RBI / Cvičenie 02 / Využitie procesov, služieb a prostriedkov v OS Windows pre SOC analytika

Požiadavky

- Počítač s OS Windows
- Balík nástrojov SysInternals
  https://technet.microsoft.com/en-us/sysinternals/bb842062.aspx
- Windows Debugging Tools for Windows z balíčku Win SDK
  https://go.microsoft.com/fwlink/p/?linkid=2196241

Inštrukcie a scenár

V tomto laboratórnom cvičení študenti pracujú na počítačoch s OS Windows. Naučíme sa ako pracovať s nástrojmi, ktoré slúžia na prácu s procesmi a službami. Každý študent bude pracovať samostatne.

Toto laboratórne cvičenie vzniklo na základe týchto oficiálnych Netacad labov a ich doplnením:

- 3.0.3 - Identify Running Processes
- 3.2.11 - Exploring Processes, Threads, Handles and Windows Registry
- 3.3.12 - Windows Task Manager
- 3.3.11 - Using Windows PowerShell
- 3.3.10 - Create User Accounts
- 3.3.13 - Monitor and Manage System Resources in Windows

Časť 1: Identifikácia procesov

1. **Stiahnutie nástrojov**
   a. Stiahnite si nástroje na prácu s procesmi (45 MB)
      i. Klikni na link https://technet.microsoft.com/en-us/sysinternals/bb842062.aspx
   b. Z toho balíka nástrojov budeme používať nasledovné:
      i. tcpview (TCP/UDP Endpoint viewer)
         - Otvoríme tcpview.exe
      ii. procexp.exe
      iii. Správca úloh (Task manager)
2. **Zistite aké procesy bežia na zariadení**
   a. TCPview

i. V hlavnom okne vidíme bežiace procesy
   - O aké procesy sa jedná?
   - Čo všetko sa môžeme dozvedieť o týchto procesoch?

ii. Otvorte webový prehliadač
   - Vidíme tento proces v okne TCPview?

iii. Zavrite prehliadač a pozri čo sa stalo s procesom?

b. Proces Explorer

i. V hlavnom okne sú bežiace procesy
   - Vidíme všetky bežiace procesy?
   - Čo všetko môžeme o procesoch zistiť?
   - V nasledujúcich krokoch vyskúšame niektoré možnosti, ktoré tento nástroj ponúka

ii. Na lokalizáciu niektorého vami vybraného procesu, potiahnite Find Window's Process ikonu( ) do otvoreného okna procesu a proces sa vyhľadá v Process Exploreri
   - Kliknite na proces pravým tlačidlom
   - Aké operácie môžeme robiť s procesom? (Window, Set.., Kil, ...)

iii. Otvorte príkazový riadok
   - Presuňte ikonu Find Window's Process do okna príkazového riadka a nájdite zvýraznený proces príkazového riadka v Process Explorer
   - Proces pre príkazový riadok je cmd.exe. Procesy sú v hierarchickej štruktúre, t.j. jeden proces môže mať ďalší proces ako svojho potomka, alebo iný proces ako nadradený, tzv. rodičovský (parent/child). Rodičovský proces pre cmd.exe je proces explorer.exe, a . potomok je proces conhost.exe
   - Prejdite do okna príkazového riadka. Spustite ping a sledujte zmeny pre proces cmd.exe
   - Čo sa stalo počas procesu ping?

iv. Keď si prezeráte zoznam aktívnych procesov, zistíte, že detský proces conhost.exe môže byť podozrivý. Ak chcete skontrolovať proces na škodlivý obsah, kliknite pravým tlačidlom myši na súbor **conhost.exe** a vyberte možnosť **Check VirusTotal**. Keď sa zobrazí výzva, kliknite na **Yes**, aby ste vyjadrili súhlas so zmluvnými podmienkami VirusTotal (tie sa vám otvoria v otvorenom okne v predvolenom prehliadači). Potom kliknite na tlačidlo **OK** pre ďalšiu výzvu

v. Rozbaľte okno pre Process Explorer alebo sa posuňte doprava, kým neuvidíte stĺpec VirusTotal. Kliknite na odkaz v stĺpci VirusTotal. Otvorí sa predvolený webový prehliadač s výsledkami týkajúcimi sa škodlivého obsahu pre conhost.exe

vi. Kliknite pravým tlačidlom myši na proces cmd.exe a vyberte možnosť **Kill Process**
   - Čo sa stalo s potomkom conhost.exe?

c. Správca úloh (ctrl + alt + del)

i. Procesy vidíme v hlavnom okne
   - O aké procesy sa jedná?
   - Čo všetko sa môžeme o procese dozvedieť?
   - Upozornenie: Ak nevidíte v zobrazení procesy zoskupené do 3 základných skupín, tak si ich zobrazte cez Zobraziť > ... > ...

ii. Procesy na pozadí
   - Niektoré procesy nevidíme v oknách a bežia len na pozadí. Sú spustené aplikáciami, ktoré sú práve otvorené

