

CYBERSECURITY

70+ Comprehensive Cybersecurity Tools for Modern Threat Defense by Category

[in/harunseker/](https://www.harunseker.com/in/harunseker/)

Information Gathering

1. Nmap
2. Shodan
3. Maltego
4. TheHarvester
5. Recon-NG
6. Amass
7. Censys
8. OSINT Framework
9. Gobuster
10. Spiderfoot

Wireless Hacking

1. Aircrack-NG
2. Wifite
3. Kismet
4. TCPDump
5. Reaver
6. Wireshark

Social Engineering

1. GoPhish
2. HiddenEye
3. SocialFish
4. EvilURL
5. Evilginx
6. SET
(Social-Engineering Toolkit)

Exploitation

1. Metasploit Framework
2. Burp Suite
3. SQL Map
4. ExploitDB
5. Core Impact
6. Cobalt Strike
7. Empire

Password Cracking

1. Hashcat
2. John the Ripper
3. Hydra
4. Medusa
5. Cain & Abel
6. Ophcrack

Vulnerability Scanning

1. Nessus
2. OpenVAS
3. Nexpose
4. Qualys
5. Acunetix
6. Lynis

Forensics

1. Wireshark
2. Autopsy
3. Volatility
4. SleuthKit
5. Binwalk
6. Foremost
7. EnCase

Web Application

Assessment

1. OWASP ZAP
2. Burp Suite
3. Nikto
4. WPScan
5. Acunetix
6. Arachni

Network Defense

1. Snort
2. Suricata
3. pfSense
4. Security Onion
5. AlienVault OSSIM

Endpoint Security

1. CrowdStrike Falcon
2. SentinelOne
3. Carbon Black
4. Symantec Endpoint Protection
5. Microsoft Defender for Endpoint

Cloud Security

1. AWS GuardDuty
2. Azure Security Center
3. Google Cloud Security Command Center
4. Prisma Cloud
5. Lacework

Threat Intelligence

1. ThreatConnect
2. Recorded Future
3. AlienVault OTX
4. IBM X-Force Exchange
5. MISP (Malware Information Sharing Platform)

No	Tool	Explanation	Example Usage	URLs
Information Gathering				
1	Nmap	Network scanning and discovery tool used to find open ports, services, and OS information	<code>nmap -sV 192.168.1.0/24</code> to scan a network for open ports and service versions	Nmap: https://nmap.org/
2	Shodan	Search engine for Internet-connected devices, allowing users to find specific types of devices, vulnerabilities, or services	Searching for " <code>webcamxp country:US</code> " to find exposed webcams in the United States	Shodan: https://www.shodan.io/
3	Maltego	Data mining and visual link analysis tool for investigating relationships between pieces of information	Creating a graph of an organization's online presence, including domains, email addresses, and social media accounts	Maltego: https://www.maltego.com/
4	TheHarvester	Tool for gathering email addresses, subdomains, hosts, and employee names from various public sources	<code>theHarvester -d example.com -b all</code> to gather information about a domain using all available data sources	TheHarvester: https://github.com/laramies/theHarvester
5	Recon-NG	Full-featured reconnaissance framework designed for web-based open source reconnaissance	Using the <code>whois_pocs</code> module to gather contact information for a target domain	Recon-NG: https://github.com/lanmaster53/recon-ng
6	Amass	Tool for in-depth DNS enumeration and network mapping	<code>amass enum -d example.com</code> to enumerate subdomains of a target domain	Amass: https://github.com/OWASP/Amass

7	Censys	Search engine that allows users to find specific types of devices connected to the internet	Searching for "80.http.get.headers.server: Apache" to find Apache web servers	Censys: https://search.censys.io/
8	OSINT Framework	Collection of various OSINT tools and resources categorized by function	Using the framework to find social media profiles associated with an email address	OSINT Framework: https://osintframework.com/
9	Gobuster	Tool used to brute-force URIs, DNS subdomains, and virtual host names	<code>gobuster dir -u http://example.com -w wordlist.txt</code> to find hidden directories on a website	Gobuster: https://github.com/OJ/gobuster
10	Spiderfoot	Automated OSINT framework that integrates with multiple data sources for gathering intelligence	Running a scan on a domain to automatically gather associated IP addresses, email addresses, and social media profiles	Spiderfoot: https://intel471.com/attack-surface-documentation

