurarea programelor **antivirus** este, de asemenea, importantă pentru a proteja dispozitivele împotriva programelor malware. În general, utilizatorii ar trebui să își configureze programele antivirus pentru a actualiza automat semnăturile de detecție a amenințărilor și pentru a rula scanări periodice ale dispozitivelor lor. De asemenea, utilizatorii ar trebui să fie atenți la semnele de atac cibernetic, cum ar fi e-mailurile nesolicitate sau mesajele de pe rețelele sociale, și să evite să descarce sau să instaleze software-uri din surse nesigure.

Securitatea informației este o preocupare tot mai mare în zilele noastre, este important să fim conștienți de amenințările cibernetice și să luăm măsuri corespunzătoare pentru a ne proteja datele și dispozitivele.

**Analiza statică** se referă la examinarea codului sursă, a fișierelor și a componentelor programului malware fără a rula programul într-un mediu sigur. Acest tip de analiză este util în identificarea funcționalității și a resurselor utilizate de programul malware, precum și a eventualelor vulnerabilități de securitate ale sistemului.

Printre instrumentele utilizate în analiza statică a malware-ului se numără analizatoare de cod, **decompiler**-e și **debugger**-e. Aceste instrumente permit cercetătorilor de securitate să examineze în detaliu codul sursă și să descopere funcționalități ascunse, să identifice zonele critice ale programului, să identifice și să examineze resursele utilizate de program și să detecteze eventualele vulnerabilități de securitate.

**Analiza dinamică** implică rularea programului malware într-un mediu sigur și monitorizarea comportamentului acestuia. Acest tip de analiză este util în detectarea activităților suspecte sau dăunătoare ale programului malware și în identificarea modului în care acesta încearcă să se ascundă sau să se protejeze.

Instrumentele utilizate în analiza dinamică includ **sandbox**-uri și **emulator**-e. Aceste instrumente permit cercetătorilor de securitate să execute programul malware într-un mediu **izolat** și să monitorizeze comportamentul acestuia în timp real. Astfel, ei pot detecta orice activitate suspectă, precum crearea de fișiere noi, modificarea fișierelor existente sau rularea de procese ascunse.

Atât analiza statică, cât și analiza dinamică sunt esențiale în dezvoltarea de soluții de securitate eficiente împotriva malware-ului. Folosind aceste două metode, cercetătorii de securitate pot identifica vulnerabilitățile de securitate ale sistemului și pot dezvolta măsuri adecvate de protecție împotriva oricăror amenințări viitoare.

**Programele malare pot fi clasificate ca:**

**Virus**: Un virus este un program malițios care poate infecta alte fișiere și programe. Virusul se atașează de un fișier sau program și se răspândește atunci când utilizatorii deschid sau utilizează acel fișier sau program. Virusul poate cauza daune semnificative sistemului și poate fi utilizat pentru a accesa informații confidențiale.

**Worm**: Un worm este un program malițios care se răspândește de la un sistem la altul prin intermediul rețelei. Wormul poate provoca daune semnificative rețelei și poate fi folosit pentru a accesa informații confidențiale.

**Trojan**: Un Trojan este un program malițios care se prezintă ca o aplicație legitimă, dar care are în mod ascuns obiective malițioase. Trojanii pot fi folosiți pentru a fura informații confidențiale, cum ar fi parolele sau datele bancare, sau pentru a prelua controlul sistemului.

**Ransomware**: Ransomware-ul este un tip de malware care restricționează accesul utilizatorului la sistem sau la datele sale și solicită plata unei sume de bani pentru a debloca sistemul sau a recupera datele. Ransomware-ul poate fi foarte dăunător pentru companii sau indivizi care dețin date critice.

**Spyware**: Spyware-ul este un tip de malware care colectează informații despre activitățile utilizatorului, cum ar fi tastarea parolelor sau navigarea pe web, fără ca utilizatorul să fie conștient. Informațiile colectate sunt apoi trimise atacatorilor pentru a fi utilizate în scopuri malițioase.

**Adware**: Adware-ul este un tip de malware care afișează anunțuri nedorite și pop-up-uri pe ecranul utilizatorului, de obicei în încercarea de a convinge utilizatorul să descarce alte programe malware sau să viziteze site-uri web malițioase.

**Rootkit**: Rootkit-ul este un program care se ascunde în sistemul de operare al dispozitivului infectat, utilizat pentru a obține acces neautorizat la dispozitivul infectat sau pentru a ascunde alte programe malware.

