



自动化渗透测试那些事儿

杭州安恒信息技术有限公司
—安全研究院上海分院院长
—自动化渗透测试平台产品经理
阿诺(arno)



提纲

- 什么是自动化渗透测试
- 昨天的自动化渗透测试
- 今天的自动化渗透测试
- 明天的自动化渗透测试



什么是自动化渗透测试

■ 渗透测试

渗透测试(penetration test)是通过模拟恶意黑客的攻击方法，来评估计算机网络系统安全的一种评估方法。这个过程包括对系统的任何弱点、技术缺陷或漏洞的主动分析，这个分析是从一个攻击者可能存在的位置来进行的，并且从这个位置有条件主动利用安全漏洞，达到一定的控制权限。

■ 特点

- 0),信息收集
- 1),发现弱点
- 2),利用弱点
- 3),获取权限



什么是自动化渗透测试

- 按评估定
将渗透
的降低人机
确地快速执行



度
准



自动化渗透测试的意义

- 渗透测试是真实反映信息安全风险
- 渗透测试结果依赖于安全专家个人
- 渗透测试安全专家出场费用过高
- 渗透测试技术复杂，难以短期内学习掌握
- 自动化的全面的渗透测试评估方法意义重大



提纲

- 什么是自动化渗透测试
- 昨天的自动化渗透测试
- 今天的自动化渗透测试
- 明天的自动化渗透测试



昨天的渗透测试

- 几种常见的模式：
 - 1) , 弱点自动化模式
 - 2) , 阶段自动化模式
 - 3) , 渗透测试框架
 - 4) , 商业化渗透测试产品



弱点自动化模式

- 以单个弱点为基础进行自动化模式

针对渗透测试中的某一阶段的或者某一个环节中的某一个信息安全弱点进行的自动化工作，称之为弱点自动化模式。

代表：

Google hacking

Sqlmap

Pangolin

椰树

Jboss AutoPwn

Struts代码执行漏洞



弱点自动化模式

- Sqlmap
- <http://sqlmap.org/>

```
(master) bernardo@ubuntu:~/sqlmap$ python sqlmap.py -u http://debian32/sqlmap/mysql/get_int.php?id=1 --tamper between,randomcase,space2comment -v 3
```

```
sqlmap/1.0-dev-c9bbd14 - automatic SQL injection and database takeover tool  
http://sqlmap.org
```

```
[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program
```

```
[*] starting at 23:47:32
```

```
[23:47:32] [DEBUG] cleaning up configuration parameters  
[23:47:32] [INFO] loading tamper script 'between'  
[23:47:32] [INFO] loading tamper script 'randomcase'  
[23:47:32] [INFO] loading tamper script 'space2comment'  
[23:47:32] [DEBUG] setting the HTTP timeout  
[23:47:32] [DEBUG] setting the HTTP method to GET  
[23:47:32] [DEBUG] creating HTTP requests opener object  
[23:47:32] [INFO] testing connection to the target url  
[23:47:32] [INFO] heuristics detected web page charset 'ascii'  
[23:47:32] [INFO] testing if the url is stable, wait a few seconds  
[23:47:33] [INFO] url is stable  
[23:47:33] [INFO] testing if GET parameter 'id' is dynamic  
[23:47:33] [PAYLOAD] 6001  
[23:47:33] [DEBUG] setting match ratio for current parameter to 0.711  
[23:47:33] [INFO] confirming that GET parameter 'id' is dynamic  
[23:47:33] [PAYLOAD] 8127  
[23:47:33] [INFO] GET parameter 'id' is dynamic  
[23:47:33] [PAYLOAD] 1'"((()))'()''  
[23:47:33] [WARNING] reflective value(s) found and filtering out  
[23:47:33] [INFO] heuristic test shows that GET parameter 'id' might be injectable (possible DBMS: MySQL)
```



弱点自动化模式

- 椰树1.7.0
- Web漏洞自动化渗透工具





弱点自动化模式

- Struts代码执行漏洞

Struts2终极漏洞利用工具 Powered By 独孤城 9904211/4 Thanks to 峙眼君edwardz

目标地址:

字符集: 提交方式: 空格编码



弱点自动化模式

■ 优点:

1) , 针对某一个(类型)漏洞能够快速进行渗透测试

■ 缺点

1) , 五花八门的利用工具(各种修改版)

