

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
2. Repere teoretice	4
3. Sarcini practice.....	7
3.1 Pregatirea sistemului gazda pentru virtualizare.....	7
3.2 Importarea masinilor virtuale in hypervisorul VirtualBox.....	8
3.3 Analiza fisierelor si url-ului in VirusTotal.....	9
4. Concluzii	14
5. Bibliografie.....	15

1. 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 necesare:

- 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:

- pregătirea sistemului gazda pentru virtualizare
- importarea masinilor virtuale in hypervisorul VirtualBox
- analiza fișierelor 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, **de-compiler-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.

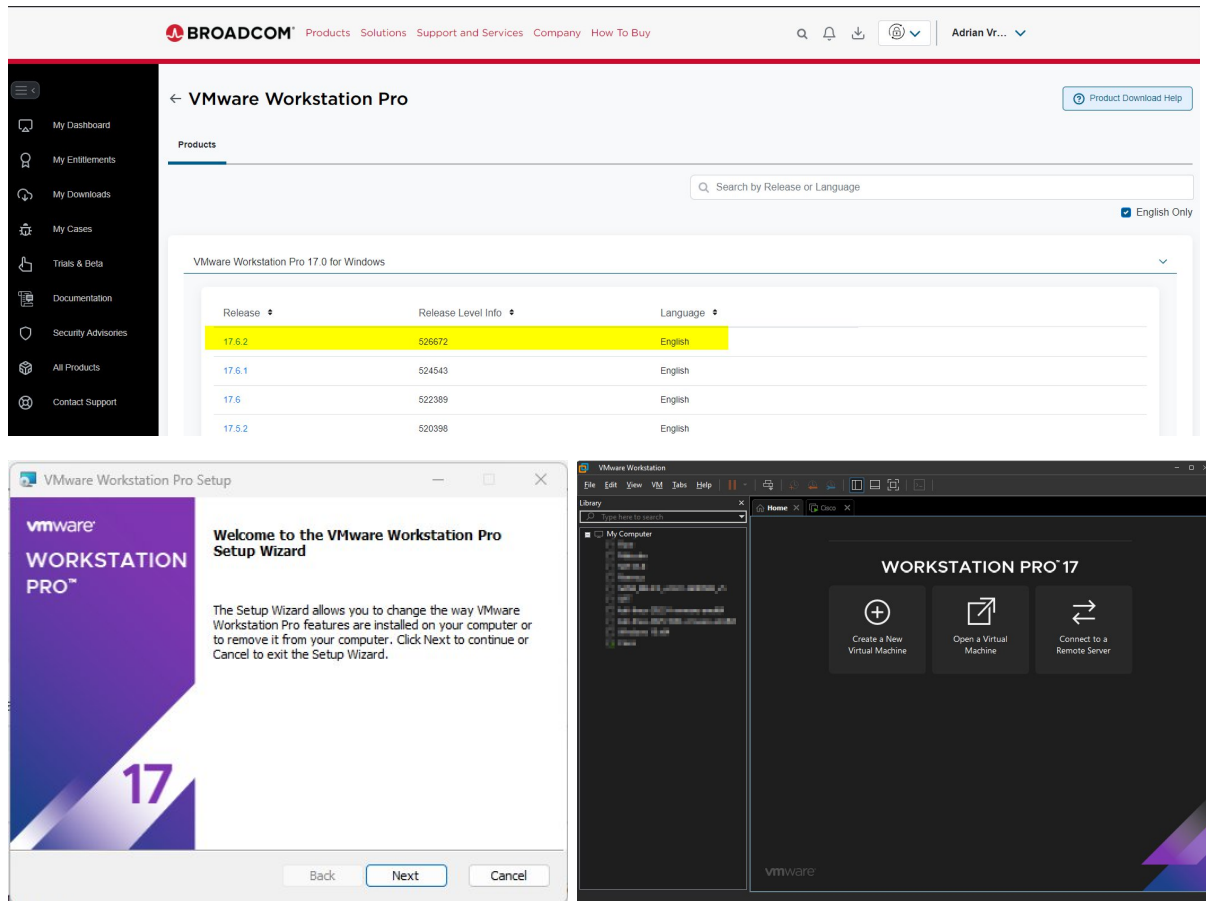
Acestea sunt doar câteva dintre cele mai comune tipuri de malware. Altele includ keylogger, backdoor, fileless malware, botnet și multe altele. Pentru a proteja dispozitivele împotriva malware-ului, este important să instalați un program antivirus de încredere și să evitați descărcarea și instalarea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

3. Sarcini practice

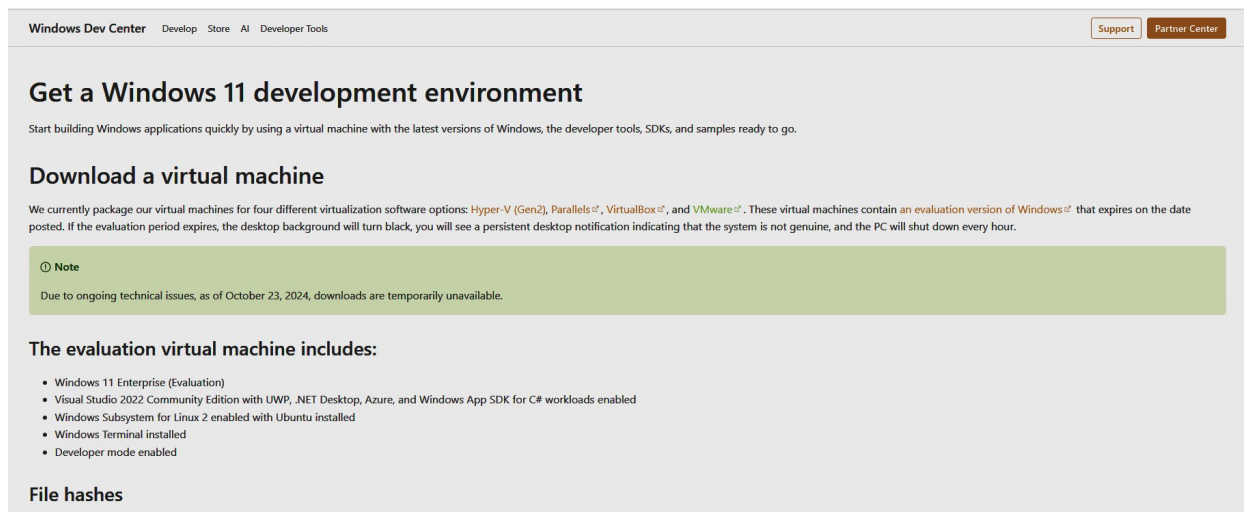
3.1 Pregatirea sistemului gazda pentru virtualizare

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



Download Windows 11 Disk Image (ISO) for x64 devices

This option is for users that want to create a bootable installation media (USB flash drive, DVD) or create a virtual machine (.ISO file) to install Windows 11. This download is a multi-edition ISO which uses your product key to unlock the correct edition.

