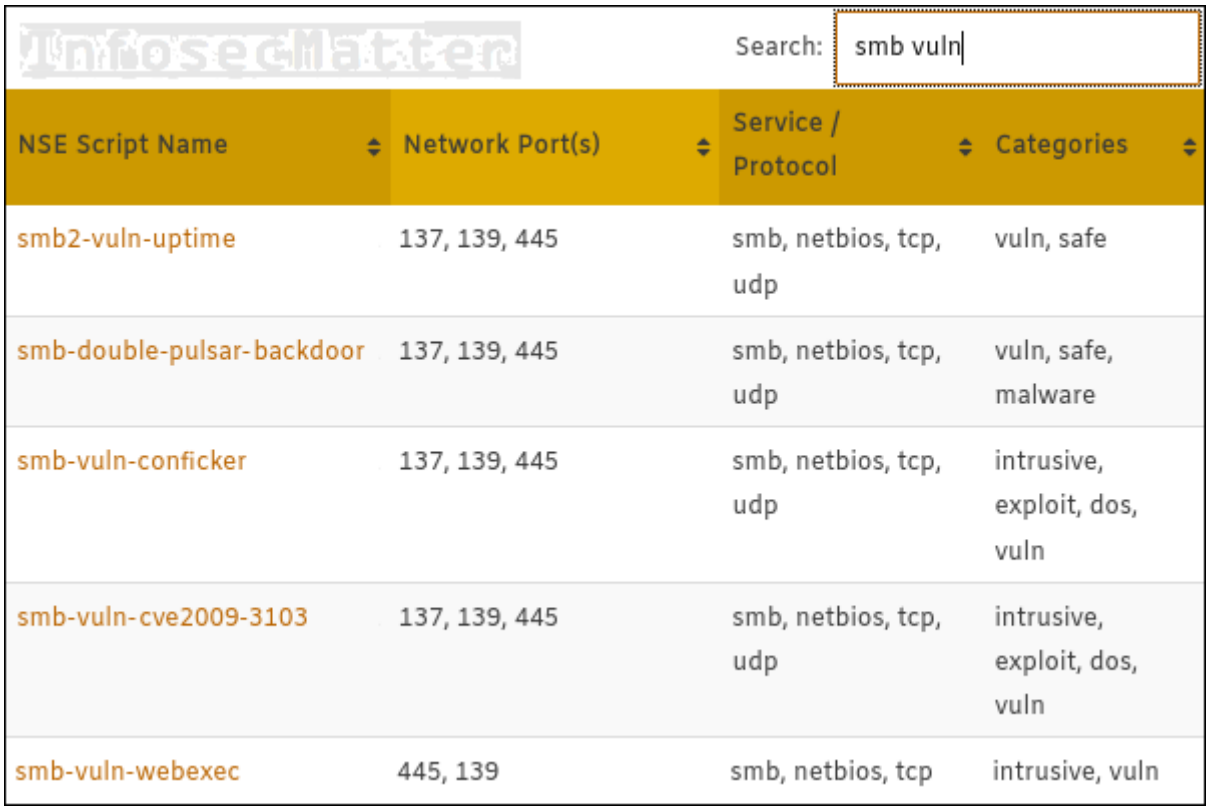
Nmap NSE Library

infosecmatter.com/nmap-nse-library

April 7, 2021



NSE Script Name	Network Port(s)	Service / Protocol	Categories
smb2-vuln-uptime	137, 139, 445	smb, netbios, tcp, udp	vuln, safe
smb-double-pulsar-backdoor	137, 139, 445	smb, netbios, tcp, udp	vuln, safe, malware
smb-vuln-conficker	137, 139, 445	smb, netbios, tcp, udp	intrusive, exploit, dos, vuln
smb-vuln-cve2009-3103	137, 139, 445	smb, netbios, tcp, udp	intrusive, exploit, dos, vuln
smb-vuln-webexec	445, 139	smb, netbios, tcp	intrusive, vuln

If you are looking to explore the world of NSE (Nmap Scripting Language) scripts, this page will hopefully help you find what you are looking for, quickly and effectively.

On this page you will find a comprehensive list of all available NSE scripts, organized in an interactive table (spreadsheet) with all the relevant information in one place.

Introduction

Whether you are looking for a specific NSE script to use in your scenario or you just want to see which scripts target a specific protocol or a port, the spreadsheet below will hopefully give you a quick answer and give you a good overview of what is available in the world of Nmap scripts.

Below spreadsheet contains a list of all 604 Nmap NSE scripts that are currently available in the latest Nmap release. The spreadsheet is interactive and it allows you to:

- Use the search filtering to quickly find relevant scripts (see examples below)
- Sort by any column (in ascending or descending order), e.g. sort by a port number
- Click on the script name to see the official documentation with all the relevant details

Filtering examples

As mentioned above, you can use the search function to interactively filter out scripts based on a pattern of your interest. Here are couple of examples:

- Search for: `smb discovery`
  Display only scripts related to the “smb” protocol from the “discovery” category.
- Search for `1521`
  Display only scripts targeting port 1521 (Oracle database).
- Search for: `http brute`
  Display only scripts related to brute forcing of web services and web applications.
- Search for: `ftp`
  Display only scripts related to FTP.

Let’s have a look.

Nmap script list (interactive spreadsheet)

NSE Script Name	Network Port(s)	Service / Protocol	Categories
acarsd-info	2202	acarsd, tcp	safe, discovery
address-info	-	-	default, safe
afp-brute	548	afp	intrusive, brute
afp-ls	548	afp	discovery, safe
afp-path-vuln	548	tcp	exploit, intrusive, vuln
afp-serverinfo	548	afp	default, discovery, safe
afp-showmount	548	tcp	discovery, safe
ajp-auth	8009	ajp13, tcp	default, auth, safe
ajp-brute	8009	ajp13, tcp	intrusive, brute
ajp-headers	8009	ajp13, tcp	discovery, safe

NSE Script Name	Network Port(s)	Service / Protocol	Categories
ajp-methods	8009	ajp13, tcp	default, safe
ajp-request	8009	ajp13, tcp	discovery, safe
allseeingeye-info	1258, 2126, 3123, 12444, 13200, 23196, 26000, 27138, 27244, 27777, 28138	allseeingeye, udp	discovery, safe, version
amqp-info	5672	amqp, tcp	default, discovery, safe, version
asn-query	-	-	discovery, external, safe
auth-owners	113	auth	default, safe
auth-spoof	113	auth	malware, safe
backorifice-brute	151-222, 1024-1512, 25252, 31337	udp	intrusive, brute
backorifice-info	151-222, 1024-1512, 25252, 31337	udp	default, discovery, safe
bacnet-info	47808	bacnet, tcp, udp	discovery, version
banner	any	any	discovery, safe
bitcoin-getaddr	8333	bitcoin, tcp	discovery, safe
bitcoin-info	8333	bitcoin, tcp	discovery, safe
bitcoinrpc-info	8332	-	default, discovery, safe
bittorrent-discovery	-	-	discovery, safe
bjnp-discover	8611, 8612	udp	safe, discovery

NSE Script Name	Network Port(s)	Service / Protocol	Categories
broadcast-ataoe-discover	-	-	broadcast, safe
broadcast-avahi-dos	-	-	broadcast, dos, intrusive, vuln
broadcast-bjnp-discover	-	-	safe, broadcast
broadcast-db2-discover	-	-	broadcast, safe
broadcast-dhcp6-discover	-	-	broadcast, safe
broadcast-dhcp-discover	-	-	broadcast, safe
broadcast-dns-service-discovery	-	-	broadcast, safe
broadcast-dropbox-listener	-	-	broadcast, safe
broadcast-eigrp-discovery	-	-	discovery, broadcast, safe
broadcast-hid-discoveryd	-	-	discovery, broadcast, safe
broadcast-igmp-discovery	-	-	discovery, safe, broadcast
broadcast-jenkins-discover	-	-	discovery, broadcast, safe
broadcast-listener	-	-	broadcast, safe
broadcast-ms-sql-discover	-	-	broadcast, safe