2) , 时效性不高

3) , 通用性不强

4) , 开发成本高



阶段自动化

- 渗透测试中某一个环节的自动化

渗透测试过程中，以某一个阶段工作进行自动化的模式。

代表：

Nmap 网络层扫描自动化

WebScan web扫描自动化

Nessus 主机扫描自动化

Metasploit 漏洞利用自动化



阶段自动化

- Nmap
- <http://nmap.org/>

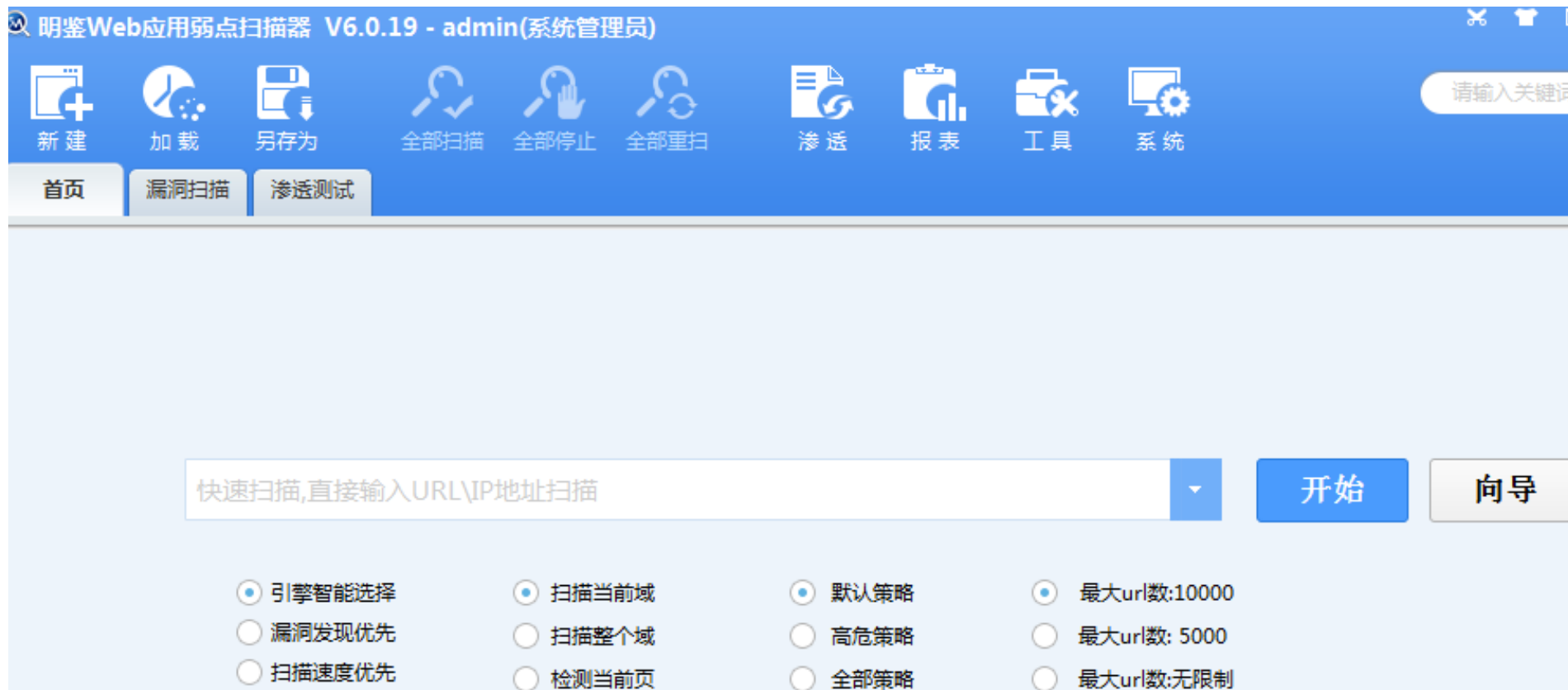
```
arno — bash — 85x27
arnotekiMacBook-Pro:~ arno$ nmap -v -A 127.0.0.1

Starting Nmap 6.40-2 ( http://nmap.org ) at 2013-12-27 17:14 CST
NSE: Loaded 110 scripts for scanning.
NSE: Script Pre-scanning.
Initiating Ping Scan at 17:14
Scanning 127.0.0.1 [2 ports]
Completed Ping Scan at 17:14, 0.00s elapsed (1 total hosts)
Initiating Connect Scan at 17:14
Scanning localhost (127.0.0.1) [1000 ports]
Discovered open port 631/tcp on 127.0.0.1
Increasing send delay for 127.0.0.1 from 0 to 5 due to max_successful_ryno increase to 4
Completed Connect Scan at 17:14, 7.22s elapsed (1000 total ports)
Initiating Service scan at 17:14
Scanning 1 service on localhost (127.0.0.1)
Completed Service scan at 17:14, 6.00s elapsed (1 service on 1 host)
NSE: Script scanning 127.0.0.1.
Initiating NSE at 17:14
Completed NSE at 17:14, 0.01s elapsed
Nmap scan report for localhost (127.0.0.1)
Host is up (0.00025s latency).
Not shown: 999 closed ports
PORT      STATE SERVICE VERSION
```



阶段自动化

- webscan
- <http://www.dbappsecurity.com.cn/>





阶段自动化

- Metasploit
- <http://www.metasploit.com/>

```
msf > _  
      =[ metasploit v4.9.0-dev [core:4.9 api:1.0]  
+ -- --=[ 1231 exploits - 672 auxiliary - 193 post  
+ -- --=[ 324 payloads - 31 encoders - 8 nops
```




阶段自动化模式

■ 优点:

1) , 阶段化渗透测试易于快速开始完成

■ 缺点:

1) , 基本上不存在与其他环节调用的接口

2) , 各自独大, 没有相同的安全标准

3) , 非商业化产品使用复杂, 文档稀缺

4) , 缺少统一的payload



渗透测试框架

- 渗透测试框架：

重新定义信息安全问题，在此基础上以自己的模型和标准建立起来的漏洞检测、利用框架，称之为渗透测试框架。

代表作：

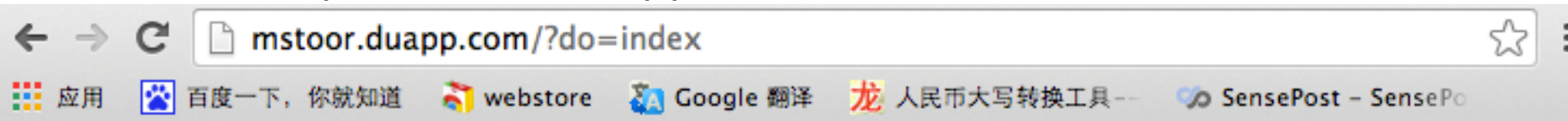
Metasploit Framework

MST[<http://mstoor.duapp.com/>]



渗透测试框架

- MST [<http://mstoor.duapp.com/>]



[首页](#) [下载](#) [文档](#) [关于](#) [反馈](#)

最新插件 [我要提交]

时间	作者	插件	类型
2013-12-25 14:57:26	Mr.x	xiaomayi_SQLInject	exploit
2013-12-04 20:38:12	Mr.Half	Struts2_S2-016_Getshell.py	exploit
2013-11-26 14:33:11	Mr.x	WordPress_Password_Fazz	exploit
2013-11-22 19:43:46	Mr.x	metinfo_lfi_xss_VULNERABLE	exploit
2013-11-22 14:59:20	Mr.x	Struts2_S2-016_CommandExec	exploit
2013-11-14 20:07:28	Mr.x	phpweb_news_SQLInject	exploit
2013-11-14 20:06:21	Mr.x	Qibocms_s_rcp_sqlinject	exploit
2013-11-14 09:46:30	Mr.x	ecshop_2.7_user.php_SQLInject	exploit
2013-11-14 09:45:39	Mr.x	08cms_pays.php_SQLInject	exploit
2013-11-09 12:51:07	mst	sameIP_web[chinaz]	multi
2013-11-04 11:14:18	L34Rn	what_cms.py	multi
2013-11-03 23:51:52	teamtopkarl	Zuitu_Call.php_SQLInject	exploit



渗透测试框架

■ 优点:

- 1) , 定义了对内对外调用接口
- 2) , 实现了通用的payload
- 3) , 扩展性增强, 可自定义脚本
- 4) , 功能强大

■ 缺点:

- 1) , 使用复杂, 要求使用人员业务素质较高
- 2) , 图形化、智能化欠缺



成熟的商业化产品

- Canvas
- Core impact
- Metasploit pro



提纲

- 什么是自动化渗透测试
- 昨天的自动化渗透测试
- 今天的自动化渗透测试
- 明天的自动化渗透测试



今天的自动化渗透测试

- 全新的定义：

自动化渗透测试，应该是将任何渗透测试过程中用到的技术手段，包括信息收集，漏洞扫描，漏洞利用，包括漏洞利用之后的权限控制手段全部自动化的一种更高效、准备的评估方法。

简而言之：

给你一个目标，点击“开始”，就有shell了。思密达 :)：)



一个简单的实现demo

■ <https://github.com/jcran/pentest-console>

GitHub, Inc. [US] <https://github.com/jcran/pentest-console/blob/master/automationPlatform/jcran-autoAttack/auto-pentest.sh>

百度一下，你就知道 webstore Google 翻译 人民币大写转换工具 SensePost - SensePo Black Hat ® Technic 外国佬blog 镇中像

英文 网页，是否需要翻译？ 否 翻译

branch: master **pentest-console / automationPlatform / jcran-autoAttack / auto-pentest.sh**



jcran 2 years ago initial commit

1 contributor



executable file | 93 lines (80 sloc) | 2.404 kb



Open



Edit



Raw



Blame



History

```
1  #!/bin/bash
2  ## Owner: jcran
3  ## Purpose: Automate a pentest's initial work
4  ## Description:
5  ##      1) Gather user input
6  ##      2) Set up environment for automatic pentest
7  ##      3) Kick off auto pentest
8  ##
9  ## Notes: Script should be run from consulting.rapid7.com
10 ##
11
12 ## Set up Initial Environment
13 ## -----
14 export AP="1"
```




一个简单的实现demo










- <https://github.com/jcran/pentest-console>

- 实现思路:

