# 第十二课 MetaSploit扫描探测模块目录讲解

**Author：陈殷**

**公众号：山丘安全攻防实验室**

Metaspoilt内置了很多强大的模块，在渗透测试 (Penetration Testing)中无疑会给我们带来很大的便利

在下面的列表，我们将MetasPoilt的所有扫描模块进行了整理和说明，方便在渗透测试 (Penetration Testing)中直接明了的查询

```
Name     描述
----     -----------
auxiliary/admin/appletv/appletv_display_image    苹果电视图像遥控器
auxiliary/admin/appletv/appletv_display_video    苹果电视视频遥控器
auxiliary/gather/windows_deployment_services_shares microsoftwindows部署服务自动收集程序
auxiliary/scanner/acpp/login     苹果机场ACPP认证扫描仪
auxiliary/scanner/afp/afp_login 苹果备案协议登录实用工具
auxiliary/scanner/afp/afp_server_info    苹果文件协议信息枚举器
auxiliary/scanner/backdoor/energizer_duo_detect 劲量二特洛伊扫描器
auxiliary/scanner/chargen/chargen_probe Chargen调查工具
auxiliary/scanner/couchdb/couchdb_enum  CouchDB Enum效用
auxiliary/scanner/couchdb/couchdb_login CouchDB登录工具
auxiliary/scanner/db2/db2_auth  DB2身份验证蛮力实用程序
auxiliary/scanner/db2/db2_version   DB2探针实用程序
auxiliary/scanner/db2/discovery DB2发现服务检测
auxiliary/scanner/dcerpc/endpoint_mapper     端点映射器服务发现
auxiliary/scanner/dcerpc/hidden 隐藏的DCERPC服务发现
auxiliary/scanner/dcerpc/management 远程管理接口发现
auxiliary/scanner/dcerpc/tcp_dcerpc_auditor DCERPC TCP服务审计
auxiliary/scanner/dcerpc/windows_deployment_services    Microsoft Windows部署服务自动检索
auxiliary/scanner/dect/call_scanner DECT调用扫描仪
auxiliary/scanner/dect/station_scanner  DECT基站扫描仪
auxiliary/scanner/discovery/arp_sweep   ARP扫描本地网络发现
auxiliary/scanner/discovery/empty_udp   UDP空探测器
auxiliary/scanner/discovery/ipv6_multicast_ping IPv6链接本地/节点本地Ping发现
auxiliary/scanner/discovery/ipv6_neighbor   IPv6本地邻居发现
auxiliary/scanner/discovery/ipv6_neighbor_router_advertisement  IPv6本地邻居发现使用路由器广告
auxiliary/scanner/discovery/udp_probe   UDP服务探测器
auxiliary/scanner/discovery/udp_sweep   UDP服务清洁工
auxiliary/scanner/dlsw/dlsw_leak_capture     思科DLSw信息披露扫描仪
auxiliary/scanner/dns/dns_amp   DNS放大扫描
auxiliary/scanner/elasticsearch/indices_enum     弹性搜索指数枚举效用
auxiliary/scanner/emc/alphastor_devicemanager   EMC AlphaStor设备管理器服务
auxiliary/scanner/emc/alphastor_librarymanager  EMC AlphaStor Library Manager服务
auxiliary/scanner/etcd/open_key_scanner Etcd密钥API信息收集
auxiliary/scanner/etcd/version  Etcd版本扫描仪
auxiliary/scanner/finger/finger_users    手指服务用户枚举数
```

```
auxiliary/scanner/ftp/anonymous 匿名FTP访问检测
auxiliary/scanner/ftp/bison_ftp_traversal   BisonWare BisonFTP服务器3.5目录遍历信息公开
auxiliary/scanner/ftp/colorado_ftp_traversal    ColoradoFTP Server 1.3构建8个目录遍历信息公开
auxiliary/scanner/ftp/easy_file_sharing_ftp 轻松的文件共享FTP服务器3.6目录遍历
auxiliary/scanner/ftp/ftp_login FTP认证扫描仪
auxiliary/scanner/ftp/ftp_version   FTP版本扫描仪
auxiliary/scanner/ftp/konica_ftp_traversal  柯尼卡美能达FTP实用工具1.00目录遍历信息披露
auxiliary/scanner/ftp/pcman_ftp_traversal   PCMan FTP服务器2.0.7目录遍历信息公开
auxiliary/scanner/ftp/titanftp_xcrc_traversal   泰坦FTP XCRC目录遍历信息公开
auxiliary/scanner/gopher/gopher_gophermap   金花鼠gophermap扫描仪
auxiliary/scanner/gprs/gtp_echo 三磷酸鸟苷回声扫描仪
auxiliary/scanner/h323/h323_version H.323版本扫描仪
auxiliary/scanner/http/a10networks_ax_directory_traversal   A10网络AX负载均衡器目录遍历
auxiliary/scanner/http/accellion_fta_statecode_file_read    Accellion FTA 'statecode' Cookie任意文件读取
auxiliary/scanner/http/adobe_xml_inject adobexml外部实体注入
auxiliary/scanner/http/advantech_webaccess_login    Advantech WebAccess登录
auxiliary/scanner/http/allegro_rompager_misfortune_cookie   Allegro Software RomPager ' evil Cookie' (CVE-2014-9222)扫描仪
auxiliary/scanner/http/apache_activemq_source_disclosure    Apache ActiveMQ JSP文件源代码公开
auxiliary/scanner/http/apache_activemq_traversal    Apache ActiveMQ目录遍历
auxiliary/scanner/http/apache_mod_cgi_bash_env  Apache mod_cgi Bash环境变量注入(Shellshock)扫描器
auxiliary/scanner/http/apache_optionsbleed  Apache Optionsbleed扫描仪
auxiliary/scanner/http/apache_userdir_enum  Apache“mod_userdir”用户枚举
auxiliary/scanner/http/appletv_login    苹果电视AirPlay登录实用程序
auxiliary/scanner/http/atlassian_crowd_fileaccess   XML实体扩展远程文件访问
auxiliary/scanner/http/axis_local_file_include  Apache Axis2 v1.4.1本地文件包含
auxiliary/scanner/http/axis_login   Apache Axis2蛮力实用程序
auxiliary/scanner/http/backup_file  HTTP备份文件扫描器
auxiliary/scanner/http/barracuda_directory_traversal    梭鱼多产品“地区”目录遍历
auxiliary/scanner/http/bavision_cam_login   BAVision IP摄像头Web服务器登录
auxiliary/scanner/http/binom3_login_config_pass_dump    Binom3 Web管理登录扫描器，配置和密码文件转储
auxiliary/scanner/http/bitweaver_overlay_type_traversal Bitweaver overlay_type目录遍历
auxiliary/scanner/http/blind_sql_query  HTTP盲SQL注入扫描器
auxiliary/scanner/http/bmc_trackit_passwd_reset BMC TrackIt !未经身份验证的任意用户密码更改
auxiliary/scanner/http/brute_dirs   HTTP目录蛮力扫描器
