# Behavior Chain Report (ReportV2 - Full Chain Restorability)

## Report Metadata

| Field | Value |
|---|---|
| **Report ID** | `7f8a9b2c3d4e5f6a7b8c9d0e1f2a3b4c5d6e7f8a9b0c1d2e3f4a5b6c7d8e9f0a` |
| **Chain ID** | `chain-ent-usr123-win24h-1706086400000` |
| **Revision** | 2 |
| **Report Version** | **v2** (Full Chain Restorability) |

---

## Timeline (12 Nodes: 8 BCP + 2 BSP + 2 BF)

### Phase 1: SSH Brute Force Attack (seq 0-6)

#### Seq 0: BCP (Behavior Coordinate Point)

| Field | Value |
|---|---|
| Type | **BCP** |
| Timestamp | 2023-01-23 06:00:00 UTC (1674453600000) |
| Log ID | 1001 |
| Event | SSH login failed (user: root, src: 203.0.113.50) |

### Seq 1: BCP

| Field | Value |
|---|---|
| Type | **BCP** |
| Timestamp | 2023-01-23 06:00:01 UTC (1674453601000) |
| Log ID | 1002 |
| Event | SSH login failed (user: root, src: 203.0.113.50) |

### Seq 2: BCP

| Field | Value |
|---|---|
| Type | **BCP** |
| Timestamp | 2023-01-23 06:00:02 UTC (1674453602000) |
| Log ID | 1003 |
| Event | SSH login failed (user: root, src: 203.0.113.50) |

### Seq 3: BCP

| Field | Value |
|---|---|
| Type | **BCP** |
| Timestamp | 2023-01-23 06:00:03 UTC (1674453603000) |
| Log ID | 1004 |
| Event | SSH login failed (user: root, src: 203.0.113.50) |

### Seq 4: BCP

| Field | Value |
|---|---|
| Type | **BCP** |
| Timestamp | 2023-01-23 06:00:04 UTC (1674453604000) |
| Log ID | 1005 |
| Event | SSH login failed (user: root, src: 203.0.113.50) |

### Seq 5: BSP (Behavior Success Point)

| Field | Value |
|---|---|
| Type | **BSP** |
| Timestamp | 2023-01-23 06:00:05 UTC (1674453605000) |
| Log ID | 1006 |
| Event | SSH login **SUCCESS** (user: root, src: 203.0.113.50) |

### Seq 6: BF (Behavior Fragment)

| Field | Value |
|---|---|
| Type | **BF** |
| BF ID | `bf-a1b2c3d4-e5f6-7890-1234-567890abcdef` |
| Time Range | 06:00:00 - 06:00:05 UTC (5 seconds) |
| **BFL** | **3 (HIGH)** |

**BFL Explain**:

| Factor | Value | Weight |
|---|---|---|
| action_id | AUTH | - |
| base_score | 10 | - |
| attempt_count | 5 | +10 |
| has_external_ip | true | +20 |
| time_window_seconds | 5 | +5 |
| **final_score** | **90** | - |

**MITRE ATT&CK Mapping**:

| Field | Value |
|---|---|
| bf_attack_family | **CREDENTIAL_ACCESS** |
| bf_attack_stage | **TA0006** |
| bf_attack_tags | `bruteforce`, `high_fail`, `mitre:T1110.001`, `external_source` |

**Bindings** (Chain Restorability):

| Binding | Value |
|---|---|
| member_bcp_log_ids | [1001, 1002, 1003, 1004, 1005] |
| derived_bpp_id | `bpp-e5f6-7890-1234-567890abcdef` |
| anchor_bsp_log_id | 1006 |

**BPP (Behavior Pivot Point)** - Embedded in BF:

| Field | Value |
| --- | --- |
| BPP ID | `bpp-e5f6-7890-1234-567890abcdef` |
| Anchor BSP Log ID | 1006 |
| **PTI** | **0.92** |
| Evidence Log IDs | [1001, 1002, 1003, 1004, 1005] |

**PTI Explain**:

| Factor | Value |
| --- | --- |
| base_score | 0.5 |
| failed_attempts_before_success | 5 |
| time_window_seconds | 5 |
| unique_source_ips | 1 |
| source_ip | 203.0.113.50 |
| target_user | root |
| is_external_ip | true |
| pti_raw | 0.85 |
| source_weight | 1.08 |
| **pti_final** | **0.92** |

---

## Phase 2: Privilege Escalation (seq 7-11)

### Seq 7: BCP

| Field | Value |
|---|---|
| Type | **BCP** |
| Timestamp | 2023-01-23 06:01:00 UTC (1674453660000) |
| Log ID | 2001 |
| Event | sudo command failed (user: root, cmd: sudo su -) |

### Seq 8: BCP

| Field | Value |
|---|---|
| Type | **BCP** |
| Timestamp | 2023-01-23 06:01:01 UTC (1674453661000) |
| Log ID | 2002 |
| Event | sudo command failed (user: root, cmd: sudo su -) |

### Seq 9: BCP

| Field | Value |
|---|---|
| Type | **BCP** |
| Timestamp | 2023-01-23 06:01:02 UTC (1674453662000) |
| Log ID | 2003 |
| Event | sudo command failed (user: root, cmd: sudo su -) |

### Seq 10: BSP

| Field | Value |
|---|---|
| Type | **BSP** |
| Timestamp | 2023-01-23 06:01:03 UTC (1674453663000) |
| Log ID | 2004 |
| Event | sudo command **SUCCESS** (user: root, cmd: sudo su -) |

