CYT-250-Threat Investigation

Practical steps of using YARA by utilizing rules from the repository

Elaborate by:

Leandro Delgado

Student Number: 114416241

Professor: Tatiana Outkina

CYT250 Lab 6 Winter 2025_Part1 - 3%

Individual work

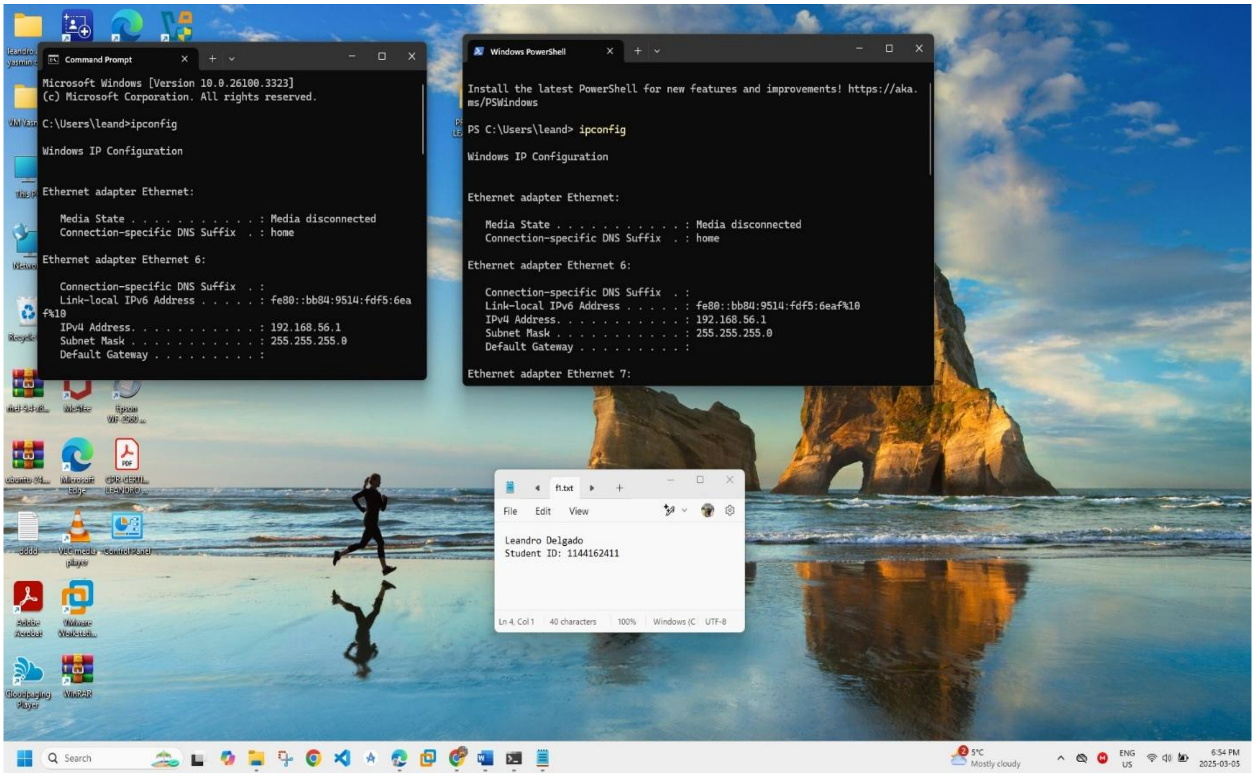
Objectives: learn practical steps of using YARA by utilizing rules from the repository.

Your task is to follow the steps as described and perform them on your own computer. The list of steps include:

- Getting a set of rules to use
- Download a specific rule file
- Running YARA from the command line.
- Make and run your own simple Yara rule.

This lab is divided to two parts, where Part 1 start from introduction and basic learning, followed by Part 2 where you develop and run your own rules. By running both parts 1 and 2 you develop technical skills:

- Install Yara
- Use posted GitHub rules in practice to hunt malware
- Develop your own rules
- Run the rules for malware detection and hunting



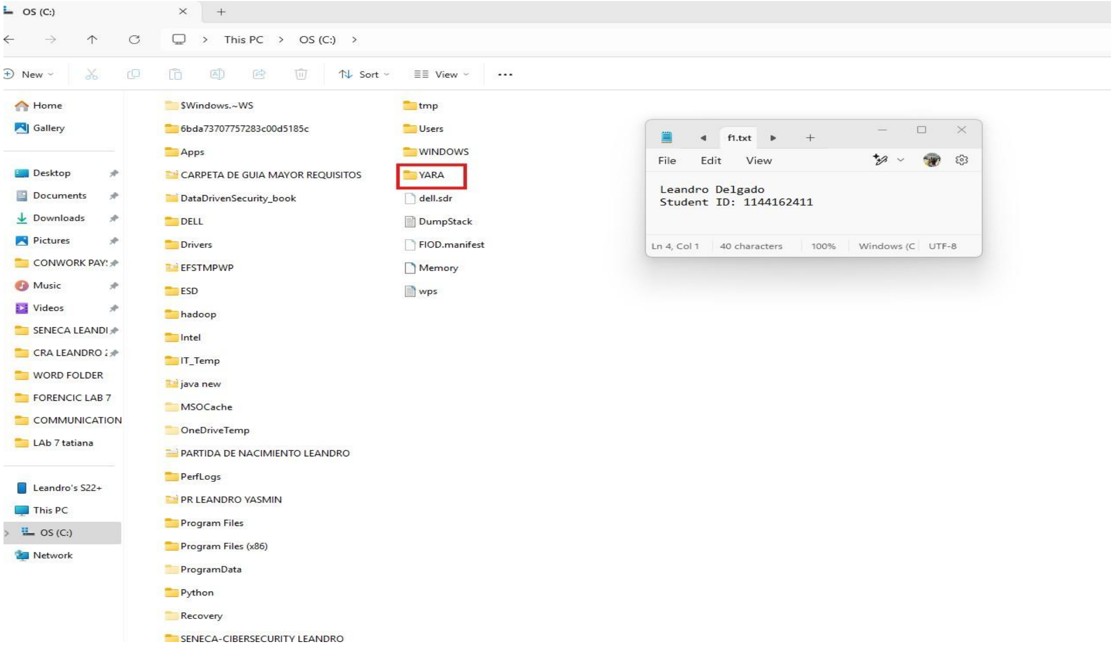
```
Microsoft Windows [Version 10.0.26100.3323]
(c) Microsoft Corporation. All rights reserved.

C:\Users\leand>ipconfig

Windows IP Configuration


Ethernet adapter Ethernet:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . : home

Ethernet adapter Ethernet 6:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::bb84:9514:fdf5:6ea
f%10
   IPv4 Address. . . . . . . . . . . : 192.168.56.1
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :
```

```
Install the latest PowerShell for new features and improvements! https://aka.
ms/PSWindows

PS C:\Users\leand> ipconfig

Windows IP Configuration


Ethernet adapter Ethernet:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . : home

Ethernet adapter Ethernet 6:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::bb84:9514:fdf5:6eaf%10
   IPv4 Address. . . . . . . . . . . : 192.168.56.1
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :

Ethernet adapter Ethernet 7:
```

```
Leandro Delgado
Student ID: 1144162411
```

