LAB 08

Thầy Mai Hoàng Đỉnh
Trường đại học FPT

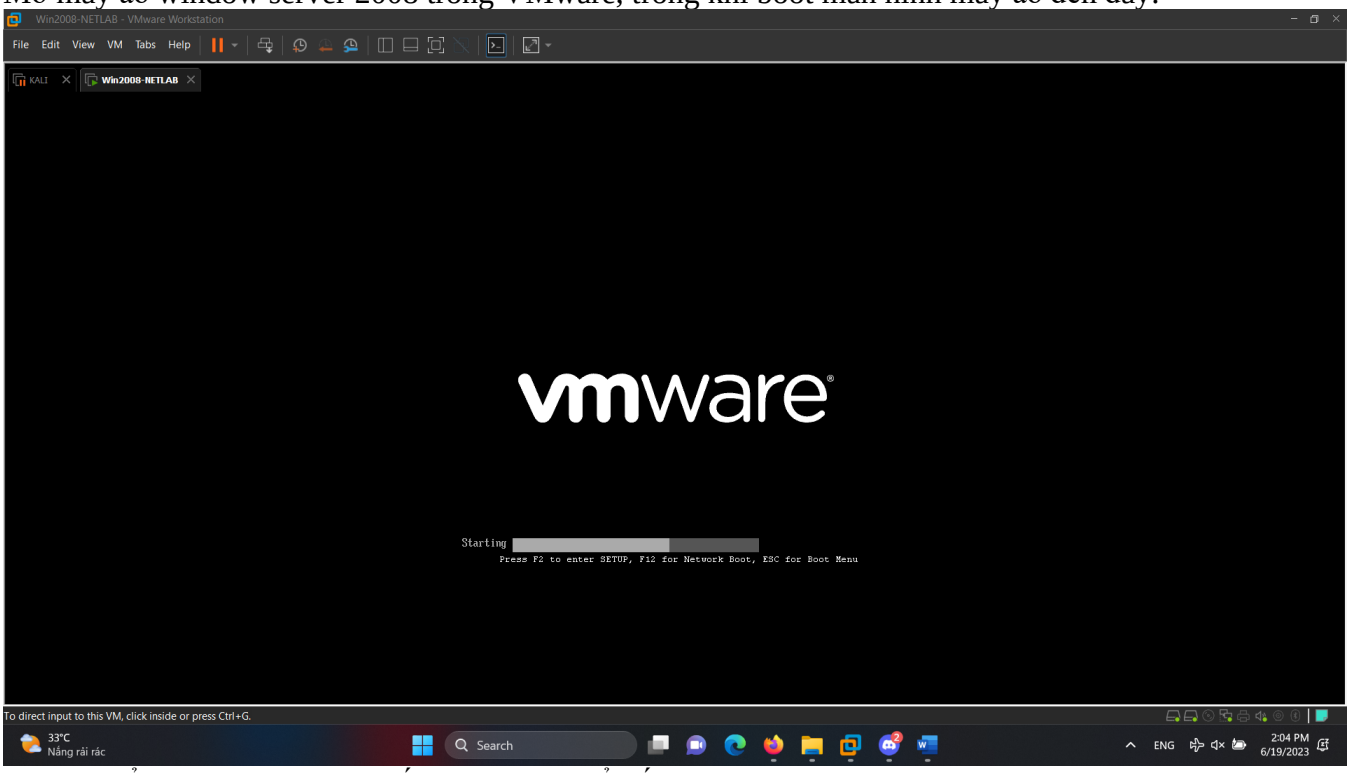
Người thực hiện

Đặng Hoàng Nguyên

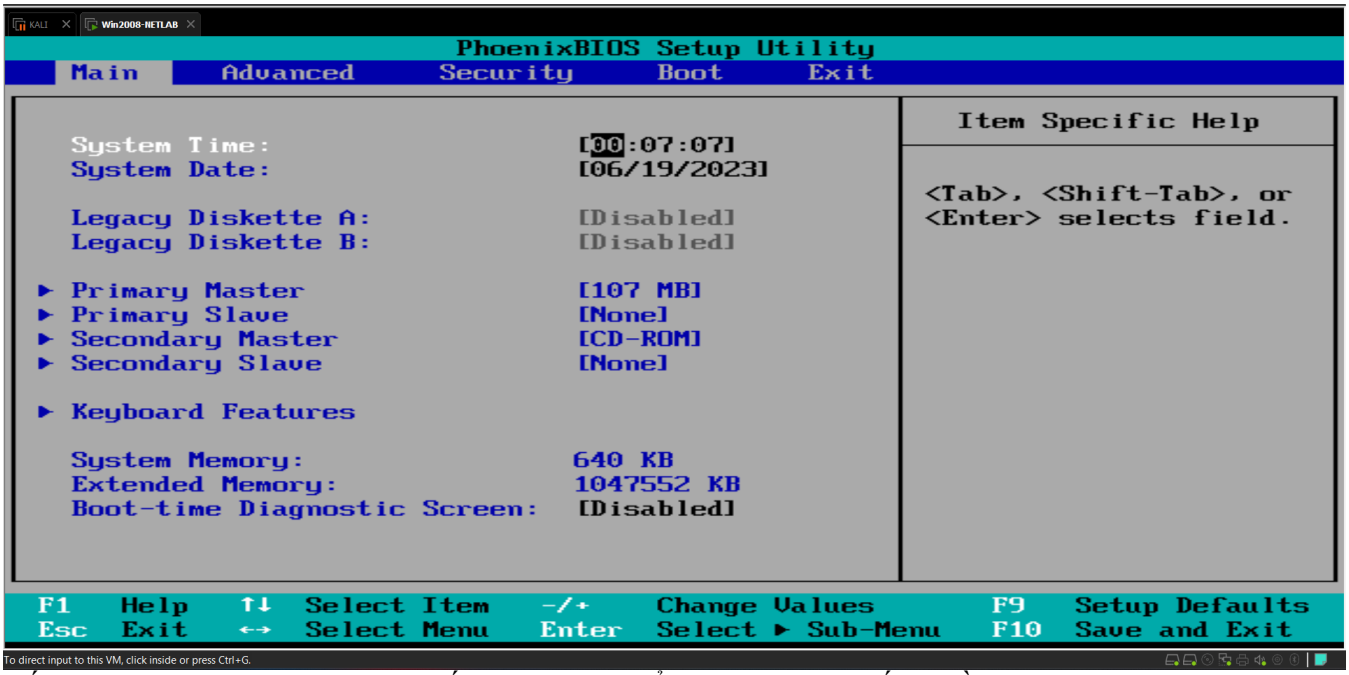
Lab-Project 8: Breaking a BIOS Password

Chỉnh password bios

Mở máy ảo window server 2008 trong VMware, trong khi boot màn hình máy ảo đến đây:



