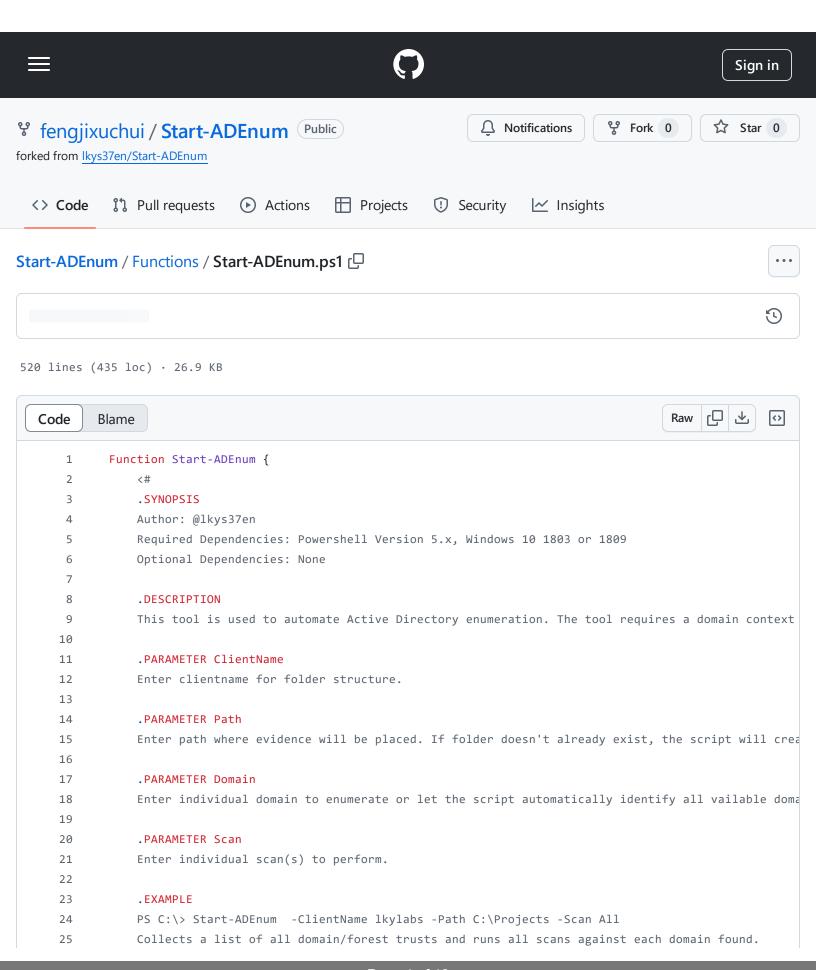
Start-ADEnum/Functions/Start-ADEnum.ps1 at e237a739db98b6104427d833004836507da36a58 · fengjixuchui/Start-ADEnum · GitHub - 31/10/2024 18:53 https://github.com/fengjixuchui/Start-



```
26
27
           .EXAMPLE
28
           PS C:\> Start-ADEnum -ClientName lkylabs -Path C:\Projects -Domain lkylabs.com -Scan All
           Runs all scans against lkylabs.com and corp.lkylabs.com.
29
30
31
            .EXAMPLE
32
           PS C:\> Start-ADEnum -ClientName lkylabs -Path C:\Projects -Domain lkylabs.com,corp.lkylabs.cd
33
           Runs PowerView and Bloodhound scans against lkylabs.com and corp.lkylabs.com domains.
34
35
           #>
           [CmdletBinding()]
36
           Param (
37
                [Parameter(Mandatory = $true)]
38
               [ValidateNotNullOrEmpty()]
39
40
               [String]
               $ClientName,
41
42
               [Parameter(Mandatory = $true)]
43
                [ValidateNotNullOrEmpty()]
44
               [String]
45
46
               $Path,
47
                [Parameter(Mandatory = $false)]
48
49
                [String[]]
50
               $Domains,
51
52
               [Parameter(Mandatory = $True)]
53
                [ValidateSet("ADCS", "Bloodhound", "GPOReport", "PowerView", "PingCastle", "PrivExchange",
               [String[]]
54
               $Scan
55
           )
56
57
           Begin {
58
               #Folders variable
59
60
               Folders = @(
                    "PingCastle"
61
                    "PowerView"
62
                    "Bloodhound"
63
                    "GP0"
64
                    "Microsoft Services\Exchange"
65
                    "Microsoft Services\ADCS"
66
               )
67
68
69
               #Installs all preregs if missing
               Write-Host -ForegroundColor Green "[*] Performing prereqs check"
70
               Start-PrereaCheck
71
```

```
72
                Import-Module C:\Tools\PowerSploit\Recon\PowerView.ps1
73
 74
 75
                #Creating Path and evidence folder structure
                if ((Test-Path $Path) -eq $false) {
 76
 77
                    try {
                        Write-Host -ForegroundColor Green "[+] Creating $Path Folder "
 78
 79
                        mkdir -Path $Path | Out-Null
 80
                    }
 81
 82
                    catch {
 83
                        throw "An error has occurred $($_.Exception.Message)"
 84
                    }
 85
 86
                    try {
 87
                        Write-Host -ForegroundColor Green "[+] Creating $ClientName Folder"
 88
                        mkdir -Path $Path\$ClientName | Out-Null
 89
 90
                    }
 91
                    catch {
 92
                        throw "An error has occurred $($_.Exception.Message)"
 93
 94
                    }
 95
 96
                    try {
97
                        if ($Domain) {
                             Write-host -ForegroundColor Green "[+] Performing Enumeration only on $Domain"
98
                             $Domains = $Domain
99
                        }
100
101
102
                        else {
                             $Domains = (Get-DomainTrustMapping -API).TargetName | Select-Object -Unique
103
                             if ($Domains -eq $null) { $Domains = (Get-NetDomain).Name }
104
105
                        }
106
                        foreach ($Domain in $Domains) {
107
                             Write-Host -ForegroundColor Magenta "[*] Creating $Domain evidence folders"
108
109
                             mkdir -Path "$Path\$ClientName\$Domain" | Out-Null
110
                             foreach ($folder in $folders) {
111
                                 mkdir -Path "$Path\$ClientName\$Domain\$folder" | Out-Null
112
113
                             }
                        }
114
                    }
115
116
117
                     catch S
```

