○ ○

Scanner

The list

Packages that scan selected systems for vulnerabilities or information about the network

Tool count: 255

BlackArch scanner

Name	Version	Description	Homepage
0trace	1.5	A hop enumeration tool.	↗
a2sv	135.973ba13	Auto Scanning to SSL Vulnerability.	↗
admsnmp	0.1	ADM SNMP audit scanner.	↗
allthevhosts	1.0	A vhost discovery tool that scrapes various web applications.	↗
amass	332.18d4be1	In-depth subdomain enumeration written in Go.	↗
apache-users	2.1	This perl script will enumerate the usernames on a unix system that use the apache module UserDir.	↗
athena-ssl-scanner	0.6.2	A SSL cipher scanner that checks all cipher codes. It can identify about 150 different ciphers.	↗
atscan	2321.787e448	Server, Site and Dork Scanner.	↗
aws-extender-cli	10.e5df716	Script to test S3 buckets as well as Google Storage buckets and Azure Storage containers for common misconfiguration issues.	↗
barmie	1.01	Java RMI enumeration and attack tool.	↗
belati	72.49577a1	The Traditional Swiss Army Knife for OSINT.	↗
bingoo	3.698132f	A Linux bash based Bing and Google Dorking Tool.	↗
birp	65.b2e108a	A tool that will assist in the security assessment of mainframe applications served over TN3270.	↗
blackbox-scanner	1.7a25220	Dork scanner & bruteforcing & hash cracker with blackbox framework.	↗
bleah	53.6a2fd3a	A BLE scanner for "smart" devices hacking.	↗
blindy	12.59de8f2	Simple script to automate brutforcing blind sql injection vulnerabilities.	↗
bluto	129.b74a182	Recon, Subdomain Bruting, Zone Transfers.	↗
braa	0.82	A mass snmp scanner	↗
cameradar	139.0984607	Hacks its way into RTSP videosurveillance cameras.	↗
camscan	1.0057215	A tool which will analyze the CAM table of Cisco switches to look for anamolies.	↗

Name	Version	Description	Homepage
cangibrina	123.6de0165	Dashboard Finder.	⬀
cecster	5.15544cb	A tool to perform security testing against the HDMI CEC (Consumer Electronics Control) and HEC (HDMI Ethernet Channel) protocols.	⬀
changeme	240.3a6e2f7	A default credential scanner.	⬀
check-weak-dh-ssh	0.1	Debian OpenSSL weak client Diffie-Hellman Exchange checker.	⬀
chiron	48.524abe1	An all-in-one IPv6 Penetration Testing Framework.	⬀
cipherscan	413.edfec2c	A very simple way to find out which SSL ciphersuites are supported by a target.	⬀
ciscos	1.3	Scans class A, B, and C networks for cisco routers which have telnet open and have not changed the default password from cisco.	⬀
clair	2.0.8	Vulnerability Static Analysis for Containers.	⬀
climber	30.5530a78	Check UNIX/Linux systems for privilege escalation.	⬀
cloudflare-enum	10.412387f	Cloudflare DNS Enumeration Tool for Pentesters.	⬀
cloudsploit	274.b2e0656	AWS security scanning checks.	⬀
cmsmap	8.59dd0e2	A python open source Content Management System scanner that automates the process of detecting security flaws of the most popular CMSs.	⬀
configpush	0.8.5	This is a tool to span /8-sized networks quickly sending snmpset requests with default or otherwise specified community string to Cisco devices.	⬀
corstest	5.b203683	A simple CORS misconfigurations checker.	⬀
cpfinder	0.1	Simple script that looks for administrative web interfaces.	⬀
crackmapexec	438.a258bcf	A swiss army knife for pentesting Windows/Active Directory environments.	⬀
creepy	137.9f60449	A geolocation information gatherer. Offers geolocation information gathering through social networking platforms.	⬀