Tới đây để vào được bios ta nhấn liên tục F2 để tiến hành vào bios

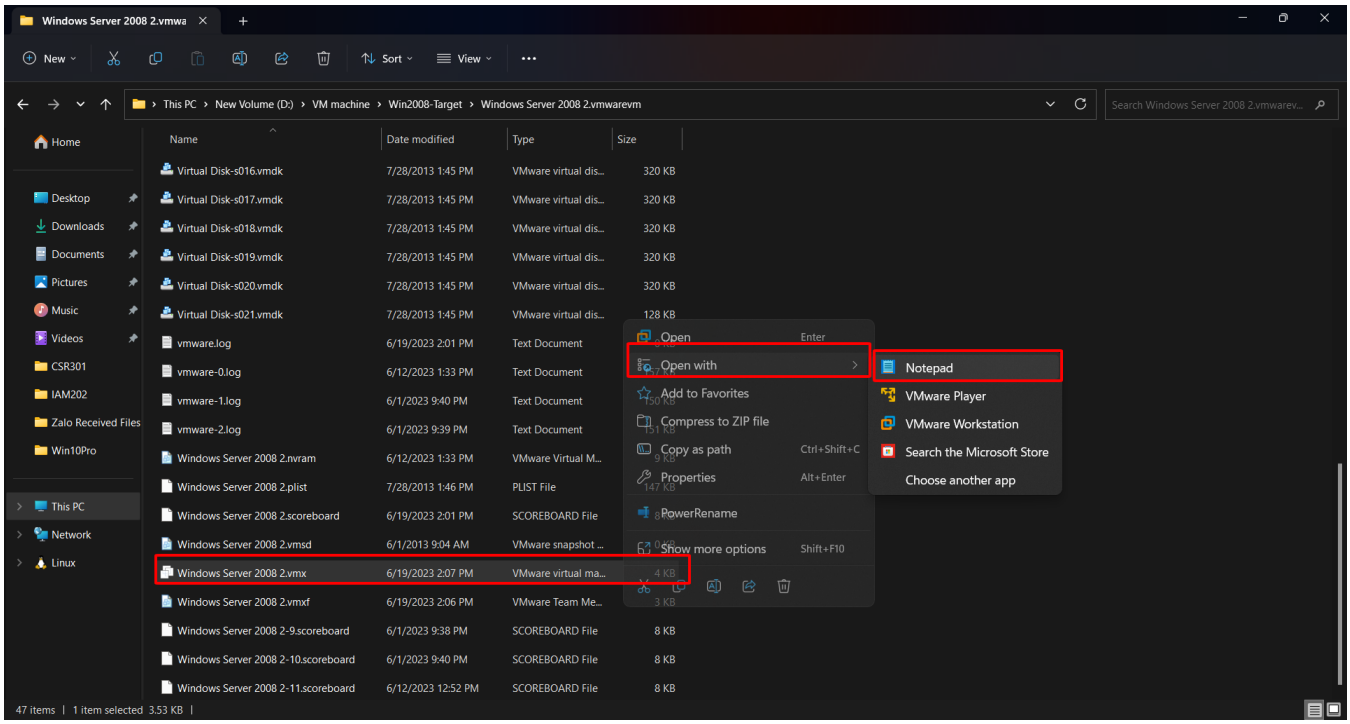


Nếu máy khởi động quá nhanh khiến bạn không thể vào BIOS, hãy tắt nguồn máy ảo, tìm tệp .vmx của nó và thêm dòng này vào cuối máy:

- bios.bootdelay = 5000

Muốn tìm tệp vmx của máy, ta cần vào nơi chứa máy ảo ban đầu. Ở đây là D:\\Virtual Machine\Window2008 Netlab\

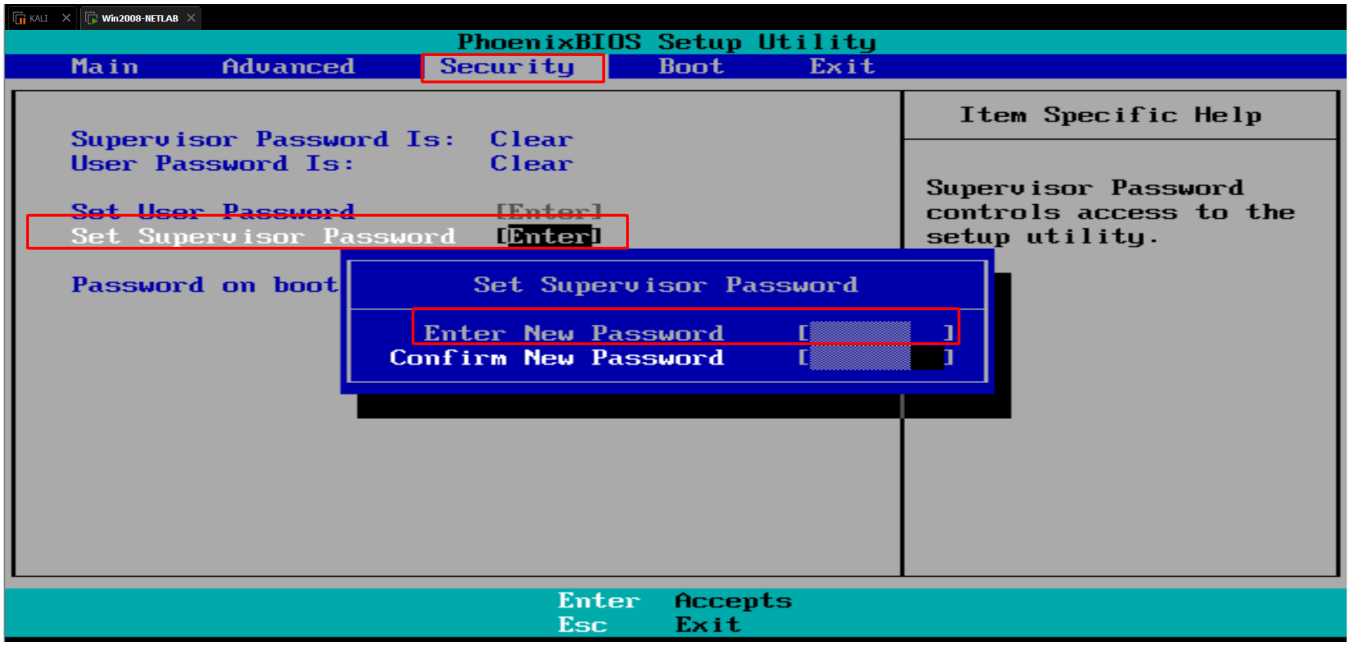
Sau đó tìm đến file có đuôi lưu trữ là .vmx và vào bằng notepad



Sau đó thêm vào câu lệnh “bios.bootdelay = 5000” để chỉnh thời gian trước khi vào bios là 5 giây

Có thể xem hướng dẫn tại đây:

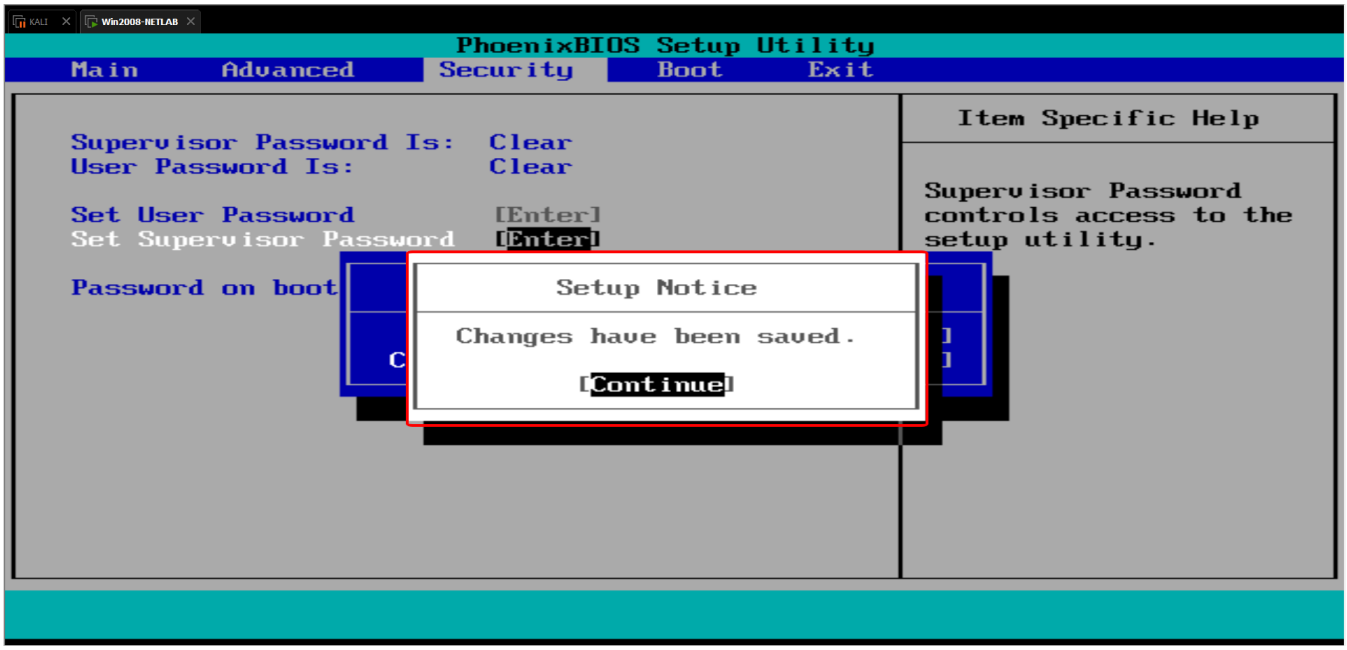
- http://www.howtogeek.com/howto/16876/how-to-increase-the-vmware-boot-screen-delay/