auxiliary/scanner/http/buffalo_login    水牛NAS登录实用程序
auxiliary/scanner/http/buildmaster_login    Inedo BuildMaster登录扫描器
auxiliary/scanner/http/caidao_bruteforce_login  中国菜刀后门蛮力
auxiliary/scanner/http/canon_wireless   佳能打印机无线配置公开
auxiliary/scanner/http/cert HTTP SSL证书检查器
auxiliary/scanner/http/cgit_traversal   cgit目录遍历
auxiliary/scanner/http/chef_webui_login Chef Web UI蛮力工具
auxiliary/scanner/http/chromecast_webserver Chromecast Web服务器扫描程序
auxiliary/scanner/http/chromecast_wifi  Chromecast Wifi枚举
auxiliary/scanner/http/cisco_asa_asdm   思科ASDM Bruteforce登录工具
```

```
auxiliary/scanner/http/cisco_device_manager Cisco设备HTTP设备管理器访问
auxiliary/scanner/http/cisco_directory_traversal    Cisco ASA目录遍历
auxiliary/scanner/http/cisco_firepower_download 思科火力管理控制台6.0后，Auth报告下载目录遍历
auxiliary/scanner/http/cisco_firepower_login    思科火力管理控制台6.0登录
auxiliary/scanner/http/cisco_ios_auth_bypass    Cisco IOS HTTP未经授权的管理访问
auxiliary/scanner/http/cisco_ironport_enum  Cisco Ironport Bruteforce登录工具
auxiliary/scanner/http/cisco_nac_manager_traversal  Cisco网络访问管理器目录遍历漏洞
auxiliary/scanner/http/cisco_ssl_vpn    思科SSL VPN Bruteforce登录工具
auxiliary/scanner/http/cisco_ssl_vpn_priv_esc   Cisco ASA SSL VPN权限升级漏洞
auxiliary/scanner/http/clansphere_traversal 本地文件包含漏洞
auxiliary/scanner/http/cnpilot_r_web_login_loot 形成层cnPilot r200/r201登录扫描器和配置转储
auxiliary/scanner/http/coldfusion_locale_traversal  ColdFusion服务器检查
auxiliary/scanner/http/coldfusion_version   ColdFusion版本扫描仪
auxiliary/scanner/http/concrete5_member_list    混凝土5成员列表枚举
auxiliary/scanner/http/copy_of_file HTTP复制文件扫描器
auxiliary/scanner/http/crawler  网站爬虫
auxiliary/scanner/http/dell_idrac   戴尔iDRAC默认登录
auxiliary/scanner/http/dicoogle_traversal   Dicoogle PACS Web服务器目录遍历
auxiliary/scanner/http/dir_listing  HTTP目录列表扫描器
auxiliary/scanner/http/dir_scanner  HTTP目录扫描
auxiliary/scanner/http/dir_webdav_unicode_bypass    IIS6 WebDAV Unicode Auth旁路目录扫描器
auxiliary/scanner/http/directadmin_login    DirectAdmin网络控制面板登录实用工具
auxiliary/scanner/http/dlink_dir_300_615_http_login D-Link DIR-300A / DIR-320 / DIR-615D HTTP登录实用程序
auxiliary/scanner/http/dlink_dir_615h_http_login    D-Link DIR-615H HTTP登录实用工具
auxiliary/scanner/http/dlink_dir_session_cgi_http_login D-Link DIR-300B / DIR-600B / DIR-815 / DIR-645 HTTP登录实用程序
auxiliary/scanner/http/dlink_user_agent_backdoor    D-Link用户代理后门扫描器
auxiliary/scanner/http/dnalims_file_retrieve    DnaLIMS目录遍历
auxiliary/scanner/http/docker_version   Docker服务器版本扫描器
auxiliary/scanner/http/dolibarr_login   Dolibarr ERP/CRM登录工具
auxiliary/scanner/http/drupal_views_user_enum   Drupal查看模块用户枚举
auxiliary/scanner/http/ektron_cms400net Ektron CMS400。网络默认密码扫描器
auxiliary/scanner/http/elasticsearch_traversal  对ElasticSearch快照API目录进行遍历
auxiliary/scanner/http/enum_wayback Archive.org存储域url
auxiliary/scanner/http/epmp1000_dump_config 形成层epmp1000转储设备配置
auxiliary/scanner/http/epmp1000_dump_hashes ePMP 1000 'ping'密码散列提取器(最多v2.5)
auxiliary/scanner/http/epmp1000_get_chart_cmd_exec  形成层ePMP 1000 'get_chart'命令注入(v3.1-3.5-RC7)
auxiliary/scanner/http/epmp1000_ping_cmd_exec   形成层ePMP 1000 'ping'命令注入(最多v2.5)
auxiliary/scanner/http/epmp1000_reset_pass  epmp1000账户密码重置
auxiliary/scanner/http/epmp1000_web_login   形成层epmp1000登录扫描仪
auxiliary/scanner/http/error_sql_injection  基于HTTP错误的SQL注入扫描器
auxiliary/scanner/http/es_file_explorer_open_port   ES文件资源管理器打开端口
auxiliary/scanner/http/etherpad_duo_login   EtherPAD Duo登录Bruteforce实用程序
```

```
auxiliary/scanner/http/f5_bigip_virtual_server  F5 BigIP HTTP虚拟服务器扫描器
auxiliary/scanner/http/f5_mgmt_scanner  F5网络设备管理接口扫描器
auxiliary/scanner/http/file_same_name_dir   HTTP文件同名目录扫描器
auxiliary/scanner/http/files_dir    HTTP有趣的文件扫描器
auxiliary/scanner/http/fortinet_ssl_vpn Fortinet SSL VPN Bruteforce登录工具
auxiliary/scanner/http/frontpage_credential_dump    FrontPage .pwd文件凭据转储
auxiliary/scanner/http/frontpage_login  FrontPage服务器扩展匿名登录扫描
auxiliary/scanner/http/gavazzi_em_login_loot    Carlo Gavazzi能源表-登录蛮力，提取信息和转储植物数据库
auxiliary/scanner/http/git_scanner  HTTP Git扫描仪
auxiliary/scanner/http/gitlab_login GitLab登录工具
auxiliary/scanner/http/gitlab_user_enum GitLab用户枚举
auxiliary/scanner/http/glassfish_login  玻璃鱼蛮力效用
auxiliary/scanner/http/glassfish_traversal  路径遍历在Oracle GlassFish服务器开源版
auxiliary/scanner/http/goahead_traversal    此GoAhead嵌入式Web服务器目录遍历
auxiliary/scanner/http/groupwise_agents_http_traversal  Novell Groupwise代理HTTP目录遍历
auxiliary/scanner/http/host_header_injection    HTTP主机头注入检测
auxiliary/scanner/http/hp_imc_bims_downloadservlet_traversal    HP智能管理BIMS下载servlet目录遍历
