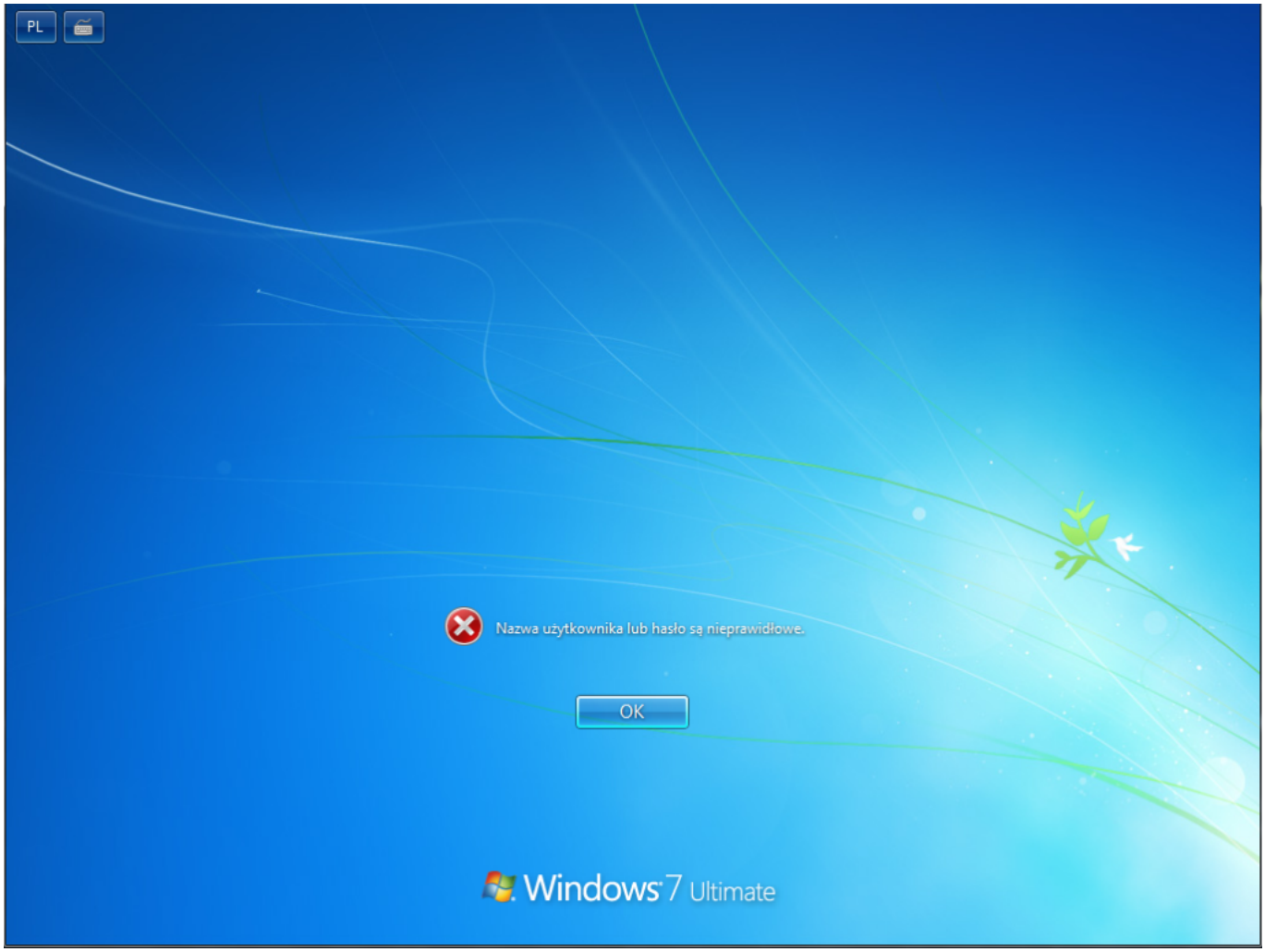
Każdemu może zdarzyć się zapomnieć hasło. Do tej pory byłem święcie przekonany, że jestem w stanie zapamiętać wszystkie loginy i hasła do zarządzanych przeze mnie systemów. Aż do dziś. Z czystego lenistwa zamiast przeinstalować komputer, który do tej pory pracował w domenie postanowiłem użyć go jako odrębnej stacji. I tu pojawił się problem. Okazało się, że nie znam hasła do użytkownika lokalnego.

Ale zacznijmy od początku. Nie sprawdzając najpierw czy mam gdzieś zapisane/zapamiętane hasło do konta administratora (powiedzmy, że był to user „pht”) wyklikałem odłączenie od domeny i podłączenie z powrotem do grupy roboczej „WORKGROUP”. Ponowne uruchomienie, aby system wczytał nowe ustawienia, komputer zaopatrzony w system operacyjny Windows 7 wstał dosyć szybko jak na tylko jeden gigabajt ramu. Moim oczom ukazał się panel logowania, przekonany o swoim sukcesie postanowiłem się zalogować. Moim oczom ukazał się taki oto obrazek:

How to open the window(s) – Czyli otwieranie „okna” bez hasła.



Nie ukrywam, że mojemu zdziwieniu nie było końca gdy po wpisaniu wszystkich możliwych kombinacji system nadal odpowiadał mi jedynie krótkim komunikatem informującym, o złym loginie lub haśle. Wiele osób, jak i ja kilka lat temu w tym momencie rzuca się do poszukiwać odpowiedzi w google. Myślę, że najtrafniejszym zapytaniem, które powinniśmy wpisać w wyszukiwarkę jest „How hack windows 7 lost password”. Kilka lat temu gdy pojawiła się na rynku systemów operacyjnych Vista, w internecie pojawiły się sprytne protipy jak obejść panel logowania gdy zapomnimy hasła (gdy zapomnimy, przecież nikt nikomu nie będzie się włamywał ;>).

