Stosowanie zabezpieczenia systemów, korzystanie z modułu Security w PowerShell.

1. Opracuj wykaz kolejnych czynności, w PowerShell dotyczących korzystania z modułu Security.
2. Przedstaw opracowany wykaz kolejnych czynności, w PowerShell dotyczących korzystania z modułu Security.
3. Wykonaj notatkę zawierająca wykaz kolejnych czynności, w PowerShell dotyczących korzystania z modułu Security.

Czynności w PowerShell dotyczących korzystania z modułu Security:

Zapoznanie się z modułem Security w PowerShell może być ważne dla administratorów systemów, którzy chcą zabezpieczyć swoje środowiska i utrzymać je bezpiecznymi. W tym zestawie ćwiczeń omówimy kilka podstawowych zadań, które można wykonać z użyciem modułu Security.

1. Sprawdzenie statusu usługi Windows Defender

a) Otwórz PowerShell jako administrator

b) Uruchom polecenie:

Get-MpComputerStatus

- służy do wyświetlania informacji o stanie ochrony przed złośliwym oprogramowaniem Windows Defender.

c) Uruchom polecenie:

Set-MpPreference -DisableRealtimeMonitoring $true -DisableIntrusionPreventionSystem $true

- polecenie wyłącza w czasie rzeczywistym monitorowanie systemu Windows Defender i systemu zapobiegania intruzom. Opcja -DisableRealtimeMonitoring ustawiona na wartość $true wyłącza monitorowanie w czasie rzeczywistym, a opcja -DisableIntrusionPreventionSystem ustawiona na wartość $true wyłącza system zapobiegania intruzom.

d) Uruchom polecenie:

Set-MpPreference -SignatureUpdateInterval 1 -MAPSReporting Basic

- polecenie ustawia preferencje programu antywirusowego Windows Defender tak, aby program pobierał aktualizacje sygnatur wirusów co godzinę i raportował tylko podstawowe informacje na temat wykrytych zagrożeń do Microsoft Active Protection Service.

e) Uruchom polecenie:

Add-MpPreference -ExclusionPath "C:\Program Files\MyApp" -ExclusionProcess "MyApp.exe"

- służy do dodawania ustawień preferencji do programu Windows Defender. To polecenie doda wyjątki do skanowania dla plików znajdujących się w folderze "C:\Program Files\MyApp" oraz procesu "MyApp.exe".

f) Uruchom polecenie:

Add-MpPreference -ExclusionExtension ".txt", ".log"

- doda wyjątek dla plików o rozszerzeniach .txt i .log, które nie będą skanowane przez program antywirusowy.

2. Skanowanie systemu w poszukiwaniu złośliwego oprogramowania

a) Otwórz PowerShell jako administrator

b) Uruchom polecenie:

Start-MpScan -ScanType QuickScan

- uruchamia szybkie skanowanie systemu przy użyciu programu Windows Defender. Start-MpScan jest cmdlet'em Powershella używanym do uruchamiania skanowania systemu pod kątem szkodliwego oprogramowania.
Parametr -ScanType określa typ skanowania do wykonania, "QuickScan" oznacza skanowanie szybkie, które skanuje tylko najczęściej używane lokalizacje i pliki systemowe w celu szybkiego sprawdzenia, czy nie ma złośliwego oprogramowania. W wyniku tego skanowania użytkownik otrzymuje raport o ewentualnych zagrożeniach wykrytych przez program Windows Defender.
FullScan - pełne skanowanie, które przeskanuje cały dysk systemowy, w tym pliki, foldery i obszary startowe.

Przygotowanie

Wpisz w PowerShell jako administrator:

New-Item -ItemType File "C:\eicar.com"

Set-Content "C:\eicar.com" -Value 'X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H'*

c) Uruchom polecenie:

Start-MpScan -ScanType CustomScan -ScanPath "C:\"

- CustomScan - niestandardowe skanowanie, które pozwala użytkownikowi wybrać określone foldery i pliki do przeskanowania.

3. Aktualizacja definicji wirusów dla Windows Defender

a) Otwórz PowerShell jako administrator

b) Uruchom polecenie:

Update-MpSignature

- służy do aktualizacji sygnatur wirusów programu Microsoft Defender (dawniej Windows Defender). Dzięki tej komendzie możesz pobrać i zainstalować najnowsze definicje wirusów, co pozwoli na skuteczniejszą ochronę przed nowymi zagrożeniami. Aktualizacje sygnatur są ważne, ponieważ pomagają zidentyfikować nowe typy złośliwego oprogramowania i zapewniają lepszą ochronę przed cyberatakami.