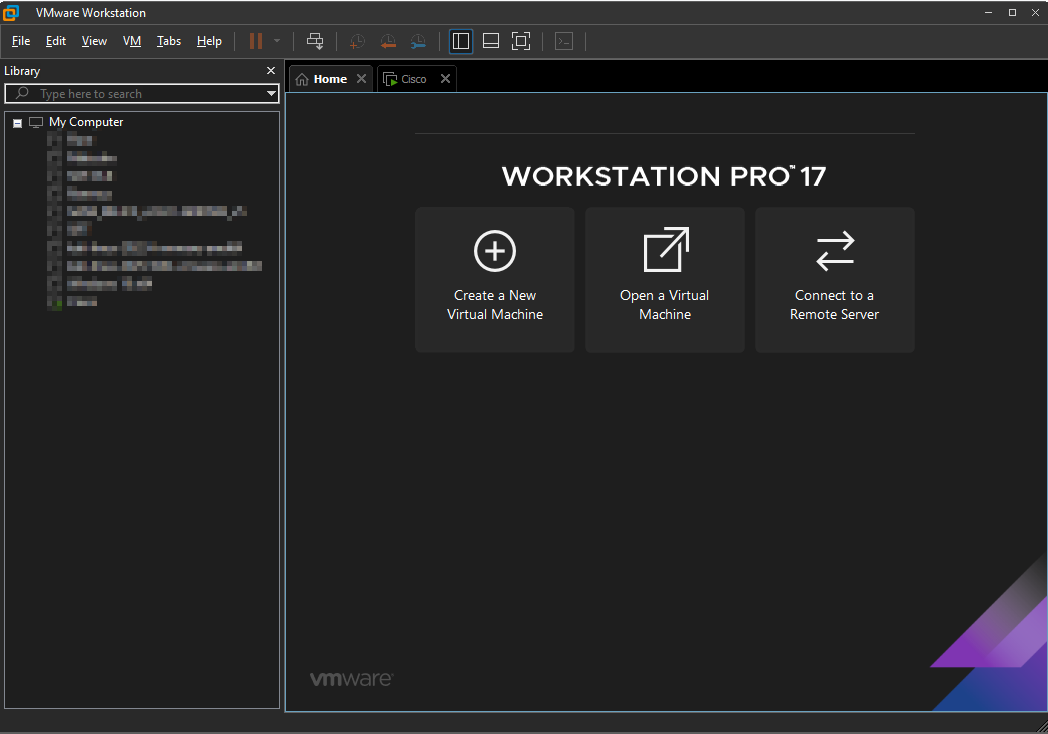
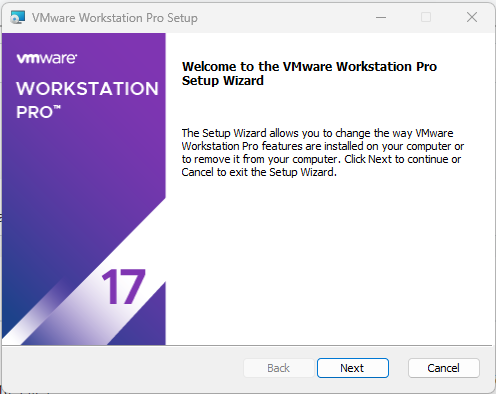
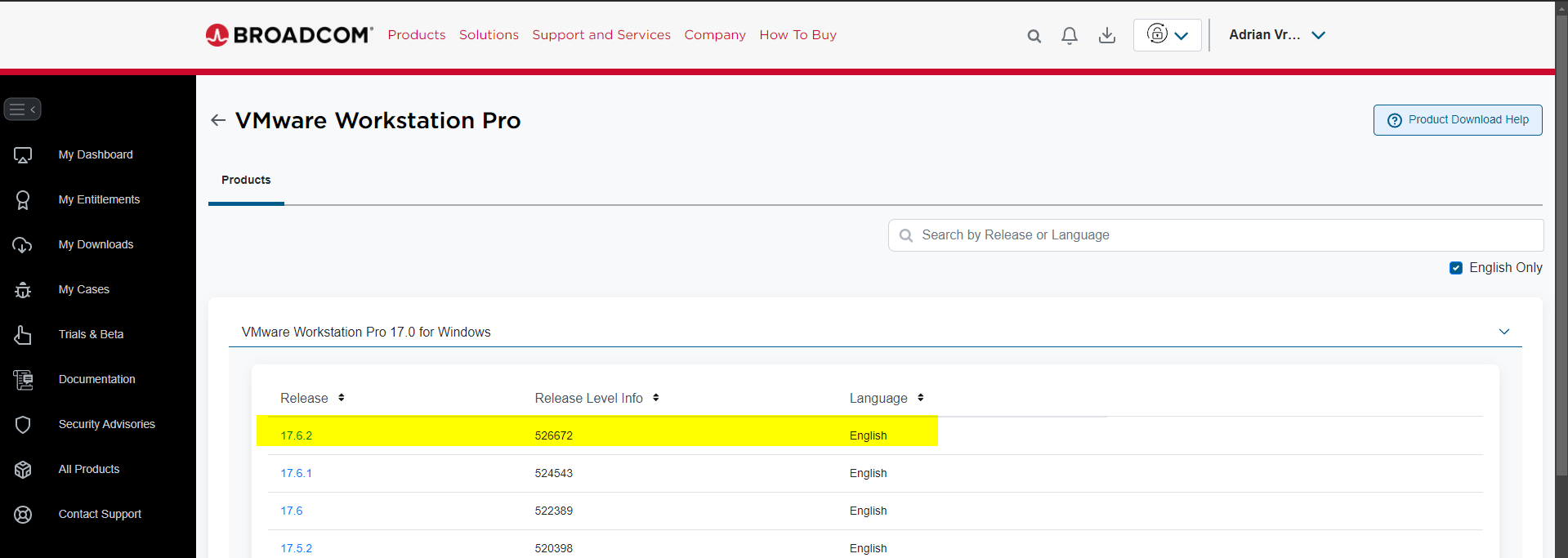
Acestea sunt doar câteva dintre cele mai comune tipuri de malware. Altele includ keylogger, backdoor, fileless malware, botnet și multe altele. Pentru a proteja dispozitivele împotriva malware-ului, este important să instalați un program antivirus de încredere și să evitați descărcarea și instalarea software-ului din surse nesigure.