Name	Version	Description	Homepage
ct-exposer	21.aa8d817	An OSINT tool that discovers sub-domains by searching Certificate Transparency logs	↗
cvechecker	3.5	The goal of cvechecker is to report about possible vulnerabilities on your system, by scanning the installed software and matching the results with the CVE database.	↗
d-tect	13.9555c25	Pentesting the Modern Web.	↗
darkbing	0.1	A tool written in python that leverages bing for mining data on systems that may be susceptible to SQL injection.	↗
davtest	1.0	Tests WebDAV enabled servers by uploading test executable files, and then (optionally) uploading files which allow for command execution or other actions directly on the target	↗
dbusmap	13.1870475	This is a simple utility for enumerating D-Bus endpoints, an nmap for D-Bus.	↗
dcrawl	7.3273c35	Simple, but smart, multi-threaded web crawler for randomly gathering huge lists of unique domain names.	↗
deblaze	0.3	A remote method enumeration tool for flex servers	↗
delldrac	0.1a	DellDRAC and Dell Chassis Discovery and Brute Forcer.	↗
dhcpig	92.9fd8df5	Enhanced DHCPv4 and DHCPv6 exhaustion and fuzzing script written in python using scapy network library.	↗
dirb	2.22	A web content scanner, brute forceing for hidden files.	↗
dirbuster	1.0_RC1	An application designed to brute force directories and files names on web/application servers	↗
dirscanner	0.1	This is a python script that scans webservers looking for administrative directories, php shells, and more.	↗

Name	Version	Description	Homepage
dmitry	1.3a	Deepmagic Information Gathering Tool. Gathers information about hosts. It is able to gather possible subdomains, email addresses, and uptime information and run tcp port scans, whois lookups, and more.	↗
dnmap	0.6	The distributed nmap framework	↗
dns2geoip	0.1	A simple python script that brute forces DNS and subsequently geolocates the found subdomains.	↗
dnsa	0.5	DNSA is a dns security swiss army knife	↗
dnsbf	0.3	Search for available domain names in an IP range.	↗
dnsgoblin	0.1	Nasty creature constantly searching for DNS servers. It uses standard dns querys and waits for the replies.	↗
dnspredict	0.0.2	DNS prediction.	↗
dnstwist	214.ca6fd8c	Domain name permutation engine for detecting typo squatting, phishing and corporate espionage.	↗
dockerscan	51.c93e277	Docker security analysis & hacking tools.	↗
dorkbot	73.27ccf04	Command-line tool to scan Google search results for vulnerabilities.	↗
dorkme	56.73305d6	Tool designed with the purpose of making easier the searching of vulnerabilities with Google Dorks, such as SQL Injection vulnerabilities.	↗
dpscan	0.1	Drupal Vulnerabilty Scanner.	↗
driftnet	v1.2.0.r30.ge4ef851	Listens to network traffic and picks out images from TCP streams it observes.	↗
dripper	v1.r1.gc9bb0c9	A fast, asynchronous DNS scanner; it can be used for enumerating subdomains and enumerating boxes via reverse DNS.	↗
dvcs-ripper	52.0672a34	Rip web accessible (distributed) version control systems: SVN/GIT/BZR/CVS/HG.	↗
eazy	0.1	This is a small python tool that scans websites to look for PHP shells, backups, admin panels, and more.	↗

