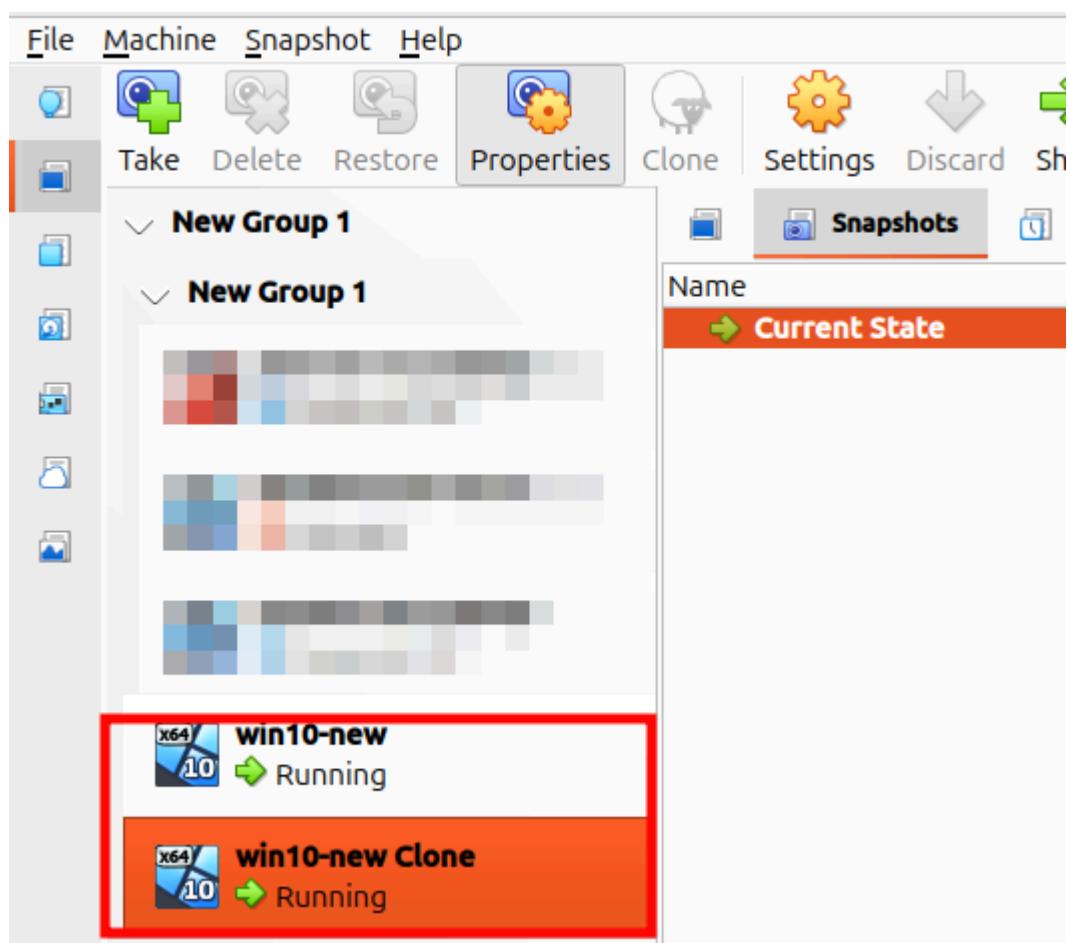


In this lab we are going to see how to detect and analyse lateral movement using PsExec, a legitimate Windows sysinternals tool often exploited by attackers.

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.

