==========

INVESTIGATION STEPS LOG - INC-2025-001

Timestamp Format: 2025-11-19

Investigator: Mr_Chandan_Prasad

==========

Timestamp	Action	Duration	Status
16:02:50 UTC	Alert received from Wazuh	1 min	✓ Complete
16:03:00 UTC	Logged into Wazuh Dashboard	2 min	✓ Complete
16:05:00 UTC	Verified Event ID 4672 in Event Log	3 min	✓ Complete
16:08:00 UTC	Identified affected system: MR-CHANDAN	5 min	✓ Complete
16:10:00 UTC	Extracted account names (IOCs)	4 min	✓ Complete
16:14:00 UTC	Extracted privilege names (9 total)	3 min	✓ Complete
16:17:00 UTC	Searched for related events (4624,4738)	5 min	✓ Complete
16:22:00 UTC	Checked for lateral movement evidence	8 min	✓ Complete
16:30:00 UTC	Revoked unauthorized privileges	5 min	✓ Complete
16:35:00 UTC	Disabled user account "mrhac"	3 min	✓ Complete
16:38:00 UTC	Isolated workstation from network	4 min	✓ Complete
16:42:00 UTC	Initiated memory dump collection	10 min	✓ Complete
16:52:00 UTC	Created forensic disk image	15 min	⧖ In Progress
17:07:00 UTC	Hashed evidence (SHA256)	5 min	⧖ In Progress
17:12:00 UTC	Documented chain of custody	3 min	⧖ In Progress
17:15:00 UTC	Drafted escalation email to Tier 2	5 min	✓ Complete
17:20:00 UTC	Reviewed incident timeline	10 min	✓ Complete

| 17:30:00 UTC | Cross-referenced with threat intel | 8 min | ✓ Complete|

| 17:38:00 UTC | Created incident ticket documentation | 5 min | ✓ Complete|

| 17:43:00 UTC | Sent escalation to Tier 2 team | 2 min | ✓ Complete|

==========

DETAILED ACTION LOG

==========

ACTION 1: Alert Received from Wazuh

Time: 16:02:50 UTC

Duration: 1 minute

What: Wazuh alert ID 003 received

Evidence: High severity alert - Special privileges assigned

Status: ✓ VERIFIED AS LEGITIMATE

Details: Event ID 4672 confirmed in Windows logs

ACTION 2: Logged into Wazuh Dashboard

Time: 16:03:00 UTC

Duration: 2 minutes

What: Accessed Wazuh Dashboard via https://127.0.0.1

System: MR-CHANDAN-PRAS workstation

Status: ✓ ACCESSED SUCCESSFULLY

Details: Dashboard showed real-time alert information

ACTION 3: Verified Event ID 4672

Time: 16:05:00 UTC

Duration: 3 minutes

What: Checked Windows Security Event Log directly

Evidence: Event ID 4672 (Special Privileges Assigned)

Status: ✓ CONFIRMED - Authentic security event

Details: Timestamp: 2025-11-19T16:02:42Z

Matched Wazuh alert exactly

ACTION 4: Identified Affected System

Time: 16:08:00 UTC

Duration: 5 minutes

What: Determined scope of incident

System: Windows Workstation - MR-CHANDAN-PRAS

Agent: Mr-Chandan-Prasad-indian (Agent ID: 001)

Status: ✓ SINGLE SYSTEM AFFECTED

Details: No other systems showing similar events

ACTION 5: Extracted Account Names (IOCs)

Time: 16:10:00 UTC

Duration: 4 minutes

What: Collected all user account indicators

Accounts:

- mrhacker.indian@outlook.com
- mrhac
- MR-CHANDAN-PRAS$
- SYSTEM
- administrator (failed login)

Status: ✓ IOCs COLLECTED

Details: All accounts documented and saved

ACTION 6: Extracted Privilege Names

Time: 16:14:00 UTC

Duration: 3 minutes

What: Listed all assigned privileges

Count: 9 dangerous privileges

Privileges:

1. SeSecurityPrivilege
2. SeTakeOwnershipPrivilege

3. SeLoadDriverPrivilege (DANGEROUS)
4. SeBackupPrivilege
5. SeRestorePrivilege
6. SeDebugPrivilege (DANGEROUS)
7. SeSystemEnvironmentPrivilege
8. SeImpersonatePrivilege (DANGEROUS)
9. SeDelegateSessionUserImpersonatePrivilege

Status: ✓ PRIVILEGES DOCUMENTED

Details: Shared with Tier 2 team

ACTION 7: Searched for Related Events

Time: 16:17:00 UTC

Duration: 5 minutes

What: Found correlated Windows events

Events Found:

- Event ID 4738 (Account modification)
- Event ID 4624 (Successful logon)
- Event ID 4634 (Account logoff)
- Event ID 4625 (Failed logon)

Status: ✓ TIMELINE CREATED

Details: All events timestamped and sequenced

ACTION 8: Checked for Lateral Movement

Time: 16:22:00 UTC

Duration: 8 minutes

What: Searched for evidence of spread to other systems

Systems: Scanned all agents, checked all event logs

Result: ✓ NO LATERAL MOVEMENT DETECTED

Details: Incident appears contained to single workstation

ACTION 9: Revoked Unauthorized Privileges

Time: 16:30:00 UTC

Duration: 5 minutes

What: Removed all dangerous privileges

Accounts: mrhacker.indian@outlook.com

Method: Windows Group Policy / System configuration

Status: ✓ PRIVILEGES REVOKED

Details: Privileges removed immediately, verified removal

ACTION 10: Disabled User Account

Time: 16:35:00 UTC

Duration: 3 minutes

What: Disabled compromised account

Account: mrhac

Method: Active Directory disable

Status: ✓ ACCOUNT DISABLED

Details: Account locked pending investigation completion

ACTION 11: Isolated Workstation

Time: 16:38:00 UTC

Duration: 4 minutes

What: Disconnected system from network

System: MR-CHANDAN-PRAS

Method: Unplugged network cable, disabled WiFi

Status: ✓ ISOLATED

Details: No network communication possible

Prevention: Prevents lateral movement, data exfiltration

ACTION 12: Initiated Memory Dump

Time: 16:42:00 UTC

Duration: 10 minutes

What: Collected system RAM snapshot

Size: 8 GB (System total memory)

Method: Using Velociraptor/forensic tools

Status: ⧖ IN PROGRESS

Details: Preserving volatile data before system shutdown

ACTION 13: Created Forensic Disk Image

Time: 16:52:00 UTC

Duration: 15 minutes

What: Bit-by-bit copy of hard drive

Size: ~100 GB

Method: Write-blocked forensic imaging

Status: ⧖ IN PROGRESS

Details: Preserving all data for analysis

ACTION 14: Hashed Evidence (SHA256)

Time: 17:07:00 UTC

Duration: 5 minutes

What: Calculated SHA256 hashes of evidence

Evidence: Memory dump, disk image, event logs

Status: ⧖ IN PROGRESS

Details: Documenting evidence integrity

ACTION 15: Documented Chain of Custody

Time: 17:12:00 UTC

Duration: 3 minutes

What: Created evidence handling record

Details: Who collected, when, where stored, transfers

Status: ⧖ IN PROGRESS

Details: Maintaining evidence integrity for legal proceedings

ACTION 16: Drafted Escalation Email

Time: 17:15:00 UTC

Duration: 5 minutes

What: Wrote escalation message to Tier 2

Content: Incident summary, IOCs, timeline, recommendations

Status: ✓ COMPLETE

Details: Ready for sending to Tier 2 Security Team

ACTION 17: Reviewed Incident Timeline

Time: 17:20:00 UTC

Duration: 10 minutes

What: Compiled chronological sequence of events

Events: 9 major events documented

Status: ✓ COMPLETE

Details: Clear incident progression established

ACTION 18: Cross-Referenced with Threat Intel

Time: 17:30:00 UTC

Duration: 8 minutes

What: Compared pattern with known attack techniques

Database: MITRE ATT&CK T1484 (Domain Policy Modification)

Result: ✓ MATCH FOUND - Known attack pattern

Status: ✓ COMPLETE

Details: Confirms deliberate privilege escalation attack

ACTION 19: Created Incident Ticket Documentation

Time: 17:38:00 UTC

Duration: 5 minutes

What: Documented all findings in official ticket

Ticket ID: INC-2025-001

Details: Executive summary, IOCs, timeline, analysis

Status: ✓ COMPLETE

Details: Ready for management review

ACTION 20: Sent Escalation to Tier 2 Team

Time: 17:43:00 UTC

Duration: 2 minutes

What: Emailed escalation message to Tier 2

To: tier2-security@company.com

Content: High-priority incident requiring expert analysis

Status: ✓ SENT

Details: Awaiting Tier 2 response and involvement

==========

INVESTIGATION SUMMARY

==========

Total Actions: 20

Completed: 14 (70%)

In Progress: 5 (25%)

Pending: 1 (5%)

Duration: ~1 hour 45 minutes (16:02 - 17:43 UTC)

Efficiency: Rapid response achieved

Evidence Collected: ✓ YES

Chain of Custody: ✓ MAINTAINED

Escalation: ✓ COMPLETED

Next Steps: Await Tier 2 investigation and remediation

==========