auxiliary/scanner/http/hp_imc_faultdownloadservlet_traversal    HP智能管理FaultDownloadServlet目录遍历
auxiliary/scanner/http/hp_imc_ictdownloadservlet_traversal  HP智能管理IctDownloadServlet目录遍历
auxiliary/scanner/http/hp_imc_reportimgservlt_traversal HP智能管理报告gservlt目录遍历
auxiliary/scanner/http/hp_imc_som_file_download HP智能管理SOM文件下载下载下载
auxiliary/scanner/http/hp_sitescope_getfileinternal_fileaccess  HP SiteScope SOAP调用getFileInternal远程文件访问
auxiliary/scanner/http/hp_sitescope_getsitescopeconfiguration   HP SiteScope SOAP调用getSiteScopeConfiguration配置访问
auxiliary/scanner/http/hp_sitescope_loadfilecontent_fileaccess  HP SiteScope SOAP调用loadFileContent远程文件访问
auxiliary/scanner/http/hp_sys_mgmt_login    HP系统管理主页登录工具
auxiliary/scanner/http/http_header  HTTP报头检测
auxiliary/scanner/http/http_hsts    HTTP严格传输安全(HSTS)检测
auxiliary/scanner/http/http_login   HTTP登录工具
auxiliary/scanner/http/http_put HTTP可写路径放入/删除文件访问
auxiliary/scanner/http/http_sickrage_password_leak  HTTP病假密码泄露
auxiliary/scanner/http/http_traversal   通用的HTTP目录遍历实用程序
auxiliary/scanner/http/http_version HTTP版本检测
auxiliary/scanner/http/httpbl_lookup    Http:提单查询
auxiliary/scanner/http/httpdasm_directory_traversal Httpdasm目录遍历
auxiliary/scanner/http/iis_internal_ip  Microsoft IIS HTTP内部IP公开
auxiliary/scanner/http/iis_shortname_scanner    Microsoft IIS短名称漏洞扫描器
auxiliary/scanner/http/influxdb_enum    InfluxDB Enum效用
auxiliary/scanner/http/infovista_enum   InfoVista VistaPortal应用程序Bruteforce登录实用工具
auxiliary/scanner/http/intel_amt_digest_bypass  Intel AMT摘要身份验证绕过扫描器
auxiliary/scanner/http/ipboard_login    IP板登录辅助模块
auxiliary/scanner/http/jboss_status JBoss状态Servlet信息收集
auxiliary/scanner/http/jboss_vulnscan   JBoss漏洞扫描器
auxiliary/scanner/http/jenkins_command  Jenkins-CI未经身份验证的脚本控制台扫描器
auxiliary/scanner/http/jenkins_enum Jenkins-CI枚举
```

```
auxiliary/scanner/http/jenkins_login    Jenkins-CI登录工具
auxiliary/scanner/http/joomla_bruteforce_login  Joomla Bruteforce登录实用程序
auxiliary/scanner/http/joomla_ecommercewd_sqli_scanner  网络黄金国电子商务WD为Joomla!search_category_id SQL注入扫描器
auxiliary/scanner/http/joomla_gallerywd_sqli_scanner    Joomla的WD画廊!未经验证的SQL注入扫描器
auxiliary/scanner/http/joomla_pages Joomla页扫描
auxiliary/scanner/http/joomla_plugins   Joomla插件扫描
auxiliary/scanner/http/joomla_version   Joomla版本扫描仪
auxiliary/scanner/http/kodi_traversal   Kodi 17.0本地文件包含漏洞
auxiliary/scanner/http/linknat_vos_traversal    Linknat Vos管理器遍历
auxiliary/scanner/http/linksys_e1500_traversal  Linksys E1500目录遍历漏洞
auxiliary/scanner/http/litespeed_source_disclosure  LiteSpeed源代码公开/下载
auxiliary/scanner/http/lucky_punch  HTTP Microsoft SQL注入表XSS感染
auxiliary/scanner/http/majordomo2_directory_traversal   遍历目录
auxiliary/scanner/http/manageengine_desktop_central_login   ManageEngine桌面中央登录实用程序
auxiliary/scanner/http/manageengine_deviceexpert_traversal  ManageEngine DeviceExpert 5.6调度esultviewer文件名遍历
auxiliary/scanner/http/manageengine_deviceexpert_user_creds ManageEngine DeviceExpert用户凭证
auxiliary/scanner/http/manageengine_securitymanager_traversal ManageEngine SecurityManager + 5.5目录遍历
auxiliary/scanner/http/mediawiki_svg_fileaccess MediaWiki SVG XML实体展开远程文件访问
auxiliary/scanner/http/meteocontrol_weblog_extractadmin Meteocontrol网络日志密码提取器
auxiliary/scanner/http/mod_negotiation_brute    Apache HTTPD mod_negotiation文件名Bruter
auxiliary/scanner/http/mod_negotiation_scanner  Apache HTTPD mod_negotiation扫描器
auxiliary/scanner/http/ms09_020_webdav_unicode_bypass   IIS6 WebDAV Unicode认证绕过
auxiliary/scanner/http/ms15_034_http_sys_memory_dump    HTTP协议栈请求处理HTTP。系统内存信息公开
auxiliary/scanner/http/mybook_live_login    西部数字我的书实时登录实用程序
auxiliary/scanner/http/netdecision_traversal    NetDecision夜视服务器目录遍历
auxiliary/scanner/http/netgear_sph200d_traversal    Netgear SPH200D目录遍历漏洞
auxiliary/scanner/http/nginx_source_disclosure  Nginx源代码公开/下载
auxiliary/scanner/http/novell_file_reporter_fsfui_fileaccess    NFR代理FSFUI记录任意远程文件访问
auxiliary/scanner/http/novell_file_reporter_srs_fileaccess  NFR代理SRS记录任意远程文件访问
auxiliary/scanner/http/novell_mdm_creds Novell Zenworks移动设备管理管理凭证
auxiliary/scanner/http/ntlm_info_enumeration    通过NTLM身份验证的主机信息枚举
auxiliary/scanner/http/octopusdeploy_login  八达通部署登入工具
auxiliary/scanner/http/onion_omega2_login   洋葱Omega2登录蛮力
auxiliary/scanner/http/open_proxy   HTTP开放代理检测
auxiliary/scanner/http/openmind_messageos_login OpenMind消息操作系统门户登录蛮力实用程序
auxiliary/scanner/http/options  HTTP选项检测
auxiliary/scanner/http/oracle_demantra_database_credentials_leak    Oracle Demantra数据库凭证泄漏
auxiliary/scanner/http/oracle_demantra_file_retrieval   Oracle通过认证绕过任意文件检索
