Cyber Analysis Domain	Cyber Tool	Tool Description
Reverse Engineering (Firmware)	BinWalk	Firmware analysis tool Tool Type: Firmware Analysis Download: https://github.com/ReFirmLabs/binwalk
Reverse Engineering (Firmware)	QEMU	Emulation and virtualization tool Tool Type: Emulation and Virtualization Download: https://www.qemu.org/download/
Reverse Engineering (Firmware)	FAT-ng	Firmware analysis toolkit Tool Type: Firmware Analysis Download: https://github.com/attify/firmware-analysis-toolkit
Reverse Engineering (Firmware)	Firmwalker	Firmware analysis script Tool Type: Firmware Analysis Download: https://github.com/craigz28/firmwalker
Malware Analysis	PE Studio	PE file analysis tool Tool Type: PE File Analysis Download: https://www.winitor.com/
Malware Analysis	QEMU	Emulation and virtualization tool Tool Type: Emulation and Virtualization Download: https://www.qemu.org/download/
Malware Analysis	Cuckoo Sandbox	Automated malware analysis sandbox Tool Type: Malware Analysis Sandbox Download: https://cuckoosandbox.org/
Malware Analysis	Process Monitor (ProcMon)	System monitoring tool Tool Type: System Monitoring Download: https://docs.microsoft.com/en-us/sysinternals/downloads/procmon
Malware Analysis	OllyDbg	Debugger for Windows binaries Tool Type: Debugger Download: http://www.ollydbg.de/
Malware Analysis	Fakenet-ng	Network simulation tool Tool Type: Network Simulation Download: https://github.com/fireeye/flare-fakenet-ng
Malware Analysis	PEiD	Packing detection tool Tool Type: Packing Detection Download: https://www.aldeid.com/wiki/PEiD
Malware Analysis	Detect It Easy (DIE)	Packing detection tool Tool Type: Packing Detection Download: https://github.com/horsicq/Detect-It-Easy
Malware Analysis	oletools	Malicious document analysis tool Tool Type: Maldoc Analysis Download: https://github.com/decalage2/oletools
Malware Analysis	olevba	VBA macro analysis tool Tool Type: Maldoc Analysis Download: https://github.com/decalage2/oletools/wiki/olevba
Malware Analysis	XLMMacroDeobfuscator	Excel 4.0 macro deobfuscator Tool Type: Maldoc Analysis Download: https://github.com/DissectMalware/XLMMacroDeobfuscator
Malware Analysis	Yara	Pattern matching tool Tool Type: Malware Analysis Download: https://github.com/VirusTotal/yara

Malware Analysis	signsrch	Signature-based malware detection tool Tool Type: Malware Analysis Download: https://github.com/sherpya/signsrch
Software Exploitation Analysis	OllyDbg	Debugger for Windows binaries Tool Type: Debugger Download: http://www.ollydbg.de/
Software Exploitation Analysis	x64dbg	Debugger for Windows binaries Tool Type: Debugger Download: https://x64dbg.com/
Software Exploitation Analysis	WinDbg	Debugger for Windows binaries Tool Type: Debugger Download: https://docs.microsoft.com/en-us/windows-hardware/drivers/debugger/debugger-download-tools
Software Exploitation Analysis	GDB (GNU Debugger)	Debugger for Unix-based systems Tool Type: Debugger Download: https://www.gnu.org/software/gdb/
Software Exploitation Analysis	Metasploit	Exploitation framework Tool Type: Exploitation Framework Download: https://www.metasploit.com/
Common Analysis Tools	Data Duplicator (DD command)	Data duplication and imaging tool Tool Type: Data Duplication Built-in tool in Unix-based systems
Common Analysis Tools	File command	File type identification tool Tool Type: File Type Identification Built-in tool in Unix-based systems
Common Analysis Tools	Strings command	String extraction tool Tool Type: String Extraction Built-in tool in Unix-based systems
Common Analysis Tools	IDA Pro	Disassembler and debugger Tool Type: Disassembler and Decompiler Download: https://www.hex-rays.com/products/ida/
Common Analysis Tools	Ghidra	Reverse engineering tool Tool Type: Disassembler and Decompiler Download: https://ghidra-sre.org/
Common Analysis Tools	Wireshark	Network protocol analyzer Tool Type: Network Analysis Download: https://www.wireshark.org/
Common Analysis Tools	Burp Suite	Web application security testing tool Tool Type: Web Application Security Download: https://portswigger.net/burp
Online Analysis Tools	Joe Sandbox	Automated malware analysis platform Tool Type: Malware Analysis Access: https://www.joesecurity.org/
Online Analysis Tools	Any.Run	Interactive malware analysis platform Tool Type: Malware Analysis Access: https://any.run/
Online Analysis Tools	Hybrid Analysis	Malware analysis and threat intelligence platform Tool Type: Malware Analysis Access: https://www.hybrid-analysis.com/
Online Analysis Tools	URLhaus	Malicious URL database Tool Type: Threat Intelligence Access: https://urlhaus.abuse.ch/