# **3. Sarcini practice**

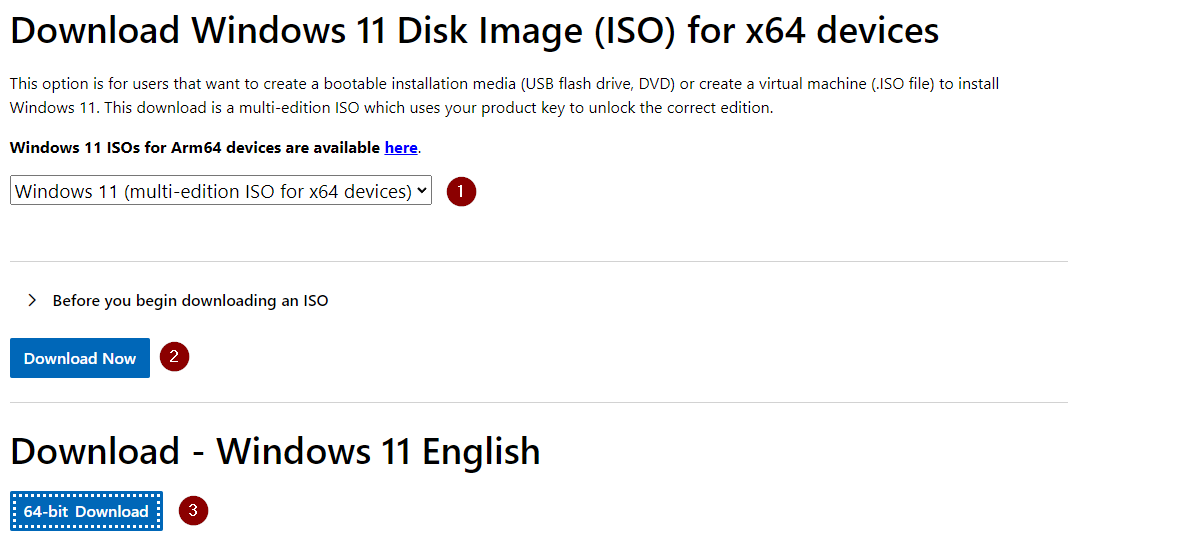
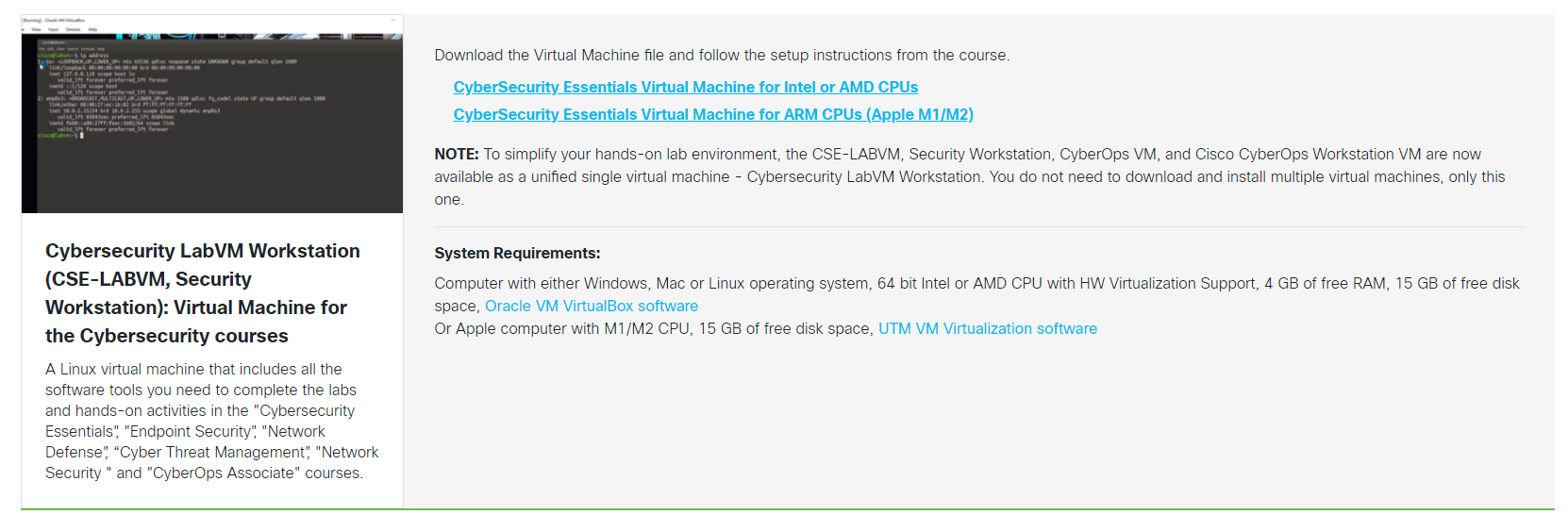
## **3.1 Pregatirea sistemului gazda pentru virtualizare**

În partea 1 se pregătește sistemul gazdă pentru virtualizare, se va descărca și instala software-ul de virtualizare desktop și, de asemenea, se vor descărca fișierele imagine care pot fi folosite pentru a finaliza lucrările de laborator planificate în cadrul cursului de Tehnologii ale securității informaționale. Se vor rula mașini virtuale cu sistemele de operare Linux Ubuntu și Windows 11 Pro.

