List of NMAP Scripts

Use with the nmap –script option

acarsd-info	Retrieves information from a listening acarsd daemon. Acarsd decodes ACARS (Aircraft Communication Addressing and Reporting System) data in real time. The information retrieved by this script includes the daemon version, API version, administrator e-mail address and listening frequency.
address-info	Shows extra information about IPv6 addresses, such as embedded MAC or IPv4 addresses when available.
afp-brute	Performs password guessing against Apple Filing Protocol (AFP).
afp-ls	Attempts to get useful information about files from AFP volumes. The output is intended to resemble the output of `ls`.
afp-path-vuln	Detects the Mac OS X AFP directory traversal vulnerability, CVE-2010-0533.
afp-serverinfo	Shows AFP server information. This information includes the server's hostname, IPv4 and IPv6 addresses, and hardware type (for example `Macmini` or `MacBookPro`).
afp-showmount	Shows AFP shares and ACLs.
ajp-auth	Retrieves the authentication scheme and realm of an AJP service (Apache JServ Protocol) that requires authentication.
ajp-brute	Performs brute force passwords auditing against the Apache JServ protocol. The Apache JServ Protocol is commonly used by web servers to communicate with back-end Java application server containers.
ajp-headers	Performs a HEAD or GET request against either the root directory or any optional directory of an Apache JServ Protocol server and returns the server response headers.
ajp-methods	Discovers which options are supported by the AJP (Apache JServ Protocol) server by sending an OPTIONS request and lists potentially risky methods.
ajp-request	Requests a URI over the Apache JServ Protocol and displays the

	result (or stores it in a file). Different AJP methods such as; GET, HEAD, TRACE, PUT or DELETE may be used.
allseeingeye-info	Detects the All-Seeing Eye service. Provided by some game servers for querying the server's status.
amqp-info	Gathers information (a list of all server properties) from an AMQP (advanced message queuing protocol) server.
asn-query	Maps IP addresses to autonomous system (AS) numbers.
auth-owners	Attempts to find the owner of an open TCP port by querying an auth daemon which must also be open on the target system. The auth service, also known as identd, normally runs on port 113.
auth-spoof	Checks for an identd (auth) server which is spoofing its replies.
backorifice-brute	Performs brute force password auditing against the BackOrifice service. The `backorifice-brute.ports` script argument is mandatory (it specifies ports to run the script against).
backorifice-info	Connects to a BackOrifice service and gathers information about the host and the BackOrifice service itself.
bacnet-info	Discovers and enumerates BACNet Devices collects device information based off standard requests. In some cases, devices may not strictly follow the specifications, or may comply with older versions of the specifications, and will result in a BACNET error response. Presence of this error positively identifies the device as a BACNet device, but no enumeration is possible.
banner	A simple banner grabber which connects to an open TCP port and prints out anything sent by the listening service within five seconds.
bitcoin-getaddr	Queries a Bitcoin server for a list of known Bitcoin nodes
bitcoin-info	Extracts version and node information from a Bitcoin server
bitcoinrpc-info	Obtains information from a Bitcoin server by calling `getinfo` on its JSON-RPC interface.
bittorrent-discovery	Discovers bittorrent peers sharing a file based on a user-supplied torrent file or magnet link. Peers implement the Bittorrent

	protocol and share the torrent, whereas the nodes (only shown if the include-nodes NSE argument is given) implement the DHT protocol and are used to track the peers. The sets of peers and nodes are not the same, but they usually intersect.
bjnp-discover	Retrieves printer or scanner information from a remote device supporting the BJNP protocol. The protocol is known to be supported by network based Canon devices.
broadcast-ataoe-discover	Discovers servers supporting the ATA over Ethernet protocol. ATA over Ethernet is an ethernet protocol developed by the Brantley Coile Company and allows for simple, high-performance access to SATA drives over Ethernet.
broadcast-avahi-dos	Attempts to discover hosts in the local network using the DNS Service Discovery protocol and sends a NULL UDP packet to each host to test if it is vulnerable to the Avahi NULL UDP packet denial of service (CVE-2011-1002).
broadcast-bjnp-discover	Attempts to discover Canon devices (Printers/Scanners) supporting the BJNP protocol by sending BJNP Discover requests to the network broadcast address for both ports associated with the protocol.
broadcast-db2-discover	Attempts to discover DB2 servers on the network by sending a broadcast request to port 523/udp.
broadcast-dhcp-discover	Sends a DHCP request to the broadcast address (255.255.255.255) and reports the results. The script uses a static MAC address (DE:AD:CO:DE:CA:FE) while doing so in order to prevent scope exhaustion.
broadcast-dhcp6-discover	Sends a DHCPv6 request (Solicit) to the DHCPv6 multicast address, parses the response, then extracts and prints the address along with any options returned by the server.
broadcast-dns-service-discovery	Attempts to discover hosts' services using the DNS Service Discovery protocol. It sends a multicast DNS-SD query and collects all the responses.
broadcast-dropbox-listener	Listens for the LAN sync information broadcasts that the Dropbox.com client broadcasts every 20 seconds, then prints all the discovered client IP addresses, port numbers, version numbers, display names, and more.
broadcast-eigrp-discovery	Performs network discovery and routing information gathering

	through Cisco's Enhanced Interior Gateway Routing Protocol (EIGRP).
broadcast-igmp-discovery	Discovers targets that have IGMP Multicast memberships and grabs interesting information.
broadcast-listener	Sniffs the network for incoming broadcast communication and attempts to decode the received packets. It supports protocols like CDP, HSRP, Spotify, DropBox, DHCP, ARP and a few more. See packetdecoders.lua for more information.
broadcast-ms-sql-discover	Discovers Microsoft SQL servers in the same broadcast domain.
broadcast-netbios-master-browser	Attempts to discover master browsers and the domains they manage.
broadcast-networker-discover	Discovers EMC Networker backup software servers on a LAN by sending a network broadcast query.
broadcast-novell-locate	Attempts to use the Service Location Protocol to discover Novell NetWare Core Protocol (NCP) servers.
broadcast-pc-anywhere	Sends a special broadcast probe to discover PC-Anywhere hosts running on a LAN.
broadcast-pc-duo	Discovers PC-DUO remote control hosts and gateways running on a LAN by sending a special broadcast UDP probe.
broadcast-pim-discovery	Discovers routers that are running PIM (Protocol Independent Multicast).
broadcast-ping	Sends broadcast pings on a selected interface using raw ethernet packets and outputs the responding hosts' IP and MAC addresses or (if requested) adds them as targets. Root privileges on UNIX are required to run this script since it uses raw sockets. Most operating systems don't respond to broadcast-ping probes, but they can be configured to do so.
broadcast-pppoe-discover	Discovers PPPoE (Point-to-Point Protocol over Ethernet) servers using the PPPoE Discovery protocol (PPPoED). PPPoE is an ethernet based protocol so the script has to know what ethernet interface to use for discovery. If no interface is specified, requests are sent out on all available interfaces.
broadcast-rip-discover	Discovers hosts and routing information from devices running

	RIPv2 on the LAN. It does so by sending a RIPv2 Request command and collects the responses from all devices responding to the request.
broadcast-ripng-discover	Discovers hosts and routing information from devices running RIPng on the LAN by sending a broadcast RIPng Request command and collecting any responses.
broadcast-sybase-asa-discover	Discovers Sybase Anywhere servers on the LAN by sending broadcast discovery messages.
broadcast-tellstick-discover	Discovers Telldus Technologies TellStickNet devices on the LAN. The Telldus TellStick is used to wirelessly control electric devices such as lights, dimmers and electric outlets. For more information: http://www.telldus.com/
broadcast-upnp-info	Attempts to extract system information from the UPnP service by sending a multicast query, then collecting, parsing, and displaying all responses.
broadcast-versant-locate	Discovers Versant object databases using the broadcast srvloc protocol.
broadcast-wake-on-lan	Wakes a remote system up from sleep by sending a Wake-On-Lan packet.
broadcast-wpad-discover	Retrieves a list of proxy servers on a LAN using the Web Proxy Autodiscovery Protocol (WPAD). It implements both the DHCP and DNS methods of doing so and starts by querying DHCP to get the address. DHCP discovery requires nmap to be running in privileged mode and will be skipped when this is not the case. DNS discovery relies on the script being able to resolve the local domain either through a script argument or by attempting to reverse resolve the local IP.
broadcast-wsdd-discover	Uses a multicast query to discover devices supporting the Web Services Dynamic Discovery (WS-Discovery) protocol. It also attempts to locate any published Windows Communication Framework (WCF) web services (.NET 4.0 or later).
broadcast-xdmcp-discover	Discovers servers running the X Display Manager Control Protocol (XDMCP) by sending a XDMCP broadcast request to the LAN. Display managers allowing access are marked using the keyword Willing in the result.
cassandra-brute	Performs brute force password auditing against the Cassandra

	database.
cassandra-info	Attempts to get basic info and server status from a Cassandra database.
cccam-version	Detects the CCcam service (software for sharing subscription TV among multiple receivers).
citrix-brute-xml	Attempts to guess valid credentials for the Citrix PN Web Agent XML Service. The XML service authenticates against the local Windows server or the Active Directory.
citrix-enum-apps	Extracts a list of published applications from the ICA Browser service.
citrix-enum-apps-xml	Extracts a list of applications, ACLs, and settings from the Citrix XML service.
citrix-enum-servers	Extracts a list of Citrix servers from the ICA Browser service.
citrix-enum-servers-xml	Extracts the name of the server farm and member servers from Citrix XML service.
couchdb-databases	Gets database tables from a CouchDB database.
couchdb-stats	Gets database statistics from a CouchDB database.
creds-summary	Lists all discovered credentials (e.g. from brute force and default password checking scripts) at end of scan.
cups-info	Lists printers managed by the CUPS printing service.
cups-queue-info	Lists currently queued print jobs of the remote CUPS service grouped by printer.
cvs-brute	Performs brute force password auditing against CVS pserver authentication.
cvs-brute-repository	Attempts to guess the name of the CVS repositories hosted on the remote server. With knowledge of the correct repository name, usernames and passwords can be guessed.
daap-get-library	Retrieves a list of music from a DAAP server. The list includes artist names and album and song titles.

