Get-WinEvent  -FilterHashtable @{Logname='Security';StartTime="5/14/2014";EndTime="5/20/2014"}|? { ($\_.id -eq 4720) -or ($\_.id -eq 4722) -or ($\_.id -eq 4723) } | ForEachObject

*Above this scenario for Get-WinEvent where we can restrict with dates rather scanning the complete event log.*

**User Management on AD:**

This script will display query the event log ( security log) and display the user level changes on the AD and display it.

Write-Host "Message `t On Whom `t Who did `t Domain `t Timecreated `t Record ID `t ObjectType"

Write-Host "--------------------------------------------------------------------------------------------"

$obj = "user"

Get-WinEvent -FilterHashtable @{Logname='Security'}|? { ($\_.id -eq 4720) -or ($\_.id -eq 4722) -or ($\_.id -eq 4723) -or ($\_.id -eq 4724) -or ($\_.id -eq 4725) -or ($\_.id -eq 4726) -or ($\_.id -eq 4738) -or ($\_.id -eq 4740) -or ($\_.id -eq 4765) -or ($\_.id -eq 4766) -or ($\_.id -eq 4767) -or ($\_.id -eq 4780) -or ($\_.id -eq 4781) -or ($\_.id -eq 4794) -or ($\_.id -eq 5376) -or ($\_.id -eq 5377)} | foreach-object {

$Event = $\_

$splt = $Event.Message.Split("`n")

$msg = $splt | Select -First 1

$eventXML = [xml]$Event.ToXml()

foreach ($attr in $eventXML.Event.EventData.Data)

{

if($attr.name -eq "TargetUserName")

{

$user = $attr.'#text'

}

if($attr.name -eq "TargetDomainName")

{

$domain = $attr.'#text'

}

if($attr.name -eq "SubjectUserName")

{

$auser = $attr.'#text'

}

}

$Eid = $Event.Id

$timec = $Event.TimeCreated

if($user)

{

"{0,-45} {1,-10} {2,-10} {3,-20} {4,-20} {5,-8} {6,-10}" -f $msg, $user, $auser, $domain, $timec, $Eid, $obj

}

}

**Computer Management on AD:**

This script will display query the event log ( security log) and display the Computer level changes on the AD and display it

Write-Host "Message `t On Whom `t Who did `t Domain `t Timecreated `t Event ID `t ObjectName"

Write-Host "--------------------------------------------------------------------------------------------"

$obj = "computer"

Get-WinEvent -FilterHashtable @{Logname='Security'}|? { ($\_.id -eq 4743) -or ($\_.id -eq 4742) -or ($\_.id -eq 4741) } | foreach-object {

$Event = $\_

$splt = $Event.Message.Split("`n")

$msg = $splt | Select -First 1

$eventXML = [xml]$Event.ToXml()

foreach ($attr in $eventXML.Event.EventData.Data)

{

if($attr.name -eq "TargetUserName")

{

$user = $attr.'#text'

}

if($attr.name -eq "TargetDomainName")

{

$domain = $attr.'#text'

}

if($attr.name -eq "SubjectUserName")

{

$auser = $attr.'#text'

}

}

$Eid = $Event.Id

$timec = $Event.TimeCreated

if($user)

{

"{0,-45} {1,-10} {2,-10} {3,-20} {4,-20} {5,-8} {6,-10}" -f $msg, $user, $auser, $domain, $timec, $Eid, $obj

}

}

**Group Management on AD:**

This script will display query the event log ( security log) and display the Group level changes on the AD and display it

Write-Host "Message `t MemberName `t On Whom `t Who did `t Domain `t Timecreated `t Event ID `t ObjectType"

Write-Host "------------------------------------------------------------------------------------------------------------"

$obj = "group"

Get-WinEvent -FilterHashtable @{Logname='Security'}|? { ($\_.id -eq 4727) -or ($\_.id -eq 4728) -or ($\_.id -eq 4729) -or ($\_.id -eq 4730) -or ($\_.id -eq 4731) -or ($\_.id -eq 4732) -or ($\_.id -eq 4733) -or ($\_.id -eq 4734) -or ($\_.id -eq 4735) -or ($\_.id -eq 4737) -or ($\_.id -eq 4754) -or ($\_.id -eq 4755) -or ($\_.id -eq 4756) -or ($\_.id -eq 4757) -or ($\_.id -eq 4758) -or ($\_.id -eq 4764) -or ($\_.id -eq 4744) -or ($\_.id -eq 4745) -or ($\_.id -eq 4746) -or ($\_.id -eq 4747) -or ($\_.id -eq 4748) -or ($\_.id -eq 4749) -or ($\_.id -eq 4750) -or ($\_.id -eq 4751) -or ($\_.id -eq 4752) -or ($\_.id -eq 4753) -or ($\_.id -eq 4759) -or ($\_.id -eq 4760) -or ($\_.id -eq 4761) -or ($\_.id -eq 4762) -or ($\_.id -eq 4763) } | foreach-object {

$Event = $\_

$splt = $Event.Message.Split("`n")

$msg = $splt | Select -First 1

$eventXML = [xml]$Event.ToXml()

foreach ($attr in $eventXML.Event.EventData.Data)

{

if($attr.name -eq "MemberName")

{

$mn = $attr.'#text'

}

if($attr.name -eq "TargetUserName")

{

$user = $attr.'#text'

}

if($attr.name -eq "TargetDomainName")

{

$domain = $attr.'#text'

}

if($attr.name -eq "SubjectUserName")

{

$auser = $attr.'#text'

}

}

$Eid = $Event.Id

$timec = $Event.TimeCreated

if($user)

{

"{0,-45} {1,-40} {2,-10} {3,-20} {4,-20} {5,-8} {6,-10} {7,-10}" -f $msg, $mn, $user, $auser, $domain, $timec, $Eid, $obj

}

}