Start-ADEnum/Functions/Start-ADEnum.ps1 at e237a739db98b6104427d833004836507da36a58 · fengjixuchui/Start-ADEnum · GitHub - 31/10/2024 18:53 https://github.com/fengjixuchui/Start-ADEnum/blob/e237a739db98b6104427d833004836507da36a58/Functions/Start-ADEnum.ps1#L450

Start-ADEnum/Functions/Start-ADEnum.ps1 at e237a739db98b6104427d833004836507da36a58 · fengjixuchui/Star ADEnum · GitHub - 31/10/2024 18:53 https://github.com/fengjixuchui/Start- ADEnum/blob/e237a739db98b6104427d833004836507da36a58/Functions/Start-ADEnum.ps1#L450	rt-

$Start-ADEnum/Functions/Start-ADEnum.ps1\ at\ e237a739db98b6104427d833004836507da36a58\cdot fengjixuchui/Start-ADEnum\cdot GitHub - 31/10/2024\ 18:53\ https://github.com/fengjixuchui/Start-ADEnum/blob/e237a739db98b6104427d833004836507da36a58/Functions/Start-ADEnum.ps1#L450$	

$Start-ADEnum/Functions/Start-ADEnum.ps1\ at\ e237a739db98b6104427d833004836507da36a58\cdot fengjixuchui/Start-ADEnum\cdot GitHub - 31/10/2024\ 18:53\ https://github.com/fengjixuchui/Start-ADEnum/blob/e237a739db98b6104427d833004836507da36a58/Functions/Start-ADEnum.ps1#L450$	

$Start-ADEnum/Functions/Start-ADEnum.ps1\ at\ e237a739db98b6104427d833004836507da36a58\cdot fengjixuchui/Start-ADEnum\cdot GitHub - 31/10/2024\ 18:53\ https://github.com/fengjixuchui/Start-ADEnum/blob/e237a739db98b6104427d833004836507da36a58/Functions/Start-ADEnum.ps1#L450$	

$Start-ADEnum/Functions/Start-ADEnum.ps1\ at\ e237a739db98b6104427d833004836507da36a58\cdot fengjixuchui/Start-ADEnum\cdot GitHub - 31/10/2024\ 18:53\ https://github.com/fengjixuchui/Start-ADEnum/blob/e237a739db98b6104427d833004836507da36a58/Functions/Start-ADEnum.ps1#L450$	