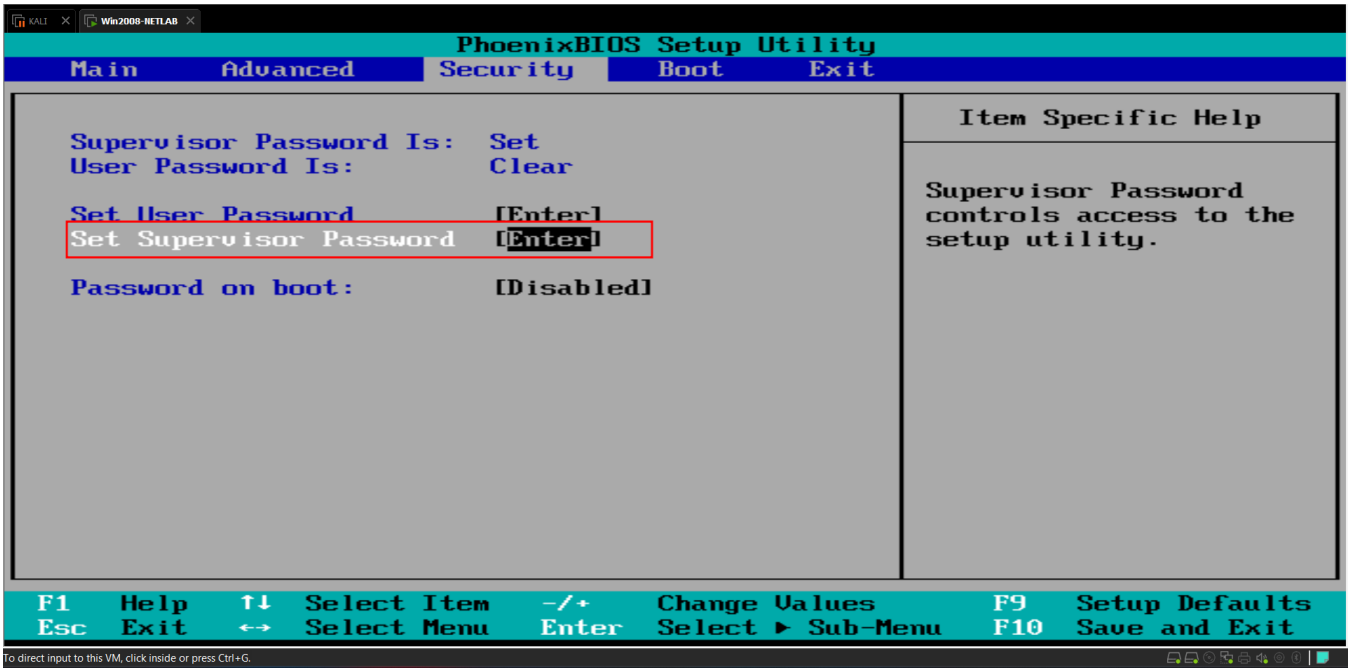
Khi màn hình "PhoenixBIOS Setup Utility" xuất hiện. Sử dụng các phím mũi tên trên bàn phím để chọn menu Security. Nhấn chọn Set supervisor Password.

Đặt password là 123456 và chọn confirm, sau đó nhấn enter để xác nhận đổi password.

Sau khi nhập mật khẩu vào cả hai trường, hãy nhấn Enter. Hộp " Setup Notice " xuất hiện cho biết " Changes have been saved.". Nhấn **Enter** lần nữa

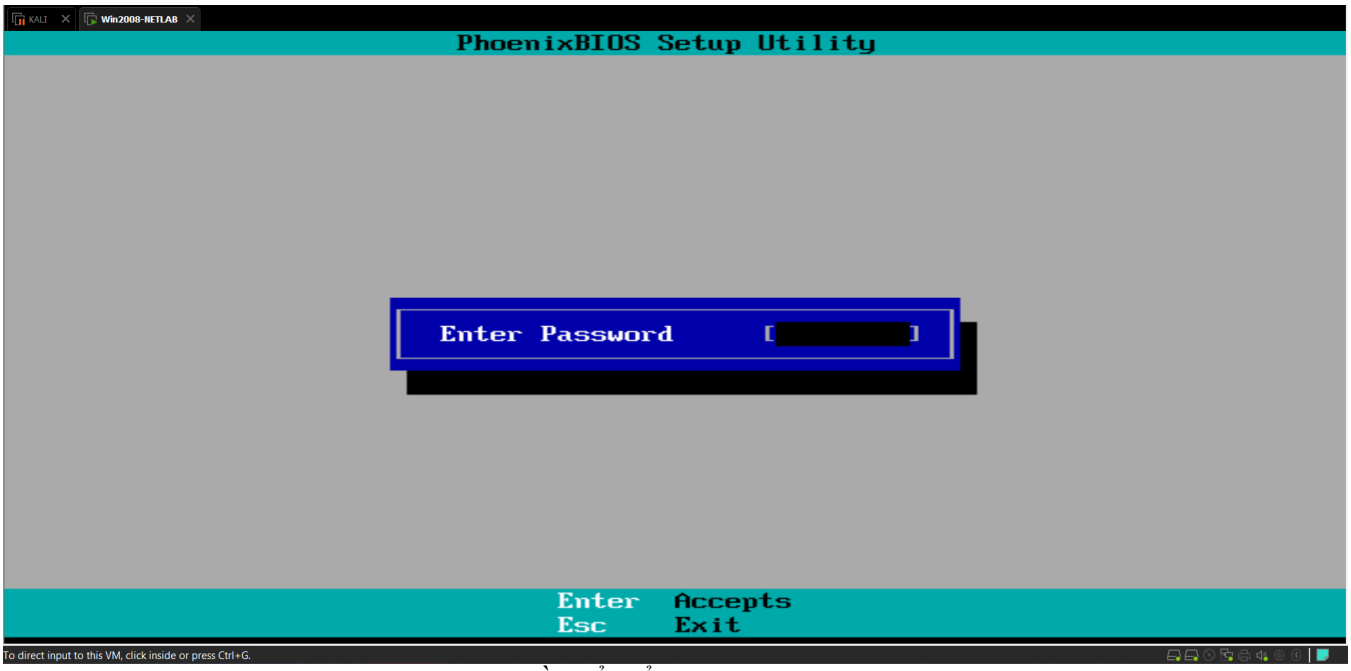


Bios của chúng ta bây giờ phần Set Supervisior Password đã hiển thị màu trắng thay vì màu xanh là đã set password thành công. Sau đó nhấn F10 để lưu lại setting trong bios

