Odzyskiwanie danych 2019
Zadania kwalifikacyjne na WWW15

Arkadiusz Kozdra

11 maja 2019

1 Przygotowanie

Do wykonania poniższych zadań polecam serdecznie ustawić sobie linuksa (np. Manjaro). Jeśli jest to straszliwie przerażające, to zachęcam do użycia maszyny wirtualnej (np. VirtualBox) i zainstalowania linuksa w środku. Jeśli nawet to jest za trudne, to w ostateczności można użyć oprogramowania na Windę (HxD lub windowsowa wersja Midnight Commandera).

Nie bój się szukać znaczenia słów, których nie rozumiesz! Pomoże ci w tym wikipedia i w przypadkach wyjątkowo trudnych słów OSDev wiki (niestety tylko w jęz. angielskim). Zawsze można pisać do mnie (`arek_koz maupa o2 kropka pl`), wpisując w temacie WWW15. Chętnie odpowiem na wszystkie pytania.

Nie musisz rozwiązywać wszystkich zadań, ale nie są one trudne. Odpowiedzi wyślij na moją pocztę elektroniczną (też wpisz WWW15). Jestem gotów przyznawać punkty częściowe, więc śmiało. (dla zainteresowanych: mój klucz publiczny jest m.in. na http://hkps.pool.sks-keyservers.net)

W przypadku wybrania linuksa należy zainstalować program `mc` („Midnight Commander"). Na linuksie przeważnie nie instaluje się programów ściągając je z czeluści internetu, tylko z linii poleceń (na Manjaro poleceniem `pacman -S`) lub z graficznego programu do zarządzania zainstalowanymi programami (na Manjaro jest to `octopi`). (artykuł o instalowaniu na Manjaro)

Po zainstalowaniu Midnight Commandera otworzyć terminal w katalogu zawierającym zawartość rozpakowanego archiwum i wykonać polecenie `mc`. Ukaże się niebieskie tło rodem z lat 90. i lista plików. Strzałkami najechać na plik, który zmieniamy i wybrać podgląd przyciskiem F3 (to otworzy plik do odczytu, zgodnie z opisem na dole okna), a następnie przełączyć podgląd szesnastkowy / ASCII za pomocą F4.

Oprócz `mc` istnieje parę innych programów, w tym `hexedit`, `hexeditor`, `xxd`, `hd`, które służą do przeglądania plików z danymi i dysków. Jeśli chcesz, przetestuj je i wybierz swój ulubiony.

2 Czy umiesz korzystać ze swojego sprzętu

Rozwiązaniem jest zrzut ekranu, na którym pokażesz swojego linuksa, `mc`, albo chociaż tego HxD na innym systemie, z otwartym szesnastkowo jakimś plikiem.

3 Szukanie w pliku

Żeby wykazać się umiejętnością znajdywania w pliku danych binarnych, znajdź fragment danych binarnych zapisanych w pliku `losowedane.bin` dostępnym w archiwum z zadaniami, który zaczyna się od bajtów `80 9F 4D 9A 7E AB 56` i kończy na `90 32 0F F3 57 1E` (bez obaw, jest tylko jeden).

Odpowiedź na to zadanie powinna zawierać zapis szesnastkowy (jak w poleceniu), oba końce, które podałem, i to, co pomiędzy nimi. Oprócz tego napisz (w dowolnym formacie), na jakiej pozycji w pliku znajduje się ten ciąg bajtów (od którego z kolei bajtu w pliku zaczyna się ten ciąg).

4 Przeglądanie dysku przenośnego (trudniejsze)

W tym celu wykorzystaj dysk przenośny USB lub kartę pamięci SD czy też cokolwiek podobnego (najlepiej nie duży dysk zewnętrzny, ani dysk wewnętrzny).

Utwórz na tym dysku plik `ELOBEKON.TXT` (istotne jest, by nazwa miała mniej niż 9 znaków i była zapisana wielkimi literami) i wpisz do niego trochę tekstu (podpowiedź: polskie znaki będzie za chwilę trudniej znaleźć!). Zapisz plik, wysuń bezpiecznie dysk, a następnie włóż go z powrotem i otwórz go w swoim ulubionym narzędziu do oglądania szesnastkowego. (Otwórz cały dysk, na linuksie będzie to jeden z plików `/dev/sda`, `/dev/sdb`, ...; nie każdy z edytorów umie to zrobić!).

Na dysku zlokalizuj nazwę pliku i jego treść. Odpowiedzią do tego zadania jest pozycja (w bajtach) początku i końca treści pliku względem dysku i podobna pozycja nazwy pliku. Jeśli odpowiedź na któreś pytanie nie mieści się w wyznaczonym przeze mnie formacie (na przykład nazwa w dwóch miejscach), możesz odpowiedzieć po swojemu.

W szczególności możesz wysłać zrzuty ekranu z dysku otwartego w tym narzędziu.