**Pasul 1:** *Descărcarea și instalarea VirtualBox*



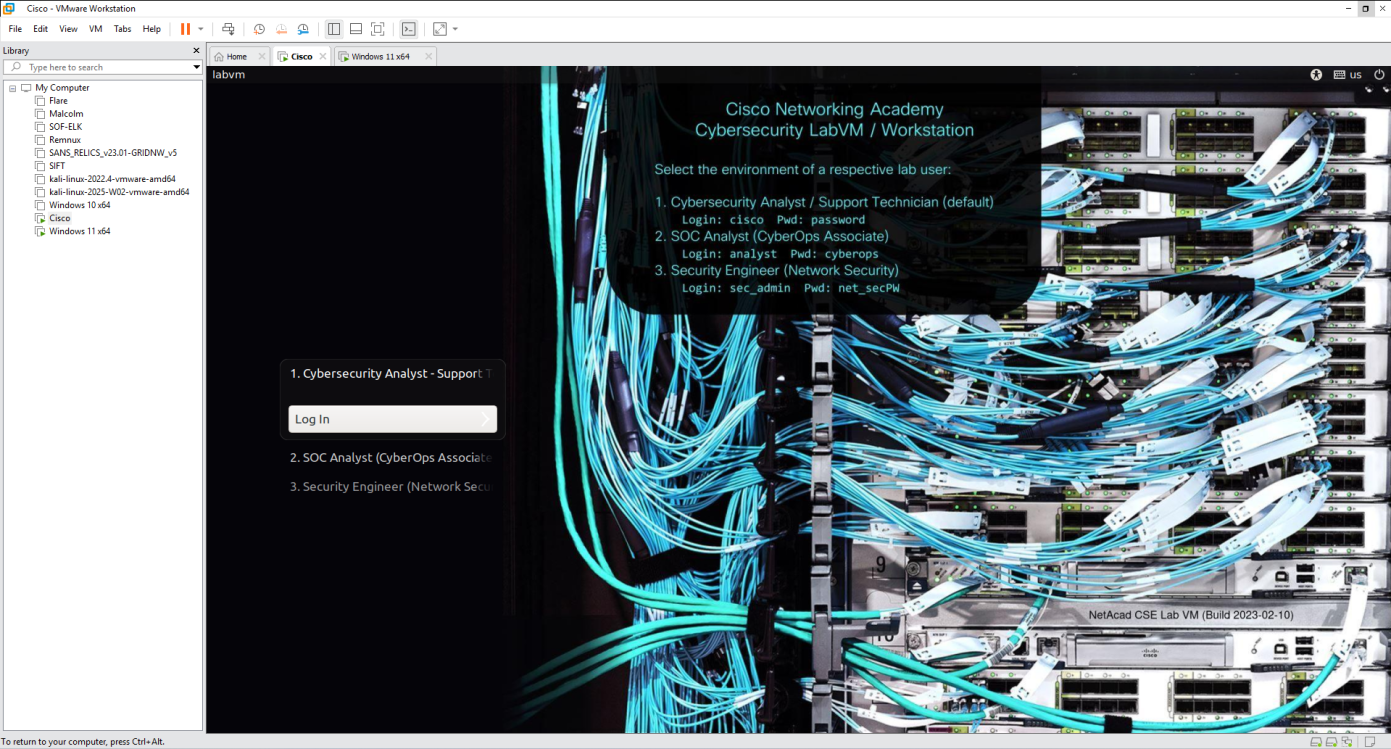
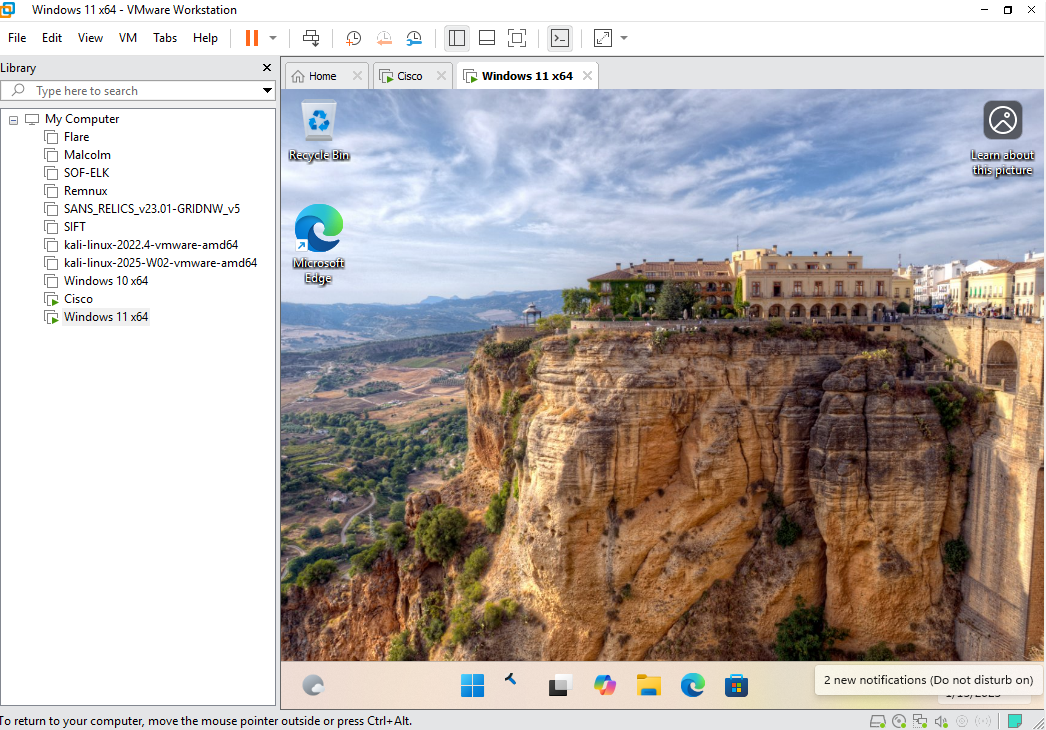
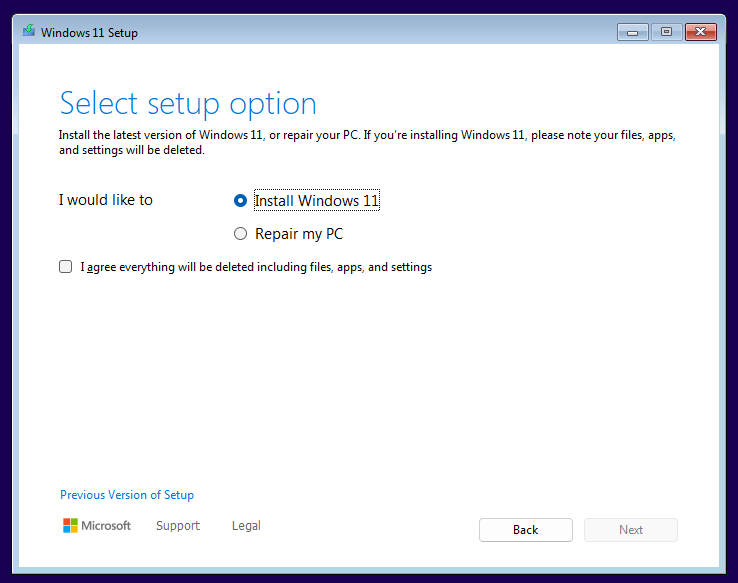
**Pasul 2:** *Descărcarea fișierelor imagine a mașinilor virtuale Linux și Windows 11 Pro*