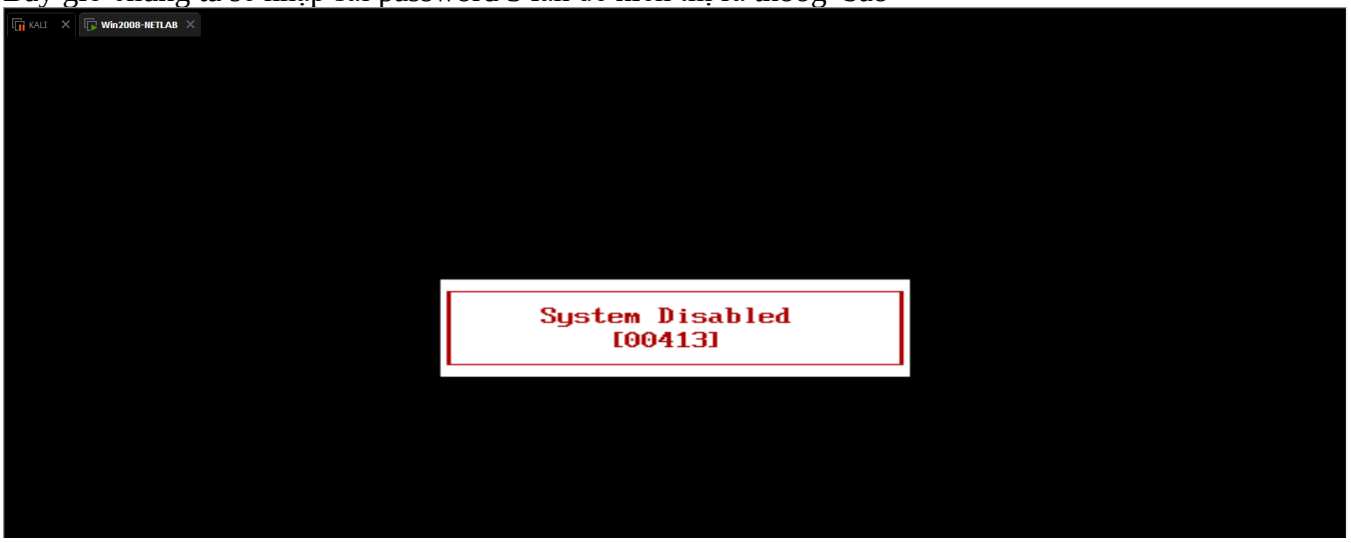


Entering the Wrong Password Three Times

Chúng ta bắt đầu restart máy vào vào lại bios và lần này đã khi vào bios đã bị hỏi password.

