浅谈分布式扫描器搭建

分享者

白细胞安全团队:dark3r

演讲者简介

陈香锡 & dark3r

清远职业技术学院学生

白细胞安全团队SRC小组负责人

研究方向:Web前端安全,软件开发

Weibo: @三寸笔尖

目录概要

Web扫描器类型

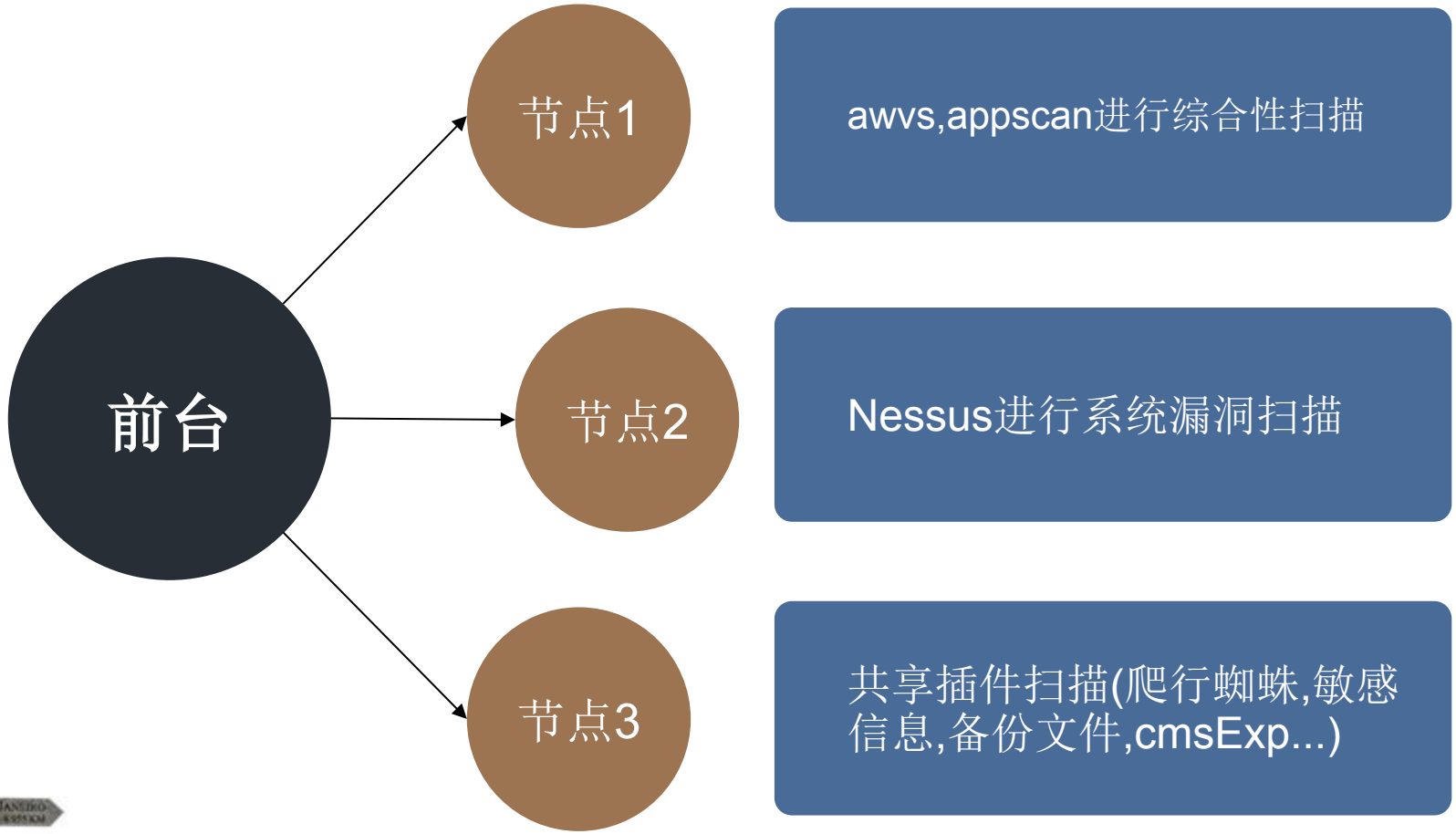
客户端模式

AWVS
Appscan
safe3
.....

云端模式

Bugscan
Nessus
绿盟极光
scanv
...

融合式分布扫描搭建


前台
节点1
节点2
节点3
awvs,appscan进行综合性扫描
Nessus进行系统漏洞扫描
共享插件扫描(爬行蜘蛛,敏感信息,备份文件,cmsExp...)