daytime	Retrieves the day and time from the Daytime service.
db2-das-info	Connects to the IBM DB2 Administration Server (DAS) on TCP or UDP port 523 and exports the server profile. No authentication is required for this request.
dhcp-discover	Sends a DHCPINFORM request to a host on UDP port 67 to obtain all the local configuration parameters without allocating a new address.
dict-info	Connects to a dictionary server using the DICT protocol, runs the SHOW SERVER command, and displays the result. The DICT protocol is defined in RFC 2229 and is a protocol which allows a client to query a dictionary server for definitions from a set of natural language dictionary databases.
distcc-cve2004-2687	Detects and exploits a remote code execution vulnerability in the distributed compiler daemon distcc. The vulnerability was disclosed in 2002, but is still present in modern implementation due to poor configuration of the service.
dns-blacklist	Checks target IP addresses against multiple DNS anti-spam and open proxy blacklists and returns a list of services for which an IP has been flagged. Checks may be limited by service category (eg: SPAM, PROXY) or to a specific service name.
dns-brute	Attempts to enumerate DNS hostnames by brute force guessing of common subdomains. With the `dns-brute.srv` argument, dns-brute will also try to enumerate common DNS SRV records.
dns-cache-snoop	Performs DNS cache snooping against a DNS server.
dns-check-zone	Checks DNS zone configuration against best practices, including RFC 1912. The configuration checks are divided into categories which each have a number of different tests.
dns-client-subnet-scan	Performs a domain lookup using the edns-client-subnet option which allows clients to specify the subnet that queries supposedly originate from. The script uses this option to supply a number of geographically distributed locations in an attempt to enumerate as many different address records as possible. The script also supports requests using a given subnet.
dns-fuzz	Launches a DNS fuzzing attack against DNS servers.
dns-ip6-arpa-scan	Performs a quick reverse DNS lookup of an IPv6 network using

	a technique which analyzes DNS server response codes to dramatically reduce the number of queries needed to enumerate large networks.
dns-nsec-enum	Enumerates DNS names using the DNSSEC NSEC-walking technique.
dns-nsec3-enum	Tries to enumerate domain names from the DNS server that supports DNSSEC NSEC3 records.
dns-nsid	Retrieves information from a DNS nameserver by requesting its nameserver ID (nsid) and asking for its id.server and version.bind values. This script performs the same queries as the following two dig commands: - dig CH TXT bind.version @target - dig +nsid CH TXT id.server @target
dns-random-srcport	Checks a DNS server for the predictable-port recursion vulnerability. Predictable source ports can make a DNS server vulnerable to cache poisoning attacks (see CVE-2008-1447).
dns-random-txid	Checks a DNS server for the predictable-TXID DNS recursion vulnerability. Predictable TXID values can make a DNS server vulnerable to cache poisoning attacks (see CVE-2008-1447).
dns-recursion	Checks if a DNS server allows queries for third-party names. It is expected that recursion will be enabled on your own internal nameservers.
dns-service-discovery	Attempts to discover target hosts' services using the DNS Service Discovery protocol.
dns-srv-enum	Enumerates various common service (SRV) records for a given domain name. The service records contain the hostname, port and priority of servers for a given service. The following services are enumerated by the script: - Active Directory Global Catalog - Exchange Autodiscovery - Kerberos KDC Service - Kerberos Passwd Change Service - LDAP Servers - SIP Servers - XMPP S2S - XMPP C2S
dns-update	Attempts to perform a dynamic DNS update without authentication.
dns-zeustracker	Checks if the target IP range is part of a Zeus botnet by querying ZTDNS @ abuse.ch. Please review the following information before you start to scan:

	• https://zeustracker.abuse.ch/ztdns.php
dns-zone-transfer	Requests a zone transfer (AXFR) from a DNS server.
docker-version	Detects the Docker service version.
domcon-brute	Performs brute force password auditing against the Lotus Domino Console.
domcon-cmd	Runs a console command on the Lotus Domino Console using the given authentication credentials (see also: domcon-brute)
domino-enum-users	Attempts to discover valid IBM Lotus Domino users and download their ID files by exploiting the CVE-2006-5835 vulnerability.
dpap-brute	Performs brute force password auditing against an iPhoto Library.
drda-brute	Performs password guessing against databases supporting the IBM DB2 protocol such as Informix, DB2 and Derby
drda-info	Attempts to extract information from database servers supporting the DRDA protocol. The script sends a DRDA EXCSAT (exchange server attributes) command packet and parses the response.
duplicates	Attempts to discover multihomed systems by analysing and comparing information collected by other scripts. The information analyzed currently includes, SSL certificates, SSH host keys, MAC addresses, and Netbios server names.
eap-info	Enumerates the authentication methods offered by an EAP (Extensible Authentication Protocol) authenticator for a given identity or for the anonymous identity if no argument is passed.
enip-info	This NSE script is used to send a EtherNet/IP packet to a remote device that has TCP 44818 open. The script will send a Request Identity Packet and once a response is received, it validates that it was a proper response to the command that was sent, and then will parse out the data. Information that is parsed includes Vendor ID, Device Type, Product name, Serial Number, Product code, Revision Number, as well as the Device IP.
epmd-info	Connects to Erlang Port Mapper Daemon (epmd) and retrieves a

	list of nodes with their respective port numbers.
eppc-enum-processes	Attempts to enumerate process info over the Apple Remote Event protocol. When accessing an application over the Apple Remote Event protocol the service responds with the uid and pid of the application, if it is running, prior to requesting authentication.
fcrdns	Performs a Forward-confirmed Reverse DNS lookup and reports anomalous results.
finger	Attempts to retrieve a list of usernames using the finger service.
firewalk	Tries to discover firewall rules using an IP TTL expiration technique known as firewalking.
firewall-bypass	Detects a vulnerability in netfilter and other firewalls that use helpers to dynamically open ports for protocols such as ftp and sip.
flume-master-info	Retrieves information from Flume master HTTP pages.
freelancer-info	Detects the Freelancer game server (FLServer.exe) service by sending a status query UDP probe.
ftp-anon	Checks if an FTP server allows anonymous logins.
ftp-bounce	Checks to see if an FTP server allows port scanning using the FTP bounce method.
ftp-brute	Performs brute force password auditing against FTP servers.
ftp-libopie	Checks if an FTPd is prone to CVE-2010-1938 (OPIE off-by-one stack overflow), a vulnerability discovered by Maksymilian Arciemowicz and Adam "pi3" Zabrocki. See the advisory at http://nmap.org/r/fbsd-sa-opie. Be advised that, if launched against a vulnerable host, this script will crash the FTPd.
ftp-proftpd-backdoor	Tests for the presence of the ProFTPD 1.3.3c backdoor reported as OSVDB-ID 69562. This script attempts to exploit the backdoor using the innocuous `id` command by default, but that can be changed with the `ftp-proftpd-backdoor.cmd` script argument.
ftp-vsftpd-backdoor	Tests for the presence of the vsFTPd 2.3.4 backdoor reported on

	2011-07-04 (CVE-2011-2523). This script attempts to exploit the backdoor using the innocuous `id` command by default, but that can be changed with the `exploit.cmd` or `ftp-vsftpd-backdoor.cmd` script arguments.
ftp-vuln-cve2010-4221	Checks for a stack-based buffer overflow in the ProFTPD server, version between 1.3.2rc3 and 1.3.3b. By sending a large number of TELNET_IAC escape sequence, the proftpd process miscalculates the buffer length, and a remote attacker will be able to corrupt the stack and execute arbitrary code within the context of the proftpd process (CVE-2010-4221). Authentication is not required to exploit this vulnerability.
ganglia-info	Retrieves system information (OS version, available memory, etc.) from a listening Ganglia Monitoring Daemon or Ganglia Meta Daemon.
giop-info	Queries a CORBA naming server for a list of objects.
gkrellm-info	Queries a GKRellM service for monitoring information. A single round of collection is made, showing a snapshot of information at the time of the request.
gopher-ls	Lists files and directories at the root of a gopher service.
gpsd-info	Retrieves GPS time, coordinates and speed from the GPSD network daemon.
hadoop-datanode-info	Discovers information such as log directories from an Apache Hadoop DataNode HTTP status page.
hadoop-jobtracker-info	Retrieves information from an Apache Hadoop JobTracker HTTP status page.
hadoop-namenode-info	Retrieves information from an Apache Hadoop NameNode HTTP status page.
hadoop-secondary-namenode-info	Retrieves information from an Apache Hadoop secondary NameNode HTTP status page.
hadoop-tasktracker-info	Retrieves information from an Apache Hadoop TaskTracker HTTP status page.
hbase-master-info	Retrieves information from an Apache HBase (Hadoop database)

	master HTTP status page.
hbase-region-info	Retrieves information from an Apache HBase (Hadoop database) region server HTTP status page.
hddtemp-info	Reads hard disk information (such as brand, model, and sometimes temperature) from a listening hddtemp service.
hnap-info	Retrieve hardwares details and configuration information utilizing HNAP, the "Home Network Administration Protocol". It is an HTTP-Simple Object Access Protocol (SOAP)-based protocol which allows for remote topology discovery, configuration, and management of devices (routers, cameras, PCs, NAS, etc.)
hostmap-bfk	Discovers hostnames that resolve to the target's IP address by querying the online database at http://www.bfk.de/bfk_dnslogger.html.
hostmap-ip2hosts	Finds hostnames that resolve to the target's IP address by querying the online database: • http://www.ip2hosts.com (Bing Search Results)
hostmap-robtex	Discovers hostnames that resolve to the target's IP address by querying the online Robtex service at http://ip.robtex.com/.
http-adobe-coldfusion-apsa1301	Attempts to exploit an authentication bypass vulnerability in Adobe Coldfusion servers to retrieve a valid administrator's session cookie.
http-affiliate-id	Grabs affiliate network IDs (e.g. Google AdSense or Analytics, Amazon Associates, etc.) from a web page. These can be used to identify pages with the same owner.
http-apache-negotiation	Checks if the target http server has mod_negotiation enabled. This feature can be leveraged to find hidden resources and spider a web site using fewer requests.
http-auth	Retrieves the authentication scheme and realm of a web service that requires authentication.
http-auth-finder	Spiders a web site to find web pages requiring form-based or HTTP-based authentication. The results are returned in a table with each url and the detected method.

