



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:

All the study done, is on the version of the Agent mentioned in the report. The entire process of communicating with CyberArk was followed. This report is intended to provide technical support to everyone on Bypass. So, you can protect your environment effectively.



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

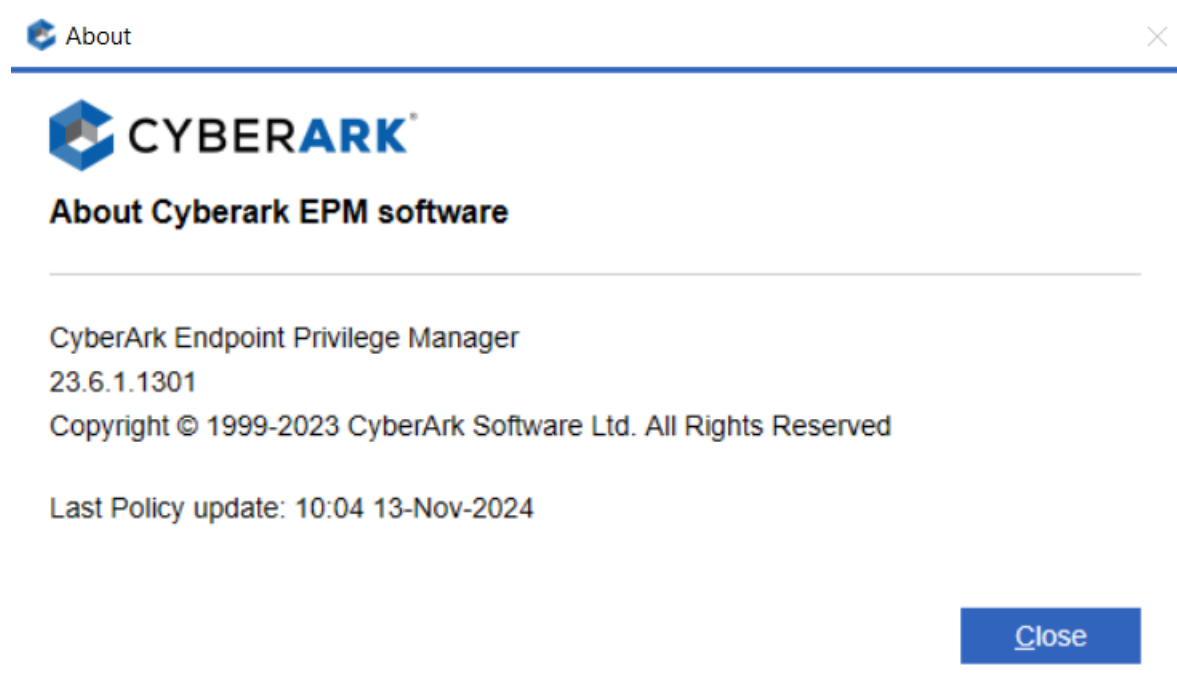
Security Implications

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.