扫描框架

前台显示与发布任务

Web

与前台交互,后台执行任务

Mutual

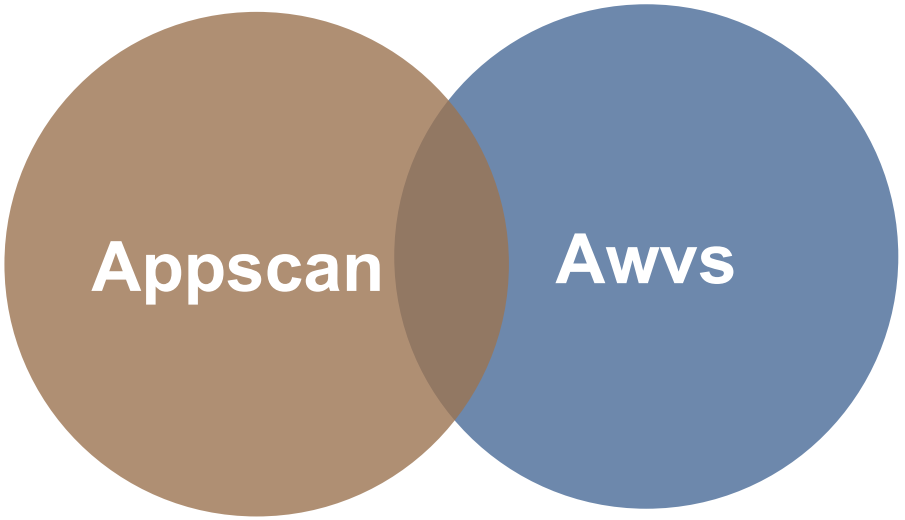
监控任务以及管理任务

Manage

Scan

扫描节点开始工作

appscan+awvs的融合



感谢明华大牛。Blog:http://0cx.cc

参考链接:
http://0cx.cc/about_wvs_console.jspx
http://0cx.cc/AppScan_Standard_CLI.jspx

```
>> USAGE: wvs_console /Scan [URL]  OR  /Crawl [URL]  OR  /ScanFromCrawl [FILE]

                OR  /ScanWSDL [WSDL URL]

>> PARAMETERS                                                    //参数
      /Scan [URL]             : Scan specified URL                    //扫描特定的URL
      /Crawl [URL]            : Crawl specified URL                   //检索指定的url
      /ScanFromCrawl [FILE]    : Scan from crawling results                //扫描检索的结果
      /ScanWSDL [WSDL URL]     : Scan web services from WSDL URL              //扫描来自wsdl的参数URL
      /Profile [PROFILE_NAME]  : Use specified scanning profile during scanning   //使用指定的扫描配置进行扫描
      /Settings [FILE]         : Use specified settings template during scanning  //使用指定的设置模板进行扫描
      /LoginSeq [FILE]          : Use specified login sequence                //使用指定的登录序列
      /Import [FILE(s)]        : Import files during crawl                //导入检索的地址进行爬行
      /Run [command line]       : Run this command during crawl                //
      /Selenium [FILE]         : Execute selenium script during crawl          //执行selenium脚本进行爬行
      /Save                   : Save scan results                       //保存结果
      /SaveFolder [DIR]        : Specify the folder were all the saved data will be stored //保存记录的目录
      /GenerateZIP             : Compress all the saved data into a zip file      //对所有的数据进行zip压缩
      /ExportXML               : Exports results as XML                  //将结果以XML方式导出
      /ExportAVDL              : Exports results as AVDL                  //将结果以AVDL方式导出
      /SavetoDatabase          : Save alerts to the database                //把警告数据保存进数据库
      /SaveLogs               : Save scan logs                         //保存扫描日志
      /SaveCrawlerData         : Save crawler data (.CWL file)               //保存检索(爬行)数据
      /GenerateReport          : Generate a report after the scan was completed   //扫描完成后生成报告
      /ReportFormat [FORMAT]    : Generated report format (REP, PDF, RTF, HTML)    //生成报告的格式
      /ReportTemplate [TEMPLATE]: Specify the report template                //特定的报告模板
      /Timestamps              : Print current timestamp with each line.         //打印每行的时间戳
      /SendEmail               : Send email notification when scan is completed, using scheduler settings. //扫描结束后发送电子邮件
      /EmailAddress [EMAIL]     : Send email notification to this email address, override scheduler settings. //邮件地址会把之前设置的给覆盖掉
      /Verbose                : Enable verbose mode                     //开启细节模式。也就是发送的具体参数
      /Password               : Application password (if required)           //如果有需要写入密码
      /?                      : Show this help screen                   //没得说，帮助
>> OPTIONS [ ? = TRUE or FALSE ]                                        //选项  =true 或者是=false
      --GetFirstOnly=?         : Get only the first URL                   //仅仅获取第一个url
      --RestrictToBaseFolder=?  : Do not fetch anything above start folder        //不扫描当前目录以上的其他目录(扫描二级目录有效)
      --FetchSubdirs=?         : Fetch files bellow base folder                //
      --ForceFetchDirindex=?    : Fetch directory indexes even if not linked       //扫描目录，即使该目录不再链接里面(就是目录匹配)
      --RobotsTxt=?            : Retrieve and process robots.txt              //从robots.txt里面获取目录进行爬行
      --CaseInsensitivePaths=?  : Use case insensitive paths                   //
      --UseWebKit=?            : Use WebKit based browser for discovery          //使用基于WebKit的浏览器
      --ScanningMode=*         : Scanning mode (* = Quick, Heuristic, Extensive)  //扫描模式(快速、启发式、广泛的)
      --ManipHTTPHeaders=?      : Manipulate HTTP headers                    //http头可以修改(个人暂时理解为可以修改http头进行提交)
      --UseAcuSensor=?         : Use AcuSensor technology                  //使用AcuSensor 技术(不明所以)
      --EnablePortScanning=?    : Enable port scanning                    //启用端口扫描
      --UseSensorDataFromCrawl=*: Use sensor data from crawl(* = Yes, No, Revalidate) //抓取fuzz提交的数据( = 是,否，重新验证)
      --HtmlAuthUser=?         : Username for HTML based authentication          //基于HTTP认证的用户名
      --HtmlAuthPass=?         : Password for HTML based authentication          //基于HTTP认证的密码
      --ToolTimeout=?          : Timeout for testing tool in seconds           //设置提交的超时时间
>> EXAMPLES

wvs_console /Scan http://testphp.vulnweb.com  /SaveFolder c:\temp\scanResults\ /Save

wvs_console /ScanWSDL http://test/WS.asmx?WSDL /Profile ws_default /Save

wvs_console /Scan http://testphp.vulnweb.com /Profile default /Save --UseWebKit=false --ScanningMode=Heuristic]]
```