NSE Script Name	Network Port(s)	Service / Protocol	Categories
broadcast-netbios-master-browser	-	-	broadcast, safe
broadcast-networker-discover	-	-	broadcast, safe
broadcast-novell-locate	-	-	broadcast, safe
broadcast-ospf2-discover	-	-	broadcast, discovery, safe
broadcast-pc-anywhere	-	-	broadcast, safe
broadcast-pc-duo	-	-	broadcast, safe
broadcast-pim-discovery	-	-	discovery, safe, broadcast
broadcast-ping	-	-	discovery, safe, broadcast
broadcast-pppoe-discover	-	-	broadcast, safe
broadcast-rip-discover	-	-	broadcast, safe
broadcast-ripng-discover	-	-	broadcast, safe
broadcast-sonicwall-discover	-	-	broadcast, safe
broadcast-sybase-asa-discover	-	-	broadcast, safe
broadcast-tellstick-discover	-	-	broadcast, safe

NSE Script Name	Network Port(s)	Service / Protocol	Categories
broadcast-upnp-info	-	-	broadcast, safe
broadcast-versant-locate	-	-	broadcast, safe
broadcast-wake-on-lan	-	-	broadcast, safe
broadcast-wpad-discover	-	-	broadcast, safe
broadcast-wsdd-discover	-	-	broadcast, safe
broadcast-xdmcp-discover	-	-	broadcast, safe
cassandra-brute	9160	cassandra	intrusive, brute
cassandra-info	9160	cassandra	default, discovery, safe
cccam-version	10000, 10001, 12000, 12001, 16000, 16001	cccam	version
cics-enum	23, 992	tn3270	intrusive, brute
cics-info	23, 992	tn3270	discovery, safe
cics-user-brute	23, 992	tn3270	intrusive, brute
cics-user-enum	23, 992	tn3270	intrusive, brute
citrix-brute-xml	8080, 80, 443	http, https, tcp	intrusive, brute
citrix-enum-apps	1604	udp	discovery, safe
citrix-enum-apps-xml	8080, 80, 443	http, https, tcp	discovery, safe
citrix-enum-servers	1604	udp	discovery, safe

NSE Script Name	Network Port(s)	Service / Protocol	Categories
citrix-enum-servers-xml	8080, 80, 443	http, https, tcp	discovery, safe
clamav-exec	3310	clam	exploit, vuln
clock-skew	various	-	default, safe
coap-resources	5683	coap, udp	safe, discovery
couchdb-databases	5984	-	discovery, safe
couchdb-stats	5984	-	discovery, safe
creds-summary	-	-	auth, default, safe
cups-info	631	ipp, tcp	safe, discovery
cups-queue-info	631	ipp, tcp	safe, discovery
cvs-brute	2401	cvspserver	intrusive, brute
cvs-brute-repository	2401	cvspserver	intrusive, brute
daap-get-library	3689	daap	discovery, safe
daytime	13	daytime, tcp, udp	discovery, safe
db2-das-info	523	tcp, udp	safe, discovery, version
deluge-rpc-brute	58846	deluge-rpc	intrusive, brute
dhcp-discover	67	udp	discovery, safe
dicom-brute	104, 2345, 2761, 2762, 4242, 11112	dicom, tcp	auth, brute

NSE Script Name	Network Port(s)	Service / Protocol	Categories
dicom-ping	104, 2345, 2761, 2762, 4242, 11112	dicom, tcp	discovery, default, safe, auth
dict-info	2628	dict, tcp	discovery, safe
distcc-cve2004-2687	3632	distcc	exploit, intrusive, vuln
dns-blacklist	-	-	external, safe
dns-brute	-	-	intrusive, discovery
dns-cache-snoop	53	dns, udp	intrusive, discovery
dns-check-zone	-	-	discovery, safe, external
dns-client-subnet-scan	53	dns, udp, tcp	discovery, safe
dns-fuzz	53	dns, udp, tcp	fuzzer, intrusive
dns-ip6-arpa-scan	-	-	intrusive, discovery
dns-nsec3-enum	53	dns, udp, tcp	discovery, intrusive
dns-nsec-enum	53	dns, udp, tcp	discovery, intrusive
dns-nsid	53	dns, udp, tcp	discovery, default, safe
dns-random-srcport	53	dns, udp	external, intrusive
dns-random-txid	53	dns, udp	external, intrusive
dns-recursion	53	dns, udp	default, safe

NSE Script Name	Network Port(s)	Service / Protocol	Categories
dns-service-discovery	5353	dns, udp	default, discovery, safe
dns-srv-enum	-	-	discovery, safe
dns-update	53	dns, udp, tcp	vuln, intrusive
dns-zeustracker	-	-	safe, discovery, external, malware
dns-zone-transfer	53	dns, tcp	intrusive, discovery
docker-version	2375, 2376	docker, docker-s, tcp	version
domcon-brute	2050	tcp	intrusive, brute
domcon-cmd	2050	dominoconsole, tcp	intrusive, auth
domino-enum-users	1352	lotusnotes, tcp	intrusive, auth
dpap-brute	8770	apple-iphoto	intrusive, brute
drda-brute	50000, 60000	drda, ibm-db2, tcp	intrusive, brute
drda-info	50000, 60000, 9090, 1526, 1527	-	safe, discovery, version
duplicates	-	-	safe
eap-info	-	-	broadcast, safe
enip-info	44818	tcp, udp	discovery, version
epmd-info	4369	epmd	default, discovery, safe

NSE Script Name	Network Port(s)	Service / Protocol	Categories
eppc-enum-processes	3031	eppc, tcp	discovery, safe
fcrdns	-	-	discovery, safe
finger	79	finger	default, discovery, safe
fingerprint-strings	79, any	finger	version
firewalk	-	-	safe, discovery
firewall-bypass	-	-	vuln, intrusive
flume-master-info	35871	flume-master	default, discovery, safe
fox-info	1911, 4911	niagara-fox, tcp	discovery, version
freelancer-info	2302	freelancer, udp	default, discovery, safe, version
ftp-anon	21, 990	ftp, ftps	default, auth, safe
ftp-bounce	21, 990	ftp, ftps	default, safe
ftp-brute	21	ftp	intrusive, brute
ftp-libopie	21	ftp	vuln, intrusive
ftp-proftpd-backdoor	21	ftp	exploit, intrusive, malware, vuln
ftp-syst	21, 990	ftp, ftps	default, discovery, safe

NSE Script Name	Network Port(s)	Service / Protocol	Categories
ftp-vsftpd-backdoor	21	ftp	exploit, intrusive, malware, vuln
ftp-vuln-cve2010-4221	21	ftp	intrusive, vuln
ganglia-info	8649, 8651	ganglia, tcp	default, discovery, safe
giop-info	2809, 1050, 1049	giop, tcp	default, discovery, safe
gkrellm-info	19150	gkrellm, tcp	discovery, safe
gopher-ls	70	gopher, tcp	default, discovery, safe
gpsd-info	2947	gpsd-ng, tcp	discovery, safe
hadoop-datanode-info	50075	hadoop-datanode	default, discovery, safe
hadoop-jobtracker-info	50030	hadoop-jobtracker	default, discovery, safe
hadoop-namenode-info	50070	hadoop-namenode	default, discovery, safe
hadoop-secondary-namenode-info	50090	hadoop-secondary-namenode	default, discovery, safe
hadoop-tasktracker-info	50060	hadoop-tasktracker	default, discovery, safe
hbase-master-info	60010	hbase-master	default, discovery, safe

NSE Script Name	Network Port(s)	Service / Protocol	Categories
hbase-region-info	60030	hbase-region	default, discovery, safe
hddtemp-info	7634	hddtemp, tcp	default, discovery, safe
hnap-info	80, 8080	http	safe, discovery, default, version
hostmap-bfk	-	-	external, discovery
hostmap-crtsh	-	-	external, discovery
hostmap-robtex	-	-	discovery, safe, external
http-adobe-coldfusion-apsa1301	80, 443, 631, 7080, 8080, 8443, 8088, 5800, 3872, 8180, 8000	http, https	exploit, vuln
http-affiliate-id	80, 443, 631, 7080, 8080, 8443, 8088, 5800, 3872, 8180, 8000	http, https	safe, discovery
http-apache-negotiation	80, 443, 631, 7080, 8080, 8443, 8088, 5800, 3872, 8180, 8000	http, https	safe, discovery
http-apache-server-status	80, 443, 631, 7080, 8080, 8443, 8088, 5800, 3872, 8180, 8000	http, https	discovery, safe
http-aspnet-debug	80, 443, 631, 7080, 8080, 8443, 8088, 5800, 3872, 8180, 8000	http, https	vuln, discovery
http-auth-finder	80, 443, 631, 7080, 8080, 8443, 8088, 5800, 3872, 8180, 8000	http, https	discovery, safe
http-auth	80, 443, 631, 7080, 8080, 8443, 8088, 5800, 3872, 8180, 8000	http, https	default, auth, safe
http-avaya-ipoffice-users	80, 443, 631, 7080, 8080, 8443, 8088, 5800, 3872, 8180, 8000	http, https	exploit, vuln
http-awstatstotals-exec	80, 443, 631, 7080, 8080, 8443, 8088, 5800, 3872, 8180, 8000	http, https	vuln, intrusive, exploit