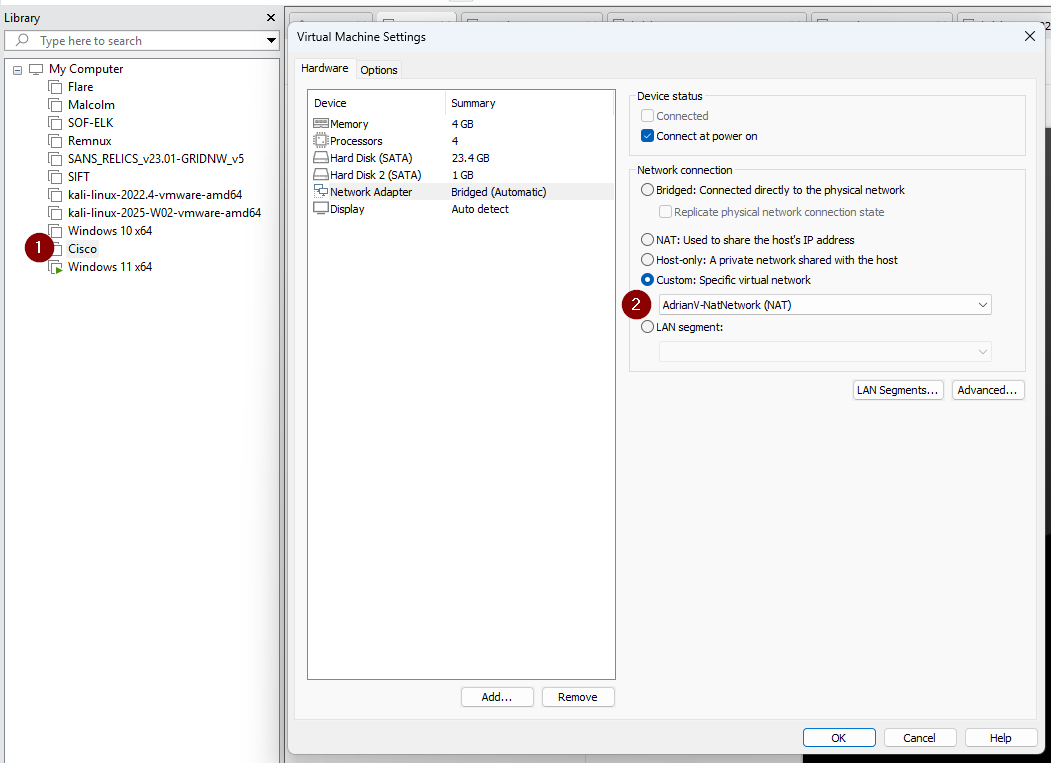
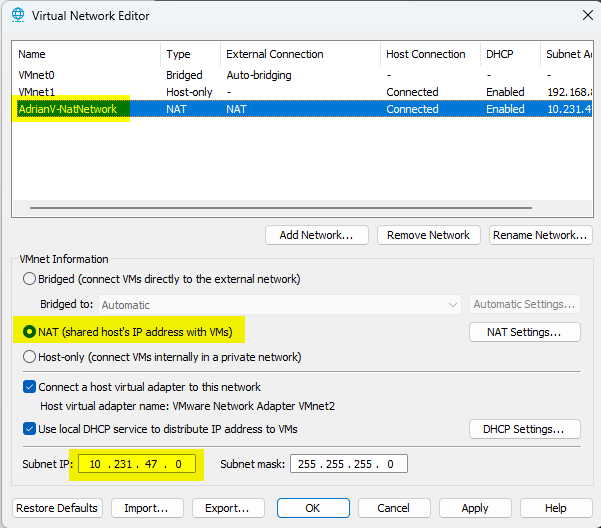
## **3.2 Importarea masinilor virtuale in hypervisorul VirtualBox**