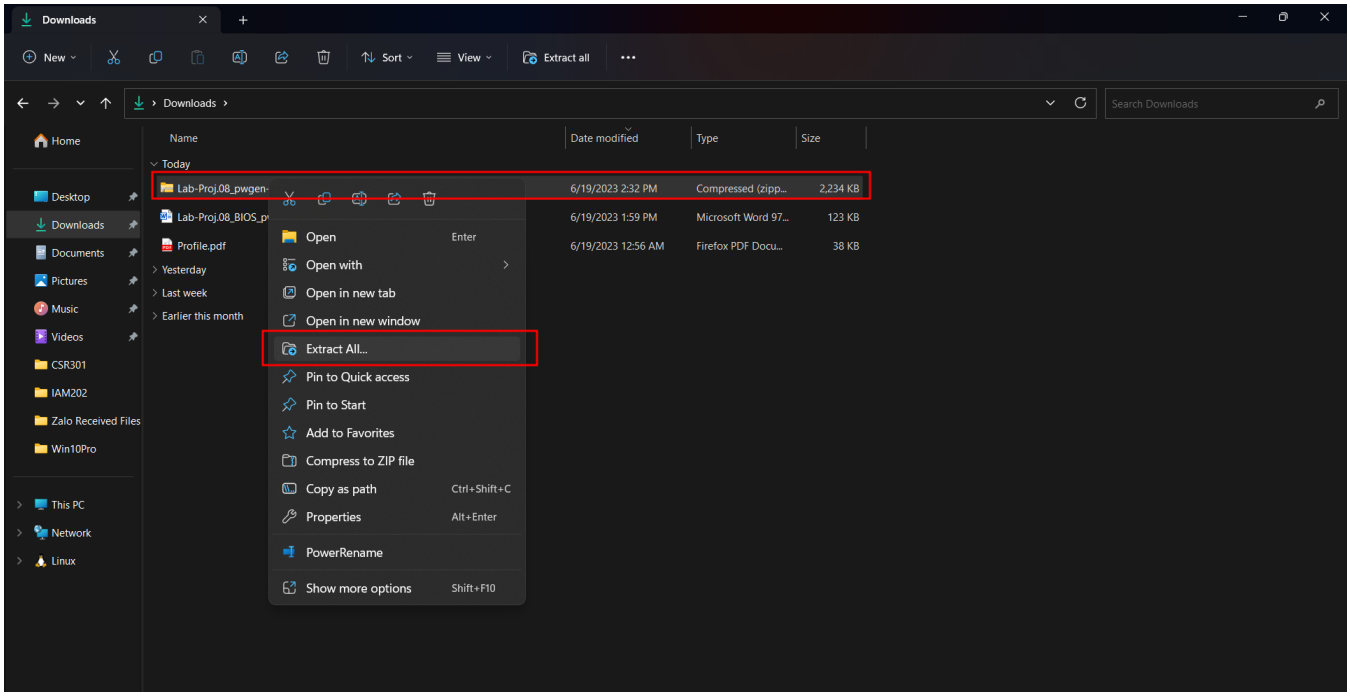


Bây giờ chúng ta sẽ nhập sai password 3 lần để hiển thị ra thoog báo

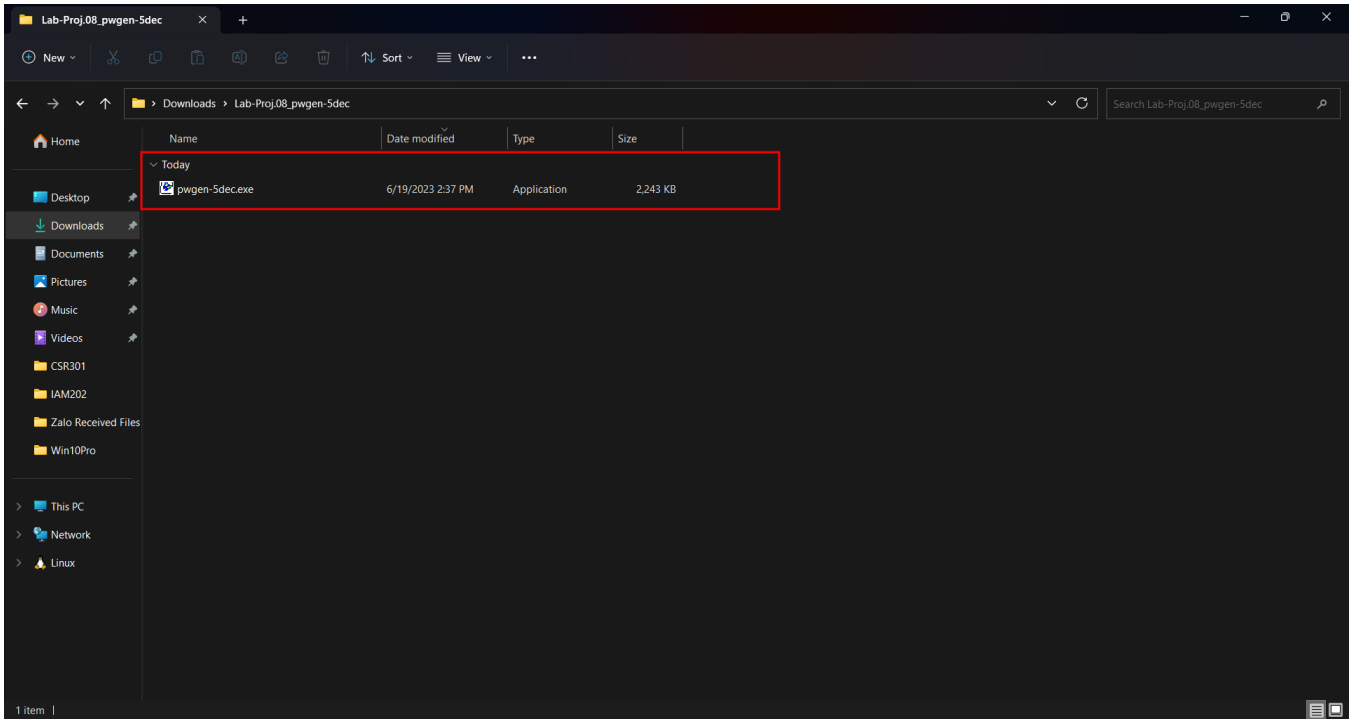


Downloading the BIOS Keygen

1. Tải tại đường link trên onedrive, lưu bên file ở bên trong thư mục nào đó mà chúng ta muốn, trong trường hợp này ở folder Downloads.



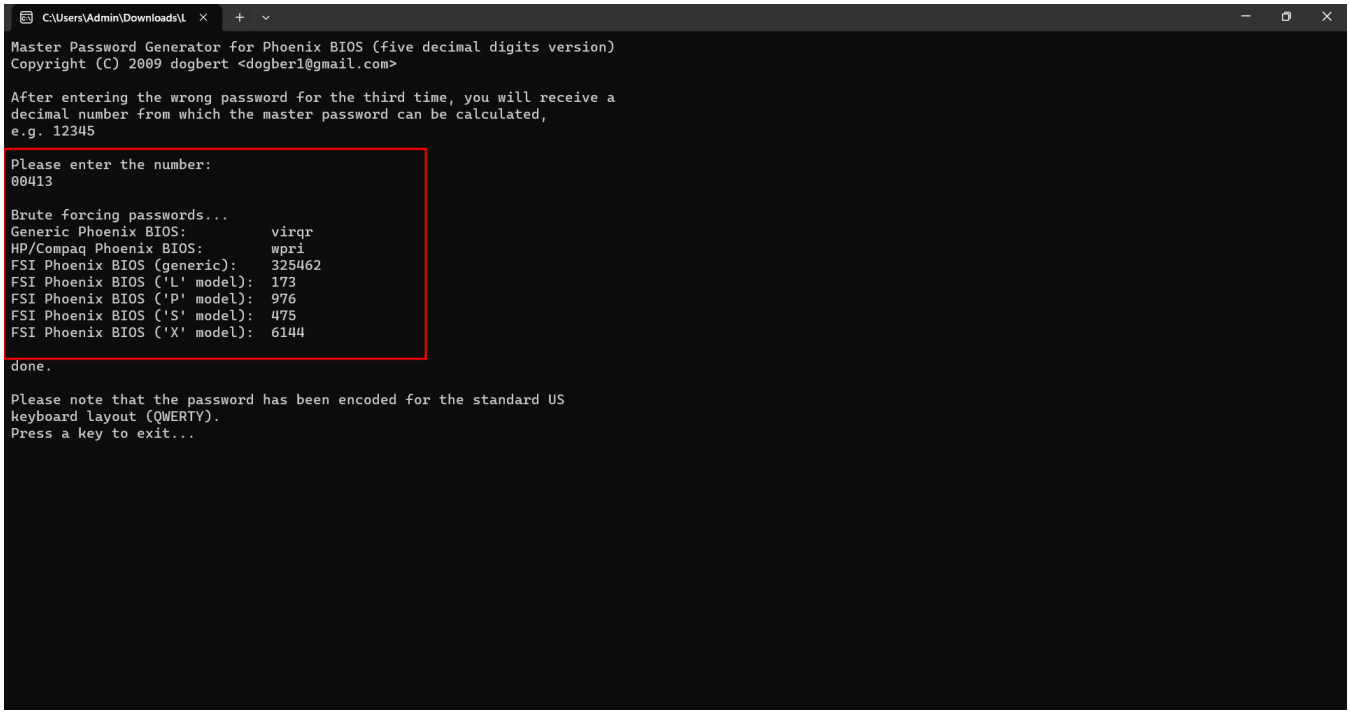
Sau khi extract xong bên trong sẽ có một file exe bên trong. Vậy là chúng ta đã cài đặt thành công



Using the Keygen

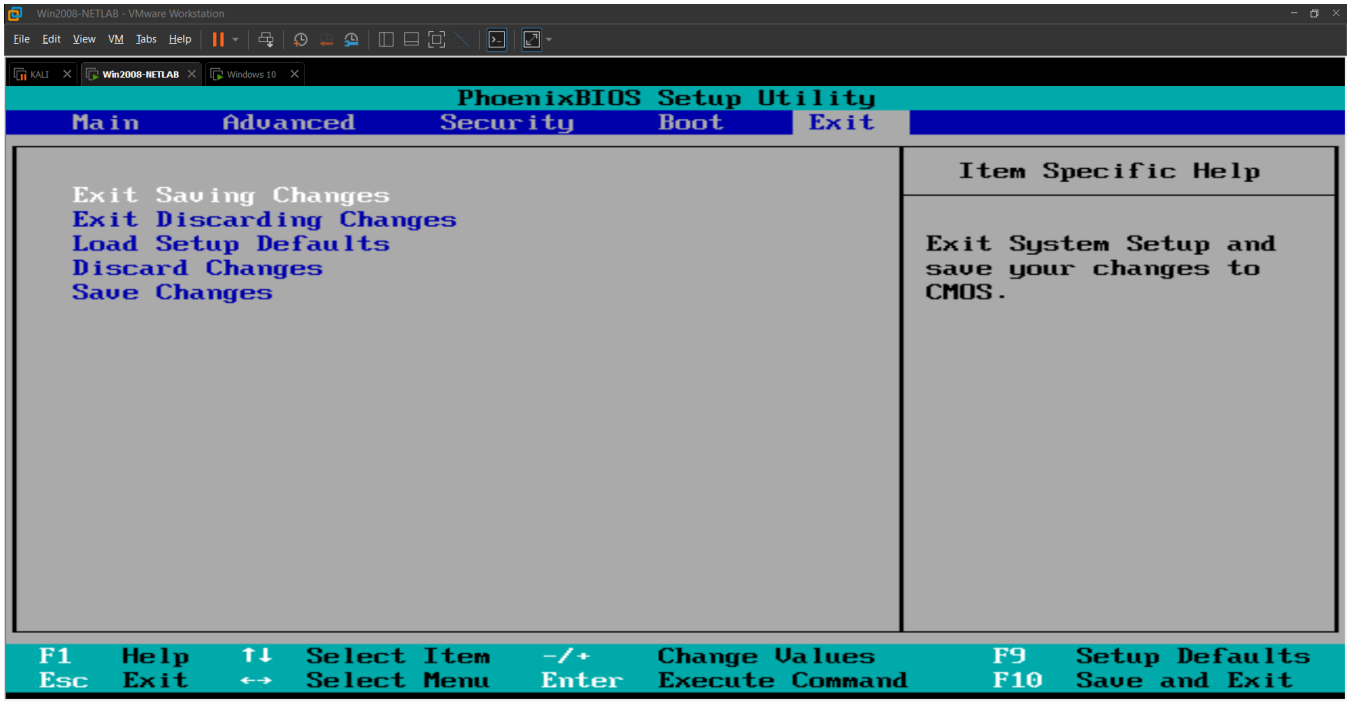
Sau khi vào được chúng ta sẽ có một file exe với tên gọi là **pwgen-5dec.exe.** Nhấn đúp chuoojg vào nó, có một file xuất hiện và nhấn chọn vào **Run.**