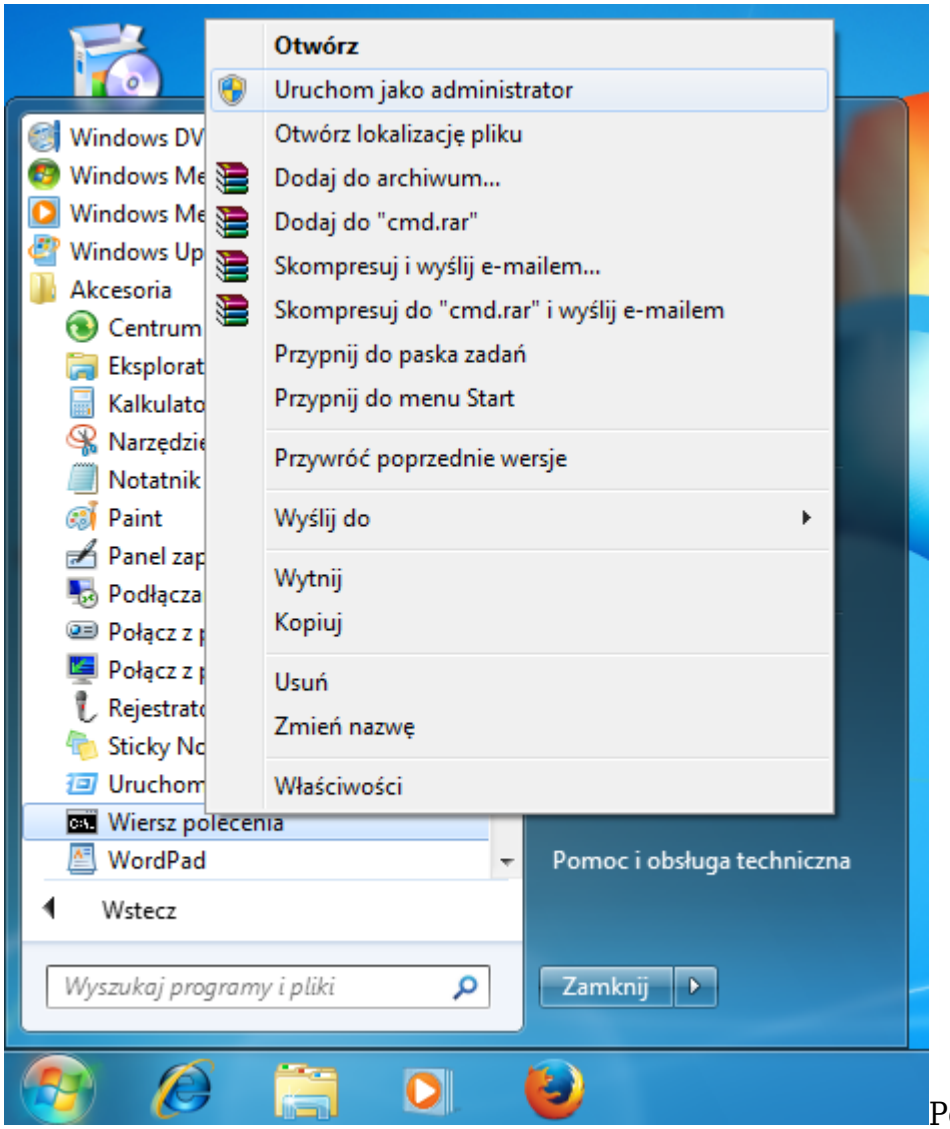
Oczywiście jako, że juz wtedy byłem zapalonym fanem rozwiązań bezpieczeństwa rożnej skali, kilka z owych protipów zapadło mi w pamięć. Z okazji mojego zapominalstwa postanowiłem podzielić się z swoimi czytelnikami małym „How to open the window(s)” .

Pierwsza, podstawową rzeczą, która chcę wyjaśnić to kwestia co dokładnie chcemy zrobić oraz przede wszystkim gdzie znajduje się podatność, którą wykorzystamy.