http-avaya-ipoffice-users	Attempts to enumerate users in Avaya IP Office systems 7.x.
http-awstatstotals-exec	Exploits a remote code execution vulnerability in Awstats Totals 1.0 up to 1.14 and possibly other products based on it (CVE: 2008-3922).
http-axis2-dir-traversal	Exploits a directory traversal vulnerability in Apache Axis2 version 1.4.1 by sending a specially crafted request to the parameter `xsd` (OSVDB-59001). By default it will try to retrieve the configuration file of the Axis2 service `'/conf/axis2.xml'` using the path `'/axis2/services/'` to return the username and password of the admin account.
http-backup-finder	Spiders a website and attempts to identify backup copies of discovered files. It does so by requesting a number of different combinations of the filename (eg. index.bak, index.html~, copy of index.html).
http-barracuda-dir-traversal	Attempts to retrieve the configuration settings from a Barracuda Networks Spam & Virus Firewall device using the directory traversal vulnerability described at http://seclists.org/fulldisclosure/2010/Oct/119.
http-brute	Performs brute force password auditing against http basic, digest and ntlm authentication.
http-cakephp-version	Obtains the CakePHP version of a web application built with the CakePHP framework by fingerprinting default files shipped with the CakePHP framework.
http-chrono	Measures the time a website takes to deliver a web page and returns the maximum, minimum and average time it took to fetch a page.
http-cisco-anyconnect	Connect as Cisco AnyConnect client to a Cisco SSL VPN and retrieves version and tunnel information.
http-coldfusion-subzero	Attempts to retrieve version, absolute path of administration panel and the file 'password.properties' from vulnerable installations of ColdFusion 9 and 10.
http-comments-displayer	Extracts and outputs HTML and JavaScript comments from HTTP responses.
http-config-backup	Checks for backups and swap files of common content

	management system and web server configuration files.
http-cors	Tests an http server for Cross-Origin Resource Sharing (CORS), a way for domains to explicitly opt in to having certain methods invoked by another domain.
http-cross-domain-policy	Checks the cross-domain policy file (/crossdomain.xml) and the client-acces-policy file (/clientaccesspolicy.xml) in web applications and lists the trusted domains. Overly permissive settings enable Cross Site Request Forgery attacks and may allow attackers to access sensitive data. This script is useful to detect permissive configurations and possible domain names available for purchase to exploit the application.
http-csrf	This script detects Cross Site Request Forgeries (CSRF) vulnerabilities.
http-date	Gets the date from HTTP-like services. Also prints how much the date differs from local time. Local time is the time the HTTP request was sent, so the difference includes at least the duration of one RTT.
http-default-accounts	Tests for access with default credentials used by a variety of web applications and devices.
http-devframework	
http-dlink-backdoor	Detects a firmware backdoor on some D-Link routers by changing the User-Agent to a "secret" value. Using the "secret" User-Agent bypasses authentication and allows admin access to the router.
http-dombased-xss	It looks for places where attacker-controlled information in the DOM may be used to affect JavaScript execution in certain ways. The attack is explained here: http://www.webappsec.org/projects/articles/071105.shtml
http-domino-enum-passwords	Attempts to enumerate the hashed Domino Internet Passwords that are (by default) accessible by all authenticated users. This script can also download any Domino ID Files attached to the Person document. Passwords are presented in a form suitable for running in John the Ripper.
http-drupal-enum	Enumerates the installed Drupal modules/themes by using a list of known modules and themes.
http-drupal-enum-users	Enumerates Drupal users by exploiting an information disclosure

	vulnerability in Views, Drupal's most popular module.
http-enum	Enumerates directories used by popular web applications and servers.
http-errors	This script crawls through the website and returns any error pages.
http-exif-spider	Spiders a site's images looking for interesting exif data embedded in .jpg files. Displays the make and model of the camera, the date the photo was taken, and the embedded geotag information.
http-favicon	Gets the favicon ("favorites icon") from a web page and matches it against a database of the icons of known web applications. If there is a match, the name of the application is printed; otherwise the MD5 hash of the icon data is printed.
http-feed	This script crawls through the website to find any rss or atom feeds.
http-fetch	The script is used to fetch files from servers.
http-fileupload-exploiter	Exploits insecure file upload forms in web applications using various techniques like changing the Content-type header or creating valid image files containing the payload in the comment.
http-form-brute	Performs brute force password auditing against http form-based authentication.
http-form-fuzzer	Performs a simple form fuzzing against forms found on websites. Tries strings and numbers of increasing length and attempts to determine if the fuzzing was successful.
http-frontpage-login	Checks whether target machines are vulnerable to anonymous Frontpage login.
http-generator	Displays the contents of the "generator" meta tag of a web page (default: /) if there is one.
http-git	Checks for a Git repository found in a website's document root /.git/<something>) and retrieves as much repo information as possible, including language/framework, remotes, last commit message, and repository description.
http-gitweb-projects-enum	Retrieves a list of Git projects, owners and descriptions from a

	gitweb (web interface to the Git revision control system).
http-google-malware	Checks if hosts are on Google's blacklist of suspected malware and phishing servers. These lists are constantly updated and are part of Google's Safe Browsing service.
http-grep	Spiders a website and attempts to match all pages and urls against a given string. Matches are counted and grouped per url under which they were discovered.
http-headers	Performs a HEAD request for the root folder ("/") of a web server and displays the HTTP headers returned.
http-huawei-hg5xx-vuln	Detects Huawei modems models HG530x, HG520x, HG510x (and possibly others...) vulnerable to a remote credential and information disclosure vulnerability. It also extracts the PPPoE credentials and other interesting configuration values.
http-icloud-findmyiphone	Retrieves the locations of all "Find my iPhone" enabled iOS devices by querying the MobileMe web service (authentication required).
http-icloud-sendmsg	Sends a message to a iOS device through the Apple MobileMe web service. The device has to be registered with an Apple ID using the Find My Iphone application.
http-iis-short-name-brute	Attempts to brute force the 8.3 filenames (commonly known as short names) of files and directories in the root folder of vulnerable IIS servers. This script is an implementation of the PoC "iis shortname scanner".
http-iis-webdav-vuln	Checks for a vulnerability in IIS 5.1/6.0 that allows arbitrary users to access secured WebDAV folders by searching for a password-protected folder and attempting to access it. This vulnerability was patched in Microsoft Security Bulletin MS09-020, http://nmap.org/r/ms09-020.
http-joomla-brute	Performs brute force password auditing against Joomla web CMS installations.
http-litespeed-sourcecode-download	Exploits a null-byte poisoning vulnerability in Litespeed Web Servers 4.0.x before 4.0.15 to retrieve the target script's source code by sending a HTTP request with a null byte followed by a .txt file extension (CVE-2010-2333).
http-ls	Shows the content of an "index" Web page.

http-majordomo2-dir-traversal	Exploits a directory traversal vulnerability existing in Majordomo2 to retrieve remote files. (CVE-2011-0049).
http-malware-host	Looks for signature of known server compromises.
http-method-tamper	Attempts to bypass password protected resources (HTTP 401 status) by performing HTTP verb tampering. If an array of paths to check is not set, it will crawl the web server and perform the check against any password protected resource that it finds.
http-methods	Finds out what options are supported by an HTTP server by sending an OPTIONS request. Lists potentially risky methods. It tests those methods not mentioned in the OPTIONS headers individually and sees if they are implemented. Any output other than 501/405 suggests that the method is if not in the range 400 to 600. If the response falls under that range then it is compared to the response from a randomly generated method.
http-mobileversion-checker	Checks if the website holds a mobile version.
http-ntlm-info	This script enumerates information from remote HTTP services with NTLM authentication enabled.
http-open-proxy	Checks if an HTTP proxy is open.
http-open-redirect	Spiders a website and attempts to identify open redirects. Open redirects are handlers which commonly take a URL as a parameter and responds with a http redirect (3XX) to the target. Risks of open redirects are described at http://cwe.mitre.org/data/definitions/601.html.
http-passwd	Checks if a web server is vulnerable to directory traversal by attempting to retrieve `/etc/passwd` or `\boot.ini`.
http-php-version	Attempts to retrieve the PHP version from a web server. PHP has a number of magic queries that return images or text that can vary with the PHP version. This script uses the following queries: • `/?=PHPE9568F36-D428-11d2-A769-00AA001ACF42`: gets a GIF logo, which changes on April Fool's Day. • `/?=PHPB8B5F2A0-3C92-11d3-A3A9-4C7B08C10000`: gets an HTML credits page.

http-phpmyadmin-dir-traversal	Exploits a directory traversal vulnerability in phpMyAdmin 2.6.4-pl1 (and possibly other versions) to retrieve remote files on the web server.
http-phpself-xss	Crawls a web server and attempts to find PHP files vulnerable to reflected cross site scripting via the variable `$_SERVER["PHP_SELF"]`.
http-proxy-brute	Performs brute force password guessing against HTTP proxy servers.
http-put	Uploads a local file to a remote web server using the HTTP PUT method. You must specify the filename and URL path with NSE arguments.
http-qnap-nas-info	Attempts to retrieve the model, firmware version, and enabled services from a QNAP Network Attached Storage (NAS) device.
http-referer-checker	Informs about cross-domain include of scripts. Websites that include external javascript scripts are delegating part of their security to third-party entities.
http-rfi-spider	Crawls webservers in search of RFI (remote file inclusion) vulnerabilities. It tests every form field it finds and every parameter of a URL containing a query.
http-robots.txt	Checks for disallowed entries in `/robots.txt` on a web server.
http-robtex-reverse-ip	Obtains up to 100 forward DNS names for a target IP address by querying the Robtex service (http://www.robtex.com/ip/).
http-robtex-shared-ns	Finds up to 100 domain names which use the same name server as the target by querying the Robtex service at http://www.robtex.com/dns/.
http-server-header	Uses the HTTP Server header for missing version info. This is currently infeasible with version probes because of the need to match non-HTTP services correctly.
http-shellshock	Attempts to exploit the "shellshock" vulnerability (CVE-2014-6271 and CVE-2014-7169) in web applications.
http-sitemap-generator	Spiders a web server and displays its directory structure along with number and types of files in each folder. Note that files listed as having an 'Other' extension are ones that have no

	extension or that are a root document.
http-slowloris	Tests a web server for vulnerability to the Slowloris DoS attack by launching a Slowloris attack.
http-slowloris-check	Tests a web server for vulnerability to the Slowloris DoS attack without actually launching a DoS attack.
http-sql-injection	Spiders an HTTP server looking for URLs containing queries vulnerable to an SQL injection attack. It also extracts forms from found websites and tries to identify fields that are vulnerable.
http-stored-xss	Unfiltered '>' (greater than sign). An indication of potential XSS vulnerability.
http-svn-enum	Enumerates users of a Subversion repository by examining logs of most recent commits.
http-svn-info	Requests information from a Subversion repository.
http-title	Shows the title of the default page of a web server.
http-tplink-dir-traversal	Exploits a directory traversal vulnerability existing in several TP-Link wireless routers. Attackers may exploit this vulnerability to read any of the configuration and password files remotely and without authentication.
http-trace	Sends an HTTP TRACE request and shows if the method TRACE is enabled. If debug is enabled, it returns the header fields that were modified in the response.
http-traceroute	Exploits the Max-Forwards HTTP header to detect the presence of reverse proxies.
http-unsafe-output-escaping	Spiders a website and attempts to identify output escaping problems where content is reflected back to the user. This script locates all parameters, ?x=foo&y=bar and checks if the values are reflected on the page. If they are indeed reflected, the script will try to insert ghz>hzx"zxc'xcv and check which (if any) characters were reflected back onto the page without proper html escaping. This is an indication of potential XSS vulnerability.
http-useragent-tester	Checks if various crawling utilities are allowed by the host.
http-userdir-enum	Attempts to enumerate valid usernames on web servers running

