1110111011011

1001100

110011001100

10101010101010

00011001001

Social engineering, Zip Bomb

metody włamań

Hacking i Cyberbezpieczeństwo | Giganci Programowania

Opracowanie: Michał Suchoń

Przypomnienie

1. Co to jest **cmd**? Wymień przykładowe poznane polecenia
2. Do czego używa się pliki z formatem **.bat**?
3. Jak działa wirus **overload memory**?

Przypomnienie

1. Co to jest **cmd**? Wymień przykładowe poznane polecenia
   To wiersz poleceń, umożliwiający pracę w systemie w trybie tekstowym. Czynności w cmd wykonujemy przez zadanie poleceń z określonymi parametrami. Przykładowe komendy to:
   ping, tracert, ver, netstat czy systeminfo

2. Do czego używa się pliki z formatem **.bat**?

3. Jak działa wirus **overload memory**?

Przypomnienie

1. Co to jest **cmd**? Wymień przykładowe poznane polecenia
   To wiersz poleceń, umożliwiający pracę w systemie w trybie tekstowym. Czynności w cmd wykonujemy przez zadanie poleceń z określonymi parametrami. Przykładowe komendy to: *ping, tracert, ver, netstat czy systeminfo*

2. Do czego używa się pliki z formatem **.bat**?
   Pliki z formatem .bat to tzw. pliki wsadowe. Używa się je, aby wykonać coś bez interakcji użytkownika

3. Jak działa wirus **overload memory**?

Przypomnienie

1. Co to jest **cmd**? Wymień przykładowe poznane polecenia
   To wiersz poleceń, umożliwiający pracę w systemie w trybie tekstowym. Czynności w cmd wykonujemy przez zadanie poleceń z określonymi parametrami. Przykładowe komendy to: *ping, tracert, ver, netstat czy systeminfo*

2. Do czego używa się pliki z formatem **.bat**?
   Pliki z formatem .bat to tzw. pliki wsadowe. Używa się je, aby wykonać coś bez interakcji użytkownika

3. Jak działa wirus **overload memory**?
   Jego zadaniem jest „zapchanie” pamięci RAM poprzez jego stałe obciążenie jakimś procesem systemowym, np. nieustanne uruchamianie kalkulatora

WYZWANIE NR 1

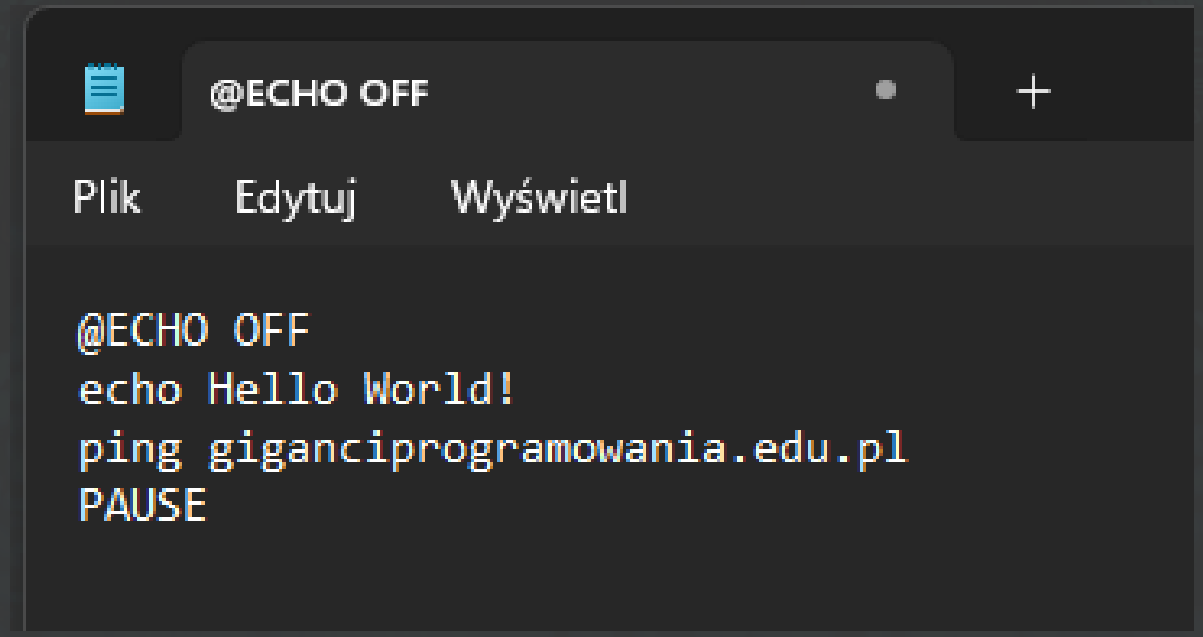
Stwórz plik wsadowy, którego zadaniem będzie:

