

# Trickbot rdp scandll – Transforming Candidate Credentials for Brute-Forcing RDP Servers

Archived: 2026-04-05 21:49:39 UTC

EmptyPass tries an empty password GetHost fills in the hostname of the currently attacked IP (ex: myhost) IP mothe currently attacked IP address (ex: 234.234.234.234)re Port fills in the currently attacked port (ex: 3389) IpReplaceDot 234.234.234.234 → 234234234234 remove the dots of the IP address RemoveNumerics us3rn4me → usrnme removes all number from the username RemoveLetters us3rn4m3 → 343 removes all letters from the username RemoveOtherSymbols usern@m3 → usernm3 removes all non-alphanumeric characters from the username OriginalUsernameLettersBeginInverse 123admin456 → 123654nimda keeps all non-letters (i.e. digits, special chars) at the beginning of the username and reverses the rest (“invert [from where] letters begin”) OriginalUsernameLettersBeginSwap 123admin456 → admin456123 swaps all non-letters (i.e. digits, special chars) at the beginning of the username with the rest (“swap [where] letters begin”) OriginalUsernameLettersEndInverse admin123root → admintoor321 keeps all letters at the beginning of the username and reverses the rest (“invert [where] letters end”) OriginalUsernameLettersEndSwap admin123root → 123rootadmin swaps all letters at the beginning of the username with the rest (“swap [where] letters end”) OriginalUsernameNumsBeginInverse admin123root → admintoor321 keeps all non-digits at the beginning of the username and reverses the rest (“invert [from where] nums begin”) OriginalUsernameNumsBeginSwap admin123root → admintoor321 swaps all non-digits at the beginning of the username with the rest (“swap [where] nums begin”) OriginalUsernameNumsEndInverse 123admin → 123nimda keeps all digits at the beginning of the username and reverses the rest (“invert [where] nums end”) OriginalUsernameNumsEndSwap 123admin456 → admin456123 swaps all digits at the beginning of the username with the rest (“swap [where] nums end”) OriginalUsernameInsert %OriginalUsernameInsert%(N)SOMESTRING → SOMEusernameSTRING (ex: N = 4) insert username after Nth character of SOMESTRING OriginalUsername use the username as password OnlyName Firstname Lastname → Firstname uses only the first name (everything left of the first space) of the username as password OnlySurname Firstname Lastname → Lastname uses only the last name (everything right of the first space) of the username as password username Admin → admin username in lowercase Username AdMin → Admin username lowercase but first char upper UsErNaMe Admin → AdMiN username in alternating case, starting with uppercase uSeRnAmE Admin → aDmIn username in alternating case, starting with lowercase USERNAME Admin → ADMIN username in uppercase EMANRESU Admin → NIMDA username in uppercase and reversed EmanresuLowercase AdMin → Nimda username reversed and lowercase, first char uppercase Emanresu AdMin → NiMdA username reversed, first char upper emanresuLowercase AdMin → nimda username reversed and lowercase emanresuUppercase AdMin → NIMDA username reversed and uppercase emanresu Admin → nimda username reversed and lowercase ReplaceFirst\_X-x administrator → @dministrator (ex: %ReplaceFirst\_a-@%) replaces the first occurrence of X with x in the username (needle and replacement can be more than 1 char) ReplaceFirstI\_X-x Administrator → @dministrator (ex: %ReplaceFirstI\_a-@%) case insensitively replaces the first occurrence of X with x in the username (needle and replacement can be more than 1 char) ReplaceLast\_X-x administrator → @dministrator (ex: %ReplaceLast\_a-@%) replaces the last occurrence of X with x in the username (needle and replacement can be more than 1 char) ReplaceLastI\_X-x Administrator →

