

Ćwiczenie Metody ataków sieciowych

Cel ogólny lekcji: Poznanie metod ataków sieciowych oraz nauka konfiguracji maszyn serwerowych i klientów.

Cele szczegółowe:

1. Zapoznanie się z atakiem sieciowym z użyciem metasploita na Kali Linux oraz przejęcie domeny Active Directory za pomocą delegacji Kerberos.
2. Wykonanie analizy aktywnych i nasłuchujących portów oraz nauka konfiguracji serwera z Windows 2019 z kontrolerem domeny i klienta z Windows 10.
3. Nauka konfiguracji karty sieciowej, ustawienia adresu IP, bramy i serwera DNS, a także instalacja usług IIS na maszynie klienta z Windows 10.
4. Konfiguracja maszyny serwera z Windows 2019 z kontrolerem domeny poprzez instalację roli RDS, ustawienie połączenia zdalnego, start usługi SSH i utworzenie reguł zaporowych.

Przed przystąpieniem do ćwiczenia przywróć pierwszy punkt kontrolny.

1. Wykonaj analizę ataku sieciowego, zapisz w zeszycie jakie informacje uzyskałeś których nie znałeś. Jak to daje zagrożenia i możliwości (**teleinformatycy wykonują po punkcie 2.**).
 - a. Atak na Windows 10 z metasploita na Kali Linux opisany w [tym ćwiczeniu](#).
 - b. Przejęcie domeny Active Directory za pomocą delegacji Kerberos opisany w [tym artykule](#).
2. Wykonaj znajdowanie i analizę aktywnych i nasłuchujących portów.

Przygotuj maszynę serwera z Windows 2019 z kontrolerem domeny

Karta sieciowa podłączona do przełącznika wirtualnego (Default Switch)

- system serwera:

Wpisz i sprawdź nazwę interfejsu i zastosuj go w poleceniach poniżej

```
netsh interface show interface
```

```
netsh interface ip set address "Ethernet 3" dhcp
```

```
Get-WindowsCapability -Online | Where-Object name -like 'OpenSSH*'
```

```
Add-WindowsCapability -Online -Name OpenSSH.Server~~~~0.0.1.0
```

```
Get-WindowsCapability -Online | Where-Object name -like 'OpenSSH*'
```

W konfiguracji karta sieciowa podłączona do przełącznika prywatnego (sieć wewnętrzna)

Adres ip 192.167.0.1/24

```
netsh interface ip set address name="Ethernet 3" static 192.167.0.1 255.255.255.0
```

Przygotuj maszynę klienta z Windows 10

- ustawienie maszyny wirtualnej klienta Windows 10

Karta sieciowa pđłączona do przełącznika prywatnego (seć wewnętrzna)

- system klienta Windows 10:

Na kliencie Windows 10 uruchom PowerShell jako administrator i wpisz kolejno w jednej linii:

Adres ip 192.167.0.111/24

```
netsh interface ip set address "Ethernet 2" static 192.167.0.111 255.255.255.0 192.167.0.1 1
```

Brama i serwer DNS: 192.167.0.1

```
netsh interface ipv4 add dnsserver "Ethernet 2" address=192.167.0.1 index=1
```

Instalacja usług IIS

```
Enable-WindowsOptionalFeature -Online -FeatureName IIS-WebServerRole, IIS-WebServer, IIS-CommonHttpFeatures, IIS-ManagementConsole, IIS-HttpErrors, IIS-HttpRedirect, IIS-WindowsAuthentication, IIS-StaticContent, IIS-DefaultDocument, IIS-HttpCompressionStatic, IIS-DirectoryBrowsing
```

Sprawdź statusu uruchomionego serwera WWW:

```
Get-Service W3SVC
```

Status	Name	DisplayName
Running	W3SVC	Usługa publikowania w sieci WWW

Wykonaj restart, pozostaw uruchomione usługi IIS:

```
iisreset
```

```
Przed próbą uruchomienia...
Usługi internetowe zostały pomyślnie uruchomione ponownie
PS C:\WINDOWS\system32>
```

Przygotuj maszynę serwera z Windows 2019 z kontrolerem domeny

Na serwerze Windows dc 2019 otwórz PowerShell jako administrator i wpisz kolejno:

```
Install-WindowsFeature Remote-Desktop-Services
```

i naciśnij klawisz Enter, aby zainstalować rolę RDS.

```
Enable-NetFirewallRule -DisplayGroup "Pulpit zdalny"
```

