Krishna Dauliya

Lab Number: NetLabs4

VM Types/ User: Win12R2 VM ( administrator/ Train1ng$)

DVL VM (root /toor)

In this lab, you will use PowerShell to perform an active reconnaissance of a Windows server and a windows client. This is one of the common pen testing techniques used by threat actors to gain information about a target.

1. ***Active Reconnaissance of a Windows Server***

We logged into Window server-12R and opened power shell as Administrator. We created a variable $cred to store the credential object.

*PS C:\Windows\system32> $cred=Get-Credential*

Above command stores all user Credential in the variable $cred. Now, we are going to filter SAMAccountName (Security Account Manager) from the above variable and select the.

*PS C:\Windows\system32> Get-ADGroupMember -Credential $cred -server Win12R2 “Domain Users” | select samaccountname*

Above command gives all SAMAccountName User; however, we want to identify the Domain admin. Below command help to identify the Domain Admin member.

*PS C:\Windows\system32> Get-ADGroupMember -Credential $cred -server Win12R2 “Domain Admins”*

To Filter SAMAccountName with Domain Admin, we can use below command

*PS C:\Windows\system32> Get-ADGroupMember -Credential $cred -server Win12R2 “Domain Admins” | select samaccountname*

To View domain itself

*PS C:\Windows\system32> Get-ADDomain*

To View any specific user

*PS C:\Windows\system32> Get-ADUser -filter ‘samaccountname -eq “User\_Name”’*