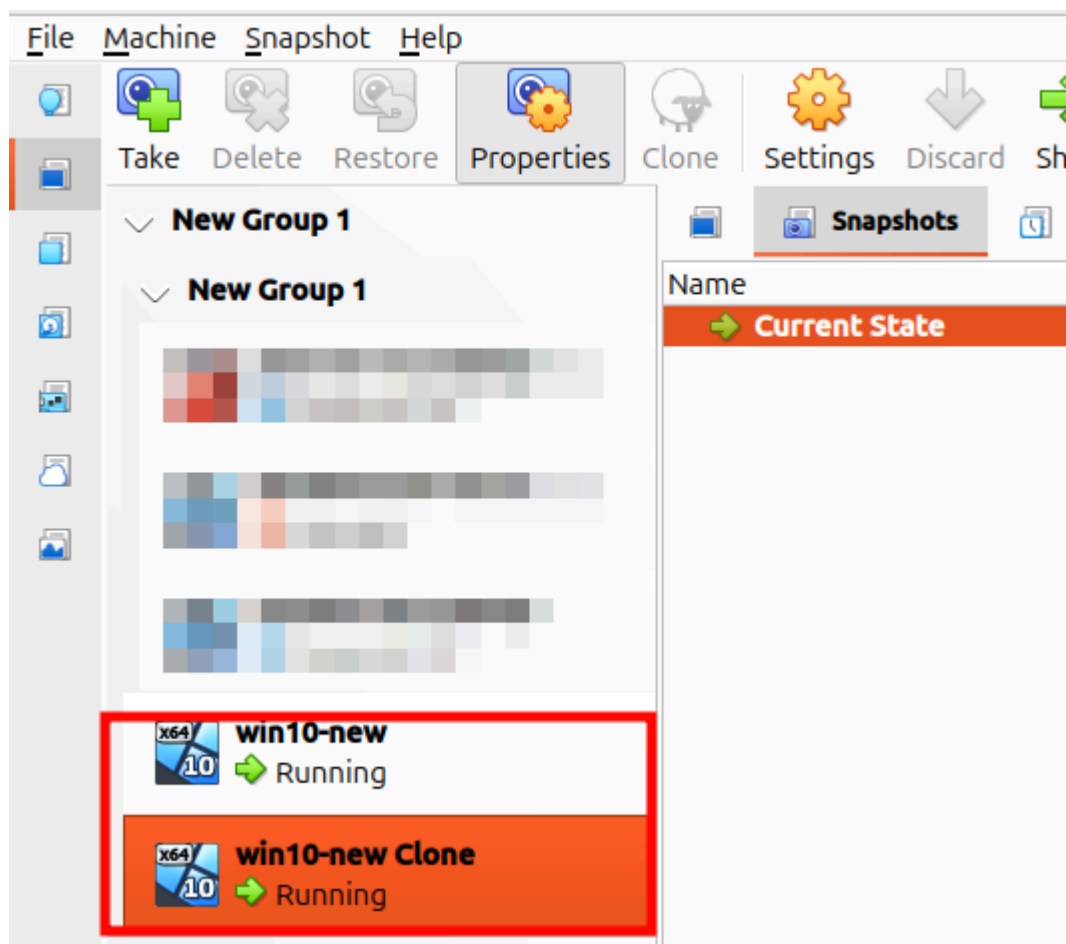



In this lab we are going to see how to detect and analyse lateral movement using PsExec, a legitimate Windows sysinternals tool often exploited by attackers.

Now we are going to start from using two windows VMs, one going to be the machine that we are using to exploit and other that will be the target.



Win10-new will be our machine to exploit and the win10-new clone will be our target.

 | **Learn** Documentation ▾ Training ▾ Q&A ▾ Topics ▾

Sysinternals Downloads Community Resources

[Learn / Sysinternals /](#)

[Ask Learn](#)

[Focus mode](#)

Home


▼ Downloads

- Downloads
 - > File and Disk Utilities
 - > Networking Utilities
 - ▼ Process Utilities
 - Process Utilities
 - AutoRuns
 - Handle
 - ListDLLs
 - Portmon
 - ProcDump
 - Process Explorer
 - Process Monitor

