# Configuration Manual

Practicum 2
MSc in Cyber Security

Mabika Mabika
Student ID: X21132135

School of Computing
National College of Ireland

Supervisor: Vikas Sahni

**National College of Ireland**

**MSc Project Submission Sheet**

**School of Computing**

| | | | |
|---|---|---|---|
| **Student Name:** | Mabika Mabika | | |
| **Student ID:** | X21132135 | | |
| **Programme:** | MSc Cyber Security | **Year:** | 2024 |
| **Module:** | Practicum 2 | | |
| **Lecturer:** | Vikas Sahni | | |
| **Submission Due Date:** | 03/01/2025 | | |
| **Project Title:** | Supervised Learning on Active directory with overcoming cybersecurity challenges | | |
| **Word Count:** | 878 | **Page Count:** | 14 |

I hereby certify that the information contained in this (my submission) is information pertaining to research I conducted for this project. All information other than my own contribution will be fully referenced and listed in the relevant bibliography section at the rear of the project.

ALL internet material must be referenced in the bibliography section. Students are required to use the Referencing Standard specified in the report template. To use other author's written or electronic work is illegal (plagiarism) and may result in disciplinary action.

**Signature:** Mabika Mabika

**Date:** 28/12/2024

**PLEASE READ THE FOLLOWING INSTRUCTIONS AND CHECKLIST**

| | |
|---|---|
| Attach a completed copy of this sheet to each project (including multiple copies) | □ |
| **Attach a Moodle submission receipt of the online project submission,** to each project (including multiple copies). | □ |
| **You must ensure that you retain a HARD COPY of the project**, both for your own reference and in case a project is lost or mislaid. It is not sufficient to keep a copy on computer. | □ |

Assignments that are submitted to the Programme Coordinator Office must be placed into the assignment box located outside the office.

| | |
|---|---|
| **Office Use Only** | |
| Signature: | |
| Date: | |
| Penalty Applied (if applicable): | |

# Configuration Manual

Mabika Mabika

X21132135

## 1. Introduction

The configuration manual provides a walk-through of the research study setup of Supervised Learning on Active directory with overcoming cybersecurity challenges. The research study had a mix of already configured software & tools and software & tools which were configured during the research period. A brief overview of each step will be provided below outlining important steps.

## 2. System Requirements

### 2.1 Host System Specification

- Device name: LAPTOP-IGQ51UO2
- Processor: Intel(R) Core (TM) i3-1005G1 CPU @ 1.20GHz 1.19 GHz
- Installed RAM: 8.00 GB
- Product ID: 00325-81930-70792-AAOEM
- System type 64-bit operating system, x64-based processor

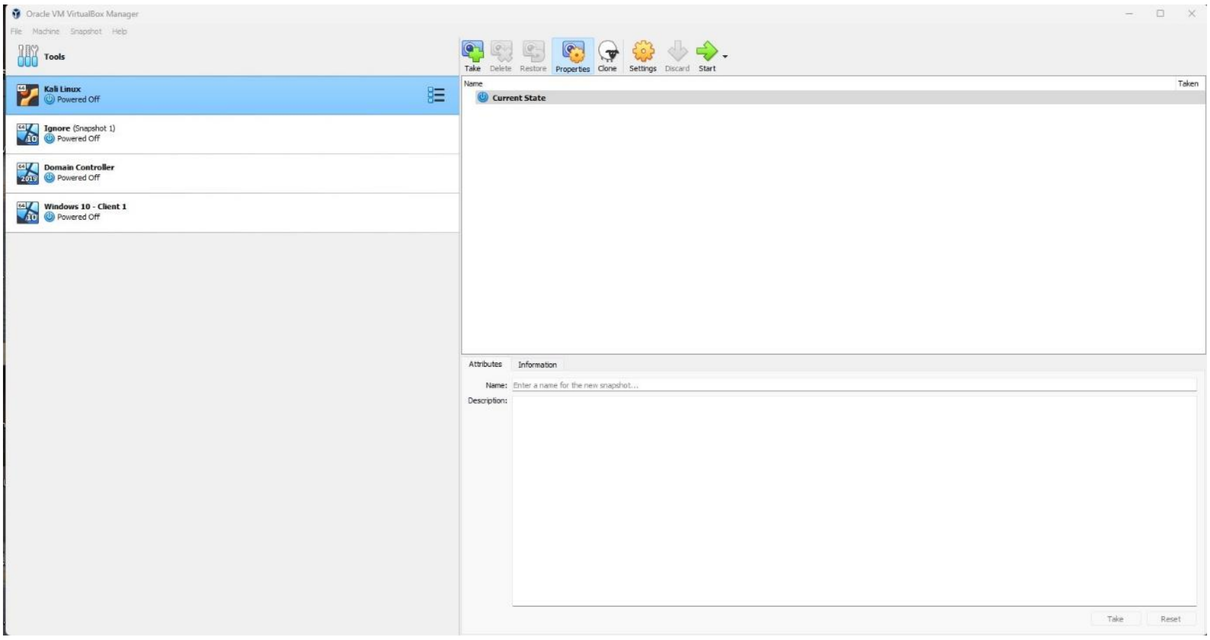
### 2.2 Virtual Machines - VirtualBox 7.0

**Attacker**

- Operating System: Kali-Linux - 6.11.2 (Ubuntu - 64 bit)
- Processors: 1
- Storage: 128GB
- RAM: 2GB

**Victim - Domain Controller**

- Operating System: Windows Server 2019 (64 bit)
- Processors: 2
- Storage: 50GB
- RAM: 2GB



## 3. Prerequisites

- Understanding of Cybersecurity principles
- Responsible use of any tests
- Necessary permission to conduct tests
- Controlled and authorized environment
- Datasets and articles used in the research as outline in references

## 4. Software Specifications

A brief overview of the software used are outlined below:

**4.1 Hydra v9.5** – it is a preinstalled software on Kali Linux used as a password cracking tool. Hydra supports many protocols which include SSH, HTTP, LPAD and SMP. When using Hydra a user can perform attacks such as brute force enabling them to be able to attempt usernames and passwords.

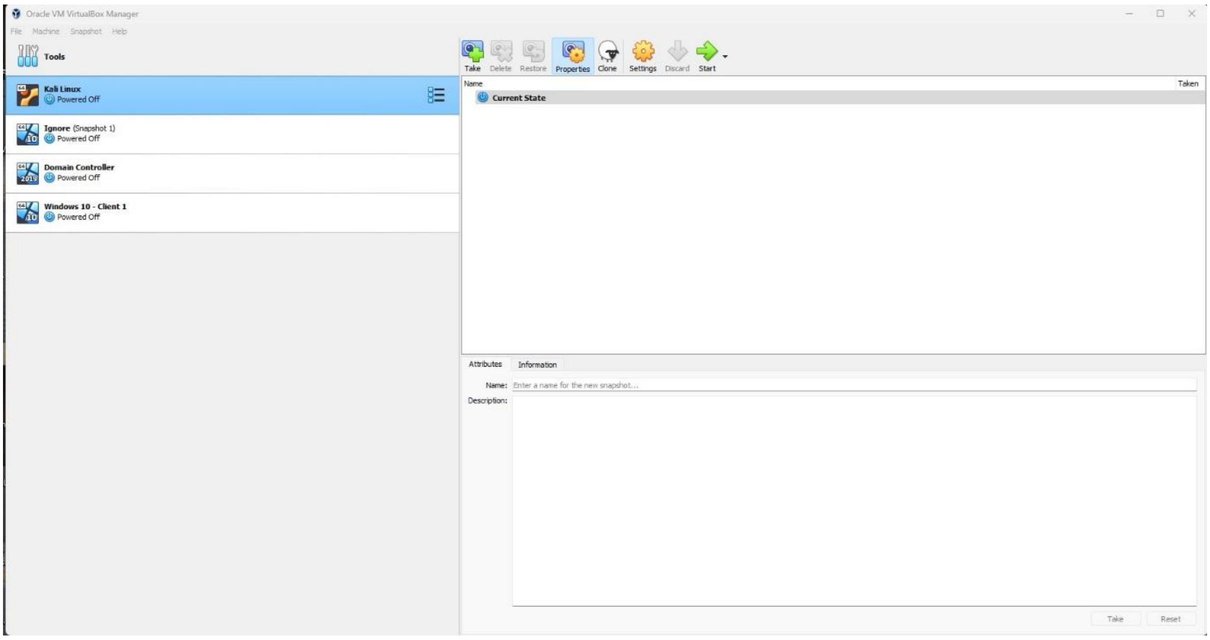
**4.2 Sysmon v15.15** – it is a Windows monitoring tool, which is used to track any malicious behaviour or activity on the system.