În partea a doua se vor importa imaginile mașinilor virtuale în VirtualBox, se vor configura.

**Pasul 1:** *Importarea fișierelor mașinilor virtuale și instalare OS*

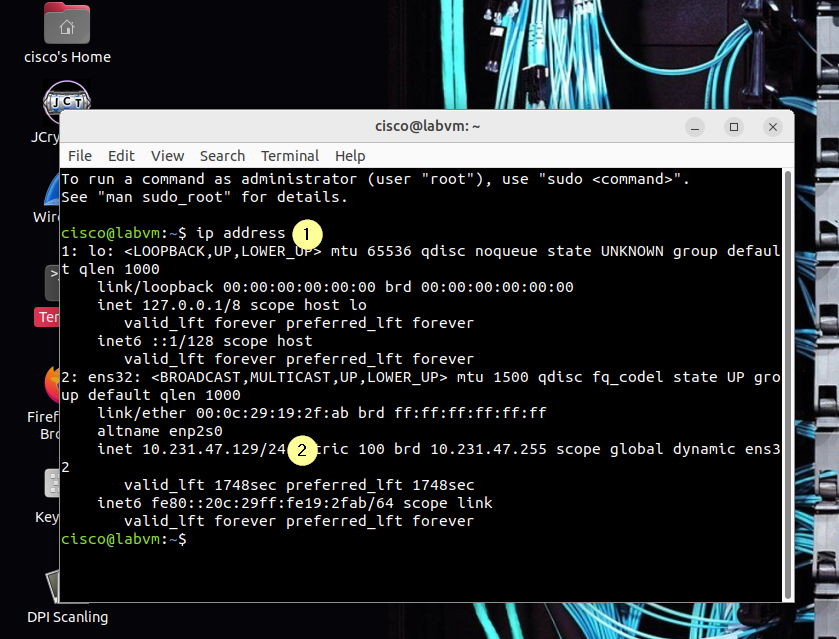


**Pasul 2:** *Configurarea și personalizarea mașinilor virtuale*



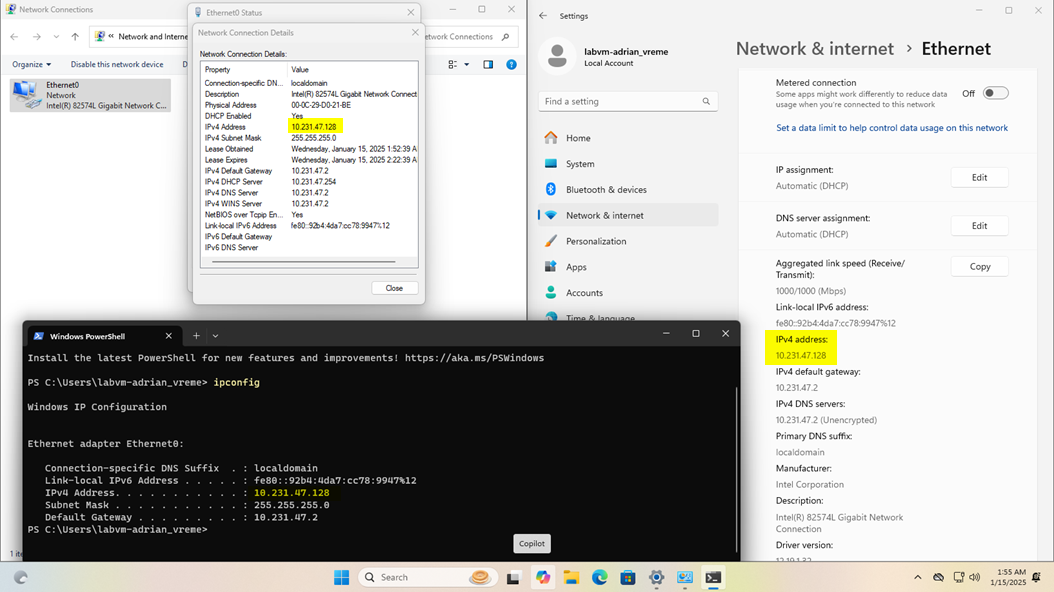
Crearea Retelei virtuale NAT si selectarea adapterului pentru CiscoVM si Windows VM

