
# Security+ Lab Series

# Lab 04: Performing Active Reconnaissance with Windows

**Document Version: 2018-11-01**

# Contents



## Introduction

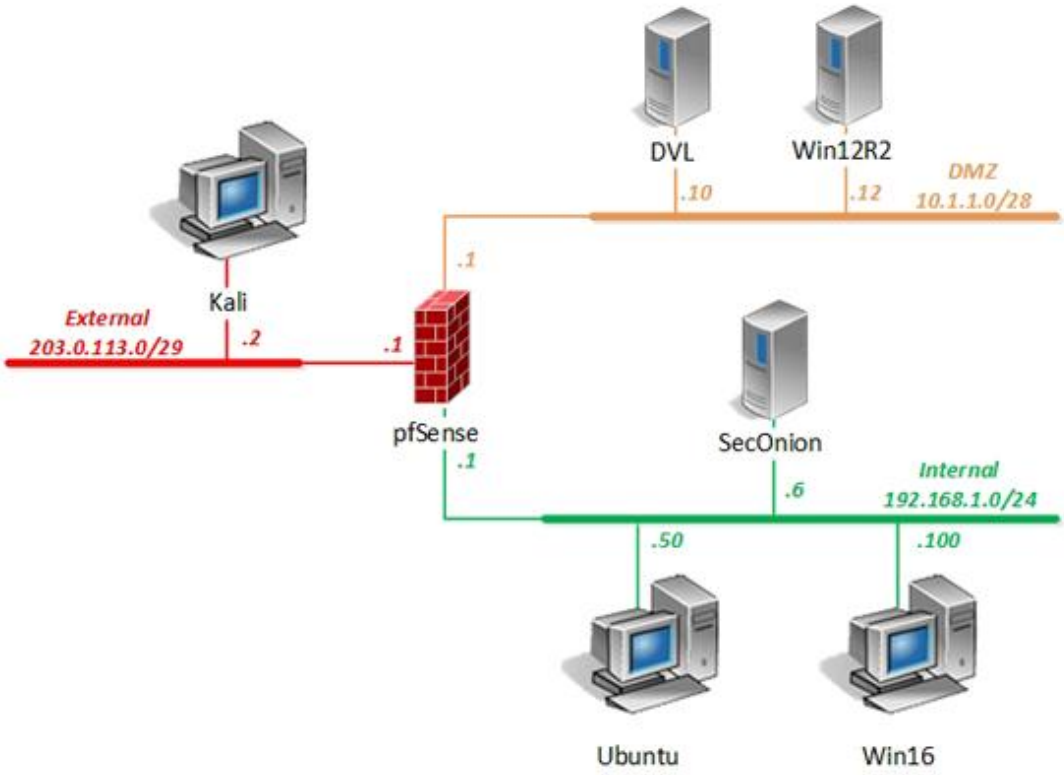
In this lab, you will use *PowerShell* to perform an active reconnaissance of a *Windows* server and a *Windows* client. This is one of the common pen testing techniques used by threat actors to gain information about a target.

## Objectives

- Explain penetration testing concepts

## Lab Topology



## Lab Settings

The information in the table below will be needed to complete the lab. The task sections below provide details on the use of this information.

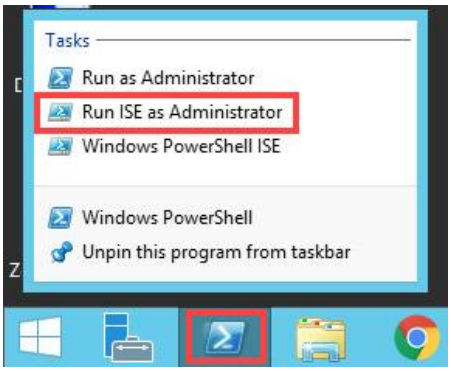
| Virtual Machine | IP Address | Account | Password |
|---|---|---|---|
| DVL | 10.1.1.10 /28 | root | toor |
| Kali | 203.0.113.2 /29 | root | toor |
| pfSense | eth0: 192.168.1.1 /24<br>eth1: 10.1.1.1 /28<br>eth2: 203.0.113.1 /29 | admin | pfsense |
| SecOnion | 192.168.1.6 /24 | soadmin | mypassword |
| | | root | mypassword |
| Ubuntu | 192.168.1.50 /24 | student | securepassword |
| | | root | securepassword |
| Win12R2 | 10.1.1.12 /28 | administrator | Train1ng$ |
| Win16 | 192.168.1.100 /24 | lab-user | Train1ng$ |
| | | Administrator | Train1ng$ |

# 1 Use PowerShell to Perform an Active Reconnaissance of a Windows Server

In this task, you will utilize *PowerShell* on the *Windows* server to gather extensive information.