1. Wyświetlenie napisu *Hello World*
2. Sprawdzenie połączenia ze stroną **giganciprogramowania.edu.pl**

Skrypt **nie powinien wyświetlać wykonywanych poleceń** oraz **zamyka się dopiero po naciśnięciu przez nas dowolnego przycisku**

WYZWANIE NR 1

rozwiązanie



autostart

Do czego go używamy?

autostart

Do czego go używamy?

za pomocą autostartu możemy ustawić, aby określone aplikacje czy skrypty uruchamiały się od razu po starcie systemu

autostart

Dodajmy nasz program do autostartu!

Co to Social Engineering?

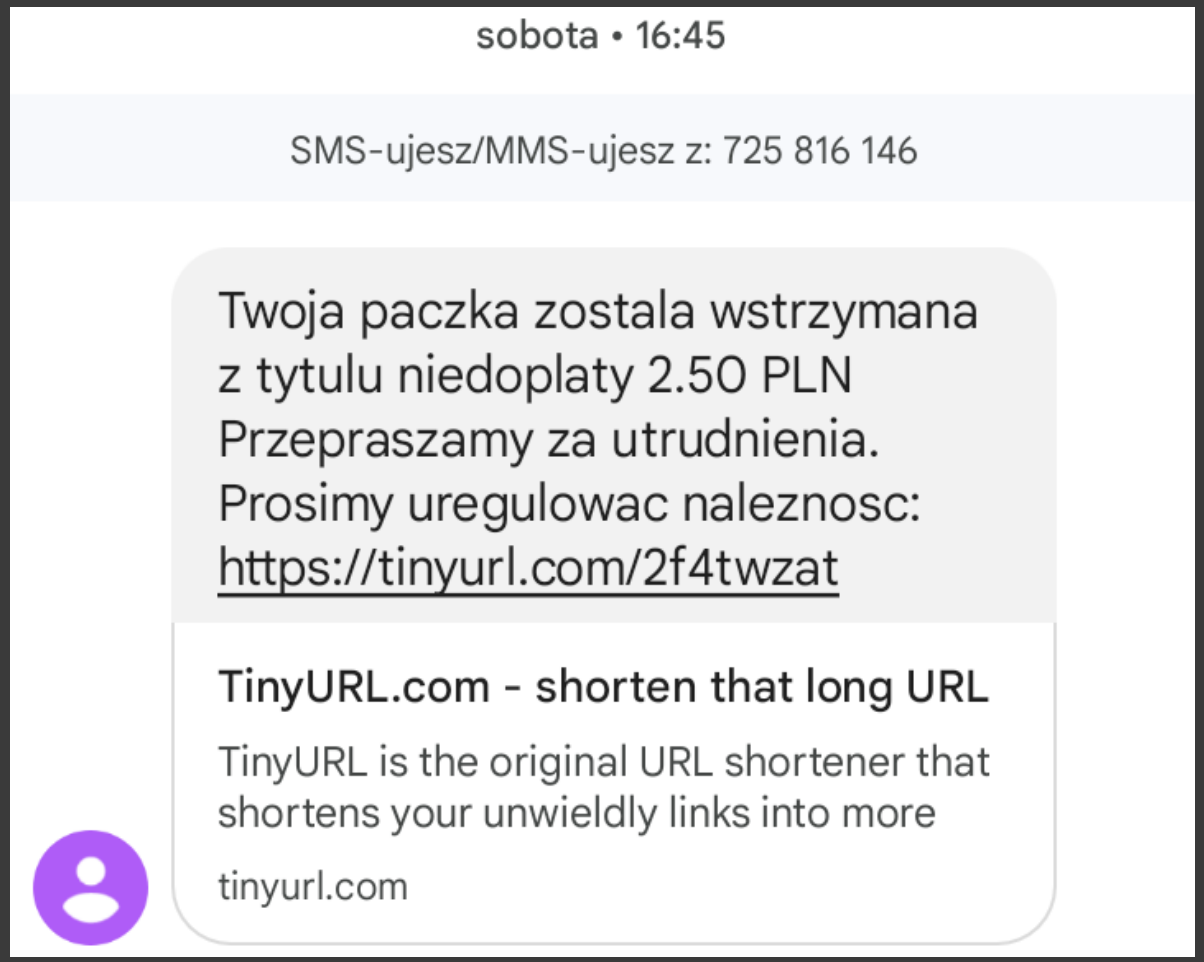
Social Engineering

z ang.: inżynieria społeczna / socjalna lub socjotechnika:
metody, których celem jest uzyskanie niejawnych informacji przez cyberprzestępców. Głównym czynnikiem, przez który ludzie ulegają socjotechnikom, jest ich niewiedza na techniczne tematy czy łatwowierność. W social engineeringu najsłabszym ogniwem w łańcuchu bezpieczeństwa jest człowiek i dlatego to jego naturę wykorzystuje się celem złamania zabezpieczeń i kradzieży danych

Przykładowe metody socjotechniczne

SMS

Informujący o konieczności dopłacenia za coś, sprawdzenia czegoś czy potwierdzenia poprzez kliknięcie w link, który **imituje** zaufaną stronę / aplikację firmy, z której usług skorzystaliśmy



Przykładowe metody socjotechniczne

OLX / VINTED

wiadomość w aplikacji / mail z linkiem, za pomocą którego rzekomo możemy odebrać płatność, wysłaną przez kupującego, przez podanie danych karty