**Pasul 3:** *Pornirea mașinii virtuale CSE-LABVM și conectarea si familiarizarea*



Detectarea adresei IP din NAT-ul creat si utilizarea browser-ului pentru a demonstra ca DNS-ul lucreaza correct.

**Pasul 4:** *Pornirea mașinii virtuale Windows 11 pro și conectarea si familiarizarea*



## **3.3 Analiza fisierelor si url-ului in VirusTotal**

Pentru analiza au fost selectate următoarele fișiere: **0TJN0DC8.exe**, **1MHR5TKD.exe**, **1POYVC5E.exe** din arhiva de fișiere malițioase “78-suspect-file.zip“, **mailsa.exe**, **ngusp.exe**, **tleditor.exe** din arhiva de fișiere malițioase “x 001.zip“, **X 000 A (27).exe**, **X 000 A (28).exe, X 000 A (29).exe** din arhiva de fișiere malițioase “x 002.zip“, In continuare, pentru recunoașterea tipurilor de malware din mostrele selectate vom utiliza VirusTotal, un instrument online care verifica exemplarul încărcat prin mai multe produse antivirus si oferă o descriere a tipului de malware identificat de fiecare din produsele utilizate.

|  |  |  |  |
| --- | --- | --- | --- |
| **Nume mostra** | **VirusTotal** | **Rezultat** | **Tip malware** |
| **0TJN0DC8.exe** |  | 46/67(68.65%) | Trojan |
| **1MHR5TKD.exe** |  | 64/71(90.14%) | Trojan, dropper |
| **1POYVC5E.exe** |  | 54/71(76.05%) | Trojan |
| **mailsa.exe** |  | 54/57(94.73%) | Trojan, adware |
| **ngusp.exe** |  | 61/69(88.40%) | Trojan, worm, ransomware |
| **tleditor.exe** |  | 52/72(72.22%) | Trojan, dropper, downloader |
| **X 000 A (27).exe** |  | 44/47(93.61%) | Virus |
| **X 000 A (28).exe** |  | 14/53(26.41%) | Trojan, adware |
| **X 000 A (29).exe** |  | 53/72(73.61%) | Trojan, downloader |

* **MSIL** în numele malware-ului indică faptul că acest malware este scris în limbajul de programare Microsoft Intermediate Language (MSIL), ceea ce îi permite să funcționeze pe o gamă largă de sisteme de operare Windows.