NSE Script Name	Network Port(s)	Service / Protocol	Categories
http-axis2-dir-traversal	80, 443, 631, 7080, 8080, 8443, 8088, 5800, 3872, 8180, 8000	http, https	vuln, intrusive, exploit
http-backup-finder	80, 443, 631, 7080, 8080, 8443, 8088, 5800, 3872, 8180, 8000	http, https	discovery, safe
http-barracuda-dir-traversal	8000	barracuda, tcp	intrusive, exploit, auth
http-bigip-cookie	80, 443, 631, 7080, 8080, 8443, 8088, 5800, 3872, 8180, 8000	http, https	discovery, safe
http-brute	80, 443	http, https	intrusive, brute
http-cakephp-version	80, 443, 631, 7080, 8080, 8443, 8088, 5800, 3872, 8180, 8000	http, https	discovery, safe
http-chrono	80, 443, 631, 7080, 8080, 8443, 8088, 5800, 3872, 8180, 8000	http, https	discovery, intrusive
http-cisco-anyconnect	261, 271, 324, 443, 465, 563, 585, 636, 853, 989, 990, 992, 993, 994, 995, 2221, 2252, 2376, 3269, 3389, 4911, 5061, 5986, 6679, 6697, 8443, 9001, 8883	ssl	default, discovery, safe
http-coldfusion-subzero	80, 443, 631, 7080, 8080, 8443, 8088, 5800, 3872, 8180, 8000	http, https	exploit
http-comments-displayer	80, 443	http, https	discovery, safe
http-config-backup	80, 443, 631, 7080, 8080, 8443, 8088, 5800, 3872, 8180, 8000	http, https	auth, intrusive
http-cookie-flags	80, 443, 631, 7080, 8080, 8443, 8088, 5800, 3872, 8180, 8000	http, https	default, safe, vuln
http-cors	80, 443, 631, 7080, 8080, 8443, 8088, 5800, 3872, 8180, 8000	http, https	default, discovery, safe
http-cross-domain-policy	80, 443, 631, 7080, 8080, 8443, 8088, 5800, 3872, 8180, 8000	http, https	safe, external, vuln

NSE Script Name	Network Port(s)	Service / Protocol	Categories
http-csrf	80, 443	http, https	intrusive, exploit, vuln
http-date	80, 443, 631, 7080, 8080, 8443, 8088, 5800, 3872, 8180, 8000	http, https	discovery, safe
http-default-accounts	80, 443, 631, 7080, 8080, 8443, 8088, 5800, 3872, 8180, 8000	http, https	discovery, auth, intrusive
http-devframework	80, 443	http, https	discovery, intrusive
http-dlink-backdoor	80, 443, 631, 7080, 8080, 8443, 8088, 5800, 3872, 8180, 8000	http, https	exploit, vuln
http-dombased-xss	80, 443	http, https	intrusive, exploit, vuln
http-domino-enum-passwords	80, 443	http, https	intrusive, auth
http-drupal-enum	80, 443, 631, 7080, 8080, 8443, 8088, 5800, 3872, 8180, 8000	http, https	discovery, intrusive
http-drupal-enum-users	80, 443, 631, 7080, 8080, 8443, 8088, 5800, 3872, 8180, 8000	http, https	discovery, intrusive
http-enum	80, 443, 631, 7080, 8080, 8443, 8088, 5800, 3872, 8180, 8000	http, https	discovery, intrusive, vuln
http-errors	80, 443	http, https	discovery, intrusive
http-exif-spider	80, 443, 631, 7080, 8080, 8443, 8088, 5800, 3872, 8180, 8000	http, https	intrusive
http-favicon	80, 443, 631, 7080, 8080, 8443, 8088, 5800, 3872, 8180, 8000	http, https	default, discovery, safe
http-feed	80, 443	http, https	discovery, intrusive
http-fetch	80, 443, 631, 7080, 8080, 8443, 8088, 5800, 3872, 8180, 8000	http, https	safe

NSE Script Name	Network Port(s)	Service / Protocol	Categories
http-fileupload-exploiter	80, 443	http, https	intrusive, exploit, vuln
http-form-brute	80, 443	http, https	intrusive, brute
http-form-fuzzer	80, 443, 631, 7080, 8080, 8443, 8088, 5800, 3872, 8180, 8000	http, https	fuzzer, intrusive
http-frontpage-login	80, 443, 631, 7080, 8080, 8443, 8088, 5800, 3872, 8180, 8000	http, https	vuln, safe
http-generator	80, 443, 631, 7080, 8080, 8443, 8088, 5800, 3872, 8180, 8000	http, https	default, discovery, safe
http-git	80, 443, 631, 7080, 8080, 8443, 8088, 5800, 3872, 8180, 8000	http, https	default, safe, vuln
http-gitweb-projects-enum	80, 443, 631, 7080, 8080, 8443, 8088, 5800, 3872, 8180, 8000	http, https	discovery, safe
http-google-malware	80, 443, 631, 7080, 8080, 8443, 8088, 5800, 3872, 8180, 8000	http, https	malware, discovery, safe, external
http-grep	80, 443, 631, 7080, 8080, 8443, 8088, 5800, 3872, 8180, 8000	http, https	discovery, safe
http-headers	80, 443, 631, 7080, 8080, 8443, 8088, 5800, 3872, 8180, 8000	http, https	discovery, safe
http-hp-ilo-info	80, 443, 631, 7080, 8080, 8443, 8088, 5800, 3872, 8180, 8000	http, https	safe, discovery
http-huawei-hg5xx-vuln	80, 443, 631, 7080, 8080, 8443, 8088, 5800, 3872, 8180, 8000	http, https	exploit, vuln
http-icloud-findmyiphone	-	-	discovery, safe, external
http-icloud-sendmsg	-	-	discovery, safe, external
http-iis-short-name-brute	80, 443, 631, 7080, 8080, 8443, 8088, 5800, 3872, 8180, 8000	http, https	intrusive, brute
http-iis-webdav-vuln	80, 443, 631, 7080, 8080, 8443, 8088, 5800, 3872, 8180, 8000	http, https	vuln, intrusive

NSE Script Name	Network Port(s)	Service / Protocol	Categories
http-internal-ip-disclosure	80, 443, 631, 7080, 8080, 8443, 8088, 5800, 3872, 8180, 8000	http, https	vuln, discovery, safe
http-joomla-brute	80, 443, 631, 7080, 8080, 8443, 8088, 5800, 3872, 8180, 8000	http, https	intrusive, brute
http-jsonp-detection	80, 443, 631, 7080, 8080, 8443, 8088, 5800, 3872, 8180, 8000	http, https	safe, vuln, discovery
http-litespeed-sourcecode-download	80, 443, 631, 7080, 8080, 8443, 8088, 5800, 3872, 8180, 8000	http, https	vuln, intrusive, exploit
http-ls	80, 443, 631, 7080, 8080, 8443, 8088, 5800, 3872, 8180, 8000	http, https	default, discovery, safe
http-majordomo2-dir-traversal	80, 443, 631, 7080, 8080, 8443, 8088, 5800, 3872, 8180, 8000	http, https	intrusive, vuln, exploit
http-malware-host	80, 443, 631, 7080, 8080, 8443, 8088, 5800, 3872, 8180, 8000	http, https	malware, safe
http-mcmp	80, 443, 631, 7080, 8080, 8443, 8088, 5800, 3872, 8180, 8000	http, https	safe, discovery
http-methods	80, 443, 631, 7080, 8080, 8443, 8088, 5800, 3872, 8180, 8000	http, https	default, safe
http-method-tamper	80, 443, 631, 7080, 8080, 8443, 8088, 5800, 3872, 8180, 8000	http, https	auth, vuln
http-mobileversion-checker	80, 443	http, https	discovery, safe
http-ntlm-info	80, 443, 631, 7080, 8080, 8443, 8088, 5800, 3872, 8180, 8000	http, https	default, discovery, safe
http-open-proxy	8123, 3128, 8000, 8080	polipo, squid-http, http-proxy	default, discovery, external, safe
http-open-redirect	80, 443, 631, 7080, 8080, 8443, 8088, 5800, 3872, 8180, 8000	http, https	discovery, intrusive
http-passwd	80, 443, 631, 7080, 8080, 8443, 8088, 5800, 3872, 8180, 8000	http, https	intrusive, vuln