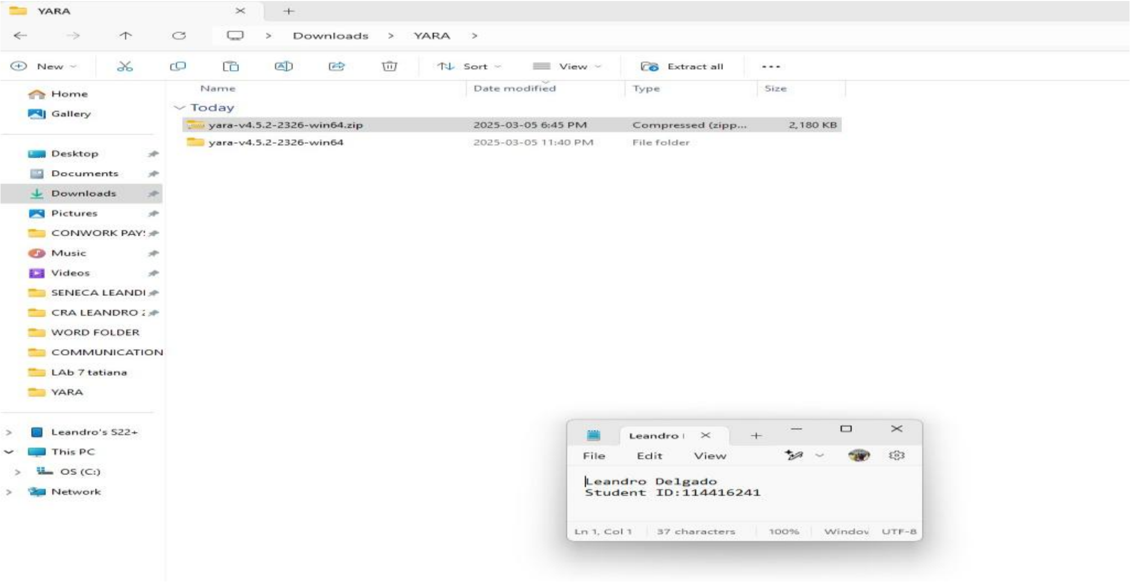
Task 1. Install Yara – 1%

- Installing YARA



Leandro Delgado
Student ID: 1144162411

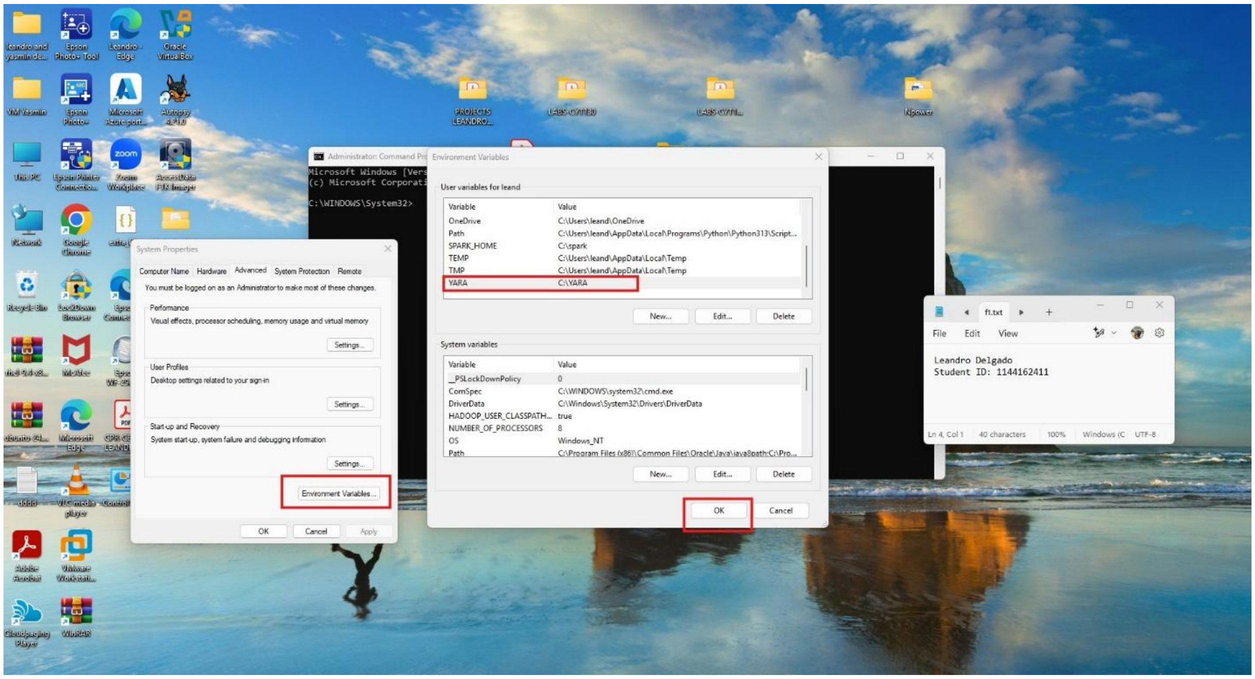
-
-



Name	Date modified	Type	Size
Today			
yara-v4.5.2-2326-win64.zip	2025-03-05 6:45 PM	Compressed (zipp...	2,180 KB
yara-v4.5.2-2326-win64	2025-03-05 11:40 PM	File folder	

Leandro Delgado
Student ID:114416241

First, I downloaded the YARA ZIP file from its original source; save it to your folder. After downloading, go to File Explorer and right-click the file to find "Extract All...". Then select the folder where the extracted files will be located before clicking the "Extract" button on its window. Immediately after completing it, click to open the newly extracted folder (yara-v4.52-2326-win64) to make sure the files are all there.



```
Administrator: Command Pr
Microsoft Windows [Vers
(c) Microsoft Corporati

C:\WINDOWS\System32>
```

System Properties

You must be logged on as an Administrator to make most of these changes.

Performance

Visual effects, processor scheduling, memory usage and virtual memory

User Profiles

Desktop settings related to your sign-in

Start-up and Recovery

System start-up, system failure and debugging information

Environment Variables

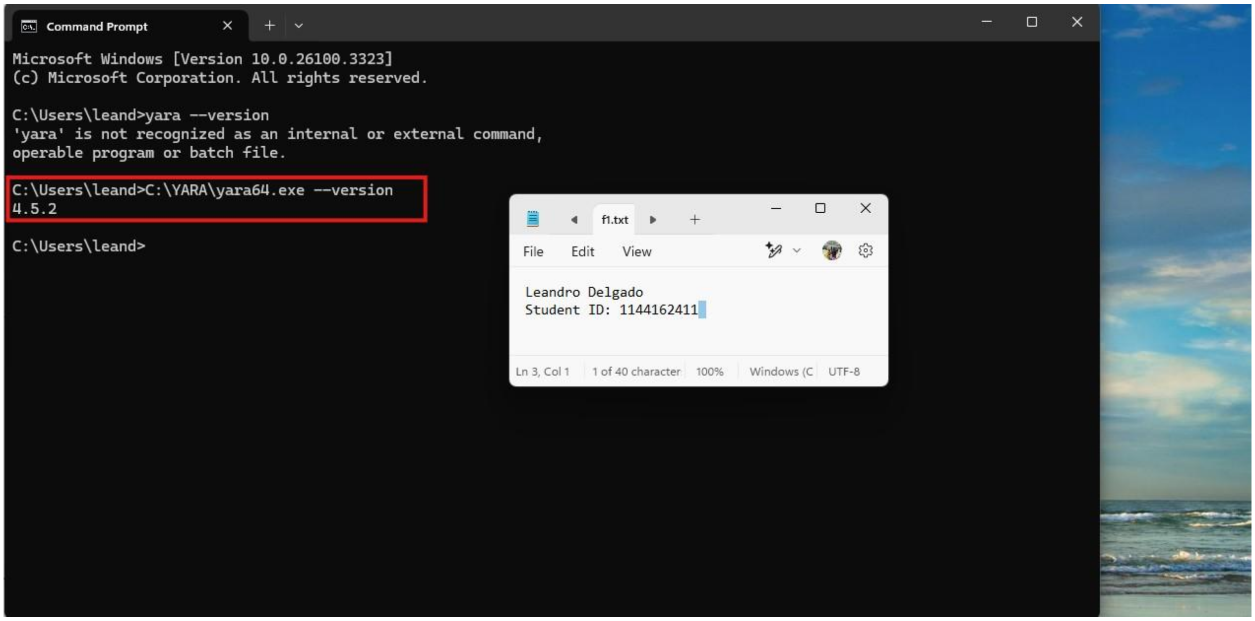
User variables for leand

Variable	Value
OneDrive	C:\Users\leand\OneDrive
Path	C:\Users\leand\AppData\Local\Programs\Python\Python313\Script...
SPARK_HOME	C:\spark
TEMP	C:\Users\leand\AppData\Local\Temp
TMP	C:\Users\leand\AppData\Local\Temp
YARA	C:\YARA

System variables

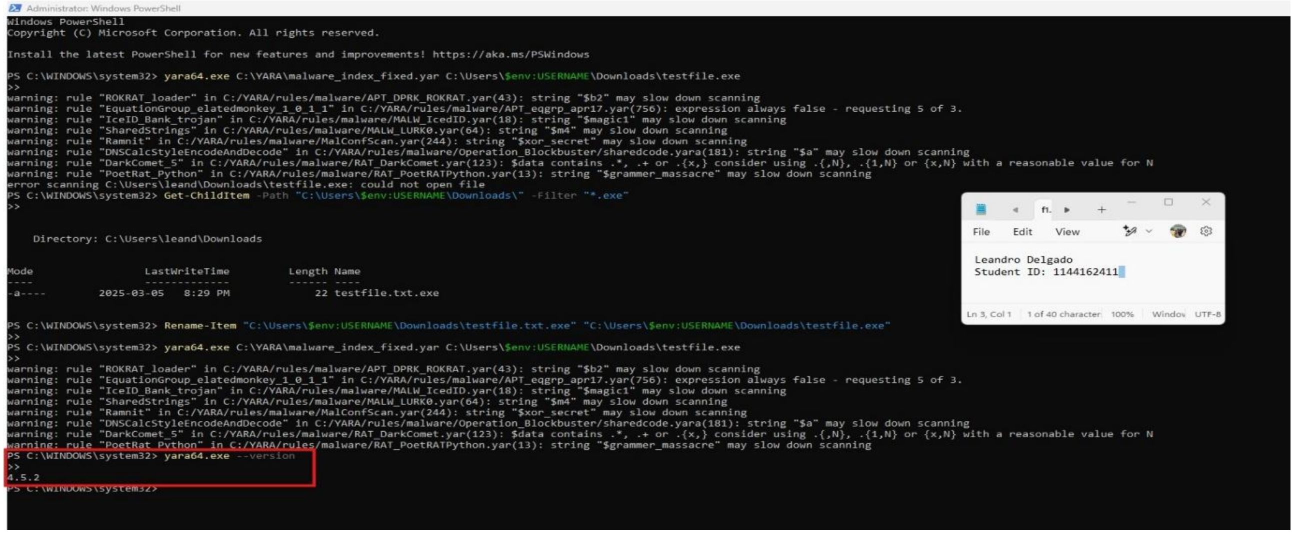
Variable	Value
_PSLockDownPolicy	0
ComSpec	C:\WINDOWS\system32\cmd.exe
DriverData	C:\Windows\System32\Drivers\DriverData
HADOOP_USER_CLASSPATH...	true
NUMBER_OF_PROCESSORS	8
OS	Windows_NT
Path	C:\Program Files (x86)\Common Files\Oracle\Java\java8path;C:\Pro...

```
Leandro Delgado
Student ID: 1144162411
```