Online Analysis Tools	CyberChef	Web-based data transformation tool Tool Type: Data Transformation Access: https://gchq.github.io/CyberChef/
Online Analysis Tools	VirusTotal	Online malware analysis and threat intelligence platform Tool Type: Malware Analysis Access: https://www.virustotal.com/
Analysis Platforms	Radare2	Reverse engineering framework Tool Type: Reverse Engineering Download: https://rada.re/n/radare2.html
Analysis Platforms	FLARE VM	Reverse engineering and malware analysis framework Tool Type: Malware Analysis Download: https://github.com/fireeye/flare-vm
Analysis Platforms	Kali Linux	Linux distribution for security testing and analysis Tool Type: Security Testing Download: https://www.kali.org/
Analysis Platforms	REMnux	Linux distribution for reverse engineering and malware analysis Tool Type: Malware Analysis Download: https://remnux.org/
Analysis Platforms	Capa	Malware analysis framework Tool Type: Malware Analysis Download: https://github.com/fireeye/capa

Cyber Analysis Domain	Cyber Tool	Usage	File Type
Reverse Engineering (Firmware)	BinWalk	Extracts firmware components	Firmware
Reverse Engineering (Firmware)	QEMU	Emulates firmware environment	Firmware
Reverse Engineering (Firmware)	FAT-ng	Automates firmware analysis tasks	Firmware
Reverse Engineering (Firmware)	Firmwalker	Searches for interesting files and patterns	Firmware
Malware Analysis	PE Studio	Analyzes PE file structure and properties	PE
Malware Analysis	QEMU	Emulates malware environment	PE, ELF, Mach-O
Malware Analysis	Cuckoo Sandbox	Analyzes malware behavior in a controlled environment	PE, ELF, Mach-O

Malware Analysis	Process Monitor (ProcMon)	Monitors system activities and process behavior	PE
Malware Analysis	OllyDbg	Debugs and analyzes malware at the assembly level	PE
Malware Analysis	Fakenet-ng	Simulates network services and Internet connectivity	N/A
Malware Analysis	PEiD	Detects common packers, cryptors, and compilers	PE
Malware Analysis	Detect It Easy (DIE)	Detects packers, cryptors, and compilers	PE, ELF, Mach-O
Malware Analysis	oletools	Analyzes and extracts information from Microsoft Office files	Office Documents
Malware Analysis	olevba	Extracts and analyzes VBA macros from Office documents	Office Documents
Malware Analysis	XLMMacroDeobfuscator	Deobfuscates and analyzes Excel 4.0 macros	Excel Documents
Malware Analysis	Yara	Defines and matches patterns in malware samples	PE, ELF, Mach-O
Malware Analysis	signsrch	Searches for specific byte sequences in files	PE, ELF, Mach-O
Software Exploitation Analysis	OllyDbg	Debugs and analyzes software at the assembly level	PE
Software Exploitation Analysis	x64dbg	Debugs and analyzes software at the assembly level	PE
Software Exploitation Analysis	WinDbg	Debugs and analyzes software at the assembly level	PE
Software Exploitation Analysis	GDB (GNU Debugger)	Debugs and analyzes software at the assembly level	ELF
Software Exploitation Analysis	Metasploit	Develops and executes exploits against vulnerable systems	N/A
Common Analysis Tools	Data Duplicator (DD command)	Creates forensic disk images	N/A