**4.3 VirtualBox 7.0**

## 5. Software Configuration

### 5.1 Configuring Virtual Machine

Oracle VirtualBox 7.0 were already installed beforehand. Kali Linux 6.11.2 and Windows Server 2019 was also already installed in Virtual Box.

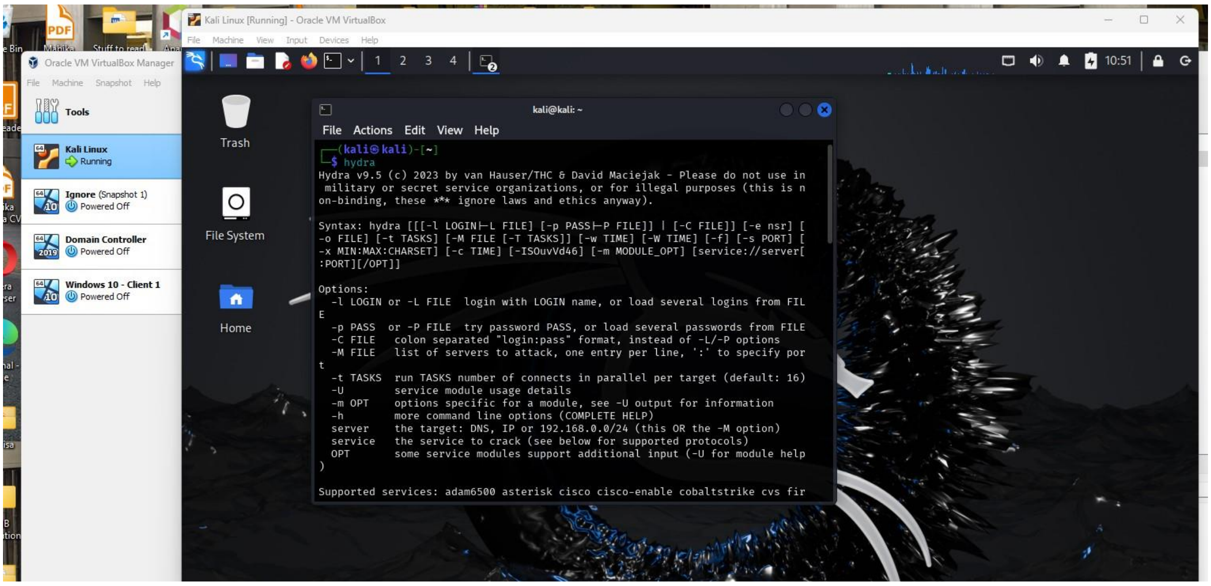


### 5.2 Hydra v9.5

The instructions below will illustrate how to install Hydra:

Ensure Hydra is installed on your Kali Linux system

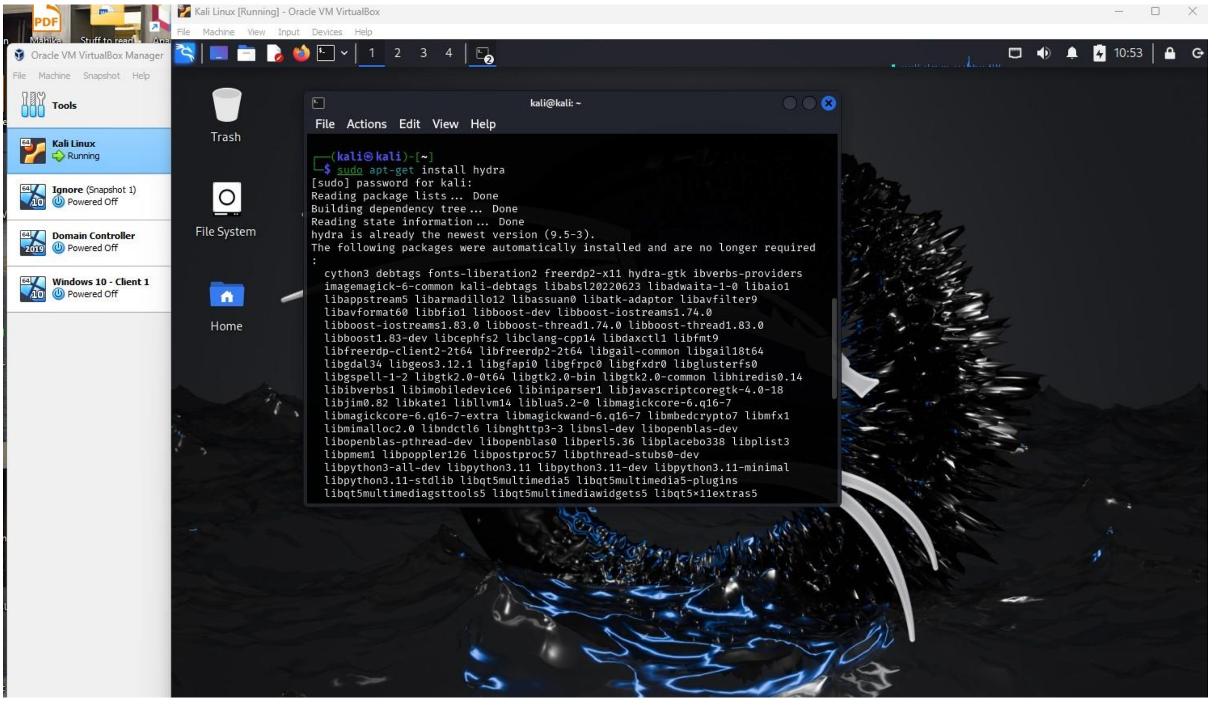
*hydra –version*



```
┌──(kali㉿kali)-[~]
└─$ hydra
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in
 military or secret service organizations, or for illegal purposes (this is n
on-binding, these *** ignore laws and ethics anyway).

Syntax: hydra [[[-l LOGIN|-L FILE] [-p PASS|-P FILE]] | [-C FILE]] [-e nsr] [
-o FILE] [-t TASKS] [-M FILE [-T TASKS]] [-w TIME] [-W TIME] [-f] [-s PORT] [
-x MIN:MAX:CHARSET] [-c TIME] [-ISOuvVd46] [-m MODULE_OPT] [service://server[
:PORT][/OPT]]

Options:
  -l LOGIN or -L FILE  login with LOGIN name, or load several logins from FIL
E
  -p PASS  or -P FILE  try password PASS, or load several passwords from FILE
  -C FILE   colon separated "login:pass" format, instead of -L/-P options
  -M FILE   list of servers to attack, one entry per line, ':' to specify por
t
  -t TASKS  run TASKS number of connects in parallel per target (default: 16)
  -U        service module usage details
  -m OPT    options specific for a module, see -U output for information
  -h        more command line options (COMPLETE HELP)
  server    the target: DNS, IP or 192.168.0.0/24 (this OR the -M option)
  service   the service to crack (see below for supported protocols)
  OPT       some service modules support additional input (-U for module help
)

Supported services: adam6500 asterisk cisco cisco-enable cobaltstrike cvs fir
```

If Hydra is not installed use the following command to install Hydra:

*sudo apt-get install hydra*



```
┌──(kali㉿kali)-[~]
└─$ sudo apt-get install hydra
[sudo] password for kali:
Reading package lists ... Done
Building dependency tree ... Done
Reading state information ... Done
hydra is already the newest version (9.5-3).
The following packages were automatically installed and are no longer required
:
  cython3 debtags fonts-liberation2 freerdp2-x11 hydra-gtk ibverbs-providers
  imagemagick-6-common kali-debtags libabsl20220623 libadwaita-1-0 libaio1
  libappstream5 libarmadillo12 libassuan0 libatk-adaptor libavfilter9
  libavformat60 libbfio1 libboost-dev libboost-iostreams1.74.0
  libboost-iostreams1.83.0 libboost-thread1.74.0 libboost-thread1.83.0
  libboost1.83-dev libcephfs2 libclang-cpp14 libdaxctl1 libfmt9
  libfreerdp-client2-2t64 libfreerdp2-2t64 libgail-common libgail18t64
  libgdal34 libgeos3.12.1 libgfapi0 libgfrpc0 libgfxdr0 libglusterfs0
  libgspell-1-2 libgtk2.0-0t64 libgtk2.0-bin libgtk2.0-common libhiredis0.14
  libibverbs1 libimobiledevice6 libiniparser1 libjavascriptcoregtk-4.0-18
  libjim0.82 libkate1 libllvm14 liblua5.2-0 libmagickcore-6.q16-7
  libmagickcore-6.q16-7-extra libmagickwand-6.q16-7 libmbedcrypto7 libmfx1
  libmimalloc2.0 libndctl6 libnghttp3-3 libnsl-dev libopenblas-dev
  libopenblas-pthread-dev libopenblas0 libperl5.36 libplacebo338 libplist3
  libpmem1 libpoppler126 libpostproc57 libpthread-stubs0-dev
  libpython3-all-dev libpython3.11 libpython3.11-dev libpython3.11-minimal
  libpython3.11-stdlib libqt5multimedia5 libqt5multimedia5-plugins
  libqt5multimediagsttools5 libqt5multimediawidgets5 libqt5×11extras5
```

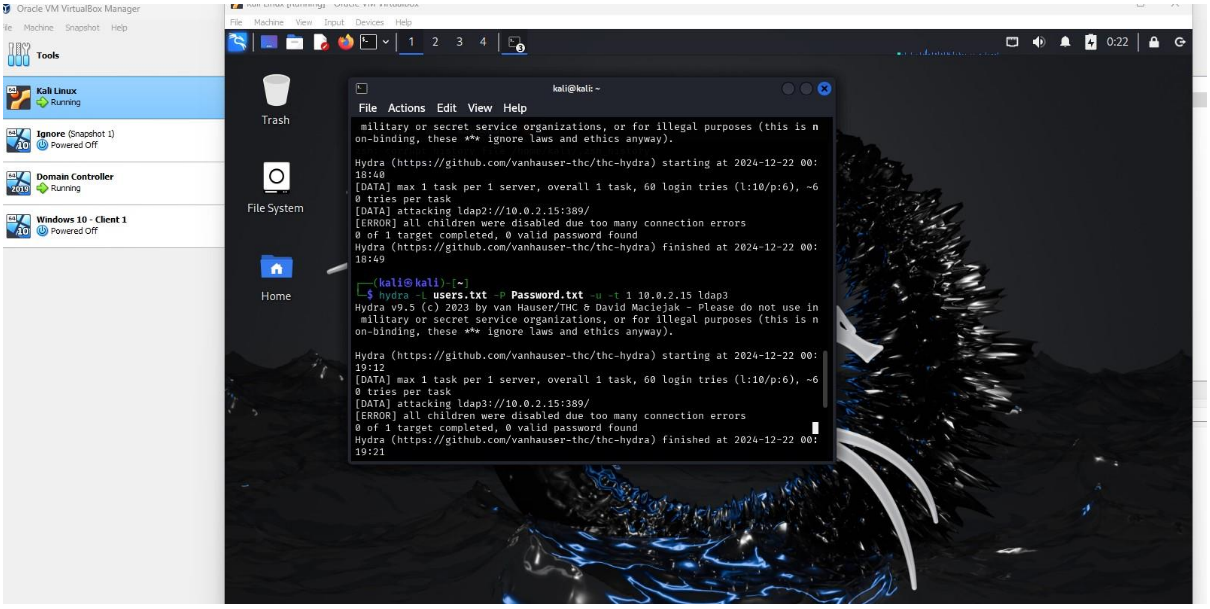
After completing the installation of Hydra, one has to consider the following important conditions and considerations before going on to do any attacks:

- Ensuring that the activity is legal and ethical.
- Attack systems that you have explicit permission to test for example your own home lab.
- Isolate testing environment from the productive environment so that if any mistakes happen, they do not breach or cause any consequences.

## 6. Conducting Brute-Force Attack

In our research we aimed to crack password for a LDAP, the following command was used:

*hydra -l users.txt -p Password.txt -u -t 1 10.0.2.15 ldap3*



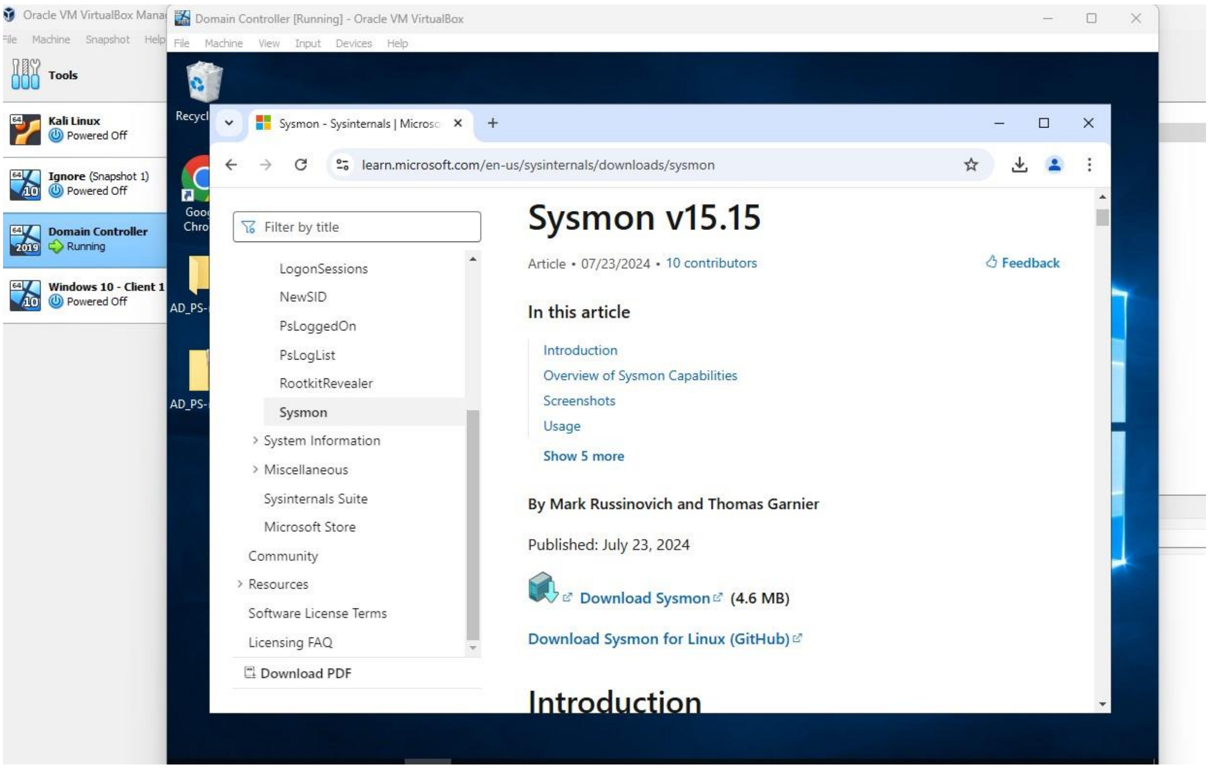
```
 military or secret service organizations, or for illegal purposes (this is n
on-binding, these *** ignore laws and ethics anyway).
zsh: corrupt history file /home/kali/.zsh_history
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-12-22 00:
18:40
[DATA] max 1 task per 1 server, overall 1 task, 60 login tries (l:10/p:6), ~6
0 tries per task
[DATA] attacking ldap2://10.0.2.15:389/
[ERROR] all children were disabled due too many connection errors
0 of 1 target completed, 0 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-12-22 00:
18:49

┌──(kali㉿kali)-[~]
└─$ hydra -L users.txt -P Password.txt -u -t 1 10.0.2.15 ldap3
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in
 military or secret service organizations, or for illegal purposes (this is n
on-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-12-22 00:
19:12
[DATA] max 1 task per 1 server, overall 1 task, 60 login tries (l:10/p:6), ~6
0 tries per task
[DATA] attacking ldap3://10.0.2.15:389/
[ERROR] all children were disabled due too many connection errors
0 of 1 target completed, 0 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-12-22 00:
19:21
```