Sysinternals Documentation Training Q&A Topics

Sysinternals Downloads Community Resources

Find by title 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

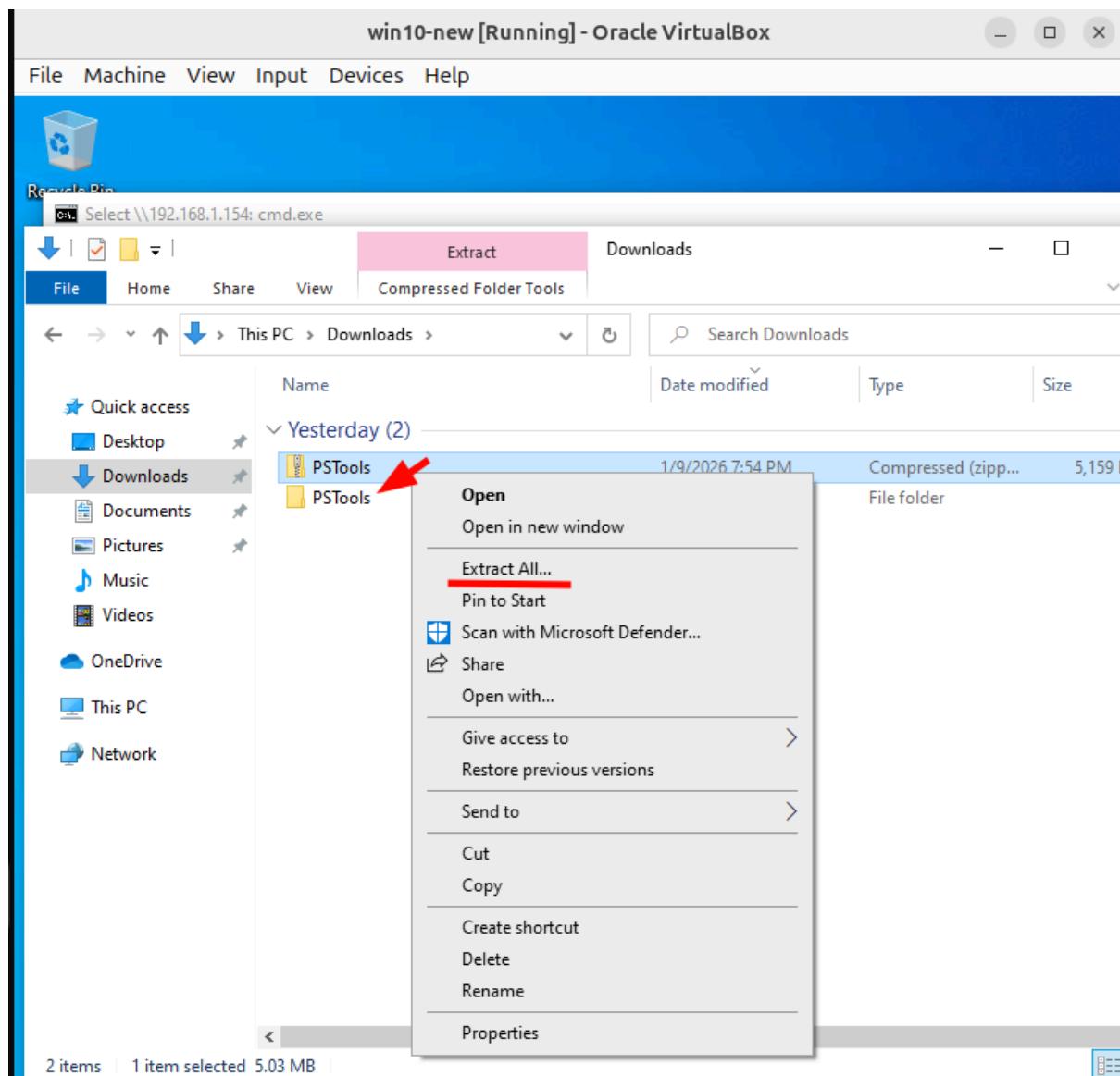
Published: April 11, 2023

 Download PsTools (5 MB)

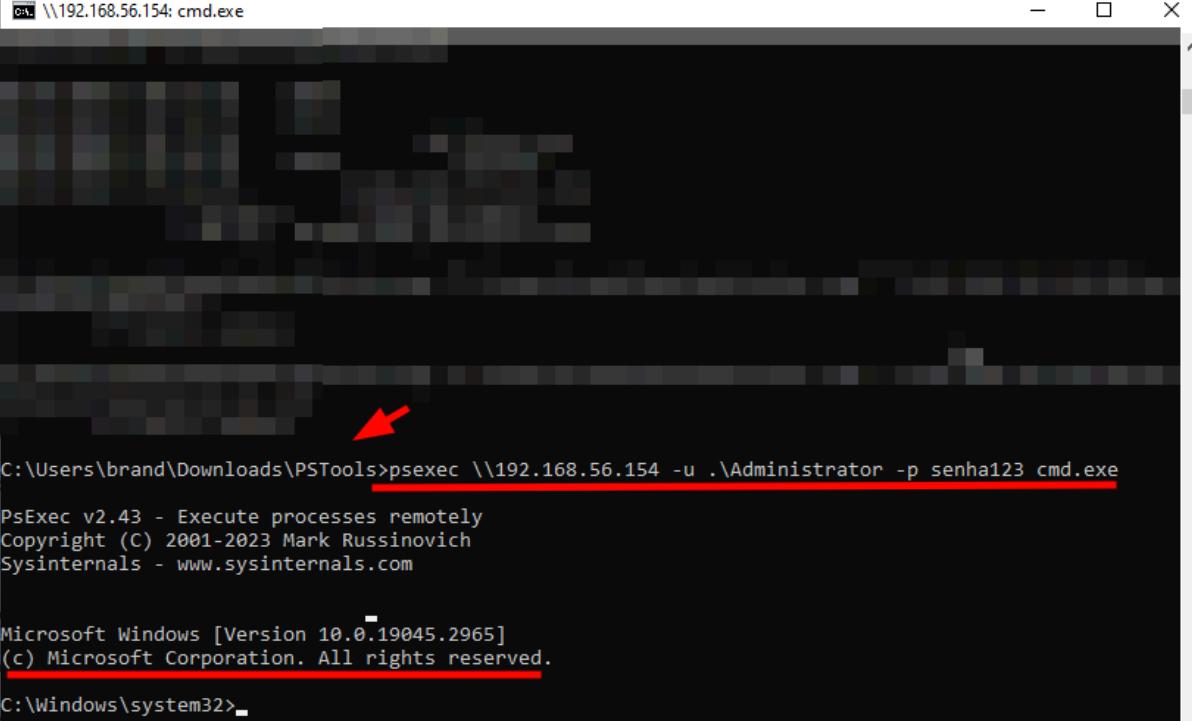
Introduction

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 features include launching interactive command prompts on remote systems and remote debugging.

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.