	with the mod_userdir module or similar enabled.
http-vhosts	Searches for web virtual hostnames by making a large number of HEAD requests against http servers using common hostnames.
http-virustotal	Checks whether a file has been determined as malware by Virustotal. Virustotal is a service that provides the capability to scan a file or check a checksum against a number of the major antivirus vendors. The script uses the public API which requires a valid API key and has a limit on 4 queries per minute. A key can be acquired by registering as a user on the virustotal web page: • http://www.virustotal.com
http-vlcstreamer-ls	Connects to a VLC Streamer helper service and lists directory contents. The VLC Streamer helper service is used by the iOS VLC Streamer application to enable streaming of multimedia content from the remote server to the device.
http-vmware-path-vuln	Checks for a path-traversal vulnerability in VMWare ESX, ESXi, and Server (CVE-2009-3733).
http-vuln-cve2006-3392	Exploits a file disclosure vulnerability in Webmin (CVE-2006-3392)
http-vuln-cve2009-3960	Exploits cve-2009-3960 also known as Adobe XML External Entity Injection.
http-vuln-cve2010-0738	Tests whether a JBoss target is vulnerable to jmx console authentication bypass (CVE-2010-0738).
http-vuln-cve2010-2861	Executes a directory traversal attack against a ColdFusion server and tries to grab the password hash for the administrator user. It then uses the salt value (hidden in the web page) to create the SHA1 HMAC hash that the web server needs for authentication as admin. You can pass this value to the ColdFusion server as the admin without cracking the password hash.
http-vuln-cve2011-3192	Detects a denial of service vulnerability in the way the Apache web server handles requests for multiple overlapping/simple ranges of a page.
http-vuln-cve2011-3368	Tests for the CVE-2011-3368 (Reverse Proxy Bypass) vulnerability in Apache HTTP server's reverse proxy mode. The

	script will run 3 tests: • the loopback test, with 3 payloads to handle different rewrite rules • the internal hosts test. According to Contextis, we expect a delay before a server error. • The external website test. This does not mean that you can reach a LAN ip, but this is a relevant issue anyway.
http-vuln-cve2012-1823	Detects PHP-CGI installations that are vulnerable to CVE-2012-1823, This critical vulnerability allows attackers to retrieve source code and execute code remotely.
http-vuln-cve2013-0156	Detects Ruby on Rails servers vulnerable to object injection, remote command executions and denial of service attacks. (CVE-2013-0156)
http-vuln-cve2013-7091	An 0 day was released on the 6th December 2013 by rubina119, and was patched in Zimbra 7.2.6.
http-vuln-cve2014-2126	Detects whether the Cisco ASA appliance is vulnerable to the Cisco ASA ASDM Privilege Escalation Vulnerability (CVE-2014-2126).
http-vuln-cve2014-2127	Detects whether the Cisco ASA appliance is vulnerable to the Cisco ASA SSL VPN Privilege Escalation Vulnerability (CVE-2014-2127).
http-vuln-cve2014-2128	Detects whether the Cisco ASA appliance is vulnerable to the Cisco ASA SSL VPN Authentication Bypass Vulnerability (CVE-2014-2128).
http-vuln-cve2014-2129	Detects whether the Cisco ASA appliance is vulnerable to the Cisco ASA SIP Denial of Service Vulnerability (CVE-2014-2129).
http-vuln-cve2015-1427	This script attempts to detect a vulnerability, CVE-2015-1427, which allows attackers to leverage features of this API to gain unauthenticated remote code execution (RCE).
http-vuln-cve2015-1635	Checks for a remote code execution vulnerability (MS15-034) in Microsoft Windows systems (CVE2015-2015-1635).
http-vuln-misfortune-cookie	Detects the RomPager 4.07 Misfortune Cookie vulnerability by safely exploiting it.

http-vuln-wnr1000-creds	A vulnerability has been discovered in WNR 1000 series that allows an attacker to retrieve administrator credentials with the router interface. Tested On Firmware Version(s): V1.0.2.60_60.0.86 (Latest) and V1.0.2.54_60.0.82NA
http-waf-detect	Attempts to determine whether a web server is protected by an IPS (Intrusion Prevention System), IDS (Intrusion Detection System) or WAF (Web Application Firewall) by probing the web server with malicious payloads and detecting changes in the response code and body.
http-waf-fingerprint	Tries to detect the presence of a web application firewall and its type and version.
http-webdav-scan	A script to detect WebDAV installations. Uses the OPTIONS and PROPFIND methods.
http-wordpress-brute	performs brute force password auditing against Wordpress CMS/blog installations.
http-wordpress-enum	Enumerates themes and plugins of Wordpress installations. The script can also detect outdated plugins by comparing version numbers with information pulled from api.wordpress.org.
http-wordpress-users	Enumerates usernames in Wordpress blog/CMS installations by exploiting an information disclosure vulnerability existing in versions 2.6, 3.1, 3.1.1, 3.1.3 and 3.2-beta2 and possibly others.
http-xssed	This script searches the xssed.com database and outputs the result.
iax2-brute	Performs brute force password auditing against the Asterisk IAX2 protocol. Guessing fails when a large number of attempts is made due to the maxcallnumber limit (default 2048). In case your getting "ERROR: Too many retries, aborted ..." after a while, this is most likely what's happening. In order to avoid this problem try: - reducing the size of your dictionary - use the brute delay option to introduce a delay between guesses - split the guessing up in chunks and wait for a while between them
iax2-version	Detects the UDP IAX2 service.
icap-info	Tests a list of known ICAP service names and prints information about any it detects. The Internet Content Adaptation Protocol (ICAP) is used to extend transparent proxy servers and is

	generally used for content filtering and antivirus scanning.
ike-version	Obtains information (such as vendor and device type where available) from an IKE service by sending four packets to the host. This scripts tests with both Main and Aggressive Mode and sends multiple transforms per request.
imap-brute	Performs brute force password auditing against IMAP servers using either LOGIN, PLAIN, CRAM-MD5, DIGEST-MD5 or NTLM authentication.
imap-capabilities	Retrieves IMAP email server capabilities.
informix-brute	Performs brute force password auditing against IBM Informix Dynamic Server.
informix-query	Runs a query against IBM Informix Dynamic Server using the given authentication credentials (see also: informix-brute).
informix-tables	Retrieves a list of tables and column definitions for each database on an Informix server.
ip-forwarding	Detects whether the remote device has ip forwarding or "Internet connection sharing" enabled, by sending an ICMP echo request to a given target using the scanned host as default gateway.
ip-geolocation-geobytes	Tries to identify the physical location of an IP address using the Geobytes geolocation web service (http://www.geobytes.com/iplocator.htm). The limit of lookups using this service is 20 requests per hour. Once the limit is reached, an nmap.registry["ip-geolocation-geobytes"].blocked boolean is set so no further requests are made during a scan.
ip-geolocation-geoplugin	Tries to identify the physical location of an IP address using the Geoplugin geolocation web service (http://www.geoplugin.com/). There is no limit on lookups using this service.
ip-geolocation-ipinfodb	Tries to identify the physical location of an IP address using the IPInfoDB geolocation web service (http://ipinfodb.com/ip_location_api.php).
ip-geolocation-maxmind	Tries to identify the physical location of an IP address using a Geolocation Maxmind database file (available from http://www.maxmind.com/app/ip-location). This script supports queries using all Maxmind databases that are supported by their

	API including the commercial ones.
ipidseq	Classifies a host's IP ID sequence (test for susceptibility to idle scan).
ipv6-node-info	Obtains hostnames, IPv4 and IPv6 addresses through IPv6 Node Information Queries.
ipv6-ra-flood	Generates a flood of Router Advertisements (RA) with random source MAC addresses and IPv6 prefixes. Computers, which have stateless autoconfiguration enabled by default (every major OS), will start to compute IPv6 suffix and update their routing table to reflect the accepted announcement. This will cause 100% CPU usage on Windows and platforms, preventing to process other application requests.
irc-botnet-channels	Checks an IRC server for channels that are commonly used by malicious botnets.
irc-brute	Performs brute force password auditing against IRC (Internet Relay Chat) servers.
irc-info	Gathers information from an IRC server.
irc-sasl-brute	Performs brute force password auditing against IRC (Internet Relay Chat) servers supporting SASL authentication.
irc-unrealircd-backdoor	Checks if an IRC server is backdoored by running a time-based command (ping) and checking how long it takes to respond.
iscsi-brute	Performs brute force password auditing against iSCSI targets.
iscsi-info	Collects and displays information from remote iSCSI targets.
isns-info	Lists portals and iSCSI nodes registered with the Internet Storage Name Service (iSNS).
jdwp-exec	Attempts to exploit java's remote debugging port. When remote debugging port is left open, it is possible to inject java bytecode and achieve remote code execution. This script abuses this to inject and execute a Java class file that executes the supplied shell command and returns its output.
jdwp-info	Attempts to exploit java's remote debugging port. When remote debugging port is left open, it is possible to inject java bytecode and achieve remote code execution. This script injects and

	execute a Java class file that returns remote system information.
jdwp-inject	Attempts to exploit java's remote debugging port. When remote debugging port is left open, it is possible to inject java bytecode and achieve remote code execution. This script allows injection of arbitrary class files.
jdwp-version	Detects the Java Debug Wire Protocol. This protocol is used by Java programs to be debugged via the network. It should not be open to the public Internet, as it does not provide any security against malicious attackers who can inject their own bytecode into the debugged process.
knx-gateway-discover	Discovers KNX gateways by sending a KNX Search Request to the multicast address 224.0.23.12 including a UDP payload with destination port 3671. KNX gateways will respond with a KNX Search Response including various information about the gateway, such as KNX address and supported services.
knx-gateway-info	Identifies a KNX gateway on UDP port 3671 by sending a KNX Description Request.
krb5-enum-users	Discovers valid usernames by brute force querying likely usernames against a Kerberos service. When an invalid username is requested the server will respond using the Kerberos error code KRB5KDC_ERR_C_PRINCIPAL_UNKNOWN, allowing us to determine that the user name was invalid. Valid user names will illicit either the TGT in a AS-REP response or the error KRB5KDC_ERR_PREAUTH_REQUIRED, signaling that the user is required to perform pre authentication.
ldap-brute	Attempts to brute-force LDAP authentication. By default it uses the built-in username and password lists. In order to use your own lists use the `userdb` and `passdb` script arguments.
ldap-novell-getpass	Universal Password enables advanced password policies, including extended characters in passwords, synchronization of passwords from eDirectory to other systems, and a single password for all access to eDirectory.
ldap-rootdse	Retrieves the LDAP root DSA-specific Entry (DSE)
ldap-search	Attempts to perform an LDAP search and returns all matches.
lexmark-config	Retrieves configuration information from a Lexmark S300-S400