- Otvorte vlastnosti takéhoto procesu bežiaceho na pozadí
  - Aké vlastnosti môžeme zistiť z tohto výpisu?
  - Upozornenie: Ak vám nezobrazuje procesy podľa typu, treba si danú funkcionalitu aktivovať v správcovi úloh v „Zobraziť“->“Zoskupiť podľa typu“

iii. Procesy systému Windows
- Procesy Windows sú služby OS Microsoft Windows, ktoré bežia na pozadí
  - Aké procesy tu môžeme vidieť?

iv. Asociácia niektorých procesov
- Niektoré procesy na pozadí alebo procesy Windows môžu byť spojené s aplikačnými procesmi
- Otvorte okno príkazového riadku. Všimnite si, že Console Window Host proces sa spustí v časti procesov systému windows
- Kliknite pravým tlačidlom myši na Console Window Host a vyberte **Properties**
  - Aké je umiestnenie tohto súboru a umiestnenie tohto procesu?
- Zatvorte okno príkazového riadku
  - Čo sa stane s Windows Command Processor a Console Window Host, keď je okno príkazového riadku zatvorené?

v. Preskúmajte ďalšie záložky správcu úloh
- Zistite aké informácie poskytujú

3. Porovnanie nástrojov

a. Zo zistených poznatkov o procesných nástrojoch vypíš hlavné vlastnosti týchto nástrojov a vypíš ich hlavné výhody a nevýhody
   i. Ktorý nástroj má najviac informácii o procesoch?
   ii. Ktoré funkcionality majú rozdielne a ktoré spoločné?

Časť 2: Threads a Handles

1. Preskúmajte Threads

a. Procesy majú jedno alebo viac vlákien. Threads alebo tzv. vlákna sú nezávislé bežiace úlohy, na ktoré je rozdelený program
   i. Otvorte procexp.exe
      - Zapni príkazový riadok
   ii. Nájdite ho v Process Exploreri a kliknite pravým a vyberte vlastnosti
   iii. Vo vlastnostiach vyberte okno threads
      - Upozornenie: Ak sa vám zobrazí okno upozornenia, treba si doinštalovať Windows Debugging Tools for Windows v balíčku Win SDK. Link na stiahnutie: https://go.microsoft.com/fwlink/p/?linkid=2196241 (z daného balička stačí inštalovať „Debugging Tools for Windows“)
      - Aké informácie sa môžeme z daného výpisu v okne dozvedieť?

2. Preskúmajte Handles

a. Handles sa používajú, keď softvér odkazuje na blok pamäti alebo objekt manažovaný iným systémom
   i. Označte podproces príkazového riadka conhost.exe
   ii. V Process Exploreri vyberte v hornom menu **View > Lower Pane View > Handles** na zobrazenie handles príslušných s procesom conhost.exe
      - Prezrite si, na čo tieto handles odkazujú

Časť 3: Preskúmanie Windows registrov

Registre OS Windows sú hierarchickou databázou, ktorú ukladá väčšina operačných systémov. V databáze sú uložené konfiguračné nastavenie pre prostredie OS Windows.

1. **Zobrazte registre systému Windows**
    a. Klikni na štart, vyhľadajte regedit a vyberte Registry Editor
    b. Z registrov nezistíme, čo sa v nich presne nachádza treba čerpať z teoretických poznatkov
        i. Skúste pomocou internetu zistiť, čo sa v priečinkoch nachádza a načo ich je možné využiť
        ii. **Práca v skupine**: Rozdelíme sa do 5 skupín, a každá skupina preskúma jeden priečinok s registrami, a podá výsledok prieskumu aj s nejakým konkrétnym príkladom
    c. Pri prvom otvorení nástroja Process Explorer ste prijali jeho EULA (licenčnú zmluvu). Prejdite na EulaAccepted register kľúča pre Process Explorer
        i. Kliknutím vyberte Process Explorer v **HKEY_CURRENT_USER > Software > Sysinternals > Process Explorer**. Prejdite nadol a nájdite kľúč **EulaAccepted**. Aktuálne hodnota pre register kľúča EulaAccepted je 0x00000001(1)
    d. Dvakrát kliknite na register kľúča **EulaAccepted**. Aktuálne je hodnota nastavená na 1. Hodnota 1 označuje, že EULA bola akceptovaná používateľom
    e. Zmeňte hodnotu **1** na **0** pre Value data. Hodnota 0 znamená, že EULA nebola prijatá. Kliknite na tlačidlo **OK** pre pokračovanie
        i. Aká je hodnota pre tento register kľúča v Data stĺpci?
        ii. Zavrite a znovu otvorte Registry Editor, a presvedčte sa, že hodnota 0 sa skutočne uložila
    f. Otvorte **Process Explorer**. Prejdite do priečinka, v ktorom je SysInternals. Otvorte priečinok **SysInternalsSuite** > otvorte **procexp.exe**
        i. Keď otvoríte Process Explorer, čo je možné pozorovať?

V nasledujúcich častiach sú potrebné admin práva, pracujete na svojich PC:

Časť 4: Windows PowerShell

Upozornenie: Vykonávate na svojich PC.