auxiliary/scanner/http/oracle_ilom_login    Oracle ILO经理登录蛮力效用
```

```
auxiliary/scanner/http/owa_ews_login    OWA Exchange Web服务(EWS)登录扫描器
auxiliary/scanner/http/owa_iis_internal_ip  Outlook Web App (OWA) /客户端访问服务器(CAS) IIS HTTP内部IP公开
auxiliary/scanner/http/owa_login    Outlook Web应用(OWA)蛮力工具
auxiliary/scanner/http/phpmyadmin_login PhpMyAdmin登录扫描仪
auxiliary/scanner/http/pocketpad_login  PocketPAD登录蛮力工具
auxiliary/scanner/http/prev_dir_same_name_file  HTTP前一个目录文件扫描器
auxiliary/scanner/http/radware_appdirector_enum Radware AppDirector Bruteforce登录工具
auxiliary/scanner/http/rails_json_yaml_scanner  Ruby on Rails JSON处理器YAML反序列化扫描器
auxiliary/scanner/http/rails_mass_assignment    Ruby On Rails属性质量分配扫描器
auxiliary/scanner/http/rails_xml_yaml_scanner   Ruby on Rails XML处理器YAML反序列化扫描器
auxiliary/scanner/http/replace_ext  HTTP文件扩展扫描程序
auxiliary/scanner/http/rewrite_proxy_bypass Apache反向代理绕过漏洞扫描器
auxiliary/scanner/http/rfcode_reader_enum   RFCode阅读器的Web界面登录/Bruteforce实用工具
auxiliary/scanner/http/rips_traversal   rip扫描器目录遍历
auxiliary/scanner/http/riverbed_steelhead_vcx_file_read 河床钢头VCX文件读取
auxiliary/scanner/http/robots_txt   txt内容扫描器
auxiliary/scanner/http/s40_traversal    S40 0.4.2 CMS目录遍历漏洞
auxiliary/scanner/http/sap_businessobjects_user_brute   SAP BusinessObjects用户Bruteforcer
auxiliary/scanner/http/sap_businessobjects_user_brute_web   SAP BusinessObjects Web用户Bruteforcer
auxiliary/scanner/http/sap_businessobjects_user_enum    SAP BusinessObjects用户枚举
auxiliary/scanner/http/sap_businessobjects_version_enum SAP BusinessObjects版本检测
auxiliary/scanner/http/scraper  HTTP页面刮刀
auxiliary/scanner/http/sentry_cdu_enum  哨兵切换基民盟蛮力登录实用程序
auxiliary/scanner/http/servicedesk_plus_traversal   ManageEngine ServiceDesk加上路径遍历
auxiliary/scanner/http/sevone_enum  SevOne网络性能管理应用程序蛮力登录实用工具
auxiliary/scanner/http/simple_webserver_traversal   简单的Web服务器2.3-RC1目录遍历
auxiliary/scanner/http/smt_ipmi_49152_exposure  超微型板载IPMI端口49152敏感文件曝光
auxiliary/scanner/http/smt_ipmi_cgi_scanner 超微板载IPMI CGI漏洞扫描器
auxiliary/scanner/http/smt_ipmi_static_cert_scanner 超微型板载IPMI静态SSL证书扫描仪
auxiliary/scanner/http/smt_ipmi_url_redirect_traversal  超微型板载IPMI url_redirect.cgi认证目录遍历
auxiliary/scanner/http/soap_xml HTTP SOAP动词/名词蛮力扫描器
auxiliary/scanner/http/sockso_traversal Sockso音乐主机服务器1.5目录遍历
auxiliary/scanner/http/splunk_web_login Splunk Web界面登录实用工具
auxiliary/scanner/http/springcloud_traversal    Spring云配置服务器目录遍历
auxiliary/scanner/http/squid_pivot_scanning Squid代理端口扫描器
auxiliary/scanner/http/squiz_matrix_user_enum   Squiz矩阵用户枚举扫描器
auxiliary/scanner/http/ssl  HTTP SSL证书信息
auxiliary/scanner/http/ssl_version  HTTP SSL/TLS版本检测(贵宾扫描器)
auxiliary/scanner/http/support_center_plus_directory_traversal ManageEngine支持中心加上目录遍历
auxiliary/scanner/http/surgenews_user_creds SurgeNews用户凭证
auxiliary/scanner/http/svn_scanner  HTTP Subversion扫描仪
auxiliary/scanner/http/svn_wcdb_scanner SVN wc.db扫描仪
```

```
auxiliary/scanner/http/sybase_easerver_traversal    Sybase Easerver 6.3目录遍历
auxiliary/scanner/http/symantec_brightmail_ldapcreds    赛门铁克消息网关10暴露存储广告密码漏洞
auxiliary/scanner/http/symantec_brightmail_logfile  赛门铁克消息网关9.5日志文件下载漏洞
auxiliary/scanner/http/symantec_web_gateway_login   赛门铁克Web网关登录实用工具
auxiliary/scanner/http/titan_ftp_admin_pwd  泰坦FTP管理密码泄露
auxiliary/scanner/http/title    HTTP HTML标题标签内容抓取器
auxiliary/scanner/http/tomcat_enum  Apache Tomcat用户枚举
auxiliary/scanner/http/tomcat_mgr_login Tomcat应用程序管理器登录实用程序
auxiliary/scanner/http/totaljs_traversal    .js之前的3.2.4目录遍历
auxiliary/scanner/http/tplink_traversal_noauth  TP-Link无线精简N接入点目录遍历漏洞
auxiliary/scanner/http/trace    HTTP跨站点跟踪检测
auxiliary/scanner/http/trace_axd    HTTP痕迹。axd内容扫描仪
auxiliary/scanner/http/typo3_bruteforce Typo3登录Bruteforcer
auxiliary/scanner/http/vcms_login   V-CMS登录工具
auxiliary/scanner/http/verb_auth_bypass HTTP谓词身份验证绕过扫描器
auxiliary/scanner/http/vhost_scanner    HTTP虚拟主机蛮力扫描器
auxiliary/scanner/http/wangkongbao_traversal    网箱包CNS-1000和1100 UTM目录遍历
auxiliary/scanner/http/web_vulndb   HTTP Vuln扫描仪
auxiliary/scanner/http/webdav_internal_ip   HTTP WebDAV内部IP扫描器
auxiliary/scanner/http/webdav_scanner   HTTP WebDAV扫描仪
auxiliary/scanner/http/webdav_website_content   HTTP WebDAV网站内容扫描器
auxiliary/scanner/http/webpagetest_traversal    WebPageTest目录遍历
auxiliary/scanner/http/wildfly_traversal    WildFly目录遍历
auxiliary/scanner/http/wordpress_content_injection  WordPress REST API内容注入
auxiliary/scanner/http/wordpress_cp_calendar_sqli   WordPress CP多视图日历未经身份验证的SQL注入扫描器
auxiliary/scanner/http/wordpress_ghost_scanner  WordPress XMLRPC幽灵漏洞扫描器