表 1. Exec 命令参数

参数	说明
/starting_url	设置扫描的起始 URL。起始 URL 也可以在 /base_scan 或者 /scan_template 中指定。starting_url 参数会覆盖前两者参数中的起始 URL。
/base_scan	设置源扫描文件（必须包含完整路径），新建扫描文件将使用该源扫描文件中的扫描配置。
/dest_scan	设置新扫描文件的保存位置（必须包含完整路径）。此参数若未设置的话，AppScanCMD 会把新扫描文件保存到 Temp 文件夹，并提示新扫描文件的完整路径。
/scan_template	设置扫描模板文件，新建扫描文件将使用该模板文件中的扫描配置。
/old_host /new_host	/old_host 跟 /new_host 配合使用，新扫描文件将会用 new_host 来替换扫描中所有的 old_host 路径。这个参数非常有利于脚本重用，譬如 FVT 阶段的 AppScan 脚本即可通过这种方式重用到 UAT 环境中。
/login_file	指定新扫描文件需导入的登录序列。
/multi_step_file	指定新扫描文件需导入的多步骤文件
/manual_explore_file	指定新扫描文件需导入的手工探索文件。
/policy_file	指定新扫描文件所使用的测试策略文件。
/additional_domains	指定新扫描文件在扫描中包含的、除起始 URL 之外的域。如果有多个域，建议用分号将它们分隔。
/report_file	设定新扫描文件需生成的报告名称和路径（必须包括完整路径）。
/report_type	设定报告格式。支持 <xml|pdf|rtf|txt|html|rc_ase> 六种报告格式，缺省值为 XML。rc_ase 指的是 AppScan Enterprise 报告，使用时需保证设置好 AppScan Enterprise 的连接参数。
/min_severity	指定要在报告中包含的最低结果严重性（仅适用于非 XML 报告），支持四种严重性 <low|medium|high|informational>，缺省值为 low。
/test_type	指定要在报告中包含哪些类型的测试，支持四大类型 <All|Application|Infrastructure|ThirdParty>，缺省值为 All。
/verbose	包含此标志，则在输出中包含进度行。
/scan_log	包含此标志，则在扫描时显示扫描日志。
/explore_only	包含此标志，则仅运行"探索"阶段。
/test_only	包含此标志，则仅运行"测试"阶段。
/multi-step	包含此标志，则仅测试多步骤操作。
/continue	包含此标志，则继续扫描 base_scan 文件。