PsExec v2.43

By Mark Russinovich

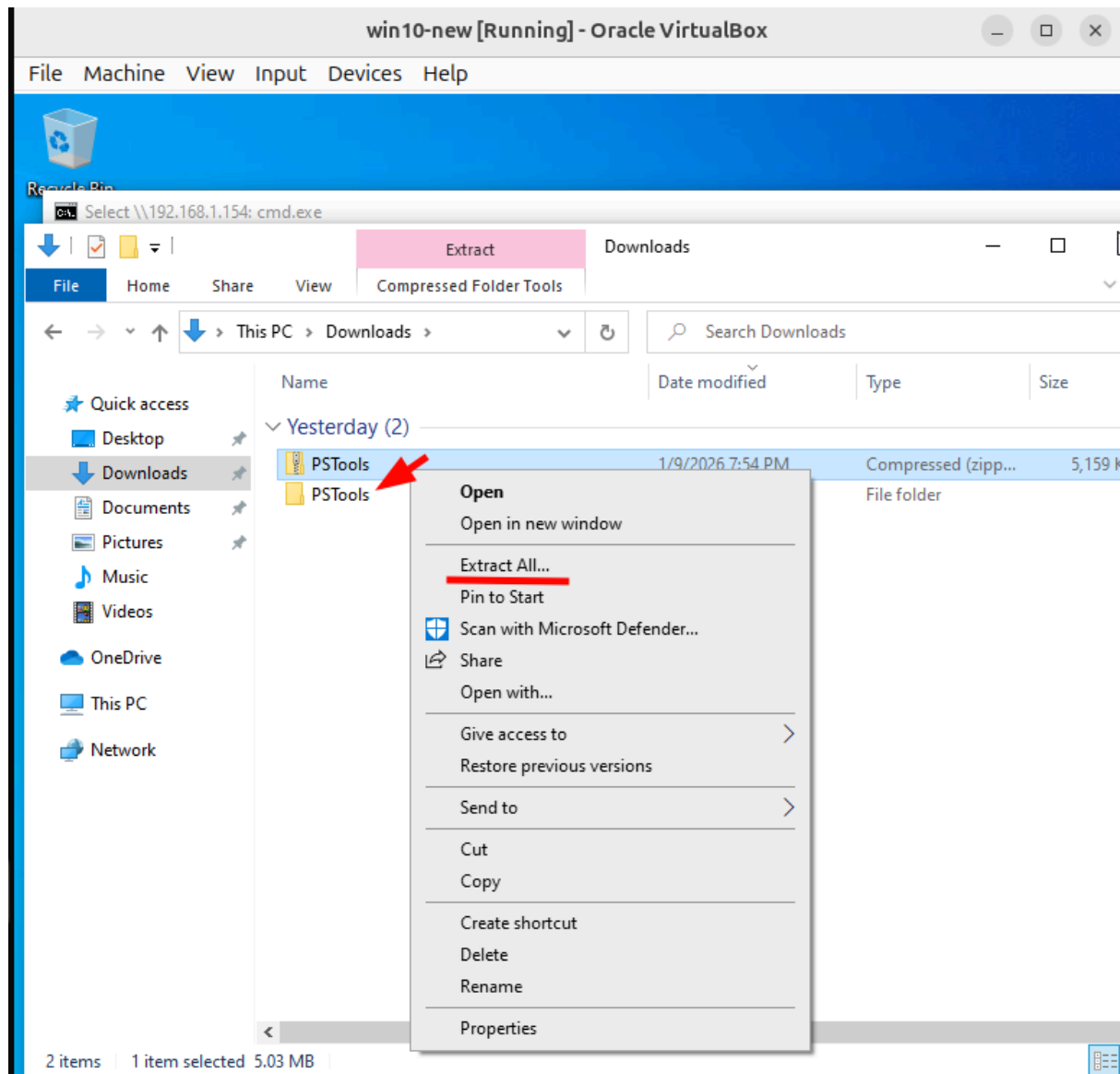
Published: April 11, 2023

 [Download PsTools](#) (5 MB)

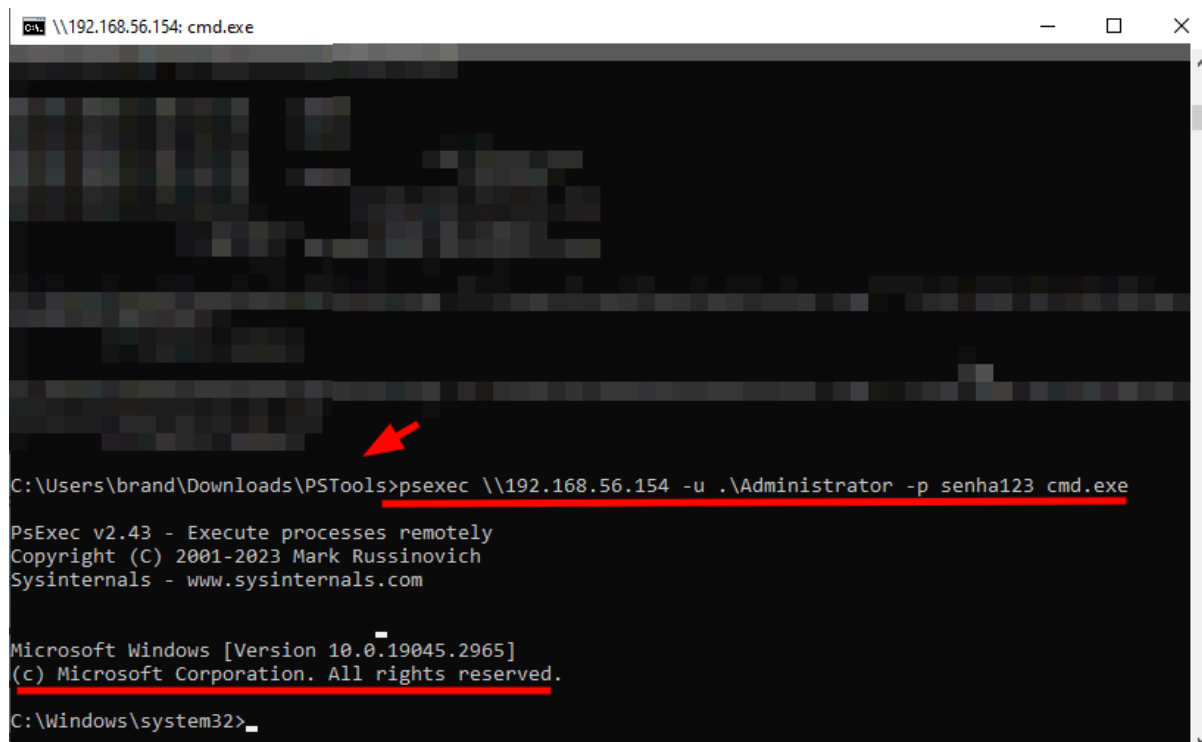
Introduction

Utilities like Telnet and remote control programs like Symantec's PC Anywhere let you execute programs on remote systems, but they can be a pain to set up and require that you install client software on the remote systems that you wish to access. PsExec is a light-weight telnet-replacement that lets you execute processes on other systems, complete with full interactivity for console applications, without having to manually install client software. PsExec's most powerful uses include launching interactive command prompts on remote systems and remote applications.

To use the PsExec, we have to enter in the site of Microsoft and downloaded the file PsExec v2.43.



After downloading, we just need to extract the contents of the folder.



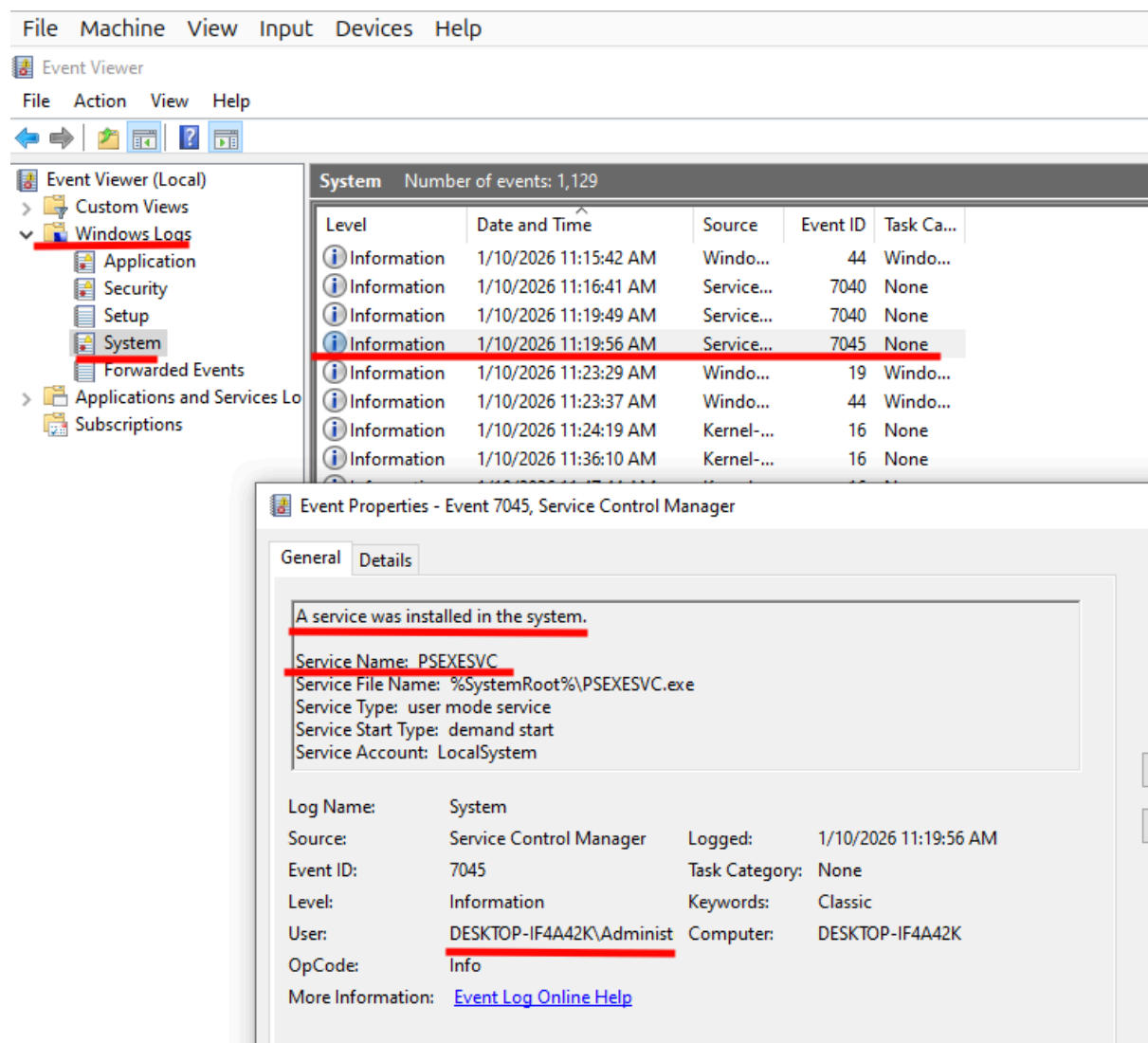
```
\\192.168.56.154: cmd.exe
C:\Users\brand\Downloads\PSTools>psexec \\192.168.56.154 -u .\Administrator -p senha123 cmd.exe
PsExec v2.43 - Execute processes remotely
Copyright (C) 2001-2023 Mark Russinovich
Sysinternals - www.sysinternals.com
Microsoft Windows [Version 10.0.19045.2965]
(c) Microsoft Corporation. All rights reserved.
C:\Windows\system32>
```