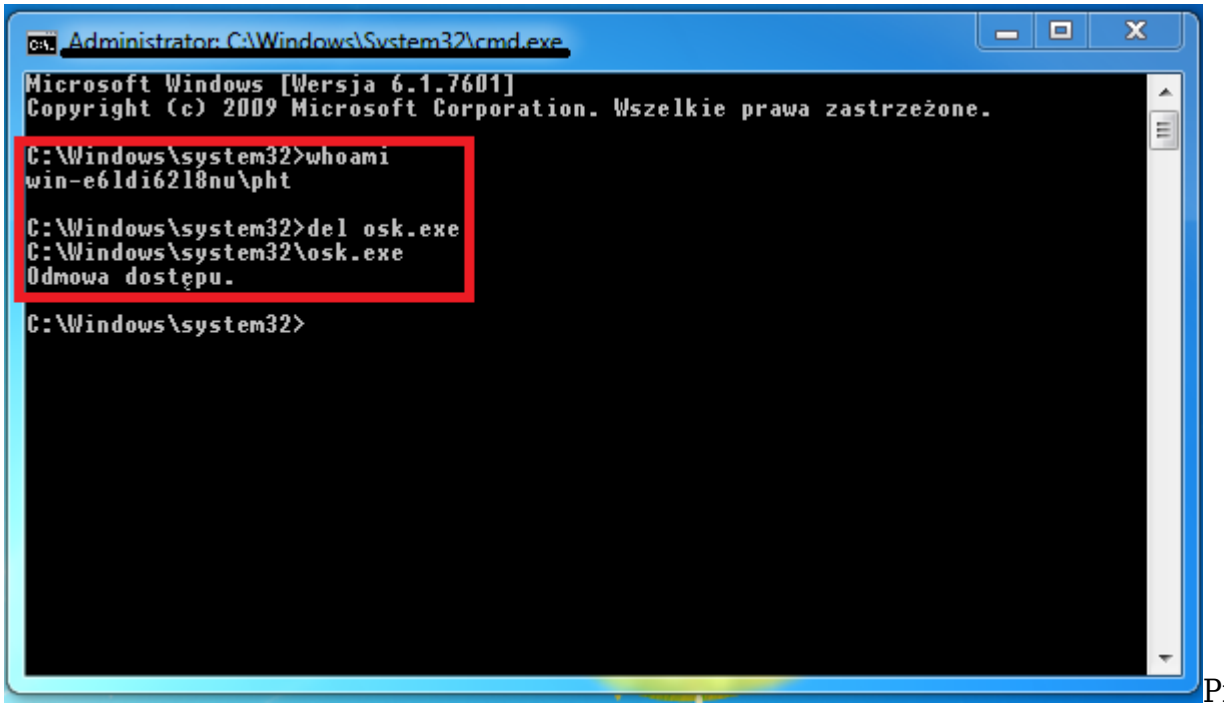
Spis treści

1. Podatność

Od dawna mówi się, że sam windows jest jednym wielkim bugiem. Nie uważam, by było to do końca prawda. To na co chcę zwrócić uwagę jest typowy problem związany z tym z jakimi uprawnieniami są uruchamiane programy na naszym komputerze. Każdy średnio zaawansowany użytkownik windowsa zna zapewne Wiersz Poleceń (cmd.exe). Chwilowo zapomnijmy o tym, że chcemy obejść hasło logowania do systemu i przypuśćmy, że jesteśmy zalogowani jako administrator systemu. Zobaczmy co może zrobić maksymalnie użytkownik. Aby uruchomić wiersz poleceń w trybie administratora klikamy na Start -> Wszystkie programy -> Akcesoria, a następnie prawym uruchom jako administrator.



Po wykonaniu powyższych instrukcji ukaże się nam czarne okienko wiersza poleceń.



Pierwszym co rzuca się nam w oczy po otwarciu naszego cli (command line, inna nazwa Wiesza Poleceń) jest tytuł okna, czyli „Administrator: C:\Windows\System32\cmd.exe”. Podpowiada nam to dwie rzeczy:

- Otworzyliśmy cmd.exe z uprawnieniami Administratora
- cmd.exe znajduje się w katalogu „C:\Windows\System32”

Musimy pamiętać, że katalog „C:\Windows\System32” jest katalogiem ściśle systemowym. Więc jedynie administrator powinien mieć możliwość edycji tego katalogu. Aby sprawdzić możliwość edycji plików w tym katalogu spróbujemy coś usunąć. Przykładowo może być to osk.exe (plik wykonywalny zawierający klawiaturę ekranową), ale zanim to zrobimy, użyjmy komendy „whoami”. Komenda ta zwraca nam odpowiedź z jakimi uprawnieniami wykonujemy działania, czy też jako jaki user jesteśmy zalogowani. Kilka kroków temu uruchomiliśmy Wiersz Poleceń z uprawnieniami administratora. Oznacza, to że system powinien zwrócić nam login odpowiadający użytkownikowi o najwyższych uprawnieniach. Jak widać na powyższym obrazku cmd zwrócił nam „win-e6ldi62l8nu/pht” gdzie:

- win-e6ldi62l8nu – domena (gdy komputer nie jest połączony z domeną ta wartość przyjmuje hostname)
- pht – login użytkownika

Sugeruje to, że użytkownik „pht” w tym momencie jest użytkownikiem o najwyższych

uprawnieniach. Nic bardziej mylnego. Kolejna wprowadzona komenda jasno pokazuje, że tak nie jest. Po wprowadzeniu polecenia „del osk.exe” otrzymujemy informacje o braku dostępu do pliku. Co to znaczy?

W tym momencie zaczyna się właściwa zabawa. Często windows przy instalacji prosi o uruchomienie w trybie administratora (tak jak zrobiliśmy w tym przypadku) i wtedy to wystarczy. Czy to znaczy, że nad systemowym Administratorem jest ktoś z większymi uprawnianiami? Odpowiedź jest **prawie** prosta. Dlaczego prawie? Ponieważ, z pewnością można stwierdzić dwie rzeczy.