Common Analysis Tools	File command	Identifies file types based on file signatures	N/A
Common Analysis Tools	Strings command	Extracts printable strings from files	N/A
Common Analysis Tools	IDA Pro	Disassembles and analyzes binary code	PE, ELF, Mach-O
Common Analysis Tools	Ghidra	Disassembles and analyzes binary code	PE, ELF, Mach-O
Common Analysis Tools	Wireshark	Captures and analyzes network traffic	PCAP
Common Analysis Tools	Burp Suite	Analyzes and tests web application security	N/A
Online Analysis Tools	Joe Sandbox	Analyzes malware behavior in a cloud environment	PE, ELF, Mach-O
Online Analysis Tools	Any.Run	Analyzes malware behavior in a web-based environment	PE, ELF, Mach-O
Online Analysis Tools	Hybrid Analysis	Analyzes malware and provides threat intelligence	PE, ELF, Mach-O
Online Analysis Tools	URLhaus	Provides information on malicious URLs	N/A
Online Analysis Tools	CyberChef	Performs various data transformations and analyses	N/A
Online Analysis Tools	VirusTotal	Analyzes malware samples and provides threat intelligence	PE, ELF, Mach-O
Analysis Platforms	Radare2	Disassembles, analyzes, and debugs binary code	PE, ELF, Mach-O
Analysis Platforms	FLARE VM	Provides tools and scripts for malware analysis	PE, ELF, Mach-O
Analysis Platforms	Kali Linux	Provides a wide range of security tools	N/A
Analysis Platforms	REMnux	Provides tools and scripts for malware analysis	PE, ELF, Mach-O
Analysis Platforms	Capa	Detects capabilities and behaviors in executable files	PE, ELF, Mach-O

Cyber Analysis Domain	Cyber Tool	Reason for Cyber Analysis to Use It
Reverse Engineering (Firmware)	BinWalk	Identify firmware structure and contents
Reverse Engineering (Firmware)	QEMU	Analyze firmware behavior in a controlled environment
Reverse Engineering (Firmware)	FAT-ng	Streamline firmware analysis process
Reverse Engineering (Firmware)	Firmwalker	Identify potential security issues and sensitive information
Malware Analysis	PE Studio	Understand PE file characteristics and potential malicious behavior
Malware Analysis	QEMU	Analyze malware behavior in a controlled environment
Malware Analysis	Cuckoo Sandbox	Understand malware functionality and interactions
Malware Analysis	Process Monitor (ProcMon)	Identify malware's interactions with the system
Malware Analysis	OllyDbg	Understand malware's low-level behavior and code execution
Malware Analysis	Fakenet-ng	Analyze malware's network communications and interactions
Malware Analysis	PEiD	Identify packed or obfuscated malware
Malware Analysis	Detect It Easy (DIE)	Identify packed or obfuscated malware
Malware Analysis	oletools	Identify malicious macros, scripts, and shellcode in Office documents
Malware Analysis	olevba	Identify malicious VBA macros in Office documents
Malware Analysis	XLMMacroDeobfuscator	Identify malicious Excel 4.0 macros
Malware Analysis	Yara	Identify and classify malware based on specific patterns
Malware Analysis	signsrch	Identify malware based on known signatures
Software Exploitation Analysis	OllyDbg	Understand software's low-level behavior and code execution
Software Exploitation Analysis	x64dbg	Understand software's low-level behavior and code execution
Software Exploitation Analysis	WinDbg	Understand software's low-level behavior and code execution

Software Exploitation Analysis	GDB (GNU Debugger)	Understand software's low-level behavior and code execution
Software Exploitation Analysis	Metasploit	Test software vulnerabilities and exploit them
Common Analysis Tools	Data Duplicator (DD command)	Preserve and analyze disk data
Common Analysis Tools	File command	Determine the file type and format
Common Analysis Tools	Strings command	Identify interesting strings and potential indicators
Common Analysis Tools	IDA Pro	Understand binary code structure and functionality
Common Analysis Tools	Ghidra	Understand binary code structure and functionality
Common Analysis Tools	Wireshark	Understand network communication and protocols
Common Analysis Tools	Burp Suite	Identify vulnerabilities and misconfigurations in web applications
Online Analysis Tools	Joe Sandbox	Understand malware functionality and interactions
Online Analysis Tools	Any.Run	Understand malware functionality and interactions
Online Analysis Tools	Hybrid Analysis	Understand malware characteristics and associated threats
Online Analysis Tools	URLhaus	Identify and investigate malicious URLs
Online Analysis Tools	CyberChef	Manipulate and analyze data
Online Analysis Tools	VirusTotal	Understand malware characteristics and associated threats
Analysis Platforms	Radare2	Understand binary code structure and functionality
Analysis Platforms	FLARE VM	Automate malware analysis tasks
Analysis Platforms	Kali Linux	Perform various security testing and analysis tasks
Analysis Platforms	REMnux	Analyze malware behavior and characteristics
Analysis Platforms	Capa	Identify malware capabilities and behaviors

