Zakład Systemów Złożonych

Politechnika Rzeszowska

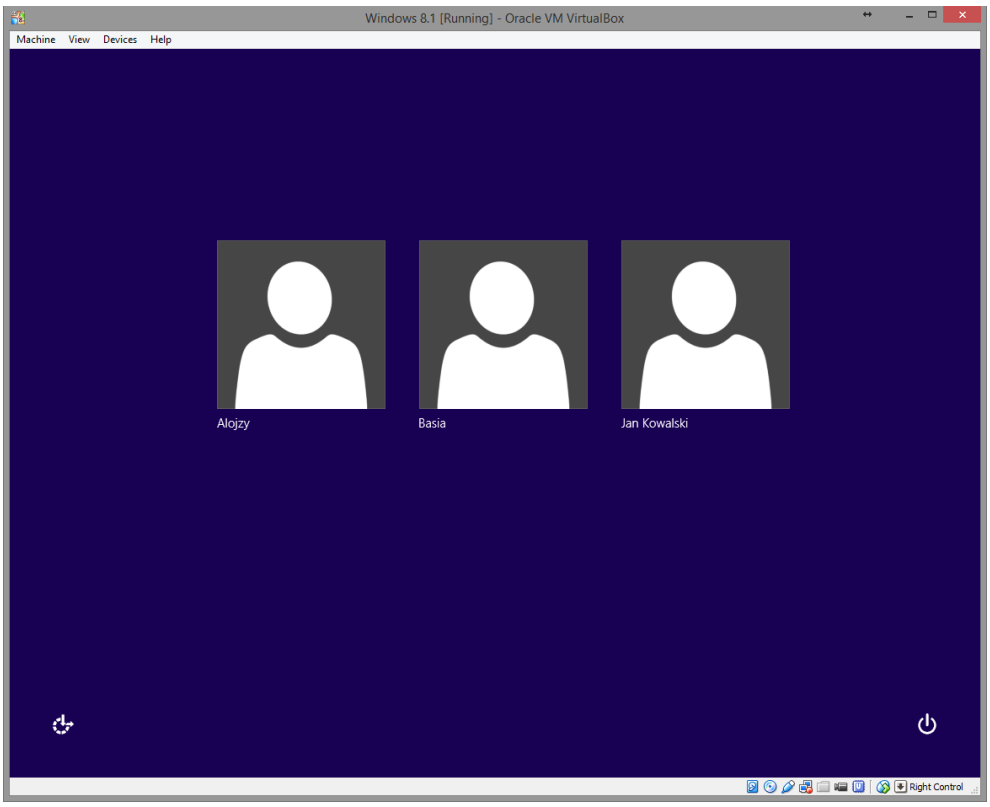
BEZPIECZEŃSTWO SYSTEMÓW I SIECI KOMPUTEROWYCH

Laboratorium zdalne nr 9:

Metody łamania haseł na przykładzie Windows 8.1

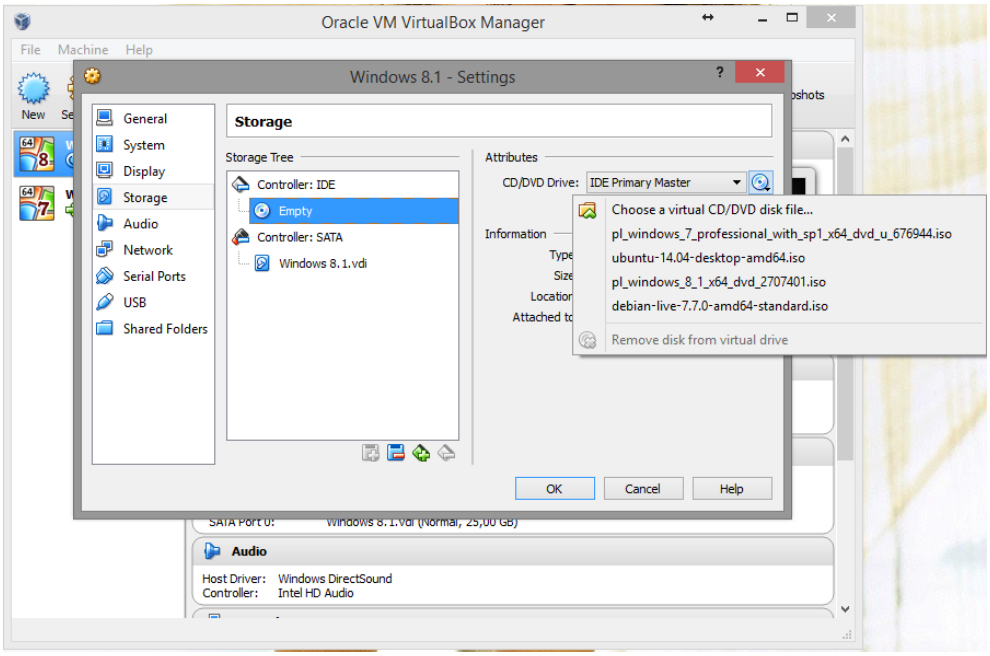
1. Uzyskiwanie dostępu do konta lokalnego.

Aby uzyskać dostęp do konta lokalnego z zapomnianym lub nieznanym hasłem potrzebujemy tylko płyty z zainstalowanym systemem operacyjnym.



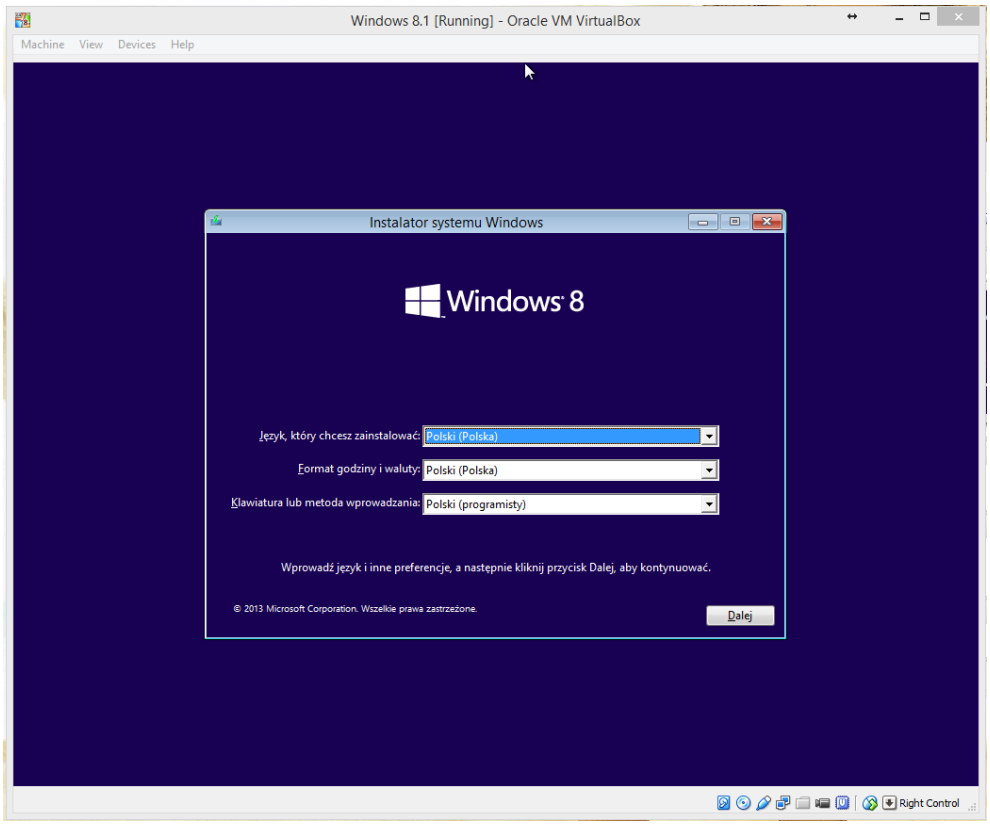
Windows 8.1 z utworzonymi użytkownikami

Następnie należy w ustawieniach BIOS (w tym przypadku w ustawieniach programu) bootowanie z płyty, pendrive, obrazu płyty w zależności od tego jakim nośnikiem z systemem dysponujemy.