Windows 11 ISOs for Arm64 devices are available [here](#).

Windows 11 (multi-edition ISO for x64 devices) ▾

1

> Before you begin downloading an ISO

Download Now

2

Download - Windows 11 English

64-bit Download

3



Download the Virtual Machine file and follow the setup instructions from the course.

[CyberSecurity Essentials Virtual Machine for Intel or AMD CPUs](#)

[CyberSecurity Essentials Virtual Machine for ARM CPUs \(Apple M1/M2\)](#)

NOTE: To simplify your hands-on lab environment, the CSE-LABVM, Security Workstation, CyberOps VM, and Cisco CyberOps Workstation VM are now available as a unified single virtual machine - Cybersecurity LabVM Workstation. You do not need to download and install multiple virtual machines, only this one.

System Requirements:

Computer with either Windows, Mac or Linux operating system, 64 bit Intel or AMD CPU with HW Virtualization Support, 4 GB of free RAM, 15 GB of free disk space, [Oracle VM VirtualBox software](#)
Or Apple computer with M1/M2 CPU, 15 GB of free disk space, [UTM VM Virtualization software](#)

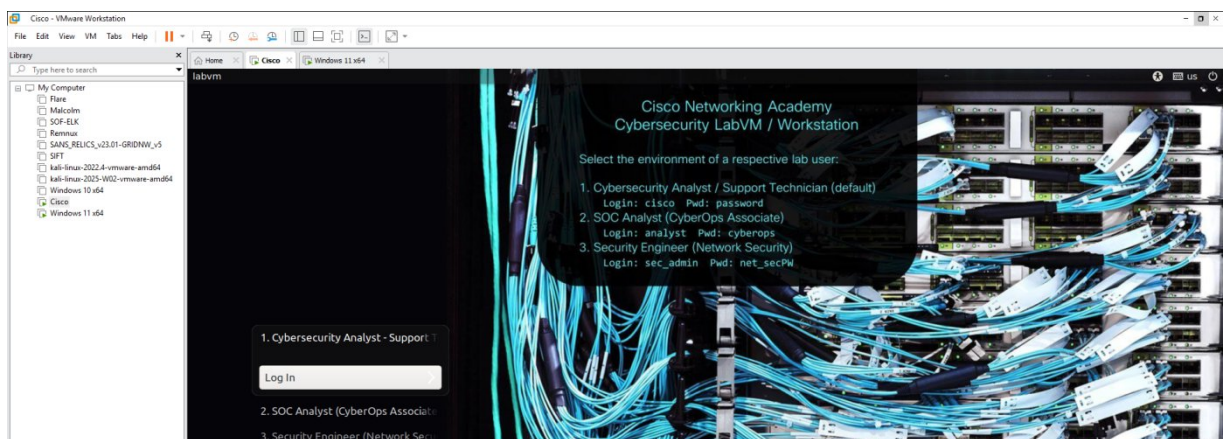
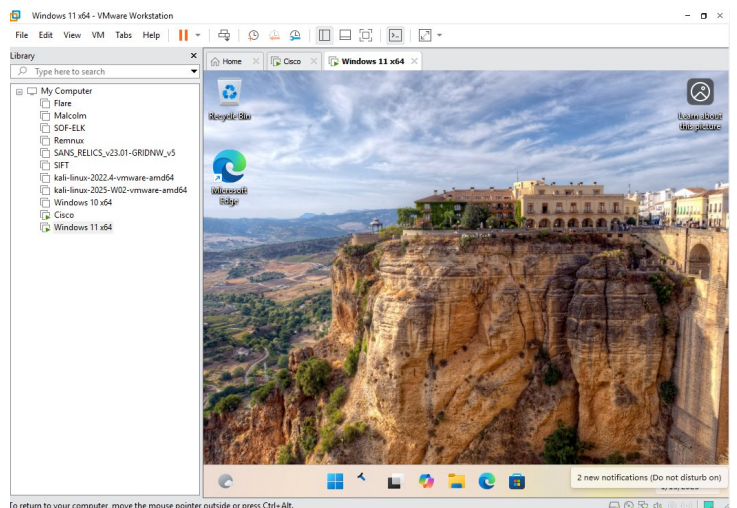
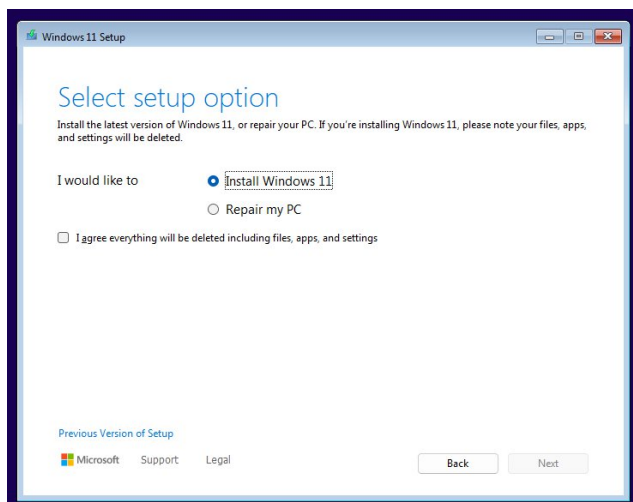
Cybersecurity LabVM Workstation (CSE-LABVM, Security Workstation): Virtual Machine for the Cybersecurity courses

A Linux virtual machine that includes all the software tools you need to complete the labs and hands-on activities in the "Cybersecurity Essentials", "Endpoint Security", "Network Defense", "Cyber Threat Management", "Network Security" and "CyberOps Associate" courses.