NSE Script Name	Network Port(s)	Service / Protocol	Categories
http-phpmyadmin-dir-traversal	80, 443, 631, 7080, 8080, 8443, 8088, 5800, 3872, 8180, 8000	http, https	vuln, exploit
http-phpself-xss	80, 443, 631, 7080, 8080, 8443, 8088, 5800, 3872, 8180, 8000	http, https	fuzzer, intrusive, vuln
http-php-version	80, 443, 631, 7080, 8080, 8443, 8088, 5800, 3872, 8180, 8000	http, https	discovery, safe
http-proxy-brute	8123, 3128, 8000, 8080	polipo, squid-http, http-proxy	brute, intrusive, external
http-put	80, 443, 631, 7080, 8080, 8443, 8088, 5800, 3872, 8180, 8000	http, https	discovery, intrusive
http-qnap-nas-info	443, 8080	https, tcp	safe, discovery
http-referer-checker	80, 443	http, https	discovery, safe
http-rfi-spider	80, 443	http, https	intrusive
http-robots.txt	80, 443, 631, 7080, 8080, 8443, 8088, 5800, 3872, 8180, 8000	http, https	default, discovery, safe
http-robtex-reverse-ip	-	-	discovery, safe, external
http-robtex-shared-ns	-	-	discovery, safe, external
http-sap-netweaver-leak	80, 443, 631, 7080, 8080, 8443, 8088, 5800, 3872, 8180, 8000	http, https	safe, discovery
http-security-headers	80, 443	http, tcp	discovery, safe
http-server-header	80, 443, 631, 7080, 8080, 8443, 8088, 5800, 3872, 8180, 8000	http, https	version
http-shellshock	80, 443, 631, 7080, 8080, 8443, 8088, 5800, 3872, 8180, 8000	http, https	exploit, vuln, intrusive

NSE Script Name	Network Port(s)	Service / Protocol	Categories
http-sitemap-generator	80, 443	http, https	discovery, intrusive
http-slowloris-check	80, 443, 631, 7080, 8080, 8443, 8088, 5800, 3872, 8180, 8000	http, https	vuln, safe
http-slowloris	80, 443, 631, 7080, 8080, 8443, 8088, 5800, 3872, 8180, 8000	http, https	dos, intrusive
http-sql-injection	80, 443	http, https	intrusive, vuln
https-redirect	80, 443, 631, 7080, 8080, 8443, 8088, 5800, 3872, 8180, 8000	http, https	version
http-stored-xss	80, 443	http, https	intrusive, exploit, vuln
http-svn-enum	80, 443, 631, 7080, 8080, 8443, 8088, 5800, 3872, 8180, 8000	http, https	default, discovery, safe
http-svn-info	80, 443, 631, 7080, 8080, 8443, 8088, 5800, 3872, 8180, 8000	http, https	default, discovery, safe
http-title	80, 443, 631, 7080, 8080, 8443, 8088, 5800, 3872, 8180, 8000	http, https	default, discovery, safe
http-tplink-dir-traversal	80, 443, 631, 7080, 8080, 8443, 8088, 5800, 3872, 8180, 8000	http, https	vuln, exploit
http-trace	80, 443, 631, 7080, 8080, 8443, 8088, 5800, 3872, 8180, 8000	http, https	vuln, discovery, safe
http-traceroute	80, 443, 631, 7080, 8080, 8443, 8088, 5800, 3872, 8180, 8000	http, https	discovery, safe
http-trane-info	80, 443, 631, 7080, 8080, 8443, 8088, 5800, 3872, 8180, 8000	http, https	discovery, version, safe
http-unsafe-output-escaping	80, 443, 631, 7080, 8080, 8443, 8088, 5800, 3872, 8180, 8000	http, https	discovery, intrusive
http-useragent-tester	80, 443	http, https	discovery, safe

NSE Script Name	Network Port(s)	Service / Protocol	Categories
http-userdir-enum	80, 443, 631, 7080, 8080, 8443, 8088, 5800, 3872, 8180, 8000	http, https	auth, intrusive
http-vhosts	80, 443, 631, 7080, 8080, 8443, 8088, 5800, 3872, 8180, 8000	http, https	discovery, intrusive
http-virustotal	-	-	safe, malware, external
http-vlcstreamer-ls	54340	vlcstreamer, tcp	discovery, safe
http-vmware-path-vuln	80, 443, 8222, 8333	http, https	vuln, safe
http-vuln-cve2006-3392	10000	-	exploit, vuln, intrusive
http-vuln-cve2009-3960	80, 443, 631, 7080, 8080, 8443, 8088, 5800, 3872, 8180, 8000	http, https	exploit, intrusive, vuln
http-vuln-cve2010-0738	80, 443, 631, 7080, 8080, 8443, 8088, 5800, 3872, 8180, 8000	http, https	safe, auth, vuln
http-vuln-cve2010-2861	80, 443, 631, 7080, 8080, 8443, 8088, 5800, 3872, 8180, 8000	http, https	intrusive, vuln
http-vuln-cve2011-3192	80, 443, 631, 7080, 8080, 8443, 8088, 5800, 3872, 8180, 8000	http, https	vuln, safe
http-vuln-cve2011-3368	80, 443, 631, 7080, 8080, 8443, 8088, 5800, 3872, 8180, 8000	http, https	intrusive, vuln
http-vuln-cve2012-1823	80, 443, 631, 7080, 8080, 8443, 8088, 5800, 3872, 8180, 8000	http, https	exploit, vuln, intrusive
http-vuln-cve2013-0156	80, 443, 631, 7080, 8080, 8443, 8088, 5800, 3872, 8180, 8000	http, https	exploit, vuln
http-vuln-cve2013-6786	80, 443, 631, 7080, 8080, 8443, 8088, 5800, 3872, 8180, 8000	http, https	exploit, vuln
http-vuln-cve2013-7091	80, 443, 631, 7080, 8080, 8443, 8088, 5800, 3872, 8180, 8000	http, https	exploit, vuln, intrusive

NSE Script Name	Network Port(s)	Service / Protocol	Categories
http-vuln-cve2014-2126	261, 271, 324, 443, 465, 563, 585, 636, 853, 989, 990, 992, 993, 994, 995, 2221, 2252, 2376, 3269, 3389, 4911, 5061, 5986, 6679, 6697, 8443, 9001, 8883	ssl	vuln, safe
http-vuln-cve2014-2127	261, 271, 324, 443, 465, 563, 585, 636, 853, 989, 990, 992, 993, 994, 995, 2221, 2252, 2376, 3269, 3389, 4911, 5061, 5986, 6679, 6697, 8443, 9001, 8883	ssl	vuln, safe
http-vuln-cve2014-2128	261, 271, 324, 443, 465, 563, 585, 636, 853, 989, 990, 992, 993, 994, 995, 2221, 2252, 2376, 3269, 3389, 4911, 5061, 5986, 6679, 6697, 8443, 9001, 8883	ssl	vuln, safe
http-vuln-cve2014-2129	261, 271, 324, 443, 465, 563, 585, 636, 853, 989, 990, 992, 993, 994, 995, 2221, 2252, 2376, 3269, 3389, 4911, 5061, 5986, 6679, 6697, 8443, 9001, 8883	ssl	vuln, safe
http-vuln-cve2014-3704	80, 443, 631, 7080, 8080, 8443, 8088, 5800, 3872, 8180, 8000	http, https	vuln, intrusive, exploit
http-vuln-cve2014-8877	80, 443, 631, 7080, 8080, 8443, 8088, 5800, 3872, 8180, 8000	http, https	vuln, intrusive, exploit
http-vuln-cve2015-1427	9200	http, tcp	vuln, intrusive
http-vuln-cve2015-1635	80, 443, 631, 7080, 8080, 8443, 8088, 5800, 3872, 8180, 8000	http, https	vuln, safe
http-vuln-cve2017-1001000	80, 443, 631, 7080, 8080, 8443, 8088, 5800, 3872, 8180, 8000	http, https	vuln, safe
http-vuln-cve2017-5638	80, 443, 631, 7080, 8080, 8443, 8088, 5800, 3872, 8180, 8000	http, https	vuln
http-vuln-cve2017-5689	623, 664, 16992, 16993	amt-soap-http	vuln, auth, exploit
http-vuln-cve2017-8917	80, 443, 631, 7080, 8080, 8443, 8088, 5800, 3872, 8180, 8000	http, https	vuln, intrusive