Sau đó, ứng dụng sẽ tự động đưa chúng ta vào bên trong terminal. Việc của chúng ta chỉ là viêcj nhập số của “System Disabled” vào bên trong terminal. Trong trường hợp này sẽ là 00413



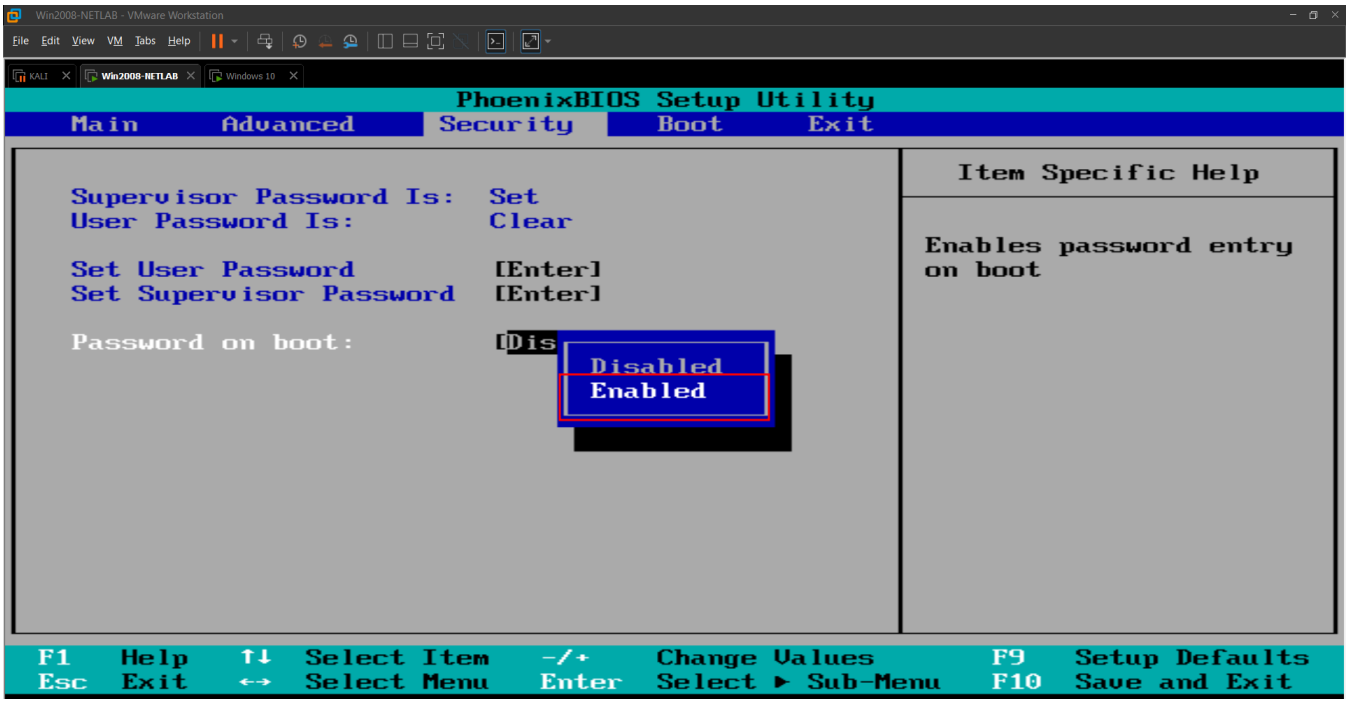
Testing the Generated Password

2. Trong VMware Workstation menu bar, click **VM**, **Power**, "**Power Off**". Click "**Power off**".
3. Từ bên trong VMware Workstation menu bar, click **VM**, **Power**, "**Power On to BIOS**".
4. Vào bios sẽ có hỏi password bioss. Chúng ta sẽ chọn password từ "Generic Phoenix BIOS" trong terminal. Tại đây là virqr
5. Nếu mật khẩu hoạt động, bạn sẽ thấy BIOS mở. Nếu không được thì chạy lại keygen. Mỗi khi bạn chạy nó, nó sẽ tìm thấy các mật khẩu khác nhau và không phải tất cả chúng đều hoạt động.