	printer.
llmnr-resolve	Resolves a hostname by using the LLMNR (Link-Local Multicast Name Resolution) protocol.
lltd-discovery	Uses the Microsoft LLTD protocol to discover hosts on a local network.
maxdb-info	Retrieves version and database information from a SAP Max DB database.
mcafee-epo-agent	Check if ePO agent is running on port 8081 or port identified as ePO Agent port.
membase-brute	Performs brute force password auditing against Couchbase Membase servers.
membase-http-info	Retrieves information (hostname, OS, uptime, etc.) from the CouchBase Web Administration port. The information retrieved by this script does not require any credentials.
memcached-info	Retrieves information (including system architecture, process ID, and server time) from distributed memory object caching system memcached.
metasploit-info	Gathers info from the Metasploit rpc service. It requires a valid login pair. After authentication it tries to determine Metasploit version and deduce the OS type. Then it creates a new console and executes few commands to get additional info.
metasploit-msgrpc-brute	Performs brute force username and password auditing against Metasploit msgrpc interface.
metasploit-xmlrpc-brute	Performs brute force password auditing against a Metasploit RPC server using the XMLRPC protocol.
mikrotik-routeros-brute	Performs brute force password auditing against Mikrotik RouterOS devices with the API RouterOS interface enabled.
mmouse-brute	Performs brute force password auditing against the RPA Tech Mobile Mouse servers.

mmouse-exec	Connects to an RPA Tech Mobile Mouse server, starts an application and sends a sequence of keys to it. Any application that the user has access to can be started and the key sequence is sent to the application after it has been started.
modbus-discover	Enumerates SCADA Modbus slave ids (sids) and collects their device information.
mongodb-brute	Performs brute force password auditing against the MongoDB database.
mongodb-databases	Attempts to get a list of tables from a MongoDB database.
mongodb-info	Attempts to get build info and server status from a MongoDB database.
mrinfo	Queries targets for multicast routing information.
ms-sql-brute	Performs password guessing against Microsoft SQL Server (ms-sql). Works best in conjunction with the `broadcast-ms-sql-discover` script.
ms-sql-config	Queries Microsoft SQL Server (ms-sql) instances for a list of databases, linked servers, and configuration settings.
ms-sql-dac	Queries the Microsoft SQL Browser service for the DAC (Dedicated Admin Connection) port of a given (or all) SQL Server instance. The DAC port is used to connect to the database instance when normal connection attempts fail, for example, when server is hanging, out of memory or in other bad states. In addition, the DAC port provides an admin with access to system objects otherwise not accessible over normal connections.
ms-sql-dump-hashes	Dumps the password hashes from an MS-SQL server in a format suitable for cracking by tools such as John-the-ripper. In order to do so the user needs to have the appropriate DB privileges.
ms-sql-empty-password	Attempts to authenticate to Microsoft SQL Servers using an empty password for the sysadmin (sa) account.
ms-sql-hasdbaccess	Queries Microsoft SQL Server (ms-sql) instances for a list of databases a user has access to.
ms-sql-info	Attempts to determine configuration and version information for Microsoft SQL Server instances.

ms-sql-query	Runs a query against Microsoft SQL Server (ms-sql).
ms-sql-tables	Queries Microsoft SQL Server (ms-sql) for a list of tables per database.
ms-sql-xp-cmdshell	Attempts to run a command using the command shell of Microsoft SQL Server (ms-sql).
msrpc-enum	Queries an MSRPC endpoint mapper for a list of mapped services and displays the gathered information.
mtrace	Queries for the multicast path from a source to a destination host.
murmur-version	Detects the Murmur service (server for the Mumble voice communication client) versions 1.2.X.
mysql-audit	Audits MySQL database server security configuration against parts of the CIS MySQL v1.0.2 benchmark (the engine can be used for other MySQL audits by creating appropriate audit files).
mysql-brute	Performs password guessing against MySQL.
mysql-databases	Attempts to list all databases on a MySQL server.
mysql-dump-hashes	Dumps the password hashes from an MySQL server in a format suitable for cracking by tools such as John the Ripper. Appropriate DB privileges (root) are required.
mysql-empty-password	Checks for MySQL servers with an empty password for `root` or `anonymous`.
mysql-enum	Performs valid-user enumeration against MySQL server using a bug discovered and published by Kingcope (http://seclists.org/fulldisclosure/2012/Dec/9).
mysql-info	Connects to a MySQL server and prints information such as the protocol and version numbers, thread ID, status, capabilities, and the password salt.
mysql-query	Runs a query against a MySQL database and returns the results as a table.
mysql-users	Attempts to list all users on a MySQL server.
mysql-variables	Attempts to show all variables on a MySQL server.

mysql-vuln-cve2012-2122	
nat-pmp-info	Gets the routers WAN IP using the NAT Port Mapping Protocol (NAT-PMP). The NAT-PMP protocol is supported by a broad range of routers including: - Apple AirPort Express - Apple AirPort Extreme - Apple Time Capsule - DD-WRT - OpenWrt v8.09 or higher, with MiniUPnP daemon - pfSense v2.0 - Tarifa (firmware) (Linksys WRT54G/GL/GS) - Tomato Firmware v1.24 or higher. (Linksys WRT54G/GL/GS and many more) - Peplink Balance
nat-pmp-mapport	Maps a WAN port on the router to a local port on the client using the NAT Port Mapping Protocol (NAT-PMP). It supports the following operations: o map - maps a new external port on the router to an internal port of the requesting IP o unmap - unmaps a previously mapped port for the requesting IP o unmapall - unmaps all previously mapped ports for the requesting IP
nbstat	Attempts to retrieve the target's NetBIOS names and MAC address.
ncp-enum-users	Retrieves a list of all eDirectory users from the Novell NetWare Core Protocol (NCP) service.
ncp-serverinfo	Retrieves eDirectory server information (OS version, server name, mounts, etc.) from the Novell NetWare Core Protocol (NCP) service.
ndmp-fs-info	Lists remote file systems by querying the remote device using the Network Data Management Protocol (ndmp). NDMP is a protocol intended to transport data between a NAS device and the backup device, removing the need for the data to pass through the backup server. The following products are known to support the protocol: • Amanda • Bacula • CA Arcserve • CommVault Simpana • EMC Networker • Hitachi Data Systems • IBM Tivoli • Quest Software Netvault Backup • Symantec Netbackup

	• Symantec Backup Exec
ndmp-version	Retrieves version information from the remote Network Data Management Protocol (ndmp) service. NDMP is a protocol intended to transport data between a NAS device and the backup device, removing the need for the data to pass through the backup server. The following products are known to support the protocol: • Amanda • Bacula • CA Arcserve • CommVault Simpana • EMC Networker • Hitachi Data Systems • IBM Tivoli • Quest Software Netvault Backup • Symantec Netbackup • Symantec Backup Exec
nessus-brute	Performs brute force password auditing against a Nessus vulnerability scanning daemon using the NTP 1.2 protocol.
nessus-xmlrpc-brute	Performs brute force password auditing against a Nessus vulnerability scanning daemon using the XMLRPC protocol.
netbus-auth-bypass	Checks if a NetBus server is vulnerable to an authentication bypass vulnerability which allows full access without knowing the password.
netbus-brute	Performs brute force password auditing against the Netbus backdoor ("remote administration") service.
netbus-info	Opens a connection to a NetBus server and extracts information about the host and the NetBus service itself.
netbus-version	Extends version detection to detect NetBuster, a honeypot service that mimes NetBus.
nexpose-brute	Performs brute force password auditing against a Nexpose vulnerability scanner using the API 1.1.
nfs-ls	Attempts to get useful information about files from NFS exports. The output is intended to resemble the output of `ls`.

nfs-showmount	Shows NFS exports, like the `showmount -e` command.
nfs-statfs	Retrieves disk space statistics and information from a remote NFS share. The output is intended to resemble the output of `df`.
nping-brute	Performs brute force password auditing against an Nping Echo service.
nrpe-enum	Queries Nagios Remote Plugin Executor (NRPE) daemons to obtain information such as load averages, process counts, logged in user information, etc.
ntp-info	Gets the time and configuration variables from an NTP server. We send two requests: a time request and a "read variables" (opcode 2) control message. Without verbosity, the script shows the time and the value of the `version`, `processor`, `system`, `refid`, and `stratum` variables. With verbosity, all variables are shown.
ntp-monlist	Obtains and prints an NTP server's monitor data.
omp2-brute	Performs brute force password auditing against the OpenVAS manager using OMPv2.
omp2-enum-targets	Attempts to retrieve the list of target systems and networks from an OpenVAS Manager server.
omron-info	This NSE script is used to send a FINS packet to a remote device. The script will send a Controller Data Read Command and once a response is received, it validates that it was a proper response to the command that was sent, and then will parse out the data.
openlookup-info	Parses and displays the banner information of an OpenLookup (network key-value store) server.
openvas-otp-brute	Performs brute force password auditing against a OpenVAS vulnerability scanner daemon using the OTP 1.0 protocol.
oracle-brute	Performs brute force password auditing against Oracle servers.
oracle-brute-stealth	Exploits the CVE-2012-3137 vulnerability, a weakness in Oracle's O5LOGIN authentication scheme. The vulnerability exists in Oracle 11g R1/R2 and allows linking the session key to a password hash. When initiating an authentication attempt as a

	valid user the server will respond with a session key and salt. Once received the script will disconnect the connection thereby not recording the login attempt. The session key and salt can then be used to brute force the users password.
oracle-enum-users	Attempts to enumerate valid Oracle user names against unpatched Oracle 11g servers (this bug was fixed in Oracle's October 2009 Critical Patch Update).
oracle-sid-brute	Guesses Oracle instance/SID names against the TNS-listener.
ovs-agent-version	Detects the version of an Oracle Virtual Server Agent by fingerprinting responses to an HTTP GET request and an XML-RPC method call.
p2p-conficker	Checks if a host is infected with Conficker.C or higher, based on Conficker's peer to peer communication.
path-mtu	Performs simple Path MTU Discovery to target hosts.
pcanywhere-brute	Performs brute force password auditing against the pcAnywhere remote access protocol.
pgsql-brute	Performs password guessing against PostgreSQL.
pjl-ready-message	Retrieves or sets the ready message on printers that support the Printer Job Language. This includes most PostScript printers that listen on port 9100. Without an argument, displays the current ready message. With the `pjl_ready_message` script argument, displays the old ready message and changes it to the message given.
pop3-brute	Tries to log into a POP3 account by guessing usernames and passwords.
pop3-capabilities	Retrieves POP3 email server capabilities.
pptp-version	Attempts to extract system information from the point-to-point tunneling protocol (PPTP) service.
qconn-exec	Attempts to identify whether a listening QNX QCONN daemon allows unauthenticated users to execute arbitrary operating system commands.
qscan	Repeatedly probe open and/or closed ports on a host to obtain a