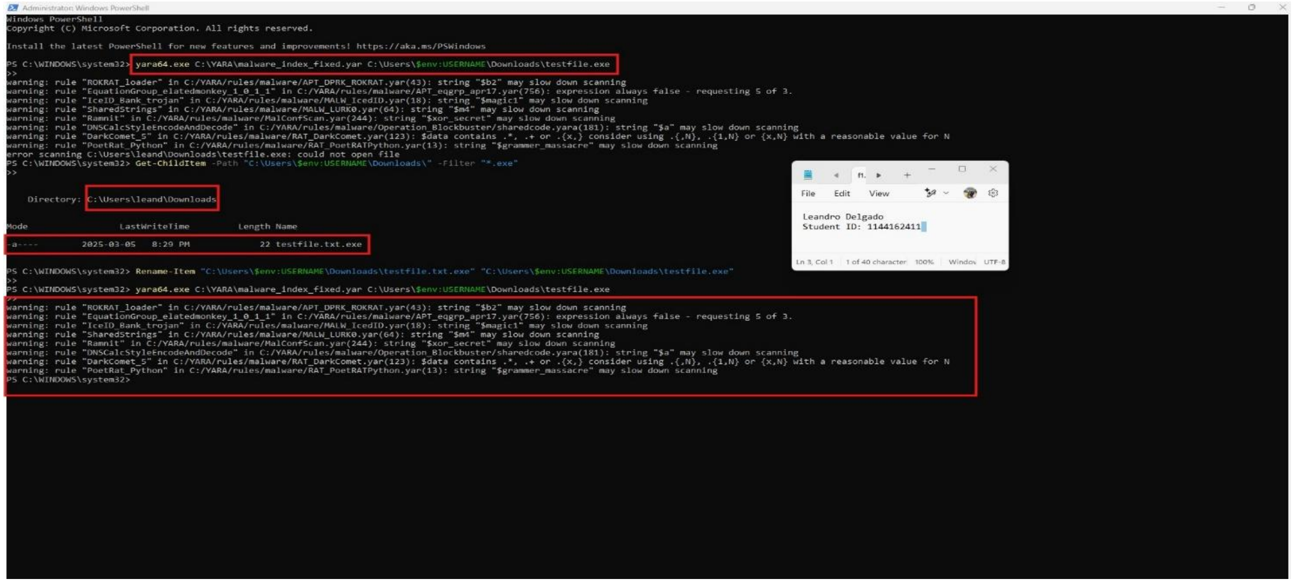
```
Microsoft Windows [Version 10.0.26100.3323]
(c) Microsoft Corporation. All rights reserved.

C:\Users\leand>yara --version
'yara' is not recognized as an internal or external command,
operable program or batch file.

C:\Users\leand>C:\YARA\yara64.exe --version
4.5.2

C:\Users\leand>
```

```
Leandro Delgado
Student ID: 1144162411
```



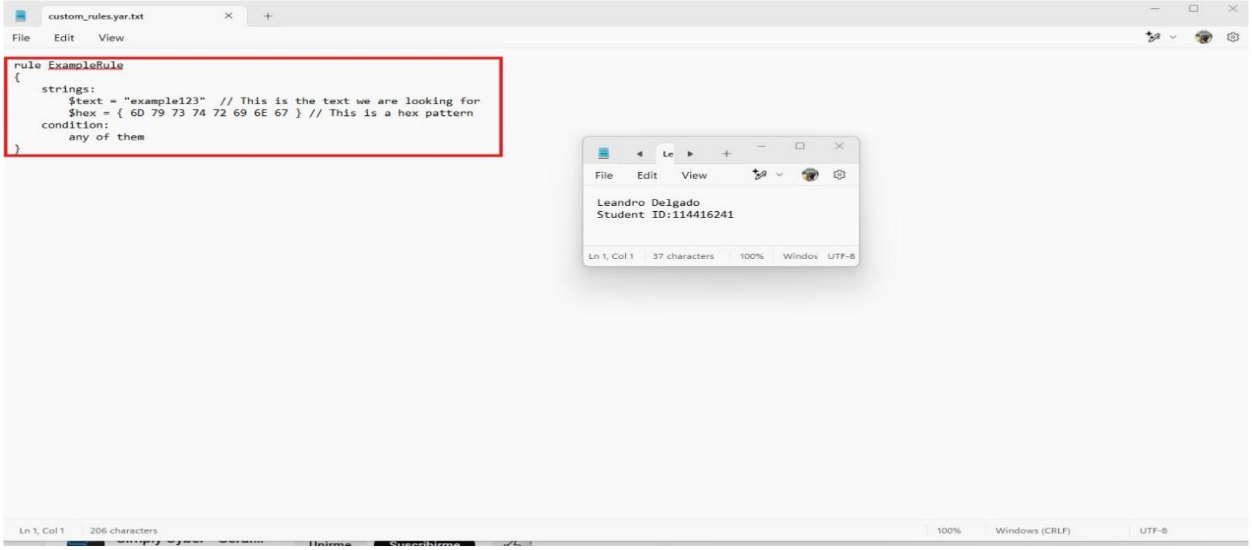
```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows

PS C:\WINDOWS\system32> yara64.exe C:\YARA\malware_index_fixed.yar C:\Users\$env:USERNAME\Downloads\testfile.exe
>>
warning: rule "ROKRAT_loader" in C:/YARA/rules/malware/APT_DPRK_ROKRAT.yar(43): string "$b2" may slow down scanning
warning: rule "EquationGroup_elatedmonkey_1_0_1_1" in C:/YARA/rules/malware/APT_eqgrp_apr17.yar(756): expression always false - requesting 5 of 3.
warning: rule "IceID_Bank_trojan" in C:/YARA/rules/malware/MALW_IcedID.yar(18): string "$magic1" may slow down scanning
warning: rule "SharedStrings" in C:/YARA/rules/malware/MALW_LURK0.yar(64): string "$m4" may slow down scanning
warning: rule "Ramnit" in C:/YARA/rules/malware/MalConfScan.yar(244): string "$xor_secret" may slow down scanning
warning: rule "DNSCalcStyleEncodeAndDecode" in C:/YARA/rules/malware/Operation_Blockbuster/sharedcode.yara(181): string "$a" may slow down scanning
warning: rule "DarkComet_5" in C:/YARA/rules/malware/RAT_DarkComet.yar(123): $data contains .*, .+ or .{x,} consider using .{,N}, .{1,N} or {x,N} with a reasonable value for N
warning: rule "PoetRat_Python" in C:/YARA/rules/malware/RAT_PoetRATPython.yar(13): string "$grammer_massacre" may slow down scanning
error scanning C:\Users\leand\Downloads\testfile.exe: could not open file
PS C:\WINDOWS\system32> Get-ChildItem -Path "C:\Users\$env:USERNAME\Downloads\" -Filter "*.exe"
>>


    Directory: C:\Users\leand\Downloads


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----        2025-03-05   8:29 PM             22 testfile.txt.exe


PS C:\WINDOWS\system32> Rename-Item "C:\Users\$env:USERNAME\Downloads\testfile.txt.exe" "C:\Users\$env:USERNAME\Downloads\testfile.exe"
>>
PS C:\WINDOWS\system32> yara64.exe C:\YARA\malware_index_fixed.yar C:\Users\$env:USERNAME\Downloads\testfile.exe
>>
warning: rule "ROKRAT_loader" in C:/YARA/rules/malware/APT_DPRK_ROKRAT.yar(43): string "$b2" may slow down scanning
warning: rule "EquationGroup_elatedmonkey_1_0_1_1" in C:/YARA/rules/malware/APT_eqgrp_apr17.yar(756): expression always false - requesting 5 of 3.
warning: rule "IceID_Bank_trojan" in C:/YARA/rules/malware/MALW_IcedID.yar(18): string "$magic1" may slow down scanning
warning: rule "SharedStrings" in C:/YARA/rules/malware/MALW_LURK0.yar(64): string "$m4" may slow down scanning
warning: rule "Ramnit" in C:/YARA/rules/malware/MalConfScan.yar(244): string "$xor_secret" may slow down scanning
warning: rule "DNSCalcStyleEncodeAndDecode" in C:/YARA/rules/malware/Operation_Blockbuster/sharedcode.yara(181): string "$a" may slow down scanning
warning: rule "DarkComet_5" in C:/YARA/rules/malware/RAT_DarkComet.yar(123): $data contains .*, .+ or .{x,} consider using .{,N}, .{1,N} or {x,N} with a reasonable value for N
warning: rule "PoetRat_Python" in C:/YARA/rules/malware/RAT_PoetRATPython.yar(13): string "$grammer_massacre" may slow down scanning
PS C:\WINDOWS\system32> yara64.exe --version
>>
4.5.2
PS C:\WINDOWS\system32>
```

```
Leandro Delgado
Student ID: 1144162411
```