Now, when we ran this command, if successful, this opens a remote shell on our target.

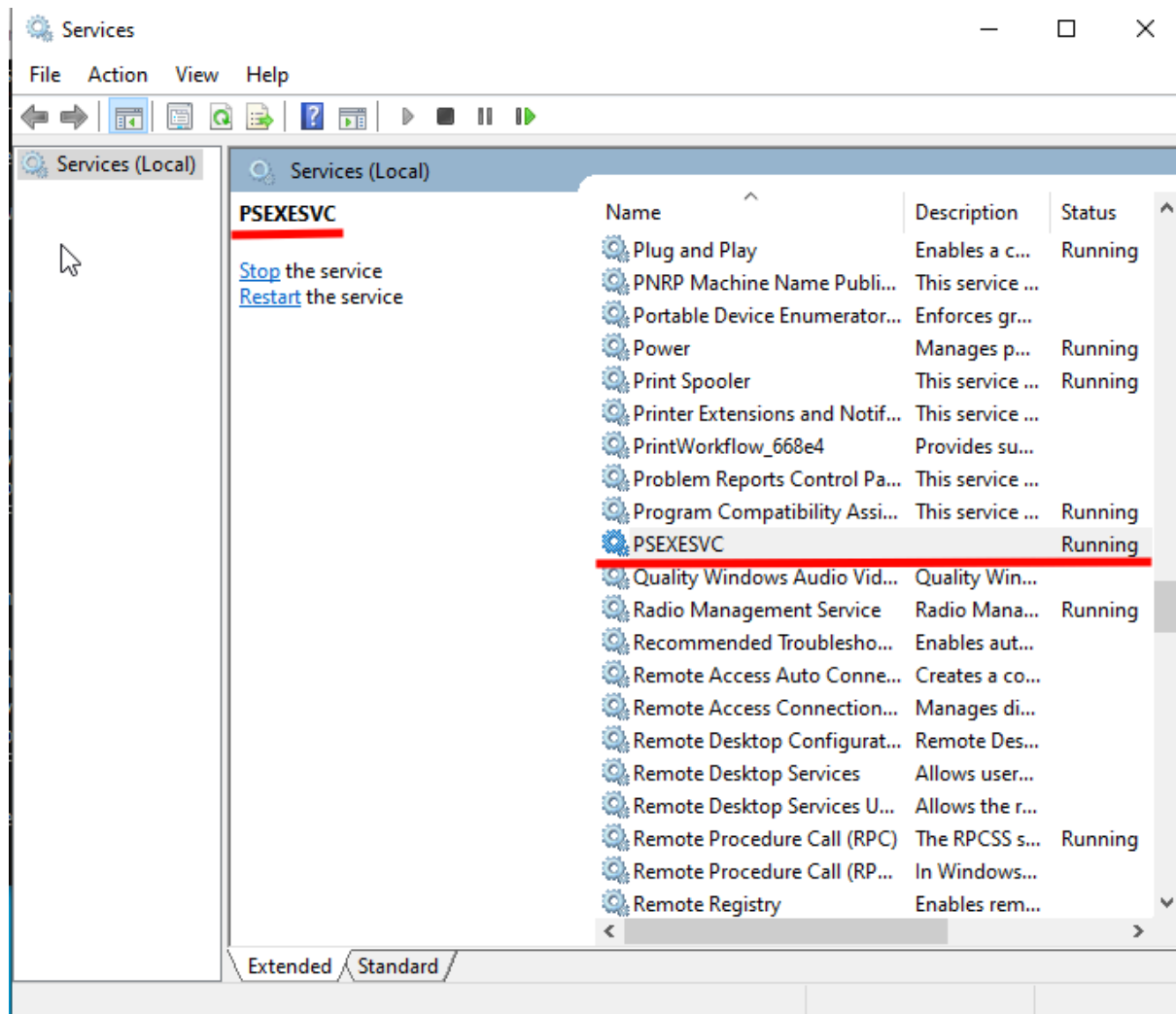
The screenshot shows the Windows Task Manager window with the 'Performance' tab selected. The 'Disk' section is highlighted in red, indicating 100% usage. The 'Processes' tab is also visible, showing a list of running applications. The 'PsExec Service (32 bit)' process is highlighted with a red underline.

Name	Status	CPU	Memory	Disk	Network
Microsoft Edge		0%	4.1 MB	0 MB/s	0 Mbps
Microsoft Edge		0%	5.1 MB	0 MB/s	0 Mbps
Microsoft Edge		0%	1.4 MB	0 MB/s	0 Mbps
Microsoft Edge Update (32 bit)		0%	0.7 MB	0 MB/s	0 Mbps
Microsoft Malware Protection Si...		0%	0.1 MB	0 MB/s	0 Mbps
Microsoft OneDrive (32 bit) Setu...		0%	2.3 MB	0.1 MB/s	0 Mbps
Microsoft OneDrive (32 bit) Setu...		0%	0.1 MB	0 MB/s	0 Mbps
Microsoft Software Protection P...		0%	2.2 MB	0 MB/s	0 Mbps
Microsoft Store		0%	3.7 MB	0.1 MB/s	0 Mbps
Microsoft Text Input Application		0%	2.5 MB	0 MB/s	0 Mbps
Microsoft Windows Search Inde...		0%	14.0 MB	0 MB/s	0 Mbps
MoUSO Core Worker Process		0%	2.7 MB	0 MB/s	0 Mbps
PsExec Service (32 bit)		0%	1.6 MB	0 MB/s	0 Mbps
Runtime Broker		0%	1.7 MB	0 MB/s	0 Mbps

If we enter in the task manager, of course in the target machine, we can see the PsExec running in the second plan.