Przykładowe metody socjotechniczne

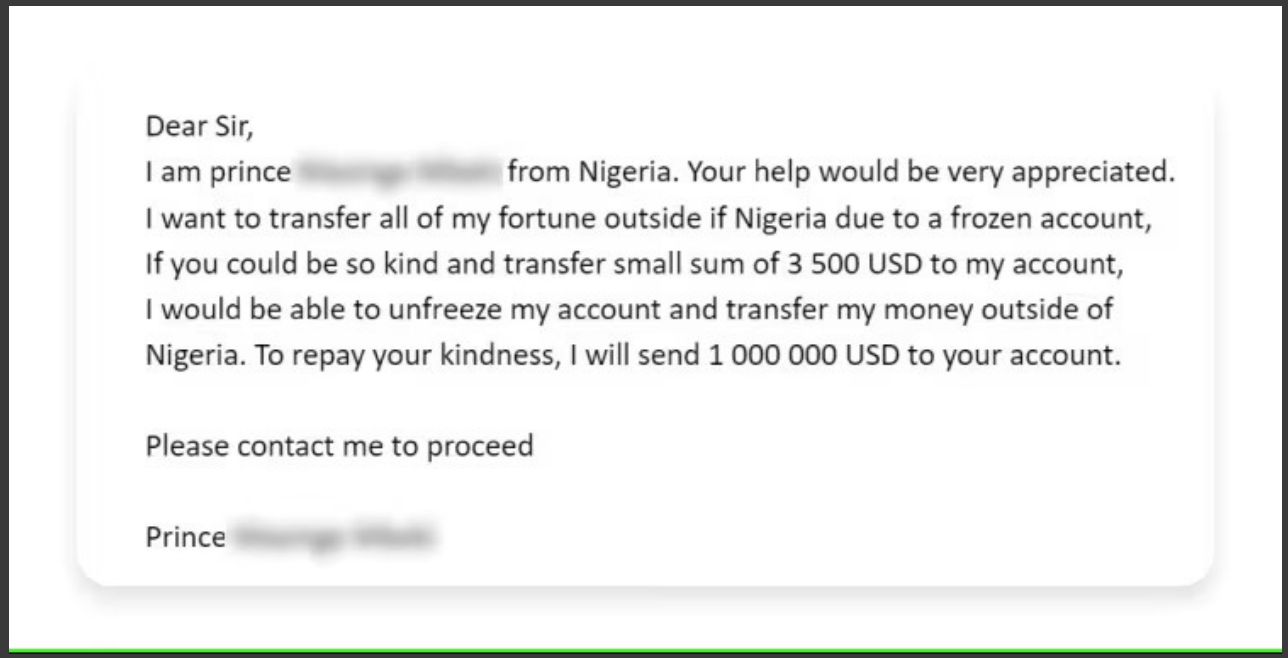
BANK

telefon z banku informujący nas, że mamy **wirusa na koncie bankowym**, bo ktoś się na nie włamał i je zainfekował.
Tzw. **spoofing połączeń**

Przykładowe metody socjotechniczne

KSIĄŻE Z NIGERII

mail od rzekomego księcia z Nigerii / zaginionego kuzyna z Libii, który chce nam oddać swój majątek, bo grozi mu niebezpieczeństwo



Dear Sir,

I am prince [redacted] from Nigeria. Your help would be very appreciated.
I want to transfer all of my fortune outside if Nigeria due to a frozen account,
If you could be so kind and transfer small sum of 3 500 USD to my account,