NSE Script Name	Network Port(s)	Service / Protocol	Categories
http-vuln-misfortune-cookie	7547	http	vuln, intrusive
http-vuln-wnr1000-creds	80, 443, 631, 7080, 8080, 8443, 8088, 5800, 3872, 8180, 8000	http, https	exploit, vuln, intrusive
http-waf-detect	80, 443, 631, 7080, 8080, 8443, 8088, 5800, 3872, 8180, 8000	http, https	discovery, intrusive
http-waf-fingerprint	80, 443, 631, 7080, 8080, 8443, 8088, 5800, 3872, 8180, 8000	http, https	discovery, intrusive
http-webdav-scan	80, 443, 631, 7080, 8080, 8443, 8088, 5800, 3872, 8180, 8000	http, https	safe, discovery, default
http-wordpress-brute	80, 443, 631, 7080, 8080, 8443, 8088, 5800, 3872, 8180, 8000	http, https	intrusive, brute
http-wordpress-enum	80, 443, 631, 7080, 8080, 8443, 8088, 5800, 3872, 8180, 8000	http, https	discovery, intrusive
http-wordpress-users	80, 443, 631, 7080, 8080, 8443, 8088, 5800, 3872, 8180, 8000	http, https	auth, intrusive, vuln
http-xssed	80, 443	http, https	safe, external, discovery
iax2-brute	4569	iax2, udp, tcp	intrusive, brute
iax2-version	4569	iax2, udp, tcp	version
icap-info	1344	icap	safe, discovery
iec-identify	2404	iec-104, tcp	discovery, intrusive
ike-version	500	isakmp, udp	default, discovery, safe, version
imap-brute	143, 993	imap, imaps	brute, intrusive

NSE Script Name	Network Port(s)	Service / Protocol	Categories
imap-capabilities	143, 993	imap, imaps	default, safe
imap-ntlm-info	143, 993	imap, imaps	default, discovery, safe
impress-remote-discover	1599	impress-remote, tcp	intrusive, brute
informix-brute	1526, 9088, 9090, 9092	informix, tcp	intrusive, brute
informix-query	1526, 9088, 9090, 9092	informix, tcp	intrusive, auth
informix-tables	1526, 9088, 9090, 9092	informix, tcp	intrusive, auth
ip-forwarding	-	-	safe, discovery
ip-geolocation-geoplugin	-	-	discovery, external, safe
ip-geolocation-ipinfodb	-	-	discovery, external, safe
ip-geolocation-map-bing	-	-	external, safe
ip-geolocation-map-google	-	-	external, safe
ip-geolocation-map-kml	-	-	safe
ip-geolocation-maxmind	-	-	discovery, external, safe
ip-https-discover	261, 271, 324, 443, 465, 563, 585, 636, 853, 989, 990, 992, 993, 994, 995, 2221, 2252, 2376, 3269, 3389, 4911, 5061, 5986, 6679, 6697, 8443, 9001, 8883	ssl	discovery, safe, default
ipidseq	-	-	safe, discovery

NSE Script Name	Network Port(s)	Service / Protocol	Categories
ipmi-brute	623	asf-rmcp, udp	intrusive, brute
ipmi-cipher-zero	623	asf-rmcp, udp	vuln, safe
ipmi-version	623	asf-rmcp, udp	discovery, safe
ipv6-multicast-mld-list	-	-	broadcast, discovery
ipv6-node-info	-	-	default, discovery, safe
ipv6-ra-flood	-	-	dos, intrusive
irc-botnet-channels	6664, 6665, 6666, 6667, 6668, 6669, 6679, 6697, 7000, 8067	irc	discovery, vuln, safe
irc-brute	6664, 6665, 6666, 6667, 6668, 6669, 6679, 6697, 7000, 8067	irc	brute, intrusive
irc-info	6664, 6665, 6666, 6667, 6668, 6669, 6679, 6697, 7000, 8067	irc	default, discovery, safe
irc-sasl-brute	6664, 6665, 6666, 6667, 6668, 6669, 6679, 6697, 7000, 8067	irc	brute, intrusive
irc-unrealircd-backdoor	6664, 6665, 6666, 6667, 6668, 6669, 6679, 6697, 7000, 8067	irc	exploit, intrusive, malware, vuln
iscsi-brute	3260	tcp	intrusive, brute
iscsi-info	3260	tcp	default, safe, discovery
isns-info	3205	isns	safe, discovery
jdwp-exec	any	tcp	exploit, intrusive
jdwp-info	any	tcp	default, safe, discovery

NSE Script Name	Network Port(s)	Service / Protocol	Categories
jdwp-inject	any	tcp	exploit, intrusive
jdwp-version	any	tcp	version
knx-gateway-discover	-	-	discovery, safe, broadcast
knx-gateway-info	3671	efcp, udp	default, discovery, safe
krb5-enum-users	88	kerberos-sec, udp, tcp	auth, intrusive
ldap-brute	389, 636	ldap, ldapssl	intrusive, brute
ldap-novell-getpass	389, 636	ldap, ldapssl	discovery, safe
ldap-rootdse	389, 636	ldap, ldapssl, tcp, udp	discovery, safe
ldap-search	389, 636	ldap, ldapssl	discovery, safe
lexmark-config	5353, 9100	udp	discovery, safe
llmnr-resolve	-	-	discovery, safe, broadcast
lltd-discovery	-	-	broadcast, discovery, safe
lu-enum	23, 992	tn3270	intrusive, brute
maxdb-info	7210	maxdb, tcp	default, version, safe
mcafee-epo-agent	8081	tcp	version, safe
membase-brute	11210, 11211	couchbase-tap, tcp	intrusive, brute

NSE Script Name	Network Port(s)	Service / Protocol	Categories
membase-http-info	8091	http, tcp	discovery, safe
memcached-info	11211	memcached, tcp, udp	discovery, safe
metasploit-info	55553	metasploit-msgrpc	intrusive, safe
metasploit-msgrpc-brute	55553	metasploit-msgrpc	intrusive, brute
metasploit-xmlrpc-brute	55553	metasploit-xmlrpc, tcp	intrusive, brute
mikrotik-routeros-brute	8728	tcp	intrusive, brute
mmouse-brute	51010	mmouse, tcp	intrusive, brute
mmouse-exec	51010	mmouse, tcp	intrusive
modbus-discover	502	modbus	discovery, intrusive
mongodb-brute	27017	mongodb, mongod	intrusive, brute
mongodb-databases	27017	mongodb, mongod	default, discovery, safe
mongodb-info	27017	mongodb, mongod	default, discovery, safe
mqtt-subscribe	1883, 8883	mqtt, secure-mqtt, tcp	safe, discovery, version
mrinfo	-	-	discovery, safe, broadcast
msrpc-enum	-	-	safe, discovery
ms-sql-brute	1433	ms-sql-s	brute, intrusive
ms-sql-config	1433	ms-sql-s	discovery, safe

NSE Script Name	Network Port(s)	Service / Protocol	Categories
ms-sql-dac	1434	udp	discovery, safe
ms-sql-dump-hashes	1433	ms-sql-s	auth, discovery, safe
ms-sql-empty-password	1433	ms-sql-s	auth, intrusive
ms-sql-hasdbaccess	1433	ms-sql-s	auth, discovery, safe
ms-sql-info	445, 1433, 1434	ms-sql-s, smb, tcp, udp	default, discovery, safe
ms-sql-ntlm-info	1433	ms-sql-s	default, discovery, safe
ms-sql-query	1433	ms-sql-s	discovery, safe
ms-sql-tables	1433	ms-sql-s	discovery, safe
ms-sql-xp-cmdshell	1433	ms-sql-s	intrusive
mtrace	-	-	discovery, safe, broadcast
murmur-version	64738	murmur, tcp, udp	version
mysql-audit	3306	mysql	discovery, safe
mysql-brute	3306	mysql	intrusive, brute
mysql-databases	3306	mysql	discovery, intrusive
mysql-dump-hashes	3306	mysql	auth, discovery, safe
mysql-empty-password	3306	mysql	intrusive, auth