If we enter in the event viewer, we can notice that a service was installed in the system, the PSEXESVC.



If we press the win + r and write service.msc, we can check the PSEXESVC running.

```
cmd.exe - \\192.168.56.154: cmd.exe

C:\Users\brand\Downloads\PSTools>psexec \\192.168.56.154 -u .\Administrator -p senha123 cmd.exe

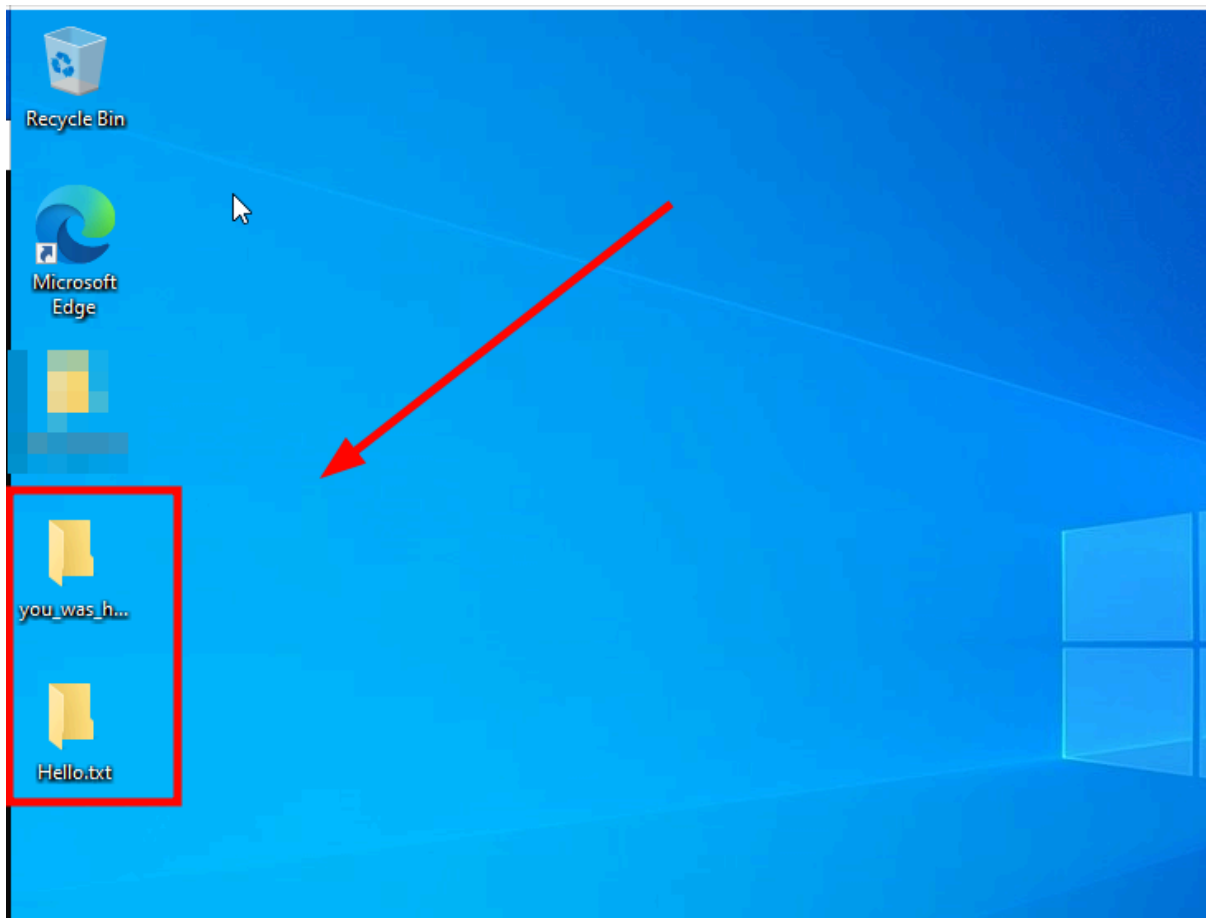
PsExec v2.43 - Execute processes remotely
Copyright (C) 2001-2023 Mark Russinovich
Sysinternals - www.sysinternals.com

Microsoft Windows [Version 10.0.19045.2965]
(c) Microsoft Corporation. All rights reserved.

C:\Windows\system32>mkdir "C:\users\Public\Desktop\you was hacked"

C:\Windows\system32>
```

Now, let's run this command to create a file in our target.



Here we can check that the file was created successfully.

Now we are going to use the elastic cloud to watch our target machine.

Assets

- Fleet
- Agents**
- Policies
- Enrollment tokens
- Uninstall tokens
- Data streams
- Settings

[Give feedback](#)

We've added new privileges that let you define more granularly who can view or edit Fleet agents, policies, and settings. [Learn more.](#)
✕

Fleet

Centralized management for Elastic Agents.

[Agents](#)
[Agent policies](#)
[Enrollment tokens](#)
[Uninstall tokens](#)
[Data streams](#)
[Settings](#)

[Ingest Overview Metrics](#)
 [Agent Info Metrics](#)

[🕒 Agent activity](#)

[Add agent](#)

Status 3 ▾

Tags 1 ▾

Agent policy 2 ▾

Upgrade available

Showing 2 agents

● Healthy 2
● Unhealthy 0
● Orphaned 0
● Updating 0
● Offline 0
● Inactive 0
● Unenrolled 0
● Uninstalled 0

<input type="checkbox"/>	Status	Host ↕	Agent policy ↕	CPU	Memory	Last activ... ↕	Version ↕	Actions
<input type="checkbox"/>	Healthy	<u>DESKTOP-AGAJ1A</u>	Agent policy 1 <small>rev. 2</small>	N/A	N/A	21 seconds ago	9.2.3	
<input type="checkbox"/>	Healthy	brandon-HP-EliteDesk	Agent policy 1 <small>rev. 2</small>	2.83 %	255 MB	30 seconds ago	9.2.3	

Rows per page: 20 ▾
< 1 >

Lets start installing the agent in the machine target.