I would be able to unfreeze my account and transfer my money outside of Nigeria. To repay your kindness, I will send 1 000 000 USD to your account.

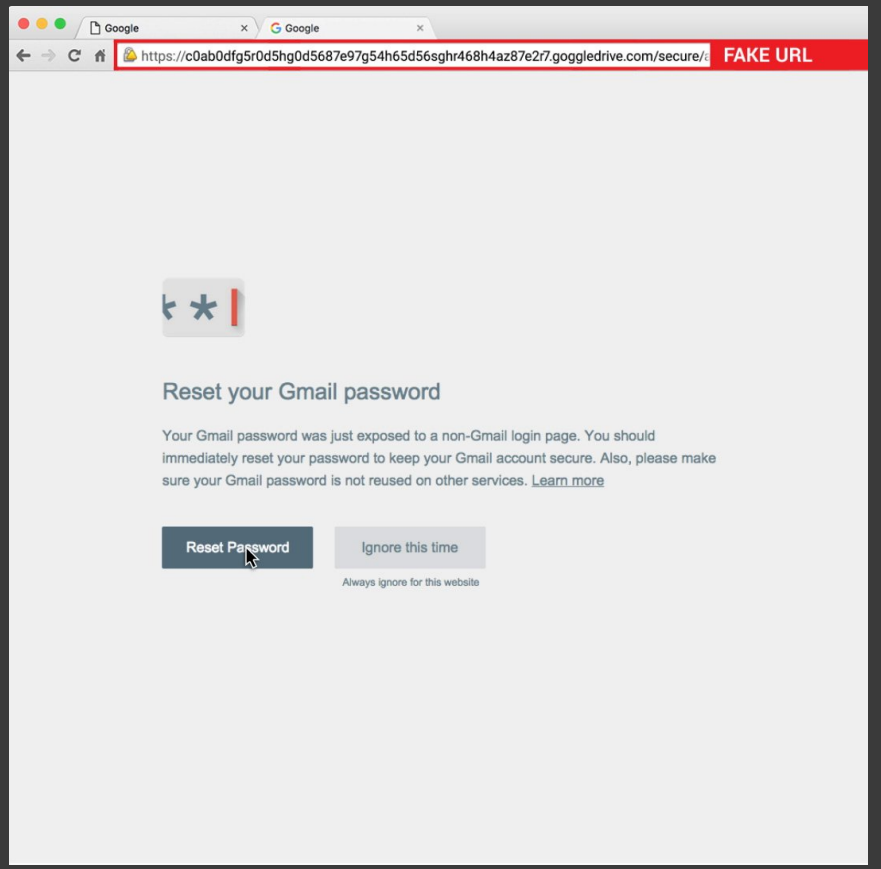
Please contact me to proceed

Prince [redacted]

Przykładowe metody socjotechniczne

RESET HASŁA

phishing, polegający na mailu z możliwością zresetowania / przypomnienia swojego hasła z linkiem, prowadzącym do fałszywej strony firmy / serwisu, na którym chcemy zmienić hasło do konta



Przykładowe metody socjotechniczne

ŹRÓDŁO:
YouTube: https://youtu.be/SbCcmLqmQSs

Przykładowe metody socjotechniczne

ŹRÓDŁO:
YouTube: https://youtu.be/o_rxgLXPBMc

Czym jest Wipe / Wiping?