auxiliary/scanner/http/wordpress_login_enum WordPress蛮力和用户枚举工具
auxiliary/scanner/http/wordpress_multicall_creds    Wordpress xml - rpc系统。多调用凭据收集器
auxiliary/scanner/http/wordpress_pingback_access    Wordpress广播定位器
auxiliary/scanner/http/wordpress_scanner    Wordpress扫描仪
auxiliary/scanner/http/wordpress_xmlrpc_login   Wordpress XML-RPC用户名/密码登录扫描器
auxiliary/scanner/http/wp_arbitrary_file_deletion   任意文件删除
auxiliary/scanner/http/wp_contus_video_gallery_sqli WordPress Contus视频画廊未经验证的SQL注入扫描器
auxiliary/scanner/http/wp_dukapress_file_read   WordPress DukaPress插件文件读取漏洞
auxiliary/scanner/http/wp_gimedia_library_file_read WordPress gimedia库插件目录遍历漏洞
auxiliary/scanner/http/wp_mobile_pack_info_disclosure   WordPress移动包信息泄露漏洞
auxiliary/scanner/http/wp_mobileedition_file_read   WordPress移动版文件读取漏洞
auxiliary/scanner/http/wp_nextgen_galley_file_read  WordPress NextGEN图库目录读取漏洞
auxiliary/scanner/http/wp_simple_backup_file_read   WordPress简单备份文件读取漏洞
```

```
auxiliary/scanner/http/wp_subscribe_comments_file_read  WordPress订阅评论文件读取漏洞
auxiliary/scanner/http/xpath    HTTP盲XPATH 1.0注入器
auxiliary/scanner/http/yaws_traversal   Yaws Web服务器目录遍历
auxiliary/scanner/http/zabbix_login Zabbix服务器蛮力实用程序
auxiliary/scanner/http/zenworks_assetmanagement_fileaccess  Novell ZENworks资产管理7.5远程文件访问
auxiliary/scanner/http/zenworks_assetmanagement_getconfig   Novell ZENworks资产管理7.5配置访问
auxiliary/scanner/ike/cisco_ike_benigncertain   思科艾克信息披露
auxiliary/scanner/imap/imap_version IMAP4横幅打捞工具
auxiliary/scanner/ip/ipidseq    IPID序列扫描
auxiliary/scanner/ipmi/ipmi_cipher_zero IPMI 2.0密码零认证绕过扫描器
auxiliary/scanner/ipmi/ipmi_dumphashes  IPMI 2.0 RAKP远程SHA1密码散列检索
auxiliary/scanner/ipmi/ipmi_version IPMI信息发现
auxiliary/scanner/jenkins/jenkins_udp_broadcast_enum    Jenkins服务器广播枚举
auxiliary/scanner/kademlia/server_info  收集Kademlia服务器信息
auxiliary/scanner/llmnr/query   LLMNR查询
auxiliary/scanner/lotus/lotus_domino_hashes Lotus Domino密码散列收集器
auxiliary/scanner/lotus/lotus_domino_login  Lotus Domino蛮力实用程序
auxiliary/scanner/lotus/lotus_domino_version    Lotus Domino版本
auxiliary/scanner/mdns/query    mdn查询
auxiliary/scanner/memcached/memcached_amp   Memcached统计放大扫描仪
auxiliary/scanner/memcached/memcached_udp_version   Memcached UDP版本扫描器
auxiliary/scanner/misc/cctv_dvr_login   CCTV DVR登录扫描工具
auxiliary/scanner/misc/cisco_smart_install  确定思科智能安装终端
auxiliary/scanner/misc/clamav_control   ClamAV远程命令发送器
auxiliary/scanner/misc/dahua_dvr_auth_bypass    大华DVR Auth旁路扫描仪
auxiliary/scanner/misc/dvr_config_disclosure    多重DVR制造商配置披露
auxiliary/scanner/misc/easycafe_server_fileaccess   EasyCafe服务器远程文件访问
auxiliary/scanner/misc/ib_service_mgr_info  Borland InterBase服务经理信息
auxiliary/scanner/misc/ibm_mq_channel_brute IBM WebSphere MQ通道名称Bruteforce
auxiliary/scanner/misc/ibm_mq_enum  标识队列管理器名称和MQ版本
auxiliary/scanner/misc/ibm_mq_login IBM WebSphere MQ登录检查
auxiliary/scanner/misc/java_jmx_server  Java JMX服务器不安全的端点代码执行扫描器
auxiliary/scanner/misc/java_rmi_server  Java RMI服务器不安全的端点代码执行扫描器
auxiliary/scanner/misc/oki_scanner  OKI打印机默认登录凭证扫描
auxiliary/scanner/misc/poisonivy_control_scanner    毒葛命令与控制扫描仪
auxiliary/scanner/misc/raysharp_dvr_passwords   Ray Sharp DVR密码找回器
auxiliary/scanner/misc/rosewill_rxs3211_passwords   Rosewill RXS-3211 IP摄像头密码检索器
auxiliary/scanner/misc/sercomm_backdoor_scanner SerComm网络设备后门检测
auxiliary/scanner/misc/sunrpc_portmapper    SunRPC端口映射程序枚举器
auxiliary/scanner/misc/zenworks_preboot_fileaccess  Novell ZENworks配置管理预引导服务远程文件访问
auxiliary/scanner/mongodb/mongodb_login MongoDB登录工具
auxiliary/scanner/motorola/timbuktu_udp 摩托罗拉Timbuktu服务检测
auxiliary/scanner/mqtt/connect  MQTT认证扫描仪
auxiliary/scanner/msf/msf_rpc_login Metasploit RPC接口登录实用程序
auxiliary/scanner/msf/msf_web_login Metasploit Web界面登录实用程序
auxiliary/scanner/mssql/mssql_hashdump  该密码Hashdump
auxiliary/scanner/mssql/mssql_login 该软件登录工具
auxiliary/scanner/mssql/mssql_ping  该软件平效用
auxiliary/scanner/mssql/mssql_schemadump    该模式转储
auxiliary/scanner/mysql/mysql_authbypass_hashdump   MySQL认证绕过密码转储
```

```
auxiliary/scanner/mysql/mysql_file_enum MYSQL文件/目录的枚举器
auxiliary/scanner/mysql/mysql_hashdump  MYSQL密码Hashdump
auxiliary/scanner/mysql/mysql_login MySQL登录工具
auxiliary/scanner/mysql/mysql_schemadump    MYSQL模式转储
auxiliary/scanner/mysql/mysql_version   MySQL服务器版本枚举
auxiliary/scanner/mysql/mysql_writable_dirs MYSQL目录写测试
auxiliary/scanner/natpmp/natpmp_portscan    NAT-PMP外部端口扫描器
auxiliary/scanner/nessus/nessus_ntp_login   Nessus NTP登录实用程序
auxiliary/scanner/nessus/nessus_rest_login  Nessus RPC接口登录实用程序
auxiliary/scanner/nessus/nessus_xmlrpc_login    Nessus XMLRPC接口登录实用程序