Name	Version	Description	Homepage
enum-shares	7.97cba5a	Tool that enumerates shared folders across the network and under a custom user account.	⬈
enumiax	1.0	An IAX enumerator.	⬈
eternal-scanner	89.d041fe1	An internet scanner for exploit CVE-0144 (Eternal Blue).	⬈
faraday	6973.e23a7d80	A new concept (IPE) Integrated Penetration-Test Environment a multiuser Penetration test IDE. Designed for distribution, indexation and analyze of the generated data during the process of a security audit.	⬈
fernmelder	6.c6d4ebe	Asynchronous mass DNS scanner.	⬈
fgscanner	11.893372c	An advanced, opensource URL scanner.	⬈
fi6s	150.e00092e	IPv6 network scanner designed to be fast.	⬈
fierce	0.9.9	A DNS scanner	⬈
find-dns	0.1	A tool that scans networks looking for DNS servers.	⬈
flashscanner	11.6815b02	Flash XSS Scanner.	⬈
flunym0us	2.0	A Vulnerability Scanner for Wordpress and Moodle.	⬈
forkingportscanner	1	Simple and fast forking port scanner written in perl. Can only scan on host at a time, the forking is done on the specified port range. Or on the default range of 1. Has the ability to scan UDP or TCP, defaults to tcp.	⬈
fs-nyarl	1.0	A network takeover & forensic analysis tool - useful to advanced PenTest tasks & for fun and profit.	⬈
fsnoop	3.4	A tool to monitor file operations on GNU/Linux systems by using the Inotify mechanism. Its primary purpose is to help detecting file race condition vulnerabilities and since version 3, to exploit them with loadable DSO modules (also called "payload modules" or "paymods").	⬈

Name	Version	Description	Homepage
ftp-spider	1.0	FTP investigation tool - Scans ftp server for the following: reveal entire directory tree structures, detect anonymous access, detect directories with write permissions, find user specified data within repository.	🗗
ftpscout	12.cf1dff1	Scans ftps for anonymous access.	🗗
gethsploit	3.144778b	Finding Ethereum nodes which are vulnerable to RPC-attacks.	🗗
gggooglescan	0.4	A Google scraper which performs automated searches and returns results of search queries in the form of URLs or hostnames.	🗗
ghost-phisher	1.62	GUI suite for phishing and penetration attacks	🗗
gitrob	7.7be4c53	Reconnaissance tool for GitHub organizations.	🗗
gloom	95.607162b	Linux Penetration Testing Framework.	🗗
grabbb	0.0.7	Clean, functional, and fast banner scanner.	🗗
greenbone-security-assistant	7.0.3	Greenbone Security Assistant (gsa) - OpenVAS web frontend	🗗
grepforrfi	0.1	Simple script for parsing web logs for RFIs and Webshells v1.2	🗗
gtp-scan	0.7	A small python script that scans for GTP (GPRS tunneling protocol) speaking hosts.	🗗
habu	179.c9b7322	Python Network Hacking Toolkit.	🗗
hakku	384.bbb434d	Simple framework that has been made for penetration testing tools.	🗗
halberd	0.2.4	Halberd discovers HTTP load balancers. It is useful for web application security auditing and for load balancer configuration testing.	🗗
hbad	1.0	This tool allows you to test clients on the heartbleed bug.	🗗
hoppy	1.8.1	A python script which tests http methods for configuration issues leaking information or just to see if they are enabled.	🗗

Name	Version	Description	Homepage
host-extract	8.0134ad7	Ruby script tries to extract all IP/Host patterns in page response of a given URL and JavaScript/CSS files of that URL.	⬀
hsecscan	64.3089ac2	A security scanner for HTTP response headers.	⬀
http-enum	0.4	A tool to enumerate the enabled HTTP methods supported on a webserver.	⬀
httpsscanner	1.2	A tool to test the strength of a SSL web server.	⬀
iaxscan	0.02	A Python based scanner for detecting live IAX/2 hosts and then enumerating (by bruteforce) users on those hosts.	⬀
icmpquery	1.0	Send and receive ICMP queries for address mask and current time.	⬀
iis-shortname-scanner	5.4ad4937	An IIS shortname Scanner.	⬀
ike-scan	1.9	A tool that uses IKE protocol to discover, fingerprint and test IPSec VPN servers	⬀
ilo4-toolbox	33.a08e718	Toolbox for HPE iLO4 analysis.	⬀
infip	0.1	A python script that checks output from netstat against RBLs from Spamhaus.	⬀
inurlbr	33.30a3abc	Advanced search in the search engines - Inurl scanner, dorker, exploiter.	⬀
ipscan	3.5.5	A very fast IP address and port scanner.	⬀
iptv	136.de37822	Search and brute force illegal iptv server.	⬀
ipv6toolkit	2.0	SI6 Networks' IPv6 Toolkit	⬀
jaadas	0.1	Joint Advanced Defect assEsment for android applications.	⬀
knock	274.231c1b6	Subdomain scanner.	⬀
knxmap	243.2d6f622	KNXnet/IP scanning and auditing tool for KNX home automation installations.	⬀
kube-hunter	489.0707954	Hunt for security weaknesses in Kubernetes clusters.	⬀
laf	12.7a456b3	Login Area Finder: scans host/s for login panels.	⬀

