AW SECURITY

IT'S YOUR SECURITY, SO TAKE CONTROL </>

Alziro Walter Nardo

Cybersecurity Executive

Ethical Hacker

Cybersecurity Engineer

Santa Maria – RS Brasil November 14th, 2024

Introduction:

I would like to point out that the failure was found in the company where I work, Coca-Cola FEMSA, and I work as a Cybersecurity Executive, but the report will be made personally. I will leave my corporate contacts. However, credits and/or payments must be made personally.

Confidentiality Notice

This report contains sensitive, privileged, and confidential information. Precautions should be taken to protect the confidentiality of the information in this document. Publication of this report may cause reputational damage to or facilitate attacks against CyberArk. Alziro Walter Nardo shall not be held liable for special, incidental, collateral, or consequential damages arising out of the use of this information.

CLASSIFICATION DEFINITIONS

Risk Classifications

Level	Score	Description
Critical	10	The vulnerability poses an immediate threat to the organization. Successful exploitation may permanently affect the organization. Remediation should be immediately performed.
High	7-9	The vulnerability poses an urgent threat to the organization, and remediation should be prioritized.
Medium	4-6	Successful exploitation is possible and may result in notable disruption of business functionality. This vulnerability should be remediated when feasible.
Low	1-3	The vulnerability poses a negligible/minimal threat to the organization. The presence of this vulnerability should be noted and remediated if possible.
Informational	0	These findings have no clear threat to the organization, but may cause business processes to function differently than desired or reveal sensitive information about the company.

Exploitation Likelihood Classifications

Likelihood	Description
Likely	Exploitation methods are well-known and can be performed using publicly available tools. Low-skilled attackers and automated tools could successfully exploit the vulnerability with minimal difficulty.
Possible	Exploitation methods are well-known, may be performed using public tools, but require configuration. Understanding of the underlying system is required for successful exploitation.
Unlikely	Exploitation requires deep understanding of the underlying systems or advanced technical skills. Precise conditions may be required for successful exploitation.

Business Impact Classifications

Impact	Description
Major	Successful exploitation may result in large disruptions of critical business functions across the organization and significant financial damage.
Moderate	Successful exploitation may cause significant disruptions to non-critical business functions.
Minor	Successful exploitation may affect few users, without causing much disruption to routine business functions.

Example Vulnerability Finding

HIGH RISK (8/10)	
Exploitation Likelihood	**Possible**
Business Impact	**Severe**

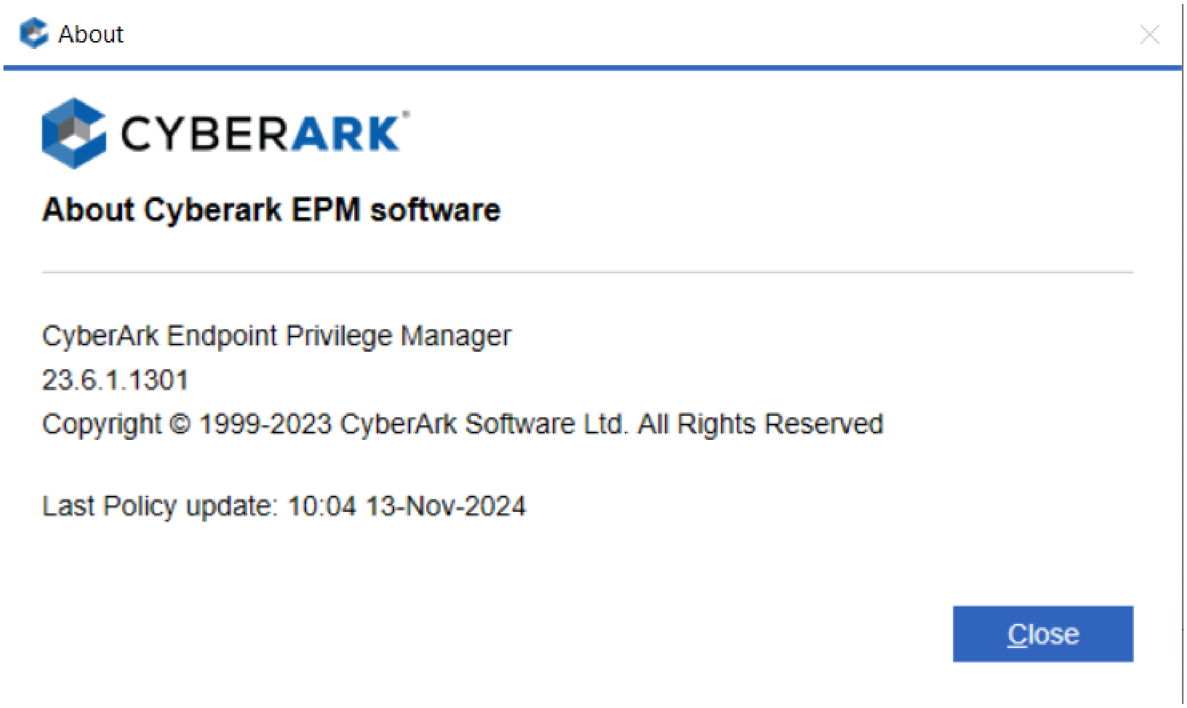
Security Implications

This is where you give a 1-2 sentence description about the major impact of the finding. This finding is very important because it can destroy the entire business if left unchecked.