Wireless Hacking

1	Aircrack-NG	Suite of tools for auditing wireless networks, capable of cracking WEP and WPA/WPA2-PSK keys	<code>aircrack-ng -w wordlist.txt capture.cap</code> to crack a WPA handshake captured in capture.cap file	Aircrack-NG: https://www.aircrack-ng.org/
2	Wifite	Automated wireless attack tool that can crack multiple networks simultaneously	<code>wifite --dict wordlist.txt</code> to automatically attack nearby networks using a wordlist	Wifite: https://github.com/derv82/wifite2
3	Kismet	Wireless network detector, sniffer, and intrusion detection system	Running Kismet to passively detect hidden wireless networks and capture packets	Kismet: https://www.kismetwireless.net/

4	TCPDump	Command-line packet analyzer	<code>tcpdump -i wlan0 -w capture.pcap</code> to capture wireless traffic on wlan0 interface	TCPDump: https://www.tcpdump.org/
5	Reaver	Tool specifically designed to attack WPS (Wi-Fi Protected Setup) enabled wireless routers	<code>reaver -i wlan0 -b 00:11:22:33:44:55 -vv</code> to attempt a WPS PIN brute-force attack on a specific access point	Reaver: https://github.com/t6x/reaver-wps-fork-t6x
6	Wireshark	Network protocol analyzer with capabilities for wireless packet analysis	Using Wireshark to capture and analyze Wi-Fi traffic, including decrypting WPA2 traffic with the correct key	Wireshark: https://www.wireshark.org/
Social Engineering				
1	GoPhish	Open-source phishing toolkit for creating and managing phishing campaigns	Setting up a simulated phishing campaign to test employee awareness by sending fake login pages	GoPhish: https://getgophish.com/
2	HiddenEye	Advanced phishing tool with multiple attack vectors	Creating a fake login page for a popular social media platform to capture credentials	HiddenEye: https://github.com/DarkSecDevelopers/HiddenEye
3	SocialFish	Educational tool for social media phishing	Generating a clone of a social networking site to demonstrate how easily users can be tricked	SocialFish: https://github.com/UndeadSec/SocialFish
4	EvilURL	Tool for generating unicode domains for phishing attacks	Creating a domain like "apple.com" that looks like "apple.com" to fool users	EvilURL: https://github.com/UndeadSec/EvilURL

5	Evilginx	Man-in-the-middle attack framework for phishing login credentials and session cookies	Setting up a proxy to intercept login attempts to a target website, bypassing two-factor authentication	Evilginx: https://github.com/kgretzky/evilginx2
6	SET (Social-Engineering Toolkit)	Framework for creating and executing social engineering attacks	Using the "Spear-Phishing Attack Vector" to send targeted emails with malicious attachments to specific individuals	SET: https://github.com/trustedsec/social-engineer-toolkit

Exploitation

1	Metasploit Framework	Open-source penetration testing and exploitation framework	Using the <code>exploit/windows/smb/ms17_010_ternalblue</code> module to exploit the EternalBlue vulnerability	Metasploit Framework: https://www.metasploit.com/
2	Burp Suite	Web application security testing platform	Intercepting and modifying HTTP requests to test for SQL injection vulnerabilities	Burp Suite: https://portswigger.net/burp
3	SQL Map	Automated SQL injection and database takeover tool	<code>sqlmap -u "http://example.com/page.php?id=1" --dbs</code> to enumerate databases on a vulnerable website	SQL Map: https://sqlmap.org/
4	ExploitDB	Archive of public exploits and corresponding vulnerable software	Searching for "Apache Struts" to find known exploits for the Apache Struts framework	ExploitDB: https://www.exploit-db.com/
5	Core Impact	Commercial penetration testing software	Conducting a network scan and automatically exploiting discovered vulnerabilities	Core Impact: https://www.coresecurity.com/products/core-impact