NSE Script Name	Network Port(s)	Service / Protocol	Categories
mysql-enum	3306	mysql	intrusive, brute
mysql-info	3306	mysql	default, discovery, safe
mysql-query	3306	mysql	auth, discovery, safe
mysql-users	3306	mysql	auth, intrusive
mysql-variables	3306	mysql	discovery, intrusive
mysql-vuln-cve2012-2122	3306	mysql	discovery, intrusive, vuln
nat-pmp-info	5351	nat-pmp, udp	default, discovery, safe
nat-pmp-mapport	5351	nat-pmp, udp	discovery, safe
nbd-info	10809	netbios-ns, tcp	discovery, intrusive
nbns-interfaces	137	netbios-ns, udp	default, discovery, safe
nbstat	135, 137, 139, 445	netbios, smb, tcp, udp	default, discovery, safe
ncp-enum-users	524	ncp, tcp	auth, safe
ncp-serverinfo	524	ncp, tcp	default, discovery, safe
ndmp-fs-info	10000	ndmp, tcp	discovery, safe
ndmp-version	10000	ndmp, tcp	version
nessus-brute	1241	nessus, tcp	intrusive, brute

NSE Script Name	Network Port(s)	Service / Protocol	Categories
nessus-xmlrpc-brute	8834	ssl/http, tcp	intrusive, brute
netbus-auth-bypass	12345	netbus, tcp	auth, safe, vuln
netbus-brute	12345	netbus, tcp	brute, intrusive
netbus-info	12345	netbus, tcp	default, discovery, safe
netbus-version	12345	netbus, tcp	version
nexpose-brute	3780	nexpose, tcp	intrusive, brute
nfs-ls	111	rpcbind, tcp, udp	discovery, safe
nfs-showmount	111	rpcbind, mountd, tcp, udp	discovery, safe
nfs-statfs	111	rpcbind, tcp, udp	discovery, safe
nje-node-brute	175, 2252	nje	intrusive, brute
nje-pass-brute	175, 2252	nje	intrusive, brute
nntp-ntlm-info	119, 433, 563	nntp, snews	default, discovery, safe
nping-brute	9929	nping-echo	brute, intrusive
nrpe-enum	5666	nrpe	discovery, intrusive
ntp-info	123	ntp, udp, tcp	default, discovery, safe
ntp-monlist	123	ntp, udp	discovery, intrusive
omp2-brute	9390	openvas	brute, intrusive

NSE Script Name	Network Port(s)	Service / Protocol	Categories
omp2-enum-targets	9390	openvas	discovery, safe
openflow-info	6633, 6653	openflow, tcp	default, safe
omron-info	9600	fins, tcp, udp	discovery, version
openlookup-info	5850	openlookup	default, discovery, safe, version
openvas-otp-brute	9390, 9391	openvas, tcp	intrusive, brute
openwebnet-discovery	20000	openwebnet	discovery, safe
oracle-brute	1521	oracle-tns	intrusive, brute
oracle-brute-stealth	1521	oracle-tns	intrusive, brute
oracle-enum-users	1521	oracle-tns	intrusive, auth
oracle-sid-brute	1521	oracle-tns	intrusive, brute
oracle-tns-version	1521, 1522, 1523	oracle-tns	version, safe
ovs-agent-version	8899	-	version
p2p-conficker	137, 139, 445	smb, netbios, tcp, udp	default, safe
path-mtu	-	-	safe, discovery
pcanywhere-brute	5631	pcanywheredata	intrusive, brute
pcworx-info	1962	pcworx, tcp	discovery
pgsql-brute	5432	postgresql	intrusive, brute

NSE Script Name	Network Port(s)	Service / Protocol	Categories
pjl-ready-message	9100	jetdirect	intrusive
pop3-brute	110, 995	pop3, pop3s	intrusive, brute
pop3-capabilities	110, 995	pop3, pop3s	default, discovery, safe
pop3-ntlm-info	110, 995	pop3, pop3s	default, discovery, safe
port-states	-	-	safe
pptp-version	1723	-	version
puppet-naivesigning	8140	puppet, tcp	intrusive, vuln
qconn-exec	8000	qconn, tcp	intrusive, exploit, vuln
qscan	-	-	safe, discovery
quake1-info	-	-	default, discovery, safe, version
quake3-info	27960-27970	quake3, udp	default, discovery, safe, version
quake3-master-getservers	20110, 20510, 27950, 30710	quake3-master, udp	default, discovery, safe
rdp-enum-encryption	3389	ms-wbt-server	safe, discovery
rdp-ntlm-info	3389	ms-wbt-server	default, discovery, safe
rdp-vuln-ms12-020	3389	ms-wbt-server	intrusive, vuln

NSE Script Name	Network Port(s)	Service / Protocol	Categories
realvnc-auth-bypass	5900, 5901, 5902	vnc	auth, safe, vuln
redis-brute	6379	redis	intrusive, brute
redis-info	6379	redis	discovery, safe
resolveall	-	-	safe, discovery
reverse-index	-	-	safe
rexec-brute	512	exec, tcp	brute, intrusive
rfc868-time	37	time, tcp, udp	discovery, safe, version
riak-http-info	8098	http	discovery, safe
rlogin-brute	513	login, tcp	brute, intrusive
rmi-dumpregistry	1098, 1099, 1090, 8901, 8902, 8903	java-rmi, rmiregistry	default, discovery, safe
rmi-vuln-classloader	1098, 1099, 1090, 8901, 8902, 8903	java-rmi, rmiregistry	intrusive, vuln
rpcap-brute	2002	rpcap, tcp	intrusive, brute
rpcap-info	2002	rpcap, tcp	discovery, safe
rpc-grind	any	rpcbind	version
rpcinfo	111	rpcbind, tcp, udp	discovery, default, safe, version
rsa-vuln-roca	22, 261, 271, 324, 443, 465, 563, 585, 636, 853, 989, 990, 992, 993, 994, 995, 2221, 2252, 2376, 3269, 3389, 4911, 5061, 5986, 6679, 6697, 8443, 9001, 8883	ssh, ssl	vuln, safe

NSE Script Name	Network Port(s)	Service / Protocol	Categories
rsync-brute	873	rsync, tcp	brute, intrusive
rsync-list-modules	873	rsync, tcp	discovery, safe
rtsp-methods	554	rtsp, tcp	default, safe
rtsp-url-brute	554	rtsp, tcp	brute, intrusive
rusers	any	rusersd, tcp, udp	discovery, safe
s7-info	102	iso-tsap, tcp	discovery, version
samba-vuln-cve-2012-1182	139	netbios-ssn	vuln, intrusive
servicetags	6481	udp	default, discovery, safe
shodan-api	-	-	discovery, safe, external
sip-brute	5060	sip, tcp, udp	intrusive, brute
sip-call-spoof	5060	sip, tcp, udp	discovery, intrusive
sip-enum-users	5060	sip, tcp, udp	auth, intrusive
sip-methods	5060	sip, tcp, udp	default, safe, discovery
skypev2-version	any	tcp	version
smb2-capabilities	137, 139, 445	smb, netbios, tcp, udp	safe, discovery
smb2-security-mode	137, 139, 445	smb, netbios, tcp, udp	safe, discovery, default

NSE Script Name	Network Port(s)	Service / Protocol	Categories
smb2-time	137, 139, 445	smb, netbios, tcp, udp	discovery, safe, default
smb2-vuln-uptime	137, 139, 445	smb, netbios, tcp, udp	vuln, safe
smb-brute	137, 139, 445	smb, netbios, tcp, udp	intrusive, brute
smb-double-pulsar-backdoor	137, 139, 445	smb, netbios, tcp, udp	vuln, safe, malware
smb-enum-domains	137, 139, 445	smb, netbios, tcp, udp	discovery, intrusive
smb-enum-groups	137, 139, 445	smb, netbios, tcp, udp	discovery, intrusive
smb-enum-processes	137, 139, 445	smb, netbios, tcp, udp	discovery, intrusive
smb-enum-services	139, 445	smb, netbios, tcp	discovery, intrusive, safe
smb-enum-sessions	137, 139, 445	smb, netbios, tcp, udp	discovery, intrusive
smb-enum-shares	137, 139, 445	smb, netbios, tcp, udp	discovery, intrusive
smb-enum-users	137, 139, 445	smb, netbios, tcp, udp	auth, intrusive
smb-flood	137, 139, 445	smb, netbios, tcp, udp	intrusive, dos
smb-ls	137, 139, 445	smb, netbios, tcp, udp	discovery, safe
smb-mbenum	137, 139, 445	smb, netbios, tcp, udp	discovery, safe
smb-os-discovery	137, 139, 445	smb, netbios, tcp, udp	default, discovery, safe
smb-print-text	137, 139, 445	smb, netbios, tcp, udp	intrusive