Start-ADEnum/Functions/Start-ADEnum.ps1 at e237a739db98b6104427d833004836507da36a58 · fengjixuchui/Star ADEnum · GitHub - 31/10/2024 18:53 https://github.com/fengjixuchui/Start- ADEnum/blob/e237a739db98b6104427d833004836507da36a58/Functions/Start-ADEnum.ps1#L450	rt-

```
447
                    #Running all scanner commands
448
449
                    foreach ($Argument in $Arguments) {
                        Set-Location $Folder; Start-Process C:\tools\PingCastle\PingCastle.exe -ArgumentLi
450
                    }
451
452
                    $Output = (Get-ChildItem $Folder -Exclude *html*, *xml*).FullName
453
454
                    #Converting PingCastle text files into CSV's
455
456
                    foreach ($Item in $Output) {
                        Import-Csv -Path $Item -Delimiter "`t" | Export-Csv -Path ($Folder + ($Item -split
457
458
                    }
459
460
                    #Remove original text files
                    (Get-ChildItem $Folder).FullName | Remove-Item -Include *.txt
461
462
                }
463
                switch ($Scan) {
464
                    "All" {
465
                        foreach ($Domain in $Domains) {
466
467
                            Write-Host -ForegroundColor Green "[+] Starting All AD Enum for $Domain"
                            Start-Job -ScriptBlock $PowerViewScriptBlock -ArgumentList $ClientName, $Path,
468
                            Start-Job -ScriptBlock $PingCastleScriptBlock -ArgumentList $ClientName, $Path,
469
                            Start-Job -ScriptBlock $BloodhoundScriptBlock -ArgumentList $ClientName, $Path,
470
471
                            Start-Job -ScriptBlock $GPOReportScriptBlock -ArgumentList $ClientName, $Path,
                            Start-Job -ScriptBlock $PrivExchangeCheck -ArgumentList $ClientName, $Path, $Dd
472
                            Start-Job -ScriptBlock $ADCS -ArgumentList $ClientName, $Path, $Domain -Name AL
473
474
                        }
                    }
475
476
                    "ADCS" {
477
478
                        foreach ($Domain in $Domains) {
                            Write-Host -ForegroundColor Green "[+] Starting AD Certificate Services Enum fo
479
                             Start-Job -ScriptBlock $ADCS -ArgumentList $ClientName, $Path, $Domain -Name Pr
480
481
                        }
482
                    }
483
```

```
"PowerView" {
484
                        foreach ($Domain in $Domains) {
485
486
                             Write-Host -ForegroundColor Green "[+] Starting PowerView Enum for $Domain"
                             Start-Job -ScriptBlock $PowerViewScriptBlock -ArgumentList $ClientName, $Path,
487
488
                        }
                    }
489
490
                    "PingCastle" {
491
                        foreach ($Domain in $Domains) {
492
                             Write-Host -ForegroundColor Green "[+] Starting Ping Castle AD Enum for $Domain
493
                             Start-Job -ScriptBlock $PingCastleScriptBlock -ArgumentList $ClientName, $Path,
494
495
                        }
                    }
496
497
                    "Bloodhound" {
498
499
                        foreach ($Domain in $Domains) {
                             Write-Host -ForegroundColor Green "[+] Starting Bloodhound AD Enum for $Domain'
500
                             Start-Job -ScriptBlock $BloodhoundScriptBlock -ArgumentList $ClientName, $Path,
501
502
                        }
                    }
503
504
                    "GPOReport" {
505
                        foreach ($Domain in $Domains) {
506
                             Write-Host -ForegroundColor Green "[+] Starting GPO Report AD Enum for $Domain'
507
508
                             Start-Job -ScriptBlock $GPOReportScriptBlock -ArgumentList $ClientName, $Path,
509
                        }
                    }
510
511
                    "PrivExchange" {
512
                        foreach ($Domain in $Domains) {
513
                             Write-Host -ForegroundColor Green "[+] Starting PrivExchange AD Enum for $Domai
514
515
                             Start-Job -ScriptBlock $PrivExchangeCheck -ArgumentList $ClientName, $Path, $Dd
                        }
516
517
                    }
518
                }
519
            }
520
        }
```