Assets

Fleet

Agents

Policies

Enrollment tokens

Uninstall tokens

Data streams

Settings

Endpoints

Endpoints

Policies

Trusted applications

Trusted devices

Event filters

Give feedback

View all agents

DESKTOP-AGAIJ1A

Agent details | Logs | Diagnostics | Settings

Actions

Overview

CPU

N/A

View more agent metrics

Memory

N/A

Status

Healthy

Last activity

Jan 12, 2026 1:47 PM

Last checkin message

Running

Agent ID

7e25203b-d79d-4417-8f9d-7efa75cb9a5a

Agent policy

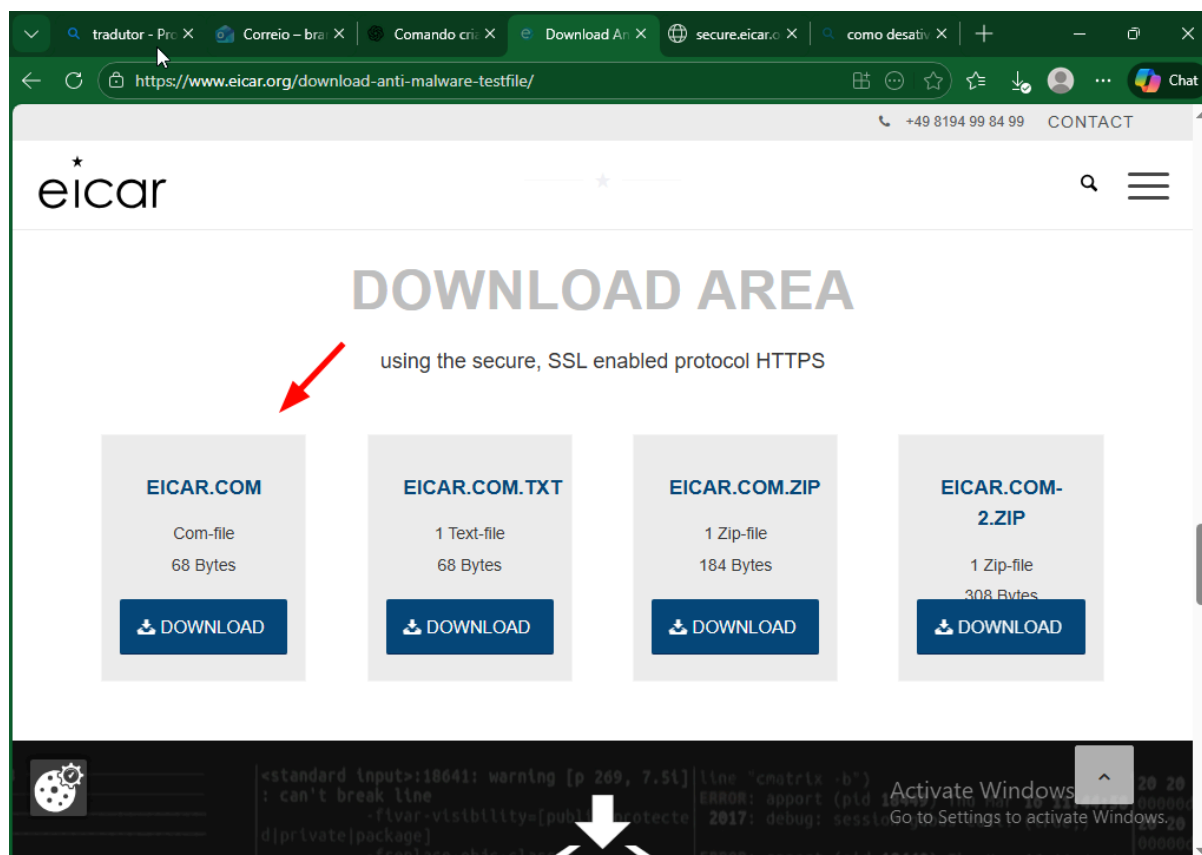
Agent policy 1 rev. 2

Integrations

elastic-defender

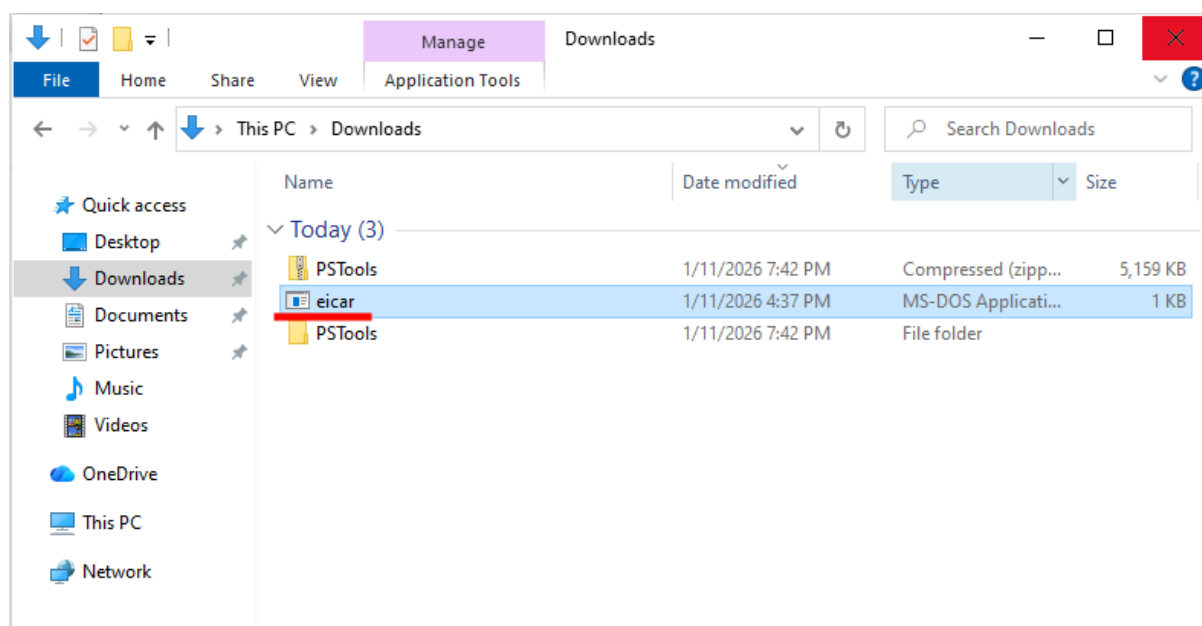
system-1

Let's add the integration elastic-defender to obtain information if something wrong happens.