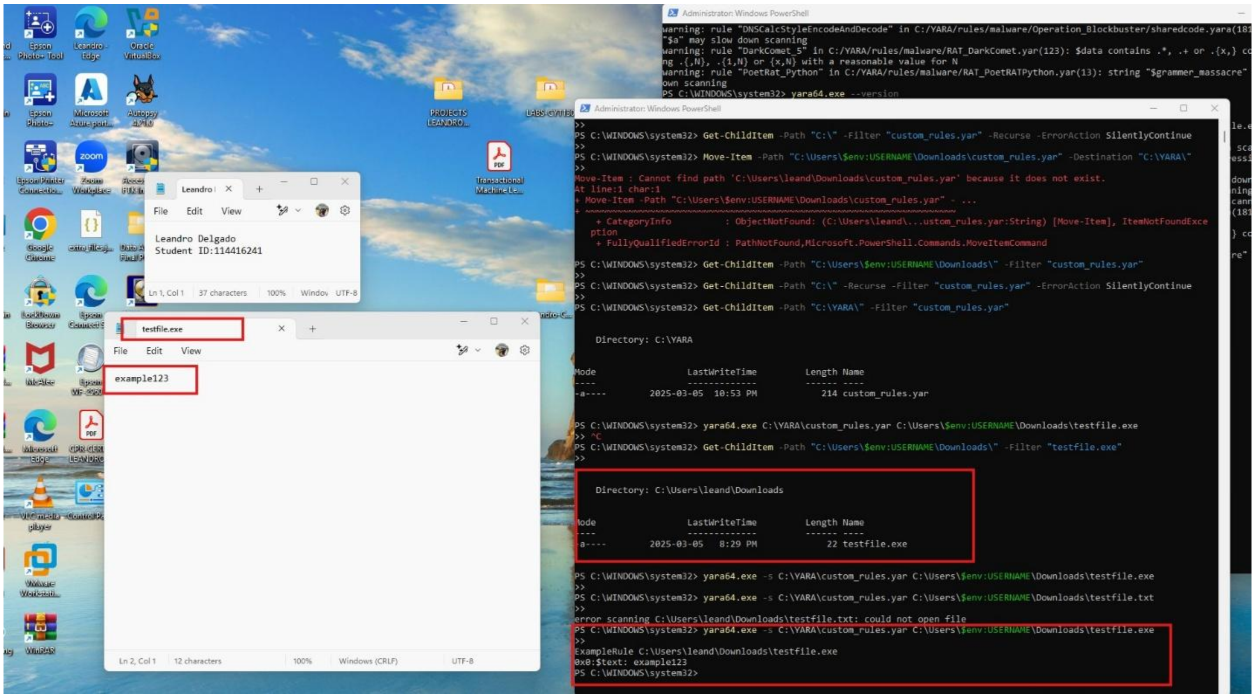
```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows

PS C:\WINDOWS\system32> yara64.exe C:\YARA\malware_index_fixed.yar C:\Users\$env:USERNAME\Downloads\testfile.exe
>>
warning: rule "ROKRAT_loader" in C:/YARA/rules/malware/APT_DPRK_ROKRAT.yar(43): string "$b2" may slow down scanning
warning: rule "EquationGroup_elatedmonkey_1_0_1_1" in C:/YARA/rules/malware/APT_eqgrp_apr17.yar(756): expression always false - requesting 5 of 3.
warning: rule "IceID_Bank_trojan" in C:/YARA/rules/malware/MALW_IcedID.yar(18): string "$magic1" may slow down scanning
warning: rule "SharedStrings" in C:/YARA/rules/malware/MALW_LURK0.yar(64): string "$m4" may slow down scanning
warning: rule "Ramnit" in C:/YARA/rules/malware/MalConfScan.yar(244): string "$xor_secret" may slow down scanning
warning: rule "DNSCalcStyleEncodeAndDecode" in C:/YARA/rules/malware/Operation_Blockbuster/sharedcode.yara(181): string "$a" may slow down scanning
warning: rule "DarkComet_5" in C:/YARA/rules/malware/RAT_DarkComet.yar(123): $data contains .*, .+ or .{x,} consider using .{,N}, .{1,N} or {x,N} with a reasonable value for N
warning: rule "PoetRat_Python" in C:/YARA/rules/malware/RAT_PoetRATPython.yar(13): string "$grammer_massacre" may slow down scanning
error scanning C:\Users\leand\Downloads\testfile.exe: could not open file
PS C:\WINDOWS\system32> Get-ChildItem -Path "C:\Users\$env:USERNAME\Downloads\" -Filter "*.exe"
>>

    Directory: C:\Users\leand\Downloads

Mode                 LastWriteTime         Length Name

-a----        2025-03-05   8:29 PM             22 testfile.txt.exe

PS C:\WINDOWS\system32> Rename-Item "C:\Users\$env:USERNAME\Downloads\testfile.txt.exe" "C:\Users\$env:USERNAME\Downloads\testfile.exe"
>>
PS C:\WINDOWS\system32> yara64.exe C:\YARA\malware_index_fixed.yar C:\Users\$env:USERNAME\Downloads\testfile.exe
>>
warning: rule "ROKRAT_loader" in C:/YARA/rules/malware/APT_DPRK_ROKRAT.yar(43): string "$b2" may slow down scanning
warning: rule "EquationGroup_elatedmonkey_1_0_1_1" in C:/YARA/rules/malware/APT_eqgrp_apr17.yar(756): expression always false - requesting 5 of 3.
warning: rule "IceID_Bank_trojan" in C:/YARA/rules/malware/MALW_IcedID.yar(18): string "$magic1" may slow down scanning
warning: rule "SharedStrings" in C:/YARA/rules/malware/MALW_LURK0.yar(64): string "$m4" may slow down scanning
warning: rule "Ramnit" in C:/YARA/rules/malware/MalConfScan.yar(244): string "$xor_secret" may slow down scanning
warning: rule "DNSCalcStyleEncodeAndDecode" in C:/YARA/rules/malware/Operation_Blockbuster/sharedcode.yara(181): string "$a" may slow down scanning
warning: rule "DarkComet_5" in C:/YARA/rules/malware/RAT_DarkComet.yar(123): $data contains .*, .+ or .{x,} consider using .{,N}, .{1,N} or {x,N} with a reasonable value for N
warning: rule "PoetRat_Python" in C:/YARA/rules/malware/RAT_PoetRATPython.yar(13): string "$grammer_massacre" may slow down scanning
PS C:\WINDOWS\system32>
```

```
Leandro Delgado
Student ID: 1144162411
```



```
rule ExampleRule
{
    strings:
        $text = "example123"  // This is the text we are looking for
        $hex = { 6D 79 73 74 72 69 6E 67 } // This is a hex pattern
    condition:
        any of them
}
```

```
Leandro Delgado
Student ID:114416241
```



```
Leandro Delgado
Student ID:114416241
```

testfile.exe

```
example123
```

```
warning: rule "DNSCalcStyleEncodeAndDecode" in C:/YARA/rules/malware/Operation_Blockbuster/sharedcode.yara(181
"$a" may slow down scanning
warning: rule "DarkComet_5" in C:/YARA/rules/malware/RAT_DarkComet.yar(123): $data contains .*, .+ or .{x,} co
ng .{,N}, .{1,N} or {x,N} with a reasonable value for N
warning: rule "PoetRat_Python" in C:/YARA/rules/malware/RAT_PoetRATPython.yar(13): string "$grammer_massacre"
own scanning
PS C:\WINDOWS\system32> yara64.exe --version
```

```
>>
PS C:\WINDOWS\system32> Get-ChildItem -Path "C:\" -Filter "custom_rules.yar" -Recurse -ErrorAction SilentlyContinue
>>
PS C:\WINDOWS\system32> Move-Item -Path "C:\Users\$env:USERNAME\Downloads\custom_rules.yar" -Destination "C:\YARA\"
>>
Move-Item : Cannot find path 'C:\Users\leand\Downloads\custom_rules.yar' because it does not exist.
At line:1 char:1
+ Move-Item -Path "C:\Users\$env:USERNAME\Downloads\custom_rules.yar" - ...
+ ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
    + CategoryInfo          : ObjectNotFound: (C:\Users\leand\...ustom_rules.yar:String) [Move-Item], ItemNotFoundExce
   ption
    + FullyQualifiedErrorId : PathNotFound,Microsoft.PowerShell.Commands.MoveItemCommand

PS C:\WINDOWS\system32> Get-ChildItem -Path "C:\Users\$env:USERNAME\Downloads\" -Filter "custom_rules.yar"
>>
PS C:\WINDOWS\system32> Get-ChildItem -Path "C:\" -Recurse -Filter "custom_rules.yar" -ErrorAction SilentlyContinue
>>
PS C:\WINDOWS\system32> Get-ChildItem -Path "C:\YARA\" -Filter "custom_rules.yar"


    Directory: C:\YARA


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----        2025-03-05  10:53 PM            214 custom_rules.yar


PS C:\WINDOWS\system32> yara64.exe C:\YARA\custom_rules.yar C:\Users\$env:USERNAME\Downloads\testfile.exe
>> ^C
PS C:\WINDOWS\system32> Get-ChildItem -Path "C:\Users\$env:USERNAME\Downloads\" -Filter "testfile.exe"
>>


    Directory: C:\Users\leand\Downloads


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----        2025-03-05   8:29 PM             22 testfile.exe


PS C:\WINDOWS\system32> yara64.exe -s C:\YARA\custom_rules.yar C:\Users\$env:USERNAME\Downloads\testfile.exe
>>
PS C:\WINDOWS\system32> yara64.exe -s C:\YARA\custom_rules.yar C:\Users\$env:USERNAME\Downloads\testfile.txt
>>
error scanning C:\Users\leand\Downloads\testfile.txt: could not open file
PS C:\WINDOWS\system32> yara64.exe -s C:\YARA\custom_rules.yar C:\Users\$env:USERNAME\Downloads\testfile.exe
>>
ExampleRule C:\Users\leand\Downloads\testfile.exe
0x0:$text: example123
PS C:\WINDOWS\system32>
```

First, I installed YARA by placing yara64.exe and yarac64.exe in C:\YARA\ and verified installation through a command line operation. Next, I obtained a set of YARA rules by cloning the official repository from GitHub and listing the available .yar files in C:\YARA\rules\malware. One file, the malware_index.yar file, was missing during this operation, but you solved it by moving the malware_index.yar file to C:\YARA\ and confirming its presence using PowerShell. After setting up the rules, YARAs were run from the command line against a file named testfile.exe, where the paths were being repaired through some sort of solving.