### Seq 11: BF (Behavior Fragment)

| Field | Value |
|---|---|
| Type | **BF** |
| BF ID | `bf-b2c3d4e5-f6a7-8901-2345-67890abcdef0` |
| Time Range | 06:01:00 - 06:01:03 UTC (3 seconds) |
| **BFL** | **2 (MEDIUM)** |

**BFL Explain**:

| Factor | Value | Weight |
|---|---|---|
| action_id | PRIV_ESC | - |
| base_score | 30 | - |
| attempt_count | 3 | +5 |
| is_sudo | true | +20 |
| **final_score** | **65** | - |

**MITRE ATT&CK Mapping**:

| Field | Value |
|---|---|
| bf_attack_family | **PRIVILEGE_ESCALATION** |
| bf_attack_stage | **TA0004** |
| bf_attack_tags | `privilege_escalation`, `elevation`, `mitre:T1548` |

**Bindings** (Chain Restorability):

| Binding | Value |
|---|---|
| member_bcp_log_ids | [2001, 2002, 2003] |
| derived_bpp_id | `bpp-f6a7-8901-2345-67890abcdef0` |
| anchor_bsp_log_id | 2004 |

**BPP (Behavior Pivot Point)** - Embedded in BF:

| Field | Value |
|---|---|
| BPP ID | `bpp-f6a7-8901-2345-67890abcdef0` |
| Anchor BSP Log ID | 2004 |
| **PTI** | **0.78** |
| Evidence Log IDs | [2001, 2002, 2003] |

**PTI Explain**:

| Factor | Value |
|---|---|
| base_score | 0.4 |
| failed_attempts_before_success | 3 |
| time_window_seconds | 3 |
| is_sudo | true |
| command | sudo su - |
| is_privilege_escalation | true |
| pti_raw | 0.72 |
| source_weight | 1.08 |
| **pti_final** | **0.78** |

---

## Timeline Summary

| Seq | Type | Time | Key Info |
|---|---|---|---|
| 0 | BCP | 06:00:00 | SSH failed (log_id: 1001) |
| 1 | BCP | 06:00:01 | SSH failed (log_id: 1002) |
| 2 | BCP | 06:00:02 | SSH failed (log_id: 1003) |
| 3 | BCP | 06:00:03 | SSH failed (log_id: 1004) |
| 4 | BCP | 06:00:04 | SSH failed (log_id: 1005) |
| 5 | **BSP** | 06:00:05 | **SSH SUCCESS** (log_id: 1006) |
| 6 | **BF** | 06:00:00-05 | **BFL=3, PTI=0.92** (CREDENTIAL_ACCESS) |
| 7 | BCP | 06:01:00 | sudo failed (log_id: 2001) |
| 8 | BCP | 06:01:01 | sudo failed (log_id: 2002) |
| 9 | BCP | 06:01:02 | sudo failed (log_id: 2003) |
| 10 | **BSP** | 06:01:03 | **sudo SUCCESS** (log_id: 2004) |
| 11 | **BF** | 06:01:00-03 | **BFL=2, PTI=0.78** (PRIVILEGE_ESCALATION) |

---

## MITRE ATT&CK Mapping Summary

| BF | Attack Family | Tactic | Technique |
|---|---|---|---|
| bf-a1b2… | CREDENTIAL_ACCESS | TA0006 (Credential Access) | T1110.001 (Brute Force: Password Guessing) |
| bf-b2c3… | PRIVILEGE_ESCALATION | TA0004 (Privilege Escalation) | T1548 (Abuse Elevation Control Mechanism) |

---

# Report Structure Reference (ReportV2)

This report follows the `ReportV2` structure defined in `internal/contract/report_v2_types.go`:

```
// KEY SEMANTIC CONSTRAINTS:
// 1. Chain nodes are ONLY: BCP, BSP, BF
// 2. BPP is NOT a chain node - it is a BF derivation/explanation
// 3. PTI only exists in BPP, never in BF
// 4. BF must have explicit bindings to its BCP/BSP/BPP components

type ReportV2 struct {
    ReportID      string          `json:"report_id"`
    ChainID       string          `json:"chain_id"`
    Revision      int             `json:"revision"`
    ReportVersion ReportVersion   `json:"report_version"`  // "v2"
    Timeline      []ReportNodeV2  `json:"timeline"`        // BCP + BSP + BF
}

type ReportNodeV2 struct {
    Seq      int           `json:"seq"`
    Type     ChainNodeType `json:"type"`      // "BCP" | "BSP" | "BF"
    TStartMs int64         `json:"t_start_ms"`
    TEndMs   int64         `json:"t_end_ms"`
    Ref      map[string]interface{} `json:"ref"`
    BF       *BFViewV2     `json:"bf,omitempty"`  // Only for BF nodes
}

type BFViewV2 struct {
    BFID       string                 `json:"bf_id"`
    BFL        int                    `json:"bfl"`
    BFLExplain map[string]interface{} `json:"bfl_explain,omitempty"`
    Bindings   BFBindingsV2           `json:"bindings"`
    BPPs       []BPPViewV2            `json:"bpps,omitempty"`  // BPP
embedded in BF
}

type BPPViewV2 struct {
    BPPID          string                 `json:"bpp_id"`
    AnchorBSPLogID int64                  `json:"anchor_bsp_log_id"`
    PTI            float64                `json:"pti"`           // PTI
belongs to BPP
    PTIExplain     map[string]interface{} `json:"pti_explain,omitempty"`
    EvidenceLogIDs []int64
`json:"evidence_log_ids,omitempty"`
}
```

**Report Generated by**: ChainForge Security Analysis System v2.0.3
**Report Schema**: ReportV2 (Full Chain Restorability)
**Classification**: CONFIDENTIAL - Internal Use Only