auxiliary/scanner/nessus/nessus_xmlrpc_ping Nessus XMLRPC接口Ping实用程序
auxiliary/scanner/netbios/nbname    NetBIOS信息发现
auxiliary/scanner/nexpose/nexpose_api_login NeXpose API接口登录实用程序
auxiliary/scanner/nfs/nfsmount  NFS装载扫描仪
auxiliary/scanner/nntp/nntp_login   NNTP登录工具
auxiliary/scanner/ntp/ntp_monlist   NTP监控列表扫描器
auxiliary/scanner/ntp/ntp_nak_to_the_future 国家结核控制项目“走向未来”
auxiliary/scanner/ntp/ntp_peer_list_dos NTP模式7 PEER_LIST DoS扫描器
auxiliary/scanner/ntp/ntp_peer_list_sum_dos NTP模式7 PEER_LIST_SUM DoS扫描器
auxiliary/scanner/ntp/ntp_readvar   NTP时钟变量披露
auxiliary/scanner/ntp/ntp_req_nonce_dos NTP模式6 REQ_NONCE DRDoS扫描器
auxiliary/scanner/ntp/ntp_reslist_dos   NTP模式7 get_restricted DRDoS扫描器
auxiliary/scanner/ntp/ntp_unsettrap_dos NTP模式6解除DRDoS扫描
auxiliary/scanner/openvas/openvas_gsad_login    OpenVAS gsad Web界面登录工具
auxiliary/scanner/openvas/openvas_omp_login OpenVAS OMP登录实用程序
auxiliary/scanner/openvas/openvas_otp_login OpenVAS OTP登录工具
auxiliary/scanner/oracle/emc_sid    Oracle Enterprise Manager控制SID发现
auxiliary/scanner/oracle/isqlplus_login Oracle iSQL* +登录工具
auxiliary/scanner/oracle/isqlplus_sidbrute  Oracle iSQLPlus SID检查
auxiliary/scanner/oracle/oracle_hashdump    甲骨文密码Hashdump
auxiliary/scanner/oracle/oracle_login   Oracle RDBMS登录实用程序
auxiliary/scanner/oracle/sid_brute  Oracle TNS监听器SID Bruteforce
auxiliary/scanner/oracle/sid_enum   Oracle TNS监听器SID枚举
auxiliary/scanner/oracle/spy_sid    Oracle应用服务器间谍Servlet SID枚举
auxiliary/scanner/oracle/tnslsnr_version    Oracle TNS监听器服务版本查询
auxiliary/scanner/oracle/tnspoison_checker  Oracle TNS监听器检查
auxiliary/scanner/oracle/xdb_sid    Oracle XML DB SID发现
auxiliary/scanner/oracle/xdb_sid_brute  通过蛮力发现Oracle XML DB SID
auxiliary/scanner/pcanywhere/pcanywhere_login   PcAnywhere登录扫描仪
auxiliary/scanner/pcanywhere/pcanywhere_tcp PcAnywhere TCP服务发现
auxiliary/scanner/pcanywhere/pcanywhere_udp PcAnywhere UDP服务发现
auxiliary/scanner/pop3/pop3_login   POP3登录工具
auxiliary/scanner/pop3/pop3_version POP3横幅打捞工具
auxiliary/scanner/portmap/portmap_amp   Portmapper放大扫描
auxiliary/scanner/portscan/ack  TCP ACK防火墙扫描器
auxiliary/scanner/portscan/ftpbounce    FTP弹跳端口扫描器
auxiliary/scanner/portscan/syn  TCP SYN端口扫描器
auxiliary/scanner/portscan/tcp  TCP端口扫描器
auxiliary/scanner/portscan/xmas TCP“圣诞节”端口扫描器
auxiliary/scanner/postgres/postgres_dbname_flag_injection   PostgreSQL数据
库名称命令行标志注入
auxiliary/scanner/postgres/postgres_hashdump    Postgres密码Hashdump
auxiliary/scanner/postgres/postgres_login   PostgreSQL登录工具
auxiliary/scanner/postgres/postgres_schemadump  Postgres模式转储
auxiliary/scanner/postgres/postgres_version PostgreSQL版本探针
auxiliary/scanner/printer/canon_iradv_pwd_extract   佳能IR-Adv密码提取器
auxiliary/scanner/printer/printer_delete_file   打印机文件删除扫描器
auxiliary/scanner/printer/printer_download_file 打印机文件下载扫描器
```

```
auxiliary/scanner/printer/printer_env_vars  打印机环境变量扫描器
auxiliary/scanner/printer/printer_list_dir  打印机目录列表扫描器
auxiliary/scanner/printer/printer_list_volumes  打印机卷列表扫描器
auxiliary/scanner/printer/printer_ready_message 打印机就绪信息扫描器
auxiliary/scanner/printer/printer_upload_file  打印机文件上传扫描器
auxiliary/scanner/printer/printer_version_info  打印机版本信息扫描器
auxiliary/scanner/quake/server_info 收集地震服务器信息
auxiliary/scanner/rdp/cve_2019_0708_bluekeep  微软远程桌面RCE检查
auxiliary/scanner/rdp/ms12_020_check  MS12-020微软远程桌面检查
auxiliary/scanner/rdp/rdp_scanner  识别使用远程桌面协议(RDP)的端点
auxiliary/scanner/redis/file_upload 复述,文件上传
auxiliary/scanner/redis/redis_login 复述,登录工具
auxiliary/scanner/redis/redis_server  Redis命令执行扫描仪
auxiliary/scanner/rogue/rogue_recv  流氓网关检测:接收器
auxiliary/scanner/rogue/rogue_send  流氓网关检测:发件人
auxiliary/scanner/rservices/rexec_login rexec认证扫描仪
auxiliary/scanner/rservices/rlogin_login  远程登录命令验证扫描仪
auxiliary/scanner/rservices/rsh_login  rsh认证扫描仪
auxiliary/scanner/rsync/modules_list  Rsync模块列表
auxiliary/scanner/sap/sap_ctc_verb_tampering_user_mgmt  SAP CTC服务动词篡改用户管理
auxiliary/scanner/sap/sap_hostctrl_getcomputersystem  SAP主机代理信息披露
auxiliary/scanner/sap/sap_icf_public_info  SAP ICF / SAP /公共/信息服务敏感信息收集
auxiliary/scanner/sap/sap_icm_urlscan  SAP URL扫描仪
auxiliary/scanner/sap/sap_mgmt_con_abaplog  SAP管理控制台ABAP Syslog公开
auxiliary/scanner/sap/sap_mgmt_con_brute_login  SAP管理控制台蛮力
auxiliary/scanner/sap/sap_mgmt_con_extractusers SAP管理控制台提取用户
auxiliary/scanner/sap/sap_mgmt_con_getaccesspoints  SAP管理控制台获取访问点
auxiliary/scanner/sap/sap_mgmt_con_getenv  SAP管理控制台getEnvironment
auxiliary/scanner/sap/sap_mgmt_con_getlogfiles  SAP管理控制台获取日志文件
auxiliary/scanner/sap/sap_mgmt_con_getprocesslist  SAP管理控制台GetProcessList