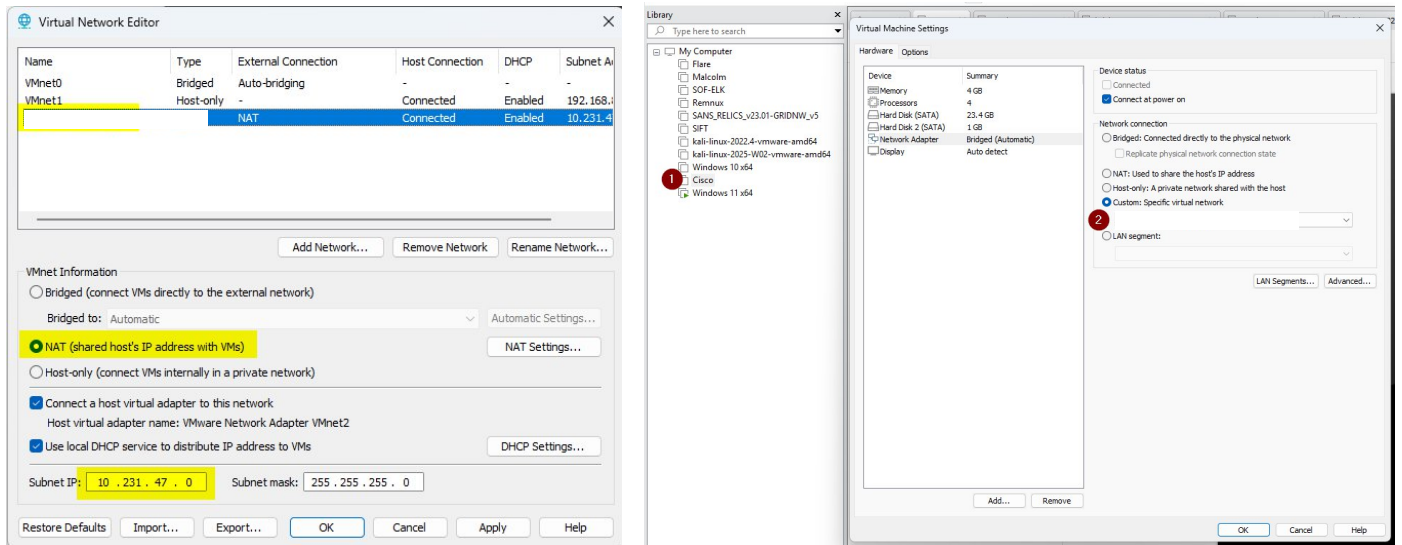
3.2 Importarea masinilor virtuale in hypervisorul VirtualBox

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

Pasul 1: Importarea fișierelor mașinilor virtuale și instalare OS

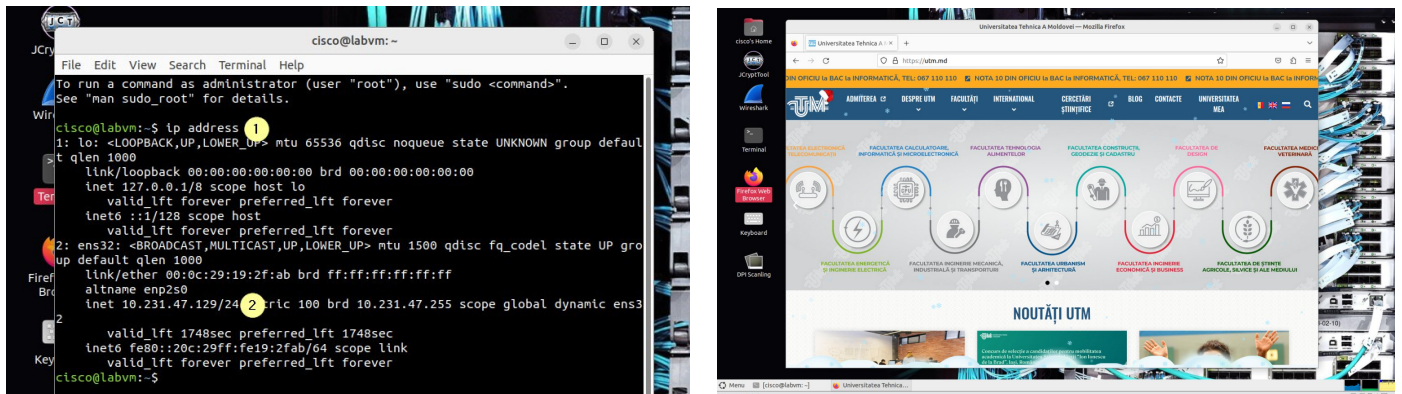


Pasul 2: Configurarea și personalizarea mașinilor virtuale



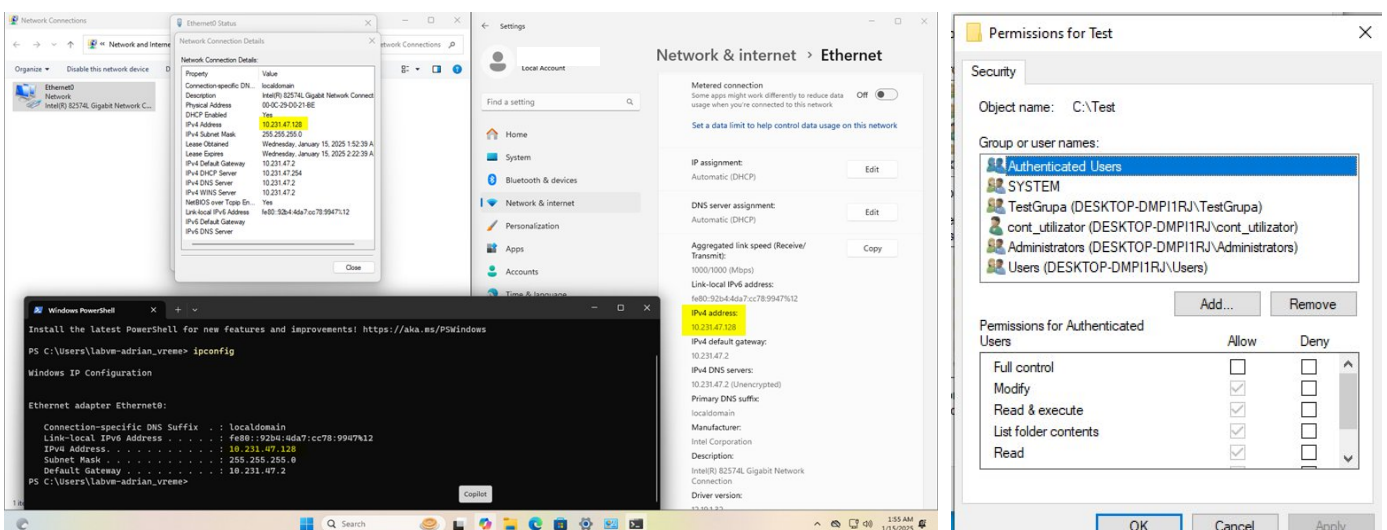
Crearea Retelei virtuale NAT si selectarea adapterului pentru CiscoVM si Windows VM