4. Konfigurowanie polityk zabezpieczeń - przypomnienie

a) Otwórz PowerShell jako administrator

b) Uruchom polecenie:

Set-ExecutionPolicy RemoteSigned

- służy do ustawienia zasad wykonywania skryptów w systemie Windows. Ustawia ono poziom zabezpieczeń, który wymaga, aby skrypty były podpisane przez zaufanego wydawcę lub były napisane na lokalnym komputerze, zanim będą mogły zostać uruchomione. Ustawienie "RemoteSigned" pozwala na uruchamianie skryptów, które pochodzą z lokalnego komputera lub z zewnętrznych źródeł, ale tylko wtedy, gdy są one podpisane przez zaufanego wydawcę.

c) Uruchom polecenie:

Set-ExecutionPolicy Restricted

- służy do ograniczenia możliwości uruchamiania skryptów w systemie Windows.
Ustawienie ExecutionPolicy na Restricted spowoduje, że system będzie miał zablokowany dostęp do skryptów, z wyjątkiem skryptów wbudowanych w PowerShell i skryptów podpisanych przez zaufane wydawców. Zmiana ustawienia ExecutionPolicy wymaga uprawnień administratora i może wpłynąć na bezpieczeństwo systemu, dlatego należy stosować je ostrożnie i z pełną świadomością konsekwencji.

d) Uruchom polecenie:

```
Set-ExecutionPolicy Unrestricted
```

- umożliwia uruchamianie skryptów w trybie nieograniczonym, co oznacza, że PowerShell nie będzie blokować wykonywania skryptów i skrypty będą mogły zawierać niebezpieczne operacje. Jest to przydatne, gdy chcemy uruchomić skrypt, który nie działa z domyślną polityką wykonania skryptów PowerShell lub gdy musimy tymczasowo zmienić tę politykę, aby wykonać skrypt z poziomu skryptu.

e) Uruchom polecenie:

```
Get-ExecutionPolicy
```

- służy do wyświetlania bieżącej polityki wykonywania skryptów PowerShell.

5. Dodawanie i usuwanie reguł zapory sieciowej

a) Otwórz PowerShell jako administrator

b) Dodaj regułę:

```
New-NetFirewallRule -DisplayName "Block Ping" -Direction Inbound -Protocol ICMPv4 -Action Block
```

- tworzy nową regułę zapory sieciowej, która uniemożliwia odbieranie pakietów ping na porcie ICMPv4. Parametr -DisplayName określa nazwę reguły wyświetlaną w zapory sieciowej, parametr -Direction określa kierunek ruchu, w tym przypadku ruch wchodzący (Inbound), parametr -Protocol określa protokół, który ma być blokowany (ICMPv4), a parametr -Action określa, jak zapora ma się zachować w przypadku dopasowania reguły - w tym przypadku, blokować ruch (Block).

c) Usuń regułę:

```
Remove-NetFirewallRule -DisplayName "Block Ping"
```

- usuwa zasadę zapory sieciowej (firewall) o nazwie "Block Ping", która zapobiega odbieraniu pakietów ICMP typu Echo Request (czyli blokuje pingi) przez komputer.

d) Dodaj zasadę zapory sieciowej:

```
New-NetFirewallRule -DisplayName "Block Port 80" -Direction Inbound -LocalPort 80 -Protocol TCP -Action Block
```

- tworzy nową regułę zapory sieciowej, która blokuje ruch przychodzący na porcie 80 z wykorzystaniem protokołu TCP. Reguła jest nazwana "Block Port 80" i działa w kierunku wejściowym, co oznacza, że dotyczy ruchu przychodzącego do komputera. Akcja ustawiona jest na "Block", co oznacza, że ruch zostanie zablokowany i nie będzie przepuszczany przez zaporę sieciową.

e) Zmodyfikuj istniejącą zasadę zapory sieciowej:

```
Set-NetFirewallRule -DisplayName "Block Port 80" -Enabled True
```

- jest wykorzystywane do konfiguracji reguł zapory sieciowej w systemie Windows. W przypadku podanej reguły "Block Port 80", polecenie ustawia jej właściwość "Enabled" na wartość "True", co oznacza, że reguła zostanie włączona i zablokuje ruch sieciowy na porcie 80. Port 80 jest standardowo wykorzystywany do protokołu HTTP, dlatego blokowanie ruchu na tym porcie może spowodować problemy z dostępem do stron internetowych.

f) Usuń zasadę zapory sieciowej:

```
Remove-NetFirewallRule -DisplayName "Block Port 80"
```

- usuwa regułę zapory sieciowej o nazwie "Block Port 80". Oznacza to, że jeśli taka reguła istniała i była aktywna, to po wykonaniu tego polecenia ruch sieciowy na porcie 80 (np. ruch HTTP) będzie ponownie dozwolony przez zaporę sieciową.