- 1) , nmap识别端口服务

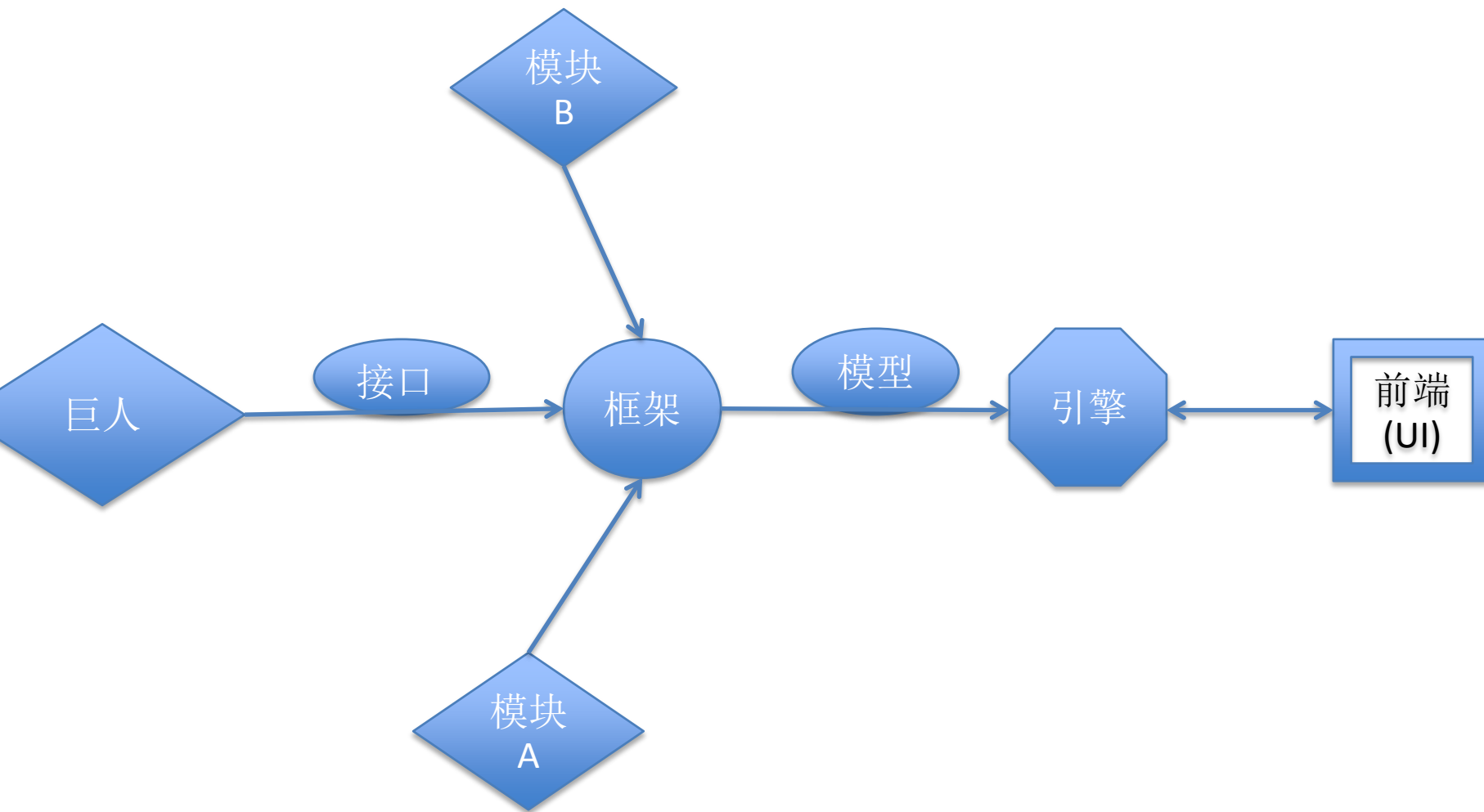
- 2) , 针对识别到的端口服务, 加载特定的扫描或者攻击脚本

- 3) , 通过console或者log查看结果

 ss-auto-	initial commit	2 years ago
 ss-auto-cifs.sh	initial commit	2 years ago
 ss-auto-dns.sh	initial commit	2 years ago
 ss-auto-ftp.sh	initial commit	2 years ago
 ss-auto-http.sh	initial commit	2 years ago
 ss-auto-https.sh	initial commit	2 years ago
 ss-auto-ipsec.sh	initial commit	2 years ago
 ss-auto-pentest.sh	initial commit	2 years ago
 ss-maintenance.sh	initial commit	2 years ago



我的实现





模型:

■ 一切安全问题都是权限问题

层级	模块	权限	说明	表示符号
OS	文件(FILE)	IRAWMD	路径信息、读取、新建、修改内容、重命名、删除、执行	<u>OS.File.IRAWMD</u>
	文件夹(DIR)	ILAMD	路径信息、列目录、新建目录、重命名目录、删除目录	OS.DIR.ILAMD
	进程(PRO)	E	启动新进程, 执行任意命令 E、启动单一命令 S、结束单一进程命令 P	OS.PRO.ESP
	网络(NET)	C	连接指定的目标	OS.NET.C
	注册表(REG)	RW	读写权限	OS.REG.RW
	权限认证接口 (LOGIN)	K	权限接口认证方式多表示用户名和密码	OS.LOGIN.K
WEB	文件(FILE)	IRAWMDX		WEB.FILE.IRAWMDX
	文件夹(DIR)	ILAMD		WEB.DIR.IRAWMDX
	权限认证接口 (LOGIN)	I	后台管理地址 URL	WEB.LOGIN.I
2	权限认证接口 (LOGIN)	K	权限接口认证方式多表示用户名	<u>WEB.LOGIN.U_user</u> WEB.LOGIN.P 密码



payload

- Meterpreter
- WebShell

```
root: sh
File Edit View Bookmarks Settings Help

Command      Description
-----
getsystem     Attempt to elevate your privilege to that of local system.

Priv: Password database Commands
=====
Command      Description
-----
hashdump     Dumps the contents of the SAM database
EGIT

Priv: Timestamp Commands
=====
Command      Description
-----
timestamp    Manipulate file MACE attributes
EGIT

meterpreter > hashdump
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
HelpAssistant:1000:89b7fa5f3c1890122e2e98275aaba976:aee870209fa62ab2d9338939de01e4e3:::
SUPPORT_388945a0:1002:aad3b435b51404eeaad3b435b51404ee:8e26d2c6ee826423781d3e47a7b8f9f8:::
meterpreter >
```