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



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

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

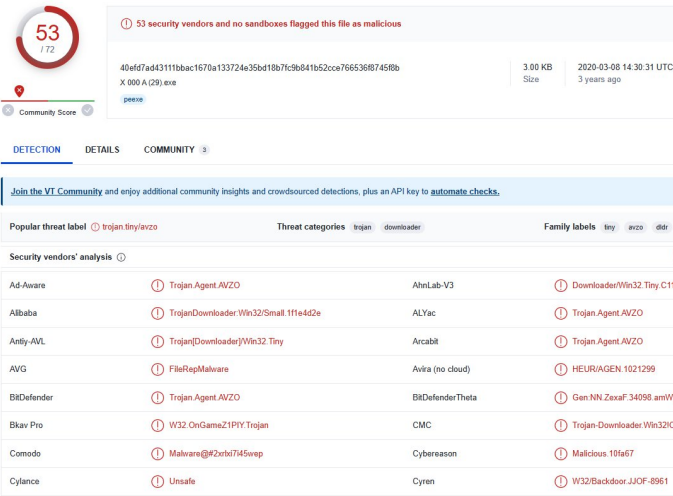


3.3 Analiza fişierelor si url-ului in VirusTotal

Pentru analiza au fost selectate următoarele fişiere: **0TJN0DC8.exe**, **1MHR5TKD.exe**, **1POYVC5E.exe** din arhiva de fişiere maliţioase “78-suspect-file.zip“, **mailsa.exe**, **ngusp.exe**, **tleditor.exe** din arhiva de fişiere maliţioase “x 001.zip“, **X 000 A (27).exe**, **X 000 A (28).exe**, **X 000 A (29).exe** din arhiva de fişiere maliţioase “x 002.zip“, In continuare, pentru recunoaşterea tipurilor de malware din mostrele selectate vom utiliza VirusTotal, un instrument online care verifică 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	<div><div><div><div>48</div><div>19</div></div><div><div>48 security vendors and no sandboxes flagged this file as malicious</div><div><div>25a409584acc040541f8acd305cd711e75d15132a7b866149d21a5d59d71e40</div><div>0TJN0DC8.exe</div><div>19.00 KB</div><div>2022-06-03 19:24:39 UTC</div><div>10 months ago</div><div>EXE</div></div></div><div><div>Community Score</div><div>pevce runtime-modules assembly direct-cpu-clock-access detect-debug-environment</div><div>DETECTIONDETAILSRELATIONSBEHAVIORCOMMUNITY</div><div>Join the VT Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.</div><div>Popular threat labelTrojan.maliciousThreat categoriesTrojanFamily labelsrootbasicgenerations</div><div>Security vendors' analysisDo you want to automate checks?</div><table><tr><td>Ad-Aware</td><td>Gen Variant Buz 609028</td><td>Alibaba</td><td>Trojan.MSL.Injector.69053db4</td></tr><tr><td>Avast</td><td>Trojan.Buz.D94804</td><td>Avast</td><td>MSL.Gen.Malicious.EDH [Tg]</td></tr><tr><td>AVG</td><td>MSL.Gen.Malicious.EDH [Tg]</td><td>Auslo (no cloud)</td><td>TR.Dropper.Gen</td></tr><tr><td>BitDefender</td><td>Gen Variant Buz 609028</td><td>BitDefender Theta</td><td>Gen.NN.ZenmF.34712.bm@baccorn</td></tr><tr><td>ClamAV</td><td>Win.Packed.Barys.6933211-0</td><td>Comodo</td><td>Makara@902a9f60f7ggp</td></tr><tr><td>CrowdStrike Falcon</td><td>WinMalicious_confidence_100% (W)</td><td>Cybereason</td><td>Malicious.aef485</td></tr><tr><td>Cylance</td><td>Unsafe</td><td>Cynet</td><td>Malicious (score: 198)</td></tr><tr><td>DrWeb</td><td>Trojan.Downloader.10.19735</td><td>Elastic</td><td>Malicious (High Confidence)</td></tr></table></div></div></div>	Ad-Aware	Gen Variant Buz 609028	Alibaba	Trojan.MSL.Injector.69053db4	Avast	Trojan.Buz.D94804	Avast	MSL.Gen.Malicious.EDH [Tg]	AVG	MSL.Gen.Malicious.EDH [Tg]	Auslo (no cloud)	TR.Dropper.Gen	BitDefender	Gen Variant Buz 609028	BitDefender Theta	Gen.NN.ZenmF.34712.bm@baccorn	ClamAV	Win.Packed.Barys.6933211-0	Comodo	Makara@902a9f60f7ggp	CrowdStrike Falcon	WinMalicious_confidence_100% (W)	Cybereason	Malicious.aef485	Cylance	Unsafe	Cynet	Malicious (score: 198)	DrWeb	Trojan.Downloader.10.19735	Elastic	Malicious (High Confidence)	46/67(68.65%)	Trojan
Ad-Aware	Gen Variant Buz 609028	Alibaba	Trojan.MSL.Injector.69053db4																																
Avast	Trojan.Buz.D94804	Avast	MSL.Gen.Malicious.EDH [Tg]																																
AVG	MSL.Gen.Malicious.EDH [Tg]	Auslo (no cloud)	TR.Dropper.Gen																																
BitDefender	Gen Variant Buz 609028	BitDefender Theta	Gen.NN.ZenmF.34712.bm@baccorn																																
ClamAV	Win.Packed.Barys.6933211-0	Comodo	Makara@902a9f60f7ggp																																
CrowdStrike Falcon	WinMalicious_confidence_100% (W)	Cybereason	Malicious.aef485																																
Cylance	Unsafe	Cynet	Malicious (score: 198)																																
DrWeb	Trojan.Downloader.10.19735	Elastic	Malicious (High Confidence)																																
1MHR5-TKD.exe	<div><div><div><div>64</div><div>23</div></div><div><div>64 security vendors and 1 sandbox flagged this file as malicious</div><div><div>61d41898371407149f2a322ac5586d41f99c2771c4221b4c0f8a6553b0d7</div><div>1MHR5TKD.exe</div><div>23.50 KB</div><div>2023-10-12 08:52:07 UTC</div><div>2 months ago</div><div>EXE</div></div></div><div><div>Community Score</div><div>pevce assembly runtime-modules detect-debug-environment temp-strings direct-cpu-clock-access checks-canon-regular persistence</div><div>DETECTIONDETAILSRELATIONSBEHAVIORCOMMUNITY</div><div>Join the VT Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.</div><div>Popular threat labelTrojan.Malicious.DropperThreat categoriesTrojandropperFamily labelsbackdoorrootdata</div><div>Security vendors' analysisDo you want to automate checks?