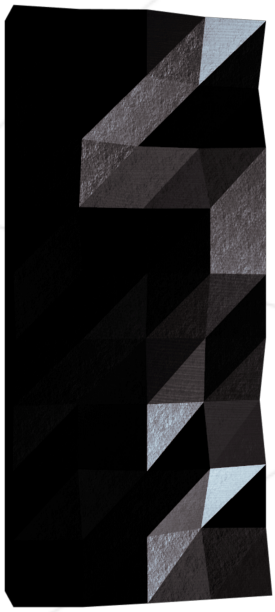


42_ActiveTechTales

BinExp in windows !

Summary: ActiveTechTales: Discover the world of binary exploitation on Windows.

Version: 1.00

Contents

Chapter I

Preamble

You're provided with a helper pdf, foundable inside the attachments of the subject.
It will show you how to access the VMs created for you to complete this subject, how to lock your VMs, etc.

This subject is the production of a partnership between 42 and Microsoft Corporation.

Microsoft Corporation is an American multinational technology corporation headquartered in Redmond, Washington.Microsoft's best-known software products are the Windows line of operating systems, the Microsoft Office suite, and the Internet Explorer and Edge web browsers.

Through this partnership, we aim to provide you with a unique opportunity to simplify your journey towards obtaining certifications offered by Microsoft. These certifications hold significant value and recognition in the industry, enabling you to enhance your professional profile and unlock exciting career prospects in the field of security.

To access the Microsoft certification programs and explore the wide range of certificates available, you can visit the following link: Microsoft Security Certification. This comprehensive platform offers extensive training resources and examinations covering various security-related topics.

By successfully completing the projects and earning Microsoft certifications, you will demonstrate your proficiency and expertise in security practices. These certifications serve as a testament to your skills and can open doors to exciting career opportunities.

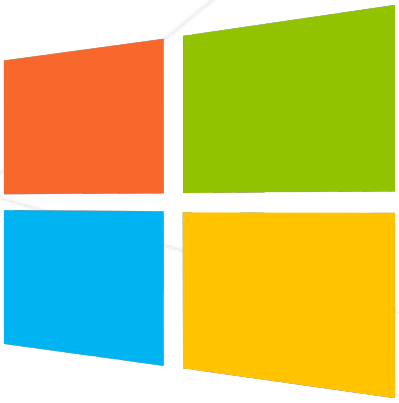


Figure I.1: https://www.microsoft.com/

Chapter II

Objectives

In partnership with Microsoft

ActiveTechTales is a captivating project dedicated to unraveling the intricacies of binary exploitation on Windows, specifically targeting the 64-bit architecture. With a series of six progressively complex executables, this project is designed to provide a hands-on experience in the realm of binary manipulation and security exploration.

The project will guide you through the fascinating world of binary exploitation, step by step, starting from the basics and progressing to more advanced techniques. Throughout this journey, you will gain a deep understanding of how binaries function on Windows systems and learn essential skills in vulnerability analysis and exploit development.

Join us in this thrilling exploration of binary exploitation on the Windows platform, where you'll unlock the secrets of software security and gain valuable insights into the inner workings of 64-bit executables.

Be careful, this project is highly challenging.

You're provided with a helper pdf, foundable inside the attachments of the subject.
It will show you how to access the VMs created for you to complete this subject, how to lock your VMs, etc.

Chapter III

General rules

- Only this page will serve as a reference: do not trust rumors.
- This project need to be done on a Virtual Machine.

You can use any libraries you want. However, it's important to be able to justify your choices.