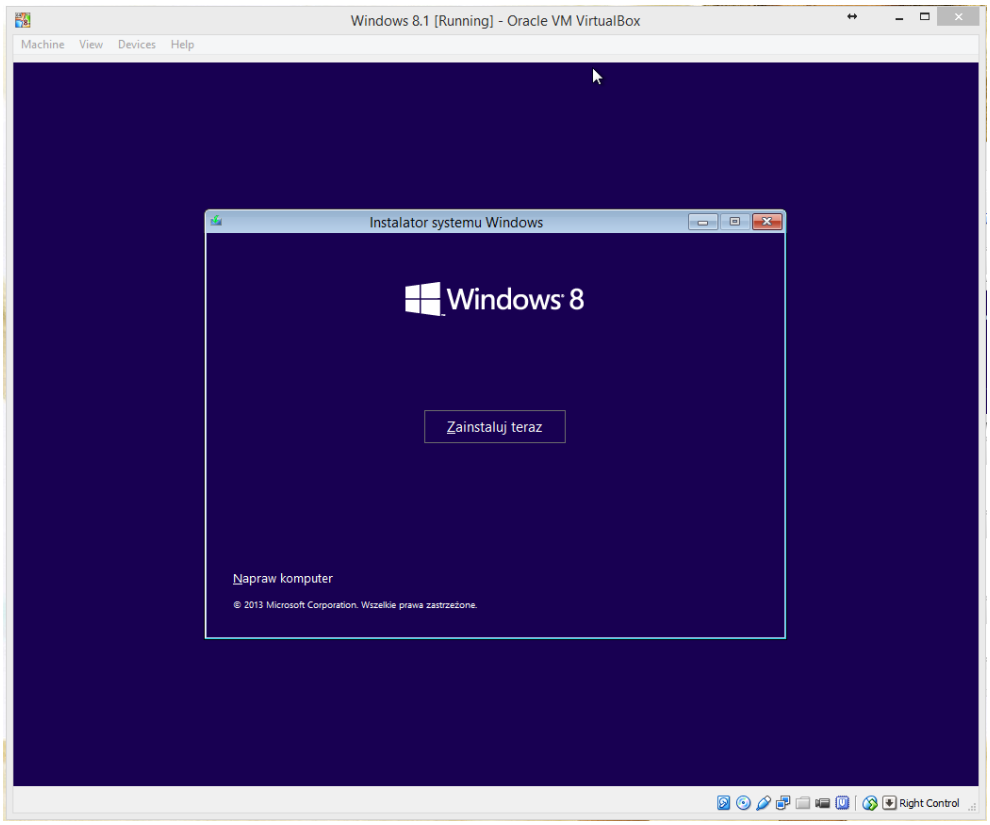
Dodawanie obrazu ISO do bootowania systemu który atakujemy

Po wybraniu kolejności bootowania w BIOS (zmianie ustawień w systemie wirtualnym). Należy zapisać zmiany i ponownie uruchomić system.



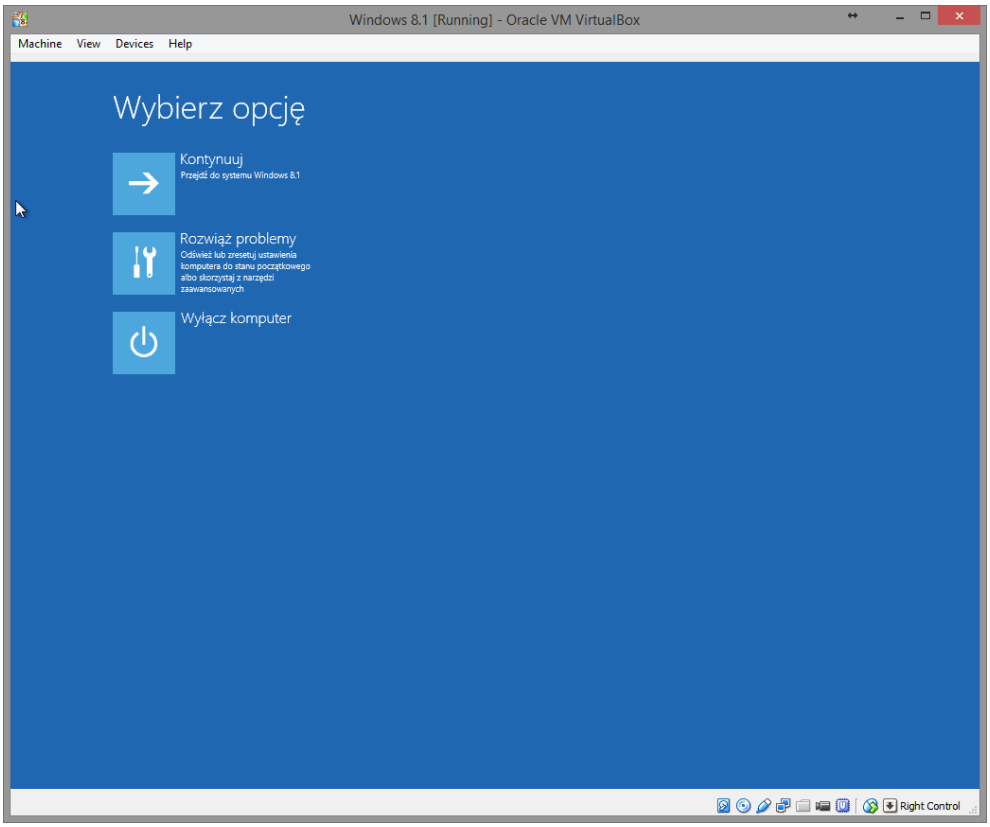
Menu wyboru języka

Gdy po zaakceptowaniu bootowania instalacji systemu pojawi się powyższe menu należy wybrać odpowiadające nam języki i klikamy przycisk „Dalej”