6	Cobalt Strike	Adversary simulation and red team operations software	Using its beacon payload for post-exploitation activities and lateral movement	Cobalt Strike: https://www.cobaltstrike.com/
7	Empire	PowerShell and Python post-exploitation framework	Executing a PowerShell script on a compromised Windows machine for privilege escalation	Empire: https://github.com/BC-SECURITY/Empire
Password Cracking				
1	Hashcat	Advanced password recovery tool that supports hundreds of hashing algorithms	<code>hashcat -m 0 -a 0 hash.txt wordlist.txt</code> to crack MD5 hashes using a wordlist	Hashcat: https://hashcat.net/
2	John the Ripper	Versatile password cracker that combines multiple cracking modes	<code>john --format=raw-md5 hash.txt</code> to crack MD5 hashes using default settings	John The Ripper: https://www.openwall.com/john/
3	Hydra	Online password cracking tool for various network protocols and services	<code>hydra -l user -P pass.txt ftp://192.168.1.1</code> to brute force FTP login	Hydra: https://github.com/vanhauser-thc/thc-hydra
4	Medusa	Parallel network login brute-forcer supporting multiple protocols	<code>medusa -h 192.168.1.1 -u admin -P passwords.txt -M http</code> to attack HTTP basic auth	Medusa: http://foofus.net/goons/jmk/medusa/medusa.html
5	Cain & Abel	Windows-based password recovery tool with multiple functions	Using the GUI to capture and crack network passwords or dump hashes	Cain & Abel: http://www.oxid.it/cain.html
6	Ophcrack	Cross-platform tool specializing in Windows password cracking using rainbow tables	Loading a Windows SAM file and cracking passwords using pre-computed tables	Ophcrack: https://ophcrack.sourceforge.io/

Vulnerability Scanning

1	Nessus	Commercial vulnerability scanner with a large plugin database. Detects vulnerabilities, misconfigurations, and compliance issues.	Scanning a network for known vulnerabilities: <code>nessus scan -t 192.168.1.0/24</code>	Nessus: https://www.tenable.com/products/nessus
2	OpenVAS	Open-source vulnerability scanner and manager. Performs authenticated/unauthenticated testing and supports various protocols.	Running a full scan on a web server: <code>omp -u admin -w password --create-target="Web Server" --hosts=192.168.1.100 --create-task="Web Server Scan" --config="Full and fast" --start-task</code>	OpenVAS: https://www.openvas.org/
3	Nexpose	Commercial vulnerability management software. Provides risk-based prioritization and integration with Metasploit.	Creating a site and running a scan: <code>nexpose_cli.rb -r CreateSite -n "TestSite" -H 192.168.1.100 -S</code>	Nexpose: https://www.rapid7.com/products/nexpose/
4	Qualys	Cloud-based vulnerability management platform. Offers continuous monitoring and asset discovery.	Scheduling a weekly scan of critical assets through the Qualys web interface	Qualys: https://www.qualys.com/
5	Acunetix	Specialized web application security scanner. Detects over 7000 web vulnerabilities including XSS and SQL injection.	Scanning a web application: <code>acunetix_console --scan http://example.com</code>	Acunetix: https://www.acunetix.com/