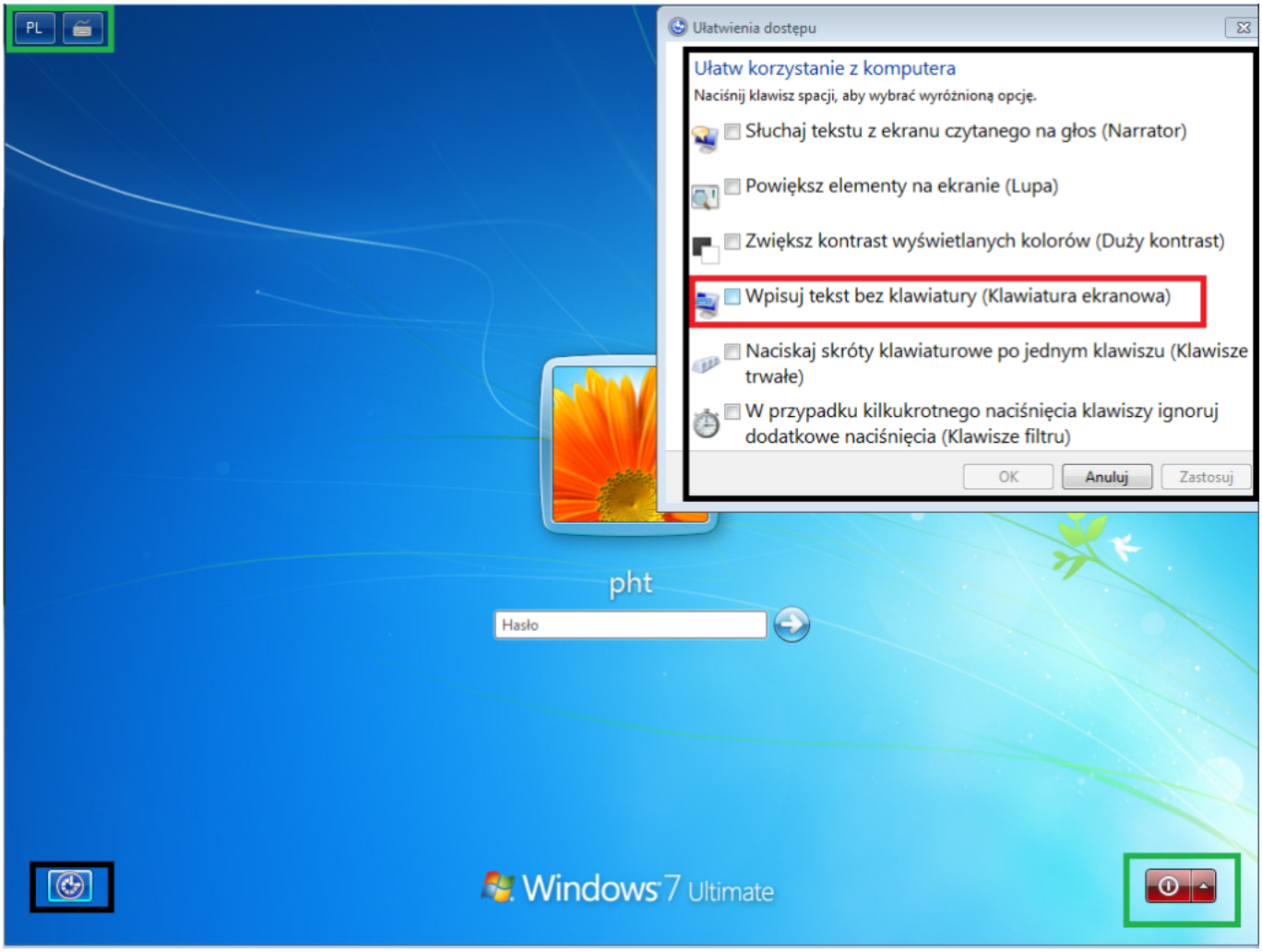
- Tak, jest użytkownik z większymi uprawnianiami
- Żaden użytkownik systemowy nie ma dostępu do katalogów systemowych

To rozwiązanie sprawia, że w systemach Vista i wyżej zniknął problem przypadkowego usunięcia istotnych danych z katalogów systemowych, ale również malware, który korzystał z „C:\Windows\System32” jako swojej bazy wypadowej, stracił prawo bytu, ponieważ sam system domyślnie nie pozwala na jego instalacje. W tym tez momencie chylę czoło w stronę ludzi z Microsoftu. To jeden z nielicznych pomysłów, które się im udały.

Ale! Podsumujmy to co już wiemy:

1. W systemie Windows Vista i wyższych znajduje się użytkownik z większymi uprawnianiami niż nasz typowy Administrator, ale niedostępny z poziomu użytkownika systemu.
2. Uruchamiając program uruchamiamy go z uprawnianiami użytkownika na którym jest uruchamiany.
3. Nawet Administrator nie ma dostępu do „C:\Windows\System32”

Po podsumowaniu czas wrócić do naszego scenariusza. Zobaczmy co oferuje nam panel logowania:



Zielonymi kwadratami zaznaczyłem elementy w tym momencie nam zbędne. Polecam przyjrzeć się guzikowi przewrotnie podpisanemu „Ułatwienia Dostępu” (zaznaczony na czarno). Po otwarciu okna Ułatwień Dostępu widzimy rózne opcje do wyboru. Odczyt wpisywanego tekstu, lupę, zmianę kontrastu, klawiaturę ekranową… jak dowiedzieliśmy się, każdy uruchomiony program w systemie windows dziedziczy uprawnienia od użytkownika, który go uruchomił. Więc zastanówmy się chwilę, skoro nie zalogowaliśmy się to na jakich uprawnieniach będą działać te programy? Odpowiedź jest prosta – żadnymi… No dobra, żartowałem. Programy działają na domyślnym systemowym użytkowniku na którego nie można się zalogować (w Windows XP istniała luka pozwalająca zalogować się w trybie awaryjnym na konto Administrator o ile ktoś nie założył na niego hasła).
Gdyby tylko dało by się tu wsadzić cmd… Któż wie, może ten użytkownik to ów user nad userami?