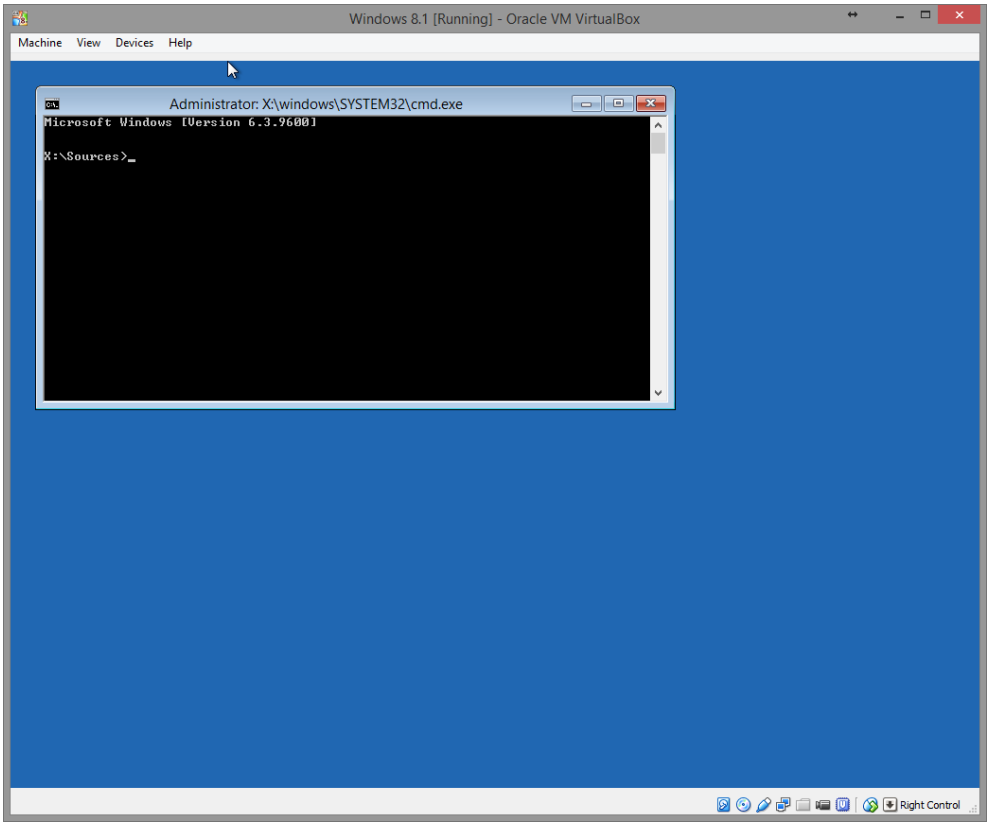
Menu wyboru instalacji lub naprawy systemu.

Po pojawieniu się powyższego okna należy wybrać opcję „Napraw komputer”.



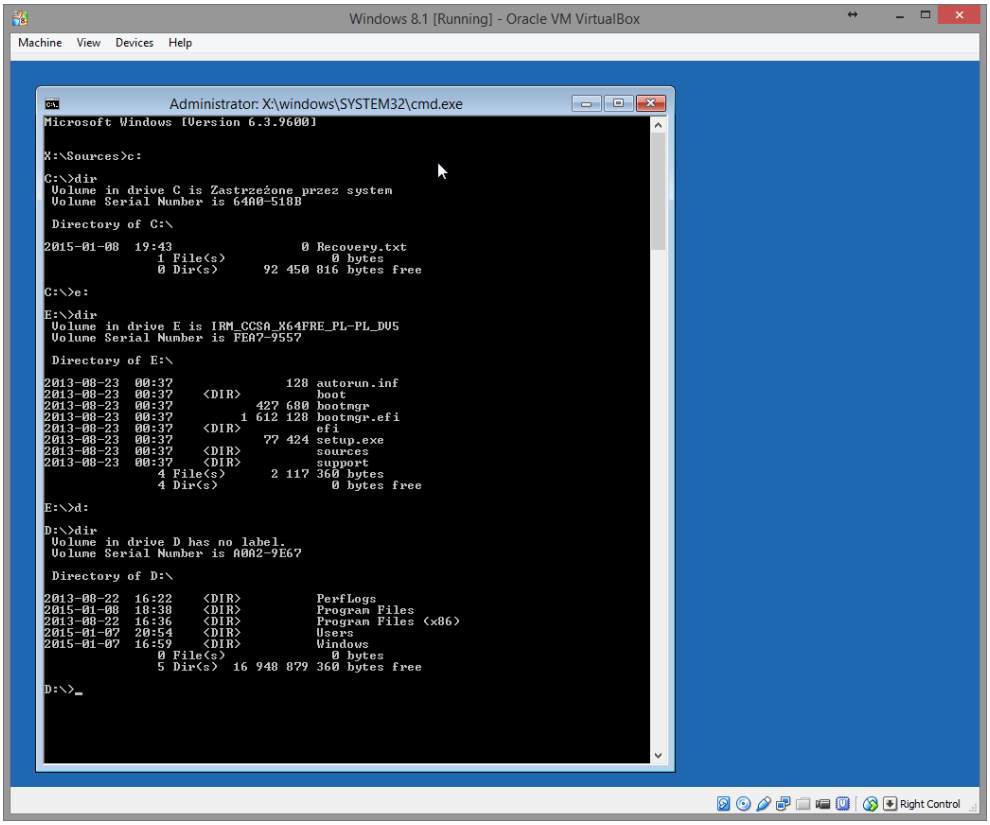
Menu wyboru dalszych czynności.

Następnie wybieramy opcję **Rozwiąż problemy → Opcje zaawansowane → Wiersz polecenia**.



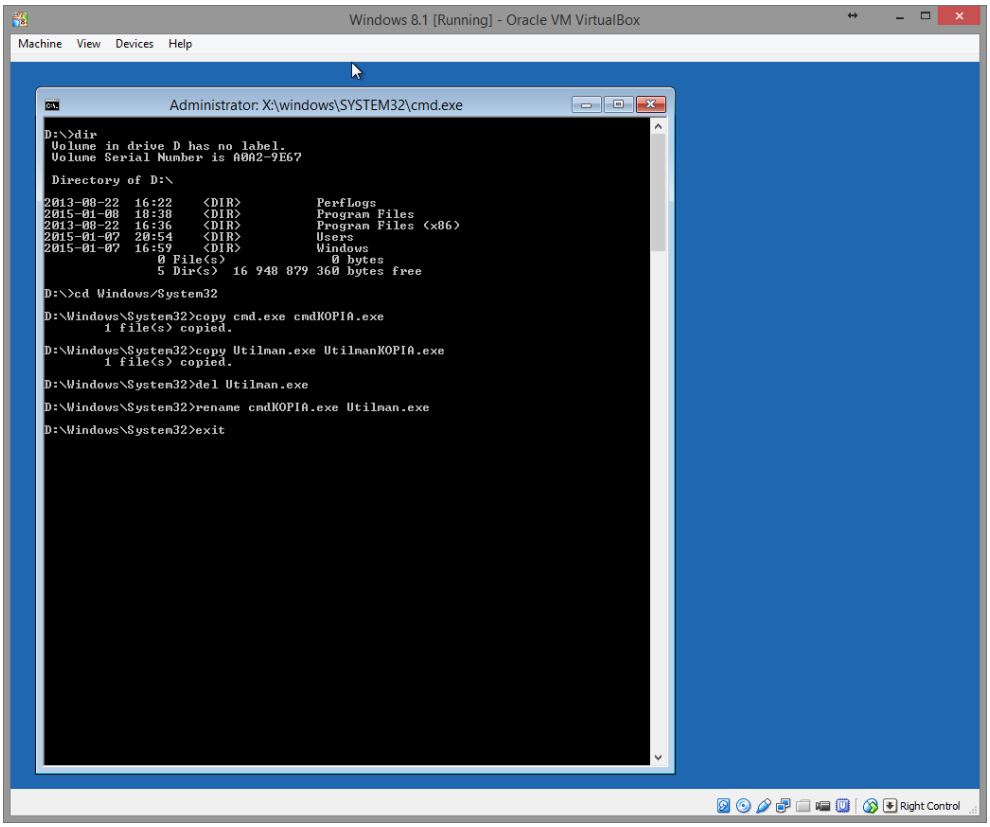
Uruchomiony wiersz poleceń

Po przejściu przez wybrane opcje powinnyśmy uzyskać okno konsoli (cmd).



