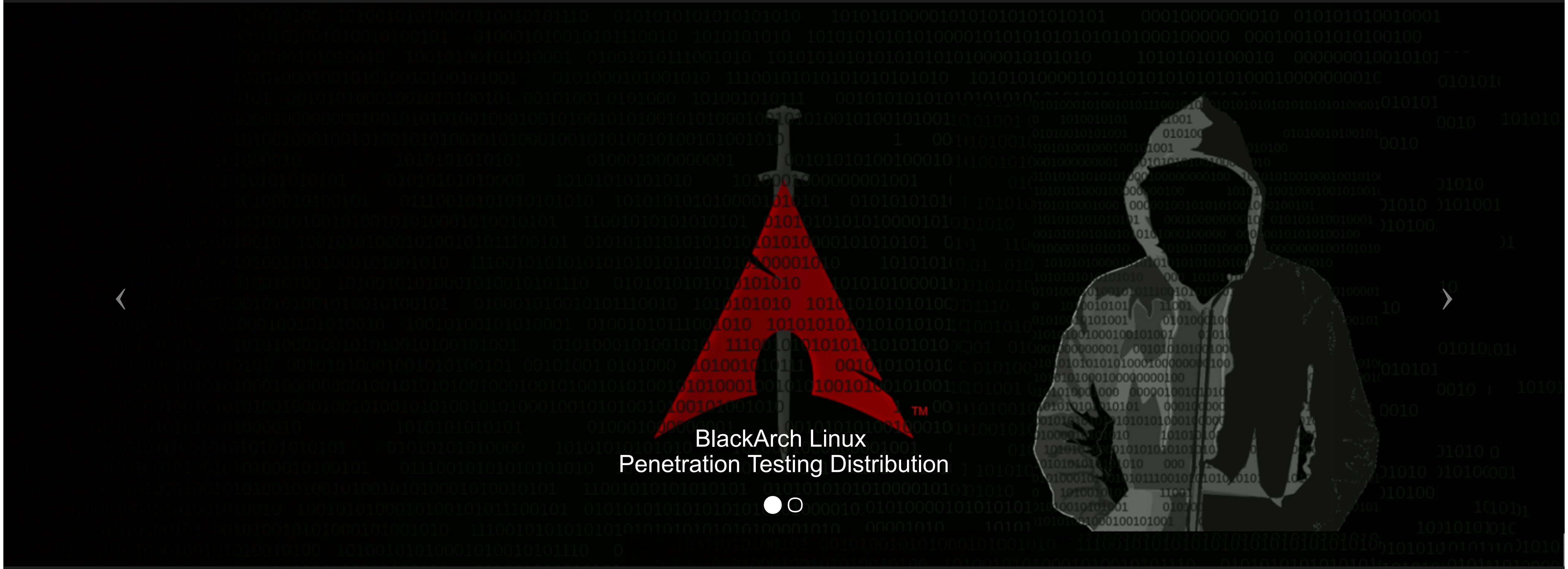

BlackArch Linux
Penetration Testing Distribution

Recon

The list

[Home](#) / [tools](#) / recon

Packages that actively seeks vulnerable exploits in the wild. More of an umbrella group for similar packages.

Tool count: 28

BlackArch recon

Name	Version	Description	Homepage
ad-ldap-enum	44.1386673	An LDAP based Active Directory user and group enumeration tool.	↗
altdns	58.319404d	Generates permutations, alterations and mutations of subdomains and then resolves them.	↗
api-dnsdumpster	59.eda15d6	Unofficial Python API for http://dnsdumpster.com/.	↗
aquatone	92.0e70504	A set of tools for performing reconnaissance on domain names.	↗
autosint	234.e1f4937	Tool to automate common osint tasks.	↗
aws-inventory	8.58eb448	Discover resources created in an AWS account.	↗
aztarna	1.0	A footprinting tool for ROS and SROS systems.	↗
badkarma	85.2c46334	Advanced network reconnaissance toolkit.	↗
basedomainname	0.1	Tool that can extract TLD (Top Level Domain), domain extensions (Second Level Domain + TLD), domain name, and hostname from fully qualified domain names.	↗
bfac	50.2d0516c	An automated tool that checks for backup artifacts that may disclose the web-application's source code.	↗
billcipher	28.3d3322a	Information Gathering tool for a Website or IP address.	↗
bing-ip2hosts	0.4	Enumerates all hostnames which Bing has indexed for a specific IP address.	↗
bloodhound	658.1503905	Six Degrees of Domain Admin	↗
catnthecanary	7.e9184fe	An application to query the canary.pw data set for leaked data.	↗
certgraph	140.97a2803	Crawl the graph of certificate Alternate Names.	↗
cloudfail	60.86e8cc3	Utilize misconfigured DNS and old database records to find hidden IP's behind the CloudFlare network.	↗