- Metasploit(MSF)
- Nmap
- Hydra
- Sqlmap
- Nessus....



接口

- webservice
- Socket
- 命令行
- 文件交换



其实你可以更牛逼

- 1、弱点、漏洞信息关联分析

Mysql注入点 + 和phpinfo →getShell

- 2、智能识别目标：

Windows目标，仅加载linux策略

- 3、社会工程

将扫描到的电话号码、邮件等，加入到弱口令扫描字典中

- 构建自己的框架

你的api，你的接口，你的payload



No pic you say a gb

工程名称: *

工程描述:

扫描地址:

www.example.com

- ☐ 是否进行ip反查
- ☐ 是否进行C段网络渗透
- ☐ 获取权限之后是否即退出

扫描方式:

全自动渗透

策略(选择):

☐ 自定义策略 ☒ 自动识别策略

更多: [高级选项](#)



渗透日志

```
[2013-12-03 04:00:11]Found New Issue:phone_no:http://192.168.28.102:8080/system/174.htm::0791-6538070 13576281815
[2013-12-03 04:01:31]Found New Issue:directory_listing:http://192.168.28.102/xampp/lang/:http://192.168.28.102/xampp/lang/
[2013-12-03 04:03:35]Found New Issue:internal_ip:http://192.168.28.102/xampp/phpinfo.php::192.168.28.99
[2013-12-03 04:03:35]Found New Issue:phpinfo:http://192.168.28.102/xampp/phpinfo.php::http://192.168.28.102/xampp/phpinfo.php
[2013-12-03 04:03:40]Found New Issue:mhtml_xss:http://192.168.28.102/phpmyadmin/index.php?lang=zh_CN%26collation_connection=utf8_general_ci%26token=e226ab5e55e0d6bdf333d0eedfa77d71:lang=zh_CN;parameter:
lang=zh_CN, xss: Content-Type%253Amultipart%252frelated%253Bboundary%253Dx%250AContent-Location%253Ax%250AContent-Transfer-
Encoding%253Abase64%250A%250APHNjcmlwdD5hbGVydCgKTS8L3NjcmlwdD4%253D-%250A%250A
[2013-12-03 04:03:41]Found New Issue:email_address:http://192.168.28.102:8080/jeeadmin/:jeeecms@163.com
[2013-12-03 04:03:46]Found New Issue:phone_no:http://192.168.28.102:8080/cjbd/411.htm::0791-6538070 13576281815
[2013-12-03 04:03:46]Found New Issue:phone_no:http://192.168.28.102:8080/cjbd/412.htm::0791-6538070 13576281815
[2013-12-03 04:03:46]Found New Issue:phone_no:http://192.168.28.102:8080/cjbd/:0791-6538070 13576281815
[2013-12-03 04:03:46]Found New Issue:phone_no:http://192.168.28.102:8080/cjbd/413.htm::0791-6538070 13576281815
[2013-12-03 04:03:47]Found New Issue:phone_no:http://192.168.28.102:8080/jjsd/405.htm::0791-6538070 13576281815
[2013-12-03 04:04:48]Found New Issue:Local_File_Inclusion:http://192.168.28.102/xampp/lang.php?es:({ID_INJECTION_SUSPECTED}}, http://192.168.28.102/xampp/lang.php?es
[2013-12-03 04:04:48]Found New Issue:Local_File_Inclusion:http://192.168.28.102/xampp/lang.php?pl:({ID_INJECTION_SUSPECTED}}, http://192.168.28.102/xampp/lang.php?pl
[2013-12-03 04:05:17]Found New Issue:robots_info:http://192.168.28.102/phpmyadmin/:http://192.168.28.102/phpmyadmin/robots.txt
[2013-12-03 04:05:17]Found New Issue:email_address:http://192.168.28.102:8080/r/cms/www/red/img/download/:jeeecms@163.com
[2013-12-03 04:05:53]Found New Issue:phone_no:http://192.168.28.102:8080/syys/index.htm::0791-6538070 13576281815
[2013-12-03 04:06:37]Found New Issue:Local_File_Inclusion:http://192.168.28.102/security/lang.php?jp_br:http://192.168.28.102/security/lang.php?jp_br
[2013-12-03 04:06:41]Found New Issue:mhtml_xss:http://192.168.28.102/examples/servlets/servlet/SessionExample?dataname=foo%26datavalue=bar.datavalue=bar;parameter.datavalue=bar, xss: Content-
Type%253Amultipart%252frelated%253Bboundary%253Dx%250AContent-Location%253Ax%250AContent-Transfer-
```