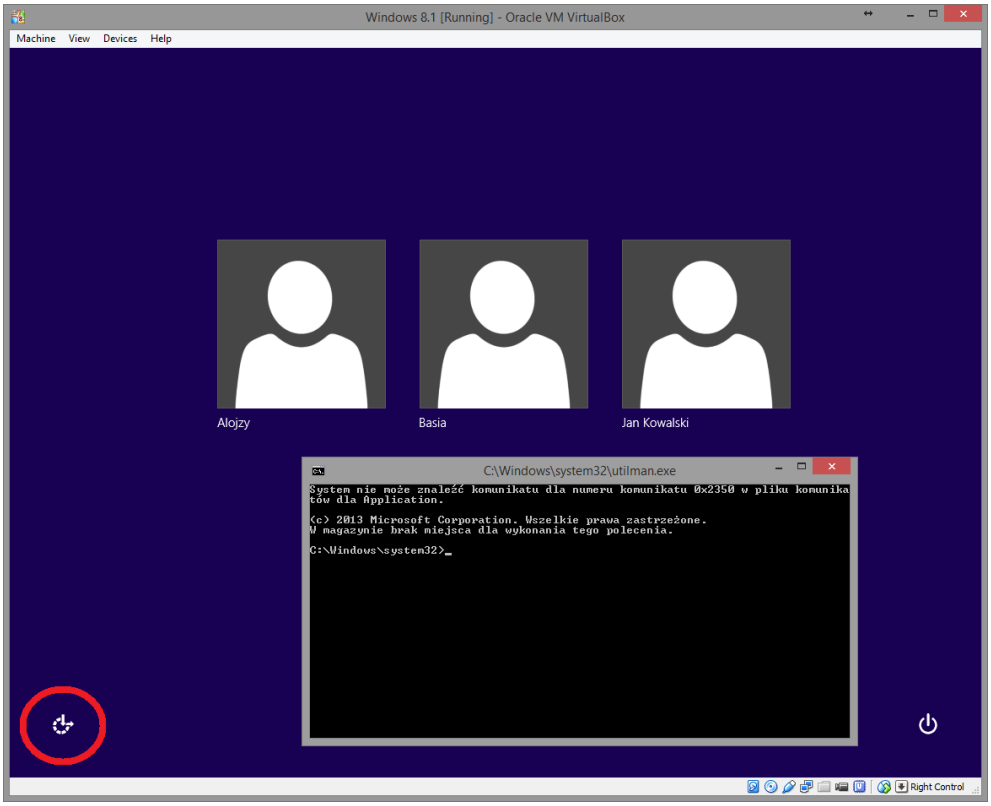
Wyszukiwanie dysku z atakowanym systemem operacyjnym.

Następnie za pomocą poleceń „**c:**”, „**dir**”, „**d:**”, „**dir**” itd. odnajdujemy dysk zawierający zainstalowany system operacyjny na którym próbujemy zmienić zapomniane hasło.



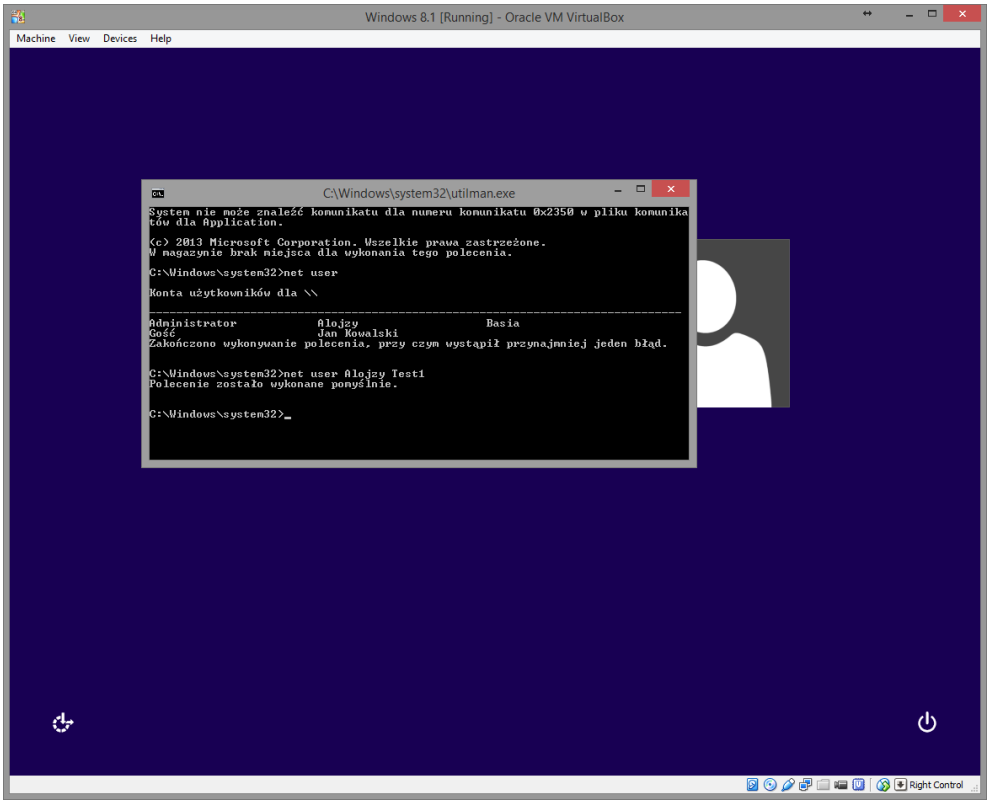
Podmiana pliku Utlman.exe na plik cmd.exe.

Gdy odnaleźliśmy atakowany system następnie musimy przejść do folderu System32 poleceniem: ***cd Windows/System32.*** Po poprawnym przejściu do folderu musimy utworzyć kopie 2 plików: *cmd.exe* (***copy cmd.exe cmdKOPIA.exe***), *Utilman.exe* (***copy Utilman.exe UtilmanKopia.exe***). Program *cmd.exe* to nic innego jak nasz konsola systemowa. Program *Utilman.exe* jest to Centrum ułatwień dostępu. Dlaczego wybieramy ten program zobaczycie w następnych krokach. Po utworzeniu kopii plików wykonywalnych programów należy usunąć plik *Utilman.exe* (**del Utilman.exe**) ,a następnie zmienić nazwę plikowi *cmdKOPIA.exe* na Utilman.exe (**rename cmdKOPIA.exe Utilman.exe**). Po zakończeniu tych czynności wpisujemy polecenie **exit** aby wyjść z konsoli. Następnie w menu klikamy „*Kontynuuj*”.



Uruchomienie konsoli z poziomu logowania do systemu.