Analysis

Hello CyberArk security team,

During an activity at the company where I work (Coca-Cola FEMSA) I needed to install Kali-Linux to perform some pentests. The corporate laptop has CyberArk EPM version 23.6.1.1301

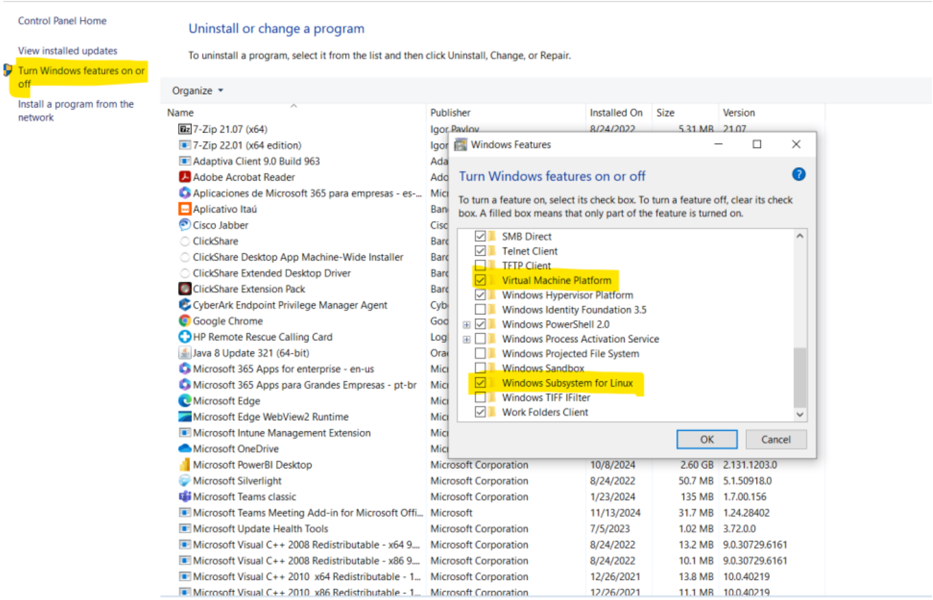


About Cyberark EPM software

CyberArk Endpoint Privilege Manager
23.6.1.1301
Copyright © 1999-2023 CyberArk Software Ltd. All Rights Reserved

Last Policy update: 10:04 13-Nov-2024

To do this, you need to activate the WSL feature in the operating system:


Control Panel Home
View installed updates
Turn Windows features on or off
Install a program from the network
Organize ▾

Uninstall or change a program

To uninstall a program, select it from the list and then click Uninstall, Change, or Repair.