Wipe

z ang.: wytrzeć

czyszczenie pamięci w komputerze

Wiping

rodzaj wirusa, którego zadaniem jest wyczyszczenie pamięci z plików.

Do czyszczenia plików czy katalogów używamy w cmd polecenia del

Wyzwanie nr 2

Stwórz na pulpicie folder, a następnie dodaj w nim kilka plików:

zadanie1.txt, zadanie2.txt, zadanie3.txt, plik.txt, zad.txt

(Pliki tworzymy dowolną metodą: przez gui lub cli)

Następnie, w wierszu poleceń **usuń** plik o nazwie *plik.txt*

Na koniec, za pomocą jednego polecenia usuń pliki **zadanie1.txt, zadanie2.txt** oraz **zadanie3.txt**

Czy na pewno `del` usuwa?

Czy na pewno `del` usuwa?

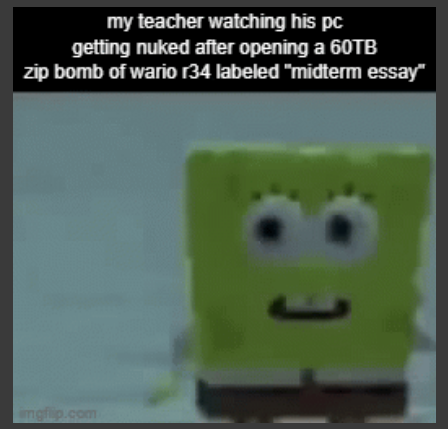
Niezupełnie! W praktyce, *del* powoduje usunięcie wskaźnika na dany plik. W pamięci, jest on nadal obecny i dlatego możliwe jest odtworzenie go za pomocą przeznaczonych do tego narzędzi.

`cipher /w`

polecenie, które nadpisuje fragment pamięci, w której przechowywany był plik innymi wartościami

Co to Bomba dekompresyjna?

ZIP Bomb / Bomba Dekompresyjna



ang. decompression bomb – *bomba komputerowa / archiwum śmierci*; sposób ataku, do którego używa się złośliwego pliku komputerowego w postaci odpowiednio spreparowanego archiwum (ZIP), które wprowadza program rozpakowujący w błąd tak, że plik wynikowy posiada nieskończenie dużą wagę (≈ 4,5 PB / 4500000 GB).

Alternatywny sposób: plik ma nietypowo wysoki stopień kompresji (np. 0,001%), przez co wypakowany plik wynikowy również będzie ekstremalnie duży.

Wirusa tego typu wprowadza się m.in. Po to, aby wymusić zatrzymanie programu antywirusowego i w międzyczasie przeprowadzić inne ataki na komputer. *Bomba komputerowa* ułatwia transport zainfekowanych plików, nie wzbudzając podejrzeń przez stosunkowo niewielki rozmiar (kilka kilobajtów).

42.zip

Tworzymy plik .txt z ogromną ilością zer (00000000000000...), np. o wielkości 10 GB. Następnie, kompresujemy do formatu .rar lub .zip – sprawdzamy wielkość. Zmaleje ona ok. 1000 razy. Wynika to z wysokiej kompresji, gdyż zapis binarny tego pliku będzie powtarzalny (redundantny).