	series of round-trip time values for each port. These values are used to group collections of ports which are statistically different from other groups. Ports being in different groups (or "families") may be due to network mechanisms such as port forwarding to machines behind a NAT.
quake1-info	Extracts information from Quake game servers and other game servers which use the same protocol.
quake3-info	Extracts information from a Quake3 game server and other games which use the same protocol.
quake3-master-getservers	Queries Quake3-style master servers for game servers (many games other than Quake 3 use this same protocol).
rdp-enum-encryption	Determines which Security layer and Encryption level is supported by the RDP service. It does so by cycling through all existing protocols and ciphers. When run in debug mode, the script also returns the protocols and ciphers that fail and any errors that were reported.
rdp-vuln-ms12-020	Checks if a machine is vulnerable to MS12-020 RDP vulnerability.
realvnc-auth-bypass	Checks if a VNC server is vulnerable to the RealVNC authentication bypass (CVE-2006-2369).
redis-brute	Performs brute force passwords auditing against a Redis key-value store.
redis-info	Retrieves information (such as version number and architecture) from a Redis key-value store.
resolveall	Resolves hostnames and adds every address (IPv4 or IPv6, depending on Nmap mode) to Nmap's target list. This differs from Nmap's normal host resolution process, which only scans the first address (A or AAAA record) returned for each host name.
reverse-index	Creates a reverse index at the end of scan output showing which hosts run a particular service. This is in addition to Nmap's normal output listing the services on each host.
rexec-brute	Performs brute force password auditing against the classic UNIX rexec (remote exec) service.

rfc868-time	Retrieves the day and time from the Time service.
riak-http-info	Retrieves information (such as node name and architecture) from a Basho Riak distributed database using the HTTP protocol.
rlogin-brute	Performs brute force password auditing against the classic UNIX rlogin (remote login) service. This script must be run in privileged mode on UNIX because it must bind to a low source port number.
rmi-dumpregistry	Connects to a remote RMI registry and attempts to dump all of its objects.
rmi-vuln-classloader	Tests whether Java rmiregistry allows class loading. The default configuration of rmiregistry allows loading classes from remote URLs, which can lead to remote code execution. The vendor (Oracle/Sun) classifies this as a design feature.
rpc-grind	Fingerprints the target RPC port to extract the target service, RPC number and version.
rpcap-brute	Performs brute force password auditing against the WinPcap Remote Capture Daemon (rpcap).
rpcap-info	Connects to the rpcap service (provides remote sniffing capabilities through WinPcap) and retrieves interface information. The service can either be setup to require authentication or not and also supports IP restrictions.
rpcinfo	Connects to portmapper and fetches a list of all registered programs. It then prints out a table including (for each program) the RPC program number, supported version numbers, port number and protocol, and program name.
rsync-brute	Performs brute force password auditing against the rsync remote file syncing protocol.
rsync-list-modules	Lists modules available for rsync (remote file sync) synchronization.
rtsp-methods	Determines which methods are supported by the RTSP (real time streaming protocol) server.
rtsp-url-brute	Attempts to enumerate RTSP media URLS by testing for common paths on devices such as surveillance IP cameras.

s7-info	Enumerates Siemens S7 PLC Devices and collects their device information. This script is based off PLCScan that was developed by Positive Research and Scadastrangelove (https://code.google.com/p/plcscan/). This script is meant to provide the same functionality as PLCScan inside of Nmap. Some of the information that is collected by PLCScan was not ported over; this information can be parsed out of the packets that are received.
samba-vuln-cve-2012-1182	Checks if target machines are vulnerable to the Samba heap overflow vulnerability CVE-2012-1182.
servicetags	Attempts to extract system information (OS, hardware, etc.) from the Sun Service Tags service agent (UDP port 6481).
sip-brute	Performs brute force password auditing against Session Initiation Protocol (SIP) accounts. This protocol is most commonly associated with VoIP sessions.
sip-call-spoof	Spoofs a call to a SIP phone and detects the action taken by the target (busy, declined, hung up, etc.)
sip-enum-users	Enumerates a SIP server's valid extensions (users).
sip-methods	Enumerates a SIP Server's allowed methods (INVITE, OPTIONS, SUBSCRIBE, etc.)
skypev2-version	Detects the Skype version 2 service.
smb-brute	Attempts to guess username/password combinations over SMB, storing discovered combinations for use in other scripts. Every attempt will be made to get a valid list of users and to verify each username before actually using them. When a username is discovered, besides being printed, it is also saved in the Nmap registry so other Nmap scripts can use it. That means that if you're going to run `smb-brute.nse`, you should run other `smb` scripts you want. This checks passwords in a case-insensitive way, determining case after a password is found, for Windows versions before Vista.
smb-enum-domains	Attempts to enumerate domains on a system, along with their policies. This generally requires credentials, except against Windows 2000. In addition to the actual domain, the "Builtin" domain is generally displayed. Windows returns this in the list of domains, but its policies don't appear to be used anywhere.

smb-enum-groups	Obtains a list of groups from the remote Windows system, as well as a list of the group's users. This works similarly to `enum.exe` with the `/G` switch.
smb-enum-processes	Pulls a list of processes from the remote server over SMB. This will determine all running processes, their process IDs, and their parent processes. It is done by querying the remote registry service, which is disabled by default on Vista; on all other Windows versions, it requires Administrator privileges.
smb-enum-sessions	Enumerates the users logged into a system either locally or through an SMB share. The local users can be logged on either physically on the machine, or through a terminal services session. Connections to a SMB share are, for example, people connected to fileshares or making RPC calls. Nmap's connection will also show up, and is generally identified by the one that connected "0 seconds ago".
smb-enum-shares	Attempts to list shares using the `srvsvc.NetShareEnumAll` MSRPC function and retrieve more information about them using `srvsvc.NetShareGetInfo`. If access to those functions is denied, a list of common share names are checked.
smb-enum-users	Attempts to enumerate the users on a remote Windows system, with as much information as possible, through two different techniques (both over MSRPC, which uses port 445 or 139; see `smb.lua`). The goal of this script is to discover all user accounts that exist on a remote system. This can be helpful for administration, by seeing who has an account on a server, or for penetration testing or network footprinting, by determining which accounts exist on a system.
smb-flood	Exhausts a remote SMB server's connection limit by by opening as many connections as we can. Most implementations of SMB have a hard global limit of 11 connections for user accounts and 10 connections for anonymous. Once that limit is reached, further connections are denied. This script exploits that limit by taking up all the connections and holding them.
smb-ls	Attempts to retrieve useful information about files shared on SMB volumes. The output is intended to resemble the output of the UNIX `ls` command.
smb-mbenum	Queries information managed by the Windows Master Browser.
smb-os-discovery	Attempts to determine the operating system, computer name,

	domain, workgroup, and current time over the SMB protocol (ports 445 or 139). This is done by starting a session with the anonymous account (or with a proper user account, if one is given; it likely doesn't make a difference); in response to a session starting, the server will send back all this information.
smb-print-text	Attempts to print text on a shared printer by calling Print Spooler Service RPC functions.
smb-psexec	Implements remote process execution similar to the Sysinternals' psexec tool, allowing a user to run a series of programs on a remote machine and read the output. This is great for gathering information about servers, running the same tool on a range of system, or even installing a backdoor on a collection of computers.
smb-security-mode	Returns information about the SMB security level determined by SMB.
smb-server-stats	Attempts to grab the server's statistics over SMB and MSRPC, which uses TCP ports 445 or 139.
smb-system-info	Pulls back information about the remote system from the registry. Getting all of the information requires an administrative account, although a user account will still get a lot of it. Guest probably won't get any, nor will anonymous. This goes for all operating systems, including Windows 2000.
smb-vuln-conficker	Detects Microsoft Windows systems infected by the Conficker worm. This check is dangerous and it may crash systems.
smb-vuln-cve2009-3103	Detects Microsoft Windows systems vulnerable to denial of service (CVE-2009-3103). This script will crash the service if it is vulnerable.
smb-vuln-ms06-025	Detects Microsoft Windows systems with Ras RPC service vulnerable to MS06-025.
smb-vuln-ms07-029	Detects Microsoft Windows systems with Dns Server RPC vulnerable to MS07-029.
smb-vuln-ms08-067	Detects Microsoft Windows systems vulnerable to the remote code execution vulnerability known as MS08-067. This check is dangerous and it may crash systems.
smb-vuln-ms10-054	Tests whether target machines are vulnerable to the ms10-054