Name	Version	Description	Homepage
cr3dov3r	46.99a1660	Search for public leaks for email addresses + check creds against 16 websites.	↗
cutycapt	10	A Qt and WebKit based command-line utility that captures WebKit's rendering of a web page.	↗
datasploit	367.a270d50	Performs automated OSINT and more.	↗
dga-detection	78.0a3186e	DGA Domain Detection using Bigram Frequency Analysis.	↗
dns-parallel-prober	56.99a7b83	PoC for an adaptive parallelised DNS prober.	↗
dnsbrute	2.b1dc84a	Multi-theaded DNS bruteforcing, average speed 80 lookups/second with 40 threads.	↗
dnsenum	1.2.4.2	Script that enumerates DNS information from a domain, attempts zone transfers, performs a brute force dictionary style attack, and then performs reverse look-ups on the results.	↗
dnsgrep	5.c982dc7	A utility for quickly searching presorted DNS names.	↗
dnsrecon	0.8.13	Python script for enumeration of hosts, subdomains and emails from a given domain using google.	↗
dnssearch	20.e4ea439	A subdomain enumeration tool.	↗
dnsspider	1.1	A very fast multithreaded bruteforcer of subdomains that leverages a wordlist and/or character permutation.	↗
dnstracer	1.9	Determines where a given DNS server gets its information from, and follows the chain of DNS servers	↗
dnswalk	2.0.2	A DNS debugger.	↗
domain-analyzer	0.8.1	Finds all the security information for a given domain name.	↗
domain-stats	28.033375f	A web API to deliver domain information from whois and alexa.	↗
dradis	3.0.0.rc1	An open source framework to enable effective information sharing.	↗

Name	Version	Description	Homepage
dradis-ce	857.692d172	An open source framework to enable effective information sharing.	↗
enum4linux	0.8.9	A tool for enumerating information from Windows and Samba systems.	↗
enumerid	13.4853066	Enumerate RIDs using pure Python.	↗
exitmap	358.2e0f62e	A fast and modular scanner for Tor exit relays.	↗
facebot	23.57f6025	A facebook profile and reconnaissance system.	↗
fbid	16.1b35eb9	Show info about the author by facebook photo url.	↗
flashlight	109.90d1dc5	Automated Information Gathering Tool for Penetration Testers.	↗
forager	115.7439b0a	Multithreaded threat Intelligence gathering utilizing.	↗
gasmask	149.9d26cb5	All in one Information gathering tool - OSINT.	↗
gatecrasher	2.3ad5225	Network auditing and analysis tool developed in Python.	↗
geoedge	0.2	This little tools is designed to get geolocalization information of a host, it get the information from two sources (maxmind and geoiptool).	↗
gitem	85.b8937c0	A Github organization reconnaissance tool.	↗
githack	7.dad9d5c	A `.git` folder disclosure exploit.	↗
gitleaks	349.5d68b48	Audit Git repos for secrets and keys.	↗
gitmails	70.ee11da1	An information gathering tool to collect git commit emails in version control host services.	↗
gitminer	53.3f81161	Tool for advanced mining for content on Github.	↗
goddi	1.2	Dumps Active Directory domain information.	↗
goodork	2.2	A python script designed to allow you to leverage the power of google dorking straight from the comfort of your command line.	↗
goofile	1.5	Command line filetype search	↗
goog-mail	1.0	Enumerate domain emails from google.	↗
googlesub	14.a7a3cc7	A python script to find domains by using google dorks.	↗

Name	Version	Description	Homepage
goohak	26.ee593c7	Automatically Launch Google Hacking Queries Against A Target Domain.	↗
gosint	104.07b811c	OSINT framework in Go.	↗
grabing	11.9c1aa6c	Counts all the hostnames for an IP adress	↗
gwtenum	7.f27a5aa	Enumeration of GWT-RCP method calls.	↗
h8mail	28.c4b8b2e	Email OSINT and password breach hunting.	↗
halcyon	0.1	A repository crawler that runs checksums for static files found within a given git repository.	↗
hasere	1.0	Discover the vhosts using google and bing.	↗
hatcloud	33.3012ad6	Bypass CloudFlare with Ruby.	↗
hoper	12.3951159	Trace URL's jumps across the rel links to obtain the last URL.	↗
howmanypeoplearearound	122.776082c	Count the number of people around you by monitoring wifi signals.	↗
id-entify	16.8e6c566	Search for information related to a domain: Emails - IP addresses - Domains - Information on WEB technology - Type of Firewall - NS and MX records.	↗
idswakeup	1.0	A collection of tools that allows to test network intrusion detection systems.	↗
infoga	13.f02cdb0	Tool for gathering e-mail accounts information from different public sources (search engines, pgp key servers).	↗
inquisitor	28.12a9ec1	OSINT Gathering Tool for Companies and Organizations.	↗
intrace	1.5	Traceroute-like application piggybacking on existing TCP connections	↗
ip-tracer	76.ce07e93	Track and retrieve any ip address information.	↗
ip2clue	0.0.94	A small memory/CPU footprint daemon to lookup country (and other info) based on IP (v4 and v6).	↗
iptodomain	18.f1afcd7	This tool extract domains from IP address based in the information saved in virustotal.	↗