Name	Version	Description	Homepage
leaklooker	5.0d2b9fc	Find open databases with Shodan.	↗
letmefuckit-scanner	3.f3be22b	Scanner and Exploit Magento.	↗
leviathan	35.a1a1d8c	A mass audit toolkit which has wide range service discovery, brute force, SQL injection detection and running custom exploit capabilities.	↗
lfi-scanner	4.0	This is a simple perl script that enumerates local file inclusion attempts when given a specific target.	↗
lfisuite	85.470e01f	Totally Automatic LFI Exploiter (+ Reverse Shell) and Scanner.	↗
linenum	54.ddfd743	Scripted Local Linux Enumeration & Privilege Escalation Checks	↗
littleblackbox	0.1.3	Penetration testing tool, search in a collection of thousands of private SSL keys extracted from various embedded devices.	↗
locasploit	117.fa48151	Local enumeration and exploitation framework.	↗
lotophagi	0.1	a relatively compact Perl script designed to scan remote hosts for default (or common) Lotus NSF and BOX databases.	↗
lte-cell-scanner	57.5fa3df8	LTE SDR cell scanner optimized to work with very low performance RF front ends (8bit A/D, 20dB noise figure).	↗
lunar	562.d6a95bf	A UNIX security auditing tool based on several security frameworks.	↗
lynis	2.7.3	Security and system auditing tool to harden Unix/Linux systems	↗
maligno	2.5	An open source penetration testing tool written in python, that serves Metasploit payloads. It generates shellcode with msfvenom and transmits it over HTTP or HTTPS.	↗
maryam	443.7f63d59	Full-featured Web Identification framework written in Python.	↗

Name	Version	Description	Homepage
masscan	1.0.5	TCP port scanner, spews SYN packets asynchronously, scanning entire Internet in under 5 minutes	↗
modscan	0.1	A new tool designed to map a SCADA MODBUS TCP based network.	↗
mongoaudit	217.c03c68a	A powerful MongoDB auditing and pentesting tool .	↗
mssqlscan	0.8.4	A small multi-threaded tool that scans for Microsoft SQL Servers.	↗
multiscanner	1403.3576699	Modular file scanning/analysis framework.	↗
nbtscan	1.5.1	NBTscan is a program for scanning IP networks for NetBIOS name information.	↗
netbios-share-scanner	1.0	This tool could be used to check windows workstations and servers if they have accessible shared resources.	↗
netscan	1.0	Tcp/Udp/Tor port scanner with: synpacket, connect TCP/UDP and socks5 (tor connection).	↗
netscan2	54.262bffe	Active / passive network scanner.	↗
nikto	2.1.6	A web server scanner which performs comprehensive tests against web servers for multiple items	↗
nili	36.97f75f4	Tool for Network Scan, Man in the Middle, Protocol Reverse Engineering and Fuzzing.	↗
nmap	7.70	Utility for network discovery and security auditing	↗
nmbscan	1.2.6	Tool to scan the shares of a SMB/NetBIOS network, using the NMB/SMB/NetBIOS protocols.	↗
nsec3map	20.1263537	A tool to enumerate the resource records of a DNS zone using its DNSSEC NSEC or NSEC3 chain.	↗
nsia	1.0.6	A website scanner that monitors websites in realtime in order to detect defacements, compliance violations, exploits, sensitive information disclosure and other issues.	↗