所有工程 > 工程概览-nike > 会话

Sessions

<input type="checkbox"/>	使用模块	类型	tunnel_peer	via_exploit	via_payload	desc	ip	状态	操作	选项
										首页 上一页 下一页 尾页

WebShell

<input type="checkbox"/>	域名	webshell地址	webshell密码	选项
<input type="checkbox"/>	172.16.80.151	http://172.16.80.151:88/1379790247705.asp	90247705_4997	删除
<input type="checkbox"/>	172.16.80.151	http://172.16.80.151:88/1379790244829.asp	90244829_4997	删除
<input type="checkbox"/>	172.16.80.151	http://172.16.80.151:88/1379790241152.asp	90241152_4997	删除
<input type="checkbox"/>	172.16.80.151	http://172.16.80.151:88/demoinfol/1379790172128.asp	90172128_4997	删除
<input type="checkbox"/>	172.16.80.151	http://172.16.80.151:88/demoinfol/1379790166323.asp	90166323_4997	删除
<input type="checkbox"/>	172.16.80.151	http://172.16.80.151:88/demoinfol/1379790163462.asp	90163462_4997	删除
<input type="checkbox"/>	172.16.80.151	http://172.16.80.151:88/demoinfol/1379790160046.asp	90160046_4997	删除
<input type="checkbox"/>	172.16.80.151	http://172.16.80.151:88/demoinfol/1379790089781.asp	90089781_4997	删除
<input type="checkbox"/>	172.16.80.151	http://172.16.80.151:88/demoinfol/1379789994925.asp	89994925_4997	删除
<input type="checkbox"/>	172.16.80.151	http://172.16.80.151:88/demoinfol/1379789992107.asp	89992107_4997	删除
<input type="checkbox"/>	172.16.80.151	http://172.16.80.151:88/demoinfol/1379789989122.asp	89989122_4997	删除
<input type="checkbox"/>	172.16.80.151	http://172.16.80.151:88/demoinfol/1379789985444.asp	89985444_4997	删除
<input type="checkbox"/>	172.16.80.151	http://172.16.80.151:99/1379789922694.asp	89922694_4997	删除
<input type="checkbox"/>	172.16.80.151	http://172.16.80.151:99/1379789916778.asp	89916778_4997	删除



Overview | Objects | Sessions | Social Engineering | Web Applications | Reports | Tasks | Abuse | **Webshell Tools**

All Projects | Project Overview-192.168.29.23 | **Webshell Management Tools**

Webshell Management | File Management | Virtual Terminal

One-line code location:

File Name	Time	Size	Attributes
			



工程概览-10.211.55.9 会话

主机ip	溢出模块名称	type	tunnel_peer	via_exploit	via_payload	desc	会话状态
undefined	exploit/windows/smb/ms08_067_netapi	meterpreter	10.211.55.9:1044	exploit/windows/smb/ms08_067_netapi		Meterpreter	活动会话

需要执行的命令

操作系统:

Computer : ARNO8AD2 OS : Windows .NET Server (Build 3790). Architecture : x86 System Language

Meterpreter : x86/win32

网络信息:

Interface 1 ===== Name : MS TCP Loopback interface Hardware MAC : 00:00:00:00:00:00 MTU : 65535
IPv4 Address : 127.0.0.1 Interface 65539 ===== Name : Parallels Ethernet Adapter Hardware
MAC : 00:1c:42:0a:f4:3f MTU : 1500 IPv4 Address : 10.211.55.9 IPv4 Netmask : 255.255.255.0

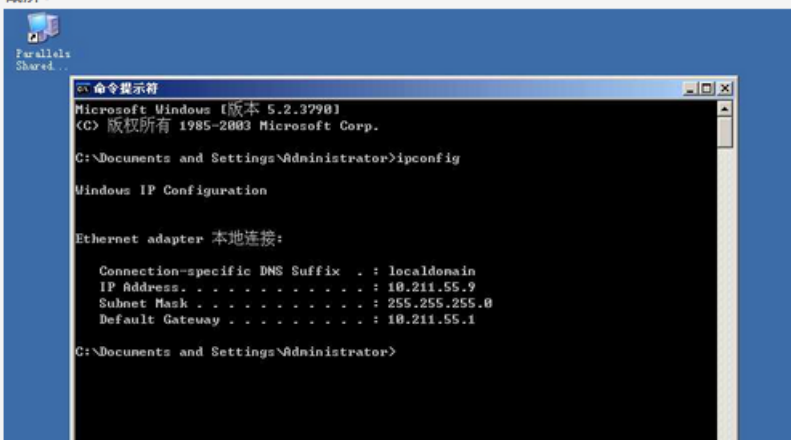
当前用户名:

Server username: NT AUTHORITY\SYSTEM

截屏:

msf命令 获取系统信息

```
list
=====
Process List
-----
Name Arch Session User Path
-----
System Process] 4294967295
system x86 0 NT AUTHORITY\SYSTEM
dfssvc.exe x86 0 NT AUTHORITY\SYSTEM
C:\Windows\system32\dfssvc.exe
smss.exe x86 0 NT AUTHORITY\SYSTEM
C:\Windows\system32\smss.exe
csrss.exe x86 0 NT AUTHORITY\SYSTEM \??
C:\Windows\system32\csrss.exe
winlogon.exe x86 0 NT AUTHORITY\SYSTEM \??
C:\Windows\system32\winlogon.exe
```