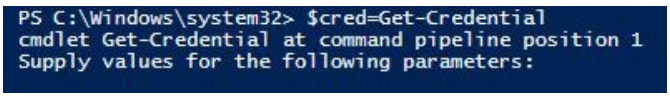
1. Launch the **Win12R2** virtual machine to access the graphical login screen.
2. While on the splash screen, focus on the *NETLAB+* tabs. Click the drop-down menu for the **Win12R2** tab and click on **Send CTRL+ALT+DEL**.
3. Log in as **administrator** using the password **`Train1ng$`**.


4. Right-click on the **PowerShell** icon in the taskbar and click **Run ISE as Administrator**.



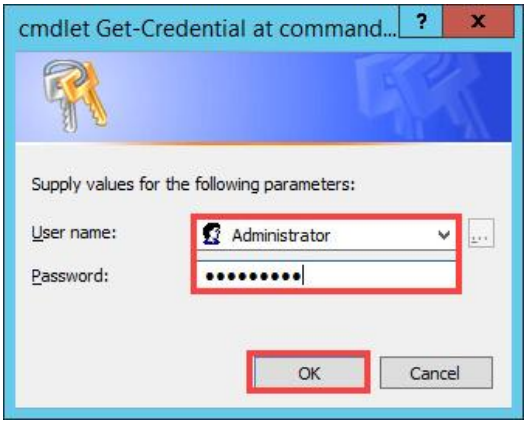

5. In the *PowerShell* window, type the command below followed by pressing the **Enter** key.

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



6. Notice a pop-up window appears. Type **Administrator** in the *User name* field, followed by typing **Train1ng$** in the *Password* field. Click **OK**.




7. Back in the *PowerShell* prompt, enter the command below to retrieve a list of domain users on the system.

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

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

samaccountname
--------------
Administrator
krbtgt
lab-user
lab-user-id
lab2-user
```

8. Enter the command below to identify which users are “*Domain Admin Members*.”

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

```
PS C:\Windows\system32> Get-ADGroupMember -Credential $cred -server Win12R2 "Domain Admins"


distinguishedName : CN=Administrator,CN=Users,DC=lab,DC=local
name              : Administrator
objectClass       : user
objectGUID        : 344a85f9-8fa2-45f0-8d6f-35dfb63c0afc
SamAccountName    : Administrator
SID               : S-1-5-21-3470663438-1104567976-3061388913-500

distinguishedName : CN=lab user,CN=Users,DC=lab,DC=local
name              : lab user
objectClass       : user
objectGUID        : 5b6f6d30-282b-4895-9397-2892f7961fef
SamAccountName    : lab-user
SID               : S-1-5-21-3470663438-1104567976-3061388913-1107
```

9. Filter the *SAM* account names.

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

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

samaccountname
--------------
Administrator
lab-user
```

10. View the domain itself.

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

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


AllowedDNSSuffixes                : {}
ChildDomains                      : {}
ComputersContainer                : CN=Computers,DC=lab,DC=local
DeletedObjectsContainer           : CN=Deleted Objects,DC=lab,DC=local
DistinguishedName                 : DC=lab,DC=local
DNSRoot                           : lab.local
DomainControllersContainer        : OU=Domain Controllers,DC=lab,DC=local
DomainMode                        : Windows2012R2Domain
DomainSID                         : S-1-5-21-3470663438-1104567976-3061388913
ForeignSecurityPrincipalsContainer : CN=ForeignSecurityPrincipals,DC=lab,DC=local
Forest                            : lab.local
InfrastructureMaster              : Win12R2.lab.local
LastLogonReplicationInterval      :
LinkedGroupPolicyObjects          : {CN={31B2F340-016D-11D2-945F-00C04FB984F9},CN=Policies,CN=System,DC=lab,DC=local}
LostAndFoundContainer             : CN=LostAndFound,DC=lab,DC=local
ManagedBy                         :
Name                              : lab
NetBIOSName                       : LAB
ObjectClass                       : domainDNS
ObjectGUID                        : 29307fce-ca8d-49a6-84f5-683244bd3d63
ParentDomain                      :
PDCEmulator                       : Win12R2.lab.local
QuotasContainer                   : CN=NTDS Quotas,DC=lab,DC=local
ReadOnlyReplicaDirectoryServers   : {}
ReplicaDirectoryServers           : {Win12R2.lab.local}
RIDMaster                         : Win12R2.lab.local
SubordinateReferences             : {DC=ForestDnsZones,DC=lab,DC=local, DC=DomainDnsZones,DC=lab,DC=local,
                                    CN=Configuration,DC=lab,DC=local}
SystemsContainer                  : CN=System,DC=lab,DC=local
UsersContainer                    : CN=Users,DC=lab,DC=local
```

11. See whether the *lab2-user* account is currently enabled.