A screenshot of a Windows command prompt window titled "C:\ \\192.168.56.154: cmd.exe". The window contains the following text:

```
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>
```

A red arrow points to the command line where "psexec" is typed.

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

The screenshot shows the Windows Task Manager interface. The title bar reads "Task Manager". The menu bar includes "File", "Options", and "View". The tabs at the top are "Processes", "Performance", "App history", "Startup", "Users", "Details", and "Services". The "Processes" tab is selected. The main area displays a list of tasks with columns for Name, Status, CPU, Memory, Disk, and Network. The "Disk" column is highlighted with a red border. The "PsExec Service (32 bit)" task is highlighted with a red rectangle. The "End task" button is visible at the bottom right.

Name	Status	7% CPU	65% Memory	100% Disk	0% 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 TextInput 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.

The screenshot shows the Windows Event Viewer interface. The left pane displays a tree view of logs: Custom Views, Windows Logs (selected), Application, Security, Setup, System (highlighted with a red box), Forwarded Events, Applications and Services Log, and Subscriptions. The right pane shows a table of events under the 'System' log, with a total of 1,129 events. One specific event is highlighted with a red box:

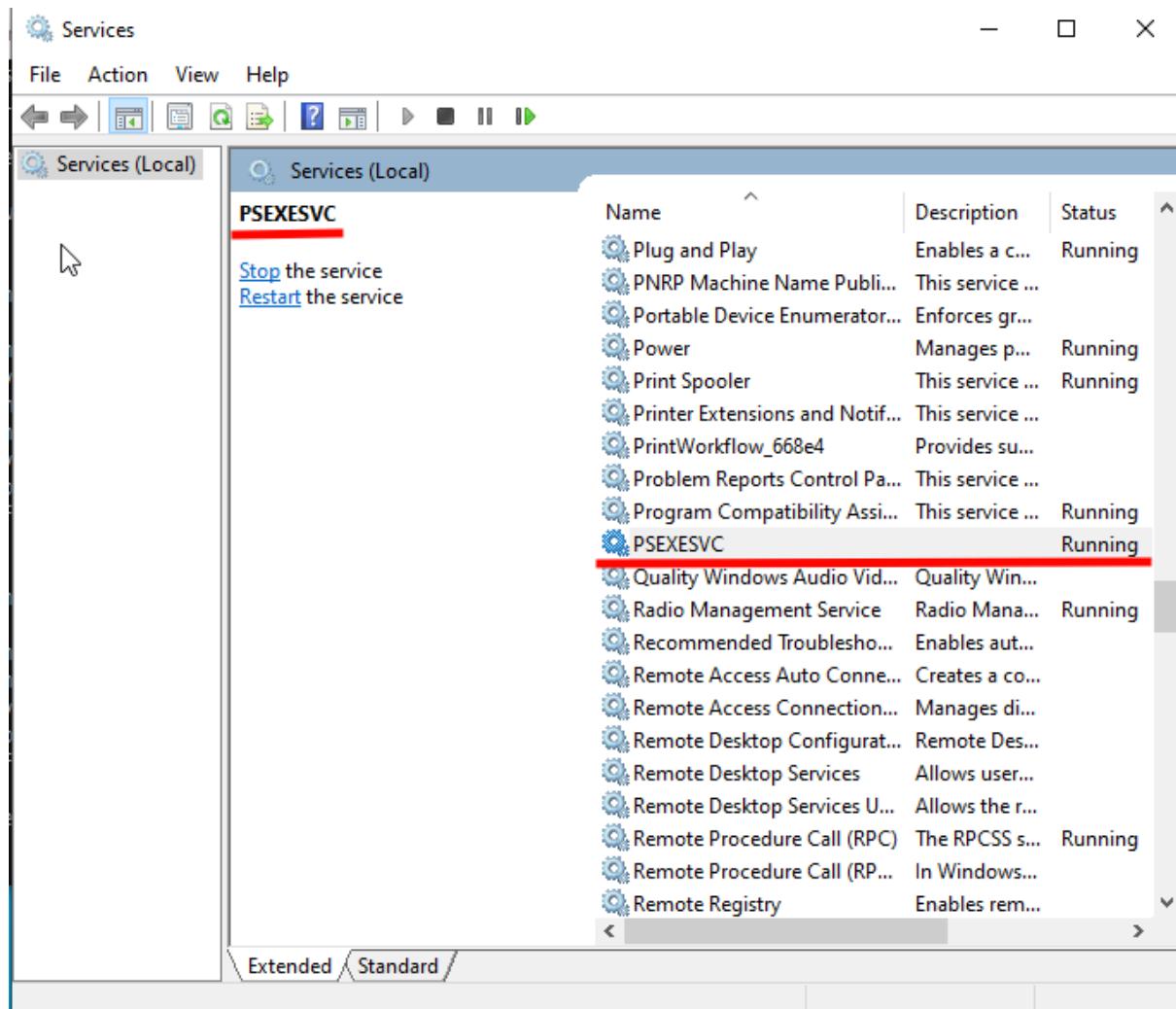
Level	Date and Time	Source	Event ID	Task Ca...
Information	1/10/2026 11:15:42 AM	Windo...	44	Wind...
Information	1/10/2026 11:16:41 AM	Service...	7040	None
Information	1/10/2026 11:19:49 AM	Service...	7040	None
Information	1/10/2026 11:19:56 AM	Service...	7045	None
Information	1/10/2026 11:23:29 AM	Windo...	19	Wind...
Information	1/10/2026 11:23:37 AM	Windo...	44	Wind...
Information	1/10/2026 11:24:19 AM	Kernel...	16	None
Information	1/10/2026 11:36:10 AM	Kernel...	16	None

