# Module 7 – Malware Threats: Practical Tools Cheat Sheet

## 1. Malware Analysis & Detection

|  |  |  |
| --- | --- | --- |
| Tool | Description | Usage / Commands |
| VirusTotal | Online service to scan files & URLs against multiple antivirus engines. | Upload via web UI or use API: virustotal --file sample.exe |
| Hybrid Analysis | Cloud malware analysis sandbox. | Upload suspicious files; review behavior report. |
| Cuckoo Sandbox | Open-source automated malware analysis system. | cuckoo submit sample.exe |
| YARA | Pattern-matching tool to identify malware families. | yara rule.yar sample.exe |
| PEiD | Detects packers, cryptors, and compilers in PE files. | Run GUI → Load file. |
| Sysinternals Process Explorer | Advanced Task Manager to inspect processes and DLLs. | Run procexp.exe → Check suspicious processes. |
| Sysinternals Autoruns | Shows programs configured to run at system startup. | autoruns.exe |

## 2. Memory Forensics

|  |  |  |
| --- | --- | --- |
| Tool | Description | Usage / Commands |
| Volatility | Memory forensics framework for analyzing RAM dumps. | volatility -f memdump.raw pslist |
| FTK Imager | Acquires forensic disk/memory images. | GUI → Create memory dump. |
| Redline | Memory and file analysis tool from FireEye. | Import memory image → Scan indicators. |

## 3. Reverse Engineering

|  |  |  |
| --- | --- | --- |
| Tool | Description | Usage / Commands |
| IDA Free | Interactive disassembler for binary analysis. | Open file → Analyze disassembly. |
| Ghidra | NSA's reverse engineering framework. | Import file → Use Code Browser. |
| x64dbg | Debugger for Windows executables. | Open binary → Set breakpoints. |

## 4. RATs (Remote Access Trojans) – Offensive Research

⚠️ For lab use only in isolated VMs

|  |  |  |
| --- | --- | --- |
| Tool | Description | Usage / Commands |
| NJRat | Popular RAT used for remote control over infected machines. | Run builder → Set IP & port → Generate client. |
| TheefRat | RAT with remote keylogging, screenshot, and file control features. | Run builder → Configure payload & listener. |
| QuasarRAT | Open-source remote administration tool. | Quasar.exe → Create server & client. |

## 5. Network Monitoring & Traffic Analysis

|  |  |  |
| --- | --- | --- |
| Tool | Description | Usage / Commands |
| Wireshark | Network packet analyzer to detect malicious traffic. | wireshark → Capture interface traffic. |
| Tcpdump | CLI packet capture tool. | tcpdump -i eth0 |
| Netstat | View active connections & ports. | netstat -ano |

## 6. Anti-Forensics & Evasion Testing

|  |  |  |
| --- | --- | --- |
| Tool | Description | Usage / Commands |
| Mimikatz | Extracts plaintext passwords from memory (lab use). | mimikatz.exe privilege::debug sekurlsa::logonpasswords |
| Veil Framework | Payload obfuscation tool to evade antivirus. | veil → Generate payload. |
| Shellter | Injects shellcode into Windows executables. | shellter |