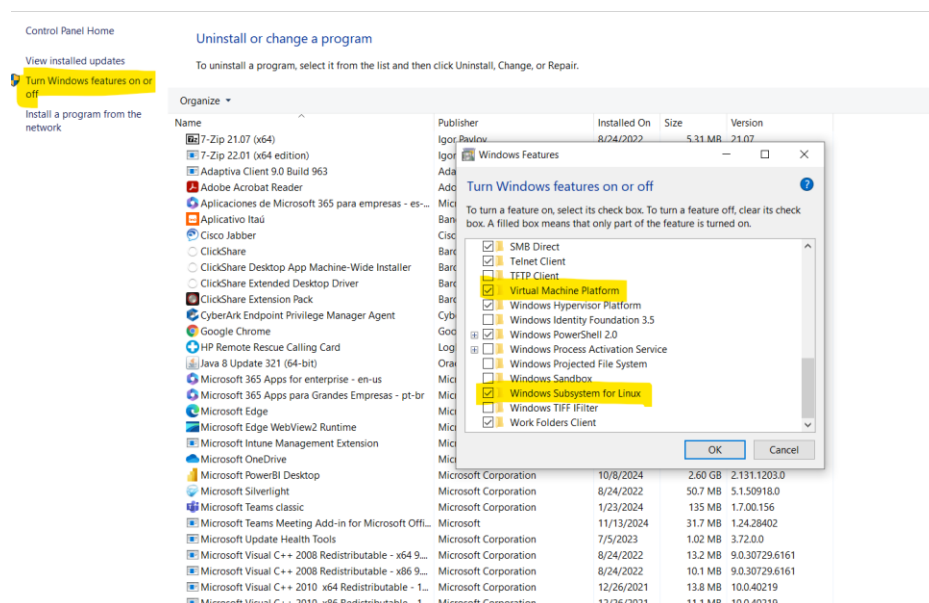
Analysis

Hello CyberArk security team,

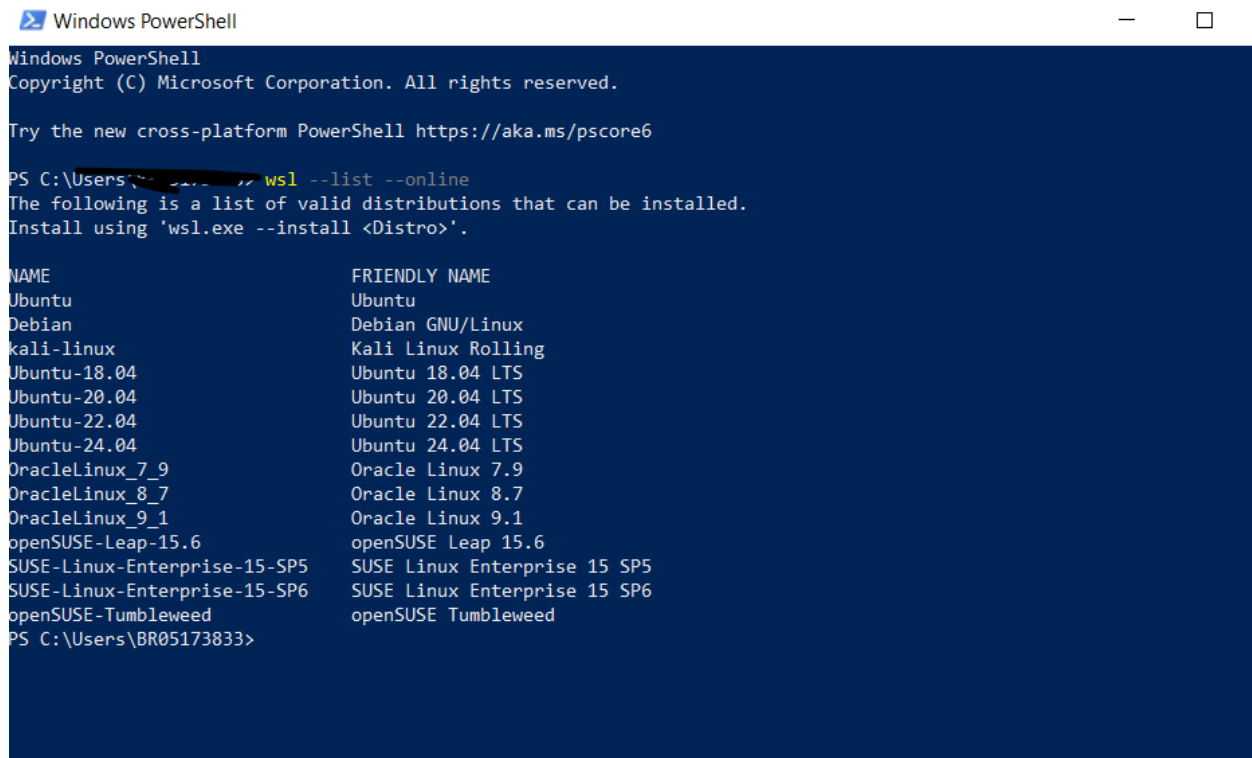
During an activity at the company where I work (Coca-Cola FEMSA) I needed to install Kali-Linux to perform some pentests. The corporate laptop has CyberArk EPM version 23.6.1.1301



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



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

A screenshot of a Windows PowerShell terminal window. The title bar says "Windows PowerShell". The terminal text shows the command 'wsl --list --online' being executed, which lists various Linux distributions available for installation. The list includes Ubuntu, Debian, Kali Linux, Oracle Linux, and openSUSE in both standard and friendly names.