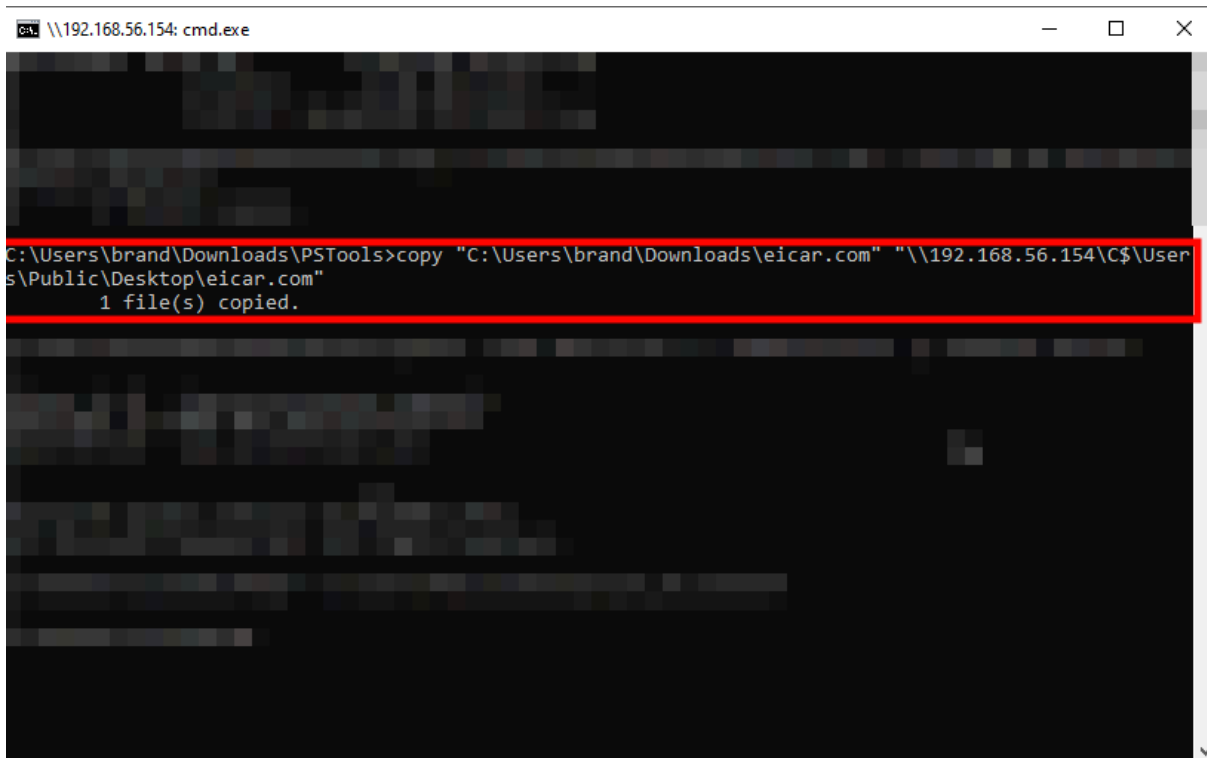


Now, in the machine that you are running the PsExec, let's download the Eicar test, it is a malware test.

To download the Eicar test, I have to turn off the windows defender.

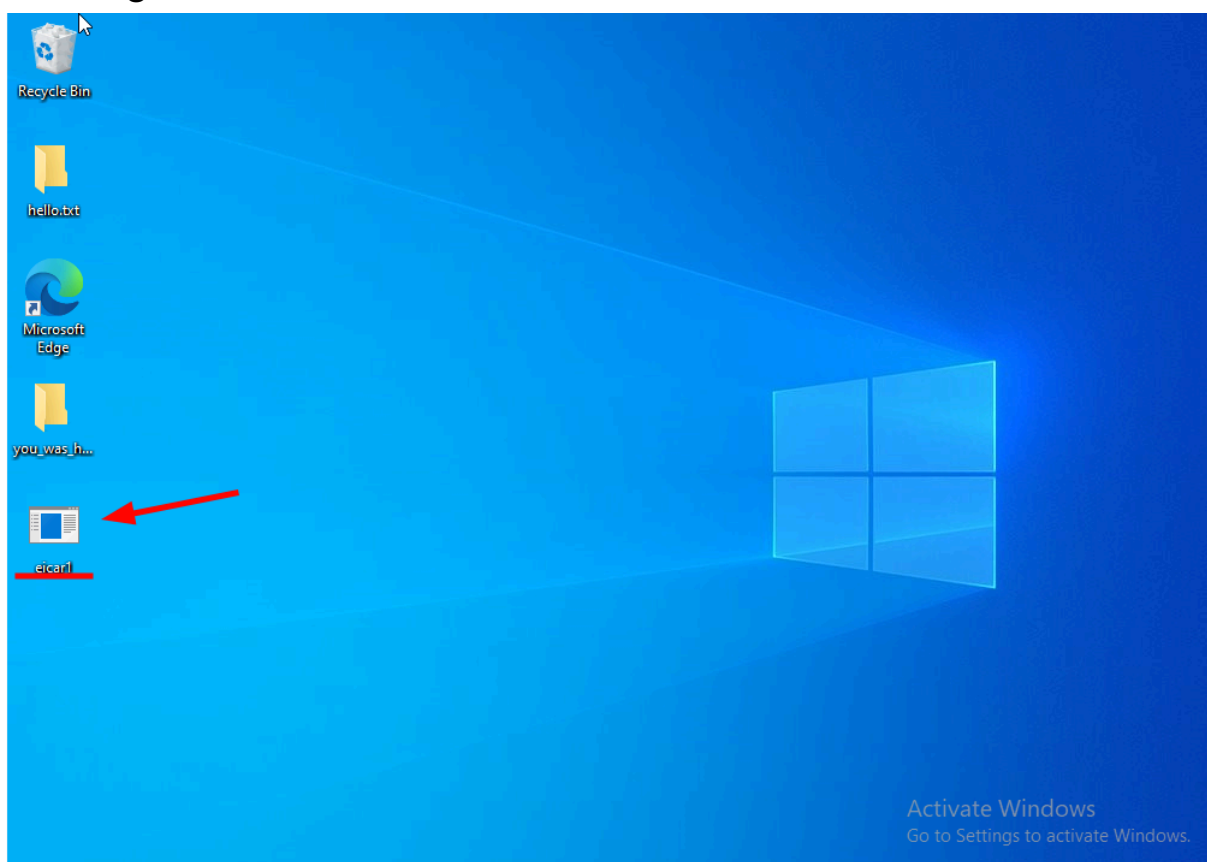


It is here, in the downloads.