A detailed view of the selected event (Event ID 7045) is shown in the bottom window. The 'General' tab is selected, displaying the following information:

A service was installed in the system.
Service Name: PSEXESVC
Service File Name: %SystemRoot%\PSEXESVC.exe
Service Type: user mode service
Service Start Type: demand start
Service Account: LocalSystem

Log Name: System
Source: Service Control Manager
Event ID: 7045
Level: Information
User: DESKTOP-IF4A42K\Administ
OpCode: Info
More Information: [Event Log Online Help](#)

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



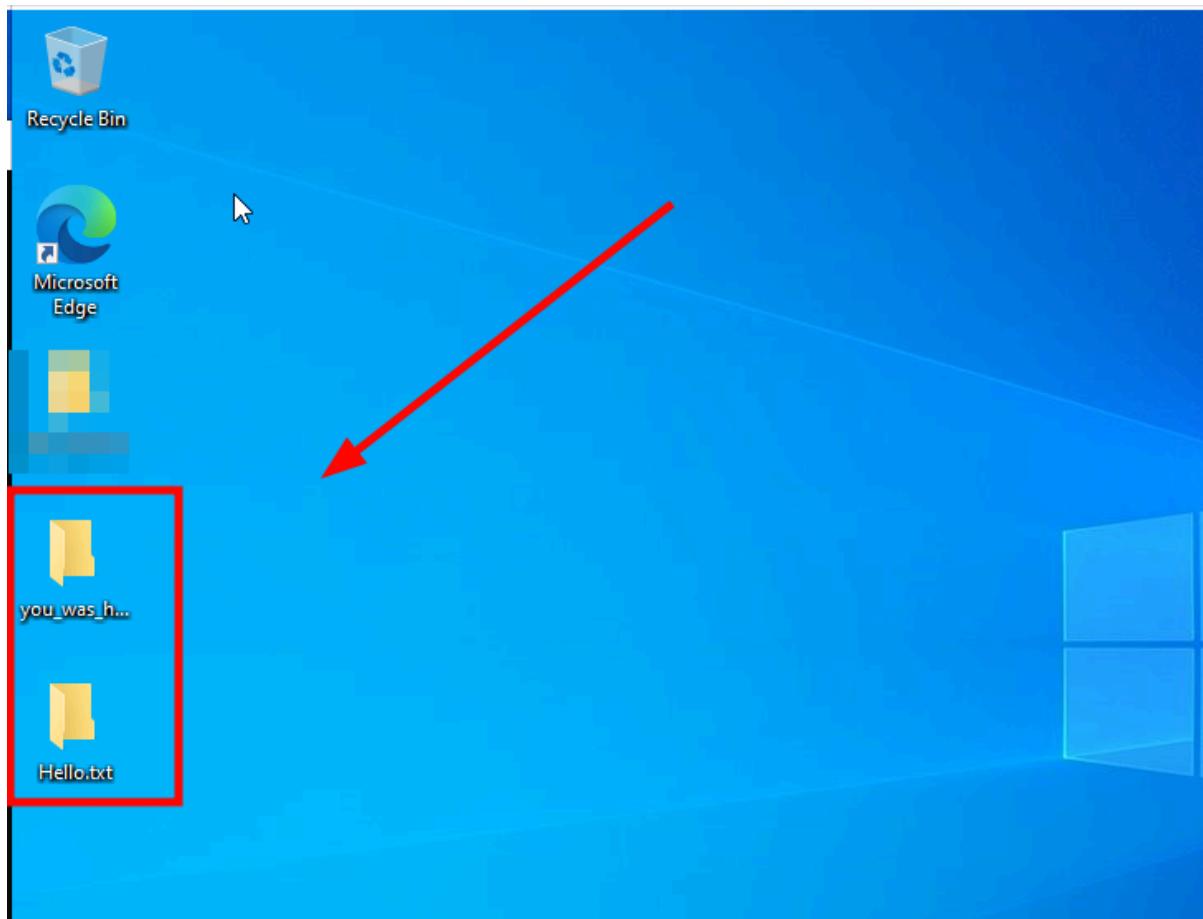
If we press the win + r and write service.msc, we can check the PSEXESVC running.

```
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.

The screenshot shows the 'Agents' section of the Fleet interface. On the left sidebar, under 'Assets', 'Agents' is selected. The main area displays a table of agents with two entries:

Status	Host	Agent policy	CPU	Memory	Last activ...	Version	Actions
Healthy	DESKTOP-AGAIJ1A	Agent policy 1 rev. 2	N/A	N/A	21 seconds ago	9.2.3	...
Healthy	brandon-HP-EliteDesk	Agent policy 1 rev. 2	2.83 %	255 MB	30 seconds ago	9.2.3	...

At the bottom, there are buttons for 'Ingest Overview Metrics', 'Agent Info Metrics', 'Agent activity', and 'Add agent'. A message at the top right says: 'We've added new privileges that let you define more granularly who can view or edit Fleet agents, policies, and settings. Learn more.' with a 'Give feedback' link.

Lets start installing the agent in the machine target.

The screenshot shows the 'Agent details' page for the host 'DESKTOP-AGAIJ1A'. The left sidebar has 'Agents' selected. The main area is divided into 'Overview' and 'Integrations' sections.

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.

tradutor - Pro X Correio – bra X Comando cri X Download An X secure.eicar.o X como desativ X +

https://www.eicar.org/download-anti-malware-testfile/ +49 8194 99 84 99 CONTACT

eicar

DOWNLOAD AREA

using the secure, SSL enabled protocol HTTPS

EICAR.COM	EICAR.COM.TXT	EICAR.COM.ZIP	EICAR.COM-2.ZIP
Com-file 68 Bytes	1 Text-file 68 Bytes	1 Zip-file 184 Bytes	1 Zip-file 308 Bytes
DOWNLOAD	DOWNLOAD	DOWNLOAD	DOWNLOAD

Activate Windows Go to Settings to activate Windows.

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.

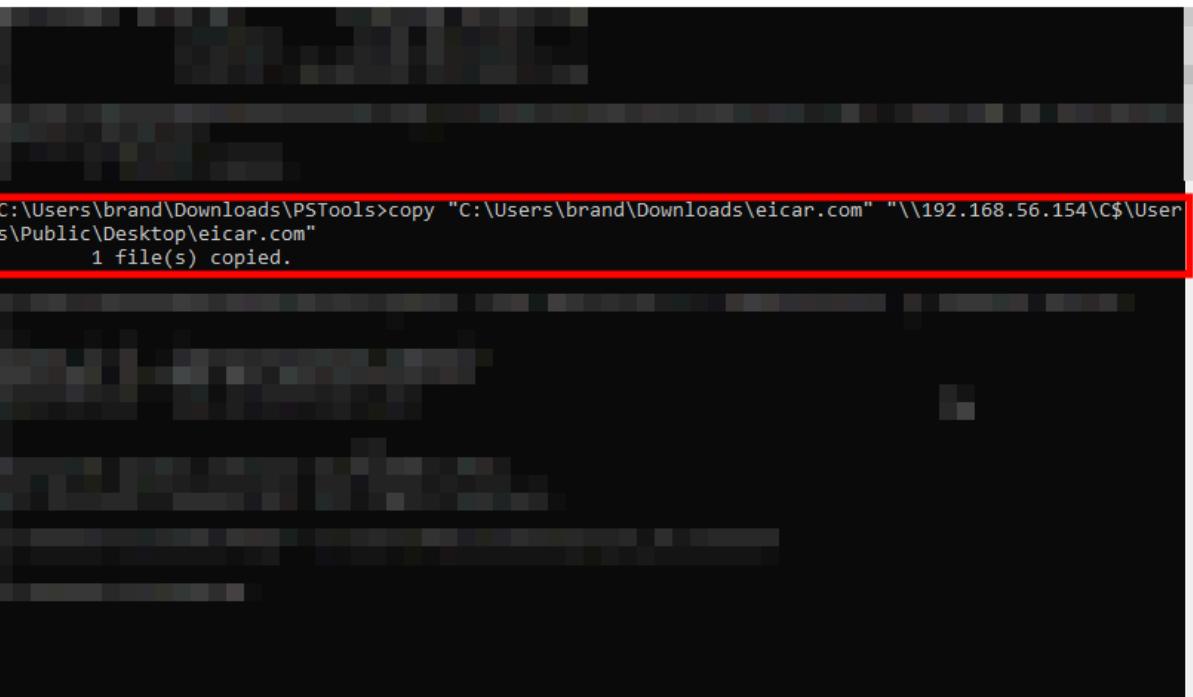
File Home Share View Manage Downloads

This PC > Downloads

Search Downloads

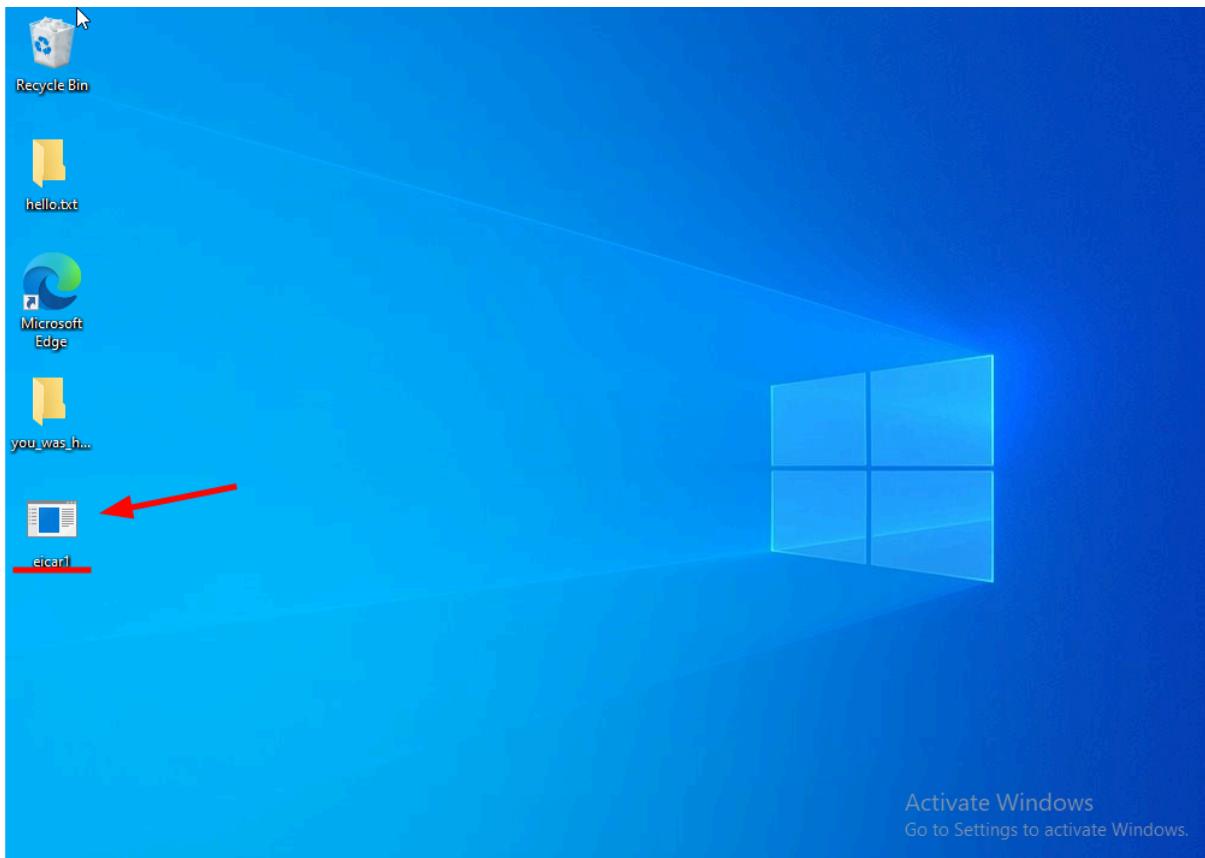
Name	Date modified	Type	Size
PSTools	1/11/2026 7:42 PM	Compressed (zipp...)	5,159 KB
eicar	1/11/2026 4:37 PM	MS-DOS Application	1 KB
PSTools	1/11/2026 7:42 PM	File folder	

It is here, in the downloads.

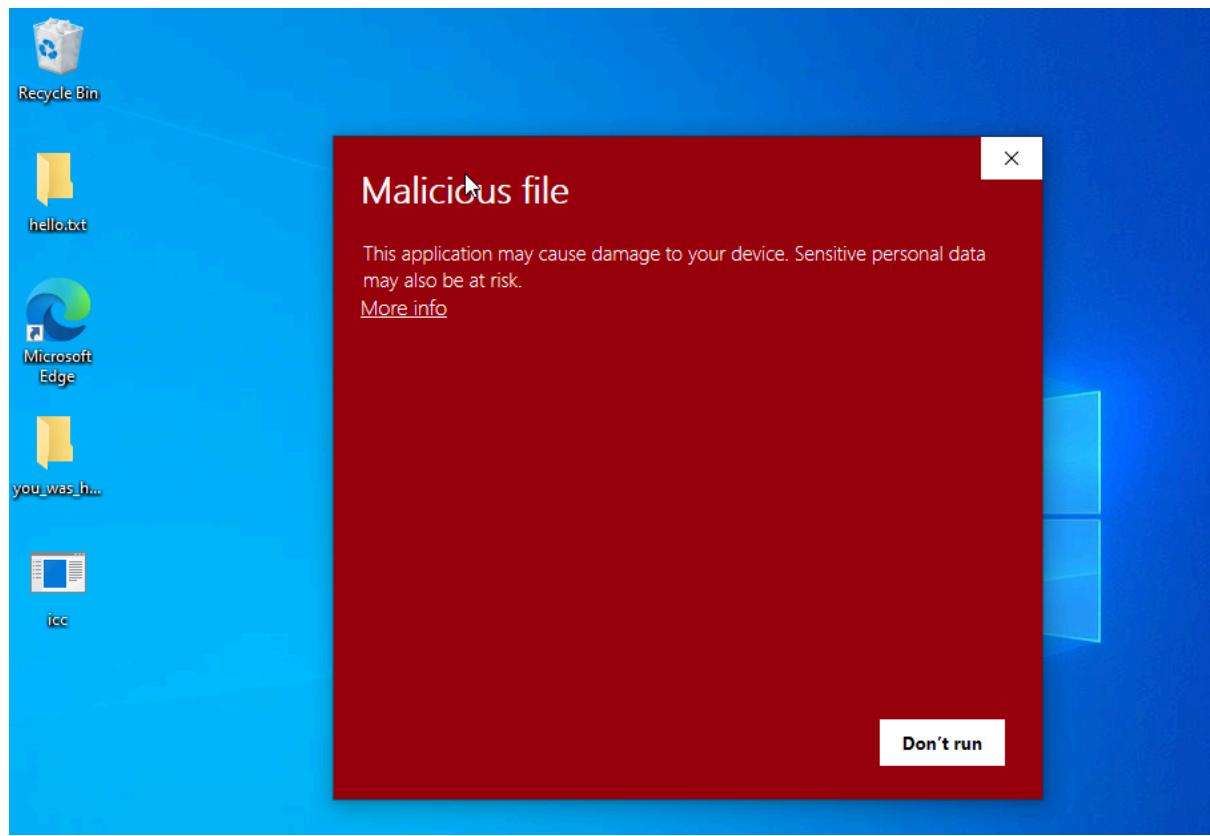