After the standard ruleset was set up, I created and validated my personally customized YARA rule. I authored a simple rule in custom_rules.yar, deposited it in the C:\YARA\ directory, and ensured the file was properly lodged in it. The goal of the rule was to detect a defined string example123, and a hex pattern. After that, I executed YARA against testfile.exe and confirmed the string was detected in the file. Now I have completed everything: installation, ruleset setup, downloading a special rule file, running YARA from the command line, and creating your own rule. The setup is now fully operational, and ready for the more advanced techniques in YARA involving directory scanning, rule optimization, and integration with other security tools.

Task 2. Work on Yara rules available at github – 2%

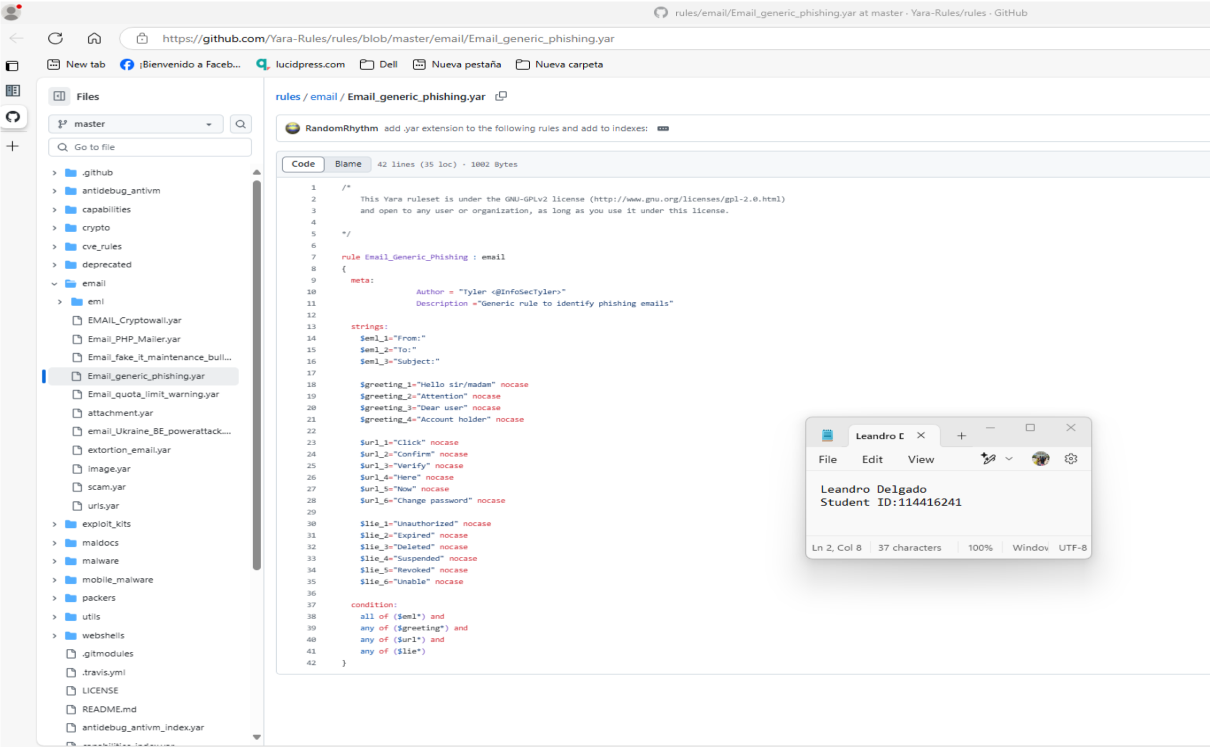
Video about rules

https://www.youtube.com/watch?v=BM23_H2GGMA

Step 1. Connect to the link:

[rules/email/Email_generic_phishing.yar at master · Yara-Rules/rules · GitHub]

Consult YARA documentation and write the comment to this YARA rule, which is one of the email set of rules. Describe in details what kind of filtering is established by this rule.


rules/email/Email_generic_phishing.yar at master · Yara-Rules/rules · GitHub
https://github.com/Yara-Rules/rules/blob/master/email/Email_generic_phishing.yar
New tab
¡Bienvenido a Faceb...
lucidpress.com
Dell
Nueva pestaña
Nueva carpeta
Files
master
Go to file
.github
antidebug_antivm
capabilities
crypto
cve_rules
deprecated
email
eml
EMAIL_Cryptowall.yar
Email_PHP_Mailer.yar
Email_fake_it_maintenance_bull...
Email_generic_phishing.yar
Email_quota_limit_warning.yar
attachment.yar
email_Ukraine_BE_powerattack....
extortion_email.yar
image.yar
scam.yar
urls.yar
exploit_kits
maldocs
malware
mobile_malware
packers
utils
webshells
.gitmodules
.travis.yml
LICENSE
README.md
antidebug_antivm_index.yar
rules / email / Email_generic_phishing.yar
RandomRhythm add .yar extension to the following rules and add to indexes:
Code
Blame
42 lines (35 loc) · 1002 Bytes
Leandro D
File
Edit
View
Ln 2, Col 8
37 characters
100%
Windov
UTF-8

```
/*
    This Yara ruleset is under the GNU-GPLv2 license (http://www.gnu.org/licenses/gpl-2.0.html)
    and open to any user or organization, as long as you use it under this license.

*/

rule Email_Generic_Phishing : email
{
  meta:
              Author = "Tyler <@InfoSecTyler>"
              Description ="Generic rule to identify phishing emails"

  strings:
    $eml_1="From:"
    $eml_2="To:"
    $eml_3="Subject:"

    $greeting_1="Hello sir/madam" nocase
    $greeting_2="Attention" nocase
    $greeting_3="Dear user" nocase
    $greeting_4="Account holder" nocase

    $url_1="Click" nocase
    $url_2="Confirm" nocase
    $url_3="Verify" nocase
    $url_4="Here" nocase
    $url_5="Now" nocase
    $url_6="Change password" nocase

    $lie_1="Unauthorized" nocase
    $lie_2="Expired" nocase
    $lie_3="Deleted" nocase
    $lie_4="Suspended" nocase
    $lie_5="Revoked" nocase
    $lie_6="Unable" nocase

  condition:
    all of ($eml*) and
    any of ($greeting*) and
    any of ($url*) and
    any of ($lie*)
}
```

```
Leandro Delgado
Student ID:114416241
```

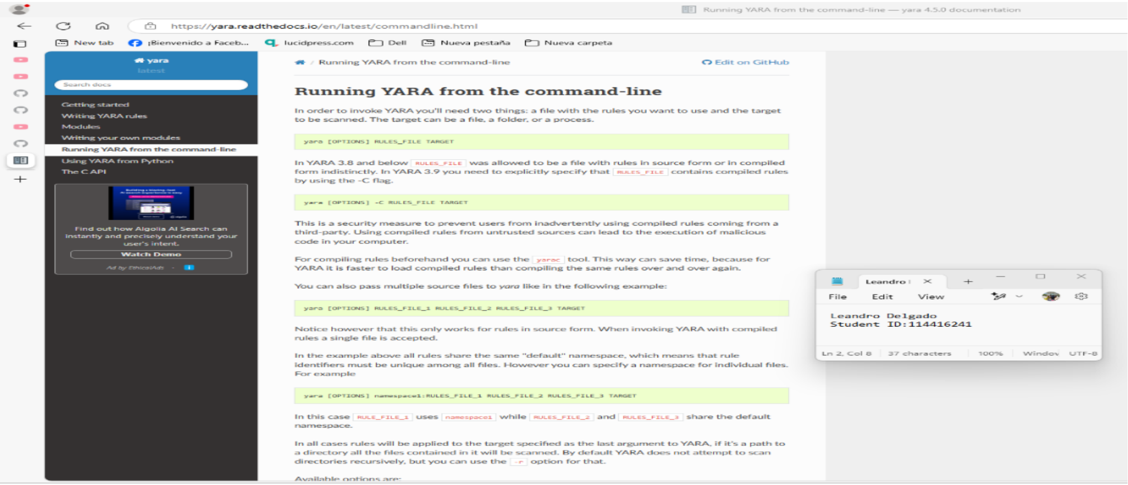
The YARA rule can look for weapons used in phishing email composition and ascertain if the email body bears any of the patterns. The keywords and phrases observed in phishing emails are matched with the keywords and phrases that are being searched for. When the rule begins, it tries to verify the file was scanned as an email from a few of the ordinary headers associated with emails: "From:", "To:", and "Subject:". If they do not show up, then the file will not be considered an email and won't be tagged as one. Generic openings for these types of emails, such as "Hello sir/madam", "Dear user", or "Attention", are being searched for as those commonly used in phishing attempts to impersonally address victims. Realistically, an organization should customize the email with the actual name of the recipient rather than using a general greeting.