6	Lynis	Open-source security auditing tool for Unix/Linux systems. Performs system hardening, compliance testing, and vulnerability scanning.	Running a system audit: <code>lynis audit system</code>	Lynis: https://cisofy.com/lynis/
Forensics				
1	Wireshark	Network protocol analyzer for capturing and analyzing network traffic	Capturing HTTP traffic to analyze a potential data exfiltration attempt: <code>wireshark -i eth0 -f "port 80"</code>	Wireshark: https://www.wireshark.org/
2	Autopsy	Digital forensics platform for disk image analysis	Analyzing a disk image to recover deleted files: <code>autopsy disk_image.dd</code>	Autopsy: https://www.autopsy.com/
3	Volatility	Memory forensics framework for analyzing RAM dumps	Extracting running processes from a memory dump: <code>volatility -f memory.dmp --profile=Win10x64 pslist</code>	Volatility: https://www.volatilityfoundation.org/
4	SleuthKit	Collection of command-line tools for investigating disk images	Extracting file system information: <code>fls -r disk_image.dd</code>	SleuthKit: https://www.sleuthkit.org/
5	Binwalk	Tool for analyzing and extracting firmware images	Identifying embedded files in firmware: <code>binwalk router_firmware.bin</code>	Binwalk: https://github.com/ReFirmLabs/binwalk
6	Foremost	Data carving tool for recovering files based on headers and footers	Recovering JPEGs from a disk image: <code>foremost -t jpeg -i disk_image.dd</code>	Foremost: http://foremost.sourceforge.net/

7	EnCase	Commercial forensic software suite for evidence acquisition and analysis	Creating a forensic image of a hard drive: <pre>encase -e /dev/sda evidence.E01</pre>	EnCase: https://www.guidancesoftware.com/encase-forensic
Web Application Assessment				
1	OWASP ZAP	Open-source web application security scanner. Performs automated scanning and allows manual testing.	Running an automated scan: <pre>zap-cli quick-scan --self-contained --start-options "-config api.disablekey=true" https://example.com</pre>	OWASP ZAP: https://www.zaproxy.org/
2	Burp Suite	Integrated platform for web application security testing. Includes tools for mapping, analyzing, and exploiting web applications.	Using Burp Proxy to intercept and modify HTTP requests: Configure browser to use Burp as proxy, then intercept and modify requests in Burp	Burp Suite: https://portswigger.net/burp
3	Nikto	Open-source web server scanner that performs comprehensive tests against web servers for multiple items.	Scanning a web server: <pre>nikto -h http://example.com</pre>	Nikto: https://cirt.net/Nikto2
4	WPScan	Black box WordPress vulnerability scanner.	Scanning a WordPress site: <pre>wpscan --url http://example.com --enumerate vp,u,tt,t</pre>	WPScan: https://wpscan.org/
5	Acunetix	Automated web application security testing tool. Detects over 7000 web vulnerabilities.	Scheduling a weekly scan of critical assets through the Acunetix web interface	Acunetix: https://www.acunetix.com/

6	Arachni	Web application security scanner framework.	Running a scan: <code>arachni http://example.com</code>	Arachni: https://www.arachni-scanner.com/
---	----------------	---	--	---

Network Defense

1	Snort	Open-source intrusion detection and prevention system (IDS/IPS) that performs real-time traffic analysis and packet logging	Configuring Snort rules to detect and alert on suspicious network traffic: alert tcp any any -> \$HOME_NET 22 (msg:"SSH brute force attempt"; flow:to_server; threshold:type both, track by_src, count 5, seconds 60; sid:1000001;)	Snort: https://www.snort.org/
2	Suricata	High-performance network IDS, IPS, and network security monitoring engine	Setting up Suricata to monitor network traffic and generate alerts: <code>suricata -c /etc/suricata/suricata.yaml -i eth0</code>	Suricata: https://suricata-ids.org/
3	pfSense	Open-source firewall and router platform based on FreeBSD	Configuring a pfSense firewall rule to allow inbound HTTPS traffic: <code>pass in on wan proto tcp from any to (wan) port 443</code>	pfSense: https://www.pfsense.org/
4	Security Onion	Linux distribution for intrusion detection, network security monitoring, and log management	Deploying Security Onion to collect and analyze network traffic: <code>sudo so-setup</code> to initiate the setup wizard	Security Onion: https://securityonion.net/
5	AlienVault OSSIM	Open-source security information and event management (SIEM) system	Using OSSIM to correlate security events from multiple sources: Configure log sources in the web interface and create correlation rules to detect complex attack patterns	AlienVault OSSIM: https://cybersecurity.att.com/products/ossim