AppScan Standard CLI 命令简介

AppScan Standard 安装完成后，会在系统变量 "PATH" 中增加 AppScan Standard 的安装根目录（譬如 C:\Program Files (x86)\IBM\Rational AppScan\）。AppScan Standard CLI 命令 AppScanCMD.exe 即存在于 AppScan 的安装根目录中。因此用户打开 DOS 命令窗口，即可以执行 AppScan Standard 的 CLI 命令。

```
AppScanCMD.exe
以下参数中至少缺失一个: base_scan, starting_url, scan_template, manual_explore_file = ''
Program Usage:

AppScanCMD exec|ex|e

        Parametrs:
        [ /starting_url|/surl|/su <http://demo.testfire.net> ]
        [ /dest_scan|/dest|/d <full_path> ]
        [ /base_scan|/base|/b <full_path> ]
        [ /old_host|/ohost|/oh <http://demo.testfire.net> ]
        [ /new_host|/nhost|/nh <http://testing.testfire.net> ]
        [ /scan_template|/stemplate|/st <full_path> ]
        [ /login_file|/lfile|/lf <full_path> ]
        [ /multi_step_file|/mstepfile|/mf <full_path> ]
        [ /manual_explore_file|/mexplorefile|/mef <full_path> ]
        [ /policy_file|/pfile|/pf <full_path> ]
        [ /additional_domains|/adomains|/ad <demo.testfire.net123> ]
        [ /report_file|/rf <full_path> ]
        [ /report_type|/rt <Xml,Pdf,Rtf,Txt,Html,rc_ase> {xml} ]
        [ /min_severity|/msev <Informational,Low,Medium,High> {informational} ]
        [ /test_type|/tt <All,Application,Infrastructure,ThirdParty>]

        Flags:
        [ /verbose|/v {false} ]
        [ /scan_log|/sl {false} ]
        [ /explore_only|/eo {false} ]
        [ /test_only|/to {false} ]
        [ /multi_step|/mstep|/ms {false} ]
        [ /continue|/c {false} ]
```

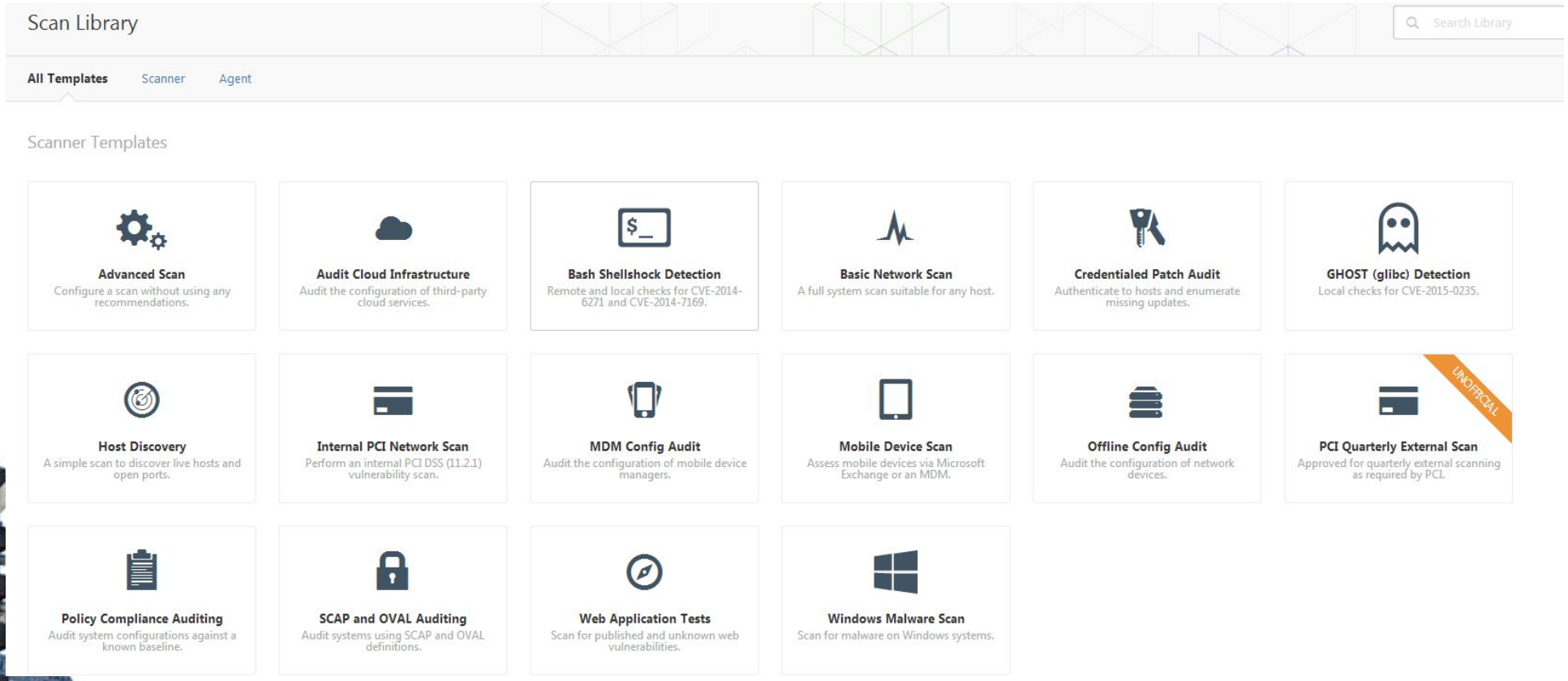
可通过 base_scan 配置、保存 dest_scan 和创建报告来创建新的扫描，如果已配置的话。

```
AppScanCMD report|rep|r

        Parametrs:
        /base_scan|/base|/b <full_path>
        /report_file|/rf <full_path>
        [ /report_type|/rt <Xml,Pdf,Rtf,Txt,Html,rc_ase> {xml} ]
        [ /min_severity|/msev <Informational,Low,Medium,High> {informational} ]
        [ /test_type|/tt <All,Application,Infrastructure,ThirdParty> ]

        Flags:
        [ /verbose|/v {false} ]
```

