Antywirus – Instrukcja

Wszystkie używane moduły są natywne dla pythona. Wymagania poprawnego funkcjonowania aplikacji to umieszczenie wszystkich czterech modułów w jednym folderze, razem z folderem scanReports na raporty, oraz signatures, który zawiera pliki z syganturami. Aplikacja niestety funkcjonuje tylko na konsoli linuxowej, ze względu na to że moduł curses, używany do implementacji gui w tej aplikacji nie jest wspierany przez windowsową consolę.

Aplikację można uruchamiać w dwóch trybach: interaktywnym, bądź za pomocą podania argumentów w terminalu:

Tryb z podaniem argumentów:

Jeśli podane zostaną argumenty, to aplikacja oczekuje jednego agrumentu pozycyjnego, w fromie ścieżki do pliku/katalogu do zeskanowania. Posiada też flagi:

-slow – skanowanie wszystkich plików, nie tylko nowych, zmodyfikowanych lub wcześniej nie skanowanych

-cut – powoduje podjęcie próby wicięcia wirusa, dla zainfekowanych plików dla których jest to możliwe

-denied – obok listy zainfekowanych plików, aplikacja wypisze również listę plików bądź katalogów do których dostęp był ograniczony

Bez flagi denied, jeśli nic nie zostało wykryte, aplikacja nic nie wypisuje. Jeśli jednak wykryje infekcje, to wypisuje je w formacie:

Ścieżka1 -> nazwa wirusa1

Ścieżka2 -> nazwa wirusa2…

Następnie, jeśli flaga -cut była podana, wypisuje ‘fixed:’, poczym listę naprawionych plików

I na końcu, jeśli flaga -denied była podana, wypisuje ‘denied access to:’, poczym listę ścieżek bez dostępu.

Tryb interaktywny:

W tym trybie, po załadowaniu sygnatur otwiera się menu, nawigowane strzałkami:

Simple scan – wykonanie pojedyńczego skanu danego katalogu/pliku

Periodic scan – wejście do trybu skanowania cyklicznego

Po wybraniu dowolnej z opcji, należy wybrać ścieżkę skanowania:

Wpisywać ścieżkę można manualnie w wyświetlonym polu tekstowym, bądź też można strzałką w dół wejść w listę propozycji pod polem. Na zielono pokazane są katalogi, na biało pliki. Dopełnianie klawiszem TAB także działa. Jeśli ścieżka wyświetla się w kolorze czerwonym, to wprowadzona ścieżka nie istnieje. Jeśli propozycje się nie wyświetlają, a ścieżka nadal jest biała, to albo nie ma dostępu do wpisanego katalogu, albo jest on pusty. Po wprowadzeniu poprawnej ścieżki, zatwierdza się ją klawiszem enter.

Simple scan:

Po zapytaniu użytkownika, czy chce on używać opcji szybkiego skanowania, rozpoczyna się skanowanie podanego katalogu.

Procentowy wskaźnik ukończenia może nie być miarodajny, jeśli w skanowanym katalogu pliki znacząco różnią się rozmiarem.

Procentowy wskaźnik przy ścieżce oznacza postęp w obrębie pliku (ten jest miarodajny)

Klawiszem escape można przerwać skan.

Po ukończeniu bądź przerwaniu skanu, pojawia się ekran stanowiący o rezultacie skanu. Jeśli rezultat nie mieści się na ekranie, to można strzałkami go przewijać.

Poza powrotem do menu głównego (ESC), dostępne są na tym etapie także opcje:

Zachowanie rezultatu (S) – rezultat skanu zostanie zapisany do pliku, w folderze scanResults

Próba naprawienia zainfekowanych plików (F) – antywirus spróbuje wyciąć wirusa z tych plików, dla których jest to możliwe. Doda do rezultatu komunikat czy udało się naprawić jakieś pliki, a jeśli tak to jakie.

Periodic scan:

Po wyborze ścieżki, program prosi też o wybranie odstępu czasowego między skanami. Maksymalny możliwy czas to 99 godzin i 59 min, a minimalny to 1 minuta. Tyle czasu program będzie czekał od ukończenia skanu, aby rozpocząć następny (oraz przed rozpoczęciem pierwszego skanu).

Podczas skanowania widoczny będzie ten sam ekran co dla opcji Simple Scan, oraz jeśli znalezione zostaną jakieś infekcje, to program wyświetli użytkownikowi rezultat, aby ten mógł zareagować. Jeśli żadna infekcja nie zostanie znaleziona, to program przechodzi do czekania na kolejny skan.

Ten skan również można przerwać. Gdy użytkownik wyjdzie z ekranu oczekiwania na skan, proces cyklicznego skanowania zostanie przerwany.

Testy:

Wszystkie pliki i foldery potrzebne do uruchomienia testów antywirusa znajdują się w repozytorium. Mimo tego, jeden z testów (test_cmdScanDenied) nie będzie przechodził, ponieważ aby tak było, musi być zabroniony dostęp do katalogu /testFiles/scanTest/hyh oraz do pliku /testFiles/scanTest/ttt.txt. Jeżeli lokalnie ustawi się taki brak dostępu, to test przejdzie. Moduł testowy AntivirusTest oczekuje także, że python dodany jest do zmiennej path, i dostępny będzie pod komendą ‘python3’.