Name	Version	Description	Homepage
o-saft	3104.3505da3	A tool to show informations about SSL certificate and tests the SSL connection according given list of ciphers and various SSL configurations.	🔗
ocs	0.2	Compact mass scanner for Cisco routers with default telnet/enable passwords.	🔗
onetwopunch	v1.0.0.r2.gd4ab4e8	Use unicornscan to quickly scan all open ports, and then pass the open ports to nmap for detailed scans.	🔗
onionscan	130.da42865	Scan Onion Services for Security Issues.	🔗
openvas-cli	1.4.5	The OpenVAS Command-Line Interface	🔗
openvas-manager	7.0.3	A layer between the OpenVAS Scanner and various client applications	🔗
openvas-scanner	5.1.3	The OpenVAS scanning Daemon	🔗
paketto	1.10	Advanced TCP/IP Toolkit.	🔗
panhunt	59.3991e5e	Searches for credit card numbers (PANs) in directories.	🔗
paranoic	1.7	A simple vulnerability scanner written in Perl.	🔗
passhunt	5.332f374	Search drives for documents containing passwords.	🔗
pbscan	10.566c3d7	Faster and more efficient stateless SYN scanner and banner grabber due to userland TCP/IP stack usage.	🔗
pcredz	45.c8bca9d	A tool that extracts credit card numbers, NTLM(DCE-RPC, HTTP, SQL, LDAP, etc), Kerberos (AS-REQ Pre-Auth etype 23), HTTP Basic, SNMP, POP, SMTP, FTP, IMAP, and more from a pcap file or from a live interface.	🔗
pentestly	1798.93d1b39	Python and Powershell internal penetration testing framework.	🔗
plcscan	0.1	This is a tool written in Python that will scan for PLC devices over s7comm or modbus protocols.	🔗
pnscan	1.11	A parallel network scanner that can be used to survey TCP network services.	🔗
poison	1.5.41	A fast, asynchronous syn and udp scanner.	🔗

Name	Version	Description	Homepage
ppscan	0.3	Yet another port scanner with HTTP and FTP tunneling support.	⬈
prads	1128.407cf7c	Is a "Passive Real-time Asset Detection System".	⬈
praeda	48.1dc2220	An automated data/information harvesting tool designed to gather critical information from various embedded devices.	⬈
proxycheck	0.1	This is a simple proxy tool that checks for the HTTP CONNECT method and grabs verbose output from a webserver.	⬈
proxyscan	0.3	A security penetration testing tool to scan for hosts and ports through a Web proxy server.	⬈
pyssltest	9.d7703f0	A python multithreaded script to make use of Qualys ssllabs api to test SSL flaws.	⬈
pytbull	2.1	A python based flexible IDS/IPS testing framework shipped with more than 300 tests.	⬈
pythem	454.e4fcb8a	python2 penetration testing framework.	⬈
ranger-scanner	149.3aae5dd	A tool to support security professionals to access and interact with remote Microsoft Windows based systems.	⬈
rawr	73.0924126	Rapid Assessment of Web Resources. A web enumerator.	⬈
relay-scanner	1.7	An SMTP relay scanner.	⬈
responder	201.0bdc183	A LLMNR and NBT-NS poisoner, with built-in HTTP/SMB/MSSQL/FTP/LDAP rogue authentication server supporting NTLMv1/NTLMv2/LMv2, Extended Security NTLMSSP and Basic HTTP authentication.	⬈
responder-multirelay	329.7339411	A LLMNR and NBT-NS poisoner, with built-in HTTP/SMB/MSSQL/FTP/LDAP rogue authentication server supporting NTLMv1/NTLMv2/LMv2 (multirelay version),	⬈
routerhunter	21.4da257c	Tool used to find vulnerable routers and devices on the Internet and perform tests.	⬈