## 7. Sysmon v15.15

The instructions below will illustrate how to install Sysmon v15.15

The attached link is available to download Sysmon v15.15 => https://learn.microsoft.com/en-us/sysinternals/downloads/sysmon

Select Download Sysmon (4.6MB) as your installation file



Sysmon v15.15

Article • 07/23/2024 • 10 contributors

Feedback

In this article

- Introduction
- Overview of Sysmon Capabilities
- Screenshots
- Usage

Show 5 more

By Mark Russinovich and Thomas Garnier

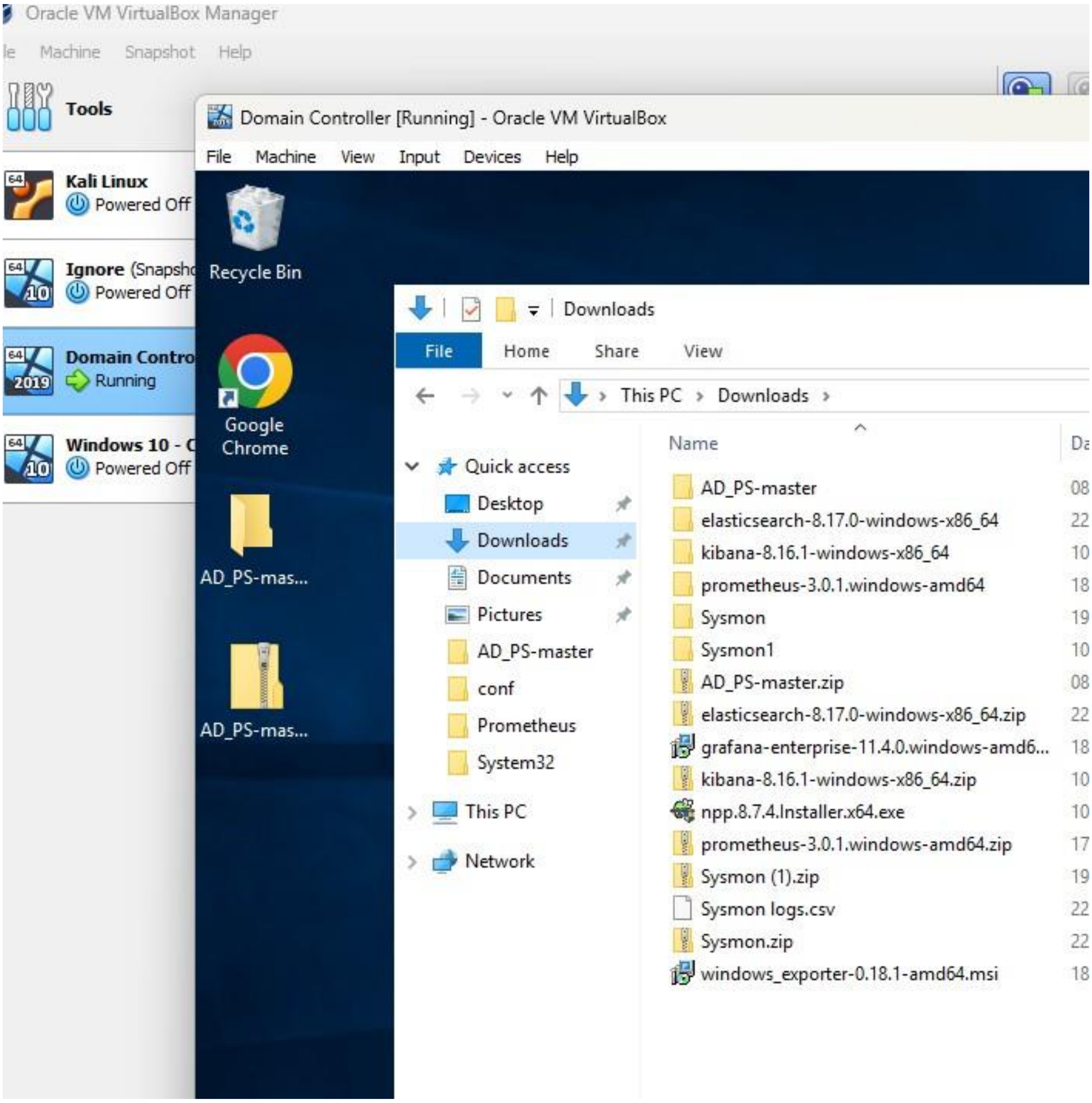
Published: July 23, 2024

Download Sysmon (4.6 MB)

Download Sysmon for Linux (GitHub)

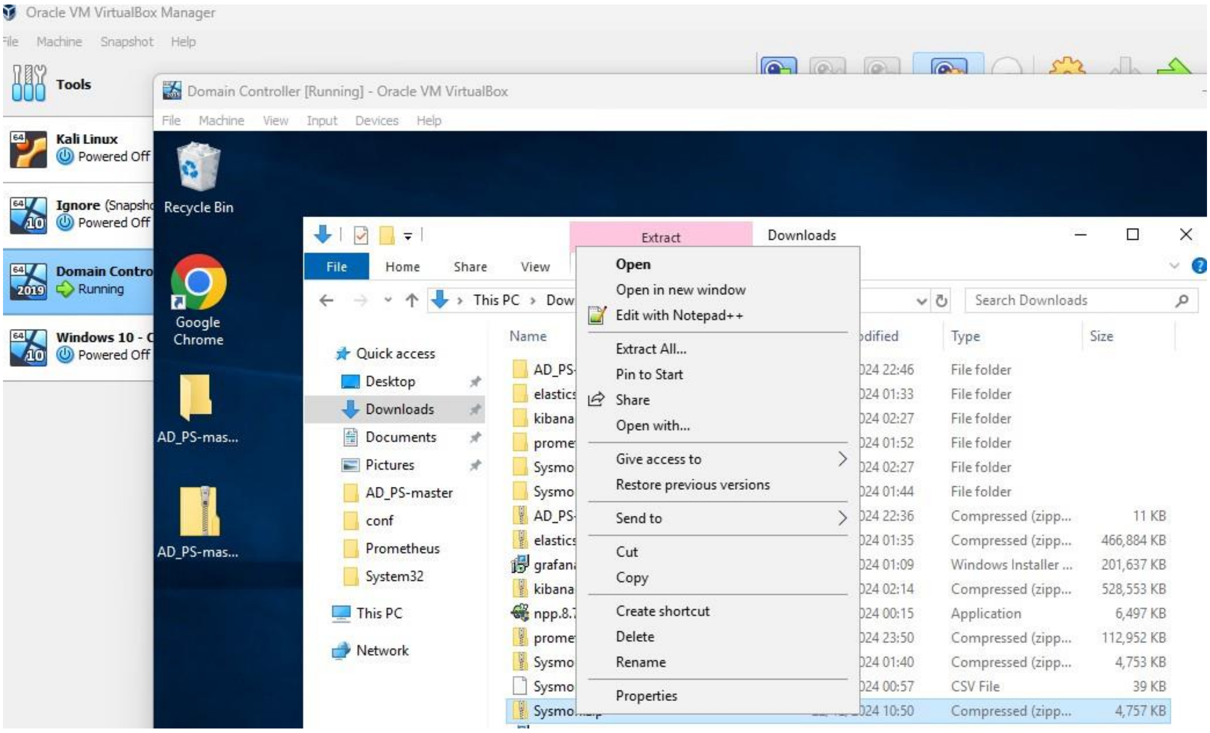
Introduction

After downloading the file, you get a zip file named Sysmon.zip.