auxiliary/scanner/sap/sap_mgmt_con_getprocessparameter  SAP管理控制台获取流程参数
auxiliary/scanner/sap/sap_mgmt_con_instanceproperties  SAP管理控制台实例属性
auxiliary/scanner/sap/sap_mgmt_con_listconfigfiles  SAP管理控制台列表配置文件
auxiliary/scanner/sap/sap_mgmt_con_listlogfiles SAP管理控制台列表日志文件
auxiliary/scanner/sap/sap_mgmt_con_startprofile SAP管理控制台getStartProfile
auxiliary/scanner/sap/sap_mgmt_con_version  SAP管理控制台版本检测
auxiliary/scanner/sap/sap_router_info_request  SAPRouter管理要求
auxiliary/scanner/sap/sap_router_portscanner  SAPRouter端口扫描器
auxiliary/scanner/sap/sap_service_discovery SAP服务发现
auxiliary/scanner/sap/sap_smb_relay SAP SMB继电器滥用
auxiliary/scanner/sap/sap_soap_bapi_user_create1  SAP / SAP /bc/soap/rfc soap服务BAPI_USER_CREATE1函数用户创建
auxiliary/scanner/sap/sap_soap_rfc_brute_login  SAP SOAP服务RFC_PING登录蛮力Forcer
auxiliary/scanner/sap/sap_soap_rfc_dbmcli_sxpg_call_system_command_e SAP / SAP /bc/soap/rfc soap Service SXPG_CALL_SYSTEM函数命令注入
auxiliary/scanner/sap/sap_soap_rfc_dbmcli_sxpg_command_exec SAP / SAP /bc/soap/rfc soap服务SXPG_COMMAND_EXEC函数命令注入
auxiliary/scanner/sap/sap_soap_rfc_eps_get_directory_listing  SAP SOAP RFC EPS_GET_DIRECTORY_LISTING目录信息公开
auxiliary/scanner/sap/sap_soap_rfc_pfl_check_os_file_existence  SAP SOAP RFC pfl_check_os_file_exist文件存在性检查
auxiliary/scanner/sap/sap_soap_rfc_ping SAP / SAP /bc/soap/rfc soap服务RFC_PING功能服务发现
```

```
auxiliary/scanner/sap/sap_soap_rfc_read_table   SAP / SAP /bc/soap/rfc soap服务RFC_READ_TABLE函数转储数据
auxiliary/scanner/sap/sap_soap_rfc_rzl_read_dir SAP SOAP RFC RZL_READ_DIR_LOCAL目录内容清单
auxiliary/scanner/sap/sap_soap_rfc_susr_rfc_user_interface  SAP / SAP /bc/soap/rfc soap服务SUSR_RFC_USER_INTERFACE函数用户创建
auxiliary/scanner/sap/sap_soap_rfc_sxpg_call_system_exec    SAP / SAP /bc/soap/rfc soap服务SXPG_CALL_SYSTEM函数命令执行
auxiliary/scanner/sap/sap_soap_rfc_sxpg_command_exec    SAP SOAP RFC SXPG_COMMAND_EXECUTE
auxiliary/scanner/sap/sap_soap_rfc_system_info  SAP / SAP /bc/soap/rfc soap服务RFC_SYSTEM_INFO函数敏感信息收集
auxiliary/scanner/sap/sap_soap_th_saprel_disclosure SAP / SAP /bc/soap/rfc soap服务的功能信息公开
auxiliary/scanner/sap/sap_web_gui_brute_login   SAP Web GUI登录蛮力
auxiliary/scanner/scada/digi_addp_reboot    Digi ADDP远程重启启动程序
auxiliary/scanner/scada/digi_addp_version   Digi ADDP信息发现
auxiliary/scanner/scada/digi_realport_serialport_scan   Digi RealPort串行服务器端口扫描器
auxiliary/scanner/scada/digi_realport_version   Digi RealPort串口服务器版本
auxiliary/scanner/scada/indusoft_ntwebserver_fileaccess Indusoft WebStudio NTWebServer远程文件访问
auxiliary/scanner/scada/koyo_login  Koyo DirectLogic PLC密码蛮力实用工具
auxiliary/scanner/scada/modbus_findunitid   Modbus单元ID和站点ID枚举器
auxiliary/scanner/scada/modbusclient    网络通讯协议客户端实用工具
auxiliary/scanner/scada/modbusdetect    网络通讯协议扫描版
auxiliary/scanner/scada/moxa_discover   Moxa UDP设备发现
auxiliary/scanner/scada/pcomclient  Unitronics PCOM客户
auxiliary/scanner/scada/profinet_siemens    西门子Profinet扫描仪
auxiliary/scanner/scada/sielco_winlog_fileaccess    Sielco Sistemi Winlog远程文件访问
auxiliary/scanner/sip/enumerator    SIP用户名枚举器(UDP)
auxiliary/scanner/sip/enumerator_tcp    SIP用户名枚举器(TCP)
auxiliary/scanner/sip/options   SIP端点扫描器(UDP)
auxiliary/scanner/sip/options_tcp   SIP端点扫描器(TCP)
auxiliary/scanner/sip/sipdroid_ext_enum SIPDroid扩展打捞工具
auxiliary/scanner/smb/impacket/dcomexec DCOM执行
auxiliary/scanner/smb/impacket/secretsdump  DCOM执行
auxiliary/scanner/smb/impacket/wmiexec  WMI执行
auxiliary/scanner/smb/pipe_auditor  SMB会话管道审计员
auxiliary/scanner/smb/pipe_dcerpc_auditor   SMB会话管道DCERPC审核员
auxiliary/scanner/smb/psexec_loggedin_users microsoftwindows验证登录在用户枚举中
auxiliary/scanner/smb/smb1  SMBv1协议检测
auxiliary/scanner/smb/smb2  SMB 2.0协议检测
auxiliary/scanner/smb/smb_enum_gpp  SMB组策略首选项保存的密码枚举
auxiliary/scanner/smb/smb_enumshares    SMB分享枚举
auxiliary/scanner/smb/smb_enumusers SMB用户枚举(SAM EnumUsers)
auxiliary/scanner/smb/smb_enumusers_domain  SMB域用户枚举
auxiliary/scanner/smb/smb_login SMB登录检查扫描仪
auxiliary/scanner/smb/smb_lookupsid SMB SID用户枚举(LookupSid)
auxiliary/scanner/smb/smb_ms17_010  MS17-010 SMB RCE检测
auxiliary/scanner/smb/smb_uninit_cred   Samba _netr_ServerPasswordSet未初始化的凭据状态
auxiliary/scanner/smb/smb_version   SMB版本检测
auxiliary/scanner/smtp/smtp_enum    SMTP用户枚举实用程序
auxiliary/scanner/smtp/smtp_ntlm_domain SMTP NTLM域提取
auxiliary/scanner/smtp/smtp_relay   SMTP开路继电器检测
```

```
auxiliary/scanner/smtp/smtp_version SMTP横幅打捞工具
auxiliary/scanner/snmp/aix_version  AIX SNMP扫描器辅助模块
auxiliary/scanner/snmp/arris_dg950  DG950A电缆调制解调器Wifi枚举
auxiliary/scanner/snmp/brocade_enumhash 博科密码散列枚举