Cyber Analysis Domain	Cyber Tool	Expected Outcome
Reverse Engineering (Firmware)	BinWalk	Understand firmware components and architecture
Reverse Engineering (Firmware)	QEMU	Observe firmware execution and interactions
Reverse Engineering (Firmware)	FAT-ng	Identify vulnerabilities and extract firmware components
Reverse Engineering (Firmware)	Firmwalker	Discover firmware vulnerabilities and misconfigurations
Malware Analysis	PE Studio	Identify suspicious PE file attributes and indicators
Malware Analysis	QEMU	Observe malware execution and interactions
Malware Analysis	Cuckoo Sandbox	Generate detailed malware analysis reports
Malware Analysis	Process Monitor (ProcMon)	Trace malware's actions and system modifications
Malware Analysis	OllyDbg	Identify malware's functionality and evasion techniques
Malware Analysis	Fakenet-ng	Identify malware's command and control (C2) servers and network indicators
Malware Analysis	PEiD	Determine the packing or obfuscation method used
Malware Analysis	Detect It Easy (DIE)	Determine the packing or obfuscation method used
Malware Analysis	oletools	Detect and extract suspicious content from Office files
Malware Analysis	olevba	Deobfuscate and understand the functionality of VBA macros
Malware Analysis	XLMMacroDeobfuscator	Understand the functionality of obfuscated Excel 4.0 macros
Malware Analysis	Yara	Detect malware variants and families
Malware Analysis	signsrch	Detect specific malware variants or families
Software Exploitation Analysis	OllyDbg	Identify vulnerabilities and exploit development opportunities
Software Exploitation Analysis	x64dbg	Identify vulnerabilities and exploit development opportunities

Software Exploitation Analysis	WinDbg	Identify vulnerabilities and exploit development opportunities
Software Exploitation Analysis	GDB (GNU Debugger)	Identify vulnerabilities and exploit development opportunities
Software Exploitation Analysis	Metasploit	Assess the impact and feasibility of exploits
Common Analysis Tools	Data Duplicator (DD command)	Create a forensic copy of the disk for analysis
Common Analysis Tools	File command	Identify file types for further analysis
Common Analysis Tools	Strings command	Extract relevant strings for analysis
Common Analysis Tools	IDA Pro	Identify interesting code segments and vulnerabilities
Common Analysis Tools	Ghidra	Identify interesting code segments and vulnerabilities
Common Analysis Tools	Wireshark	Identify suspicious network activities and indicators
Common Analysis Tools	Burp Suite	Perform manual and automated security testing of web applications
Online Analysis Tools	Joe Sandbox	Generate detailed malware analysis reports
Online Analysis Tools	Any.Run	Interact with malware execution and observe behavior
Online Analysis Tools	Hybrid Analysis	Obtain detailed malware analysis reports and threat intelligence
Online Analysis Tools	URLhaus	Obtain threat intelligence on malicious URLs
Online Analysis Tools	CyberChef	Decode, encrypt, compress, and perform various data operations
Online Analysis Tools	VirusTotal	Obtain malware analysis reports and threat intelligence
Analysis Platforms	Radare2	Identify interesting code segments and vulnerabilities
Analysis Platforms	FLARE VM	Identify malware characteristics and behavior
Analysis Platforms	Kali Linux	Conduct comprehensive security assessments and analyses
Analysis Platforms	REMnux	Perform in-depth malware analysis and reverse engineering
Analysis Platforms	Capa	Understand the functionality and intent of malware