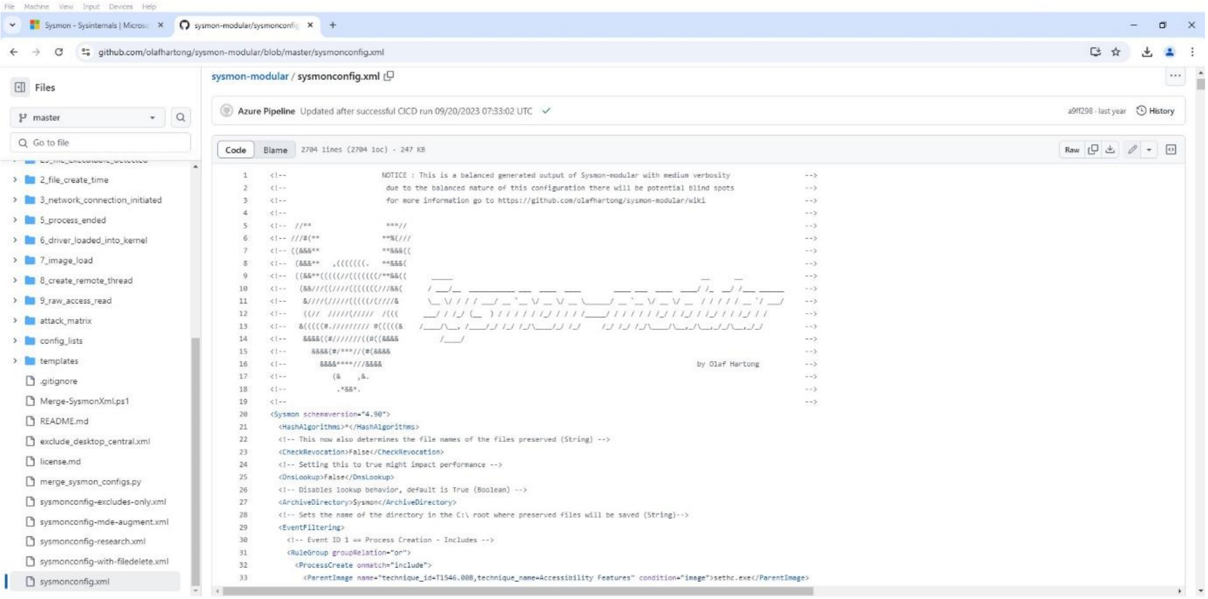


| Name | Da |
|---|---|
| AD_PS-master | 08 |
| elasticsearch-8.17.0-windows-x86_64 | 22 |
| kibana-8.16.1-windows-x86_64 | 10 |
| prometheus-3.0.1.windows-amd64 | 18 |
| Sysmon | 19 |
| Sysmon1 | 10 |
| AD_PS-master.zip | 08 |
| elasticsearch-8.17.0-windows-x86_64.zip | 22 |
| grafana-enterprise-11.4.0.windows-amd6... | 18 |
| kibana-8.16.1-windows-x86_64.zip | 10 |
| npp.8.7.4.Installer.x64.exe | 10 |
| prometheus-3.0.1.windows-amd64.zip | 17 |
| Sysmon (1).zip | 19 |
| Sysmon logs.csv | 22 |
| Sysmon.zip | 22 |
| windows_exporter-0.18.1-amd64.msi | 18 |

Next you then extract the zip file

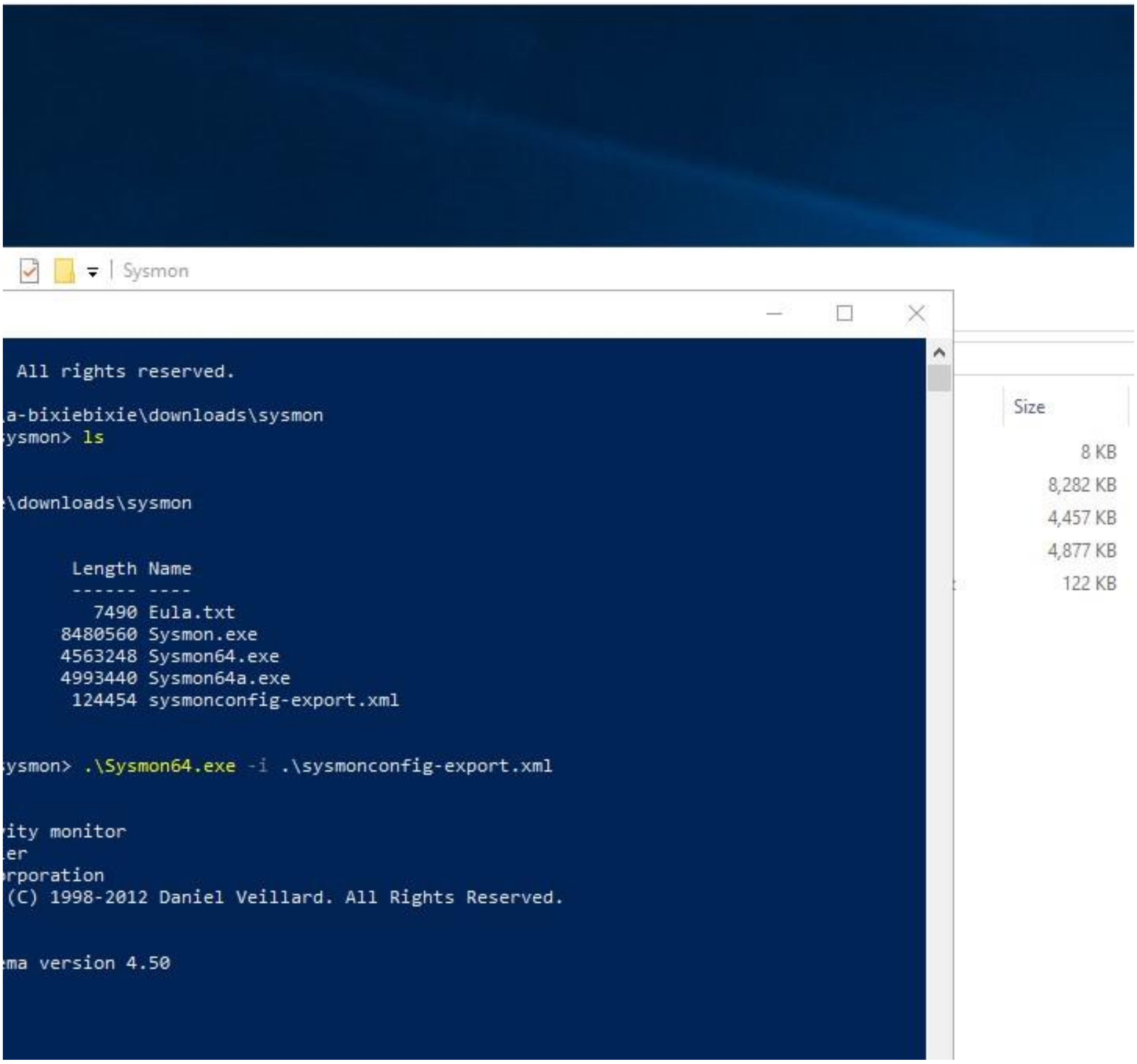


You will then have a folder with the ready Sysmon tool file, however before installation we have to prepare the configuration file so that Sysmon can collect log files. You then navigate to the Sysmon config file on Github.