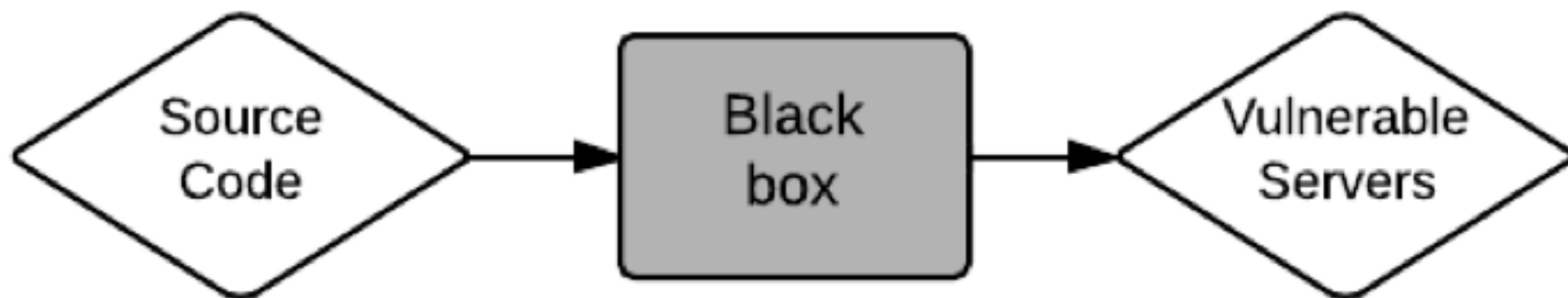
一个有趣的ideal

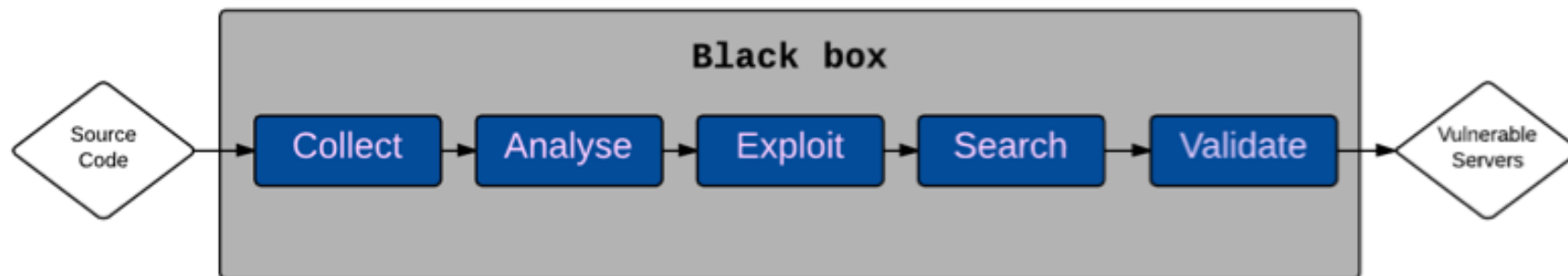
- Open Source scripts
- Shared on the internet, can be used by anyone
- Lots of attention for large projects (Wordpress, Joomla, etc)
- What about the rest?