Next on the radar are words suggesting an immediate action, like "Click", "Confirm", "Verify", and "Change password". Such words could entice their users into clicking rogue links or divulging credentials in a phishing attempt. Then follow words that instill insecurity, words such as "Unauthorized", "Suspended", "Revoked", and "Deleted". These dictionary words exert pressure on the recipient to act more quickly with an unnecessary sense of urgency when employed in the context of emails. For any instance to be deemed a phishing instance, a list of all these conditions must be satisfied: It is an email, has at least one suspicious greeting, has at least one urgent call to action, and has at least one word based on fear. If all above conditions are satisfied, then YARA will flag it as a possible phish. The policy would allow security professionals to efficiently assess possible phishing attempts and effectively react. By running this rule in YARA, users can get ahead of the malicious emails before any damage can be done.

Step 2. Work with Yara documentation to see in more details how to run the rules:

Running YARA from the command-line — yara 4.2.1 documentation

Generate your own sample content. It should contain words suitable to test the rule. Following recommendations, run the downloaded rule against your sample. You should emulate the content to run the rule.



Running YARA from the command-line — yara 4.5.0 documentation
https://yara.readthedocs.io/en/latest/commandline.html
New tab
¡Bienvenido a Faceb...
lucidpress.com
Dell
Nueva pestaña
Nueva carpeta
yara
latest
Search docs
Getting started
Writing YARA rules
Modules
Writing your own modules
Running YARA from the command-line
Using YARA from Python
The C API
Find out how Algolia AI Search can instantly and precisely understand your user's intent.
Watch Demo
Ad by EthicalAds
Running YARA from the command-line
Edit on GitHub

Running YARA from the command-line

In order to invoke YARA you'll need two things: a file with the rules you want to use and the target to be scanned. The target can be a file, a folder, or a process.

```
yara [OPTIONS] RULES_FILE TARGET
```

In YARA 3.8 and below `RULES_FILE` was allowed to be a file with rules in source form or in compiled form indistinctly. In YARA 3.9 you need to explicitly specify that `RULES_FILE` contains compiled rules by using the -C flag.

```
yara [OPTIONS] -C RULES_FILE TARGET
```

This is a security measure to prevent users from inadvertently using compiled rules coming from a third-party. Using compiled rules from untrusted sources can lead to the execution of malicious code in your computer.

For compiling rules beforehand you can use the `yarac` tool. This way can save time, because for YARA it is faster to load compiled rules than compiling the same rules over and over again.

You can also pass multiple source files to *yara* like in the following example:

```
yara [OPTIONS] RULES_FILE_1 RULES_FILE_2 RULES_FILE_3 TARGET
```

Notice however that this only works for rules in source form. When invoking YARA with compiled rules a single file is accepted.

In the example above all rules share the same "default" namespace, which means that rule identifiers must be unique among all files. However you can specify a namespace for individual files. For example

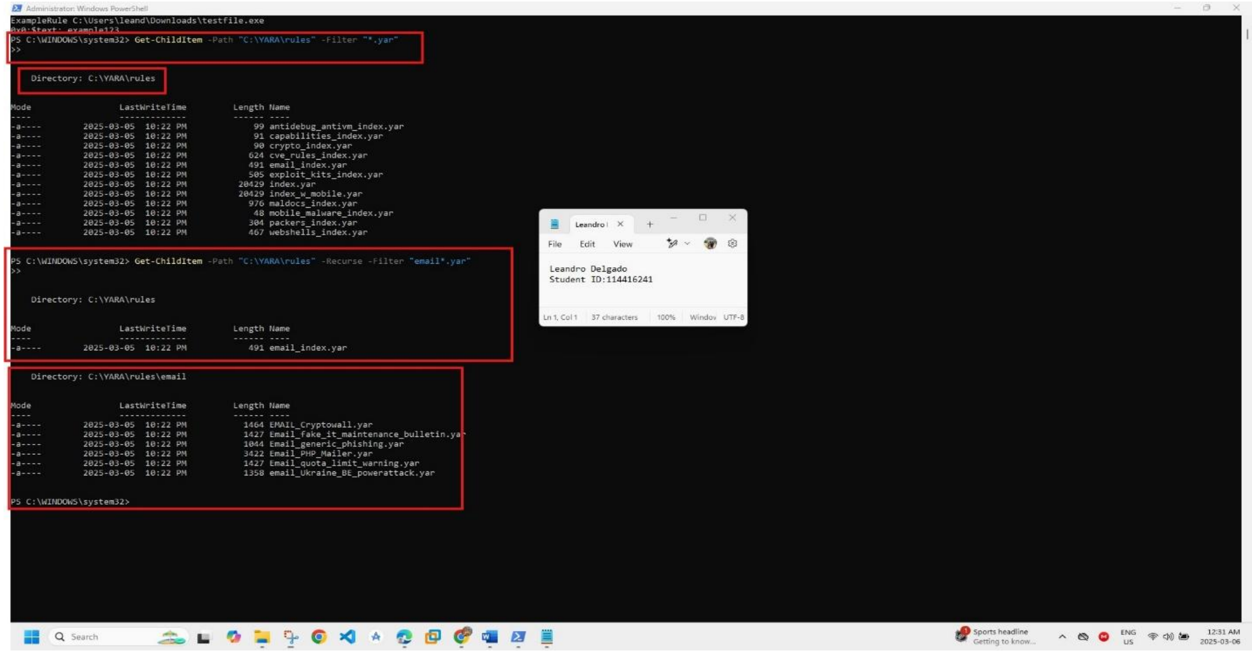
```
yara [OPTIONS] namespace1:RULES_FILE_1 RULES_FILE_2 RULES_FILE_3 TARGET
```

In this case `RULE_FILE_1` uses `namespace1` while `RULES_FILE_2` and `RULES_FILE_3` share the default namespace.

In all cases rules will be applied to the target specified as the last argument to YARA, if it's a path to a directory all the files contained in it will be scanned. By default YARA does not attempt to scan directories recursively, but you can use the `-r` option for that.

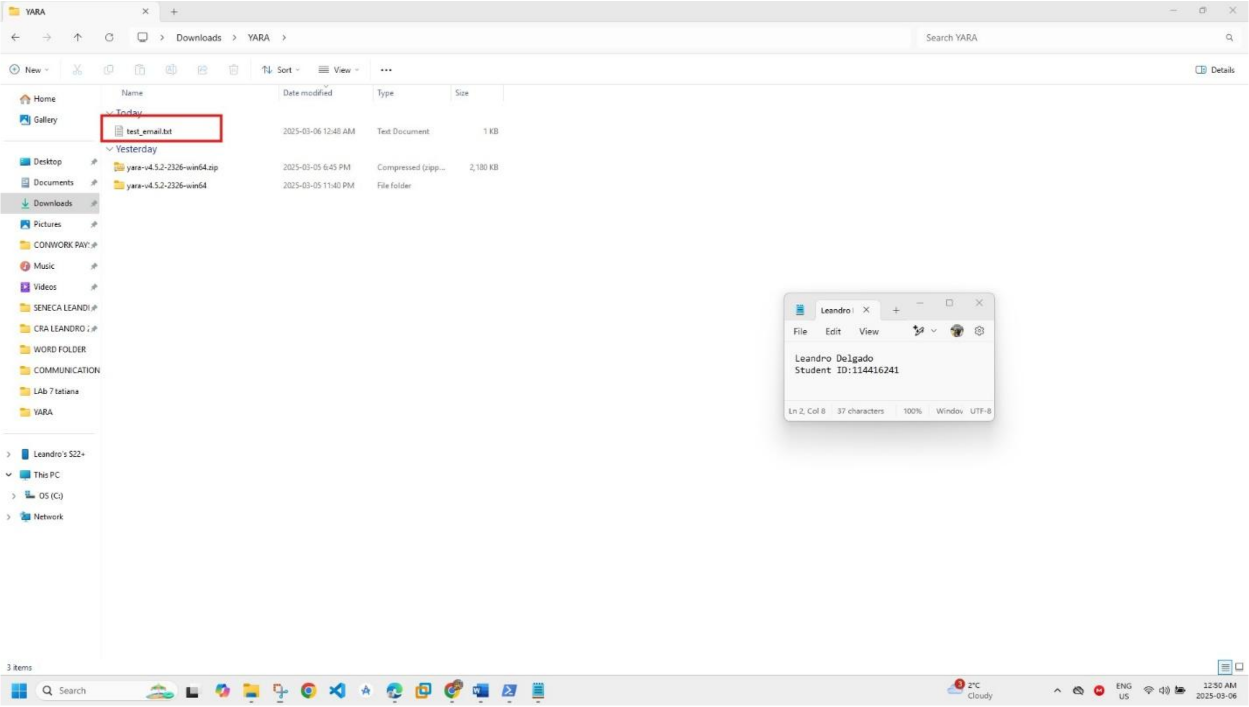
Available options are:

```
Leandro Delgado
Student ID:114416241
```