```
C:\Users\brand\Downloads\PSTools>copy "C:\Users\brand\Downloads\eicar.com" "\\192.168.56.154\C$\Users\Public\Desktop\eicar.com"
1 file(s) copied.
```

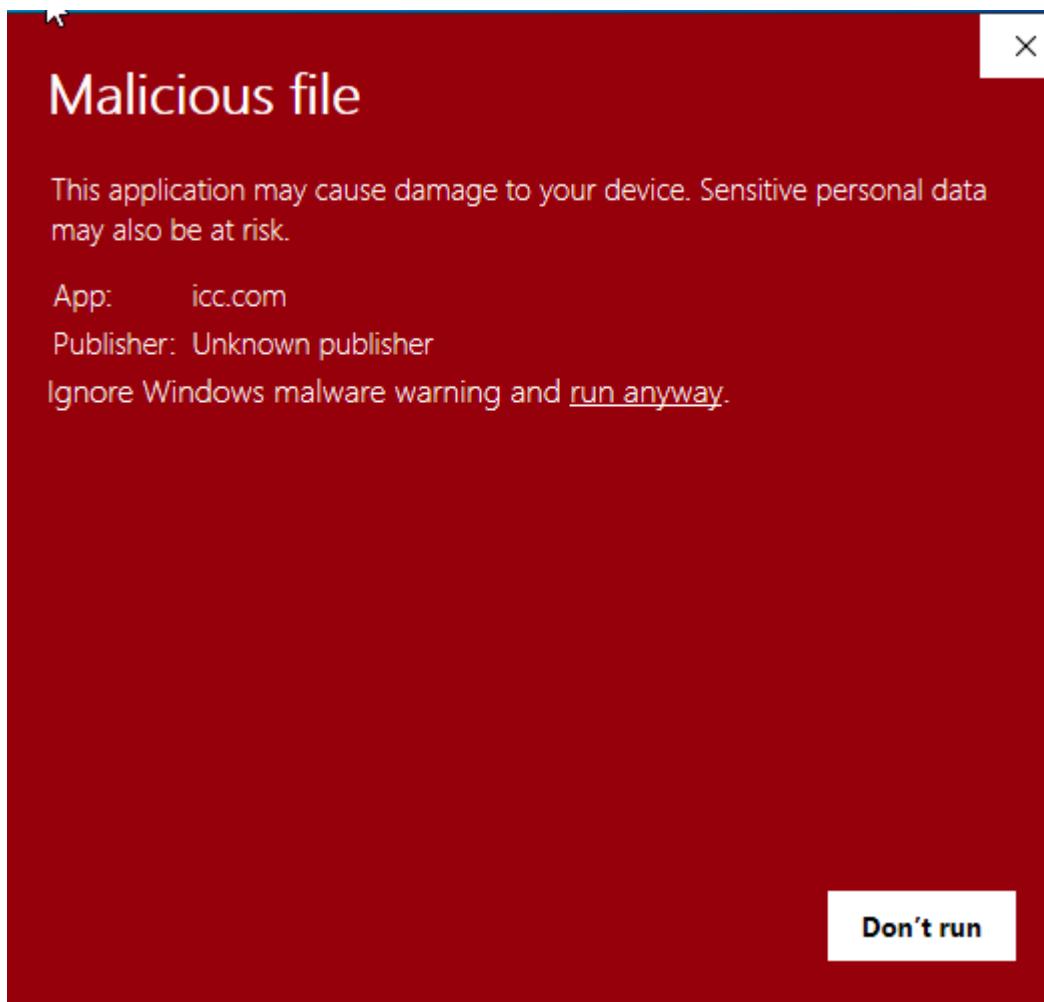
Now, we have to do this command to send this eicar test file to our target.



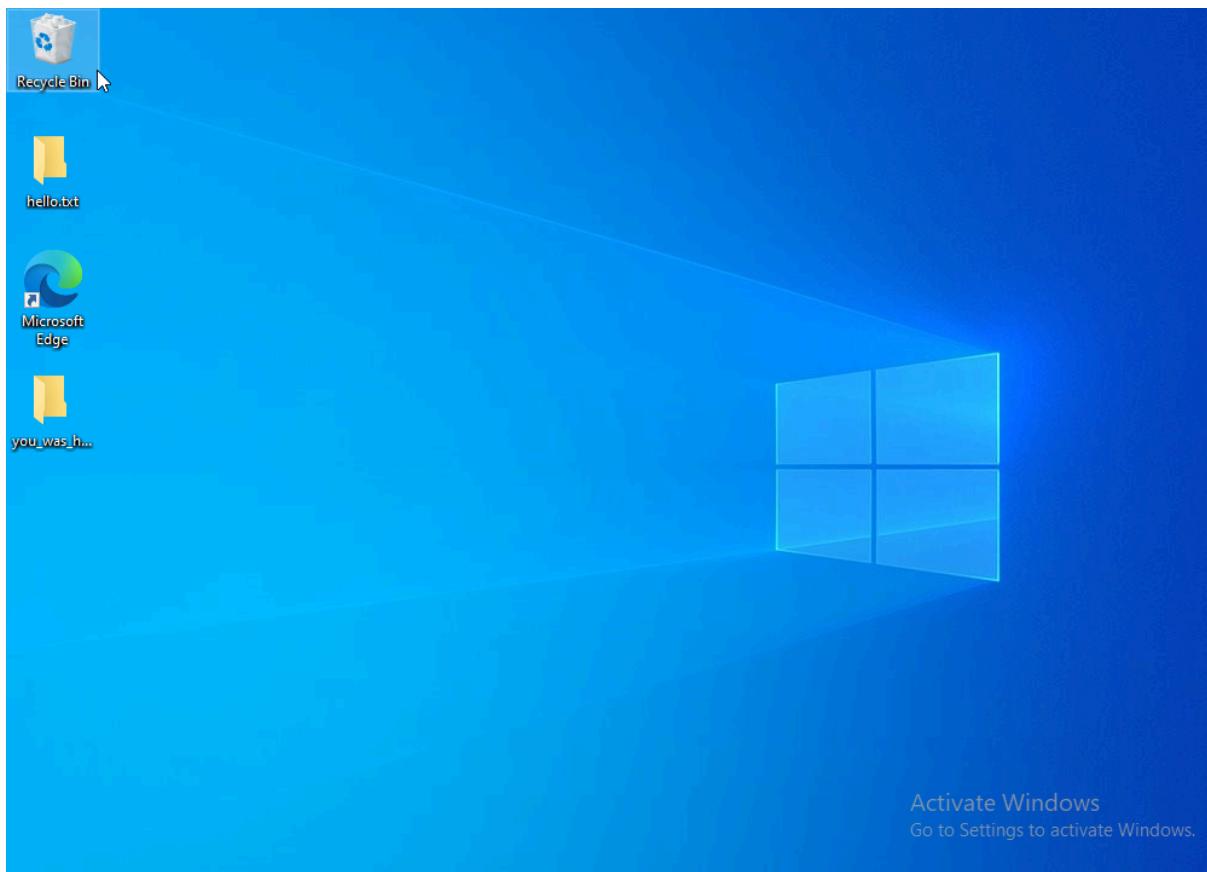
Now, in the target machine, we can see the Eicar file.



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



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



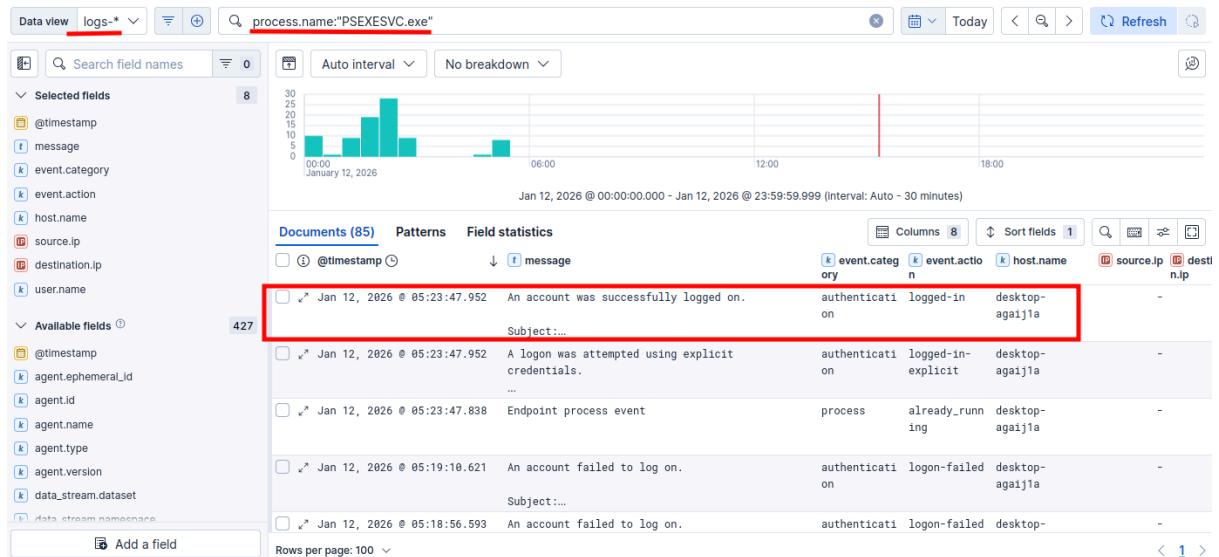
It was deleted.

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

A screenshot of the Elasticsearch alerting interface. The left sidebar shows navigation options: Discover, Dashboards, Rules, Alerts (selected), Attack recovery, and More. The main area displays three panels: 'Severity levels' (9 alerts, circled with red number 2), 'Alerts by name' (Malware Prevention Alert, circled with red number 3), and 'Top alerts by' (host.name: desktop-agalita, circled with red number 1). Below these is a table of alerts with columns: Actions, @timestamp, Rule, Assignees, Severity, Risk Score, and Reason. The first two rows are circled with red number 4.

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.