2. Exploitacja – wykorzystanie podatności.

Jak już tłumaczyłem wcześniej zarówno Klawiatura Ekranowa jak i Wiersz poleceń to pojedyncze pliki binarne .exe znajdujące się w obrębie jednego katalogu. Oczywiście rodzi się pytanie jak doprowadzić do tego by w miejscu „ułatwień dostępu” pojawił się nasz exploit (oprogramowanie pozwalające wykorzystanie podatności). Zastanówmy się co mamy na chwilę obecną

1. Możliwość uruchomienia Klawiatury Ekranowej z poziomu systemu a nie użytkownika
2. Znajomość tego co dzieje się po zaznaczeniu klawiatury ekranowej i wciśnięciu guzika „Ok”
3. cmd.exe (wiersz poleceń) którego nie możemy uruchomić a możemy wykorzystać do kompromitacji sytemu
4. osk.exe (klawiatura ekranowa) która uruchamia się po wybraniu jej z listy.
5. Znana lokalizacja osk.exe i cmd.exe

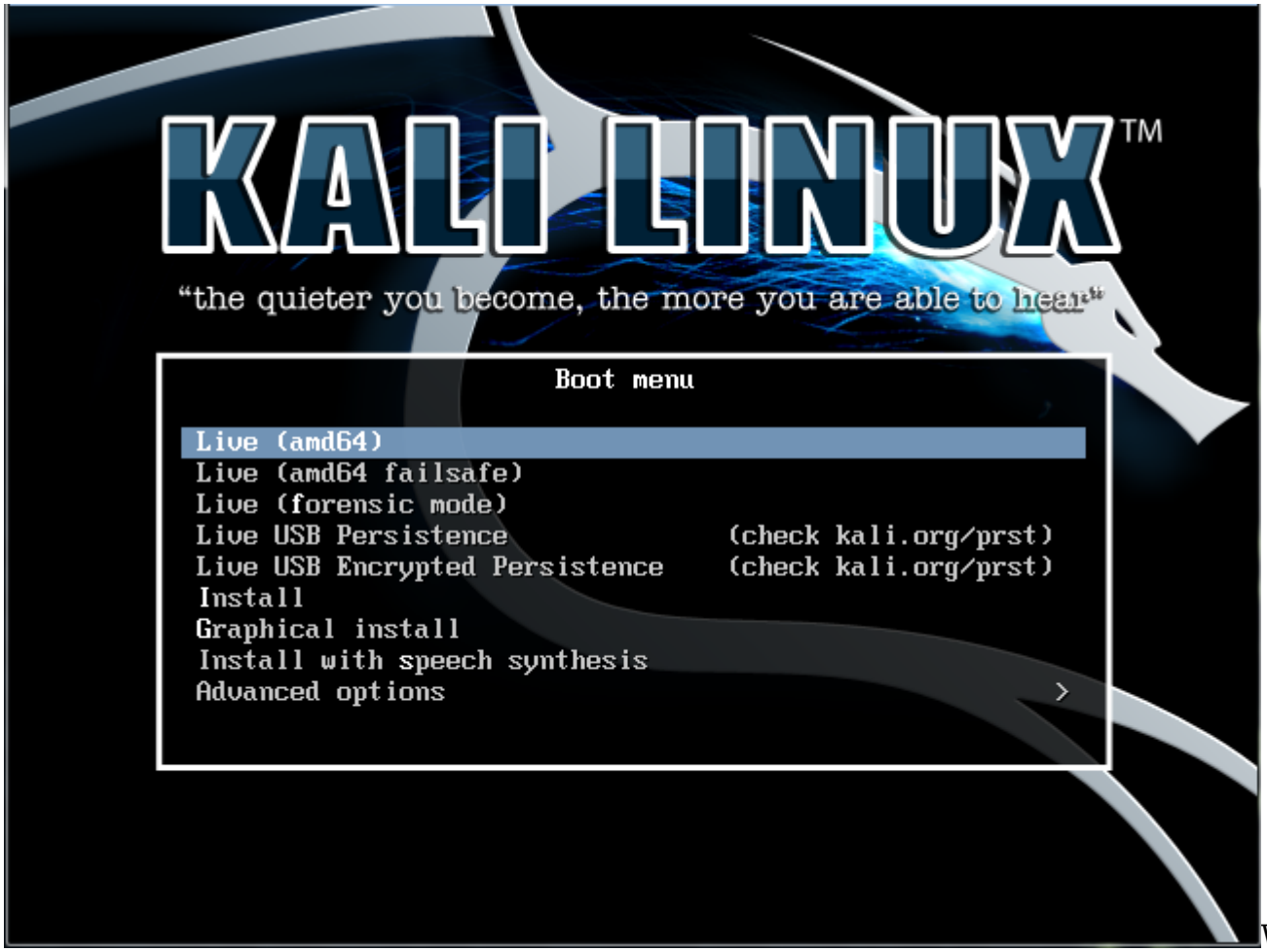
Co więcej zostaje nam do zrobienia? Wystarczy podmienić osk.exe i cmd.exe. tak by system myślał, że wywołuje klawiaturę ekranową a tak naprawdę wywoła nam konsolę i wtedy zobaczymy jakie mamy uprawnienia i co możemy zrobić. W tym konkretnym wypadku naszym exploitem okazuje się… Wiersz poleceń stworzony przez sam Microsoft, a mówią że MS nie dba o użytkowników. O to lista potrzebnych rzeczy:

- pendrive z Linuxem w wersji livecd – obraz takiego systemu (obraz jeśli ćwiczymy to na labowej wirtualce, pendrive gdy ratujemy nasz komputer)
- podstawy znajomości komend powłoki systemowej Linux

Co do obrazu, ja osobiście używam na przemian Clonezilli i KaliLinuxa. Clonezilla świetnie sprawdza się w działaniach typu forensic, Kali natomiast wykorzystuje do testów penetracyjnych ale i w momentach gdy na szybko potrzebuje w pełni funkcjonalnego linuksa a nie mam swojego laptopa pod ręką. I tym razem użyję Kalilinuksa.