创建 base_scan 报告。

Nessus的调用

Nessus我采用的是提交数据包进行下发任务与接收任务
一般我扫描会采用两种扫描方式，一种是Web Application Tests,另一种是Basic
多数情况下，我都是用Basic来对服务器进行全面扫描的。
这次测试所用的是Basic方式扫描



提交任务

Remote Address: 172.16.25.205:8834
Request URL: https://172.16.25.205:8834/scans
Request Method: POST
Status Code: 200 OK

▼ **Request Headers** view source

Accept: application/json, text/javascript, */*; q=0.01
Accept-Encoding: gzip,deflate,sdch
Accept-Language: zh-CN,zh;q=0.8
Connection: keep-alive
Content-Length: 2813
Content-Type: application/json
Host: 172.16.25.205:8834
Origin: https://172.16.25.205:8834
Referer: https://172.16.25.205:8834/
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/35.0.1916.153 Safari/537.36 SE 2.X MetaSr 1.0
X-Cookie: token=53c7d0b5cfbe07d7355636fdaefb1d01bc2cb0c3517b9e9a;
X-Requested-With: XMLHttpRequest

▼ **Request Payload** view parsed

{"uuid":"731a8e52-3ea6-a291-ec0a-d2ff0619c19d7bd788d6be818b65","settings":{"name":"xx","description":"xxx","folder_id":"3","use_dashboard":true,"scanner_id":"1","text_targets":"172.16.25.250","file_targets":"","launch":"ONETIME","enabled":false,"launch_now":true,"emails":"","filter_type":"","filters":[],"acls":[{"permissions":"0","type":"default"},{"display_name":"admin","id":"2","name":"admin","owner":1,"permissions":128,"type":"user"}],"discovery_mode":"Port scan (common ports)","ping_the_remote_host":"yes","test_local_nessus_host":"yes","fast_network_discovery":"no","arp_ping":"yes","tcp_ping":"yes","tcp_ping_dest_ports":"built-in","icmp_ping":"yes","icmp_unreach_means_host_down":"no","icmp_ping_retries":"2","udp_ping":"no","scan_network_printers":"no","scan_netware_hosts":"no","wol_mac_addresses":"","wol_wait_time":"5","network_type":"Mixed (use RFC 1918)","unscanned_closed":"no","portscan_range":"default","ssh_netstat_scanner":"yes","wmi_netstat_scanner":"yes","snmp_scanner":"yes","only_portscan_if_enum_failed":"yes","verify_open_ports":"no","syn_scanner":"yes","syn_firewall_detection":"Automatic (normal)","udp_scanner":"no","svc_detection_on_all_ports":"yes","detect_ssl":"yes","ssl_prob_ports":"Known SSL ports","cert_expiry_warning_days":"60","enumerate_all_ciphers":"yes","check_crl":"no","assessment_mode":"Default","report_paranoia":"Normal","thorough_tests":"no","provided_creds_only":"yes","test_default_oracle_accounts":"no","scan_webapps":"no","request_windows_domain_info":"yes","enum_domain_users_start_uid":"1000","enum_domain_users_end_uid":"1200","enum_local_users_start_uid":"1000","enum_local_users_end_uid":"1200","report_verbosity":"Normal","report_superseded_patches":"yes","silent_dependencies":"yes","allow_post_scan_editing":"yes","reverse_lookup":"no","log_live_hosts":"no","display_unreachable_hosts":"no","advanced_mode":"Default","safe_checks":"yes","stop_scan_on_disconnect":"no","slice_network_addresses":"no","reduce_connections_on_congestion":"no","network_receive_timeout":"5","max_checks_per_host":"5","max_hosts_per_scan":"30","max_simult_tcp_sessions_per_host":"","max_simult_tcp_sessions_per_scan":"","log_whole_attack":"no","enable_plugin_debugging":"no","ssh_known_hosts":"","ssh_port":"22","ssh_client_banner":"OpenSSH_5.0","never_send_win_creds_in_the_clear":"yes","dont_use_ntlmv1":"yes","start_remote_registry":"no","enable_admin_shares":"no","http_login_method":"POST","http_reauth_delay":"0","http_login_max_redir":"0","http_login_invert_auth_regex":"no","http_login_auth_regex_on_headers":"no","http_login_auth_regex_nocase":"no","snmp_port":"161","additional_snmp_port1":"161","additional_snmp_port2":"161","additional_snmp_port3":"161","patch_audit_over_telnet":"no","patch_audit_over_rsh":"no","patch_audit_over_rexec":"no"},"credentials":{}}

Web Application Tests:c3cbcd46-329f-a9ed-1077-554f8c2af33d0d44f09d736969bf
Basic:731a8e52-3ea6-a291-ec0a-d2ff0619c19d7bd788d6be818b65

