Capa report:

Text

Description automatically generated

Graphical user interface, text, application

Description automatically generated

Graphical user interface, text

Description automatically generated

Text

Description automatically generated

Chương trình sử dụng tham số dòng lệnh. Nếu không pass gì (argc = 1) thì chương trình sẽ tiến hành kiểm tra VM. Nếu không phát hiện thì sẽ sinh ra key và in ra màn hình.

Nếu pass vào key (argc = 2) thì chương trình sẽ check key và in ra flag.

Như vậy chỉ cần bypass hết là ta sẽ có key (hoặc chạy bằng 1 cái máy thật 100% là xong, ez flag).

1. VMWare registry

Trong hàm vmcheck(): Graphical user interface, text, application

Description automatically generated

Mảng v61 có cấu trúc: cứ mỗi cụm 3 string thì string thứ nhất là Registry key, string thứ 2 là value name và string thứ 3 là value. Hàm registrycheck sẽ nhận vào mỗi lần một cụm 3 string và query value tại registry key:value name và so sánh với string thứ 3. Nếu đúng thì sẽ return true.

Graphical user interface, text, application, email

Description automatically generated

Bypass bằng cách patch jump để không check kết quả của hàm registrycheck() nữa.

1. Check Vmware tools

Text

Description automatically generated with medium confidence

Sau đó, chương trình check registry key của vmware tool. Open key thành công thì key[1] sẽ là byte 14 của byte\_473B28, còn nếu không thì sẽ là byte thứ 13.

Bypass bằng cách patch để v3 luôn luôn bằng 13.

Graphical user interface, text, application

Description automatically generated

Kết quả:



1. Check vmware driver

Tiếp theo, chương trình check xem có driver của vmware hay không bằng cách tạo ra đường dẫn tới %systemroot%\\_\_vmwaredrivepath\_. Sau đó GetAttribute, nếu GetAttribute thành công và đường dẫn đó không phải directory (không phải directory thì là 1 file) tức là phát hiện máy ảo.

Graphical user interface, text, application

Description automatically generated

Bypass bằng patch jump không check IsVm nữa. Hoặc patch v7 = v3+1 thành v7 = v3

Kết quả:

Graphical user interface, text, application, email

Description automatically generated

Graphical user interface, text

Description automatically generated

Đoạn sau chương trình vẫn sử dụng kĩ thuật check attribute để kiểm tra xem có thư mục cài đặt vmware hay không. Bypass bằng cách patch jump hoặc patch cho v10 luôn luôn bằng 86

1. Check MAC

Graphical user interface, text, application

Description automatically generated

Chương trình check xem có địa chỉ Mac của VMWare hay không. Nếu có thì sẽ thay đổi biến v8 gây ra sai key.

Bypass bằng patch jump hoặc nop dòng 156 (++v8)

1. Check VMWare adapter

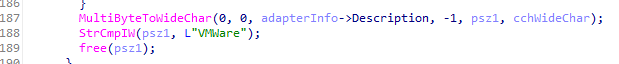
Chương trình thực hiện check description của từng adapter xem có phải là “VMWare” hay không.

Graphical user interface, text, application

Description automatically generated

Bypass bằng cách patch jump ở đoạn so sánh string hoặc nop isVm = 1.

Kết quả:



1. VMWare Host Guest File System (HGFS), VMWare Virtual Machine Communication Interface (vmci)

Chương trình thực hiện kiểm tra sự tồn tại của HGFS và VMCI.

Graphical user interface, text, application

Description automatically generated

Bypass bằng cách nop ++22 (dòng 206 trong ảnh)

1. VMWare process

Chương trình thực hiện kiểm tra xem các process của vmware có chạy hay không. Hàm IsProcessRunning() tạo snapshot các tiến trình rồi enum so sánh xem process name có trùng với string truyền vào hay không.

Text

Description automatically generated

Bypass bằng cách nop ++v24. Kết quả:

Text

Description automatically generated

1. ACPI table

Graphical user interface, text, application

Description automatically generated

Chương trình sử dụng EnumSystemFirmwareTables với FirmwareTableProviderSignature là RSMB để check xem có xuất hiện cụm từ Vmware hay không, nếu có thì sẽ thay đổi v24 thành 11.

Bypass bằng cách patch nop v24=11.

1. Final strike

Đoạn cuối cùng cũng thực hiện 1 đoạn check VM, nếu phát hiện VM thì call ExitProcess. Bypass bằng cách nop ExitProcess.

Sau khi apply patch, chạy chương trình không pass tham số thì nhận được kết quả:



Quay lại hàm main với argc = 2. Ta quan tâm tới hàm sub\_FD1260. Hàm này nhận vào string a1 (cố định), argv[1] chính là key ta pass vào, và vùng nhớ v8 mới được malloc. Có thể phỏng đoán hàm này là hàm sinh ra flag.

Timeline

Description automatically generated

Nhớ lại kết quả scan capa có thấy chương trình thực hiện RC4:



Phỏng đoán hàm này thực hiện giải mã RC4 chuỗi ở a1, key là argv[1].

Check thử:

Graphical user interface, text, application, email

Description automatically generated

Vậy khỏi cần quan tâm đoạn trên đã làm gì (chắc lại tiếp tục check Vmware)

* FL4g: vcstraining{Running\_in\_VM\_is\_ridiculous}