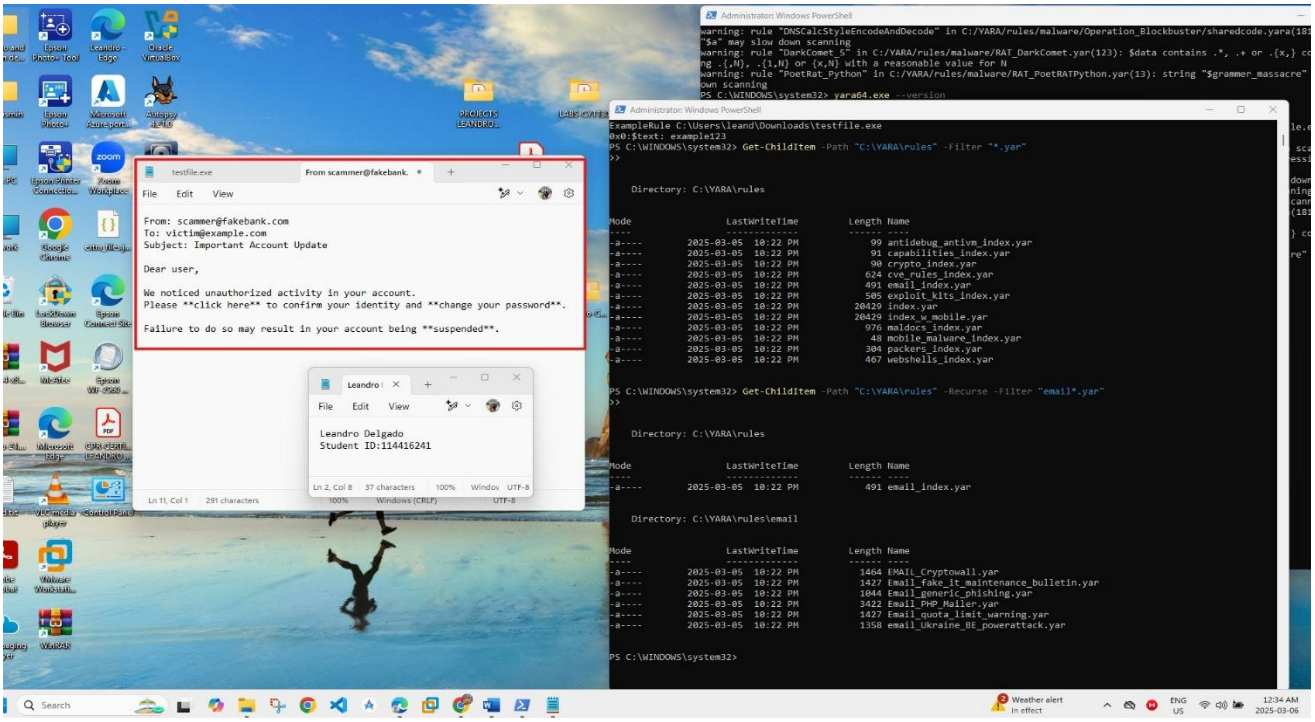
```
ExampleRule C:\Users\leand\Downloads\testfile.exe
0x0:$text: example123
PS C:\WINDOWS\system32> Get-ChildItem -Path "C:\YARA\rules" -Filter "*.yar"
>>

    Directory: C:\YARA\rules

Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----        2025-03-05  10:22 PM             99 antidebug_antivm_index.yar
-a----        2025-03-05  10:22 PM             91 capabilities_index.yar
-a----        2025-03-05  10:22 PM             90 crypto_index.yar
-a----        2025-03-05  10:22 PM            624 cve_rules_index.yar
-a----        2025-03-05  10:22 PM            491 email_index.yar
-a----        2025-03-05  10:22 PM            505 exploit_kits_index.yar
-a----        2025-03-05  10:22 PM          20429 index.yar
-a----        2025-03-05  10:22 PM          20429 index_w_mobile.yar
-a----        2025-03-05  10:22 PM            976 maldocs_index.yar
-a----        2025-03-05  10:22 PM             48 mobile_malware_index.yar
-a----        2025-03-05  10:22 PM            304 packers_index.yar
-a----        2025-03-05  10:22 PM            467 webshells_index.yar

PS C:\WINDOWS\system32> Get-ChildItem -Path "C:\YARA\rules" -Recurse -Filter "email*.yar"
>>


    Directory: C:\YARA\rules


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----        2025-03-05  10:22 PM            491 email_index.yar

    Directory: C:\YARA\rules\email


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----        2025-03-05  10:22 PM           1464 EMAIL_Cryptowall.yar
-a----        2025-03-05  10:22 PM           1427 Email_fake_it_maintenance_bulletin.yar
-a----        2025-03-05  10:22 PM           1044 Email_generic_phishing.yar
-a----        2025-03-05  10:22 PM           3422 Email_PHP_Mailer.yar
-a----        2025-03-05  10:22 PM           1427 Email_quota_limit_warning.yar
-a----        2025-03-05  10:22 PM           1358 email_Ukraine_BE_powerattack.yar


PS C:\WINDOWS\system32>
```

```
Leandro Delgado
Student ID:114416241
```



Name	Date modified	Type	Size
Today			
test_email.txt	2025-03-06 12:48 AM	Text Document	1 KB
Yesterday			
yara-v4.5.2-2326-win64.zip	2025-03-05 6:45 PM	Compressed (zipp...	2,180 KB
yara-v4.5.2-2326-win64	2025-03-05 11:40 PM	File folder	

```
Leandro Delgado
Student ID:114416241
```

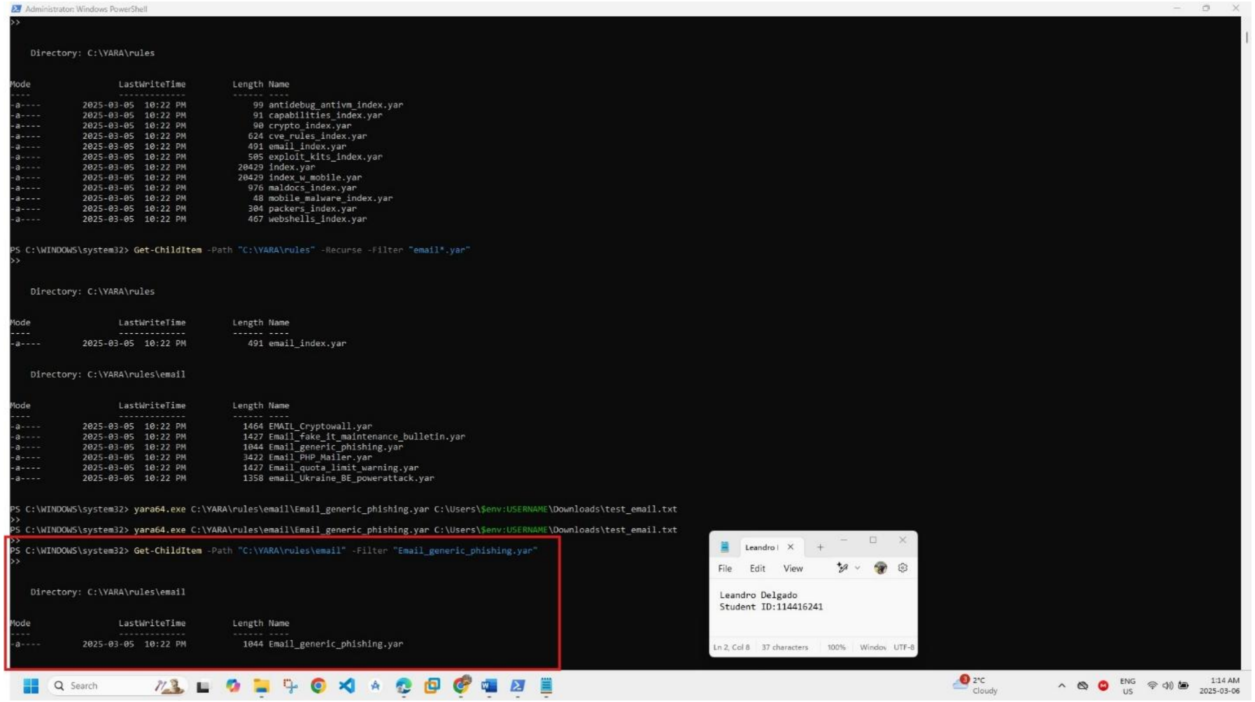


```
From: scammer@fakebank.com
To: victim@example.com
Subject: Important Account Update

Dear user,

We noticed unauthorized activity in your account.
Please **click here** to confirm your identity and **change your password**.

Failure to do so may result in your account being **suspended**.
```

```
Leandro Delgado
Student ID:114416241
```