Chapter IV

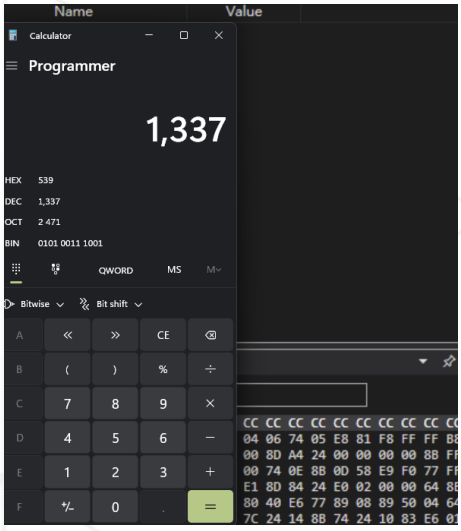
Mandatory Part

Be careful, this project is highly challenging.

Before diving into the levels, it's essential to set up your Windows environment correctly. You'll need to configure fundamental tools for binary exploitation, including but not limited to Mona, Python, Immunity Debugger (or equivalent), and any other relevant utilities. Ensuring these tools are correctly set up is crucial for a smooth learning experience.

Now that you've set up your environment, you can access the files located on your intranet as attachments.

Your next step is to make these files functional and exploit them effectively. You should aim to demonstrate successful binary exploitation by executing **calc.exe** from each of these binaries.



- Level 00

```
FileName          : C:\x\level00.exe
ARCH              : AMD64
DotNET            : False
ASLR              : False
DEP               : False
Authenticode      : False
StrongNaming      : N/A
SafeSEH           : N/A
ControlFlowGuard  : False
HighentropyVA     : True
```

- Level 01

```
FileName          : C:\x\level01.exe
ARCH              : AMD64
DotNET            : False
ASLR              : False
DEP               : False
Authenticode      : False
StrongNaming      : N/A
SafeSEH           : N/A
ControlFlowGuard  : False
HighentropyVA     : True
```

- Level 02

```
FileName          : C:\x\level02.exe
ARCH              : AMD64
DotNET            : False
ASLR              : False
DEP               : True
Authenticode      : False
StrongNaming      : N/A
SafeSEH           : N/A
ControlFlowGuard  : False
HighentropyVA     : True
```

- Level 03

```
FileName          : C:\x\level03.exe
ARCH              : AMD64
DotNET            : False
ASLR              : True
DEP               : True
Authenticode      : False
StrongNaming      : N/A
SafeSEH           : N/A
ControlFlowGuard  : False
HighentropyVA     : True
```

- Level 04

```
FileName          : C:\x\level04.exe
ARCH              : AMD64
DotNET            : False
ASLR              : True
DEP               : False
Authenticode      : False
StrongNaming      : N/A
SafeSEH           : N/A
ControlFlowGuard  : False
HighentropyVA     : True
```

Once you've achieved this, remember to push both your code and the scripts used for each level to the repository. You have the flexibility to organize your repository as you see fit, but ensure that you include all the necessary scripts for your evaluation. This means preparing multiple automation scripts.

The evaluation will take place on a clean virtual machine (VM), so your scripts should be self-contained and capable of reproducing the exploitation process seamlessly.

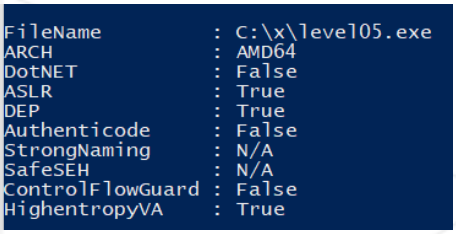
Chapter V

Bonus part

For this project, the bonus part is easy.

You need to exploit the last level of this project. It should be easy right?

- Level 05



The bonus part will only be assessed if the mandatory part is PERFECT. Perfect means the mandatory part has been integrally done and works without malfunctioning. If you have not passed ALL the mandatory requirements, your bonus part will not be evaluated at all.

Chapter VI

Submission and peer-evaluation

You're provided with a helper pdf, foundable inside the attachments of the subject.
It will show you how to access the VMs created for you to complete this subject, how to lock your VMs, etc.

Turn in your assignment in your `Git` repository as usual. Only the work inside your repository will be evaluated during the defense. Don't hesitate to double-check the names of your files to ensure they are correct.