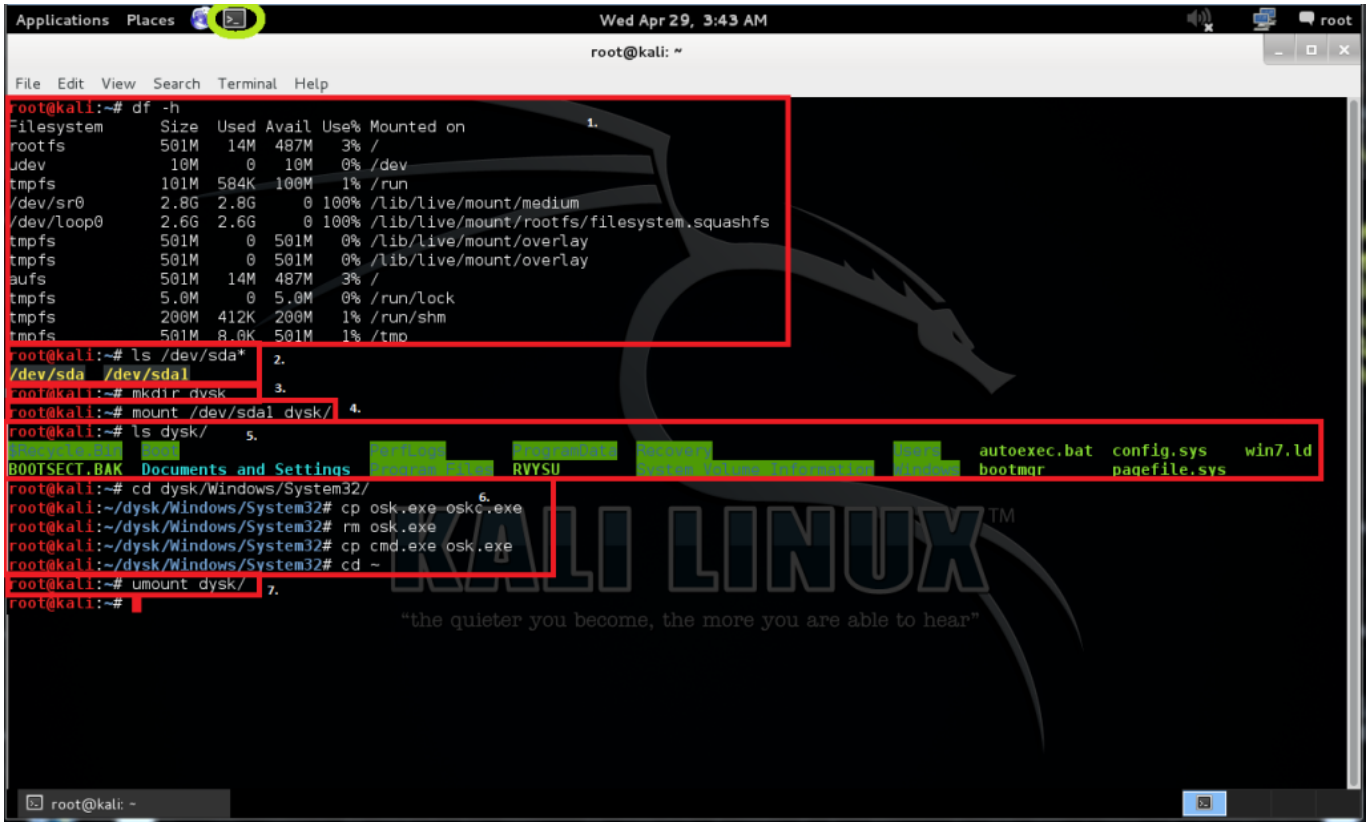
Pierwszym co musimy zrobić to zbootować naszego linuksa. Ufam, ze nie muszę tego tłumaczyć, jeśli zaś ktoś nie wie jak, zapraszam tu.

Ale przejdźmy do właściwej exploitacji podatności. Po zbootowaniu z pendrive/obrazu naszym oczom ukaże się taki oto widok.



Wybieramy „Live” i przechodzimy dalej. Dajemy chwile naszej maszynie na załadowanie systemu i po chwili naszym oczom ukazuje się pulpit.

How to open the window(s) – Czyli otwieranie „okna” bez hasła.