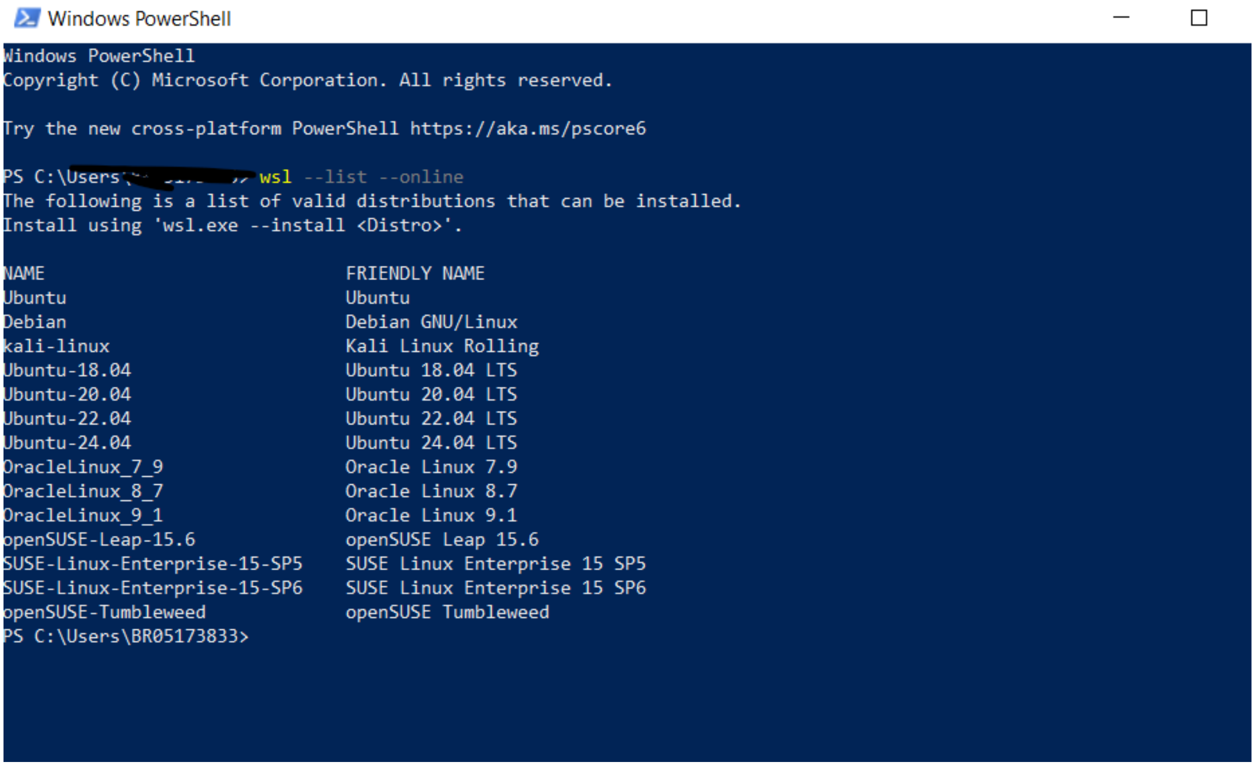
Name	Publisher	Installed On	Size	Version
7-Zip 21.07 (x64)	Igor Pavlov	8/24/2022	5.31 MB	21.07
7-Zip 22.01 (x64 edition)	Igor			
Adaptiva Client 9.0 Build 963	Ada			
Adobe Acrobat Reader	Ado			
Aplicaciones de Microsoft 365 para empresas - es-...	Mic			
Aplicativo Itaú	Ban			
Cisco Jabber	Cisc			
ClickShare	Barc			
ClickShare Desktop App Machine-Wide Installer	Barc			
ClickShare Extended Desktop Driver	Barc			
ClickShare Extension Pack	Barc			
CyberArk Endpoint Privilege Manager Agent	Cyb			
Google Chrome	Goo			
HP Remote Rescue Calling Card	Log			
Java 8 Update 321 (64-bit)	Ora			
Microsoft 365 Apps for enterprise - en-us	Mic			
Microsoft 365 Apps para Grandes Empresas - pt-br	Mic			
Microsoft Edge	Mic			
Microsoft Edge WebView2 Runtime	Mic			
Microsoft Intune Management Extension	Mic			
Microsoft OneDrive	Mic			
Microsoft PowerBI Desktop	Microsoft Corporation	10/8/2024	2.60 GB	2.131.1203.0
Microsoft Silverlight	Microsoft Corporation	8/24/2022	50.7 MB	5.1.50918.0
Microsoft Teams classic	Microsoft Corporation	1/23/2024	135 MB	1.7.00.156
Microsoft Teams Meeting Add-in for Microsoft Offi...	Microsoft	11/13/2024	31.7 MB	1.24.28402
Microsoft Update Health Tools	Microsoft Corporation	7/5/2023	1.02 MB	3.72.0.0
Microsoft Visual C++ 2008 Redistributable - x64 9....	Microsoft Corporation	8/24/2022	13.2 MB	9.0.30729.6161
Microsoft Visual C++ 2008 Redistributable - x86 9....	Microsoft Corporation	8/24/2022	10.1 MB	9.0.30729.6161
Microsoft Visual C++ 2010 x64 Redistributable - 1...	Microsoft Corporation	12/26/2021	13.8 MB	10.0.40219
Microsoft Visual C++ 2010 x86 Redistributable - 1...	Microsoft Corporation	12/26/2021	11.1 MB	10.0.40219

Turn Windows features on or off

To turn a feature on, select its check box. To turn a feature off, clear its check box. A filled box means that only part of the feature is turned on.

- ☑ SMB Direct
- ☑ Telnet Client
- □ TFTP Client
- ☑ Virtual Machine Platform
- ☑ Windows Hypervisor Platform
- □ Windows Identity Foundation 3.5
- ☑ Windows PowerShell 2.0
- □ Windows Process Activation Service
- □ Windows Projected File System
- □ Windows Sandbox
- ☑ Windows Subsystem for Linux
- □ Windows TIFF IFilter
- ☑ Work Folders Client

In powershell, you need to install the WSL instance or some Linux distribution:



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

Try the new cross-platform PowerShell https://aka.ms/pscore6

PS C:\Users[redacted] wsl --list --online
The following is a list of valid distributions that can be installed.
Install using 'wsl.exe --install <Distro>'.