W ten sposób np. plik 2TB będzie zajmował zaledwie 2GB

42.zip

0:30 – 5:20

ŹRÓDŁO:
YouTube: https://www.youtube.com/watch?v=1zWbuHDYPlk

Podsumowanie

1. Co to jest Social Engineering?
2. Jak działa bomba dekompresyjna?

Podsumowanie

1. Co to jest Social Engineering?
   Inaczej: inżynieria społeczna - metody, których celem jest uzyskanie niejawnych informacji przez cyberprzestępców przez naiwność lub niewiedzę użytkowników

2. Jak działa bomba dekompresyjna?

Podsumowanie

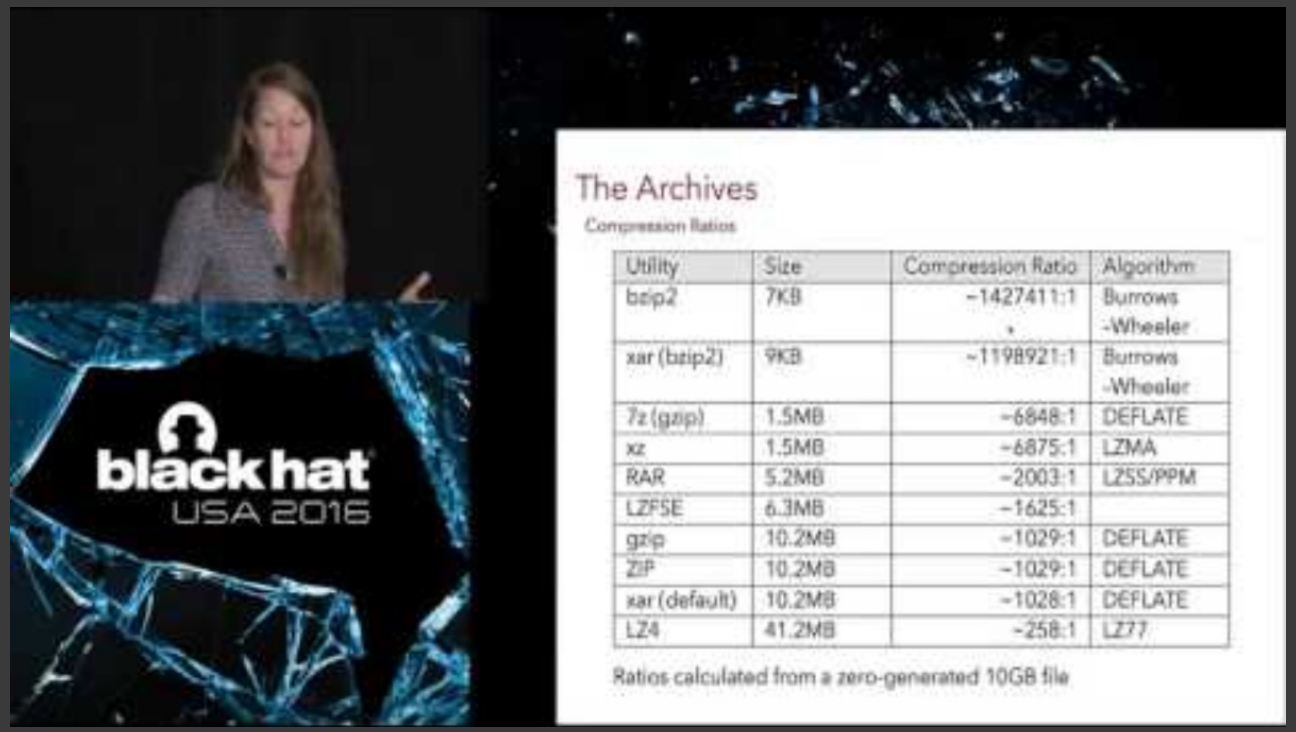
1. Co to jest Social Engineering?
   Inaczej: inżynieria społeczna - metody, których celem jest uzyskanie niejawnych informacji przez cyberprzestępców przez naiwność lub niewiedzę użytkowników

2. Jak działa bomba dekompresyjna?
   Skompresowany plik posiada niewielki rozmiar (rzędu kilku - kilkudziesięciu kilobajtów), który po rozpakowaniu zajmuje ogromną przestrzeń pamięci (nawet do kilku PETABAJTÓW), wymuszając zatrzymanie innych procesów, jak działanie antywirusa

Polecam!

ŹRÓDŁO:
YouTube: https://youtu.be/yY-IMkeZVuY

Polecam!



ŹRÓDŁO:
YouTube: https://youtu.be/IXkX2ojrKZQ