ElastAlert: Brute Force Attempt

1 message

<rangammabokka46@gmail.com> Thu, May 15, 2025 at 6:30 PM
Reply-to: rangammabokka46@gmail.com
To: rangammabokka46@gmail.com

Brute Force Attempt

At least 4 events occurred between 2025-05-15 17:35 India Standard Time and 2025-05-15 17:40 India Standard Time

@timestamp: 2025-05-15T12:10:55.281Z
_id: hBDa05YBVMJVESZS3qju
_index: .ds-winlogbeat-8.10.2-2025.05.14-000001
agent: {
"ephemeral_id": "939500f9-4f78-4b63-9ef1-e42ed1a49f45",
"id": "e5e3a761-acc3-41a2-88c5-ee2b2b236970",
"name": "DESKTOP-VCH3K89",
"type": "winlogbeat",
"version": "8.10.2"
}
ecs: {
"version": "1.12.0"
}
event: {
"action": "logon-failed",
"category": [
"authentication"
],
"code": "4625",
"created": "2025-05-15T12:10:56.766Z",
"ingested": "2025-05-15T12:10:58.668441400Z",
"kind": "event",
"module": "security",
"outcome": "failure",
"provider": "Microsoft-Windows-Security-Auditing",
"type": [
"start"
]
}
host: {
"architecture": "x86_64",
"hostname": "desktop-vch3k89",
"id": "7e25c1a1-4745-47c6-abe9-ec7f50bf1d98",
"ip": [
"fe80::2674:6aaf:881:b09b",
"192.168.52.131"
],
"mac": [
"00-0C-29-C5-7F-10"
],
"name": "desktop-vch3k89",
"os": {
"build": "19045.5854",
"family": "windows",
"kernel": "10.0.19041.5848 (WinBuild.160101.0800)",
"name": "Windows 10 Home",
"platform": "windows",
"type": "windows",
"version": "10.0"
}
}
log: {
"level": "information"
}
message: An account failed to log on.

Subject:

Security ID: S-1-5-18
Account Name: DESKTOP-VCH3K89$
Account Domain: WORKGROUP
Logon ID: 0x3E7

Logon Type: 2

Account For Which Logon Failed:
Security ID: S-1-0-0
Account Name: -
Account Domain: -

Failure Information:
Failure Reason: An Error occured during Logon.
Status: 0xC000006D
Sub Status: 0xC0000380

Process Information:
Caller Process ID: 0x41c
Caller Process Name: C:\Windows\System32\svchost.exe

Network Information:
Workstation Name: -
Source Network Address: 127.0.0.1
Source Port: 0

Detailed Authentication Information:
Logon Process: User32
Authentication Package: Negotiate
Transited Services: -
Package Name (NTLM only): -
Key Length: 0

This event is generated when a logon request fails. It is generated on the computer where access was attempted.

The 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.

The Logon Type field indicates the kind of logon that was requested. The most common types are 2 (interactive) and 3 (network).

The Process Information fields indicate which account and process on the system requested the logon.

The Network Information fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases.

The authentication information fields provide detailed information about this specific logon request.
- Transited services indicate which intermediate services have participated in this logon request.
- Package name indicates which sub-protocol was used among the NTLM protocols.
- Key length indicates the length of the generated session key. This will be 0 if no session key was requested.

num_hits: 8
num_matches: 2
process: {
"executable": "C:\\Windows\\System32\\svchost.exe",
"name": "svchost.exe",
"pid": 1052
}
related: {
"ip": [
"127.0.0.1"
],
"user": [
"-"
]
}
source: {
"domain": "-",
"ip": "127.0.0.1",
"port": 0
}
user: {
"domain": "-",
"id": "S-1-0-0",
"name": "-"
}

```
winlog: {
    "activity_id": "{043bd195-c591-0000-79d3-3b0491c5db01}",
    "api": "wineventlog",
    "channel": "Security",
    "computer_name": "DESKTOP-VCH3K89",
    "event_data": {
        "AuthenticationPackageName": "Negotiate",
        "FailureReason": "%%2304",
        "KeyLength": "0",
        "LmPackageName": "-",
        "LogonProcessName": "User32 ",
        "LogonType": "2",
        "Status": "0xc000006d",
        "SubStatus": "0xc0000380",
        "SubjectDomainName": "WORKGROUP",
        "SubjectLogonId": "0x3e7",
        "SubjectUserName": "DESKTOP-VCH3K89$",
        "SubjectUserSid": "S-1-5-18",
        "TargetDomainName": "-",
        "TargetUserName": "-",
        "TargetUserSid": "S-1-0-0",
        "TransmittedServices": "-"
    },
    "event_id": "4625",
    "keywords": [
        "Audit Failure"
    ],
    "logon": {
        "failure": {
            "reason": "An Error occured during Logon.",
            "status": "This is either due to a bad username or authentication information"
        },
        "id": "0x3e7",
        "type": "Interactive"
    },
    "opcode": "Info",
    "process": {
        "pid": 828,
        "thread": {
            "id": 5596
        }
    },
    "provider_guid": "{54849625-5478-4994-a5ba-3e3b0328c30d}",
    "provider_name": "Microsoft-Windows-Security-Auditing",
    "record_id": "28119",
    "task": "Logon"
}
```