"Logon Failure – Unknown user or bad password"

Username attempted: mrhac
Authentication method: NTLM
Logon Type: 3 (network login)

Windows rejected the login because:
Status: 0xC000006D → Bad username or password
SubStatus: 0xC000006A → Wrong password
FailureReason: Unknown username or bad password

rule.id = 60122
rule.level = 5 (Medium severity)


```
{
  "_index": "wazuh-alerts-4.x-2025.11.20",
  "_id": "4mBWoJoB3nscKqV7swoF",
  "_score": null,
  "_source": {
    "input": {
      "type": "log"
    },
    "agent": {
      "ip": "192.168.56.1",
      "name": "Mr-Chandan-Prasad-indian",
      "id": "001"
    },
    "manager": {
      "name": "wazuh.manager"
    },
    "data": {
      "win": {
        "eventdata": {
          "subjectLogonId": "0x0",
          "ipAddress": "10.14.228.46",
          "authenticationPackageName": "NTLM",
          "subStatus": "0xc000006a",
          "logonProcessName": "NtLmSsp",
          "targetUserName": "mrhac",
          "keyLength": "0",
          "subjectUserSid": "S-1-0-0",
          "processId": "0x0",
          "ipPort": "56109",
          "failureReason": "%%2313",
          "targetUserSid": "S-1-0-0",
          "logonType": "3",
          "status": "0xc000006d"
        },
        "system": {
          "eventID": "4625",
          "keywords": "0x8010000000000000",
          "providerGuid": "{54849625-5478-4994-a5ba-3e3b0328c30d}",
```

```
          "level": "0",
          "channel": "Security",
          "opcode": "0",
          "message": "\"An account failed to log
on.\r\n\r\nSubject:\r\n\tSecurity ID:\t\tS-1-0-0\r\n\tAccount Name:\t\t-
\r\n\tAccount Domain:\t\t-\r\n\tLogon ID:\t\t0x0\r\n\r\nLogon
Type:\t\t\t3\r\n\r\nAccount For Which Logon Failed:\r\n\tSecurity
ID:\t\tS-1-0-0\r\n\tAccount Name:\t\tmrhac\r\n\tAccount Domain:\t\t-
\r\n\r\nFailure Information:\r\n\tFailure Reason:\t\tUnknown user name or
bad password.\r\n\tStatus:\t\t\t0xC000006D\r\n\tSub
Status:\t\t0xC000006A\r\n\r\nProcess Information:\r\n\tCaller Process
ID:\t0x0\r\n\tCaller Process Name:\t-\r\n\r\nNetwork
Information:\r\n\tWorkstation Name:\t-\r\n\tSource Network
Address:\t10.14.228.46\r\n\tSource Port:\t\t56109\r\n\r\nDetailed
Authentication Information:\r\n\tLogon Process:\t\tNtLmSsp
\r\n\tAuthentication Package:\tNTLM\r\n\tTransited Services:\t-
\r\n\tPackage Name (NTLM only):\t-\r\n\tKey Length:\t\t0\r\n\r\nThis event
is generated when a logon request fails. It is generated on the computer
where access was attempted.\r\n\r\nThe Subject fields indicate the account
on the local system which requested the logon. This is most commonly a
service such as the Server service, or a local process such as
Winlogon.exe or Services.exe.\r\n\r\nThe Logon Type field indicates the
kind of logon that was requested. The most common types are 2
(interactive) and 3 (network).\r\n\r\nThe Process Information fields
indicate which account and process on the system requested the
logon.\r\n\r\nThe Network Information fields indicate where a remote logon
request originated. Workstation name is not always available and may be
left blank in some cases.\r\n\r\nThe authentication information fields
provide detailed information about this specific logon request.\r\n\t-
Transited services indicate which intermediate services have participated
in this logon request.\r\n\t- Package name indicates which sub-protocol
was used among the NTLM protocols.\r\n\t- Key length indicates the length
of the generated session key. This will be 0 if no session key was
requested.\"",
          "version": "0",
          "systemTime": "2025-11-20T08:16:59.8665215Z",
          "eventRecordID": "107770",
          "threadID": "12900",
          "computer": "Mr-Chandan-Prasad-indian",
          "task": "12544",
          "processID": "1440",
          "severityValue": "AUDIT_FAILURE",
          "providerName": "Microsoft-Windows-Security-Auditing"
        }
      }
    },
    "rule": {
      "mail": false,
      "level": 5,
      "pci_dss": [
        "10.2.4",
        "10.2.5"
      ],
      "hipaa": [
        "164.312.b"
```

```
      ],
      "tsc": [
        "CC6.1",
        "CC6.8",
        "CC7.2",
        "CC7.3"
      ],
      "description": "Logon Failure - Unknown user or bad password",
      "groups": [
        "windows",
        "windows_security",
        "authentication_failed"
      ],
      "nist_800_53": [
        "AU.14",
        "AC.7"
      ],
      "gdpr": [
        "IV_35.7.d",
        "IV_32.2"
      ],
      "firedtimes": 8,
      "mitre": {
        "technique": [
          "Account Access Removal"
        ],
        "id": [
          "T1531"
        ],
        "tactic": [
          "Impact"
        ]
      },
      "id": "60122",
      "gpg13": [
        "7.1"
      ]
    },
    "location": "EventChannel",
    "decoder": {
      "name": "windows_eventchannel"
    },
    "id": "1763626620.264852",
    "timestamp": "2025-11-20T08:17:00.792+0000"
  },
  "fields": {
    "timestamp": [
      "2025-11-20T08:17:00.792Z"
    ]
  },
  "sort": [
    1763626620792
  ]
}
```

What we Observed

- The Windows agent recorded multiple failed login attempts (Event ID 4625).
- Source IP 10.14.228.46 is your Kali VM performing WinRM brute-force.
- Wazuh triggered rule 60122 (Logon Failure) and 60204 (Multiple Failures).
- Username targeted: mrhac.
- Authentication type: NTLM, LogonType 3 (network logon).
- Failure Reason: *Unknown username or bad password*.
- Pattern indicates brute-force behavior.