- zmiany w oknie pozwalania aplikacjom na komunikowanie się z systemem Windows 10 przez Zaporę.

```
Set-ItemProperty -Path 'HKLM:\System\CurrentControlSet\Control\Terminal Server' -name "fDenyTSConnections" -Value 0
```

- zezwalaj na połączenie z komputerów z dowolną wersją Pulpitu zdalnego.

```
Set-Service -Name sshd -StartupType 'Automatic'
```

```
Start-Service -Name 'sshd'
```

```
Get-NetFirewallRule -Name '*ssh*' | Format-Table -AutoSize
```

```
New-NetFirewallRule -Name sshd -DisplayName 'OpenSSH Server (sshd)' -Enabled True -Direction Inbound -Protocol TCP -Action Allow -LocalPort 22
```

W Windows 2019 za pomocą przeglądarki internetowej otwórz stronę pod adresem 192.167.0.111
Co pewien czas odnawiaj połączenie.

Na kliencie Windows 10 uruchom `ssh administrator@192.167.0.1` > `yes` podaj hasło `zaq1@WSX`

Właściwe zadanie:

Zapisz w zeszycie jakie informacje uzyskałeś których nie znałeś. Jak to daje możliwości.

a. Używanie Netstat do znajdowania aktywnych i nasłuchujących portów

Netstat to narzędzie wiersza poleceń do sprawdzania połączeń sieci lokalnej. Sprawdźmy, jak go używać do znajdowania słuchanych i nawiązywanych połączeń sieciowych.

01. W Windows 2019 wykonałeś polecenie `netstat -fn`

```
C:\Users\Administrator>netstat -fn

Active Connections

Proto Local Address          Foreign Address         State
TCP   192.167.0.1:22          192.167.0.111:59661    ESTABLISHED
TCP   192.167.0.1:389        192.167.0.1:49867     ESTABLISHED
TCP   192.167.0.1:49867      192.167.0.1:389      ESTABLISHED
TCP   192.167.0.1:49900      192.167.0.111:80      ESTABLISHED
TCP   [::1]:389              [::1]:49694           ESTABLISHED
TCP   [::1]:389              [::1]:49695           ESTABLISHED
TCP   [::1]:389              [::1]:49722           ESTABLISHED
TCP   [::1]:49694            [::1]:389             ESTABLISHED
TCP   [::1]:49695            [::1]:389             ESTABLISHED
TCP   [::1]:49722            [::1]:389             ESTABLISHED
TCP   [::1]:49896            [::1]:47001           TIME_WAIT
```

02. W Windows wykonałeś polecenie `netstat -a -n -b | more`

```
C:\Users\Administrator>netstat -anb |more
```

```
C:\Users\Administrator>netstat -a -n -b | more
```

```
[dns.exe]
TCP   192.167.0.1:22          192.167.0.111:59661    ESTABLISHED
[sshd.exe]
TCP   192.167.0.1:53          0.0.0.0:0              LISTENING
[dns.exe]
TCP   192.167.0.1:139         0.0.0.0:0              LISTENING
Can not obtain ownership information
TCP   192.167.0.1:389        192.167.0.1:49867     ESTABLISHED
[lsass.exe]
TCP   192.167.0.1:49867      192.167.0.1:389      ESTABLISHED
[ServerManager.exe]
TCP   192.167.0.1:49916      192.167.0.111:80      ESTABLISHED
[IEXPLORE.EXE]
TCP   [::]:22                [::]:0                 LISTENING
[sshd.exe]
TCP   [::]:88                [::]:0                 LISTENING
```

Użycie parametru -a nakazuje netstat zwrócić nasłuchiwanie i nawiązane połączenia.

Użycie parametru -an nakazuje netstat zwrócić wszystkie nazwy w danych wyjściowych zamienione na adresy IP.

Użycie parametru -b nakazuje netstat poznać procesy Windows, które nasłuchują lub mają otwarte połączenia.

b. Używanie PowerShell do znajdowania aktywnych i nasłuchujących portów

Używanie PowerShell daje dużo większą kontrolę, aby zobaczyć tylko to, co chcesz, zamiast przewijania długich list danych wyjściowych. Polecenie cmdlet Get-NetTCPConnection jest znacznie bardziej szczegółowe niż netstat na temat tego, co chcesz zobaczyć.