Name	Version	Description	Homepage
ircsnapshot	94.cb02a85	Tool to gather information from IRC servers.	↗
isr-form	1.0	Simple html parsing tool that extracts all form related information and generates reports of the data. Allows for quick analyzing of data.	↗
ivre	0.9.12.dev77	Network recon framework	↗
ivre-docs	0.9.12.dev77	Network recon framework (documentation)	↗
ivre-web	0.9.12.dev77	Network recon framework (web application)	↗
kacak	1.0	Tools for penetration testers that can enumerate which users logged on windows system.	↗
lanmap2	127.1197999	Passive network mapping tool.	↗
lbd	20130719	Load Balancing detector	↗
ldapenum	0.1	Enumerate domain controllers using LDAP.	↗
lft	3.8	A layer four traceroute implementing numerous other features.	↗
lhf	40.51568ee	A modular recon tool for pentesting.	↗
linux-exploit-suggester	32.9db2f5a	A Perl script that tries to suggest exploits based OS version number.	↗
linux-exploit-suggester.sh	117.28a2ace	Linux privilege escalation auditing tool.	↗
loot	51.656fb85	Sensitive information extraction tool.	↗
machinae	165.cdee15f	A tool for collecting intelligence from public sites/feeds about various security-related pieces of data.	↗
mail-crawl	0.1	Tool to harvest emails from website.	↗
massbleed	16.cf7c5d6	SSL Vulnerability Scanner.	↗
mdns-recon	10.81ecf94	An mDNS recon tool written in Python.	↗
metagoofil	1.4b	An information gathering tool designed for extracting metadata of public documents.	↗
missidentify	1.0	A program to find Win32 applications.	↗

Name	Version	Description	Homepage
monocle	1.0	A local network host discovery tool. In passive mode, it will listen for ARP request and reply packets. In active mode, it will send ARP requests to the specific IP range. The results are a list of IP and MAC addresses present on the local network.	↗
nasnum	5.df5df19	Script to enumerate network attached storages.	↗
necromant	3.acbc448	Python Script that search unused Virtual Hosts in Web Servers.	↗
neglected	8.68d02b3	Facebook CDN Photo Resolver.	↗
netdiscover	0.3	An active/passive address reconnaissance tool, mainly developed for those wireless networks without dhcp server, when you are wardriving. It can be also used on hub/switched networks.	↗
netkit-bsd-finger	0.17	BSD-finger ported to Linux.	↗
netmask	2.4.4	Helps determine network masks	↗
nohidy	67.22c1283	The system admins best friend, multi platform auditing tool.	↗
nsec3walker	20101223	Enumerates domain names using DNSSEC	↗
ntp-ip-enum	0.1	Script to pull addresses from a NTP server using the monlist command. Can also output Maltego resultset.	↗
nullinux	95.9155b58	Tool that can be used to enumerate OS information, domain information, shares, directories, and users through SMB null sessions.	↗
omnibus	126.d73c1e7	OSINT tool for intelligence collection, research and artifact management.	↗
onioff	84.34dc309	An onion url inspector for inspecting deep web links.	↗
osint-spy	13.76f2c7a	Performs OSINT scan on email/domain/ip_address/organization.	↗
osinterator	3.8447f58	Open Source Toolkit for Open Source Intelligence Gathering.	↗

Name	Version	Description	Homepage
osrframework	789.83437f4	A project focused on providing API and tools to perform more accurate online researches.	↗
parsero	81.e5b585a	A robots.txt audit tool.	↗
pmapper	15.d38a5de	A tool for quickly evaluating IAM permissions in AWS.	↗
punter	45.97b7bed	Hunt domain names using DNSDumpster, WHOIS, Reverse WHOIS, Shodan, Crimeflare.	↗
pwned	585.8e60c39	A command-line tool for querying the 'Have I been pwned?' service.	↗
pymeta	13.fa74e64	Auto Scanning to SSL Vulnerability.	↗
python-ivre	0.9.12.dev77	Network recon framework (library)	↗
python-shodan	1.12.1	Python library and command-line utility for Shodan (https://developer.shodan.io).	↗
python2-ivre	0.9.12.dev77	Network recon framework (library)	↗
python2-shodan	1.12.1	Python library and command-line utility for Shodan (https://developer.shodan.io).	↗
quickrecon	0.3.2	A python script for simple information gathering. It attempts to find subdomain names, perform zone transfers and gathers emails from Google and Bing.	↗
raccoon	183.985797f	A high performance offensive security tool for reconnaissance and vulnerability scanning.	↗
recon-ng	4.9.6	A full-featured Web Reconnaissance framework written in Python.	↗
reconnoitre	396.e1027ec	A security tool for multithreaded information gathering and service enumeration.	↗
reconscan	37.d321842	Network reconnaissance and vulnerability assessment tools.	↗
red-hawk	27.f560071	All in one tool for Information Gathering, Vulnerability Scanning and Crawling.	↗
reverseip	13.42cc9c3	Ruby based reverse IP-lookup tool.	↗
revipd	5.2aaacfb	A simple reverse IP domain scanner.	↗