NSE Script Name	Network Port(s)	Service / Protocol	Categories
smb-protocols	137, 139, 445	smb, netbios, tcp, udp	safe, discovery
smb-psexec	137, 139, 445	smb, netbios, tcp, udp	intrusive
smb-security-mode	137, 139, 445	smb, netbios, tcp, udp	default, discovery, safe
smb-server-stats	137, 139, 445	smb, netbios, tcp, udp	discovery, intrusive
smb-system-info	137, 139, 445	smb, netbios, tcp, udp	discovery, intrusive
smb-vuln-conficker	137, 139, 445	smb, netbios, tcp, udp	intrusive, exploit, dos, vuln
smb-vuln-cve2009-3103	137, 139, 445	smb, netbios, tcp, udp	intrusive, exploit, dos, vuln
smb-vuln-cve-2017-7494	137, 139, 445	smb, netbios, tcp, udp	vuln, intrusive
smb-vuln-ms06-025	137, 139, 445	smb, netbios, tcp, udp	intrusive, exploit, dos, vuln
smb-vuln-ms07-029	137, 139, 445	smb, netbios, tcp, udp	intrusive, exploit, dos, vuln
smb-vuln-ms08-067	137, 139, 445	smb, netbios, tcp, udp	intrusive, exploit, dos, vuln
smb-vuln-ms10-054	137, 139, 445	smb, netbios, tcp, udp	vuln, intrusive, dos
smb-vuln-ms10-061	137, 139, 445	smb, netbios, tcp, udp	vuln, intrusive
smb-vuln-ms17-010	137, 139, 445	smb, netbios, tcp, udp	vuln, safe
smb-vuln-regsvc-dos	137, 139, 445	smb, netbios, tcp, udp	intrusive, exploit, dos, vuln

NSE Script Name	Network Port(s)	Service / Protocol	Categories
smb-vuln-webexec	445, 139	smb, netbios, tcp	intrusive, vuln
smb-webexec-exploit	445, 139	smb, netbios, tcp	intrusive, exploit
smtp-brute	25, 465, 587	smtp, smtps, submission	brute, intrusive
smtp-commands	25, 465, 587	smtp, smtps, submission	default, discovery, safe
smtp-enum-users	25, 465, 587	smtp, smtps, submission	auth, external, intrusive
smtp-ntlm-info	25, 465, 587	smtp, smtps, submission	default, discovery, safe
smtp-open-relay	25, 465, 587	smtp, smtps, submission	discovery, intrusive, external
smtp-strangeport	25, 465, 587	smtp, smtps, submission	malware, safe
smtp-vuln-cve2010-4344	25, 465, 587	smtp, smtps, submission	exploit, intrusive, vuln
smtp-vuln-cve2011-1720	25, 465, 587	smtp, smtps, submission	intrusive, vuln
smtp-vuln-cve2011-1764	25, 465, 587	smtp, smtps, submission	intrusive, vuln
sniffer-detect	-	-	discovery, intrusive
snmp-brute	161	snmp, udp	intrusive, brute
snmp-hh3c-logins	161	snmp, udp	default, discovery, safe
snmp-info	161	snmp, udp	default, version, safe

NSE Script Name	Network Port(s)	Service / Protocol	Categories
snmp-interfaces	161	snmp, udp	default, discovery, safe
snmp-ios-config	161	snmp, udp	intrusive
snmp-netstat	161	snmp, udp	default, discovery, safe
snmp-processes	161	snmp, udp	default, discovery, safe
snmp-sysdescr	161	snmp, udp	default, discovery, safe
snmp-win32-services	161	snmp, udp	default, discovery, safe
snmp-win32-shares	161	snmp, udp	default, discovery, safe
snmp-win32-software	161	snmp, udp	default, discovery, safe
snmp-win32-users	161	snmp, udp	default, auth, safe
socks-auth-info	1080, 9050	socks, socks5, tor-socks	discovery, safe, default
socks-brute	1080, 9050	socks, socks5, tor-socks	brute, intrusive
socks-open-proxy	1080, 9050	socks, socks5, tor-socks	default, discovery, external, safe
ssh2-enum-algos	22	ssh	safe, discovery
ssh-auth-methods	22	ssh	auth, intrusive

NSE Script Name	Network Port(s)	Service / Protocol	Categories
ssh-brute	22	ssh	brute, intrusive
ssh-hostkey	22	ssh	safe, default, discovery
ssh-publickey-acceptance	22	ssh	auth, intrusive
ssh-run	22	ssh	intrusive
sshv1	22	ssh	default, safe
ssl-ccs-injection	261, 271, 324, 443, 465, 563, 585, 636, 853, 989, 990, 992, 993, 994, 995, 2221, 2252, 2376, 3269, 3389, 4911, 5061, 5986, 6679, 6697, 8443, 9001, 8883	ssl	vuln, safe
ssl-cert-intaddr	261, 271, 324, 443, 465, 563, 585, 636, 853, 989, 990, 992, 993, 994, 995, 2221, 2252, 2376, 3269, 3389, 4911, 5061, 5986, 6679, 6697, 8443, 9001, 8883	ssl	vuln, discovery, safe
ssl-cert	261, 271, 324, 443, 465, 563, 585, 636, 853, 989, 990, 992, 993, 994, 995, 2221, 2252, 2376, 3269, 3389, 4911, 5061, 5986, 6679, 6697, 8443, 9001, 8883	ssl	default, safe, discovery
ssl-date	261, 271, 324, 443, 465, 563, 585, 636, 853, 989, 990, 992, 993, 994, 995, 2221, 2252, 2376, 3269, 3389, 4911, 5061, 5986, 6679, 6697, 8443, 9001, 8883	ssl	discovery, safe, default
ssl-dh-params	261, 271, 324, 443, 465, 563, 585, 636, 853, 989, 990, 992, 993, 994, 995, 2221, 2252, 2376, 3269, 3389, 4911, 5061, 5986, 6679, 6697, 8443, 9001, 8883	ssl	vuln, safe
ssl-enum-ciphers	261, 271, 324, 443, 465, 563, 585, 636, 853, 989, 990, 992, 993, 994, 995, 2221, 2252, 2376, 3269, 3389, 4911, 5061, 5986, 6679, 6697, 8443, 9001, 8883	ssl	discovery, intrusive

NSE Script Name	Network Port(s)	Service / Protocol	Categories
ssl-heartbleed	261, 271, 324, 443, 465, 563, 585, 636, 853, 989, 990, 992, 993, 994, 995, 2221, 2252, 2376, 3269, 3389, 4911, 5061, 5986, 6679, 6697, 8443, 9001, 8883	ssl	vuln, safe
ssl-known-key	261, 271, 324, 443, 465, 563, 585, 636, 853, 989, 990, 992, 993, 994, 995, 2221, 2252, 2376, 3269, 3389, 4911, 5061, 5986, 6679, 6697, 8443, 9001, 8883	ssl	safe, discovery, vuln, default
ssl-poodle	261, 271, 324, 443, 465, 563, 585, 636, 853, 989, 990, 992, 993, 994, 995, 2221, 2252, 2376, 3269, 3389, 4911, 5061, 5986, 6679, 6697, 8443, 9001, 8883	ssl	vuln, safe
sslv2-drown	261, 271, 324, 443, 465, 563, 585, 636, 853, 989, 990, 992, 993, 994, 995, 2221, 2252, 2376, 3269, 3389, 4911, 5061, 5986, 6679, 6697, 8443, 9001, 8883	ssl	intrusive, vuln
sslv2	261, 271, 324, 443, 465, 563, 585, 636, 853, 989, 990, 992, 993, 994, 995, 2221, 2252, 2376, 3269, 3389, 4911, 5061, 5986, 6679, 6697, 8443, 9001, 8883	ssl	default, safe
sstp-discover	261, 271, 324, 443, 465, 563, 585, 636, 853, 989, 990, 992, 993, 994, 995, 2221, 2252, 2376, 3269, 3389, 4911, 5061, 5986, 6679, 6697, 8443, 9001, 8883	ssl	discovery, default, safe
stun-info	3478	stun, udp	discovery, safe
stun-version	3478	stun, udp	version
stuxnet-detect	137, 139, 445	smb, netbios, tcp, udp	discovery, intrusive
supermicro-ipmi-conf	49152	tcp	exploit, vuln
svn-brute	3690	svnserve, tcp	intrusive, brute