```
PS C:\Windows\system32> Get-ADUser -filter ‘samaccountname -eq “lab2-user”’
```

```
PS C:\Windows\system32> Get-AdUser -filter 'samaccountname -eq "lab2-user"'


DistinguishedName : CN=lab2 user,CN=Users,DC=lab,DC=local
Enabled           : True
GivenName         : lab2
Name              : lab2 user
ObjectClass       : user
ObjectGUID        : 2b212ee9-f5fc-4a4d-948b-c557f58c4102
SamAccountName    : lab2-user
SID               : S-1-5-21-3470663438-1104567976-3061388913-5605
Surname           : user
UserPrincipalName : lab2-user@lab.local
```

12. Not only do we see that the account *lab2-user* is enabled, but we also have the accounts' *SID* as well. Try to retrieve more information about the *Administrator* account by entering the command below.

```
PS C:\Windows\system32> Get-ADUser -filter 'samaccountname -eq "administrator"'
```

```
PS C:\Windows\system32> Get-AdUser -filter 'samaccountname -eq "administrator"'

DistinguishedName : CN=Administrator,CN=Users,DC=lab,DC=local
Enabled           : True
GivenName         :
Name              : Administrator
ObjectClass       : user
ObjectGUID        : 344a85f9-8fa2-45f0-8d6f-35dfb63c0afc
SamAccountName    : Administrator
SID               : S-1-5-21-3470663438-1104567976-3061388913-500
Surname           :
UserPrincipalName :
```

13. View the **lab-user** account user's group memberships and confirm whether the account belongs to the *Domain Admins* group.

```
PS C:\Windows\system32> Get-ADPrincipalGroupMembership lab-user
```

```
PS C:\Windows\system32> Get-ADPrincipalGroupMembership lab-user

distinguishedName : CN=Domain Users,CN=Users,DC=lab,DC=local
GroupCategory     : Security
GroupScope        : Global
name              : Domain Users
objectClass       : group
objectGUID        : 4d7ea3dc-a14a-47b3-905f-e3f4ddd27bb1
SamAccountName    : Domain Users
SID               : S-1-5-21-3470663438-1104567976-3061388913-513

distinguishedName : CN=Remote Desktop Users,CN=Builtin,DC=lab,DC=local
GroupCategory     : Security
GroupScope        : DomainLocal
name              : Remote Desktop Users
objectClass       : group
objectGUID        : dd681b59-2af3-452c-898a-ba7eabf1e9fc
SamAccountName    : Remote Desktop Users
SID               : S-1-5-32-555

distinguishedName : CN=Domain Admins,CN=Users,DC=lab,DC=local
GroupCategory     : Security
                  : Global
name              : Domain Admins
                  : group
objectGUID        : 817fb15a-5f38-4297-8c74-a19e98d9dba9
SamAccountName    : Domain Admins
SID               : S-1-5-21-3470663438-1104567976-3061388913-512

distinguishedName : CN=Server Operators,CN=Builtin,DC=lab,DC=local
GroupCategory     : Security
GroupScope        : DomainLocal
name              : Server Operators
objectClass       : group
objectGUID        : 4db43dd3-6871-42d1-9428-1ee2cbceefeb
SamAccountName    : Server Operators
SID               : S-1-5-32-549
```

It can be verified that the *lab-user* is part of the *Domain Admins* group as well as other groups.

14. Leave the *PowerShell* window open to continue with the next task.

## 2 Use PowerShell to Perform an Active Reconnaissance of a Windows Client

In this task, you will utilize *PowerShell* on a *Windows* system to gather extensive information.

1. Identify the *Active Directory* that *lab-user* belongs to by entering the *.NET* command with *PowerShell* below.

```
PS C:\Windows\system32>
[System.directoryServices.activeDirectory.forest]::GetCurrentForest()
```

```
PS C:\Windows\system32> [System.directoryServices.activeDirectory.forest]::GetCurrentForest()


Name                  : lab.local
Sites                 : {Default-First-Site-Name}
Domains               : {lab.local}
GlobalCatalogs        : {Win12R2.lab.local}
ApplicationPartitions : {DC=DomainDnsZones,DC=lab,DC=local, DC=ForestDnsZones,DC=lab,DC=local}
ForestModeLevel       : 6
ForestMode            : Windows2012R2Forest
RootDomain            : lab.local
Schema                : CN=Schema,CN=Configuration,DC=lab,DC=local
SchemaRoleOwner       : Win12R2.lab.local
NamingRoleOwner       : Win12R2.lab.local
```

2. Since the forest is different from a domain, identify which domain the user is associated with.

```
PS C:\Windows\system32>
[System.DirectoryServices.ActiveDirectory.Domain]::GetCurrentDomain()
```

```
PS C:\Windows\system32> [System.DirectoryServices.ActiveDirectory.Domain]::GetCurrentDomain()


Forest                  : lab.local
DomainControllers       : {Win12R2.lab.local}
Children                : {}
DomainMode              : Windows2012R2Domain
DomainModeLevel         : 6
Parent                  :
PdcRoleOwner            : Win12R2.lab.local
RidRoleOwner            : Win12R2.lab.local
InfrastructureRoleOwner : Win12R2.lab.local
Name                    : lab.local
```

Using *PowerShell*, you successfully obtained the domain name, forest name, and group membership.

3. The lab is now complete; you may end the reservation.