auxiliary/scanner/snmp/cisco_config_tftp    Cisco IOS SNMP配置抓取器(TFTP)
auxiliary/scanner/snmp/cisco_upload_file    Cisco IOS SNMP文件上传(TFTP)
auxiliary/scanner/snmp/cnpilot_r_snmp_loot  形成层cnPilot r200/r201 SNMP枚举
auxiliary/scanner/snmp/epmp1000_snmp_loot   形成层epmp1000 SNMP枚举
auxiliary/scanner/snmp/netopia_enum Netopia 3347电缆调制解调器Wifi枚举
auxiliary/scanner/snmp/sbg6580_enum ARRIS / Motorola SBG6580电缆调制解调器
SNMP枚举模块
auxiliary/scanner/snmp/snmp_enum    SNMP枚举模块
auxiliary/scanner/snmp/snmp_enum_hp_laserjet    HP LaserJet打印机SNMP枚举
auxiliary/scanner/snmp/snmp_enumshares  SNMP Windows SMB共享枚举
auxiliary/scanner/snmp/snmp_enumusers   SNMP Windows用户名枚举
auxiliary/scanner/snmp/snmp_login   SNMP社区登录扫描器
auxiliary/scanner/snmp/snmp_set SNMP设置模块
auxiliary/scanner/snmp/ubee_ddw3611 Ubee DDW3611b电缆调制解调器Wifi枚举
auxiliary/scanner/snmp/xerox_workcentre_enumusers   施乐工作中心用户枚举(SNMP)
auxiliary/scanner/ssh/apache_karaf_command_execution    Apache Karaf默认凭
证命令执行
auxiliary/scanner/ssh/cerberus_sftp_enumusers   Cerberus FTP服务器SFTP用户名
枚举
auxiliary/scanner/ssh/detect_kippo  Kippo SSH蜜罐探测器
auxiliary/scanner/ssh/eaton_xpert_backdoor  Eaton Xpert表SSH私钥暴露扫描器
auxiliary/scanner/ssh/fortinet_backdoor Fortinet SSH后门扫描器
auxiliary/scanner/ssh/juniper_backdoor  Juniper SSH后门扫描器
auxiliary/scanner/ssh/karaf_login   Apache Karaf登录实用程序
auxiliary/scanner/ssh/libssh_auth_bypass    libssh身份验证绕过扫描器
auxiliary/scanner/ssh/ssh_enumusers SSH用户名枚举
auxiliary/scanner/ssh/ssh_identify_pubkeys  SSH公钥接受扫描程序
auxiliary/scanner/ssh/ssh_login SSH登录检查扫描器
auxiliary/scanner/ssh/ssh_login_pubkey  SSH公钥登录扫描器
auxiliary/scanner/ssh/ssh_version   SSH版本扫描仪
auxiliary/scanner/ssl/bleichenbacher_oracle 扫描器在RSA PKCS #1 v1.5的布莱肯
巴赫Oracle
auxiliary/scanner/ssl/openssl_ccs   OpenSSL服务器端ChangeCipherSpec注入扫描器
auxiliary/scanner/ssl/openssl_heartbleed    OpenSSL心跳(心脏出血)信息泄漏
auxiliary/scanner/steam/server_info 收集Steam服务器信息
auxiliary/scanner/telephony/wardial Wardialer
auxiliary/scanner/telnet/brocade_enable_login   启用登录检查扫描器
auxiliary/scanner/telnet/lantronix_telnet_password  Lantronix Telnet密码恢
复
auxiliary/scanner/telnet/lantronix_telnet_version   Lantronix Telnet服务横
幅检测
auxiliary/scanner/telnet/satel_cmd_exec Satel Iberia SenNet数据记录仪和电表指
令注入漏洞
auxiliary/scanner/telnet/telnet_encrypt_overflow    Telnet服务加密密钥ID溢出
检测
auxiliary/scanner/telnet/telnet_login   Telnet登录检查扫描器
auxiliary/scanner/telnet/telnet_ruggedcom   密码生成器
auxiliary/scanner/telnet/telnet_version Telnet服务横幅检测
auxiliary/scanner/teradata/teradata_odbc_login  Teradata ODBC登录扫描仪模块
auxiliary/scanner/tftp/ipswitch_whatsupgold_tftp    IpSwitch黄金TFTP目录遍历
auxiliary/scanner/tftp/netdecision_tftp NetDecision 4.2 TFTP目录遍历
auxiliary/scanner/tftp/tftpbrute    TFTP蛮冲头
auxiliary/scanner/ubiquiti/ubiquiti_discover    Ubiquiti发现扫描仪
auxiliary/scanner/udp/udp_amplification UDP放大扫描
```

```
auxiliary/scanner/upnp/ssdp_amp SSDP:所有M-SEARCH扩增扫描仪
auxiliary/scanner/upnp/ssdp_msearch m -搜索信息发现
auxiliary/scanner/varnish/varnish_cli_file_read 清漆缓存CLI文件读取
auxiliary/scanner/varnish/varnish_cli_login Varnish缓存CLI登录实用程序
auxiliary/scanner/vmware/esx_fingerprint    VMWare ESX/ESXi指纹扫描仪
auxiliary/scanner/vmware/vmauthd_login  VMWare身份验证守护程序登录扫描程序
auxiliary/scanner/vmware/vmauthd_version    VMWare身份验证守护程序版本扫描程序
auxiliary/scanner/vmware/vmware_enum_permissions    VMWare列举权限
auxiliary/scanner/vmware/vmware_enum_sessions   VMWare枚举活动会话
auxiliary/scanner/vmware/vmware_enum_users  VMWare枚举用户帐户
auxiliary/scanner/vmware/vmware_enum_vms    VMWare列举虚拟机
auxiliary/scanner/vmware/vmware_host_details    VMWare列举主机详细信息
auxiliary/scanner/vmware/vmware_http_login  VMWare Web登录扫描器
auxiliary/scanner/vmware/vmware_screenshot_stealer  VMWare截图偷窃者
auxiliary/scanner/vmware/vmware_server_dir_trav VMware服务器目录遍历漏洞
auxiliary/scanner/vmware/vmware_update_manager_traversal    VMWare Update
Manager 4目录遍历
auxiliary/scanner/vnc/ard_root_pw   苹果远程桌面根漏洞
auxiliary/scanner/vnc/vnc_login VNC认证扫描仪
auxiliary/scanner/vnc/vnc_none_auth VNC认证不检测
auxiliary/scanner/voice/recorder    电话线话音扫描器
auxiliary/scanner/vxworks/wdbrpc_bootline   VxWorks WDB代理启动参数扫描程序
auxiliary/scanner/vxworks/wdbrpc_version    VxWorks WDB代理版本扫描器
auxiliary/scanner/winrm/winrm_auth_methods  WinRM认证方法检测
auxiliary/scanner/winrm/winrm_cmd   WinRM命令运动员
auxiliary/scanner/winrm/winrm_login WinRM登录工具
auxiliary/scanner/winrm/winrm_wql   WinRM WQL查询运行器
auxiliary/scanner/wproxy/att_open_proxy 在AT&T路由器上打开WAN-to-LAN代理
auxiliary/scanner/wsdd/wsdd_query   WS-Discovery信息发现
auxiliary/scanner/x11/open_x11  X11 No-Auth扫描仪
```

下一课我将采用几个简单的辅助扫描模块进行说明

文章作者：陈殷

文章出处：山丘安全攻防实验室