Dennis Pellikaan; Thijs Houtenbos



一个有趣的ideal

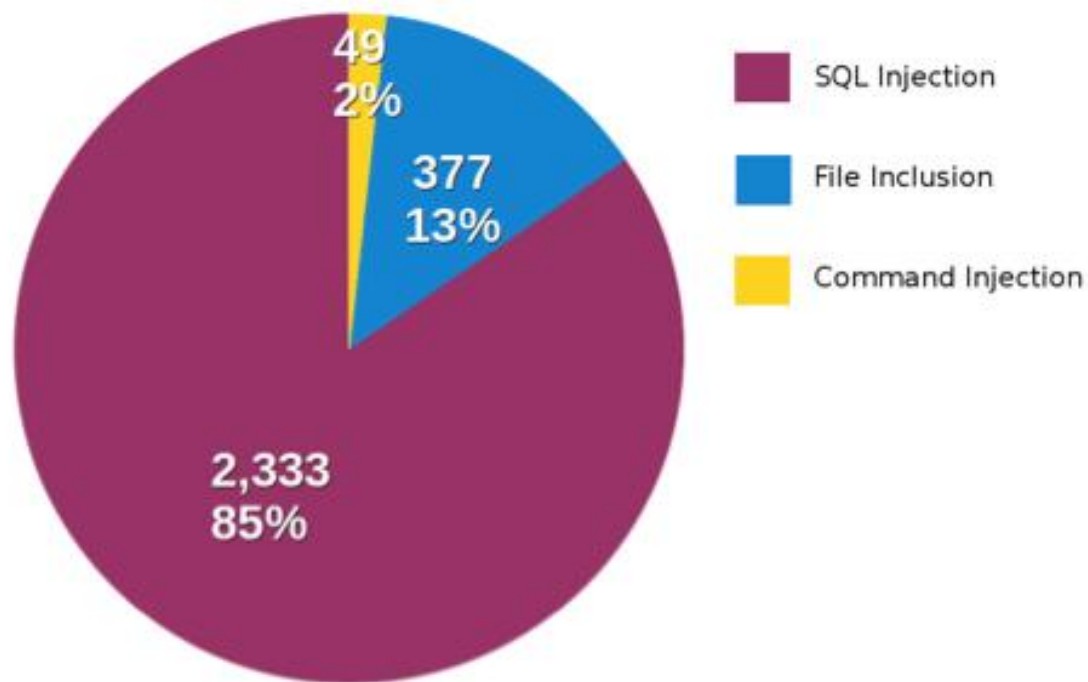


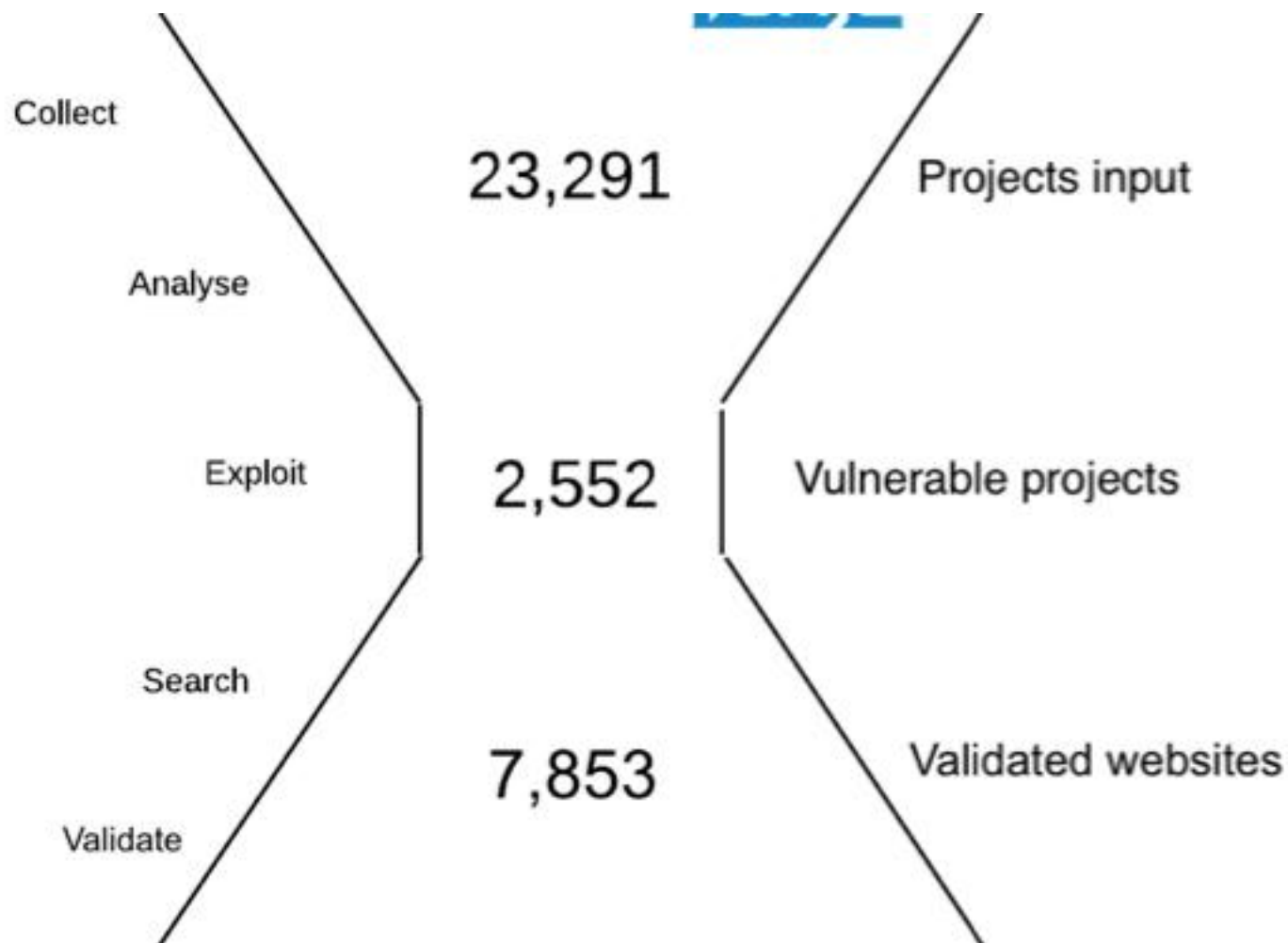


- Collect a large number of projects
- Analyse code for possible vulnerabilities
- Exploit the findings in a local environment to confirm
- Search installations of the project online
- Validate the found installation matches the project



Vulnerability categories







自动化渗透测试的明天

- 开源工程
- 商业项目
- 智能化
- 分布式



- 欢迎交流:
- qq:1626108193
- 打个广告