Name	Version	Description	Homepage
ripdc	0.3	A script which maps domains related to an given ip address or domainname.	↗
sctpscan	34.4d44706	A network scanner for discovery and security.	↗
server-status-pwn	7.0c02af0	A script that monitors and extracts requested URLs and clients connected to the service by exploiting publicly accessible Apache server-status instances.	↗
shard	1.5	A command line tool to detect shared passwords.	↗
shodan	1.12.1	Python library and command-line utility for Shodan (https://developer.shodan.io).	↗
shodanhat	13.e5e7e68	Search for hosts info with shodan.	↗
simplyemail	1.4.10.r7.6a42d37	Email recon made fast and easy, with a framework to build on CyberSyndicates	↗
sipi	13.58f0dcc	Simple IP Information Tools for Reputation Data Analysis.	↗
smbcrunch	12.313400e	3 tools that work together to simplify reconaissance of Windows File Shares.	↗
smtp-user-enum	1.2	Username guessing tool primarily for use against the default Solaris SMTP service. Can use either EXPN, VRFY or RCPT TO.	↗
spfmap	8.a42d15a	A program to map out SPF and DKIM records for a large number of domains.	↗
spiderfoot	2.12.0	The Open Source Footprinting Tool.	↗
spoofcheck	16.8cce591	Simple script that checks a domain for email protections.	↗
ssl-hostname-resolver	1	CN (Common Name) grabber on X.509 Certificates over HTTPS.	↗
stardox	41.95b0a97	Github stargazers information gathering tool.	↗
subdomainer	1.2	A tool designed for obtaining subdomain names from public sources.	↗
subfinder	410.357c340	Modular subdomain discovery tool that can discover massive amounts of valid subdomains for any target.	↗

Name	Version	Description	Homepage
sublist3r	124.69fdd12	A Fast subdomains enumeration tool for penetration testers.	↗
subscraper	18.aa377e0	Tool that performs subdomain enumeration through various techniques.	↗
sysdig	0.25	Open source system-level exploration and troubleshooting tool	↗
theharvester	703.5f8e32e	Python tool for gathering e-mail accounts and subdomain names from different public sources (search engines, pgp key servers).	↗
tilt	90.2bc2ef2	An easy and simple tool implemented in Python for ip reconnaissance, with reverse ip lookup.	↗
tinfoleak	3.6469eb3	Get detailed information about a Twitter user activity.	↗
tinfoleak2	41.c45c33e	The most complete open-source tool for Twitter intelligence analysis.	↗
traceroute	2.1.0	Tracks the route taken by packets over an IP network	↗
treasure	6.a91d52b	Hunt for sensitive information through githubs code search.	↗
trufflehog	135.a4c69fa	Searches through git repositories for high entropy strings, digging deep into commit history.	↗
trusttrees	7.0665877	A Tool for DNS Delegation Trust Graphing.	↗
twofi	2.0	Twitter Words of Interest.	↗
ubiquiti-probing	5.c28f4c1	A Ubiquiti device discovery tool.	↗
userrecon	10.3b56891	Find usernames across over 75 social networks.	↗
vbrute	1.11dda8b	Virtual hosts brute forcer.	↗
vpnpivot	22.37bbde0	Explore the network using this tool.	↗
waldo	29.ee4f960	A lightweight and multithreaded directory and subdomain bruteforcer implemented in Python.	↗
websearch	3.09935a5	Search vhost names given a host range. Powered by Bing..	↗

Name	Version	Description	Homepage
whatweb	4263.1420e9fa	Next generation web scanner that identifies what websites are running.	↗
windows-exploit-suggester	41.776bd91	This tool compares a targets patch levels against the Microsoft vulnerability database in order to detect potential missing patches on the target.	↗
xray	91.ca50a32	A tool for recon, mapping and OSINT gathering from public networks.	↗
zeus-scanner	412.f6a3ada	Advanced dork searching utility.	↗
zgrab	800.4f43262	Grab banners (optionally over TLS).	↗

BlackArch Linux 2013-2019