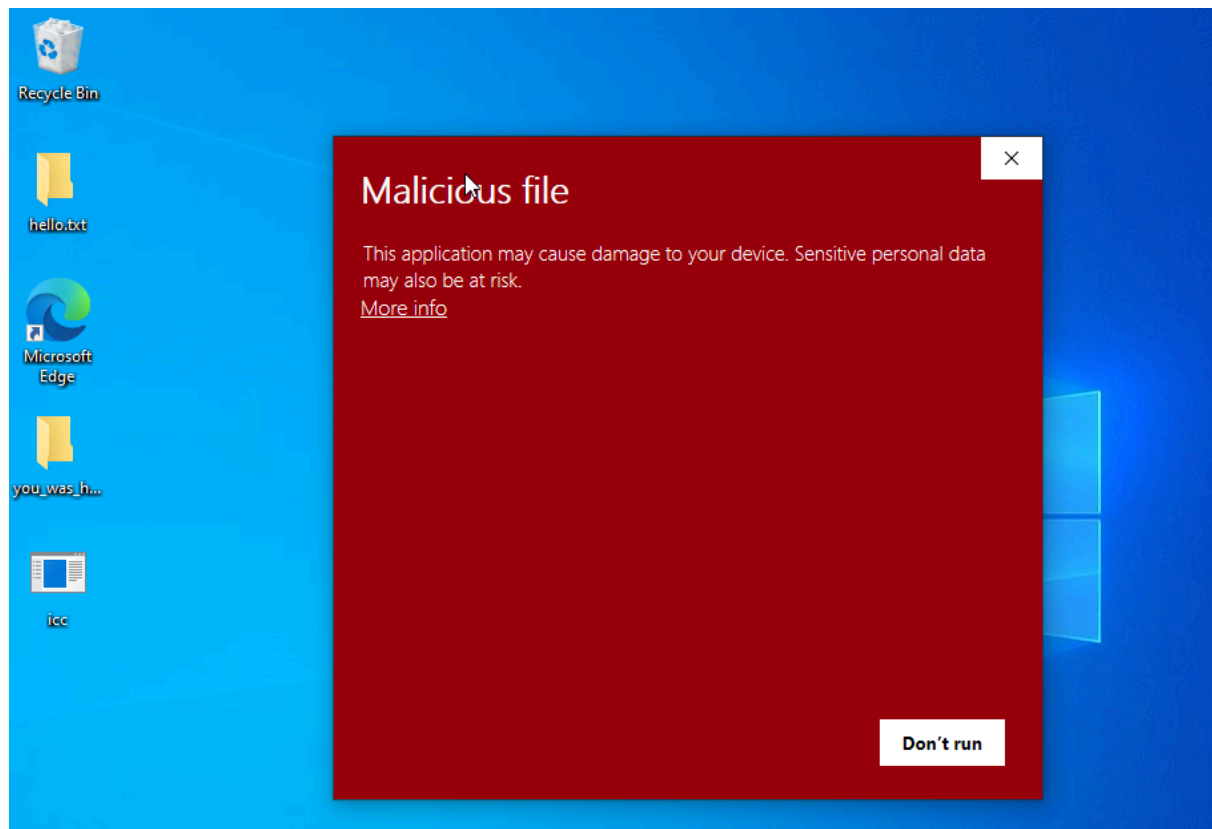


```
C:\Users\brand\Downloads\PSTools>copy "C:\Users\brand\Downloads\eicar.com" "\\192.168.56.154\C$\Users\Public\Desktop\eicar.com"
1 file(s) copied.
```

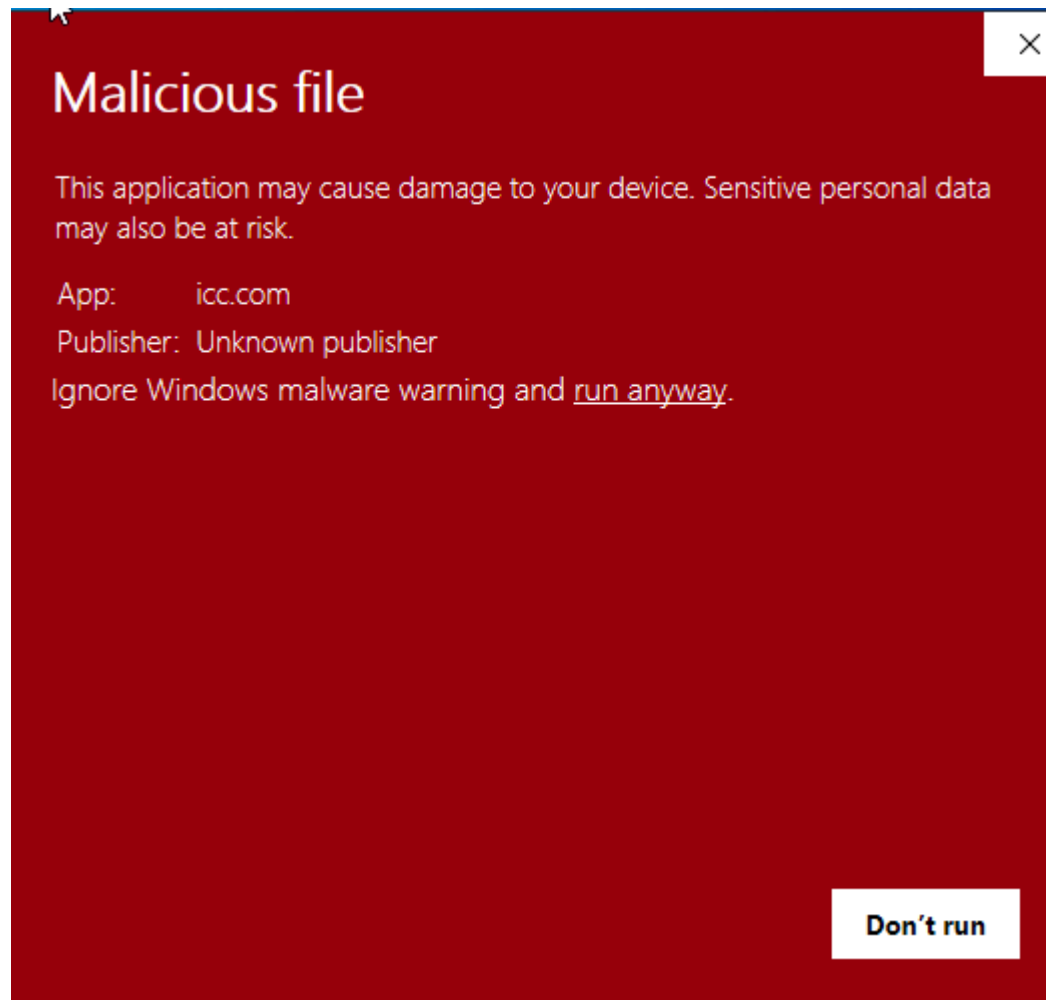
Now, we have to do this command to send this eicar test file to our target.



