**BRUTEFORCE RUN BOOK**

**L1**:

**Step 1**:

Assigned alert

|  |  |  |
| --- | --- | --- |
| 1 | Read Details | Open ID>Read details |

**Step 2**:

|  |  |  |  |
| --- | --- | --- | --- |
| 1 | The reason for login failure. | “Splunk”  index="\*" sourcetype="WinEventLog:Security'' EventCode=4625 | |
| 2 | Status Code and Sub-status code. | Windows security login event | |
| 3 | Log – on type. | * If 2 close ticket * If 3 & 10 continue | 2 - Interactive  3 - Network  10 - Remote Interactive |
| 4 | Check if there is a process involved in failed login attempt |  | |
| 5 | Check If the user is Admin or no  Weather user has got successful login or no | index="\*" sourcetype="WinEventLog: Security'' EventCode=4624 | |

Analyse Logs

**Step 3**:

Analyse the Source IP attempting to log in to our network

|  |  |  |
| --- | --- | --- |
| 1 | Check the reputation of IP in TI tools | Whoislookup, IP Void, Virus Total |
| 2 | Check the country to which the Ip belongs | Whoislookup |

**L2**:

**Step 4**:

Analyse the evidence submitted by L1.

**Step 5:**

Raise the incident to AD team or IAM team on high priority

|  |  |  |
| --- | --- | --- |
| 1 | To disable the account temporarily & terminate all the existing session if attacker has established connection | Service now |

**Step 6**:

Resetting the password change it to complex one

**Step 7:**

Enable the disabled account

**Step 8:**

Cc with user manager send a mail to user to reset the password

**Step 9:**

Block the IP on firewall by raising the INCIDENT to NOC team

**Step 10:**

Close the Incident