</div><table><tr><td>Avast (Static ML)</td><td>Suspicious</td><td>AlteLab-V3</td><td>Backdoor/Win32.Bluetooth.D91438</td></tr><tr><td>Alibaba</td><td>Trojan.Win32.Bluetooth.374</td><td>ALYac</td><td>Generic.MSL.Bluetooth.18877025</td></tr><tr><td>Avira-ML</td><td>Trojan@Backdoor/MSL.Bluetooth.as</td><td>Avast</td><td>Generic.MSL.Bluetooth.18877025</td></tr><tr><td>Avast</td><td>MSL.Agent.DRO [Tg]</td><td>AVG</td><td>MSL.Agent.DRO [Tg]</td></tr><tr><td>Auslo (no cloud)</td><td>TR.Dropper.Gen7</td><td>Baidu</td><td>MSL.Backdoor.Bluetooth.a</td></tr><tr><td>BitDefender</td><td>Generic.MSL.Bluetooth.18877025</td><td>BitDefender Theta</td><td>Gen.NN.ZenmF.36276.bm@baccorn</td></tr><tr><td>BitDefender</td><td>W32.Fam.VT.San.NN.Worm</td><td>ClamAV</td><td>Win.Packed.Generic.9796019-0</td></tr><tr><td>CrowdStrike Falcon</td><td>WinMalicious_confidence_100% (W)</td><td>Cybereason</td><td>Malicious.d2cf99</td></tr></table></div></div></div>	Avast (Static ML)	Suspicious	AlteLab-V3	Backdoor/Win32.Bluetooth.D91438	Alibaba	Trojan.Win32.Bluetooth.374	ALYac	Generic.MSL.Bluetooth.18877025	Avira-ML	Trojan@Backdoor/MSL.Bluetooth.as	Avast	Generic.MSL.Bluetooth.18877025	Avast	MSL.Agent.DRO [Tg]	AVG	MSL.Agent.DRO [Tg]	Auslo (no cloud)	TR.Dropper.Gen7	Baidu	MSL.Backdoor.Bluetooth.a	BitDefender	Generic.MSL.Bluetooth.18877025	BitDefender Theta	Gen.NN.ZenmF.36276.bm@baccorn	BitDefender	W32.Fam.VT.San.NN.Worm	ClamAV	Win.Packed.Generic.9796019-0	CrowdStrike Falcon	WinMalicious_confidence_100% (W)	Cybereason	Malicious.d2cf99	64/71(90.14%)	Trojan, dropper
Avast (Static ML)	Suspicious	AlteLab-V3	Backdoor/Win32.Bluetooth.D91438																																
Alibaba	Trojan.Win32.Bluetooth.374	ALYac	Generic.MSL.Bluetooth.18877025																																
Avira-ML	Trojan@Backdoor/MSL.Bluetooth.as	Avast	Generic.MSL.Bluetooth.18877025																																
Avast	MSL.Agent.DRO [Tg]	AVG	MSL.Agent.DRO [Tg]																																
Auslo (no cloud)	TR.Dropper.Gen7	Baidu	MSL.Backdoor.Bluetooth.a																																
BitDefender	Generic.MSL.Bluetooth.18877025	BitDefender Theta	Gen.NN.ZenmF.36276.bm@baccorn																																
BitDefender	W32.Fam.VT.San.NN.Worm	ClamAV	Win.Packed.Generic.9796019-0																																
CrowdStrike Falcon	WinMalicious_confidence_100% (W)	Cybereason	Malicious.d2cf99																																
1POYVC5E.exe	<div><div><div><div>54</div><div>71</div></div><div><div>54 security vendors and no sandboxes flagged this file as malicious</div><div><div>c29d336ae11350a04060a356dc70ce83c0cde6db0e40b150ea30a32</div><div>1POYVC5E.exe</div><div>88.00 KB</div><div>2023-02-09 16:07:27 UTC</div><div>2 months ago</div><div>EXE</div></div></div><div><div>Community Score</div><div>pevce spreader assembly direct-cpu-clock-access detect-debug-environment temp-strings runtime-modules</div><div>DETECTIONDETAILSRELATIONSBEHAVIORCOMMUNITY</div><div>Join the VT Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.</div><div>Popular threat labelTrojan.maliciousThreat categoriesTrojanFamily labelsrootbasicbasic</div><div>Security vendors' analysisDo you want to automate checks?</div><table><tr><td>Alibaba</td><td>Trojan.MSL.Kryptik.76faab2b</td><td>ALYac</td><td>Trojan.MSL.Basic.9.Gen</td></tr><tr><td>Avira-ML</td><td>Trojan/Win32.TS.Generic</td><td>Avast</td><td>Trojan.MSL.Basic.9.Gen</td></tr><tr><td>Avast</td><td>Win32.Makara-gen</td><td>AVG</td><td>Win32.Makara-gen</td></tr><tr><td>Auslo (no cloud)</td><td>HEUR/AGEN.1208257</td><td>BitDefender</td><td>Trojan.MSL.Basic.9.Gen</td></tr><tr><td>BitDefender Theta</td><td>Gen.NN.ZenmF.36276.bm@baccorn</td><td>BitDefender</td><td>W32.ADVectra.01</td></tr><tr><td>ClamAV</td><td>Win.Makara.Zpavdo-9554958-0</td><td>CrowdStrike Falcon</td><td>WinMalicious_confidence_100% (W)</td></tr><tr><td>Cybereason</td><td>Malicious.380335</td><td>Cylance</td><td>Unsafe</td></tr><tr><td>Cynet</td><td>Malicious (score: 99)</td><td>DrWeb</td><td>Backdoor.Bluetooth.461</td></tr></table></div></div></div>	Alibaba	Trojan.MSL.Kryptik.76faab2b	ALYac	Trojan.MSL.Basic.9.Gen	Avira-ML	Trojan/Win32.TS.Generic	Avast	Trojan.MSL.Basic.9.Gen	Avast	Win32.Makara-gen	AVG	Win32.Makara-gen	Auslo (no cloud)	HEUR/AGEN.1208257	BitDefender	Trojan.MSL.Basic.9.Gen	BitDefender Theta	Gen.NN.ZenmF.36276.bm@baccorn	BitDefender	W32.ADVectra.01	ClamAV	Win.Makara.Zpavdo-9554958-0	CrowdStrike Falcon	WinMalicious_confidence_100% (W)	Cybereason	Malicious.380335	Cylance	Unsafe	Cynet	Malicious (score: 99)	DrWeb	Backdoor.Bluetooth.461	54/71(76.05%)	Trojan
Alibaba	Trojan.MSL.Kryptik.76faab2b	ALYac	Trojan.MSL.Basic.9.Gen																																
Avira-ML	Trojan/Win32.TS.Generic	Avast	Trojan.MSL.Basic.9.Gen																																
Avast	Win32.Makara-gen	AVG	Win32.Makara-gen																																
Auslo (no cloud)	HEUR/AGEN.1208257	BitDefender	Trojan.MSL.Basic.9.Gen																																
BitDefender Theta	Gen.NN.ZenmF.36276.bm@baccorn	BitDefender	W32.ADVectra.01																																
ClamAV	Win.Makara.Zpavdo-9554958-0	CrowdStrike Falcon	WinMalicious_confidence_100% (W)																																
Cybereason	Malicious.380335	Cylance	Unsafe																																
Cynet	Malicious (score: 99)	DrWeb	Backdoor.Bluetooth.461																																