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

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

PS C:\Users\BR05173833> 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-upgrade -y
#apt install Kali-desktop-xfce -y
#apt install xrdp -y
#service xdrp start
```

```
root@BRJ2300K94: ~  
[kali@ ~]# 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@ ~]# service xrdp start  
Starting Remote Desktop Protocol server: xrdp-sesman xrdp.  
[root@ ~]#
```

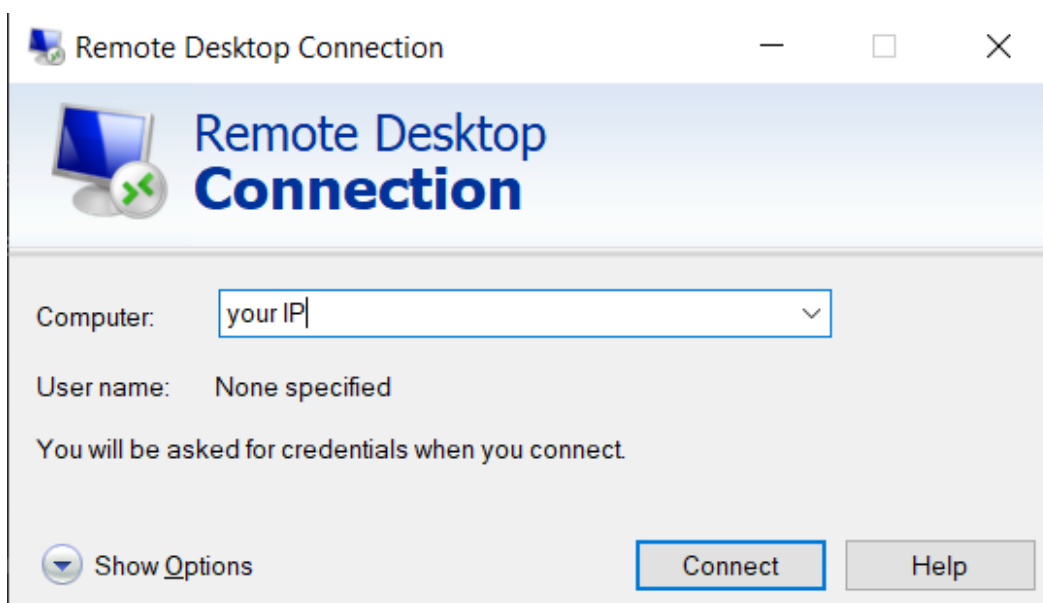
After that, it is necessary to check the IP of the Linux instance:

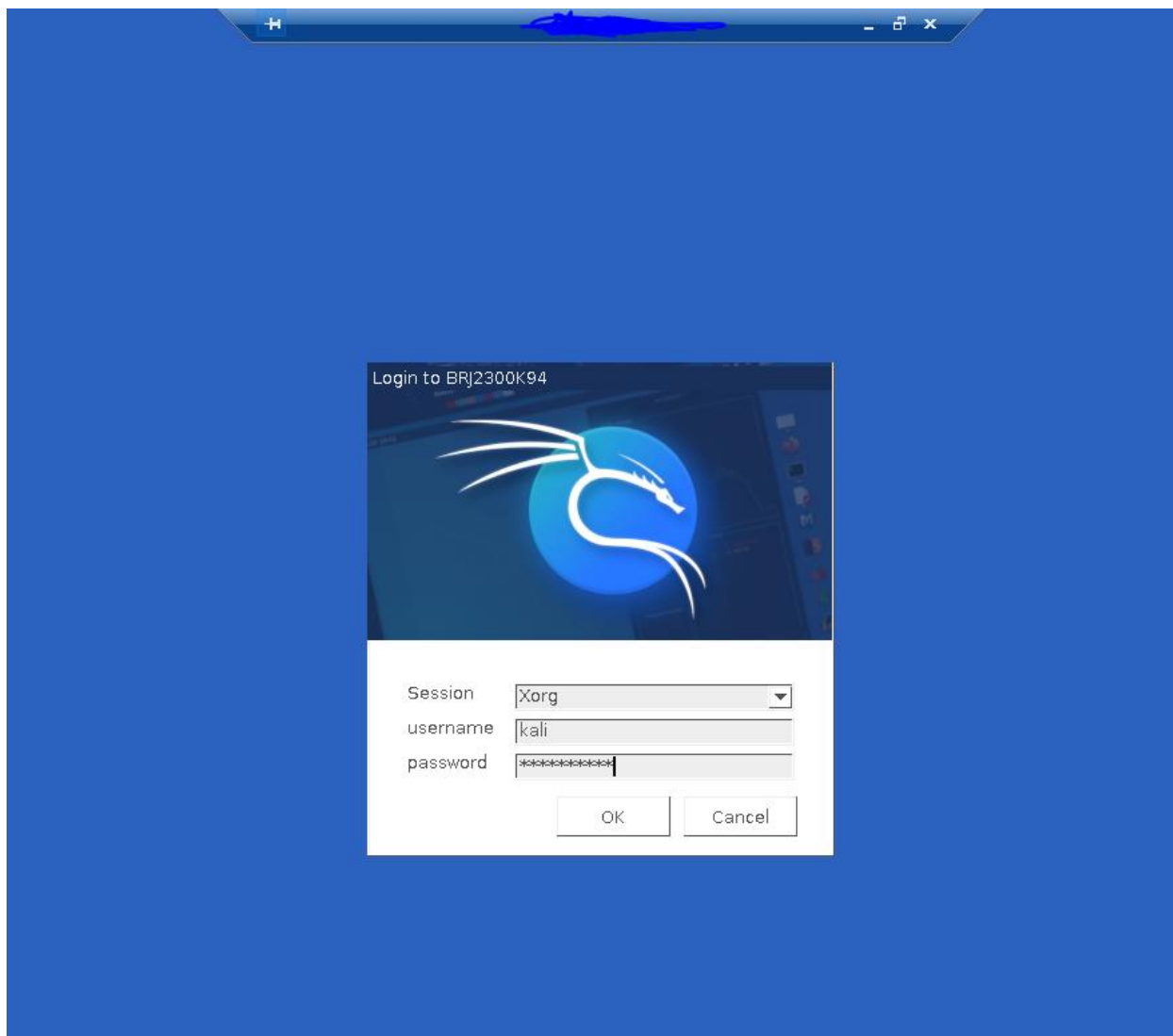
#ifconfig