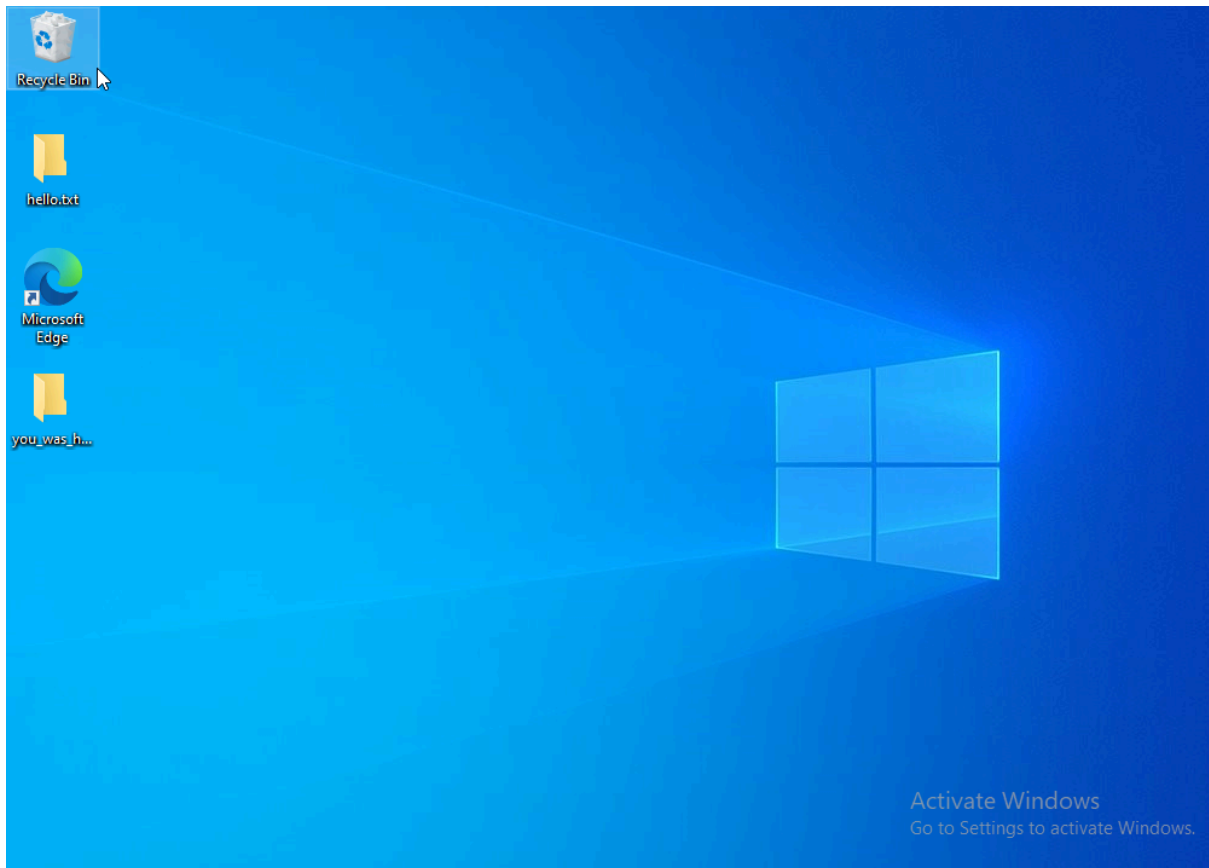
Now, in the target machine, we can see the Eicar file.



If we click in there, we will see this danger warning.

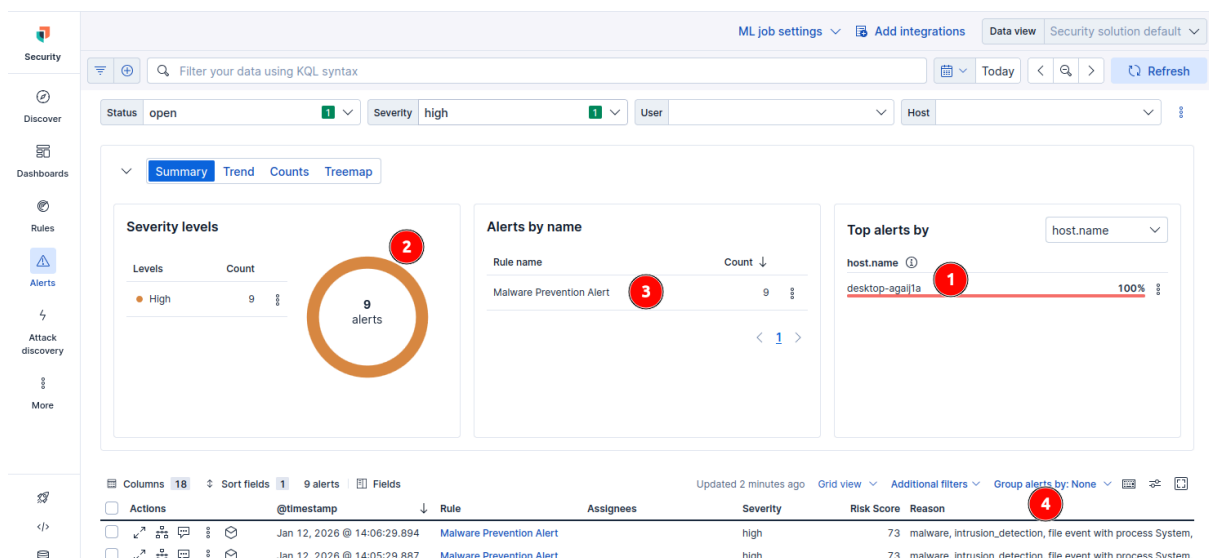


Let's click in run anyway to see what happens.



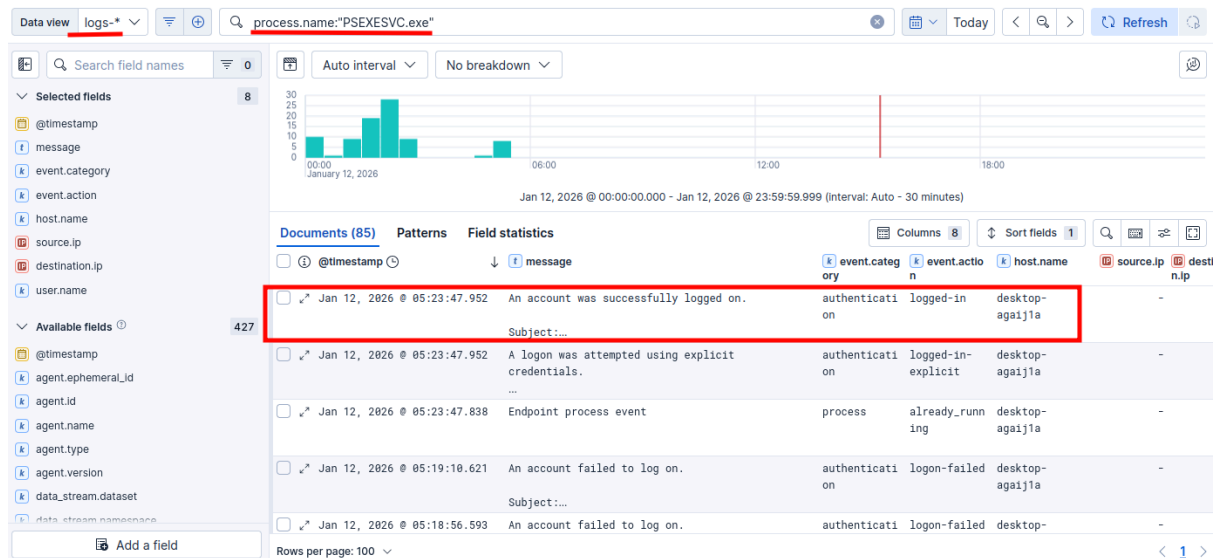
It was deleted.

Now, let's go to the Elastic cloud to see the alerts.



When we open the alerts, we can notice a lot of new advises. The number 1 means the name of our target machine, the

number 2 means how many alerts happen, the number 3 means alert by name and number 4 means the reason.



If we go to Discover, and in data view put logs-*, and write “[process.name](#):\"PSEXESVC.exe\"” we can check that someone successfully logged in our target machine.