

Remote Desktop Brute-Force Detected

High Level Summary

| Attack | Time | System | IP |
|----------------------------|----------------------------|--------|---------------|
| Remote Desktop Brute Force | 2025-04-25T16:09:10.304075 | box | 192.168.1.125 |

Timeline of Events

| Sequence | Event ID | Timestamp |
|----------|----------|------------------------------|
| 1 | 4625 | 2025-04-25T16:08:56.3819132Z |
| 2 | 4625 | 2025-04-25T16:09:04.4046272Z |
| 3 | 4625 | 2025-04-25T16:09:09.2874733Z |

Raw JSON Events

```
[
  {
    "Event": {
      "System": {
        "EventID": "4625",
        "EventRecordID": "119110",
        "Channel": "Security",
        "Computer": "box",
        "TimeCreated": "2025-04-25T16:08:56.3819132Z",
        "ActivityID": "{fa23ec0f-aa26-0002-02ed-23fa26aadb01}",
        "ProcessID": "1592",
        "ThreadID": "25284"
      },
      "EventData": {
        "SubjectUserSid": "S-1-0-0",
        "SubjectUserName": "-",
        "SubjectDomainName": "-",
        "TargetUserName": "test",
        "TargetDomainName": "-",
        "LogonType": "3",
        "WorkstationName": "-",
        "ProcessName": "-",
        "IpAddress": "192.168.1.125"
      }
    }
  },
  {
    "Event": {
      "System": {
        "EventID": "4625",
        "EventRecordID": "119111",
        "Channel": "Security",
        "Computer": "box",
        "TimeCreated": "2025-04-25T16:09:04.4046272Z",
        "ActivityID": "{fa23ec0f-aa26-0002-02ed-23fa26aadb01}",
        "ProcessID": "1592",
        "ThreadID": "25284"
      },
      "EventData": {
        "SubjectUserSid": "S-1-0-0",
        "SubjectUserName": "-",
        "SubjectDomainName": "-",
        "TargetUserName": "test",
```

```
        "TargetDomainName": "-",
        "LogonType": "3",
        "WorkstationName": "-",
        "ProcessName": "-",
        "IpAddress": "192.168.1.125"
    }
},
{
    "Event": {
        "System": {
            "EventID": "4625",
            "EventRecordID": "119112",
            "Channel": "Security",
            "Computer": "box",
            "TimeCreated": "2025-04-25T16:09:09.2874733Z",
            "ActivityID": "{fa23ec0f-aa26-0002-02ed-23fa26aadb01}",
            "ProcessID": "1592",
            "ThreadID": "25284"
        },
        "EventData": {
            "SubjectUserSid": "S-1-0-0",
            "SubjectUserName": "-",
            "SubjectDomainName": "-",
            "TargetUserName": "test",
            "TargetDomainName": "-",
            "LogonType": "3",
            "WorkstationName": "-",
            "ProcessName": "-",
            "IpAddress": "192.168.1.125"
        }
    }
}
}
```