@dministrator (ex: %ReplaceLastI\_a-@%) case insensitively replaces the last occurrence of X with x in the username (needle and replacement can be more than 1 char) ReplaceAll\_X-x administrator → @dministrator (ex: %ReplaceAll\_a-@%) replaces all occurrences of X with x in the username (needle and replacement can be more than 1 char) ReplaceAllI\_X-x Administrator → @dministrator (ex: %ReplaceAllI\_a-@%) case insensitively replaces all occurrences of X with x in the username (needle and replacement can be more than 1 char) DomainRemoveNumerics test-123.com → test-.com removes all digits from the domain DomainRemoveLetters test-123.com → -123. removes all letters from the domain DomainRemoveOtherSymbols test-123.com → test123com removes all non-alphanum chars from the domain OriginaldomainInsert %OriginaldomainInsert%(N)SOMESTRING → SOMEdomainSTRING (ex: N = 4) insert domain after Nth character of SOMESTRING OriginaldomainPart test-123.com → 123com (ex: %OriginaldomainPart%(6)) takes the last N chars of the domain name (ignoring any dots) OriginaldomainNumsBeginInverse test-123.com → test-moc.321 keeps all non-digits at the beginning of the domain and reverses the rest (“invert [from where] nums begin”) OriginaldomainNumsBeginSwap test-123.com → 123.comtest- swaps all non-digits at the beginning of the domain with the rest (“swap [where] nums begin”) OriginaldomainNumsEndInverse 123-test.com → 123moc.tset- keeps all digits at the beginning of the domain and reverses the rest (“invert [where] nums end”) OriginaldomainNumsEndSwap 123-test.com → -test.com123 swaps all digits at the beginning of the domain with the rest (“swap [where] nums end”) OriginaldomainLettersBeginInverse test-123.com → test-moc.321 keeps all non-letters (i.e. digits, special chars) at the beginning of the domain and reverses the rest (“invert [from where] letters begin”) OriginaldomainLettersBeginSwap 123-test.com → test.com123- swaps all non-letters (i.e. digits, special chars) at the beginning of the domain with the rest (“swap [where] letters begin”) OriginaldomainLettersEndInverse test-123.com → testmoc.321- keeps all letters at the beginning of the domain and reverses the rest (“invert [where] letters end”) OriginaldomainLettersEndSwap test-123.com → -123.comtest swaps all letters at the beginning of the domain with the rest (“swap [where] letters end”) Originaldomainleft test-123.com → test-123 takes the left part of the domain (everything left of the first dot) and lowercases the first character OriginalDomainleft test-123.com → Test-123 takes the left part of the domain (everything left of the first dot) and capitalizes the first character Originaldomainright test-123.com → test-123 takes the right part of the domain (everything right of the first dot) and lowercases the first character OriginalDomainright test-123.com → Test-123 takes the right part of the domain (everything right of the first dot) and capitalizes the first character Originaldomain uses the plain domain name OriginalDomain test-123.com → Test-123.com uses the domain name and capitalizes the first character NiamodLowercase abc%NiamodLowercase%123 abc123 niamodLowercase test-123.com → Moc.321-tset reverses and lowercases the domain name, first character capitalized niamodUppercase test-123.com → mOC.312-TSET reverses and capitalizes the domain name, first char lowercase domainleftHyphen test-123.com → test takes everything left of the first hyphen DOMAINLEFTHYPHEN test-123.com → TEST takes everything left of the first hyphen, capitalized DomainleftHyphen test-123.com → Test takes everything left of the first hyphen, first char capitalized domainrightHyphen test-123.com → 123.com takes everything right of the first hyphen DOMAINRIGHTHYPHEN test-123.com → 123.COM takes everything right of the first hyphen, capitalized DomainrightHyphen test-abc.com → Abc.com takes everything right of the first hyphen, first char capitalized domainleftUnderscore test\_123.com → test takes everything left of the first underscore DOMAINLEFTUNDERSCORE test\_123.com → TEST takes everything left of the first underscore, capitalized DomainleftUnderscore test\_123.com → Test takes everything left of the first underscore, first char capitalized domainrightUnderscore test\_abc.com → abc.com takes everything right of the first underscore

DOMAINRIGHTUNDERSCORE test\_123.com → 123.COM takes everything right of the first underscore, capitalized DomainrightUnderscore test\_abc.com → Abc.com takes everything right of the first underscore, first char capitalized DomainReplaceFirst\_X-x EXAMPLE-attack.com → EXAMPLE-@ttack.com (ex: %DomainReplaceFirst\_a-@%) replaces the first occurrence of X with x in the domain (needle and replacement can be more than 1 char) DomainReplaceFirstI\_X-x EXAMPLE-attack.com → EX@MPLE-attack.com (ex: %DomainReplaceFirstI\_a-@%) case insensitively replaces the first occurrence of X with x in the domain (needle and replacement can be more than 1 char) DomainReplaceLast\_X-x EXAMPLE-attack.com → EXAMPLE-att@ck.com (ex: %DomainReplaceLast\_a-@%) replaces the last occurrence of X with x in the domain (needle and replacement can be more than 1 char) DomainReplaceLastI\_X-x EXAMPLE-attack.com → EXAMPLE-att@ck.com (ex: %DomainReplaceLastI\_a-@%) case insensitively replaces the last occurrence of X with x in the domain (needle and replacement can be more than 1 char) DomainReplaceAll\_X-x EXAMPLE-attack.com → EXAMPLE-@tt@ck.com (ex: %DomainReplaceAll\_a-@%) replaces all occurrences of X with x in the domain (needle and replacement can be more than 1 char) DomainReplaceAllI\_X-x EXAMPLE-attack.com → EX@MPLE-@tt@ck.com (ex: %DomainReplaceAllI\_a-@%) case insensitively replaces all occurrences of X with x in the domain (needle and replacement can be more than 1 char) niamod test-123.com → moc.321-tset reverses the domain name Niamod test-123.com → Moc.321-tset reverses the domain name, first char capitalized domainleft TEST-123.com → test-123 everything left of the first dot, lowercased DOMAINLEFT Test-123.com → TEST-123 everything left of the first dor, capitalized Domainleft test-123.com → Test-123 everything left of the first dot, lowercased but first char capitalized domainright TEST-123.com → com everything right of the first dot, lowercased DOMAINRIGHT Test-123.com → COM everything right of the first dor, capitalized Domainright test-123.com → Com everything right of the first dot, lowercased but first char capitalized domain TEST-123.com → test-123.com domain name, lowercase Domain TEST-123.com domain name lowercased, first char capitalized DoMaIn test-123.com → TeSt-123.cOm domain name in alternating case, starting with uppercase dOmAiN test-123.com → tEsT-123.CoM domain name in alternating case, starting with lowercase DOMAIN test-123.com → TEST-123.COM domain name capitalized NIAMOD test-123.com → MOC.321-TSET domain name reversed and capitalized

---

Source: <https://cyber.wtf/2020/08/31/trickbot-rdpsscandll-password-transof/>