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.

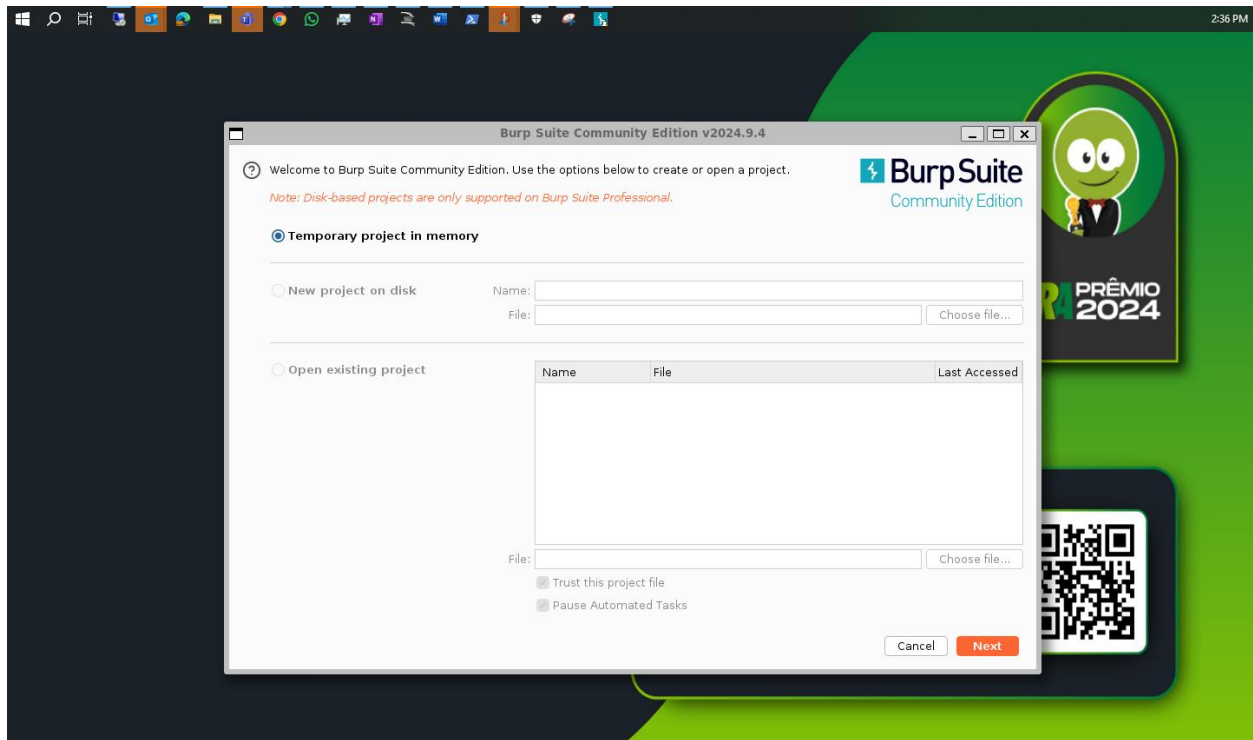




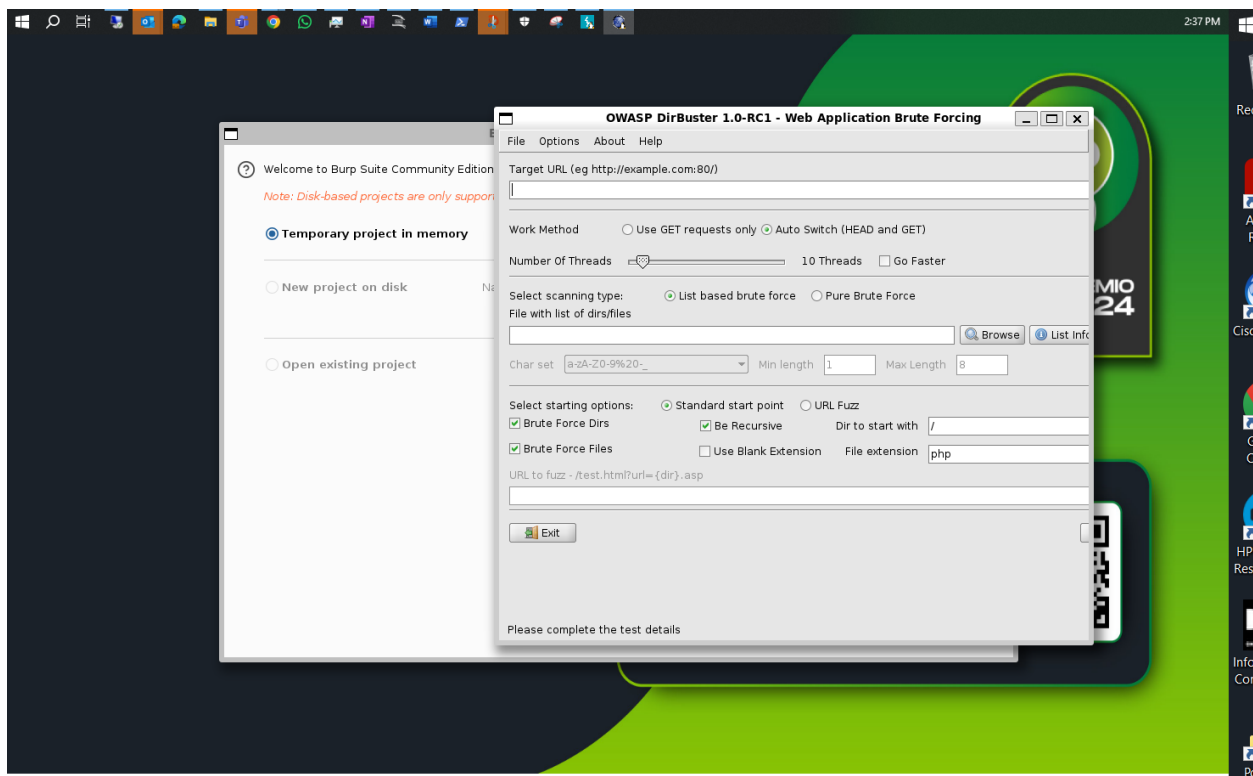
With this, I formally report a vulnerability or perhaps a misconfiguration, where it is possible to bypass the CyberArk EPM controls for software installation, where users can