mailsa.exe	<div> <div> <div>54</div> <div>1/57</div> </div> <div> <div> <div>54 security vendors and no sandboxes flagged this file as malicious</div> <div> <div>5c2d4a8f8ae7b0d8224081f5d8ba58b204d1bd4351d8d4652a3a330fab</div> <div>mailsa.exe</div> <div>23.50 KB</div> <div>2016-05-08 06:23:17 UTC</div> <div>7 years ago</div> <div>EXE</div> </div> </div> <div> <div>Community Score</div> </div> </div> <div> <div>DETECTION</div> <div>DETAILS</div> <div>COMMUNITY</div> </div> <div> <div>Join the VT Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.</div> </div> <div> <div>Popular threat label</div> <div>trojan.barys/fellic</div> <div>Threat categories</div> <div>trojan</div> <div>action</div> <div>Family labels</div> <div>barys</div> <div>idhc</div> <div>age</div> </div> <div> <div>Security vendors' analysis</div> <div>Do you want to automate checks?</div> <table> <tr> <td>Ad-Aware</td><td>Gen Variant Barys.2330</td><td>AvastLab</td><td>W32.W.Joleen.k29a</td></tr> <tr> <td>AhnLab-V3</td><td>Trojan/Win32.Murd</td><td>ALYac</td><td>Gen Variant Barys.2330</td></tr> <tr> <td>Antiy-AVL</td><td>Trojan[HEUR]Win32.Unknown</td><td>Avast</td><td>Trojan Barys.D91A</td></tr> <tr> <td>Avast</td><td>Win32.PRCBot.EPRV [Trj]</td><td>AVG</td><td>Genet28.BWYX</td></tr> <tr> <td>Avira (no cloud)</td><td>TR/Barys.2588.2</td><td>AVware</td><td>Trojan Win32.Autorun.as (v)</td></tr> <tr> <td>Baidu</td><td>Win32.Trojan.Wildem[yes.151026.9955...</td><td>Baidu-International</td><td>Adware Win32.Bhyu.AGER</td></tr> <tr> <td>BitDefender</td><td>Gen Variant Barys.2330</td><td>Bkav Pro</td><td>W32.OxGama270G5.Trojan</td></tr> <tr> <td>ClamAV</td><td>Win.Trojan.Agent-498778</td><td>CMC</td><td>Trojan Win32.Generic.7771489.gen0</td></tr> </table> </div> </div>	Ad-Aware	Gen Variant Barys.2330	AvastLab	W32.W.Joleen.k29a	AhnLab-V3	Trojan/Win32.Murd	ALYac	Gen Variant Barys.2330	Antiy-AVL	Trojan[HEUR]Win32.Unknown	Avast	Trojan Barys.D91A	Avast	Win32.PRCBot.EPRV [Trj]	AVG	Genet28.BWYX	Avira (no cloud)	TR/Barys.2588.2	AVware	Trojan Win32.Autorun.as (v)	Baidu	Win32.Trojan.Wildem[yes.151026.9955...	Baidu-International	Adware Win32.Bhyu.AGER	BitDefender	Gen Variant Barys.2330	Bkav Pro	W32.OxGama270G5.Trojan	ClamAV	Win.Trojan.Agent-498778	CMC	Trojan Win32.Generic.7771489.gen0	54/57(94.73%)	Trojan, adware
Ad-Aware	Gen Variant Barys.2330	AvastLab	W32.W.Joleen.k29a																																
AhnLab-V3	Trojan/Win32.Murd	ALYac	Gen Variant Barys.2330																																
Antiy-AVL	Trojan[HEUR]Win32.Unknown	Avast	Trojan Barys.D91A																																
Avast	Win32.PRCBot.EPRV [Trj]	AVG	Genet28.BWYX																																
Avira (no cloud)	TR/Barys.2588.2	AVware	Trojan Win32.Autorun.as (v)																																
Baidu	Win32.Trojan.Wildem[yes.151026.9955...	Baidu-International	Adware Win32.Bhyu.AGER																																
BitDefender	Gen Variant Barys.2330	Bkav Pro	W32.OxGama270G5.Trojan																																
ClamAV	Win.Trojan.Agent-498778	CMC	Trojan Win32.Generic.7771489.gen0																																
ngusp.exe	<div> <div> <div>61</div> <div>1/61</div> </div> <div> <div> <div>61 security vendors and no sandboxes flagged this file as malicious</div> <div> <div>1b0d74f6c054159d77b2c7a06137ab17d6d13686dc773e4c4fa18a2c312d5f4a</div> <div>ngusp.exe</div> <div>124.09 KB</div> <div>2022-06-01 12:12:20 UTC</div> <div>10 months ago</div> <div>EXE</div> </div> </div> <div> <div>Community Score</div> </div> </div> <div> <div>DETECTION</div> <div>DETAILS</div> <div>RELATIONS</div> <div>COMMUNITY</div> </div> <div> <div>Join the VT Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.</div> </div> <div> <div>Popular threat label</div> <div>trojan.foreign/darkbat</div> <div>Threat categories</div> <div>trojan</div> <div>worm</div> <div>ransomware</div> <div>Family labels</div> <div>foreign</div> <div>darkbat</div> </div> <div> <div>Security vendors' analysis</div> <div>Do you want to automate checks?