Počítačové viry a bezpečnost počítačových systémů
Protokol z předmětu (10b)

Tématická oblast: PowerShell

Přednášející: prof. Ing. Ivan Zelinka, Ph.D.; Ing. Jan Plucar, Ph.D.
Cvičící: Ing. Jan Plucar, Ph.D.

Jméno a číslo studenta: Daniel Trnka, TRN0038
Datum vypracování: 30. 3. 2019

Zadání:

1) Seznamte se s nástrojem PowerShell Integrated Scripting Environment(ISE)
2) Seznamte se s politikou vykonávání PS skriptů. Vyzkoušejte příkaz Get-ExecutionPolicy. Vysvětlete co znamenají návratové hodnoty:
    a. Restricted
    b. AllSigned
    c. RemoteSigned
    d. Unrestricted

3) Seznamte se s prací s proměnnými a metodami
    a. Vytvořte proměnnou a přiřaďte jí číselnou hodnotu
    b. Vytvořte metodu, která bude přebírat dva parametry. Metoda bude vracet číselnou hodnotu, která vznikne manipulací dvou vstupních parametrů. Navrácenou hodnotu vypište do konzole.
    c. Vytvořte metodu, která bude přijímat vícerozměrné pole. Toto pole bude obsahovat řetězce. V rámci metody proveďte operace s řetězci a výslednou hodnotu vypište do konzole a uložte do souboru.
4) Zjistěte informace o běžících procesech a vyzkoušejte různé metody pro práci s procesy.
5) Zkontrolujte, zda existuje vámi zadaná složka/cesta. Pokud neexistuje, tak ji vytvořte.

Úkol:
Vytvořte jednoduchý Powershell skript, který zkontroluje běžící procesy a zastaví vámi připravený proces (např. vytvořte proces „SimpleAntivirus“). Poté zkontroluje v konstantě zadanou cestu. Pokud tato cesta existuje, skript svou činnost ukončí. V opačném případě se zavolá metoda, která jako parametr příjme pole s řetězci. Různými operacemi s polem vytvořte finální řetězec. Vámi sestavený řetězec bude další jednoduchý powershell skript, který stáhne ze vzdáleného zdroje vámi připravený jednoduchý program a spustí jej.

Při práci se pokuste snížit šanci snadného odhalení vašeho skriptu tím, že použijete jednoduchou obfuskaci formou transformace skriptu do Base64.