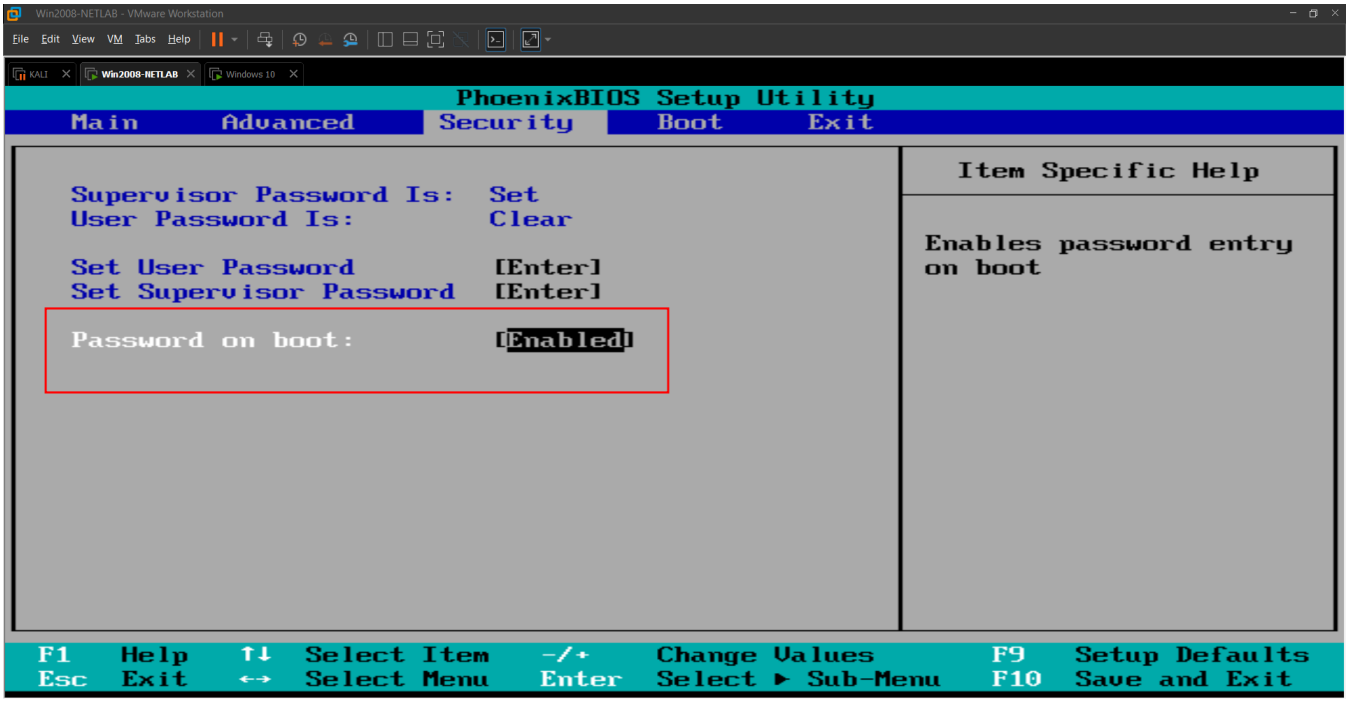


Setting a Boot Password

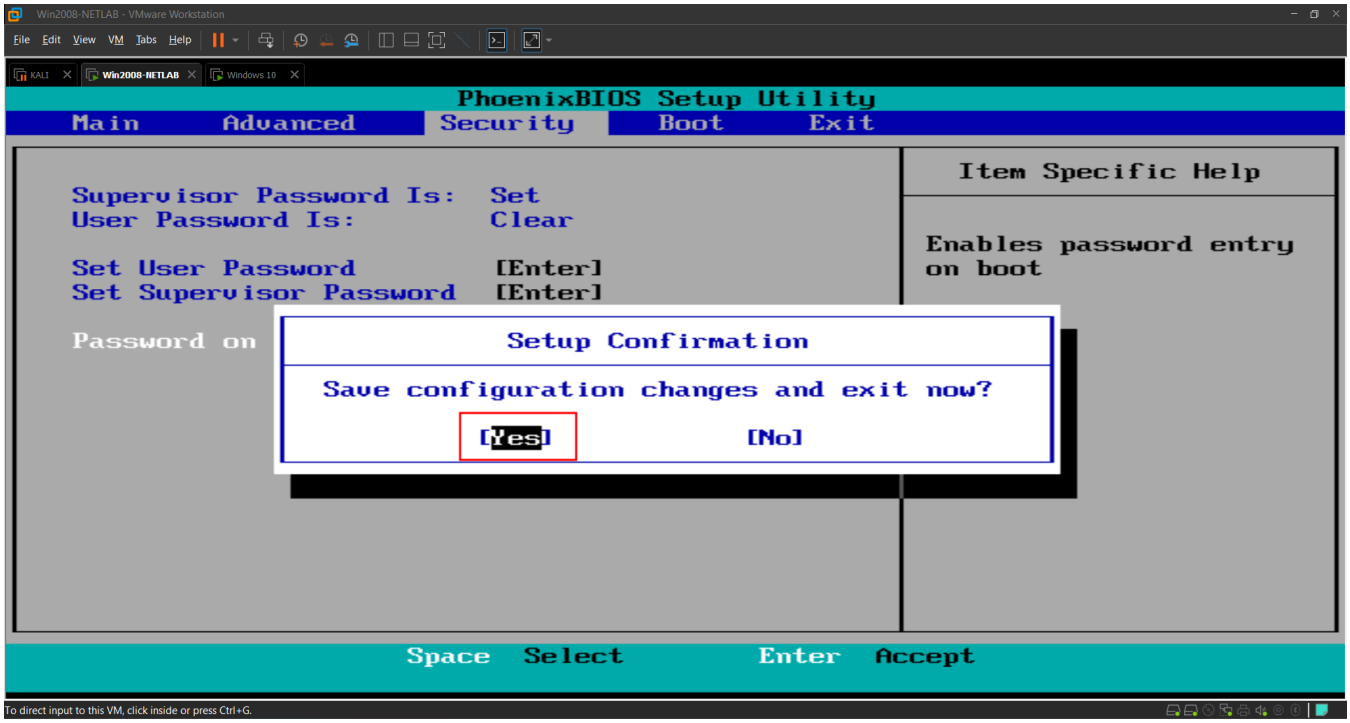
6. Trong Security menu, press the nhấn chọn vào "**Password on boot**". Nhấn **Enter** để chọn. Một hộp màu xanh xuất hiện và nhấn chọn **Enabled** và nhấn **Enter**



7. Bây giờ chúng ta sẽ thấy rằng chế độ "Password on boot" đã được bật, nó trở thnafh màu trắng



8. Nhấn F10 để lưu cài đặt.



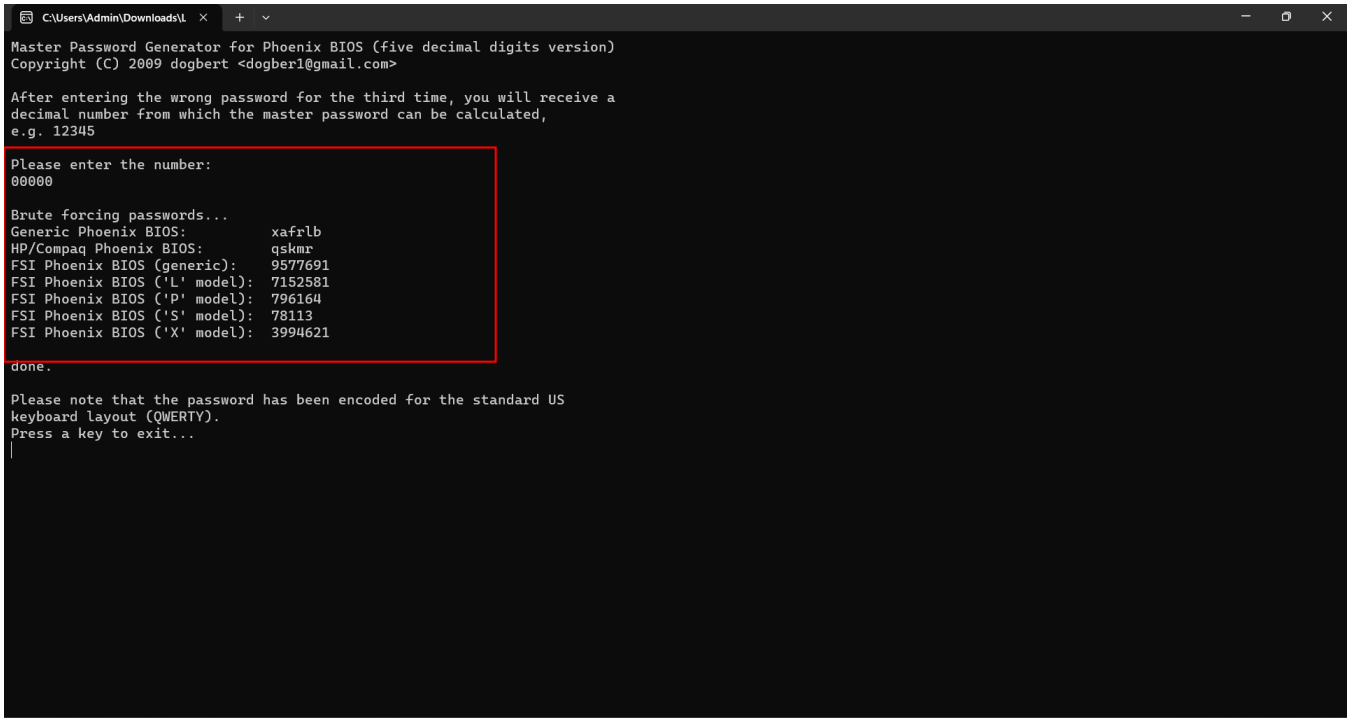
Entering the Wrong Password Three Times

Sau khi vào bios lại thêm lần nữa, chúng ta ta sẽ nhập thêm ba lần nữa để xem
Có hộp thông báo "Enter Password". Thì chúng ta sẽ nhập sai password nhiều lần.

Sẽ có bằng "System Disabled". Nhưng lần này sẽ hiện số 00000.