</div> <table> <tr> <td>Ad-Aware</td><td>Trojan.Generic.KDZ/673319</td><td>AhnLab-V3</td><td>Trojan/Win32.Jask.R30551</td></tr> <tr> <td>Alibaba</td><td>Ransom/Win32F.oreign.faa3eb59</td><td>ALYac</td><td>Trojan.Generic.KDZ/673319</td></tr> <tr> <td>Avast</td><td>Trojan.Generic.KDZ/DAM627</td><td>Avast</td><td>Win32.Malware-gen</td></tr> <tr> <td>AVG</td><td>Win32.Malware-gen</td><td>Avira (no cloud)</td><td>WORM/Darkbat.A.1018</td></tr> <tr> <td>BitDefender</td><td>Trojan.Generic.KDZ/673319</td><td>BitDefender Theta</td><td>Gen.NH.ZagpHf.34712.hmGduR9Sg</td></tr> <tr> <td>Bkav Pro</td><td>W32.Common.A230F0DA</td><td>ClamAV</td><td>Win.Worm.Eloab-9947682-0</td></tr> <tr> <td>Comodo</td><td>TrojWare.Win32.Injector.IEW@443u4</td><td>CrowdStrike Falcon</td><td>Win/malicious_confidence_80% (W)</td></tr> <tr> <td>Cybereason</td><td>Malicious.c75cd2</td><td>Cylance</td><td>Unsafe</td></tr> </table> </div> </div>	Ad-Aware	Trojan.Generic.KDZ/673319	AhnLab-V3	Trojan/Win32.Jask.R30551	Alibaba	Ransom/Win32F.oreign.faa3eb59	ALYac	Trojan.Generic.KDZ/673319	Avast	Trojan.Generic.KDZ/DAM627	Avast	Win32.Malware-gen	AVG	Win32.Malware-gen	Avira (no cloud)	WORM/Darkbat.A.1018	BitDefender	Trojan.Generic.KDZ/673319	BitDefender Theta	Gen.NH.ZagpHf.34712.hmGduR9Sg	Bkav Pro	W32.Common.A230F0DA	ClamAV	Win.Worm.Eloab-9947682-0	Comodo	TrojWare.Win32.Injector.IEW@443u4	CrowdStrike Falcon	Win/malicious_confidence_80% (W)	Cybereason	Malicious.c75cd2	Cylance	Unsafe	61/69(88.40%)	Trojan, worm, ransomware
Ad-Aware	Trojan.Generic.KDZ/673319	AhnLab-V3	Trojan/Win32.Jask.R30551																																
Alibaba	Ransom/Win32F.oreign.faa3eb59	ALYac	Trojan.Generic.KDZ/673319																																
Avast	Trojan.Generic.KDZ/DAM627	Avast	Win32.Malware-gen																																
AVG	Win32.Malware-gen	Avira (no cloud)	WORM/Darkbat.A.1018																																
BitDefender	Trojan.Generic.KDZ/673319	BitDefender Theta	Gen.NH.ZagpHf.34712.hmGduR9Sg																																
Bkav Pro	W32.Common.A230F0DA	ClamAV	Win.Worm.Eloab-9947682-0																																
Comodo	TrojWare.Win32.Injector.IEW@443u4	CrowdStrike Falcon	Win/malicious_confidence_80% (W)																																
Cybereason	Malicious.c75cd2	Cylance	Unsafe																																
tleditor.exe	<div> <div> <div>52</div> <div>1/72</div> </div> <div> <div> <div>52 security vendors and no sandboxes flagged this file as malicious</div> <div> <div>90c2583a6a394652bdc19311084fa26b5fa5250902ba44d8d7346a9608b-85dcfd</div> <div>tleditor.exe</div> <div>586.93 KB</div> <div>2020-07-20 00:35:36 UTC</div> <div>2 years ago</div> <div>EXE</div> </div> </div> <div> <div>Community Score</div> </div> </div> <div> <div>DETECTION</div> <div>DETAILS</div> <div>RELATIONS</div> <div>BEHAVIOR</div> <div>COMMUNITY</div> </div> <div> <div>Join the VT Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.</div> </div> <div> <div>Popular threat label</div> <div>trojan.ogpess/hells</div> <div>Threat categories</div> <div>trojan</div> <div>dropper</div> <div>downloader</div> <div>Family labels</div> <div>ogpess</div> <div>hell</div> <div>subogenesis</div> </div> <div> <div>Security vendors' analysis</div> <div>Do you want to automate checks?</div> <table> <tr> <td>Ad-Aware</td><td>Dropped Trojan.PWS.YWKK</td><td>AegisLab</td><td>Trojan Win32.Generic.dtc</td></tr> <tr> <td>Alibaba</td><td>Trojan/Downloader.Win32/Generic.ba460...</td><td>ALYac</td><td>Dropped Trojan.PWS.YWKK</td></tr> <tr> <td>Antiy-AVL</td><td>Trojan/Win32.Unknown</td><td>Avast</td><td>Trojan.PWS.YWKK</td></tr> <tr> <td>Avast</td><td>Win32.Dropper-EOO [Dnp]</td><td>AVG</td><td>Win32.Dropper-EOO [Dnp]</td></tr> <tr> <td>Avira (no cloud)</td><td>[TempDir]tleditor.exe</td><td>BitDefender</td><td>Dropped Trojan.PWS.YWKK</td></tr> <tr> <td>BitDefender Theta</td><td>Gen.NH.Zexaf.34136.FyibaaF.Xmmb</td><td>ClamAV</td><td>Win.Trojan.Agent.796893</td></tr> <tr> <td>Comodo</td><td>Worm.Win32.Dropper.RA@hgrag</td><td>CrowdStrike Falcon</td><td>Win/malicious_confidence_50% (W)</td></tr> <tr> <td>Cybereason</td><td>Malicious.29622c</td><td>Cylance</td><td>Unsafe</td></tr> </table> </div> </div>	Ad-Aware	Dropped Trojan.PWS.YWKK	AegisLab	Trojan Win32.Generic.dtc	Alibaba	Trojan/Downloader.Win32/Generic.ba460...	ALYac	Dropped Trojan.PWS.YWKK	Antiy-AVL	Trojan/Win32.Unknown	Avast	Trojan.PWS.YWKK	Avast	Win32.Dropper-EOO [Dnp]	AVG	Win32.Dropper-EOO [Dnp]	Avira (no cloud)	[TempDir]tleditor.exe	BitDefender	Dropped Trojan.PWS.YWKK	BitDefender Theta	Gen.NH.Zexaf.34136.FyibaaF.Xmmb	ClamAV	Win.Trojan.Agent.796893	Comodo	Worm.Win32.Dropper.RA@hgrag	CrowdStrike Falcon	Win/malicious_confidence_50% (W)	Cybereason	Malicious.29622c	Cylance	Unsafe	52/72(72.22%)	Trojan, dropper, downloader
Ad-Aware	Dropped Trojan.PWS.YWKK	AegisLab	Trojan Win32.Generic.dtc																																
Alibaba	Trojan/Downloader.Win32/Generic.ba460...	ALYac	Dropped Trojan.PWS.YWKK																																
Antiy-AVL	Trojan/Win32.Unknown	Avast	Trojan.PWS.YWKK																																
Avast	Win32.Dropper-EOO [Dnp]	AVG	Win32.Dropper-EOO [Dnp]																																
Avira (no cloud)	[TempDir]tleditor.exe	BitDefender	Dropped Trojan.PWS.YWKK																																
BitDefender Theta	Gen.NH.Zexaf.34136.FyibaaF.Xmmb	ClamAV	Win.Trojan.Agent.796893																																