Procedura Exploitacji

Faza I – Umieszczenie exploita

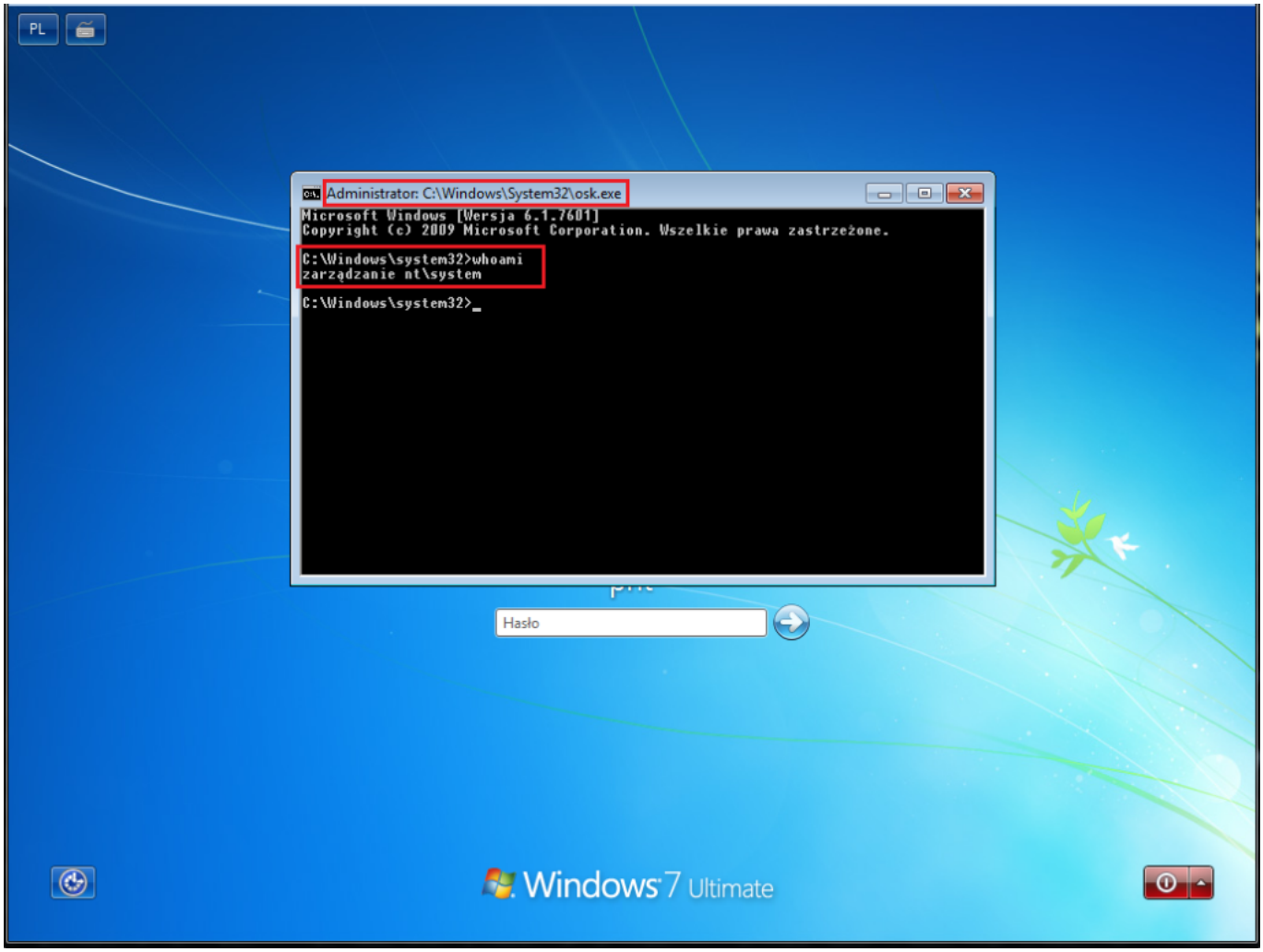
- Uruchom Terminal (przycisk w zielonej elipsie)
    1. df -h – sprawdzamy czy windowsowy dysk nie został podmontowany automatycznie. Należy szukać urządzeń znajdujących się w /dev. Najczęściej jest to /dev/sd*
    2. ls /dev/sd* – listuje dyski wykryte przez system – możliwe do podmontowania.
    3. mkdir dysk – utworzenie katalogu o nazwie dysk
    4. mount /dev/sda1 dysk – podmontowanie partycji sda1 do katalogu dysk. Dzięki temu uzyskamy dostęp do zasobów na dysku twardym. Nie zawsze jest to sda1, może być sda2 lub sdb1.
    5. ls dysk/ – wyświetla zawartość dysku w podmontowanym katalogu „dysk”. Poszukiwany katalog „Windows”. W przypadku nieznalezienia pożądanego katalogu należy podmontowywac kolejne dostępne partycje.
    6. Operacje na plikach celu podmiany klawiatury ekranowej na wiersz poleceń
        - cd dysk/Windows/System32 – przejście do katalogu w którym znajdują się osk.exe i cmd.exe

        - cp osk.exe oskc.exe – skopiowanie oryginalnego osk.exe do drugiego pliku jako kopia
        - rm osk.exe – usunięcie oryginalnego pliku binarnego klawiatury
        - cp cmd.exe osk.exe – skopiowanie w miejsce usuniętego osk.exe cmd.exe
        - cd ~ – powrót do katalogu użytkownika (w tym przypadku będzie to „/root”)
    7. umount dysk/ – odmontowanie partycje podmontowanej do katalogu „dysk”
- Reboot maszyny, uruchamiamy naszego windowsa.

Faza II – Sprawdzenie działania exploita

- Uruchamiamy windows
- Po pojawieniu się panelu logowania otwieramy ikonkę „Ułatwienia dostępu”
- Zaznaczamy klawiaturę ekranowa i klikamy „Ok”

Zapewne dotychczas na tym etapie pojawiała się klawiatura ekranowa. O ile dobrze zostały dokonane zmiany, na ekranie zamiast klawiatury powinna pojawić się konsola.



