

Windows authentication brutforce cheat-sheet

Use cases / Rules

- Wrong password
 - Adapted to internet facing resources
 - Single user
 - Multiple users
 - Adapted to internal resources
 - Single user
 - Multiple users
- Single source
 - Single destination
 - Multiple destination
- Source unique
 - Utilisateurs multiples
 - Utilisateur unique
- Unexisting account
- Denied access
- Restricted access
- Locked account
- Disabled account
- Expired account

Failure codes

- Critical
 - Wrong password
 - Unexisting account
 - Denied access
 - Relevant
 - Restricted access
 - Why not
 - Locked account
 - Disabled account
 - Expired account
- 0xC000006A STATUS_WRONG_PASSWORD
- 0xC0000064 STATUS_NO_SUCH_USER
- 0xc0000022 STATUS_ACCESS_DENIED
- 0xC0000413 STATUS_AUTHENTICATION_FIREWALL_FAILED
- 0xC000006E STATUS_ACCOUNT_RESTRICTION
- 0xC0000070 STATUS_INVALID_WORKSTATION
- 0xC000006F STATUS_INVALID_LOGON_HOURS
- 0xC000015B STATUS_LOGON_TYPE_NOT_GRANTED
- 0xC0000234 STATUS_ACCOUNT_LOCKED_OUT
- 0xC0000072 STATUS_ACCOUNT_DISABLED
- 0xC0000193 STATUS_ACCOUNT_EXPIRED

Account type

- Protected users group
 - Privileged account
 - Service account
 - Builtin admin. account
 - VIP account
 - Standard account
 - Email address
 - Machine account (*\$)
- See related Microsoft feature
- Filtering on SID *-500 cannot work
- To filter out

Event IDs

- Kerberos
 - Security
 - 4768
 - 4771
 - Authentication
 - Security
 - 4625
 - NTLM
 - Security
 - 4776
 - Protected users group
 - Microsoft-Windows-Authentication/ProtectedUserFailures-DomainController
 - 100
- Kerberos use cases not covered here
- An NTLM sign-in failure occurs for an account that is in the Protected Users security group.

Authentication method

- Interactive
 - Code : 2
 - Network
 - Code: 3
 - Clear text
 - Code: 8
 - RDP
 - Code: 10
- Frequent with Exchange or IIS authentication
- Logon type 3 reported if login failure and RDP with NLA activated

Origin

- Fields to use
 - IpAddress
 - Workstation
 - Adresse type
 - Internal address
 - IPv4/v6
 - Localhost address
 - ::1
 - 127.0.0.1
 - 0.0.0.0
 - Public address
 - Empty
- ID 4776 only provides WORKSTATION field (no IP)
- Create dedicated rules also for localhost
- ID 4776 may return in some cases a empty Workstation, which may be ignored by some correlation languages while doing some aggregation

Fields for error codes

- Status
 - Substatus
 - 0x0
 - "_"
- Prefer to focus on the "Substatus" field. If "Substatus" matches one of those terms, fallback to "Status" field

Authentication Package Name

- Negotiate
- Kerberos
- NTLM
- MSV1_0

Author: mdecrevoisier
Version: 2022.18.07
Status: stable

If RDP connection and credentials are valid, ID 4825 will also trigger (requires auditing activation)

Reported only if a deny policy configuration has been defined in your domain

Vulnerability scanners may trigger disabled accounts login (eg: Guest)