Sysmon - Sysinternals | Microsoft
sysmon-modular/sysmonconfig
github.com/olafhartong/sysmon-modular/blob/master/sysmonconfig.xml
Files
master
Go to file
2_file_create_time
3_network_connection_initiated
5_process_ended
6_driver_loaded_into_kernel
7_image_load
8_create_remote_thread
9_raw_access_read
attack_matrix
config_lists
templates
.gitignore
Merge-SysmonXml.ps1
README.md
exclude_desktop_central.xml
license.md
merge_sysmon_configs.py
sysmonconfig-excludes-only.xml
sysmonconfig-mde-augment.xml
sysmonconfig-research.xml
sysmonconfig-with-filedelete.xml
sysmonconfig.xml
sysmon-modular / sysmonconfig.xml
Azure Pipeline Updated after successful CICD run 09/20/2023 07:33:02 UTC
History
Code
Blame
2704 lines (2704 loc) · 247 KB
Raw

```
<!--                    NOTICE : This is a balanced generated output of Sysmon-modular with medium verbosity          -->
<!--                     due to the balanced nature of this configuration there will be potential blind spots          -->
<!--                     for more information go to https://github.com/olafhartong/sysmon-modular/wiki                  -->
<!--                                                                                                                    -->
<!--  //**                  ***//                                                                                       -->
<!-- ///#(**               **%(///                                                                                      -->
<!-- ((&&&**               **&&&((                                                                                      -->
<!--  (&&&**   ,(((((((.   **&&&(                                                                                       -->
<!--  ((&&**(((((//(((((((/**&&((      _____                                             __     __                      -->
<!--   (&&///((////(((((((///&&(      / ___/__  __________ ___  ____  ____       ____ ___  ____  ____/ /_  __/ /___ ______  -->
<!--    &////(/////(((((/(////&       \__ \/ / / / ___/ __ `__ \/ __ \/ __ \______/ __ `__ \/ __ \/ __  / / / / / __ `/ ___/  -->
<!--    ((//  /////(/////  /(((      ___/ / /_/ (__  ) / / / / / /_/ / / / /_____/ / / / / / /_/ / /_/ / /_/ / / /_/ / /      -->
<!--   &(((((#.///////// #(((((&   /____/\__, /____/_/ /_/ /_/\____/_/ /_/     /_/ /_/ /_/\____/\__,_/\__,_/_/\__,_/_/       -->
<!--    &&&&((#///////((#((&&&&        /____/                                                                               -->
<!--      &&&&(#/***//(#(&&&&                                                                                               -->
<!--        &&&&****///&&&&                                                                       by Olaf Hartong            -->
<!--           (&    ,&.                                                                                                    -->
<!--            .*&&*.                                                                                                      -->
<!--                                                                                                                        -->
<Sysmon schemaversion="4.90">
  <HashAlgorithms>*</HashAlgorithms>
  <!-- This now also determines the file names of the files preserved (String) -->
  <CheckRevocation>False</CheckRevocation>
  <!-- Setting this to true might impact performance -->
  <DnsLookup>False</DnsLookup>
  <!-- Disables lookup behavior, default is True (Boolean) -->
  <ArchiveDirectory>Sysmon</ArchiveDirectory>
  <!-- Sets the name of the directory in the C:\ root where preserved files will be saved (String)-->
  <EventFiltering>
    <!-- Event ID 1 == Process Creation - Includes -->
    <RuleGroup groupRelation="or">
      <ProcessCreate onmatch="include">
        <ParentImage name="technique_id=T1546.008,technique_name=Accessibility Features" condition="image">sethc.exe</ParentImage>
```

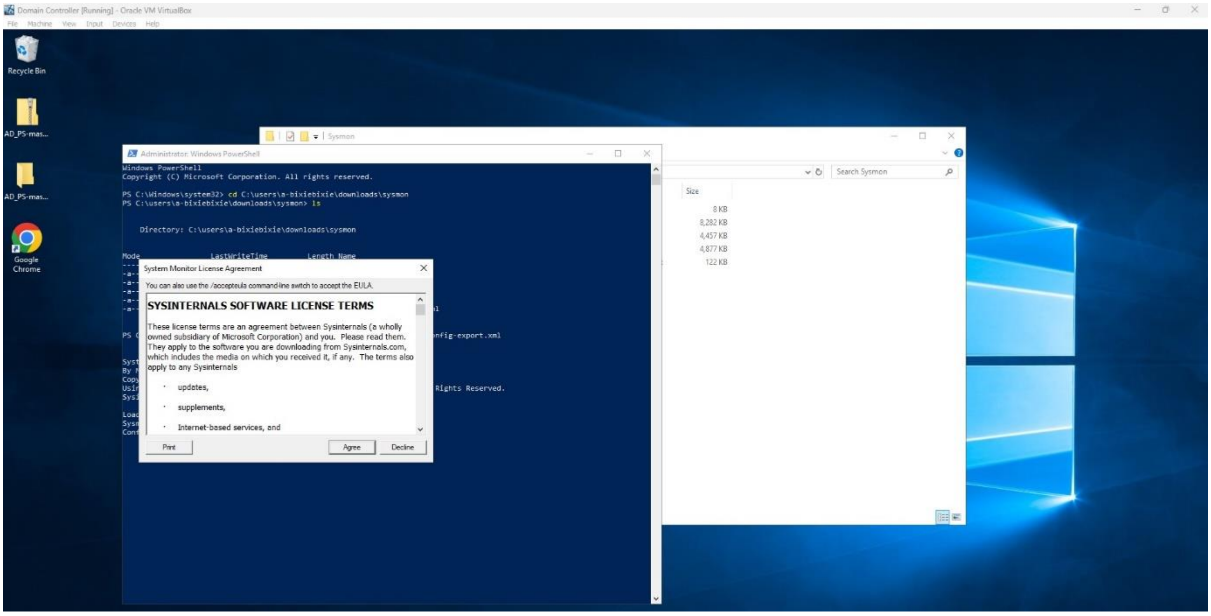
Open the file in Notepad++ and then save it as a xml file.



```
 All rights reserved.

a-bixiebixie\downloads\sysmon
ysmon> ls


\downloads\sysmon


      Length Name
      ------ ----
        7490 Eula.txt
     8480560 Sysmon.exe
     4563248 Sysmon64.exe
     4993440 Sysmon64a.exe
      124454 sysmonconfig-export.xml


ysmon> .\Sysmon64.exe -i .\sysmonconfig-export.xml


ity monitor
er
rporation
(C) 1998-2012 Daniel Veillard. All Rights Reserved.


ma version 4.50
```

Open Powershell as an administrator, and we are ready to install Sysmon. Run the following command: *.\Sysmon64.exe -i .\sysmonconfig-export.xml*

Select **Agree**



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

PS C:\Windows\system32> cd C:\users\a-bixiebixie\downloads\sysmon
PS C:\users\a-bixiebixie\downloads\sysmon> ls