NAME                            FRIENDLY NAME
Ubuntu                          Ubuntu
Debian                          Debian GNU/Linux
kali-linux                      Kali Linux Rolling
Ubuntu-18.04                    Ubuntu 18.04 LTS
Ubuntu-20.04                    Ubuntu 20.04 LTS
Ubuntu-22.04                    Ubuntu 22.04 LTS
Ubuntu-24.04                    Ubuntu 24.04 LTS
OracleLinux_7_9                 Oracle Linux 7.9
OracleLinux_8_7                 Oracle Linux 8.7
OracleLinux_9_1                 Oracle Linux 9.1
openSUSE-Leap-15.6              openSUSE Leap 15.6
SUSE-Linux-Enterprise-15-SP5    SUSE Linux Enterprise 15 SP5
SUSE-Linux-Enterprise-15-SP6    SUSE Linux Enterprise 15 SP6
openSUSE-Tumbleweed             openSUSE Tumbleweed
PS C:\Users\BR05173833>
```

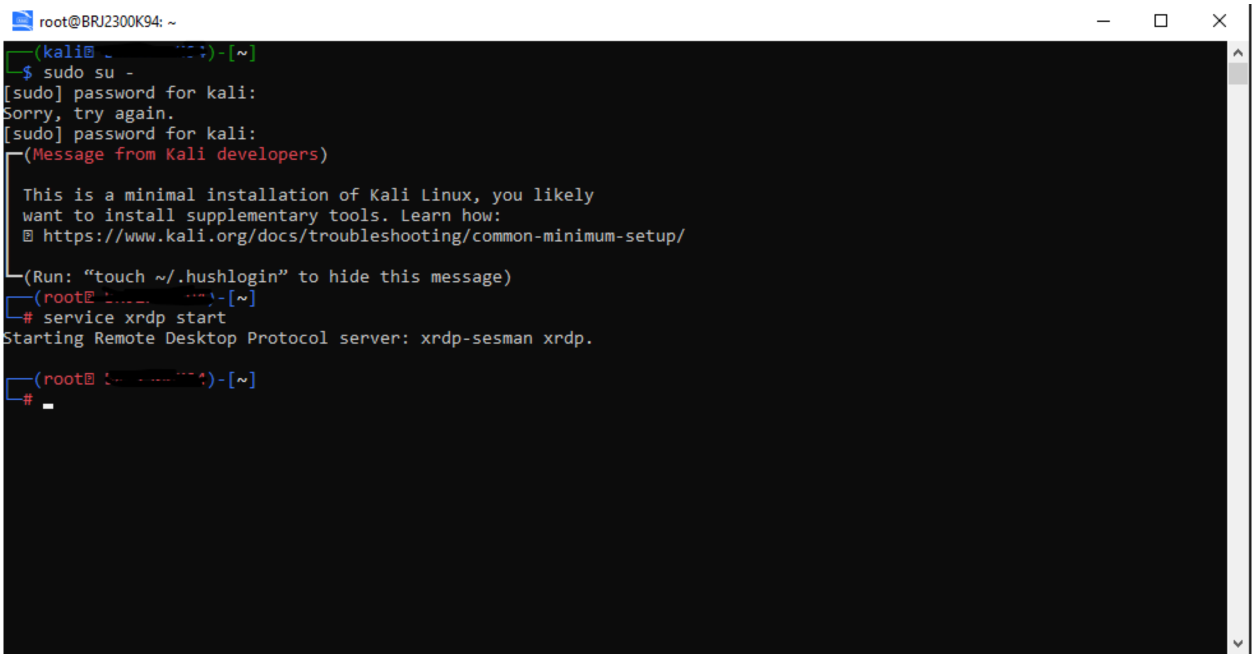
With the installation ready, it is necessary to configure the Linux instance to be accessed remotely:

# apt update && apt full-updrade -y

#apt install Kali-desktop-xfce -y

#apt install xrdp -y

#service xdrp start



root@BRJ2300K94: ~

```
┌──(kali⊠[redacted])-[~]
└─$ sudo su -
[sudo] password for kali:
Sorry, try again.
[sudo] password for kali:
┌──(Message from Kali developers)
│
│ This is a minimal installation of Kali Linux, you likely
│ want to install supplementary tools. Learn how:
│ ⊠ https://www.kali.org/docs/troubleshooting/common-minimum-setup/
│
└─(Run: “touch ~/.hushlogin” to hide this message)
┌──(root⊠[redacted])-[~]
└─# service xrdp start
Starting Remote Desktop Protocol server: xrdp-sesman xrdp.