6. Sprawdzanie logów zdarzeń związanych z zabezpieczeniami

a) Otwórz PowerShell jako administrator

b) Uruchom polecenie:

```
Get-EventLog -LogName Security -Newest 50
```

- w PowerShell zwraca 50 najnowszych wpisów zdarzeń zapisanych w dzienniku zdarzeń Security, który zawiera informacje związane z zabezpieczeniami systemu operacyjnego Windows. Te wpisy

mogą zawierać informacje o logowaniu, nieudanych próbach logowania, zmianach uprawnień użytkowników i innych zdarzeniach związanych z bezpieczeństwem systemu.

7. Konfigurowanie audytu zdarzeń

a) Otwórz PowerShell jako administrator

b) Uruchom polecenie: Auditpol /set /subcategory:"Logon" /success:enable /failure:enable

c) Uruchom polecenie: Auditpol /set /subcategory:"Logoff" /success:enable /failure:enable

8. Sprawdzanie uprawnień dla określonego użytkownika - powtórzenie

a) Otwórz PowerShell jako administrator

b) Uruchom polecenie:

Get-Acl C:\Windows\System32\drivers\etc\hosts

- zwraca informacje o kontrolce dostępu pliku hosts znajdującego się w folderze C:\Windows\System32\drivers\etc.

Kontrolka dostępu (Access Control List - ACL) to lista uprawnień związanych z plikiem lub katalogiem, która określa, kto może mieć dostęp do danego zasobu oraz jakie rodzaje działań (czytanie, zapisywanie, uruchamianie itp.) są dozwolone. Komenda Get-Acl zwraca informacje na temat właściciela, grupy i uprawnień dla określonego pliku lub katalogu.

9. Tworzenie certyfikatu SSL

a) Otwórz PowerShell jako administrator - powtórzenie

b) Uruchom polecenie:

New-SelfSignedCertificate -DnsName "localhost" -CertStoreLocation "cert:\LocalMachine\My"

- służy do tworzenia samopodpisanych certyfikatów w systemie Windows. Parametr -DnsName określa nazwę domeny (FQDN) dla certyfikatu, a parametr -CertStoreLocation określa lokalizację, w której certyfikat ma być przechowywany. W tym przypadku certyfikat zostanie zapisany w lokalnym magazynie certyfikatów (cert:\LocalMachine\My).

10. Konfigurowanie połączeń zdalnych - powtórzenie

a) Otwórz PowerShell jako administrator

b) Uruchom polecenie:

Enable-PSRemoting -Force

- jest używane w PowerShell do włączenia zdalnej obsługi na komputerze. Opcja -Force powoduje natychmiastowe uruchomienie usługi zdalnego wykonywania poleceń (Remote PowerShell), nawet jeśli usługa była już uruchomiona. Włączenie zdalnej obsługi umożliwia zdalne połączenie się z komputerem i wykonanie poleceń w celu zarządzania nim. To przydatne narzędzie w sytuacjach, gdy musisz zdalnie zarządzać komputerem.

c) Uruchom polecenie:

Enable-PSRemoting -Force -SkipNetworkProfileCheck

– poprzednie jak wyżej a parametr -SkipNetworkProfileCheck umożliwia włączenie zdalnego zarządzania w sieci prywatnej lub domowej, gdy nie zostało to automatycznie wykryte.

d) Uruchom polecenie:

Set-Item WSMan:\localhost\Client\TrustedHosts -Value "RemoteComputer"

- służy do dodania wartości "RemoteComputer" do listy komputerów, którym można ufać przy połączeniach zdalnych do lokalnego komputera.

Gdy wartość TrustedHosts jest skonfigurowana z listą zaufanych komputerów, to połączenie zdalne z dowolnym z tych komputerów będzie uznawane za zaufane i połączenie zostanie ustanowione bez konieczności podawania poświadczeń użytkownika.

To są tylko podstawowe przykłady dotyczące korzystania z modułu Security w PowerShell. Istnieje wiele innych poleceń i zadań, które można wykonać z użyciem tego moduł.