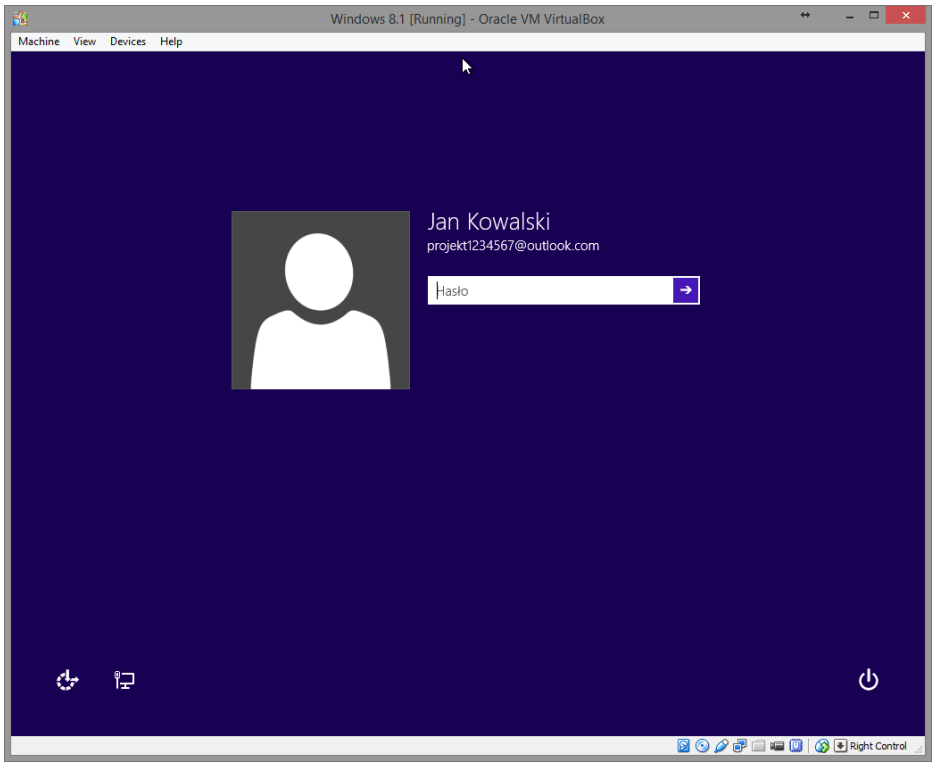
Po uruchomieniu się systemu podczas gdy wygląd ekranu logowania nie uległ zmianie, należy kliknąć na ikonę zaznaczoną czerwonym kółkiem. Jest to podmieniony program Centrum ułatwień dostępu na konsole systemową.



Zmiana hasła atakowanego konta lokalnego.

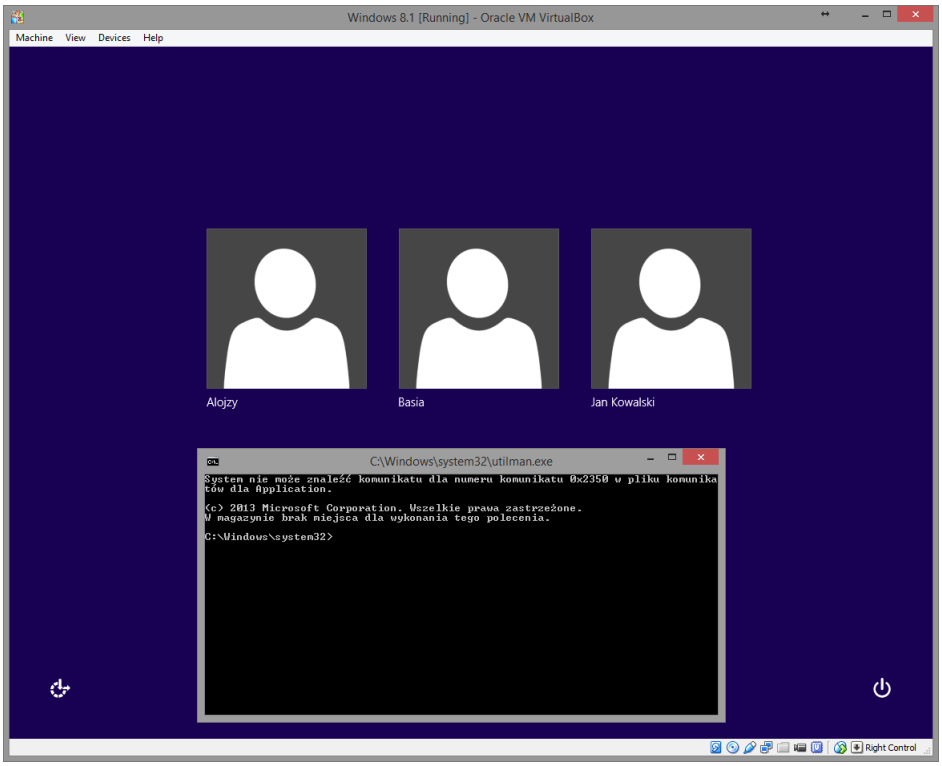
Następnie wpisujemy polecenie: **net user,** które wyświetla wszystkich użytkowników komputera. Gdy zobaczymy listę użytkowników należy wybrać z niej użytkownika któremu chcemy zmienić hasło poleceniem (konto: Alojzy): **net user Alojzy Test1**. (Nazwa konta: Alojzy, nowe hasło dla konta: Test1). Następnie poleceniem **exit** wychodzimy z konsoli. Hasło na naszym koncie zostało zmienione i już uzyskaliśmy dostęp do konta. Aby przywrócić poprzednią funkcję aplikacji Utilman.exe należy wykonać polecenia od Printscreen 2.3 do Printscreen 2.8 do polecenia **cd Windows/System32** włącznie. Następnie należy usunąć plik Utilman.exe (**del Utilman.exe)**, następnie zmienić nazwę pliku *UtilmanKOPIA.exe* na *Utilman.exe* (**rename UtilmanKOPIA.exe Utilman.exe)**. Wpisać komendę **exit** i następnie wybrać „Kontynuuj".

2. *Uzyskiwanie dostępu do danych konta Microsoft.*

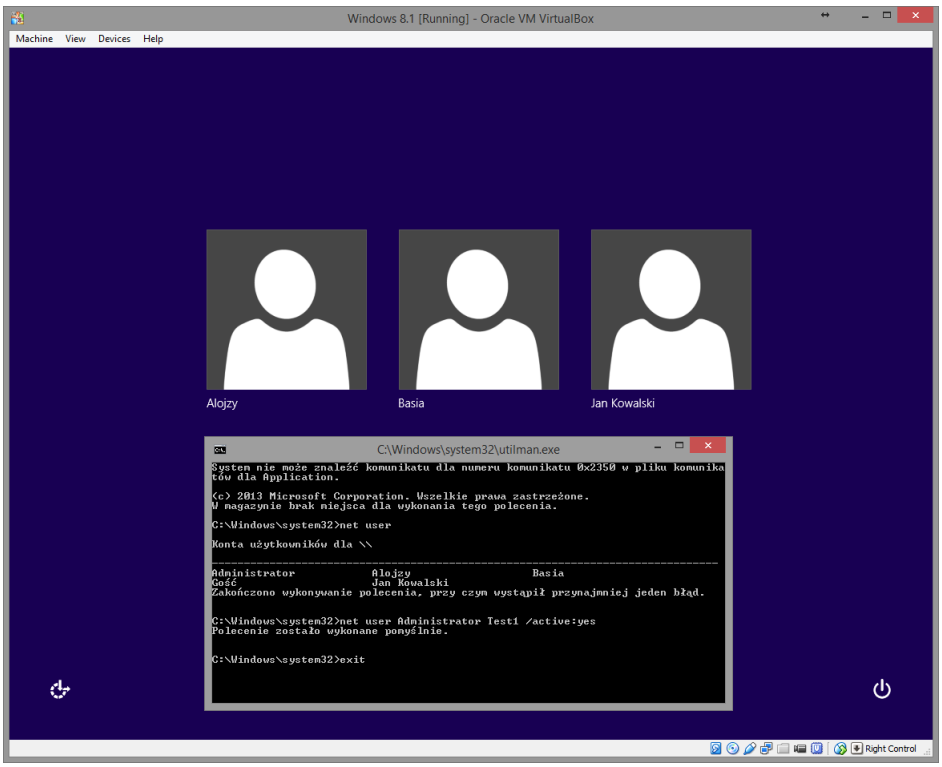


Windows 8.1 z utworzonym użytkownikiem z hasłem (konto Microsoft)

Wszystko robimy w taki sam sposób jak w przykładzie z kontem lokalnym do PrintScreena 3.9., ponieważ nie możemy zmienić w konsoli hasła użytkownika z poziomu konsoli systemowej musimy uaktywnić konto Administratora w systemie (domyślnie jest ono nieaktywne). Jedyne co możemy to uzyskać dostęp do wszystkich plików których używał dany użytkownik aby odzyskać/ukraść najważniejsze dokumenty użytkownika.