Using the Keygen

9. Sử dụng keygen để tạo password với số 00000 để tạo ra kết quả xem sao.



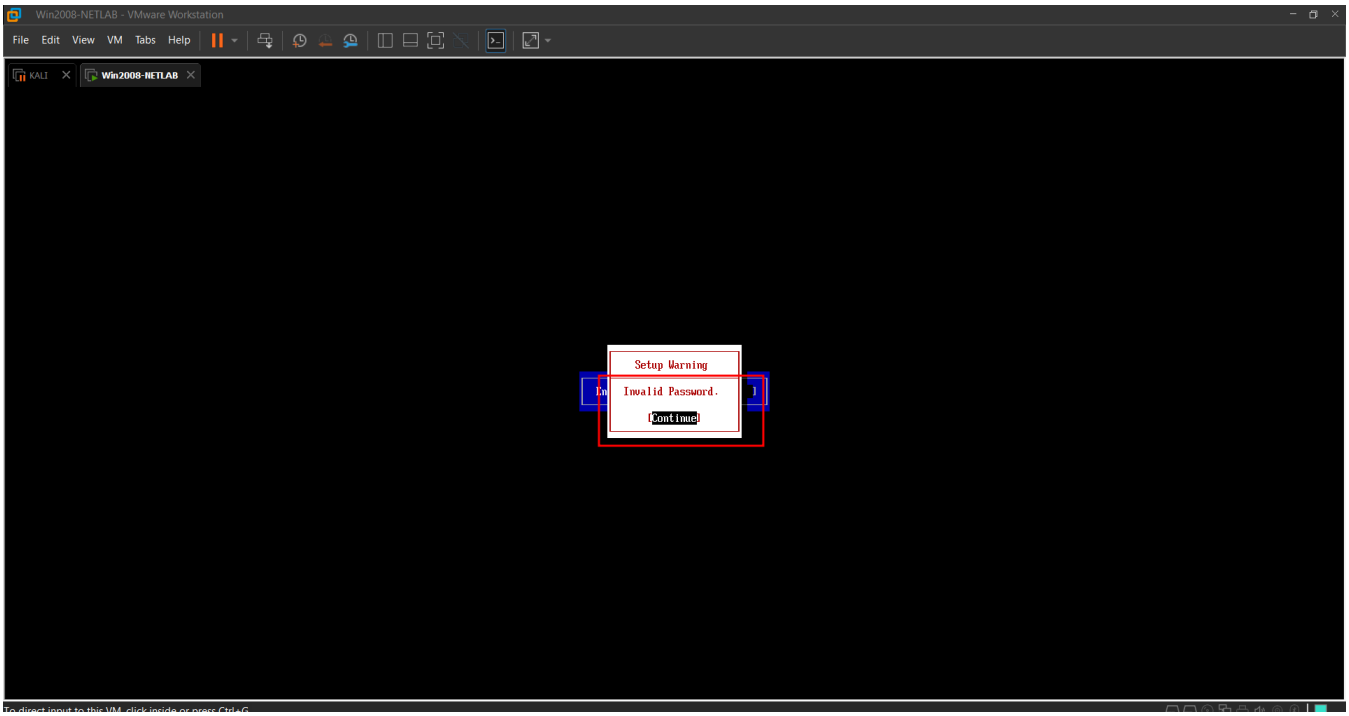
Testing the Generated Password

Press Ctrl+Alt to release the keyboard from the VM.

Từ VMware Workstation menu bar, nhấn **VM**, **Power**, "**Power Off**". Nhấn "**Power off**"

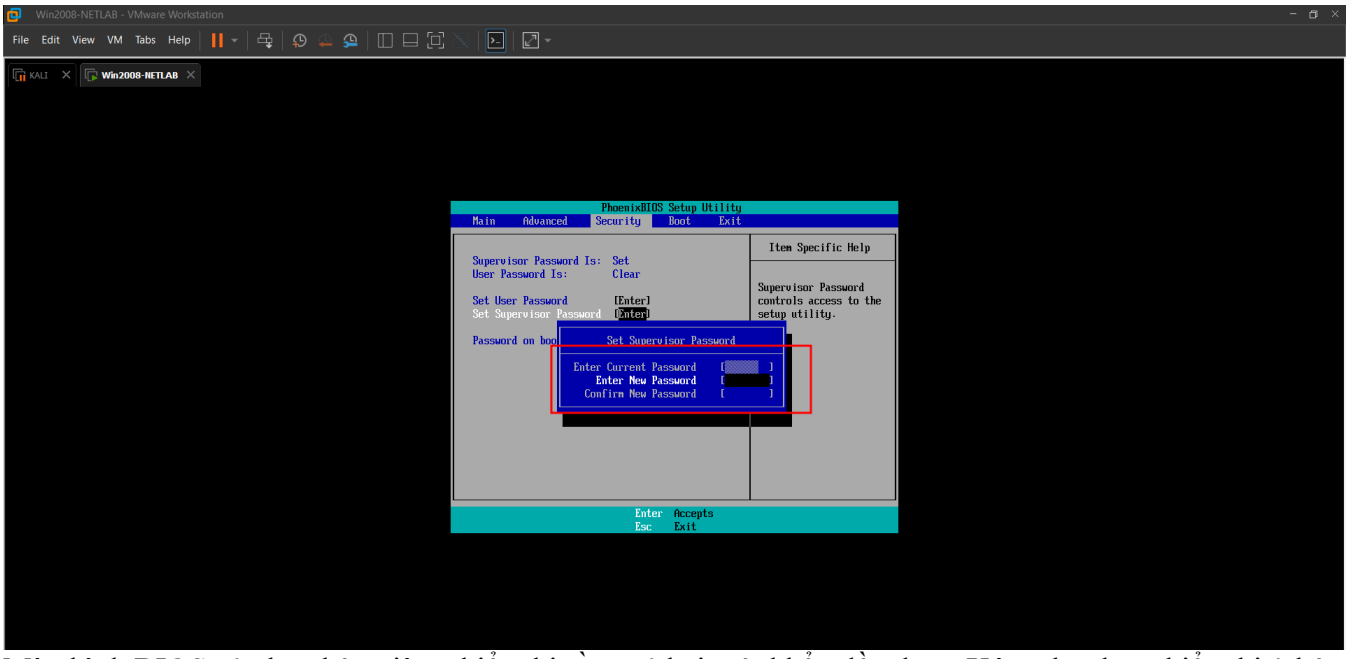
Từ VMware Workstation menu bar, nhấn **VM**, **Power**, "**Power On** ".

Sẽ có box hỏi "Enter Password". Nhập password "Generic Phoenix BIOS" trong keygen. Bây giờ sẽ ko được nữa vì số đã bị thay đổi.



Clearing the Passwords

Từ thanh menu VMware Workstation, nhấp vào **VM, Power, "Power Off".** Nhấp vào " **Power off** ".
Từ thanh menu VMware Workstation, nhấp vào **VM, Power, "Power On to BIOS".**
Một hộp màu xanh yêu cầu **"Enter Password".** Nhập mật khẩu bạn đã chọn ban đầu: 123456
Sử dụng các phím mũi tên để đến trang Security. Đánh dấu " **Password on boot"** và nhấn **Enter**. Sử dụng các phím mũi tên để tô sáng **Disabled** và nhấn **Enter**.
Trong menu Bảo mật, đặt "Mật khẩu khi khởi động" thành Đã tắt.
Sử dụng các phím mũi tên để tô sáng "Supervisor password" và nhấn Enter.
Trong hộp "Supervisor password" màu xanh lam, hãy nhập password vào dòng đầu tiên. Nhấn Enter bốn lần.



Màn hình BIOS của bạn bây giờ sẽ hiển thị rằng cả hai mật khẩu đều được Xóa, như được hiển thị ở bên phải trên trang này.

Nhấn F10 rồi Enter để lưu thay đổi.

Vậy là chúng ta đã vào thành công mà không còn bị vào password bios được nữa