**🔍 Incident Response Interview & Analysis Workbook**

**(Tool-Focused: Metasploit & Mimikatz)**

**📰1. Incident Response Field Interview Questions**

| **No.** | **Question** | **What to Write Down** | **Why Important** |
| --- | --- | --- | --- |
| 1 | Who used the tool? | Name, date, time | Know who did the test |
| 2 | Which tool? | Metasploit / Mimikatz | Which tool was used |
| 3 | What system was tested? | IP, hostname, Windows/Linux | Track target system |
| 4 | What attack method? | Exploit name or module used | Understand how attack worked |
| 5 | What happened? | Shell opened? Password dumped? | Check success |
| 6 | Any passwords found? | Username + password/hash | Proof of impact |
| 7 | Was it detected? | Did antivirus give alert? | Know if defense worked |
| 8 | What logs were created? | System logs, AV logs | For forensic trail |
| 9 | Was backdoor left? | Registry key, service added | Check persistence |
| 10 | Any suspicious connection? | Port used, IP address | For C2 or data leak check |

🧾 2. Example Notes Spreadsheet

| **Field** | **Example Data** |
| --- | --- |
| Used Tool | Metasploit |
| Target System | 192.168.1.105 |
| Exploit | EternalBlue (ms17\_010) |
| Result | Shell opened successfully |
| Payload | reverse\_tcp |
| Credentials Found | admin / NTLM hash |
| Antivirus Alert | No |
| Logs | Windows Security Log |
| Persistence? | Yes (Service backdoor.exe) |
| Analyst | Zeenat, Intern |

🔍 3. What Logs to Check

| **Source** | **What to Check** |
| --- | --- |
| Windows Logs | Login (Event 4624), Program start (4688) |
| Antivirus | Any block or alert |
| Sysmon (if running) | Process creation, network traffic |
| Firewall | Reverse shell port (like 4444) |
| SIEM | Alerts about suspicious tools |

**🔧 4. What to Investigate (By Tool)**

**💣 Metasploit**

* **Shell Opened**: Use sessions -i 1
* **Privilege Escalation**: Use getsystem
* **Files Dropped**: Check C:\Temp or AppData
* **Backdoors**: Look in registry Run key
* **Network Activity**: netstat or Wireshark

**🔐 Mimikatz**

* **Credential Dumping**: Run sekurlsa::logonpasswords
* **Hashes Found**: Save hash (proof of success)
* **Registry Access**: Was lsass.exe read?
* **Log Entries**: Check Event Viewer if access denied logs exist
* **Antivirus Response**: See if Mimikatz was blocked

🧪 5. Tools You Can Use

| **Tool** | **Use** |
| --- | --- |
| Metasploit | Exploits + Payloads |
| Mimikatz | Dumping passwords |
| Event Viewer | View system logs |
| Wireshark | View reverse shell traffic |
| Volatility | Check memory (advanced) |
| Process Explorer | Check running processes |
| Tcpview | Open connections |
| Autoruns | Startup items and backdoors |

**6. Sample Investigation Checklist ✅**

* Confirmed test authorization and scope
* Executed controlled Metasploit exploit (MS17-010)
* Obtained shell and escalated privileges
* Deployed Mimikatz to dump credentials
* Identified logs and memory traces
* Reviewed Windows Registry and Prefetch
* Verified if any AV was triggered
* Documented artifacts and hashes
* Screenshot all steps (10 screenshots ready)
* Report prepared with forensic and operational notes