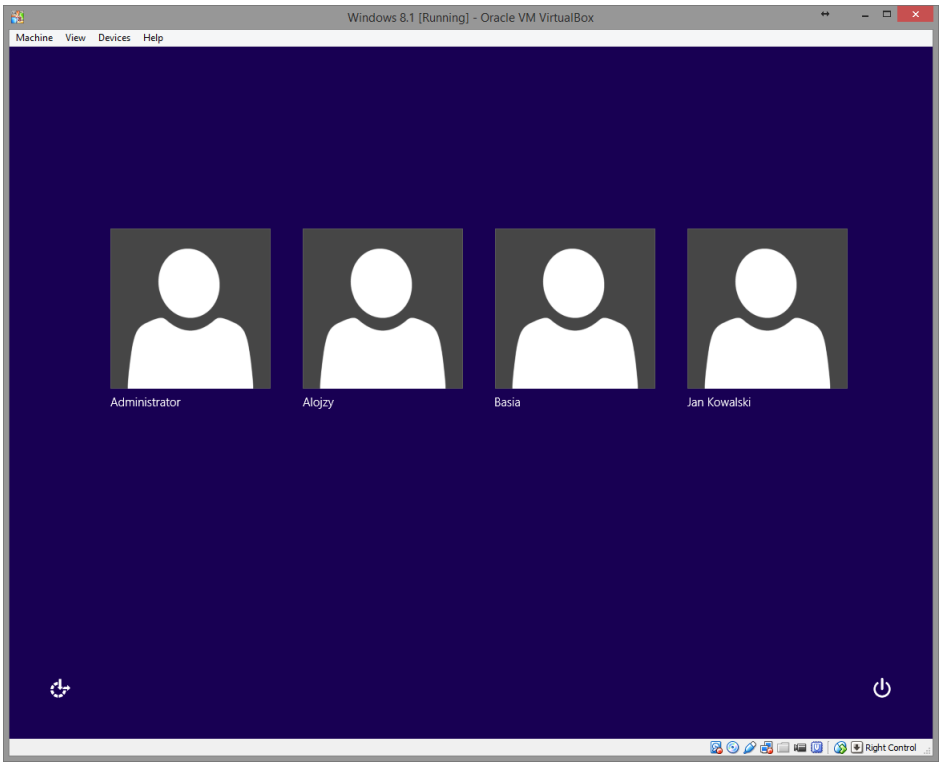


PrintScreen 2.2: Uruchomienie konsoli z poziomu logowania do systemu.



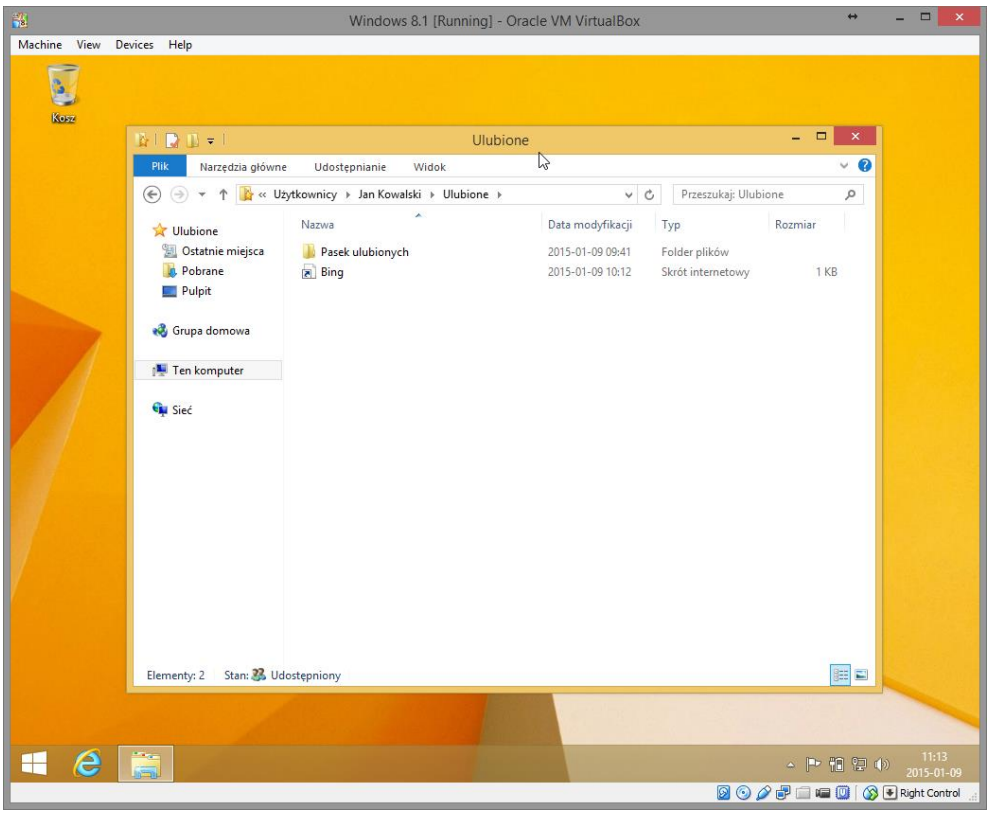
Aktywowanie konta Administratora.

Następnie należy uruchomić ponownie komputer.



Wybór konta do zalogowania.