PowerShell je výkonný automatizačný nástroj. Je to príkazová konzola a zároveň aj skriptovací jazyk. V tomto laboratóriu budete používať konzolu na vykonanie niektorých príkazov, ktoré sú dostupné v príkazovom riadku a aj v PowerShell. PowerShell má tiež funkcie, ktoré dokážu vytvárať skripty na automatizáciu úloh a spoluprácu s operačným systémom Windows.

1. **Pristúp ku konzole PowerShell**
    a. Kliknite na tlačidlo Štart. Vyhľadajte a vyberte powershell
    b. Kliknite na tlačidlo Štart. Vyhľadajte a vyberte príkazový riadok
2. **Preskúmajte príkazový riadok a príkazy v PowerShell**
    a. Zadajte príkaz **dir** v obidvoch oknách
        i. Aké sú výstupy príkazu **dir**?
    b. Skúste iný príkaz, ktorý ste použili v príkazovom riadku, napríklad **ping**, **cd** a **ipconfig**
        i. Aké sú výsledky?
3. **Preskúmajte cmdlets**
    a. Príkazy prostredia PowerShell, cmdlets, sú konštruované vo forme reťazca sloveso-podstatné meno. Na identifikáciu príkazu pre PowerShell na zoznam podadresárov a súborov v adresári zadajte **Get-Alias dir** v PowerShell-i

i. Na čo je PowerShell príkaz pre **dir**?
ii. Ak chcete získať podrobnejšie informácie o cmdletoch, vyhľadajte na internete výraz Microsoft powershell cmdlets

4. **Preskúmajte príkaz netstat pomocou prostredia PowerShell**
   a. Vo výzve(prompt) prostredia PowerShell zadajte **netstat -h**, aby ste videli možnosti dostupné pre príkaz netstat
   b. Ak chcete zobraziť smerovaciu tabuľku s aktívnymi cestami, zadajte do výzvy **netstat -r**
      i. Ktorá IP adresa je bránou?
   c. Otvorte a spustite druhý PowerShell so zvýšenými oprávneniami. Kliknite na tlačidlo Štart. Vyhľadajte PowerShell a kliknite pravým tlačidlom na Windows PowerShell a vyberte Spustiť ako správca. Kliknutím na tlačidlo Áno povolíte vytváranie tejto aplikácie zmeny na vašom zariadení
   d. Príkaz netstat môže tiež zobraziť procesy spojené s aktívnymi pripojeniami TCP. Po výzve zadajte **netstat -abno**
   e. Otvorte správcu úloh. Prejdite na kartu podrobnosti. Kliknite na nadpis PID, aby boli PID v poradí
   f. Vyberte jeden PID z výsledkov **netstat -abno**. V tomto príklade sa používa PID 756
   g. Nájdite vybraný PID v správcovi úloh. Kliknutím pravým tlačidlom myši na vybraný PID v správcovi úloh otvoríte v dialógovom okne vlastnosti, kde nájdete ďalšie informácie
      i. Aké informácie môžete získať na karte Podrobnosti a v dialógovom okne Vlastnosti pre vybratý PID?

5. **Vyprázdnenie koša pomocou PowerShell-u**

Príkazy PowerShell-u môžu zjednodušiť správu veľkej počítačovej siete. Napríklad, ak by ste chceli implementovať nové bezpečnostné riešenie na všetky servery v sieti, môžete použiť príkaz PowerShell-u alebo skript na implementáciu a overenie spustenia služieb. Môžete tiež spustiť príkazy PowerShell-u pre zjednodušenie akcie, ktorých vykonanie by vyžadovalo viacero krokov pomocou nástrojov grafickej pracovnej plochy systému Windows.

   a. Otvorte Kôš. Overte si, či existujú položky, ktoré možno natrvalo odstrániť z počítača. Ak nie, obnovte tieto súbory
   b. Ak v koši nie sú žiadne súbory, vytvorte niekoľko súborov, napríklad textový súbor pomocou programu Poznámkový blok, a umiestnite ich do koša
   c. V konzole PowerShell zadajte po výzve **clear-recyclebin**
      i. Overte, či obsah koša je prázdny

Časť 5: Vytvorte používateľské účty v OS Windows

Upozornenie: Vykonávate na svojich PC.

V kanáli predmetu v záložke **Laboratory excercises** vypracujte **LAB02-Widows-Netacad 3.3.10 Lab - Create User Accounts**.

Časť 6: Monitorujte a spravujte systémové prostriedky v systéme Windows

Upozornenie: Vykonávate na svojich PC.

V kanáli predmetu v záložke **Laboratory excercises** vypracujte **LAB02-Windows-Netacad 3.3.13 Lab - Monitor and Manage System Resources in Windows.**

Záver

PowerShell bol vyvinutý na automatizáciu úloh a správu konfigurácie. Pomocou internetu, objavte príkazy, ktoré by ste mohli použiť na zjednodušenie úloh bezpečnostného analytika. Zaznamenajte svoje zistenia.

Otázky

Prečo je dôležité, aby SOC analytik chápal, ako pracovať v správcovi úloh?