Nessus任务调用回显

停止任务:POST方式
https://a.com/scans/任务id/stop

删除任务:put方式
Https://a.com/scans/12/folder

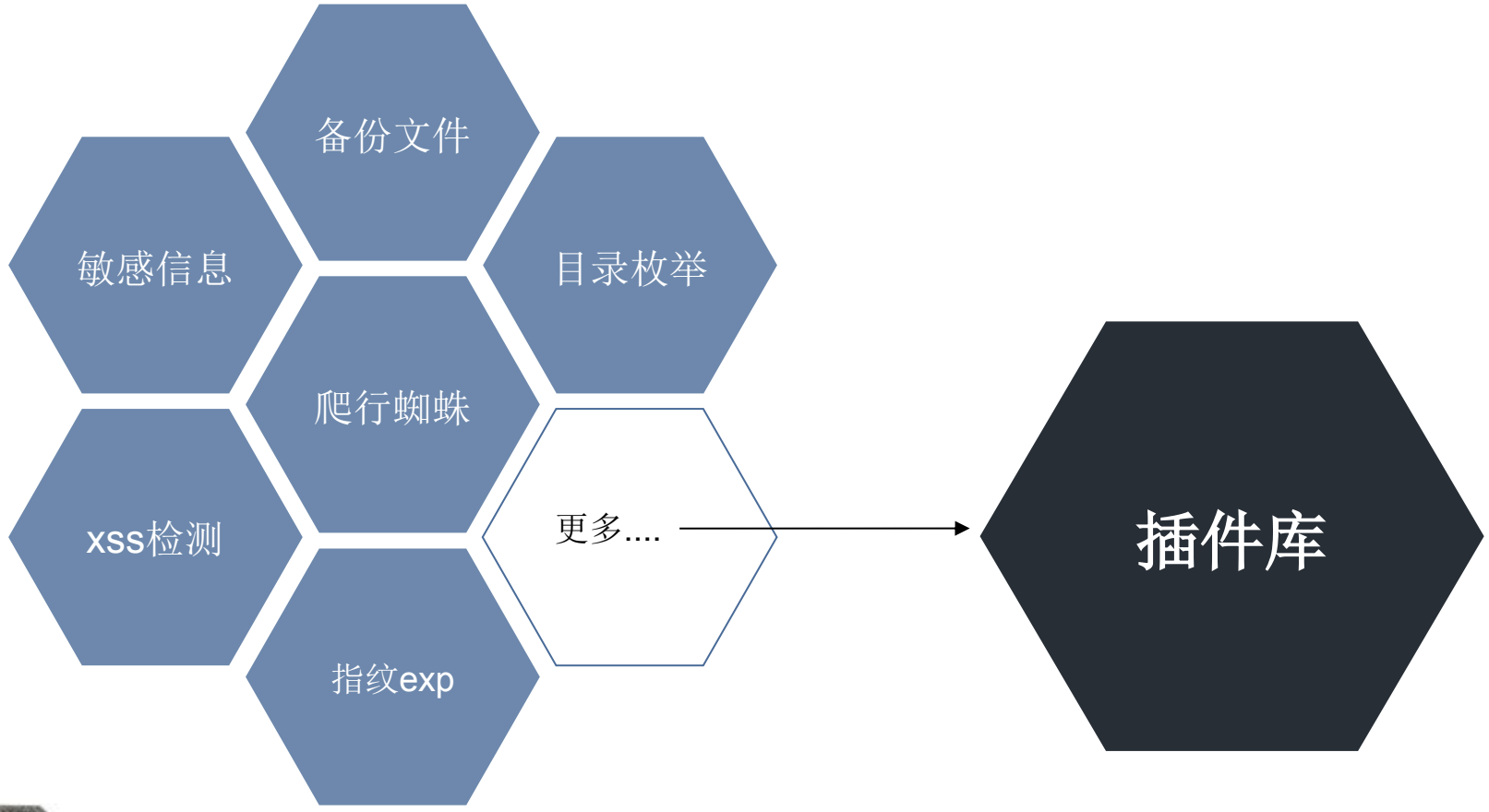
date:{"folder_id":任务id}

查看任务：get方式