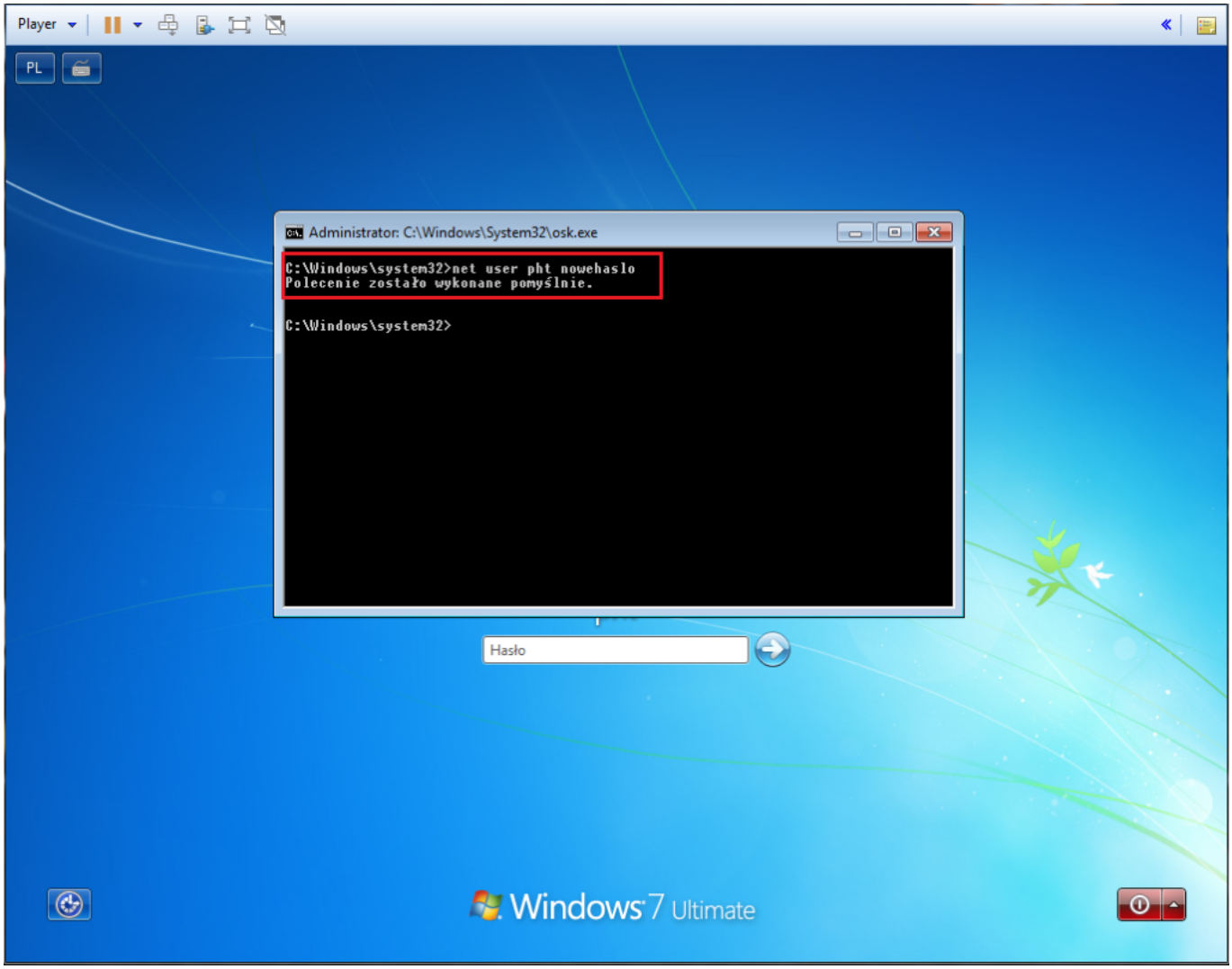
Już na pierwszy rzut oka widać zmiany. Pierwszą z nich jest fakt o którym juz wspominałem. Pomimo próby uruchomienia klawiatury ekranowej otworzył sie nam cmd. A więc nasz exploit (cmd.exe) jest na miejscu. Drugim faktem jest to, że w tytule okna widzimy: „Administrator: C:\Windows\System32\cmd.exe”. Oba te fakty upewniają nas w przekonaniu, że udało się oszukać system i uruchomić cli nie logując się do systemu. Trzecia, najistotniejsza zmiana to odpowiedz naszego komputera na zapytanie „whoami”. Jak widzimy komputer odpowiedział „zarządzanie nt\system” co jest równoznaczne z przyznaniem nam nieograniczonego dostępu.

Faza III – Wprowadzenie „złośliwego” kodu – zmiana hasła

Na chwilę obecną mamy dostęp do głównego użytkownika o nieograniczonych uprawnieniach. Od naszego celu – uzyskania dostępu do konta usera „pht” jest już blisko. Jest kilka sposobów jak to zrobić. O to one:

1. Zmiana hasła usera „pht” z poziomu cmd na uprawnieniach usera „system”
2. Dodanie nowego konta o uprawnieniach administratora, następnie zalogowanie się do systemu na utworzone konto i zmiana hasła usera „pht”
3. Za pomocą cmd uruchomić proces explorer.exe odpowiedzialny (Windows Explorer – środowisko graficzne), a następnie poprzez panel sterowania dokonać zmiany hasła

Najszybszą i najefektywniejszą jest metoda numer jeden.



Wystarczy wpisanie komendy „net user <login> <nowe_haslo>, gdzie <login> to login usera którego hasło chcemy zmienić, a <nowe_haslo> to hasło które chcemy ustawić.

Faza IV – Sprzątanie

Sprzątanie po każdym działaniu dotyczącym przełamywania zabezpieczeń jest ważne.

Nie tylko jeśli chodzi o zacieranie śladów przestępstw, ale przede wszystkim podczas wszelakich testów penetracyjnych aby minimalizować ryzyko, że wykryte przez nas podatności zostaną wykorzystane. Ważne jest też ich łatanie.

Aby przywrócić system do stanu sprzed naszych zabaw z hasłem, należy ponownie uruchomić na maszynie livecd Linuksa i podmienić osk.exe na plik który zapisaliśmy jako kopia (oskc.exe)

„Jak żyć panie premierze?”

To proste. Starać się nie zostawiać komputera w miejscach gdzie mają do niego osoby trzecie. Dodatkowym sposobem jest też szyfrowanie dysku, ale z tym niestety nie każdy sobie poradzi. Pamiętać należy również o odpowiedniej ochronie antywirusowej.

Ciekawostka…

Przy wykorzystaniu tej podatności można nie tylko złamać hasło do logowania do komputera. Zamiast kopiować cmd.exe w miejsce osk.exe można tam umieścić odpowiednio spreparowany malware, który korzystając z uprawnień superusera jakim jest „system” przejmie kontrole maszyną i może spowodować poważne zagrożenie dla bezpieczeństwa Twoich danych.