01. Wpisz **Get-NetTcpConnection**. Zobaczysz dane wyjściowe podobne do tych, które podał netstat. Zamiast tylko dużego ciągu danych wyjściowych, Get-NetTcpConnection zwraca listę obiektów PowerShell.

Możesz teraz zobaczyć te same ogólne informacje, które do tej pory dostarczył netstat; domyślnie masz informację o OwningProcess (-b w netstat) i w polu AppliedSetting, które odnosi się do profilu sieciowego, którego częścią jest połączenie.

02. Potokuj dane wyjściowe, aby Select-Object pokazał wszystkie właściwości. Zobaczysz, że PowerShell zwraca o wiele więcej informacji niż zrobił to netstat.

Get-NetTCPConnection | Select-Object -Property *

```
PS C:\Users\Administrator> Get-NetTCPConnection | Select-Object -Property *

State           : Bound
AppliedSetting  :
OffloadState    : InHost
Caption         :
Description     :
ElementName     :
InstanceID     : :++49776++::++0
CommunicationStatus :
DetailedStatus :
HealthStatus   :
```

03. Zawęż dane wyjściowe do portów nasłuchujących.

Get-NetTCPConnection -State Listen

```
PS C:\Users\Administrator> Get-NetTCPConnection -State Listen

LocalAddress      LocalPort RemoteAddress      RemotePort State      AppliedSetting
-----
::               49727    ::                  0          Listen
::               49690    ::                  0          Listen
::               49680    ::                  0          Listen
::               49677    ::                  0          Listen
::               49671    ::                  0          Listen
```

04. Znajdź nazwy procesów dla pól OwningProcess. Aby to zrobić, uruchom polecenie cmdlet **Get-Process** i podaj identyfikator procesu, który zidentyfikowałeś, jak pokazano poniżej.

Get-Process -Id 804

```
PS C:\Users\Administrator> Get-Process -Id 804
```

Handles	NPM(K)	PM(K)	WS(K)	CPU(s)	Id	SI	ProcessName
832	27	58928	81704	13,00	804	0	svchost

Jeśli chcesz utworzyć inną właściwość dla nazwy procesu, możesz opcjonalnie użyć pola obliczeniowego Select-Object.

```
Get-NetTCPConnection | Select-Object -Property *,@{'Name' = 'ProcessName';'Expression'={{(Get-Process -Id $_.OwningProcess).Name}}}
```

05. Zawęż stany do nieco większej liczby, wyszukując Listening i Established definiując State wartość parametru jako listę rozdzielaną przecinkami.

```
Get-NetTCPConnection -State Listen,Established
```

06. Ogranicz połączenia do portu, do którego jest podłączone za pomocą parametru RemotePort.

```
Get-NetTCPConnection -RemotePort 80
```

```
PS C:\Users\Administrator> Get-NetTCPConnection -RemotePort 80
```

LocalAddress	LocalPort	RemoteAddress	RemotePort	State	AppliedSetting
192.167.0.1	51565	192.167.0.111	80	Established	Datacenter

07. Ogranicz połączenia do portu, do którego jest podłączone za pomocą parametru LocalPort.

```
Get-NetTCPConnection -LocalPort 3389
```

```
PS C:\Users\Administrator> Get-NetTCPConnection -LocalPort 3389
```

LocalAddress	LocalPort	RemoteAddress	RemotePort	State	AppliedSetting	OwningProcess
::	3389	::	0	Listen		804
0.0.0.0	3389	0.0.0.0	0	Listen		804

Wniosek

Widziałeś, jak narzędzie **Netstat** i polecenie programu PowerShell cmdlet **Get-NetTCPConnection** pomagają znaleźć lokalne połączenia sieciowe.

zgłoszenie

Przywróć pierwszy punkt kontrolny

Podsumowanie:

Po wykonaniu wszystkich czynności z powyższej instrukcji przeczytaj ponownie z zrozumieniem cel ogólny i cele szczegółowe, które znajdują się na pierwszej stronie instrukcji. Jeżeli one zostały niezrealizowane to powtarzaj wykonanie tej instrukcji w szkole lub/i w domu do momentu zrealizowania.