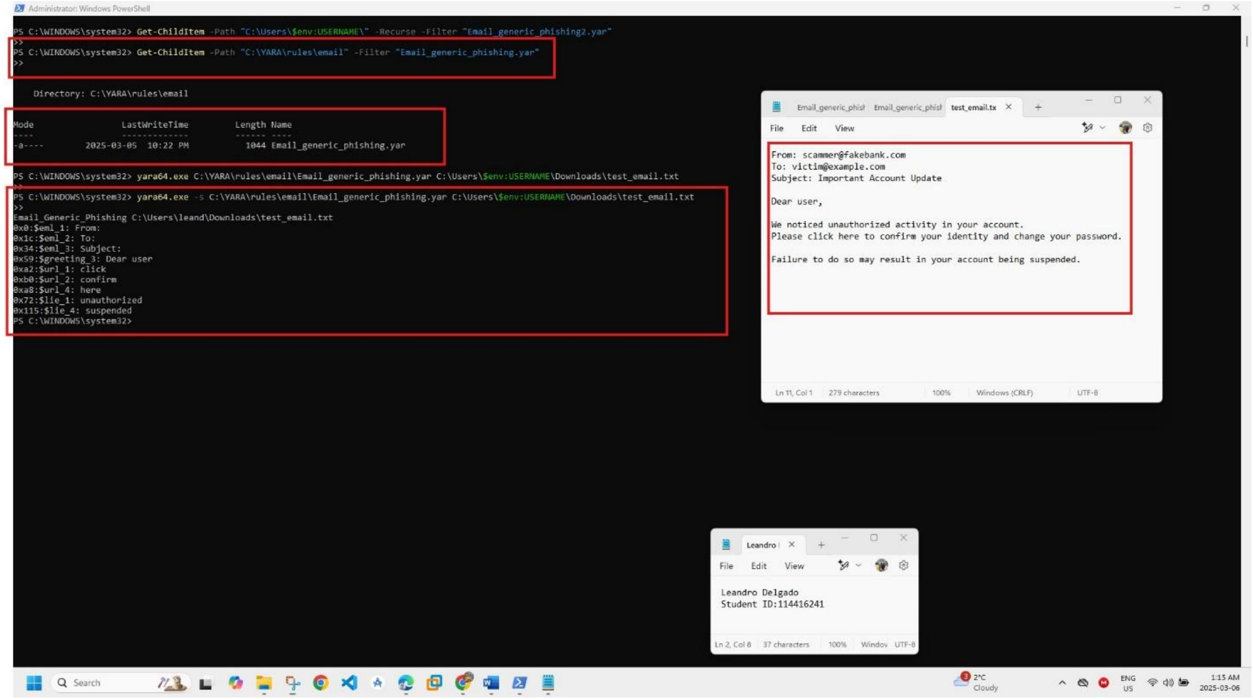
```
warning: rule "DNSCalcStyleEncodeAndDecode" in C:/YARA/rules/malware/Operation_Blockbuster/sharedcode.yara(181
"$a" may slow down scanning
warning: rule "DarkComet_5" in C:/YARA/rules/malware/RAT_DarkComet.yar(123): $data contains .*, .+ or .{x,} co
ng .{,N}, .{1,N} or {x,N} with a reasonable value for N
warning: rule "PoetRat_Python" in C:/YARA/rules/malware/RAT_PoetRATPython.yar(13): string "$grammer_massacre"
own scanning
PS C:\WINDOWS\system32> yara64.exe --version
```

```
ExampleRule C:\Users\leand\Downloads\testfile.exe
0x0:$text: example123
PS C:\WINDOWS\system32> Get-ChildItem -Path "C:\YARA\rules" -Filter "*.yar"
>>


    Directory: C:\YARA\rules


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----        2025-03-05  10:22 PM             99 antidebug_antivm_index.yar
-a----        2025-03-05  10:22 PM             91 capabilities_index.yar
-a----        2025-03-05  10:22 PM             90 crypto_index.yar
-a----        2025-03-05  10:22 PM            624 cve_rules_index.yar
-a----        2025-03-05  10:22 PM            491 email_index.yar
-a----        2025-03-05  10:22 PM            505 exploit_kits_index.yar
-a----        2025-03-05  10:22 PM          20429 index.yar
-a----        2025-03-05  10:22 PM          20429 index_w_mobile.yar
-a----        2025-03-05  10:22 PM            976 maldocs_index.yar
-a----        2025-03-05  10:22 PM             48 mobile_malware_index.yar
-a----        2025-03-05  10:22 PM            304 packers_index.yar
-a----        2025-03-05  10:22 PM            467 webshells_index.yar


PS C:\WINDOWS\system32> Get-ChildItem -Path "C:\YARA\rules" -Recurse -Filter "email*.yar"
>>


    Directory: C:\YARA\rules


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----        2025-03-05  10:22 PM            491 email_index.yar


    Directory: C:\YARA\rules\email


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----        2025-03-05  10:22 PM           1464 EMAIL_Cryptowall.yar
-a----        2025-03-05  10:22 PM           1427 Email_fake_it_maintenance_bulletin.yar
-a----        2025-03-05  10:22 PM           1044 Email_generic_phishing.yar
-a----        2025-03-05  10:22 PM           3422 Email_PHP_Mailer.yar
-a----        2025-03-05  10:22 PM           1427 Email_quota_limit_warning.yar
-a----        2025-03-05  10:22 PM           1358 email_Ukraine_BE_powerattack.yar


PS C:\WINDOWS\system32>
```



```
>>


    Directory: C:\YARA\rules


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----        2025-03-05  10:22 PM             99 antidebug_antivm_index.yar
-a----        2025-03-05  10:22 PM             91 capabilities_index.yar
-a----        2025-03-05  10:22 PM             90 crypto_index.yar
-a----        2025-03-05  10:22 PM            624 cve_rules_index.yar
-a----        2025-03-05  10:22 PM            491 email_index.yar
-a----        2025-03-05  10:22 PM            505 exploit_kits_index.yar
-a----        2025-03-05  10:22 PM          20429 index.yar
-a----        2025-03-05  10:22 PM          20429 index_w_mobile.yar
-a----        2025-03-05  10:22 PM            976 maldocs_index.yar
-a----        2025-03-05  10:22 PM             48 mobile_malware_index.yar
-a----        2025-03-05  10:22 PM            304 packers_index.yar
-a----        2025-03-05  10:22 PM            467 webshells_index.yar


PS C:\WINDOWS\system32> Get-ChildItem -Path "C:\YARA\rules" -Recurse -Filter "email*.yar"
>>


    Directory: C:\YARA\rules


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----        2025-03-05  10:22 PM            491 email_index.yar


    Directory: C:\YARA\rules\email


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----        2025-03-05  10:22 PM           1464 EMAIL_Cryptowall.yar
-a----        2025-03-05  10:22 PM           1427 Email_fake_it_maintenance_bulletin.yar
-a----        2025-03-05  10:22 PM           1044 Email_generic_phishing.yar
-a----        2025-03-05  10:22 PM           3422 Email_PHP_Mailer.yar
-a----        2025-03-05  10:22 PM           1427 Email_quota_limit_warning.yar
-a----        2025-03-05  10:22 PM           1358 email_Ukraine_BE_powerattack.yar


PS C:\WINDOWS\system32> yara64.exe C:\YARA\rules\email\Email_generic_phishing.yar C:\Users\$env:USERNAME\Downloads\test_email.txt
>>
PS C:\WINDOWS\system32> yara64.exe C:\YARA\rules\email\Email_generic_phishing.yar C:\Users\$env:USERNAME\Downloads\test_email.txt
>>
PS C:\WINDOWS\system32> Get-ChildItem -Path "C:\YARA\rules\email" -Filter "Email_generic_phishing.yar"
>>


    Directory: C:\YARA\rules\email


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----        2025-03-05  10:22 PM           1044 Email_generic_phishing.yar
```

```
Leandro Delgado
Student ID:114416241
```



```
PS C:\WINDOWS\system32> Get-ChildItem -Path "C:\Users\$env:USERNAME\" -Recurse -Filter "Email_generic_phishing2.yar"
>>
PS C:\WINDOWS\system32> Get-ChildItem -Path "C:\YARA\rules\email" -Filter "Email_generic_phishing.yar"
>>


    Directory: C:\YARA\rules\email


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----        2025-03-05  10:22 PM           1044 Email_generic_phishing.yar


PS C:\WINDOWS\system32> yara64.exe C:\YARA\rules\email\Email_generic_phishing.yar C:\Users\$env:USERNAME\Downloads\test_email.txt
>>
PS C:\WINDOWS\system32> yara64.exe -s C:\YARA\rules\email\Email_generic_phishing.yar C:\Users\$env:USERNAME\Downloads\test_email.txt
>>
Email_Generic_Phishing C:\Users\leand\Downloads\test_email.txt
0x0:$eml_1: From:
0x1c:$eml_2: To:
0x34:$eml_3: Subject:
0x59:$greeting_3: Dear user
0xa2:$url_1: click
0xb0:$url_2: confirm
0xa8:$url_4: here
0x72:$lie_1: unauthorized
0x115:$lie_4: suspended
PS C:\WINDOWS\system32>
```

```
From: scammer@fakebank.com
To: victim@example.com
Subject: Important Account Update

Dear user,

We noticed unauthorized activity in your account.
Please click here to confirm your identity and change your password.

Failure to do so may result in your account being suspended.
```

```
Leandro Delgado
Student ID:114416241
```

Various key ingredients of how to use YARA for phishing email detection were involved in the process. YARA installation onto the system was successfully done in the C:\YARA directory and was later confirmed by command-line invocation. Next step was to obtain a set of YARA rules by cloning a GitHub repository from where various predefined rules for detecting malware, phishing, and other threats could be obtained. After setting up the rules, the specific rule file for phishing emails, Email_Generic_Phishing.yar, was identified within the C:\YARA\rules\email\ directory. This rule was examined and found to have logic to detect phishing indicators such as standard email templates (From: To:, Subject:), suspicious greetings (Dear User, Attention), urgent call-to-action words (Click here, Confirm, Verify), and fear-inducing words (Unauthorized, Suspended, Revoked).

The Email_Generic_Phishing rule was tested against an actual phishing email that was created and saved as test_email.txt. The email contained classic phishing language asking the recipient to verify his account because unauthorized activity was suspected. YARA returned no results initially, prompting the need for changes. Fine-tuning was done so the email was within the rule's filtering conditions; yara64.exe C:\YARA\rules\email\Email_generic_phishing.yar C:\Users\$env: USERNAME\Downloads\test_email.txt was re-executed. This time, YARA found a multitude of phishing indicators in the email: suspicious greetings, links, and urgent warning.

Summary

This process showcased the function of YARA in attempting to detect phishing by scanning emails for predefined malicious patterns. Now that setup is complete, further improvements to the rule could include incorporating more phishing characteristics or testing with other phishing samples. The knowledge obtained during this experiment could then be extended by investigating other available YARA rules like those used for malware detection or creating their own rules for further security analysis.