	SMB remote memory corruption vulnerability.
smb-vuln-ms10-061	Tests whether target machines are vulnerable to ms10-061 Printer Spooler impersonation vulnerability.
smb-vuln-regsvc-dos	Checks if a Microsoft Windows 2000 system is vulnerable to a crash in regsvc caused by a null pointer dereference. This check will crash the service if it is vulnerable and requires a guest account or higher to work.
smbv2-enabled	Checks whether or not a server is running the SMBv2 protocol.
smtp-brute	Performs brute force password auditing against SMTP servers using either LOGIN, PLAIN, CRAM-MD5, DIGEST-MD5 or NTLM authentication.
smtp-commands	Attempts to use EHLO and HELP to gather the Extended commands supported by an SMTP server.
smtp-enum-users	Attempts to enumerate the users on a SMTP server by issuing the VRFY, EXPN or RCPT TO commands. The goal of this script is to discover all the user accounts in the remote system.
smtp-open-relay	Attempts to relay mail by issuing a predefined combination of SMTP commands. The goal of this script is to tell if a SMTP server is vulnerable to mail relaying.
smtp-strangeport	Checks if SMTP is running on a non-standard port.
smtp-vuln-cve2010-4344	Checks for and/or exploits a heap overflow within versions of Exim prior to version 4.69 (CVE-2010-4344) and a privilege escalation vulnerability in Exim 4.72 and prior (CVE-2010-4345).
smtp-vuln-cve2011-1720	Checks for a memory corruption in the Postfix SMTP server when it uses Cyrus SASL library authentication mechanisms (CVE-2011-1720). This vulnerability can allow denial of service and possibly remote code execution.
smtp-vuln-cve2011-1764	Checks for a format string vulnerability in the Exim SMTP server (version 4.70 through 4.75) with DomainKeys Identified Mail (DKIM) support (CVE-2011-1764). The DKIM logging mechanism did not use format string specifiers when logging some parts of the DKIM-Signature header field. A remote attacker who is able to send emails, can exploit this vulnerability and execute arbitrary code with the privileges of the Exim

	daemon.
sniffer-detect	Checks if a target on a local Ethernet has its network card in promiscuous mode.
snmp-brute	Attempts to find an SNMP community string by brute force guessing.
snmp-hh3c-logins	Attempts to enumerate Huawei / HP/H3C Locally Defined Users through the hh3c-user.mib OID
snmp-info	Extracts basic information from an SNMPv3 GET request. The same probe is used here as in the service version detection scan.
snmp-interfaces	Attempts to enumerate network interfaces through SNMP.
snmp-ios-config	Attempts to downloads Cisco router IOS configuration files using SNMP RW (v1) and display or save them.
snmp-netstat	Attempts to query SNMP for a netstat like output. The script can be used to identify and automatically add new targets to the scan by supplying the newtargets script argument.
snmp-processes	Attempts to enumerate running processes through SNMP.
snmp-sysdescr	Attempts to extract system information from an SNMP version 1 service.
snmp-win32-services	Attempts to enumerate Windows services through SNMP.
snmp-win32-shares	Attempts to enumerate Windows Shares through SNMP.
snmp-win32-software	Attempts to enumerate installed software through SNMP.
snmp-win32-users	Attempts to enumerate Windows user accounts through SNMP
socks-auth-info	Determines the supported authentication mechanisms of a remote SOCKS proxy server. Starting with SOCKS version 5 socks servers may support authentication. The script checks for the following authentication types: 0 - No authentication 1 - GSSAPI 2 - Username and password
socks-brute	Performs brute force password auditing against SOCKS 5 proxy servers.

socks-open-proxy	Checks if an open socks proxy is running on the target.
ssh-hostkey	Shows SSH hostkeys.
ssh2-enum-algos	Reports the number of algorithms (for encryption, compression, etc.) that the target SSH2 server offers. If verbosity is set, the offered algorithms are each listed by type.
sshv1	Checks if an SSH server supports the obsolete and less secure SSH Protocol Version 1.
ssl-ccs-injection	Detects whether a server is vulnerable to the SSL/TLS "CCS Injection" vulnerability (CVE-2014-0224), first discovered by Masashi Kikuchi. The script is based on the ccsinjection.c code authored by Ramon de C Valle (https://gist.github.com/rcvalle/71f4b027d61a78c42607)
ssl-cert	Retrieves a server's SSL certificate. The amount of information printed about the certificate depends on the verbosity level. With no extra verbosity, the script prints the validity period and the commonName, organizationName, stateOrProvinceName, and countryName of the subject.
ssl-date	Retrieves a target host's time and date from its TLS ServerHello response.
ssl-enum-ciphers	This script repeatedly initiates SSLv3/TLS connections, each time trying a new cipher or compressor while recording whether a host accepts or rejects it. The end result is a list of all the ciphersuites and compressors that a server accepts.
ssl-google-cert-catalog	Queries Google's Certificate Catalog for the SSL certificates retrieved from target hosts.
ssl-heartbleed	Detects whether a server is vulnerable to the OpenSSL Heartbleed bug (CVE-2014-0160). The code is based on the Python script ssltest.py authored by Jared Stafford (jspenguin@jspenguin.org)
ssl-known-key	Checks whether the SSL certificate used by a host has a fingerprint that matches an included database of problematic keys.
ssl-poodle	Checks whether SSLv3 CBC ciphers are allowed (POODLE)
sslv2	Determines whether the server supports obsolete and less secure

	SSLv2, and discovers which ciphers it supports.
sstp-discover	Check if the Secure Socket Tunneling Protocol is supported. This is accomplished by trying to establish the HTTPS layer which is used to carry SSTP traffic as described in: - http://msdn.microsoft.com/en-us/library/cc247364.aspx
stun-info	Retrieves the external IP address of a NAT:ed host using the STUN protocol.
stun-version	Sends a binding request to the server and attempts to extract version information from the response, if the server attribute is present.
stuxnet-detect	Detects whether a host is infected with the Stuxnet worm (http://en.wikipedia.org/wiki/Stuxnet).
supermicro-ipmi-conf	Attempts to download an unprotected configuration file containing plain-text user credentials in vulnerable Supermicro Onboard IPMI controllers.
svn-brute	Performs brute force password auditing against Subversion source code control servers.
targets-asn	Produces a list of IP prefixes for a given routing AS number (ASN).
targets-ipv6-map4to6	This script runs in the pre-scanning phase to map IPv4 addresses onto IPv6 networks and add them to the scan queue.
targets-ipv6-multicast-echo	Sends an ICMPv6 echo request packet to the all-nodes link-local multicast address (`ff02::1`) to discover responsive hosts on a LAN without needing to individually ping each IPv6 address.
targets-ipv6-multicast-invalid-dst	Sends an ICMPv6 packet with an invalid extension header to the all-nodes link-local multicast address (`ff02::1`) to discover (some) available hosts on the LAN. This works because some hosts will respond to this probe with an ICMPv6 Parameter Problem packet.
targets-ipv6-multicast-mld	Attempts to discover available IPv6 hosts on the LAN by sending an MLD (multicast listener discovery) query to the link-local multicast address (ff02::1) and listening for any responses. The query's maximum response delay set to 0 to provoke hosts to respond immediately rather than waiting for other responses from

	their multicast group.
targets-ipv6-multicast-slaac	Performs IPv6 host discovery by triggering stateless address auto-configuration (SLAAC).
targets-ipv6-wordlist	Adds IPv6 addresses to the scan queue using a wordlist of hexadecimal "words" that form addresses in a given subnet.
targets-sniffer	Sniffs the local network for a configurable amount of time (10 seconds by default) and prints discovered addresses. If the `newtargets` script argument is set, discovered addresses are added to the scan queue.
targets-traceroute	Inserts traceroute hops into the Nmap scanning queue. It only functions if Nmap's `--traceroute` option is used and the `newtargets` script argument is given.
teamspeak2-version	Detects the TeamSpeak 2 voice communication server and attempts to determine version and configuration information.
telnet-brute	Performs brute-force password auditing against telnet servers.
telnet-encryption	Determines whether the encryption option is supported on a remote telnet server. Some systems (including FreeBSD and the krb5 telnetd available in many Linux distributions) implement this option incorrectly, leading to a remote root vulnerability. This script currently only tests whether encryption is supported, not for that particular vulnerability.
tftp-enum	Enumerates TFTP (trivial file transfer protocol) filenames by testing for a list of common ones.
tls-nextprotoneg	Enumerates a TLS server's supported protocols by using the next protocol negotiation extension.
tor-consensus-checker	Checks if a target is a known Tor node.
traceroute-geolocation	Lists the geographic locations of each hop in a traceroute and optionally saves the results to a KML file, plottable on Google earth and maps.
unittest	Runs unit tests on all NSE libraries.
unusual-port	Compares the detected service on a port against the expected service for that port number (e.g. ssh on 22, http on 80) and

	reports deviations. The script requires that a version scan has been run in order to be able to discover what service is actually running on each port.
upnp-info	Attempts to extract system information from the UPnP service.
url-snarf	Sniffs an interface for HTTP traffic and dumps any URLs, and their originating IP address. Script output differs from other script as URLs are written to stdout directly. There is also an option to log the results to file.
ventrilo-info	Detects the Ventrilo voice communication server service versions 2.1.2 and above and tries to determine version and configuration information. Some of the older versions (pre 3.0.0) may not have the UDP service that this probe relies on enabled by default.
versant-info	Extracts information, including file paths, version and database names from a Versant object database.
vmauthd-brute	Performs brute force password auditing against the VMWare Authentication Daemon (vmware-authd).
vnc-brute	Performs brute force password auditing against VNC servers.
vnc-info	Queries a VNC server for its protocol version and supported security types.
voldemort-info	Retrieves cluster and store information from the Voldemort distributed key-value store using the Voldemort Native Protocol.
vuze-dht-info	Retrieves some basic information, including protocol version from a Vuze filesharing node.
wdb-version	Detects vulnerabilities and gathers information (such as version numbers and hardware support) from VxWorks Wind DeBug agents.
weblogic-t3-info	Detect the T3 RMI protocol and Weblogic version
whois-domain	Attempts to retrieve information about the domain name of the target
whois-ip	Queries the WHOIS services of Regional Internet Registries (RIR) and attempts to retrieve information about the IP Address

	Assignment which contains the Target IP Address.
wsdd-discover	Retrieves and displays information from devices supporting the Web Services Dynamic Discovery (WS-Discovery) protocol. It also attempts to locate any published Windows Communication Framework (WCF) web services (.NET 4.0 or later).
x11-access	Checks if you're allowed to connect to the X server.
xdmcp-discover	Requests an XDMCP (X display manager control protocol) session and lists supported authentication and authorization mechanisms.
xmlrpc-methods	Performs XMLRPC Introspection via the system.listMethods method.
xmpp-brute	Performs brute force password auditing against XMPP (Jabber) instant messaging servers.
xmpp-info	Connects to XMPP server (port 5222) and collects server information such as: supported auth mechanisms, compression methods, whether TLS is supported and mandatory, stream management, language, support of In-Band registration, server capabilities. If possible, studies server vendor.