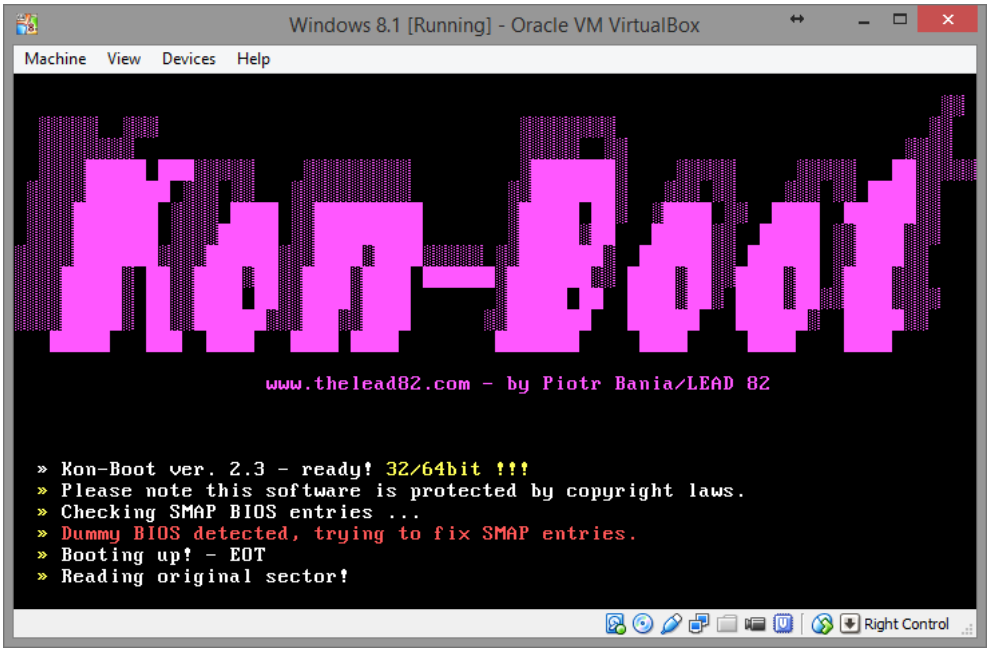
Uzyskujemy dostęp do wszystkich plików systemu, ponieważ mamy uprawnienia Administratora więc także dostęp do folderu Moje dokumentu użytkownika atakowanego.



Dostęp do danych z konta Jan Kowalski (konto Microsoft).

3. *Kon-Boot 2.3*

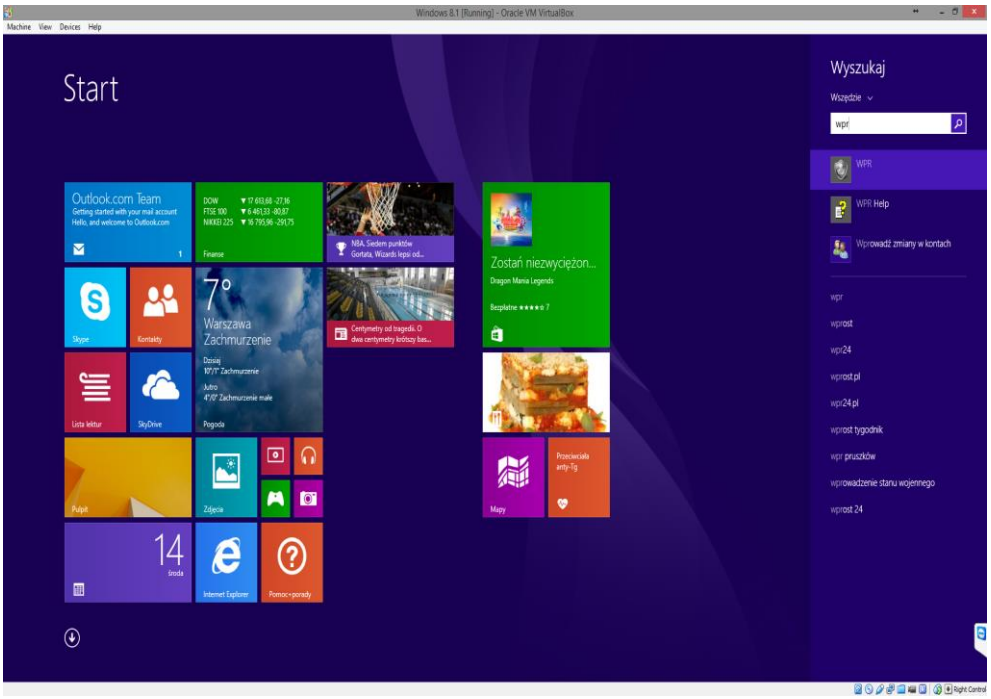
Za pomocą programu Kon-Boot można bez znajomości hasła użytkownika dostać się do systemu operacyjnego. Należy przygotować bootowalną płytą lub pendriva i po ponownym uruchomieniu komputera pojawi się poniższe okno. Następnie po załadowaniu systemu każde stworzone konto nie będzie posiadało hasła. Jedynym minusem tego rozwiązania jest brak możliwości zalogowanie się na konto połączone z kontem Microsoft (hasło nie ulega zmianie). Po wyjęciu bootowalnej płyty bądź pendrive wszystko wraca do stanu poprzedniego (o ile nie dokonaliśmy żadnych zmian w koncie na które się logowaliśmy). Jest to bardzo wygodne narzędzie jeżeli potrzebujemy bardzo szybkiego dostępu do każdego konta.



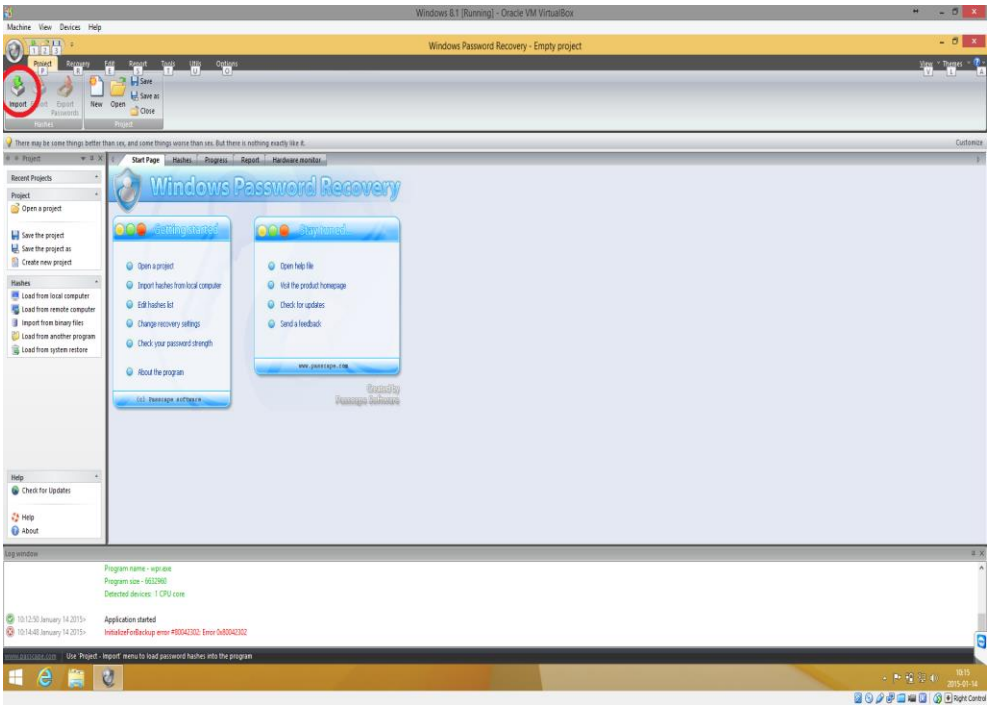
Okno ładowania programu Kon-Boot.

4. *Windows Password Recorvery*

Za pomocą programu Windows Password Recorvery można w sposób bardzo szybki uzyskać hasła wszystkich użytkowników utworzonych na komputerze. Niestety program ten jest programem płatnym, a w wersji testowej program odkrywa tylko pierwsze 3 litery hasła. Jednak na potrzeby laboratorium na utworzonych obrazach jest pełna wersja programu.