|  |  |  |
| --- | --- | --- |
| **Nume mostra** | **Tip malware** | **Descriere** |
| 0TJN0DC8.exe | Trojan MSIL Bulz | Această amenințare poate efectua o serie de acțiuni alese de un hacker rău intenționat pe computer. |
| 1MHR5TKD.exe | MSIL Bladabindi | Această familie de malware este clasificată ca un backdoor Trojan, ceea ce înseamnă că permite atacatorilor să preia controlul sistemului infectat și să execute diverse acțiuni malițioase, cum ar fi monitorizarea activității utilizatorilor, preluarea controlului asupra aplicațiilor și a fișierelor, furarea de date sau infectarea altor sisteme. |
| 1POYVC5E.exe | Trojan MSIL Basic | Este un tip de program malware Trojan care se răspândește prin diverse mijloace, cum ar fi email-uri infectate, descărcări de software piratat sau site-uri web compromise.  Acest Trojan poate fi utilizat pentru a executa diverse acțiuni malițioase, cum ar fi preluarea controlului asupra sistemului infectat, furtul de informații sau instalarea altor programe malware. |
| mailsa.exe | Trojan barys lethic | **Barys Lethic** a fost detectat pentru prima dată în 2013 și a fost cunoscut pentru utilizarea sa în campanii de phishing și spam. Acest Trojan are abilități de auto-replicare, ceea ce îl face capabil să se răspândească rapid și să infecteze mai multe sisteme.  Barys Lethic este capabil să execute o gamă largă de funcții malitioase, inclusiv:   * colectarea de informații despre sistemul infectat și utilizatorii acestuia * preluarea controlului asupra sistemului și executarea de comenzi malițioase * descărcarea și instalarea altor programe malware |
| ngusp.exe | Trojan Foreign dorkbot | **Trojanul Foreign Dorkbot** este un program malware periculos care poate compromite sistemul unui utilizator prin intermediul unor fișiere infectate sau a altor programe malware. Acesta a fost detectat pentru prima dată în 2011 și s-a răspândit rapid pe scară largă, în special prin intermediul mesajelor de socializare și a rețelelor de file-sharing.  Foreign Dorkbot este un **Trojan multifuncțional** și poate fi utilizat pentru o serie de activități malitioase, inclusiv:   * preluarea controlului asupra sistemului infectat și colectarea de informații sensibile, cum ar fi parolele și datele bancare * descărcarea și instalarea de alte programe malware * crearea de backdoor-uri pentru a permite accesul ulterior la sistemul infectat * răspândirea de mesaje spam și a altor programe malware prin intermediul sistemului infectat   Trojanul Foreign Dorkbot este capabil să se ascundă în sistemul infectat și poate fi dificil de detectat și eliminat. |
| tleditor.exe | Trojan qqpass/nsis | **Trojanul QQPass/NSIS** este capabil să se ascundă în sistemul infectat și poate fi dificil de detectat și eliminat. Acesta poate fi utilizat pentru a prelua controlul asupra sistemului infectat și a colecta informații, cum ar fi parolele și datele bancare. De asemenea, acesta poate fi utilizat pentru a descărca și a instala alte programe malware, creând astfel backdoor-uri pentru accesul ulterior la sistemul infectat.  Trojanul QQPass/NSIS poate fi deosebit de periculos datorită faptului că este capabil să se **auto-instaleze** și să se **auto-actualizeze**. Acest lucru poate face dificilă detectarea și eliminarea sa cu soluții antivirus convenționale. |
| X 000 A (27).exe | Virus jeefo/hidrag | **Virusul Jeefo/Hidrag** utilizează tehnici avansate de criptare pentru a se ascunde în sistemul infectat și pentru a evita detectarea cu soluții antivirus convenționale. Acesta poate fi distribuit sub forma unui fișier executabil care este infectat cu virusul sau poate fi utilizat pentru a descărca și a instala alte programe malware. De asemenea, acesta **poate crea backdoor-uri** pentru accesul ulterior la sistemul infectat.  Odată instalat pe un sistem, Virusul Jeefo/Hidrag poate fi utilizat pentru a colecta informații sensibile, cum ar fi parolele și datele bancare. De asemenea, acesta poate fi utilizat pentru a **prelua controlul** asupra sistemului infectat și a rula alte programe malware. |
| X 000 A (28).exe | Adware installerex/installrex | Este un tip de program malware care se concentrează pe afișarea de reclame nesolicitate utilizatorilor de pe sistemele infectate. Acesta poate fi distribuit sub forma unui software legitim, cum ar fi programe gratuite sau shareware, dar poate conține și cod malicios care va **instala și afișa reclame și alte conținuturi nedorit**e pe computerul utilizatorului.  **Adware-ul Installerex/Installrex** poate fi descărcat și instalat automat prin intermediul unor pachete software de instalare care conțin programe adiționale, cunoscute sub numele de "bloatware". Acest tip de adware poate încetini sistemul utilizatorului și poate consuma resurse prețioase, cum ar fi spațiul pe disc și lățimea de bandă.  Printre efectele negative ale acestui tip de adware se numără și creșterea numărului de mesaje publicitare nedorite, **consumul de resurse** de sistem, degradarea performanței sistemului și expunerea la riscul altor tipuri de malware. |
| X 000 A (29).exe | Trojan Agent AVZO | Este un tip de program malware Trojan, care este capabil să se autoreplice și să se răspândească pe alte sisteme din rețea sau pe internet prin diverse mijloace, cum ar fi email-uri infectate, descărcări de software piratat sau site-uri web compromise. |

# **4. Concluzii**

Lucrarea a demonstrat importanța și versatilitatea virtualizării în contextul testelor de securitate cibernetică. Prin configurarea unei mașini virtuale în VirtualBox și utilizarea imaginii Metasploitable2, a fost posibilă simularea unui mediu controlat, destinat identificării și înțelegerii vulnerabilităților comune în sistemele informatice. S-au parcurs etapele esențiale de pregătire a sistemului gazdă, configurarea rețelei virtuale și instalarea sistemului de operare, urmate de realizarea testelor de securitate asupra unei ținte vulnerabile. În plus, analiza fișierelor și a URL-urilor în VirusTotal a completat scenariul practic, evidențiind metode eficiente de evaluare a riscurilor.

Pe parcursul lucrării am întâmpinat câteva dificultăți, precum incompatibilitatea unor versiuni de hypervisor cu sistemul de operare gazdă. De asemenea, au existat provocări în utilizarea unor unelte de testare care necesitau permisiuni elevate sau configurări suplimentare pentru a funcționa corect. Cu toate acestea, prin documentare suplimentară și aplicarea unor soluții tehnice, aceste obstacole au fost depășite, iar obiectivele lucrării au fost atinse. În concluzie, activitatea desfășurată a contribuit semnificativ la înțelegerea procesului de virtualizare și la consolidarea abilităților practice în domeniul securității informatice.

# **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/>
* Cisco CSE-LABVM - Resurse oficiale: <https://www.netacad.com/>
* VirusTotal - Platformă de analiză malware: <https://www.virustotal.com/>