Name	Version	Description	Homepage
rtlizer	35.5614163	Simple spectrum analyzer.	[↗]
rtlsdr-scanner	1013.3c032de	A cross platform Python frequency scanning GUI for the OsmoSDR rtl-sdr library.	[↗]
s3scanner	225.a386b49	Scan for open S3 buckets and dump.	[↗]
sambascan	0.5.0	Allows you to search an entire network or a number of hosts for SMB shares. It will also list the contents of all public shares that it finds.	[↗]
sandy	6.531ab16	An open-source Samsung phone encryption assessment framework	[↗]
sb0x	19.04f40fe	A simple and Lightweight framework for Penetration testing.	[↗]
scamper	20180504	A tool that actively probes the Internet in order to analyze topology and performance.	[↗]
scanless	64.3e025be	Utility for using websites that can perform port scans on your behalf.	[↗]
scanssh	2.1	Fast SSH server and open proxy scanner.	[↗]
scout2	1182.5d86d46	Security auditing tool for AWS environments.	[↗]
scoutsuite	3046.5115d5b5	Multi-Cloud Security Auditing Tool.	[↗]
scrape-dns	58.3df392f	Searches for interesting cached DNS entries.	[↗]
sdnpwn	56.2ef2aa1	An SDN penetration testing toolkit.	[↗]
seat	0.3	Next generation information digging application geared toward the needs of security professionals. It uses information stored in search engine databases, cache repositories, and other public resources to scan web sites for potential vulnerabilities.	[↗]
shareenum	46.3bfa81d	Tool to enumerate shares from Windows hosts.	[↗]
sharesniffer	51.dbf05b5	Network share sniffer and auto-mounter for crawling remote file systems.	[↗]
simple-lan-scan	1.0	A simple python script that leverages scapy for discovering live hosts on a network.	[↗]
sipshock	7.6ab5591	A scanner for SIP proxies vulnerable to Shellshock.	[↗]

Name	Version	Description	Homepage
smbexec	148.7827616	A rapid psexec style attack with samba tools.	🔗
smbmap	67.b55fc05	A handy SMB enumeration tool.	🔗
smbspider	10.7db9323	A lightweight python utility for searching SMB/CIFS/Samba file shares.	🔗
smod	53.7eb8423	A modular framework with every kind of diagnostic and offensive feature you could need in order to pentest modbus protocol.	🔗
smtp-test	4.1936e5c	Automated testing of SMTP servers for penetration testing.	🔗
smtp-vrfy	1.0	An SMTP Protocol Hacker.	🔗
smtptx	1.0	A very simple tool used for sending simple email and do some basic email testing from a pentester perspective.	🔗
snmpenum	1.7	An snmp enumerator.	🔗
snmpscan	0.1	A free, multi-processes SNMP scanner.	🔗
snoopbrute	17.589fbe6	Multithreaded DNS recursive host brute-force tool.	🔗
sparta	21.b0a4514	Python GUI application which simplifies network infrastructure penetration testing by aiding the penetration tester in the scanning and enumeration phase.	🔗
sqlivulscan	249.cc8e657	This will give you the SQLi Vulnerable Website Just by Adding the Dork.	🔗
ssdp-scanner	1.0	SSDP amplification scanner written in Python. Makes use of Scapy.	🔗
ssh-audit	165.22b671e	SSH server auditing (banner, key exchange, encryption, mac, compression, compatbility, etc).	🔗
ssh-user-enum	7.ae453c1	SSH User Enumeration Script in Python Using The Timing Attack.	🔗
sslcaudit	524.f218b9b	Utility to perform security audits of SSL/TLS clients.	🔗
ssllabs-scan	245.e5a8705	Command-line client for the SSL Labs APIs	🔗
sslmap	0.2.0	A lightweight TLS/SSL cipher suite scanner.	🔗