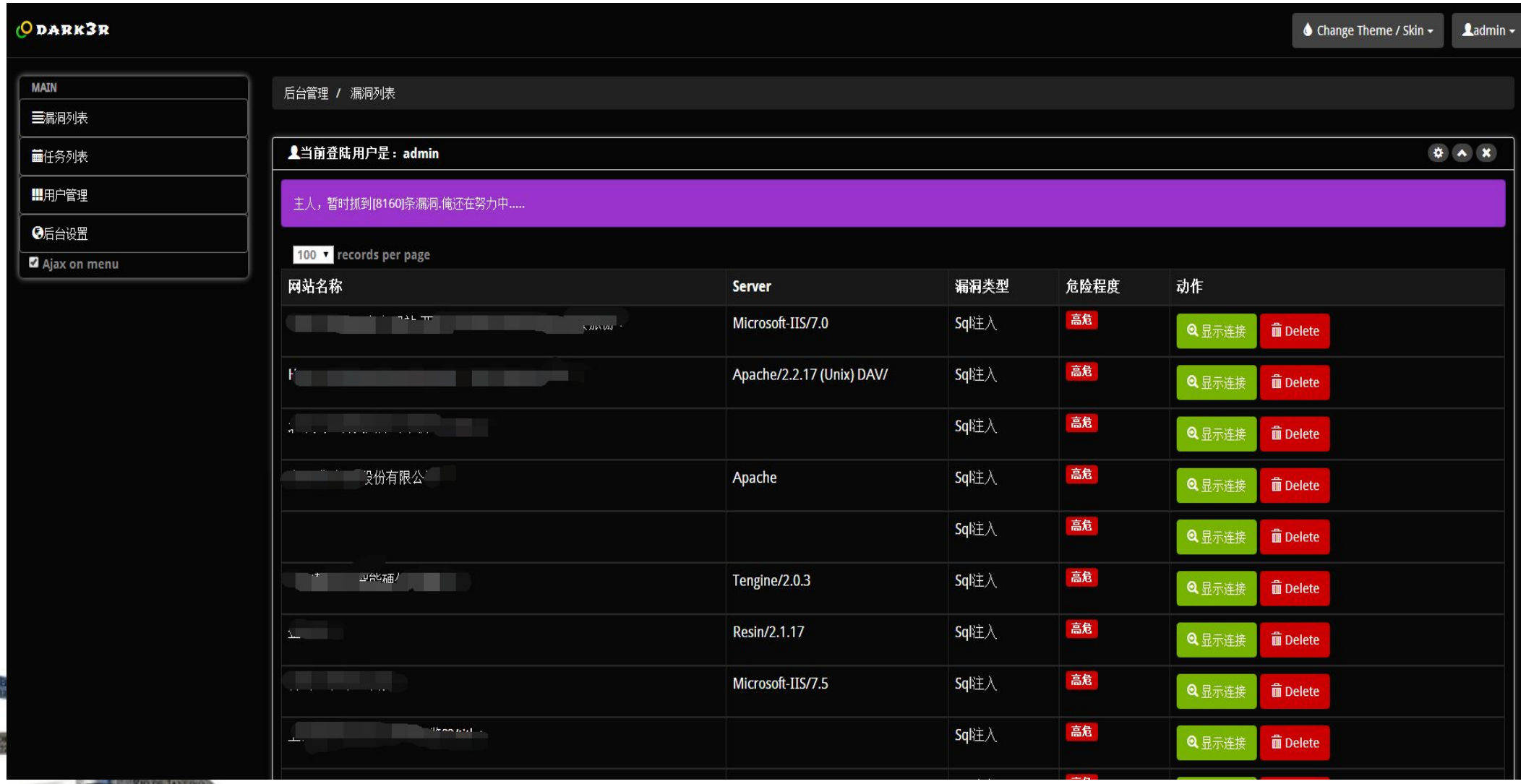
https://a.com/scans/任务id

暂停任务：POST方式
https://172.16.25.205:8834/scans/27/pause

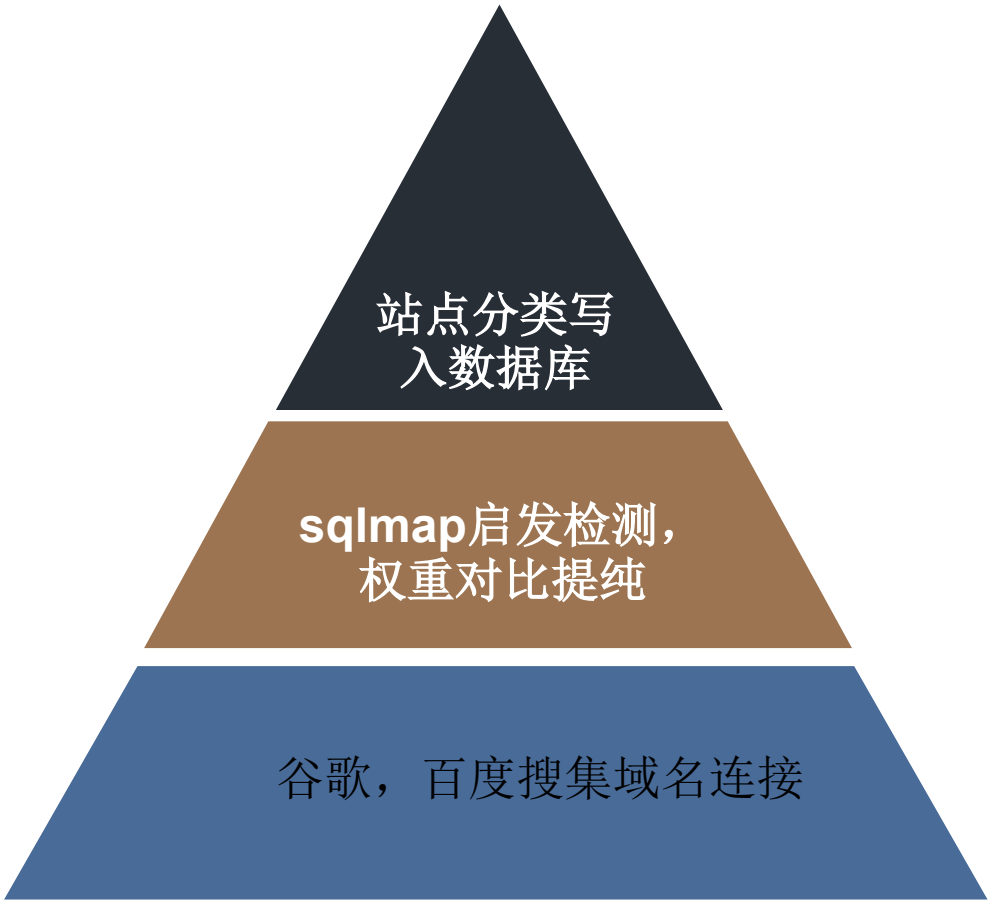
共享插件扫描



课外分享(我的漏洞挖掘机)



工作流程




BEIJING
12 933 KM
LONDON
9 123 KM
BERLIN
9 575 KM
TOKYO
4 724 KM
RIO DE JANEIRO
6 055 KM
SYDNEY
11 642 KM
JERUSALEM
7 468 KM
SOUTH POLE
6248 KM
EW DELHI
296 KM
INHALA

Thank you !