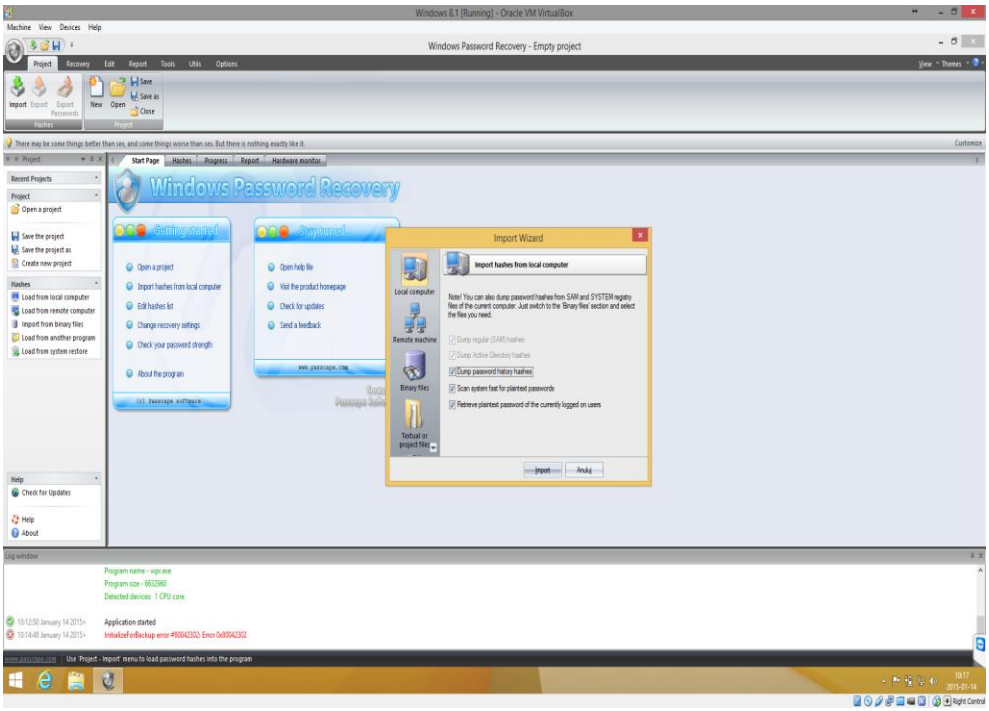


Menu start z wyszukaniem programu Windows Password Recorvery.

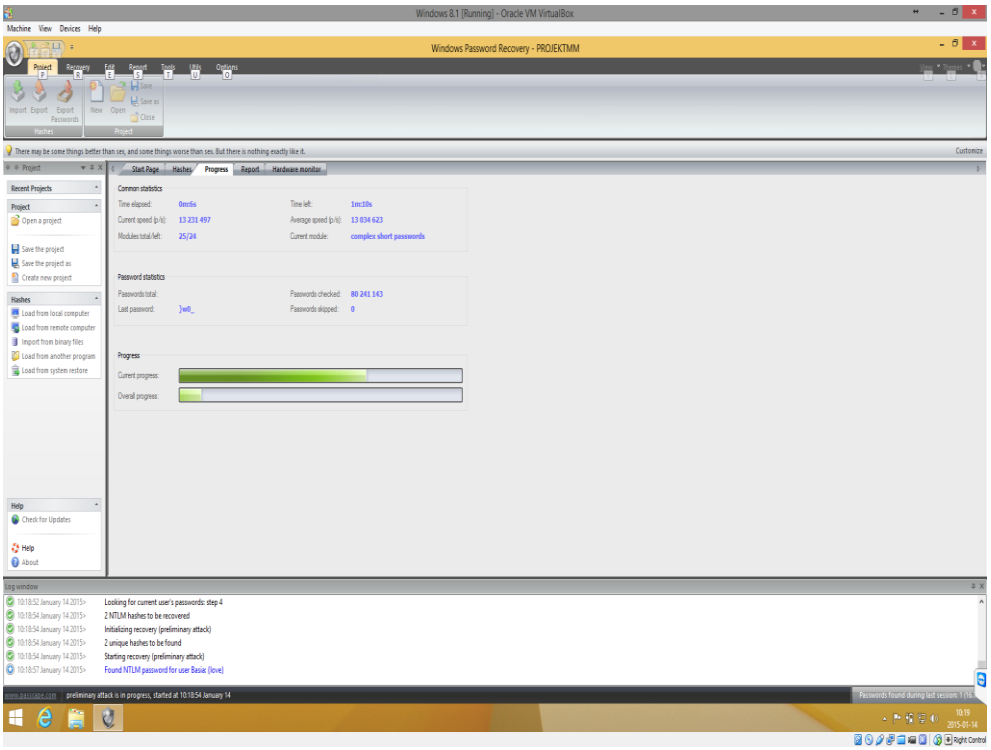


Uruchomione okno programu Windows Password Recorvery.

Po uruchomieniu programu należy wybrać opcję import aby aplikacja mogła pobrać pliki z zaszyfrowanymi hasłami systemu.

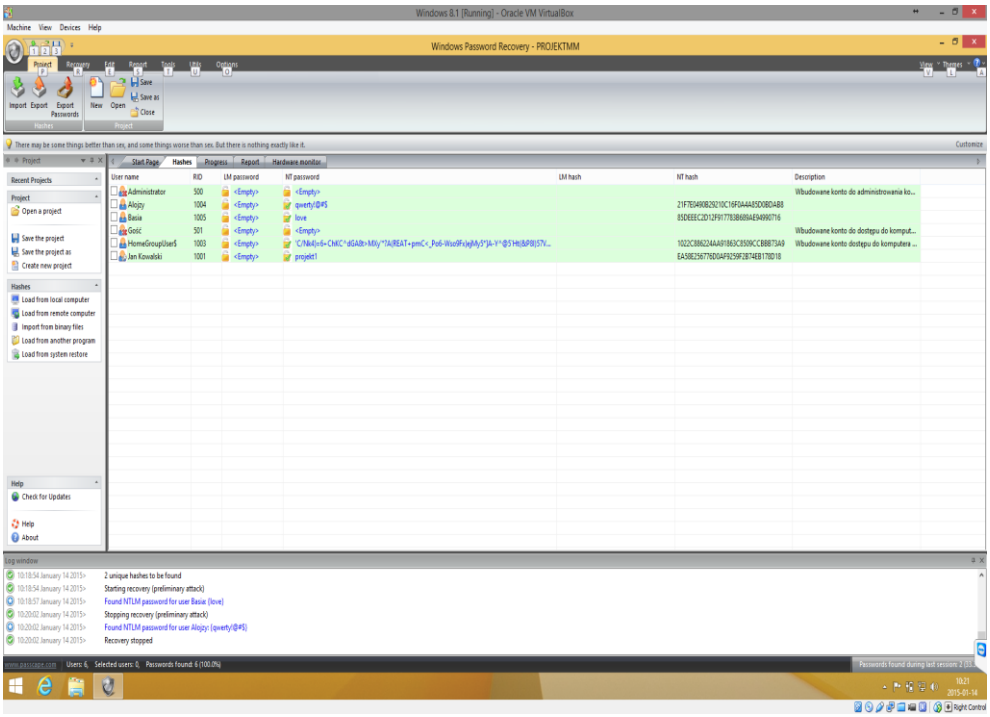


Import plików zawierających hasła.



Odzyskiwanie haseł wszystkich użytkowników systemu.

Długość odzyskiwania hasła zależy z ilu i jakich znaków się składa. Najprostsze hasła odszyfrowane są w parę sekund, a te bardziej złożone ze znaków specjalnych są dużo cięższe do rozszyfrowania i może to trwać ok. 10 minut.



Odszyfrowane wszystkie hasła systemu Windows.