Comodo	Worm.Win32.Dropper.RA@hgrag	CrowdStrike Falcon	Win/malicious_confidence_50% (W)																																
Cybereason	Malicious.29622c	Cylance	Unsafe																																
X 000 A (27).exe	<div> <div> <div>44</div> <div>1/47</div> </div> <div> <div> <div>44 security vendors and no sandboxes flagged this file as malicious</div> <div> <div>c04943d0f3d5d96a24c8b04252b26d44b55cde12e9e5b00539dbd330a27431</div> <div>X 000 A (27).exe</div> <div>280.67 KB</div> <div>2014-01-05 15:18:28 UTC</div> <div>9 years ago</div> <div>EXE</div> </div> </div> <div> <div>Community Score</div> </div> </div> <div> <div>DETECTION</div> <div>DETAILS</div> <div>BEHAVIOR</div> <div>COMMUNITY</div> </div> <div> <div>Join the VT Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.</div> </div> <div> <div>Popular threat label</div> <div>virus.jeefo/hidrag</div> <div>Threat categories</div> <div>virus</div> <div>Family labels</div> <div>jeefo</div> <div>hidrag</div> </div> <div> <div>Security vendors' analysis</div> <div>Do you want to automate checks?</div> <table> <tr> <td>Ad-Aware</td><td>Win32.Jeefo.B</td><td>AhnLab-V3</td><td>Win32Hidrag</td></tr> <tr> <td>AntiVr</td><td>W32.Jeefo.A</td><td>Avast</td><td>Win32.Jeefo</td></tr> <tr> <td>AVG</td><td>Win32Hidrag.A</td><td>Baidu-International</td><td>Virus.Win32.Jeefo.\$40</td></tr> <tr> <td>BitDefender</td><td>Win32.Jeefo.B</td><td>Bkav Pro</td><td>W32.SplitFile.TB.PE</td></tr> <tr> <td>ClamAV</td><td>W32.Jeefo-3</td><td>CommTouch</td><td>W32/Jeefo.OYRV-0749</td></tr> <tr> <td>Comodo</td><td>Win32.Jeefo.A</td><td>DrWeb</td><td>Win32.HLLP.Jeefo.36352</td></tr> <tr> <td>Emisoft</td><td>Win32.Jeefo.B (B)</td><td>eScan</td><td>Win32.Jeefo.B</td></tr> <tr> <td>ESET-NOD32</td><td>Win32/Jeefo.A</td><td>F-Pro</td><td>W32/Jeefo.A</td></tr> </table> </div> </div>	Ad-Aware	Win32.Jeefo.B	AhnLab-V3	Win32Hidrag	AntiVr	W32.Jeefo.A	Avast	Win32.Jeefo	AVG	Win32Hidrag.A	Baidu-International	Virus.Win32.Jeefo.\$40	BitDefender	Win32.Jeefo.B	Bkav Pro	W32.SplitFile.TB.PE	ClamAV	W32.Jeefo-3	CommTouch	W32/Jeefo.OYRV-0749	Comodo	Win32.Jeefo.A	DrWeb	Win32.HLLP.Jeefo.36352	Emisoft	Win32.Jeefo.B (B)	eScan	Win32.Jeefo.B	ESET-NOD32	Win32/Jeefo.A	F-Pro	W32/Jeefo.A	44/47(93.61%)	Virus
Ad-Aware	Win32.Jeefo.B	AhnLab-V3	Win32Hidrag																																
AntiVr	W32.Jeefo.A	Avast	Win32.Jeefo																																
AVG	Win32Hidrag.A	Baidu-International	Virus.Win32.Jeefo.\$40																																
BitDefender	Win32.Jeefo.B	Bkav Pro	W32.SplitFile.TB.PE																																
ClamAV	W32.Jeefo-3	CommTouch	W32/Jeefo.OYRV-0749																																
Comodo	Win32.Jeefo.A	DrWeb	Win32.HLLP.Jeefo.36352																																
Emisoft	Win32.Jeefo.B (B)	eScan	Win32.Jeefo.B																																
ESET-NOD32	Win32/Jeefo.A	F-Pro	W32/Jeefo.A																																

X 000 A (28).exe		14/53(26.41%)	Trojan, adware
X 000 A (29).exe		53/72(73.61%)	Trojan, down-loader

- **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.
1MHR5-TKD.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	<p>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.</p> <p>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.</p>
mailsa.exe	Trojan barys lethic	<p>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.</p> <p>Barys Lethic este capabil să execute o gamă largă de funcții malițioase, inclusiv:</p> <ul style="list-style-type: none"> – 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	<p>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.</p> <p>Foreign Dorkbot este un Trojan multifuncțional și poate fi utilizat pentru o serie de activități malițioase, inclusiv:</p> <ul style="list-style-type: none"> – 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 <p>Trojanul Foreign Dorkbot este capabil să se ascundă în sistemul infectat și poate fi dificil de detectat și eliminat.</p>
tleditor.exe	Trojan qq-pass/nsis	<p>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.</p> <p>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.</p>

X 000 A (27).exe	Virus jeefo/hidrag	<p>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.</p> <p>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.</p>
X 000 A (28).exe	Adware installerex/installrex	<p>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 nedorite pe computerul utilizatorului.</p> <p>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.</p> <p>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.</p>
X 000 A (29).exe	Trojan Agent AVZO	<p>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.</p>

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/>