    Directory: C:\users\a-bixiebixie\downloads\sysmon


Mode                 LastWriteTime         Length Name
```

System Monitor License Agreement

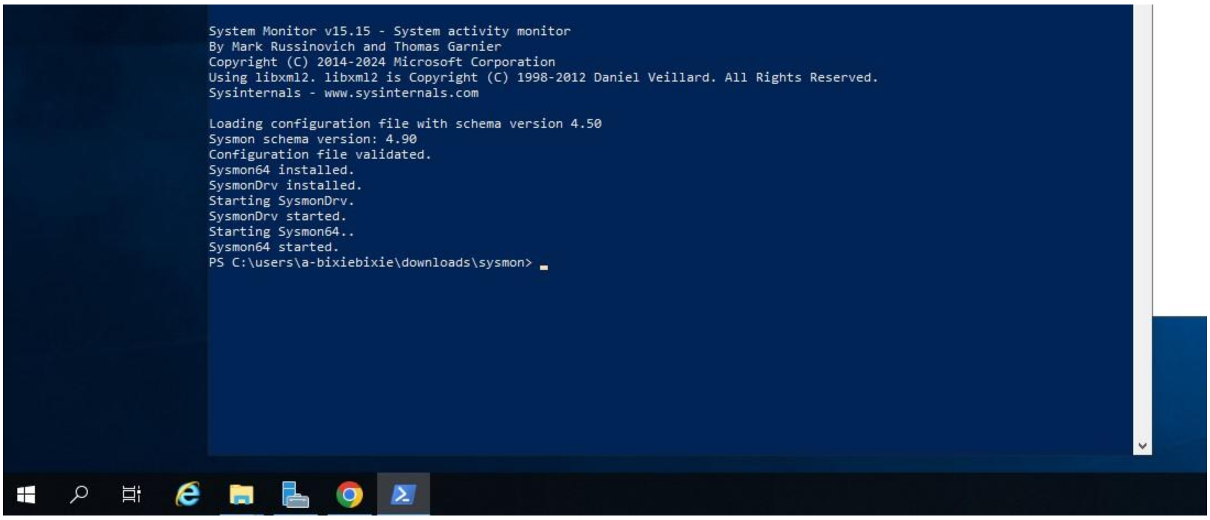
You can also use the /accepteula command-line switch to accept the EULA.

**SYSINTERNALS SOFTWARE LICENSE TERMS**

These license terms are an agreement between Sysinternals (a wholly owned subsidiary of Microsoft Corporation) and you. Please read them. They apply to the software you are downloading from Sysinternals.com, which includes the media on which you received it, if any. The terms also apply to any Sysinternals

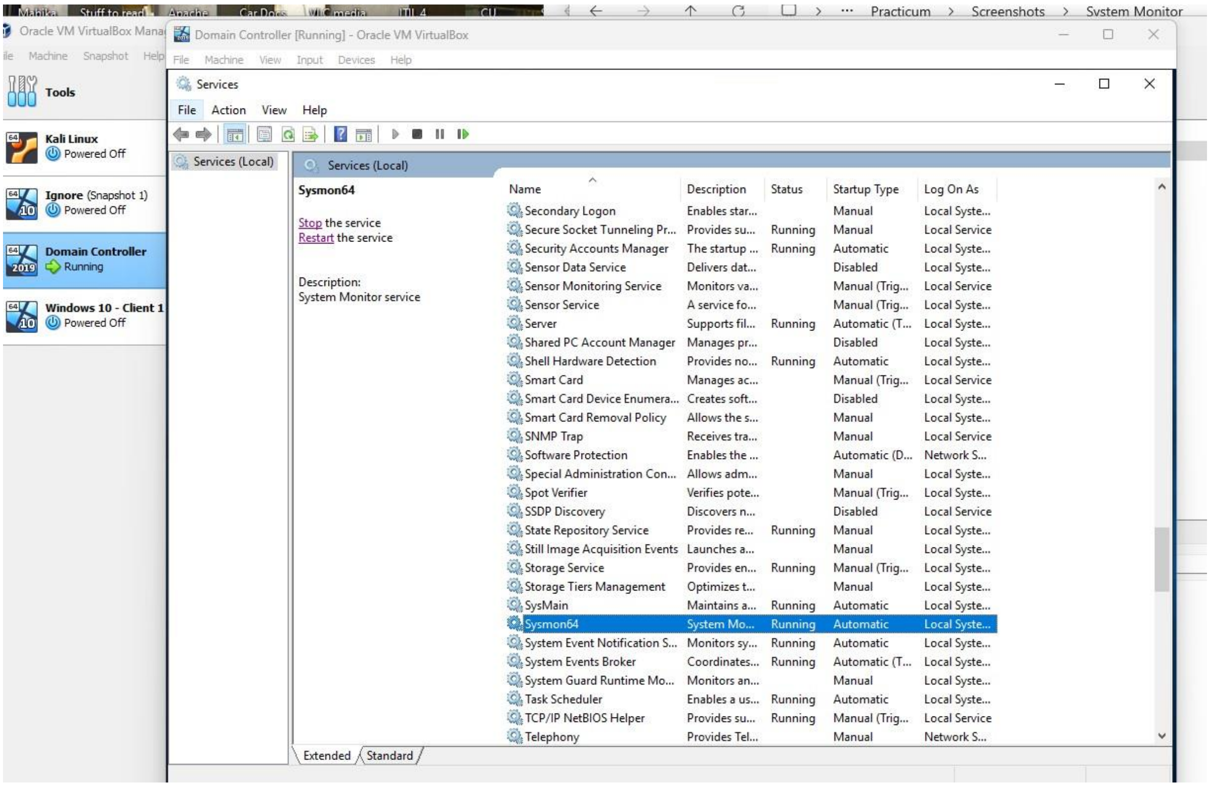
- updates,
- supplements,
- Internet-based services, and

And Sysmon is installed.



```
System Monitor v15.15 - System activity monitor
By Mark Russinovich and Thomas Garnier
Copyright (C) 2014-2024 Microsoft Corporation
Using libxml2. libxml2 is Copyright (C) 1998-2012 Daniel Veillard. All Rights Reserved.
Sysinternals - www.sysinternals.com