┌──(root⊠[redacted])-[~]
└─# ▂
```

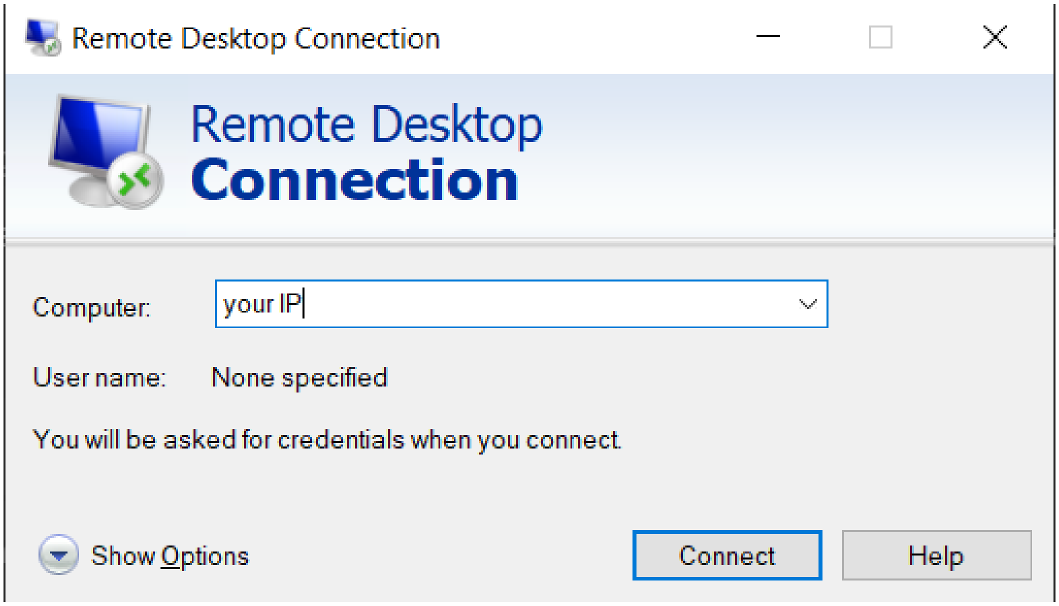
After that, it is necessary to check the IP of the Linux instance:

#ifconfig

Using the instance's IP, it is possible to connect VIA MSTSC.exe from Windows.

With this, it is possible to configure software and in the same way access it through Windows.

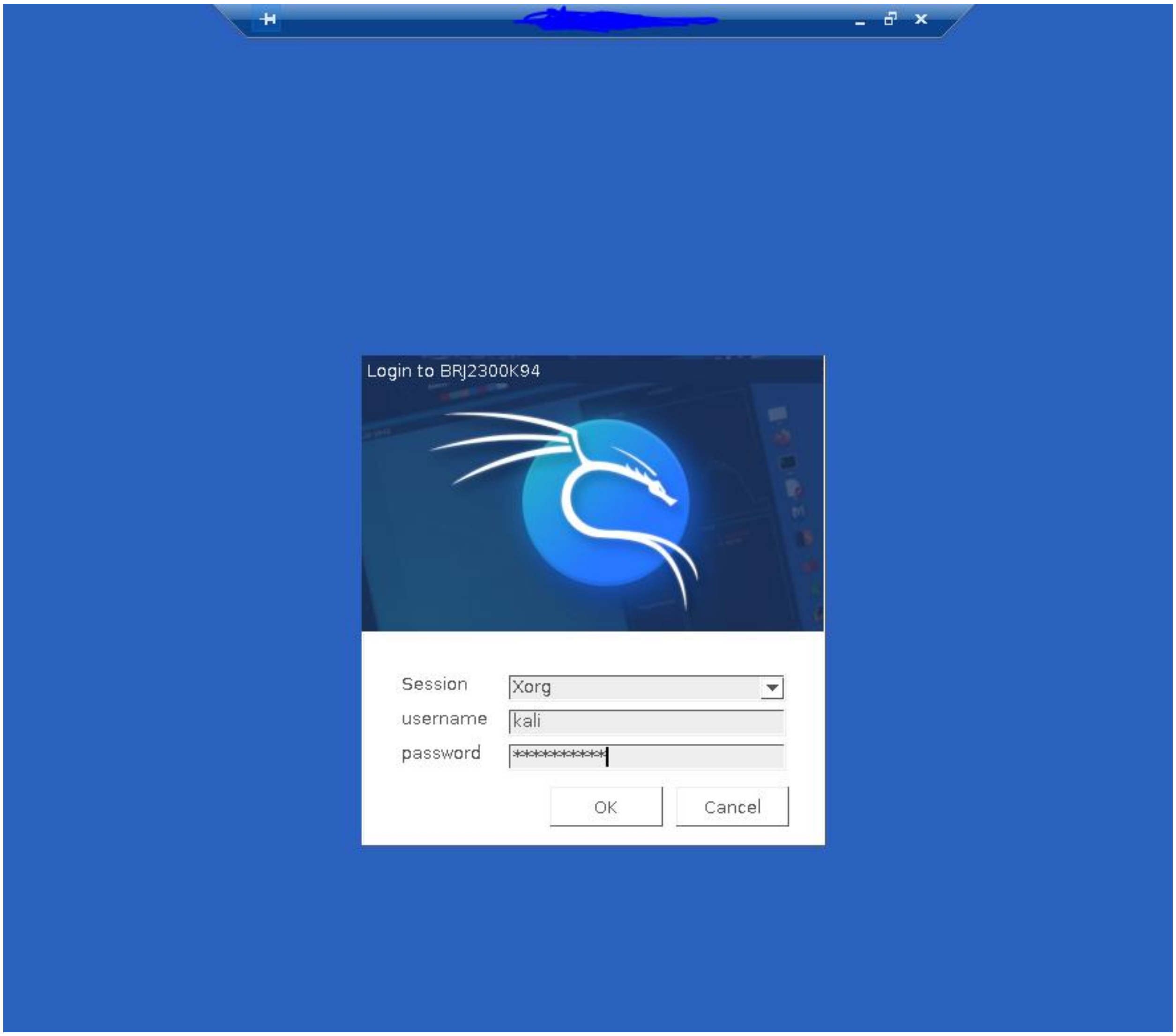
By passing the control of the EPM.



Computer: your IP

User name: None specified

You will be asked for credentials when you connect.



[redacted]

Login to BRJ2300K94

Session: Xorg

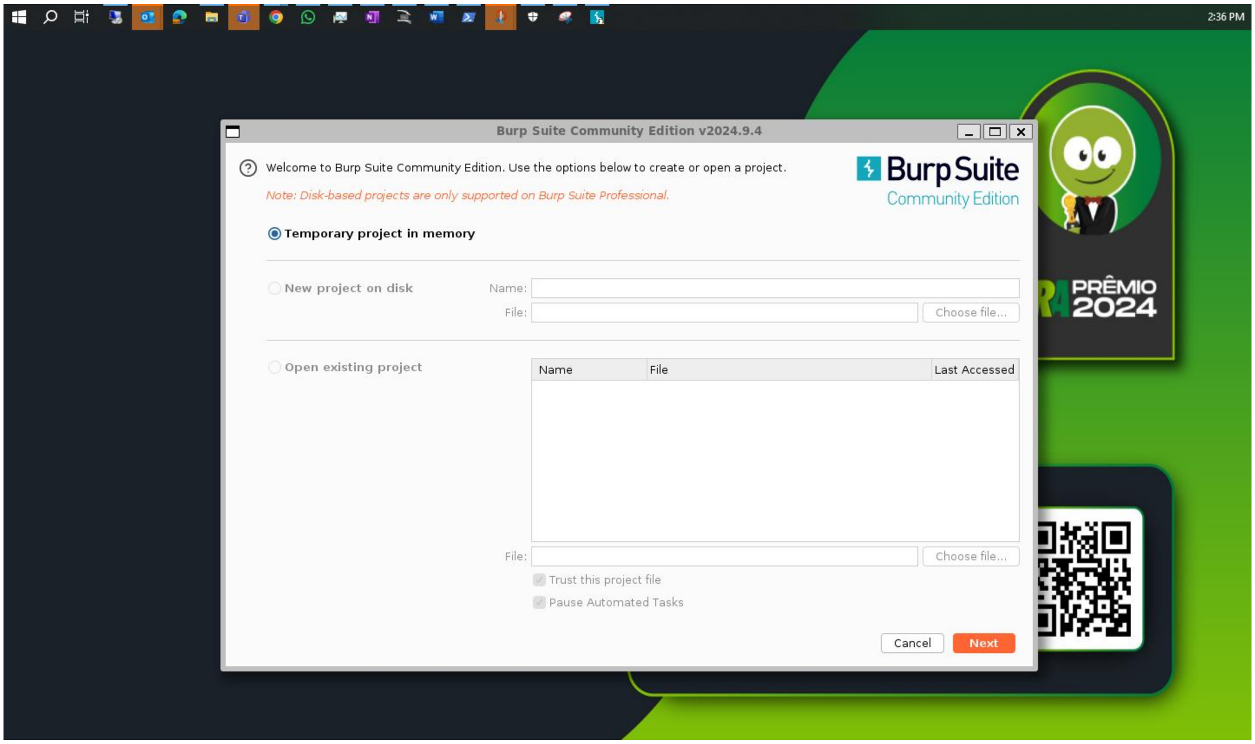
username: kali

password: ***********

With this, I formally report a vulnerability or perhaps a misconfiguration, where it is possible to bypass the CyberArk EPM controls for software installation, where users can activate and install WSL (Windows Subsystem for Linux), in which the attacker with access to the user's equipment can install and activate the Windows feature, and then start and install the tools they need, and can open it on the system itself.