Libraries

afp	This library was written by Patrik Karlsson <patrik@cqure.net> to facilitate communication with the Apple AFP Service. It is not feature complete and still missing several functions.
ajp	A basic AJP 1.3 implementation based on documentation available from Apache mod_proxy_ajp; http://httpd.apache.org/docs/2.2/mod/mod_proxy_ajp.html
amqp	The AMQP library provides some basic functionality for retrieving information about an AMQP server's properties.
anyconnect	This library implements HTTP requests used by the Cisco AnyConnect VPN Client
asn1	ASN.1 functions.
base32	Base32 encoding and decoding. Follows RFC 4648.
base64	Base64 encoding and decoding. Follows RFC 4648.

bin	Pack and unpack binary data.
bit	Bitwise operations on integers.
bitcoin	This library implements a minimal subset of the BitCoin protocol It currently supports the version handshake and processing Addr responses.
bittorrent	Bittorrent and DHT protocol library which enables users to read information from a torrent file, decode bencoded (bittorrent encoded) buffers, find peers associated with a certain torrent and retrieve nodes discovered during the search for peers.
bjnp	An implementation of the Canon BJNP protocol used to discover and query Canon network printers and scanner devices.
brute	The brute library is an attempt to create a common framework for performing password guessing against remote services.
cassandra	Library methods for handling Cassandra Thrift communication as client
citrixxml	This module was written by Patrik Karlsson and facilitates communication with the Citrix XML Service. It is not feature complete and is missing several functions and parameters.
comm	Common communication functions for network discovery tasks like banner grabbing and data exchange.
creds	The credential class stores found credentials in the Nmap registry
cvs	A minimal CVS (Concurrent Versions System) pserver protocol implementation which currently only supports authentication.
datafiles	Read and parse some of Nmap's data files: `nmap-protocols`, `nmap-rpc`, `nmap-services`, and `nmap-mac-prefixes`.
dhcp	Implement a Dynamic Host Configuration Protocol (DHCP) client.
dhcp6	Minimalistic DHCP6 (Dynamic Host Configuration Protocol for IPv6) implementation supporting basic DHCP6 Solicit requests The library is structured around the following classes: • DHCP6.Option - DHCP6 options encoders (for requests) and decoders

	(for responses) • DHCP6.Request - DHCP6 request encoder and decoder • DHCP6.Response - DHCP6 response encoder and decoder • Helper - The helper class, primary script interface
dns	Simple DNS library supporting packet creation, encoding, decoding, and querying.
dnsbl	A minimalistic DNS BlackList library implemented to facilitate querying various DNSBL services. The current list of services has been implemented based on the following compilations of services: • http://en.wikipedia.org/wiki/Comparison_of_DNS_blacklists • http://www.robtex.com • http://www.sdsc.edu/~jeff/spam/cbc.html
dnssd	Library for supporting DNS Service Discovery
drda	DRDA Library supporting a very limited subset of operations.
eap	EAP (Extensible Authentication Protocol) library supporting a limited subset of features.
eigrp	A library supporting parsing and generating a limited subset of the Cisco' EIGRP packets.
formulas	Formula functions for various calculations.
ftp	FTP functions.
giop	GIOP Library supporting a very limited subset of operations
gps	A smallish gps parsing module. Currently does GPRMC NMEA decoding
http	Implements the HTTP client protocol in a standard form that Nmap scripts can take advantage of.
httpspider	A smallish httpspider library providing basic spidering capabilities It consists of the following classes:
iax2	A minimalistic Asterisk IAX2 (Inter-Asterisk eXchange v2) VoIP protocol implementation. The library implements the minimum needed to perform brute force password guessing.
ike	

imap	A library implementing a minor subset of the IMAP protocol, currently the CAPABILITY, LOGIN and AUTHENTICATE functions. The library was initially written by Brandon Enright and later extended and converted to OO-form by Patrik Karlsson <patrik@cqure.net>
informix	Informix Library supporting a very limited subset of Informix operations
ipOps	Utility functions for manipulating and comparing IP addresses.
ipp	A small CUPS ipp (Internet Printing Protocol) library implementation
iscsi	An iSCSI library implementing written by Patrik Karlsson <patrik@cqure.net> The library currently supports target discovery and login.
isns	A minimal Internet Storage Name Service (iSNS) implementation
jdwp	JDWP (Java Debug Wire Protocol) library implementing a set of commands needed to use remote debugging port and inject java bytecode.
json	Library methods for handling JSON data. It handles JSON encoding and decoding according to RFC 4627.
ldap	Library methods for handling LDAP.
lfs	Returns a directory iterator listing the contents of the given path
listop	Functional-style list operations.
lpeg-utility	Utility functions for LPeg.
ls	Report file and directory listings.
match	Buffered network I/O helper functions.
membase	A smallish implementation of the Couchbase Membase TAP protocol Based on the scarce documentation from the Couchbase Wiki: x http://www.couchbase.org/wiki/display/membase/SASL+Authentication+Example
mobileme	A MobileMe web service client that allows discovering Apple devices using the "find my iPhone" functionality.
mongodb	Library methods for handling MongoDB, creating and parsing packets.
msrpc	By making heavy use of the `smb` library, this library will call various MSRPC functions. The functions used here can be accessed over TCP ports 445 and 139,

	with an established session. A NULL session (the default) will work for some functions and operating systems (or configurations), but not for others.
msrpcperformance	This module is designed to parse the `PERF_DATA_BLOCK` structure, which is stored in the registry under HKEY_PERFORMANCE_DATA. By querying this structure, you can get a whole lot of information about what's going on.
msrpctypes	This module was written to marshall parameters for Microsoft RPC (MSRPC) calls. The values passed in and out are based on structs defined by the protocol, and documented by Samba developers. For detailed breakdowns of the types, take a look at Samba 4.0's `.idl` files.
mssql	MSSQL Library supporting a very limited subset of operations.
mysql	Simple MySQL Library supporting a very limited subset of operations.
natpmp	This library implements the basics of NAT-PMP as described in the NAT Port Mapping Protocol (NAT-PMP) draft: o http://tools.ietf.org/html/draft-cheshire-nat-pmp-03
ncp	A tiny implementation of the Netware Core Protocol (NCP). While NCP was originally a Netware only protocol it's now present on both Linux and Windows platforms running Novell eDirectory.
ndmp	A minimalistic NDMP (Network Data Management Protocol) library
netbios	Creates and parses NetBIOS traffic. The primary use for this is to send NetBIOS name requests.
nmap	Interface with Nmap internals.
nrpc	A minimalistic library to support Domino RPC
nsedebug	Debugging functions for Nmap scripts.
omp2	This library was written to ease interaction with OpenVAS Manager servers using OMP (OpenVAS Management Protocol) version 2.
openssl	OpenSSL bindings.
ospf	A minimalistic OSPF (Open Shortest Path First routing protocol) library, currently supporting IPv4 and the following OSPF message types: HELLO
packet	Facilities for manipulating raw packets.

pcre	Perl Compatible Regular Expressions.
pgsql	PostgreSQL library supporting both version 2 and version 3 of the protocol. The library currently contains the bare minimum to perform authentication. Authentication is supported with or without SSL enabled and using the plain-text or MD5 authentication mechanisms.
pop3	POP3 functions.
pppoe	A minimalistic PPPoE (Point-to-point protocol over Ethernet) library, implementing basic support for PPPoE Discovery and Configuration requests. The PPPoE protocol is ethernet based and hence does not use any IPs or port numbers.
proxy	Functions for proxy testing.
rdp	A minimal RDP (Remote Desktop Protocol) library. Currently has functionality to determine encryption and cipher support.
re	Regular Expression functions
redis	A minimalistic Redis (in-memory key-value data store) library.
rmi	Library method for communicating over RMI (JRMP + java serialization)
rpc	RPC Library supporting a very limited subset of operations.
rpcap	This library implements the fundamentals needed to communicate with the WinPcap Remote Capture Daemon. It currently supports authenticating to the service using either NULL-, or Password-based authentication. In addition it has the capabilities to list the interfaces that may be used for sniffing.
rsync	A minimalist RSYNC (remote file sync) library
rtsp	This Real Time Streaming Protocol (RTSP) library implements only a minimal subset of the protocol needed by the current scripts.
sasl	Simple Authentication and Security Layer (SASL).
shortport	Functions for building short portrules.
sip	A SIP library supporting a limited subset of SIP commands and methods
slaxml	This is the NSE implementation of SLAXML. SLAXML is a pure-Lua SAX-like streaming XML parser. It is more robust than many (simpler) pattern-based parsers that exist, properly supporting code like `<expr test="5 > 7" />`, CDATA

	nodes, comments, namespaces, and processing instructions. It is currently not a truly valid XML parser, however, as it allows certain XML that is syntactically-invalid (not well-formed) to be parsed without reporting an error. The streaming parser does a simple pass through the input and reports what it sees along the way. You can optionally ignore white-space only text nodes using the `stripWhitespace` option. The library contains the parser class and the parseDOM function.
smb	Implements functionality related to Server Message Block (SMB, an extension of CIFS) traffic, which is a Windows protocol.
smbauth	This module takes care of the authentication used in SMB (LM, NTLM, LMv2, NTLMv2).
smtp	Simple Mail Transfer Protocol (SMTP) operations.
snmp	SNMP library.
socks	A smallish SOCKS version 5 proxy protocol implementation
srvloc	A relatively small implementation of the Service Location Protocol. It was initially designed to support requests for discovering Novell NCP servers, but should work for any other service as well.
ssh1	Functions for the SSH-1 protocol. This module also contains functions for formatting key fingerprints.
ssh2	Functions for the SSH-2 protocol.
sslcert	A library providing functions for collecting SSL certificates and storing them in the host-based registry.
stdnse	Standard Nmap Scripting Engine functions. This module contains various handy functions that are too small to justify modules of their own.
strbuf	String buffer facilities.
strict	Strict declared global library. Checks for undeclared global variables during runtime execution.
stun	A library that implements the basics of the STUN protocol (Session Traversal Utilities for NAT) per RFC3489 and RFC5389. A protocol overview is available at http://en.wikipedia.org/wiki/STUN.
tab	Arrange output into tables.

target	Utility functions to add new discovered targets to Nmap scan queue.
tftp	Library implementing a minimal TFTP server
tls	A library providing functions for doing TLS/SSL communications
tns	TNS Library supporting a very limited subset of Oracle operations
unicode	Library methods for handling unicode strings.
unittest	Unit testing support for NSE libraries.
unpwdb	Username/password database library.
upnp	A UPNP library based on code from upnp-info initially written by Thomas Buchanan. The code was factored out from upnp-info and partly re-written by Patrik Karlsson <patrik@cqure.net> in order to support multicast requests.
url	URI parsing, composition, and relative URL resolution.
versant	A tiny library allowing some basic information enumeration from Versant object database software (see http://en.wikipedia.org/wiki/Versant_Corporation). The code is entirely based on packet dumps captured when using the Versant Management Center administration application.
vnc	The VNC library provides some basic functionality needed in order to communicate with VNC servers, and derivatives such as Tight- or Ultra- VNC.
vulns	Functions for vulnerability management.
vuzedht	A Vuze DHT protocol implementation based on the following documentation: o http://wiki.vuze.com/w/Distributed_hash_table
wsdd	A library that enables scripts to send Web Service Dynamic Discovery probes and perform some very basic decoding of responses. The library is in no way a full WSDD implementation it's rather the result of some packet captures and some creative coding.
xdmcp	Implementation of the XDMCP (X Display Manager Control Protocol) based on: x http://www.xfree86.org/current/xdmcp.pdf
xmpp	A XMPP (Jabber) library, implementing a minimal subset of the protocol enough

to do authentication brute-force.