Name	Version	Description	Homepage
sslscan	1.10.2	A fast tools to scan SSL services, such as HTTPS to determine the ciphers that are supported	⬈
sticky-keys-hunter	15.c816fc9	Script to test an RDP host for sticky keys and utilman backdoor.	⬈
stig-viewer	2.8	XCCDF formatted SRGs and STIGs files viewer for SCAP validation tools.	⬈
striker	66.c28a88a	An offensive information and vulnerability scanner.	⬈
strutscan	4.8712c12	Apache Struts2 vulnerability scanner written in Perl.	⬈
subbrute	1.2.1	A DNS meta-query spider that enumerates DNS records and subdomains	⬈
subover	71.3d258e2	A Powerful Subdomain Takeover Tool.	⬈
svn-extractor	39.39941be	A simple script to extract all web resources by means of .SVN folder exposed over network.	⬈
swarm	41.1713c1e	A distributed penetration testing tool.	⬈
synscan	5.02	fast asynchronous half-open TCP portscanner	⬈
tachyon-scanner	449.b2a5226	Fast Multi-Threaded Web Discovery Tool.	⬈
tactical-exploitation	78.66f8e2b	Modern tactical exploitation toolkit.	⬈
taipan	1.7	Web application security scanner.	⬈
topera	19.3e230fd	An IPv6 security analysis toolkit, with the particularity that their attacks can't be detected by Snort.	⬈
udsim	23.35c1710	A graphical simulator that can emulate different modules in a vehicle and respond to UDS request.	⬈
umap	25.3ad8121	The USB host security assessment tool.	⬈
unicornscan	0.4.7	A new information gathering and correlation engine.	⬈
upnpscan	0.4	Scans the LAN or a given address range for UPnP capable devices.	⬈
uw-loveimap	0.1	Multi threaded imap bounce scanner.	⬈
uw-udpscan	0.1	Multi threaded udp scanner.	⬈
uw-zone	0.1	Multi threaded, randomized IP zoner.	⬈

Name	Version	Description	Homepage
v3n0m	317.b9b856a	A tool to automate mass SQLi d0rk scans and Metasploit Vulns.	⬀
vais	17.5c35c3a	SWF Vulnerability & Information Scanner.	⬀
vane	1898.872a1c2	A vulnerability scanner which checks the security of WordPress installations using a black box approach.	⬀
vcsmap	47.3889964	A plugin-based tool to scan public version control systems for sensitive information.	⬀
vhostscan	329.74e4681	A virtual host scanner that can be used with pivot tools, detect catch-all scenarios, aliases and dynamic default pages.	⬀
videosnarf	0.63	A new security assessment tool for pcap analysis	⬀
visql	49.3082e30	Scan SQL vulnerability on target site and sites of on server.	⬀
vscan	10.da4e47e	HTTPS / Vulnerability scanner.	⬀
vuls	575.fecd1ad	Vulnerability scanner for Linux/FreeBSD, agentless, written in Go.	⬀
vulscan	2.0	A module which enhances nmap to a vulnerability scanner	⬀
wafw00f	275.a1c3f3a	Identify and fingerprint Web Application Firewall (WAF) products protecting a website.	⬀
webenum	0.1	Tool to enumerate http responses using dynamically generated queries and more. Useful for penetration tests against web servers.	⬀
webhunter	12.918b606	Tool for scanning web applications and networks and easily completing the process of collecting knowledge.	⬀
webpwn3r	35.3fb27bb	A python based Web Applications Security Scanner.	⬀
webrute	3.3	Web server directory brute forcer.	⬀
whitewidow	605.4f27bfe	SQL Vulnerability Scanner.	⬀
wolpertinger	2.58ef8e2	A distributed portscanner.	⬀
wordpresscan	66.8a24768	WPScan rewritten in Python + some WPSeku ideas.	⬀

Name	Version	Description	Homepage
xcname	11.9c475a1	A tool for enumerating expired domains in CNAME records.	🔗
xpire-crossdomain-scanner	1.0cb8d3b	Scans crossdomain.xml policies for expired domain names.	🔗
xsstracer	5.f2ed21a	Python script that checks remote web servers for Clickjacking, Cross-Frame Scripting, Cross-Site Tracing and Host Header Injection.	🔗
yasat	848	Yet Another Stupid Audit Tool.	🔗
zmap	2.1.1	Fast network scanner designed for Internet-wide network surveys	🔗

BlackArch Linux 2013-2019