With this, it is possible to initiate RECON, Exfiltration, and Vulnerability analysis and brute force attacks, etc.

Burpsuite:



Burp Suite Community Edition v2024.9.4

Welcome to Burp Suite Community Edition. Use the options below to create or open a project.

Note: Disk-based projects are only supported on Burp Suite Professional.

● **Temporary project in memory**

○ New project on disk — Name: — File: — Choose file...

○ Open existing project

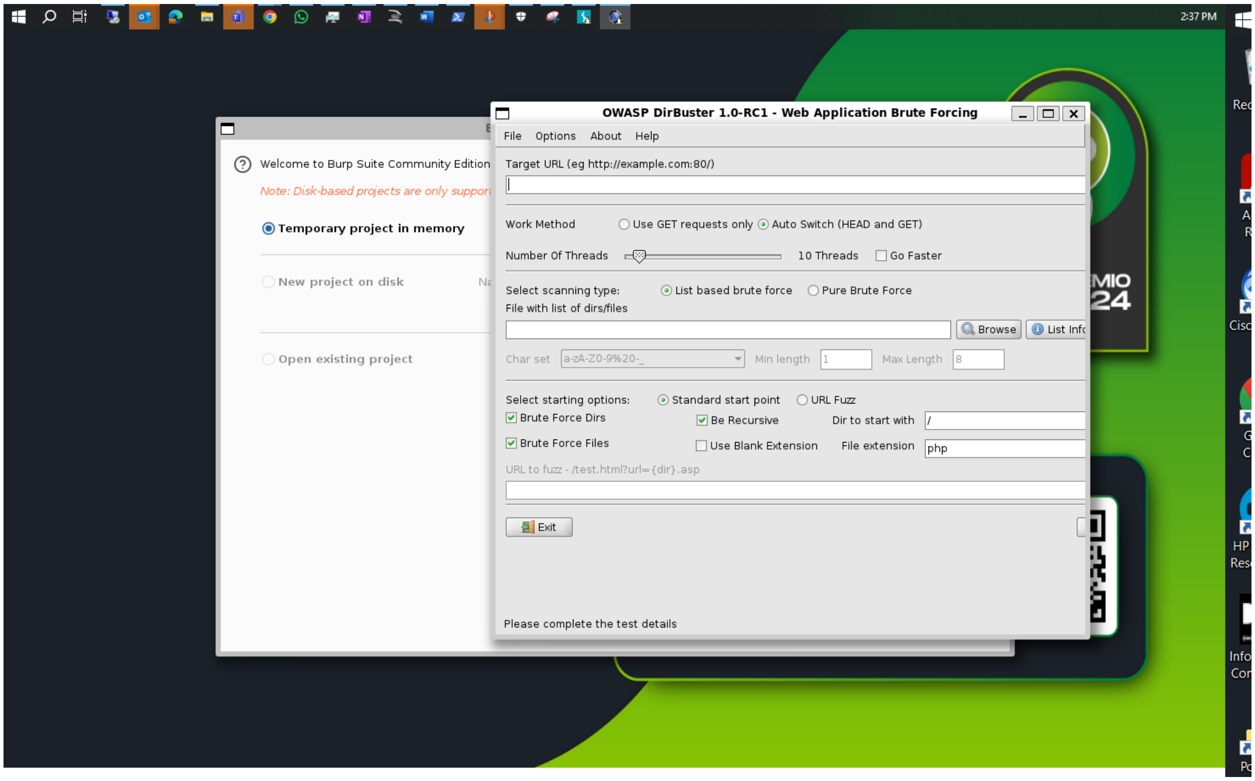
Name	File	Last Accessed

File: — Choose file...

☑ Trust this project file

☑ Pause Automated Tasks

Dirbuster:



OWASP DirBuster 1.0-RC1 - Web Application Brute Forcing

Target URL (eg http://example.com:80/)

Work Method ○ Use GET requests only ● Auto Switch (HEAD and GET)

Number Of Threads 10 Threads □ Go Faster

Select scanning type: ● List based brute force ○ Pure Brute Force