Endpoint Security

1	CrowdStrike Falcon	Cloud-native endpoint protection platform using AI and behavioral analytics	Detecting and preventing a zero-day malware attack in real-time on an employee's laptop	CrowdStrike Falcon: https://www.crowdstrike.com/
2	SentinelOne	AI-powered endpoint security platform with autonomous response capabilities	Automatically isolating an infected workstation and rolling back malicious changes	SentinelOne: https://www.sentinelone.com/
3	Carbon Black	Endpoint detection and response (EDR) solution with threat hunting capabilities	Investigating the root cause of a security incident across multiple endpoints	Carbon Black: https://www.carbonblack.com/
4	Symantec Endpoint Protection	Traditional antivirus combined with advanced threat protection	Blocking a ransomware attack attempt on a corporate server	Symantec Endpoint Protection: https://www.broadcom.com/products/cyber-security/endpoint
5	Microsoft Defender for Endpoint	Built-in endpoint security for Windows with cloud-powered protection	Identifying and remediating a vulnerability across all Windows devices in an organization	Microsoft Defender for Endpoint: https://www.microsoft.com/en-us/microsoft-365/security/endpoint-defender

Cloud Security

1	AWS GuardDuty	Intelligent threat detection service that continuously monitors AWS accounts and workloads	Detecting a potential data exfiltration attempt by identifying unusual API calls from a compromised EC2 instance	AWS GuardDuty: https://aws.amazon.com/guardduty/
2	Azure Security Center	Unified infrastructure security management system that strengthens the security posture of data centers	Using Security Center to assess the security state of all Azure resources and receive actionable recommendations to remediate vulnerabilities	Azure Security Center: https://azure.microsoft.com/en-us/services/security-center/

3	Google Cloud Security Command Center	Centralized security and risk management platform for Google Cloud resources	Utilizing the Security Health Analytics feature to detect misconfigurations in Google Cloud Platform (GCP) services	Google Cloud Security Command Center: https://cloud.google.com/security-command-center
4	Prisma Cloud	Cloud-native security platform providing visibility and threat protection across public clouds	Implementing Prisma Cloud to enforce compliance policies across multi-cloud environments and detect anomalous user activities	Prisma Cloud: https://www.paloaltonetworks.com/prisma/cloud
5	Lacework	Automated cloud security platform that provides threat detection, compliance, and vulnerability management	Using Lacework's behavioral anomaly detection to identify and alert on unusual container activities in a Kubernetes cluster	Lacework: https://www.lacework.com/

Threat Intelligence

1	ThreatConnect	A threat intelligence platform that aggregates, analyzes, and acts on threat data from multiple sources	Using ThreatConnect to correlate indicators of compromise (IoCs) across different threat feeds and internal data sources	ThreatConnect: https://threatconnect.com/
2	Recorded Future	A security intelligence platform that provides real-time threat intelligence from a wide range of sources	Leveraging Recorded Future's browser extension to get instant risk scores for IP addresses, domains, and vulnerabilities while browsing	Recorded Future: https://www.recordedfuture.com/
3	AlienVault OTX	Open Threat Exchange (OTX) is an open threat intelligence community that allows sharing of threat data	Subscribing to OTX pulses to receive real-time updates on emerging threats and incorporating this data into your security tools	AlienVault OTX: https://otx.alienvault.com/

4	IBM X-Force Exchange	A cloud-based threat intelligence sharing platform that provides detailed information about threats	Using X-Force Exchange to research a suspicious IP address and view its associated malware, vulnerabilities, and threat actor information	IBM X-Force Exchange: https://exchange.xforce.ibmcloud.com/
5	MISP (Malware Information Sharing Platform)	An open-source threat intelligence platform for sharing, storing, and correlating IoCs	Setting up a MISP instance to share threat intelligence within your organization or with trusted partners, and automating the import of this data into your security tools.	MISP: https://www.misp-project.org/