Loading configuration file with schema version 4.50
Sysmon schema version: 4.90
Configuration file validated.
Sysmon64 installed.
SysmonDrv installed.
Starting SysmonDrv.
SysmonDrv started.
Starting Sysmon64..
Sysmon64 started.
PS C:\users\a-bixiebixie\downloads\sysmon> _
```

We can begin to capture Events under Windows Event Viewer in Sysmon

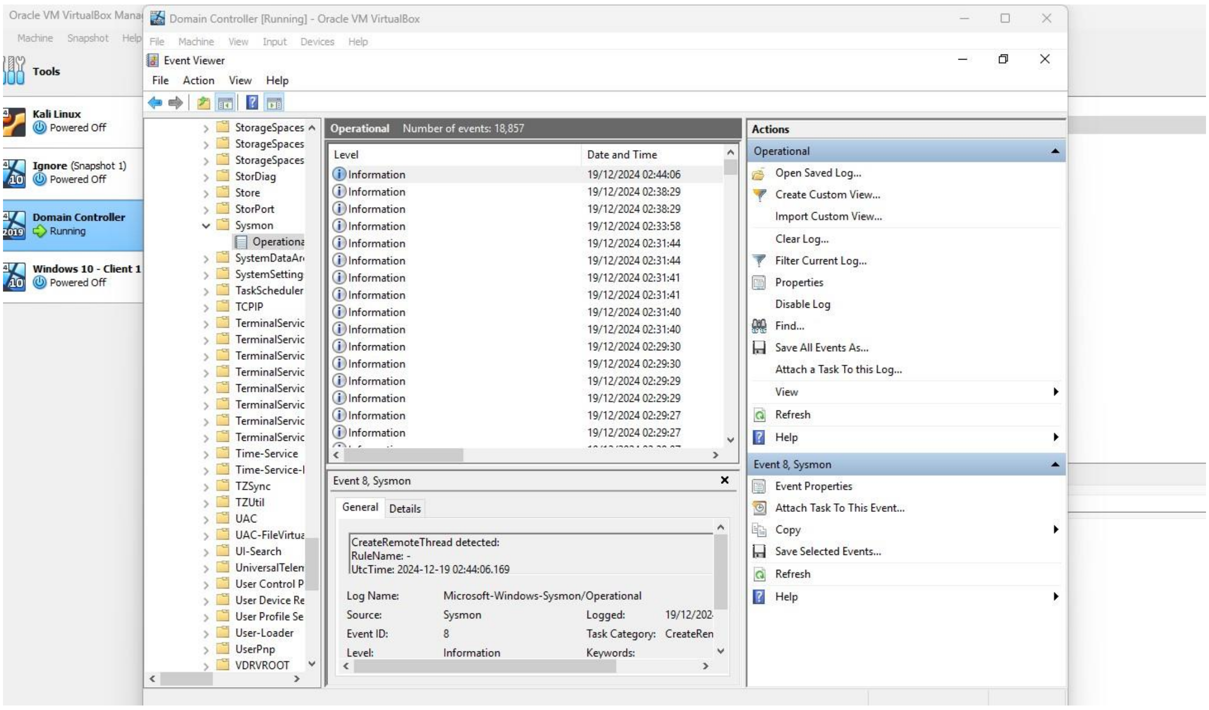


Sysmon64

Stop the service
Restart the service

Description:
System Monitor service

| Name | Description | Status | Startup Type | Log On As |
|---|---|---|---|---|
| Secondary Logon | Enables star... |  | Manual | Local Syste... |
| Secure Socket Tunneling Pr... | Provides su... | Running | Manual | Local Service |
| Security Accounts Manager | The startup ... | Running | Automatic | Local Syste... |
| Sensor Data Service | Delivers dat... |  | Disabled | Local Syste... |
| Sensor Monitoring Service | Monitors va... |  | Manual (Trig... | Local Service |
| Sensor Service | A service fo... |  | Manual (Trig... | Local Syste... |
| Server | Supports fil... | Running | Automatic (T... | Local Syste... |
| Shared PC Account Manager | Manages pr... |  | Disabled | Local Syste... |
| Shell Hardware Detection | Provides no... | Running | Automatic | Local Syste... |
| Smart Card | Manages ac... |  | Manual (Trig... | Local Service |
| Smart Card Device Enumera... | Creates soft... |  | Disabled | Local Syste... |
| Smart Card Removal Policy | Allows the s... |  | Manual | Local Syste... |
| SNMP Trap | Receives tra... |  | Manual | Local Service |
| Software Protection | Enables the ... |  | Automatic (D... | Network S... |
| Special Administration Con... | Allows adm... |  | Manual | Local Syste... |
| Spot Verifier | Verifies pote... |  | Manual (Trig... | Local Syste... |
| SSDP Discovery | Discovers n... |  | Disabled | Local Service |
| State Repository Service | Provides re... | Running | Manual | Local Syste... |
| Still Image Acquisition Events | Launches a... |  | Manual | Local Syste... |
| Storage Service | Provides en... | Running | Manual (Trig... | Local Syste... |
| Storage Tiers Management | Optimizes t... |  | Manual | Local Syste... |
| SysMain | Maintains a... | Running | Automatic | Local Syste... |
| Sysmon64 | System Mo... | Running | Automatic | Local Syste... |
| System Event Notification S... | Monitors sy... | Running | Automatic | Local Syste... |
| System Events Broker | Coordinates... | Running | Automatic (T... | Local Syste... |
| System Guard Runtime Mo... | Monitors an... |  | Manual | Local Syste... |
| Task Scheduler | Enables a us... | Running | Automatic | Local Syste... |
| TCP/IP NetBIOS Helper | Provides su... | Running | Manual (Trig... | Local Service |
| Telephony | Provides Tel... |  | Manual | Network S... |



Operational Number of events: 18,857

| Level | Date and Time |
|---|---|
| Information | 19/12/2024 02:44:06 |
| Information | 19/12/2024 02:38:29 |
| Information | 19/12/2024 02:38:29 |
| Information | 19/12/2024 02:33:58 |
| Information | 19/12/2024 02:31:44 |
| Information | 19/12/2024 02:31:44 |
| Information | 19/12/2024 02:31:41 |
| Information | 19/12/2024 02:31:41 |
| Information | 19/12/2024 02:31:40 |
| Information | 19/12/2024 02:31:40 |
| Information | 19/12/2024 02:29:30 |
| Information | 19/12/2024 02:29:30 |
| Information | 19/12/2024 02:29:29 |
| Information | 19/12/2024 02:29:29 |
| Information | 19/12/2024 02:29:27 |
| Information | 19/12/2024 02:29:27 |

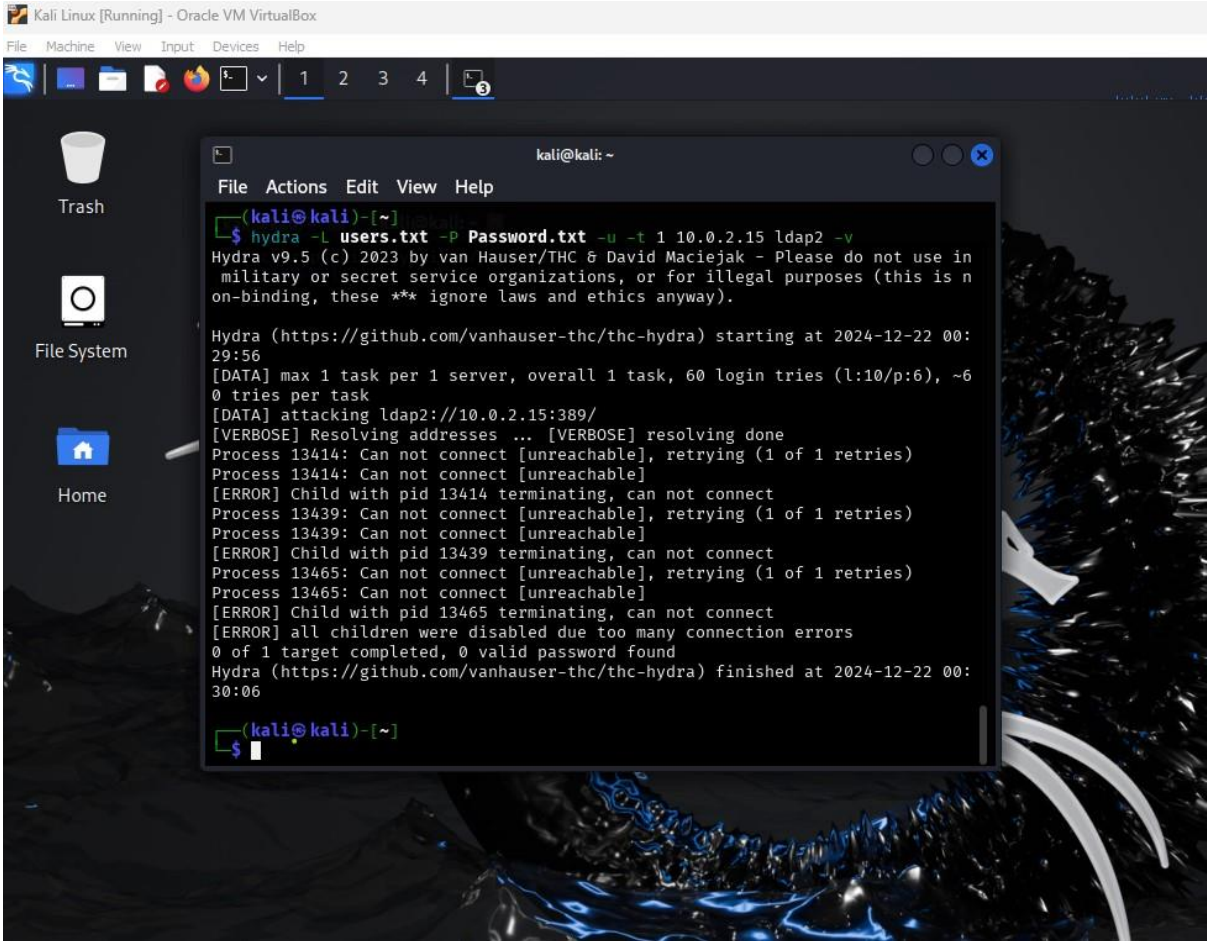
Event 8, Sysmon

General Details

```
CreateRemoteThread detected:
RuleName: -
UtcTime: 2024-12-19 02:44:06.169
```

| | | | |
|---|---|---|---|
| Log Name: | Microsoft-Windows-Sysmon/Operational | | |
| Source: | Sysmon | Logged: | 19/12/202 |
| Event ID: | 8 | Task Category: | CreateRen |
| Level: | Information | Keywords: | |

Next you can login into your Kali Linux (attacker), Open Hydra and perform an attack as highlighted in the previous Hydra installation step by step.


Kali Linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
1 2 3 4
Trash
File System
Home
kali@kali: ~
File Actions Edit View Help

```
┌──(kali㉿kali)-[~]
└─$ hydra -L users.txt -P Password.txt -u -t 1 10.0.2.15 ldap2 -v
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in
 military or secret service organizations, or for illegal purposes (this is n
on-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-12-22 00:
29:56
[DATA] max 1 task per 1 server, overall 1 task, 60 login tries (l:10/p:6), ~6
0 tries per task
[DATA] attacking ldap2://10.0.2.15:389/
[VERBOSE] Resolving addresses ... [VERBOSE] resolving done
Process 13414: Can not connect [unreachable], retrying (1 of 1 retries)
Process 13414: Can not connect [unreachable]
[ERROR] Child with pid 13414 terminating, can not connect
Process 13439: Can not connect [unreachable], retrying (1 of 1 retries)
Process 13439: Can not connect [unreachable]
[ERROR] Child with pid 13439 terminating, can not connect
Process 13465: Can not connect [unreachable], retrying (1 of 1 retries)
Process 13465: Can not connect [unreachable]
[ERROR] Child with pid 13465 terminating, can not connect
[ERROR] all children were disabled due too many connection errors
0 of 1 target completed, 0 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-12-22 00:
30:06

┌──(kali㉿kali)-[~]
└─$ 
```

## 8. References

Microsoft. (2024). *Sysinternals*. [online] Available at: https://learn.microsoft.com/en-us/sysinternals/downloads/sysmon/ [Accessed 09 December 2024].