NSE Script Name	Network Port(s)	Service / Protocol	Categories
targets-asn	-	-	discovery, external, safe
targets-ipv6-map4to6	-	-	discovery
targets-ipv6-multicast-echo	-	-	discovery, broadcast
targets-ipv6-multicast-invalid-dst	-	-	discovery, broadcast
targets-ipv6-multicast-mld	-	-	discovery, broadcast
targets-ipv6-multicast-slaac	-	-	discovery, broadcast
targets-ipv6-wordlist	-	-	discovery
targets-sniffer	-	-	broadcast, discovery, safe
targets-traceroute	-	-	safe, discovery
targets-xml	-	-	safe
teamspeak2-version	8767	teamspeak2, udp	version
telnet-brute	23	telnet	brute, intrusive
telnet-encryption	23	telnet	safe, discovery
telnet-ntlm-info	23	telnet	default, discovery, safe
tftp-enum	69	udp	discovery, intrusive

NSE Script Name	Network Port(s)	Service / Protocol	Categories
tls-alpn	261, 271, 324, 443, 465, 563, 585, 636, 853, 989, 990, 992, 993, 994, 995, 2221, 2252, 2376, 3269, 3389, 4911, 5061, 5986, 6679, 6697, 8443, 9001, 8883	ssl	discovery, safe, default
tls-nextprotoneg	261, 271, 324, 443, 465, 563, 585, 636, 853, 989, 990, 992, 993, 994, 995, 2221, 2252, 2376, 3269, 3389, 4911, 5061, 5986, 6679, 6697, 8443, 9001, 8883	ssl	discovery, safe, default
tls-ticketbleed	261, 271, 324, 443, 465, 563, 585, 636, 853, 989, 990, 992, 993, 994, 995, 2221, 2252, 2376, 3269, 3389, 4911, 5061, 5986, 6679, 6697, 8443, 9001, 8883	ssl	vuln, safe
tn3270-screen	23, 992	tn3270	safe, discovery
tor-consensus-checker	-	-	external, safe
traceroute-geolocation	-	-	safe, external, discovery
tso-brute	23, 992, 623	tn3270	intrusive
tso-enum	23, 992, 623	tn3270	intrusive, brute
ubiquiti-discovery	10001	ubiquiti-discovery, udp	default, discovery, version, safe
unittest	-	-	safe
unusual-port	any	-	safe
upnp-info	1900	udp	default, discovery, safe
uptime-agent-info	9998	uptime-agent, tcp	safe, default
url-snarf	-	-	safe

NSE Script Name	Network Port(s)	Service / Protocol	Categories
ventrilo-info	3784	ventrilo, tcp, udp	default, discovery, safe, version
versant-info	5019	versant, tcp	discovery, safe
vmauthd-brute	902	ssl/vmware-auth, vmware-auth, tcp	brute, intrusive
vmware-version	80, 443, 631, 7080, 8080, 8443, 8088, 5800, 3872, 8180, 8000	http, https	discovery, safe, version
vnc-brute	5901	vnc, tcp	intrusive, brute
vnc-info	5900, 5901, 5902	vnc, tcp	default, discovery, safe
vnc-title	5900, 5901, 5902	vnc, tcp	intrusive, discovery
voldemort-info	6666	vp3, tcp	discovery, safe
vtam-enum	23, 992	tn3270	intrusive, brute
vulners	-	-	vuln, safe, external
vuze-dht-info	17555, 49160, 49161, 49162	vuze-dht, udp	discovery, safe
wdb-version	17185	wdbrpc, udp	default, safe, version, discovery, vuln
weblogic-t3-info	7001, 7002, 7003	http	default, safe, discovery, version
whois-domain	-	-	discovery, external, safe

NSE Script Name	Network Port(s)	Service / Protocol	Categories
whois-ip	-	-	discovery, external, safe
wsdd-discover	3702	udp	safe, discovery, default
x11-access	6000-6009	-	default, safe, auth
xdmcp-discover	177	xdmcp, udp	safe, discovery
xmlrpc-methods	80, 443, 631, 7080, 8080, 8443, 8088, 5800, 3872, 8180, 8000	http, https	default, safe, discovery
xmpp-brute	5222	jabber, xmpp-client	brute, intrusive
xmpp-info	5222, 5269	jabber, xmpp-client, xmpp-server	default, safe, discovery, version

Showing 1 to 604 of 604 entries

NSE script categories

Currently there are 14 categories of NSE scripts in total. The categories include:

- auth
- broadcast
- brute
- default
- discovery
- dos
- exploit
- external
- fuzzer
- intrusive
- malware
- safe
- version
- vuln

More information about NSE script categories and their description can be found here.

How to use NSE scripts

Nmap is very flexible when it comes to running NSE scripts. For instance, it allows you to run a single script or multiple scripts in one shot using a single nmap command.

Here is a simplest example of running a single script to enumerate OS version of a target Windows system over the SMB protocol:

```
nmap -p 445 --script smb-os-discovery <target>
```

Here is an example of running multiple scripts in one shot, enumerating OS version, network shares and the NetBIOS information of a target Windows system:

```
nmap -p 139,445 --script smb-os-discovery,smb-enum-services,nbstat <target>
```

Below are a few examples of how you can run multiple scripts based on the category criteria alone:

```
nmap --script discovery <target>
nmap --script "default and safe" <target>
nmap --script "not intrusive" <target>
```

You can also use wildcards (*) to specify multiple scripts based on their name and combine it with a category criteria, e.g.:

```
nmap --script "http-* and (default or safe or intrusive)" <target>
```

Note that some scripts have arguments, which you can provide via the `--script-args` option. Here's an example of SSH login brute forcing using a custom user list and password list:

```
nmap -p 22 --script ssh-brute --script-args
userdb=users.txt,passdb=pwds.txt,brute.threads=4 <target>
```

To find out which arguments are applicable in which script is a bit tricky. Sometimes even reading the source code of the script will not help you, because the arguments could be processed in the NSE library that the script is dependent on.

The best way to find out all the script arguments is to use the official https://nmap.org/nsedoc/ documentation. The above Nmap script list / interactive spreadsheet provides links directly to each script manual page with all the details, including the script arguments.

NSE is very powerful and the information here is really only scratching the surface. For more details and examples of how to use NSE scripts, I encourage you to visit the official Usage and Examples page.

How to debug NSE script

Sometimes you may encounter a problem with a NSE script, for example you may be wondering if a particular script is running at all or if it is doing what it is supposed to be doing.

Here are couple of tips you can try to debug a NSE script:

1. Increase verbosity level using the `-v` switch. NSE engine will start producing more output and showing you little more what is going on. Note you can also increase the verbosity using multiple `-vv` or set the level directly (max is `-v3`).
2. Increase debug level using the `-d` switch. This will start producing debugging information with even more details. You can also use multiple `-dd` or set the debug level directly (up to `-d9` which is max).
3. Use the `--script-trace` switch, which will show all the network data that are being sent and received.
4. Lastly you can review the source code of the script and even insert some debugging messages by yourself. The scripts are typically located in the `/usr/share/nmap/scripts` folder.

One of the typical problems why NSE scripts are not functioning properly or not running at all is that you are not running nmap as a root user, but only as a normal user. Although most NSE scripts do not require root privileges, some of them do. For more information, see why nmap needs root privileges.

Conclusion

Hopefully this article provided some value for you and gave you the ability to orientate yourself better in the world of NSE scripts.

Nmap scripts have been around for many years, they are well tested and it is always prudent to incorporate them into our penetration tests.

SHARE THIS

TAGS | Automation | Cheatsheet | ICMP | Nmap | NSE | NSE debugging | Portscan | Scanner | Scripting | Spreadsheet | TCP | UDP