File with list of dirs/files

Char set a-zA-Z0-9%20-_ Min length 1 Max Length 8

Select starting options: ● Standard start point ○ URL Fuzz

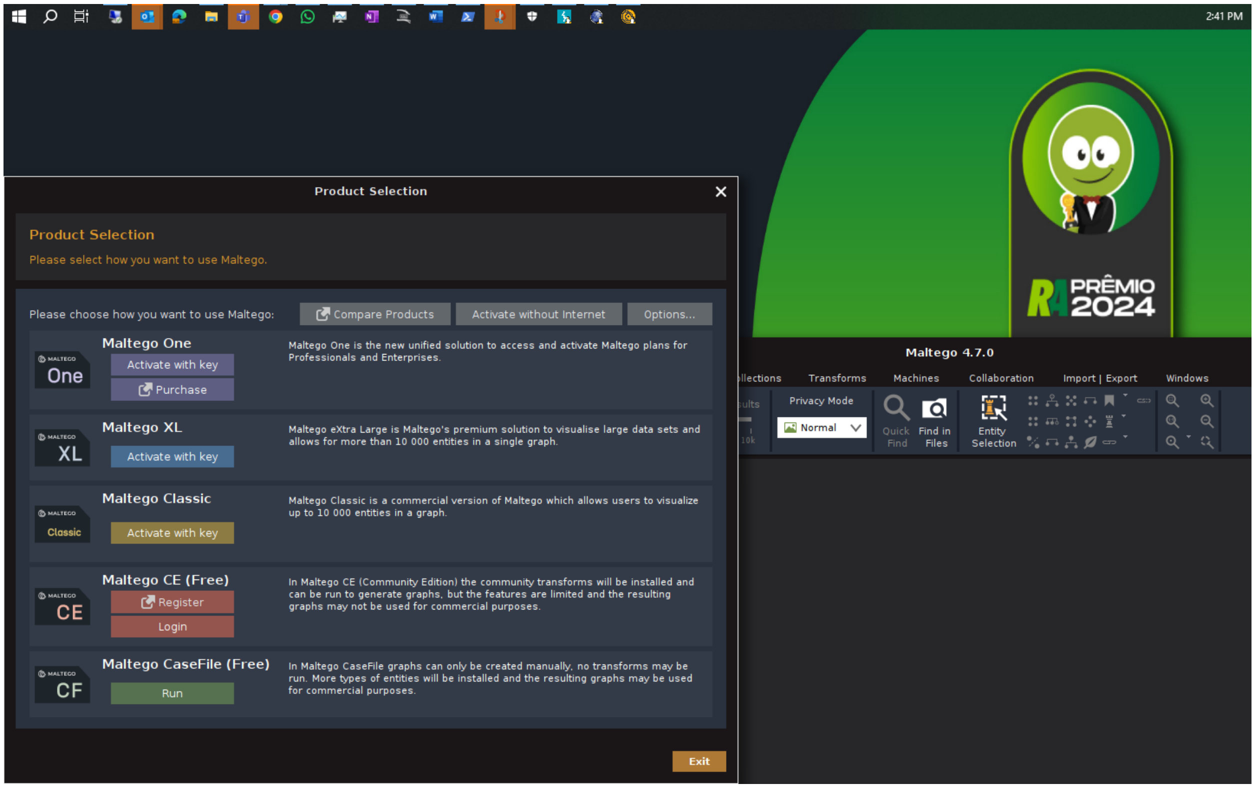
☑ Brute Force Dirs ☑ Be Recursive Dir to start with /

☑ Brute Force Files □ Use Blank Extension File extension php

URL to fuzz - /test.html?url={dir}.asp

Please complete the test details

Maltego:



Product Selection

Product Selection

Please select how you want to use Maltego.

Please choose how you want to use Maltego:

Maltego One

Maltego One is the new unified solution to access and activate Maltego plans for Professionals and Enterprises.

Maltego XL

Maltego eXtra Large is Maltego's premium solution to visualise large data sets and allows for more than 10 000 entities in a single graph.

Maltego Classic

Maltego Classic is a commercial version of Maltego which allows users to visualize up to 10 000 entities in a graph.

Maltego CE (Free)

In Maltego CE (Community Edition) the community transforms will be installed and can be run to generate graphs, but the features are limited and the resulting graphs may not be used for commercial purposes.

Maltego CaseFile (Free)

In Maltego CaseFile graphs can only be created manually, no transforms may be run. More types of entities will be installed and the resulting graphs may be used for commercial purposes.

Recommendations:

- Understand with Microsoft how these processes can be mapped.
- **Map subsystem processes to ensure full protection coverage and visibility.**

Version Information

Version	Date	Description
1.0	14/11/2024	Report Bypass CyberArk EPM

Contact Information

Name	Alziro Walter Nardo
Address	Rua Arlindo Noal, 272 São João, Santa Maria, Rio G.D. Sul - Brasil
Phone	+5555996413443 - Personal / Corporative - +5555991337267
Email	Personal - alziropercu@gmail.com / walter.nardo@kof.com.mx - Corporative
LinkedIn page	https://www.linkedin.com/in/alziroawn/