Máquina Virtual Windows 10 para VMware

1. Descargar ISO de Windows 10

Microsoft permite descargar la ISO.

1. Descargar programa de instalación de https://www.microsoft.com/en-us/software-download/windows10ISO

   Alternativa:

   https://archive.org/download/Windows10HomeProv1809ESP/Win10_1809_Spanish_x64.iso

2. Instalar y seleccionar:
   - **Windows 10 22H2**
   - Idioma: Español (u otro)
   - Arquitectura: 64 bits
3. Descargra la ISO y guardarla localmente.

2. Crear VM en VMware Workstation/Player

1. Abrir VMware > "Create a New Virtual Machine"
2. Seleccionar **Installer disc image file (ISO)** y elegir la ISO de Windows 10
3. Configurar:
   - Nombre: `Win10-Lab`
   - Disco: 40 GB (dinámico)
   - RAM: 8 GB
   - CPU: 2 núcleos
   - **Red:** Bridged o NAT con acceso a Kali
4. Finalizar y arrancar la VM para instalar Windows. Proceder a la instalación. Instalar las VMware tools (Win + R y d:\setup)

3. Configurar Windows 10

Una vez instalado:

1. **Crear un usuario local llamado `administrator` (si no se ha creado al instalar el SO)**
2. Desactivar la contraseña de inicio de sesión (opcional, solo para pruebas):

   ```
   net user administrator password
   ```

3. Asegurarse de que la red esté **"privada"** (no "pública") para habilitar descubrimiento y SMB.

4. Habilitar SMB, WinRM y otras funciones necesarias

Abrir PowerShell como administrador y ejecutae:

```
# Habilitar SMBv1 y SMBv2 (si es necesario para pruebas)
  Enable-WindowsOptionalFeature -Online -FeatureName SMB1Protocol -All -NoRestart
  Set-SmbServerConfiguration -EnableSMB2Protocol $true -Force

# Cambiar red Publica a Privada
  Get-NetConnectionProfile
  Set-NetConnectionProfile -InterfaceAlias "Ethernet0" -NetworkCategory Private

# Habilitar WINRM
  Enable-PSRemoting -Force
  Set-Item WSMan:\localhost\Service\Auth\Basic -Value $true
  Restart-Service WinRM

# Permitir ejecución de scripts (para Mimikatz o PowerShell)
  Set-ExecutionPolicy RemoteSigned -Force

# Crear carpeta compartida
  New-Item -Path "C:\LabShare" -ItemType Directory
  New-SmbShare -Name "LabShare" -Path "C:\LabShare" -FullAccess "Todos"

Restart-Computer
```

5. Desactivar protecciones (solo en LAB)

Desactivar temporalmente Windows Defender (si se va a usar Mimikatz):

```
Set-MpPreference -DisableRealtimeMonitoring $true
```

No olvidar reactivarlo después de las pruebas. También se puede usar el **Modo Seguro con red** si quieres usar Mimikatz sin ser detectado.

6, Desactivar actualizaciones automáticas:

Evitar que se parcheen las vulnerabilidades, mediante la desactivación de las actualizaciones automáticas:

```
sc stop wuauserv
sc.exe config wuauserv start= disabled
```

7. Activar Print Spooler y RDP:

```
sc.exe config spooler start= auto
sc start spooler

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

```
Enable-NetFirewallRule -DisplayGroup "Remote Desktop"
```

8. Crear usuario vulnerable:

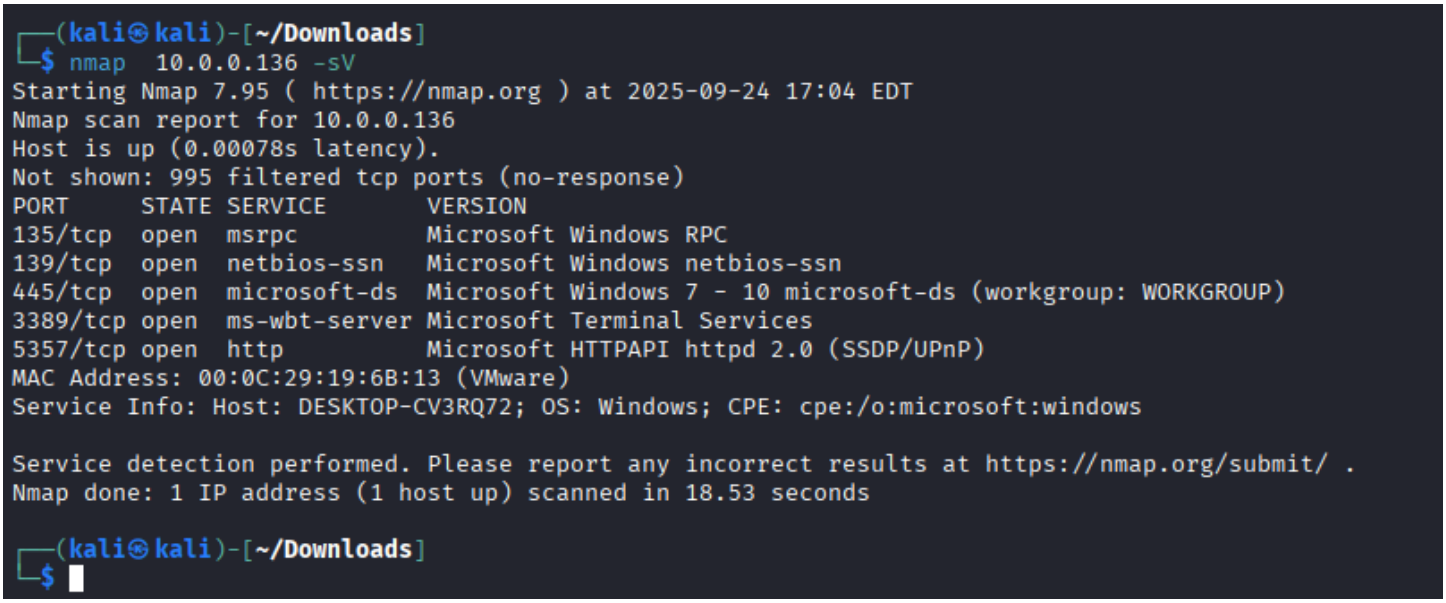
```
net user pentester Password123 /add
net localgroup administrators pentester /add

Restart-Computer
```

9. Verificación final

En Kali, ejecutar:

```
nmap 10.0.0.136 -sV
```

Salida esperada:



También se puede verificar con NetExec:

```
netexec smb 10.0.0.135
netexec winrm 10.0.0.135
```

10. Exportar la VM como plantilla

En VMware:

- **VM > Manage > Clone**
- Seleccionar **"Create a full clone"** y guárdarla como plantilla lista para futuras pruebas.