activate and install WSL (Windows Subsystem for Linux), in which the attacker with access to the user's equipment can install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

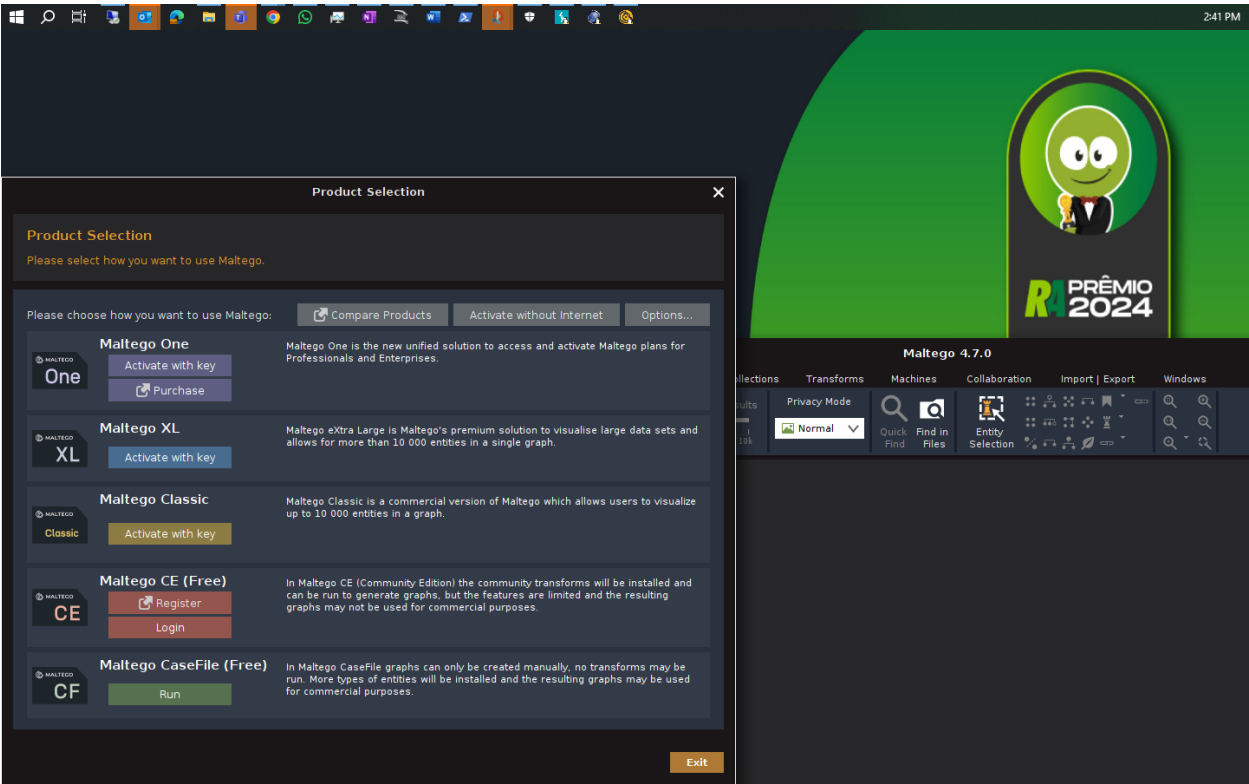
Burpsuite:



Dirbuster:



Maltego:



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/