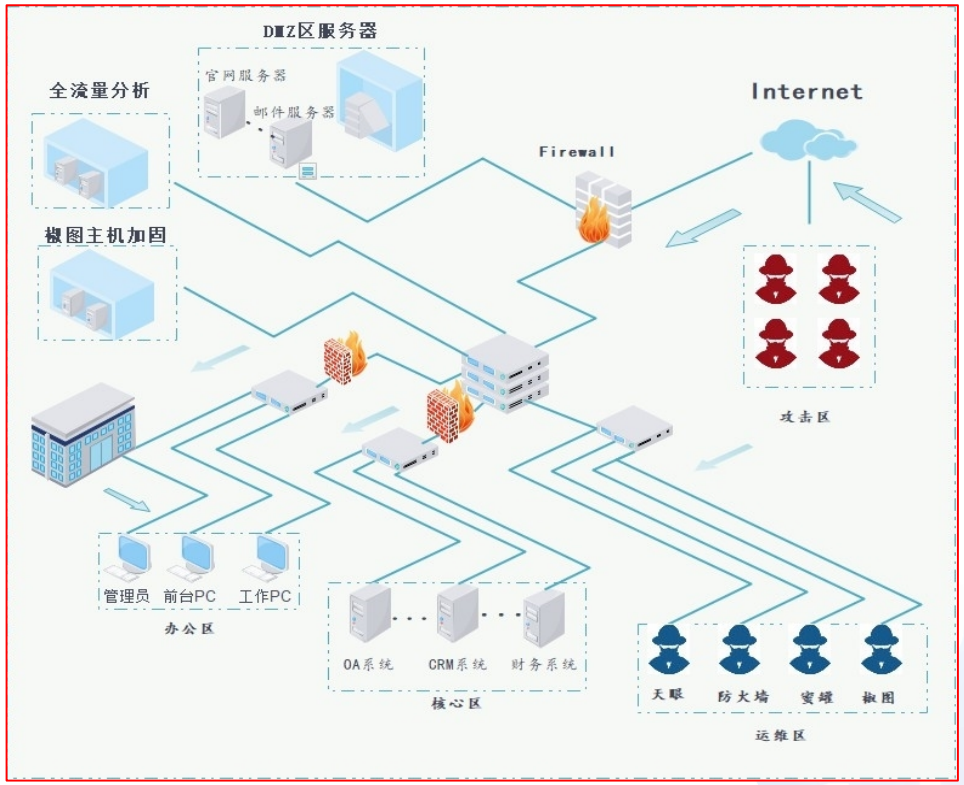
天眼平台场景二

2021-04-11

目录

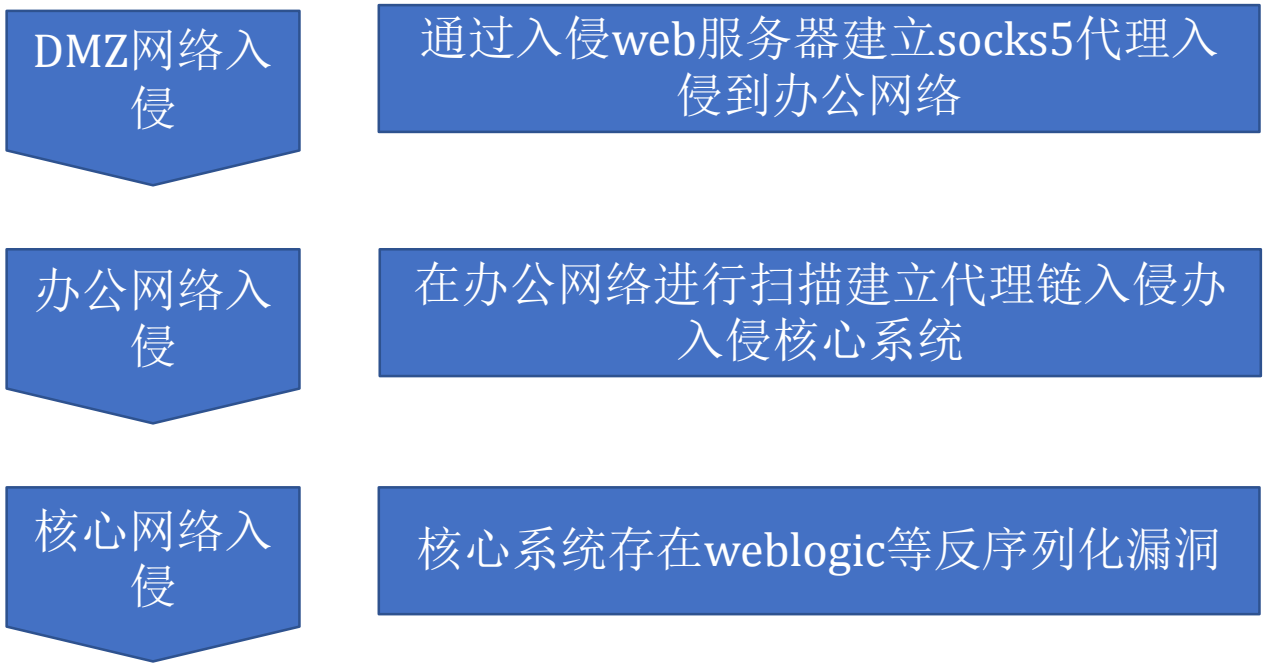
场景介绍

现有某公司的web服务器对外开放，攻击者通过入侵web服务器建立socks5代理入侵到办公区的网络，通过办公区继续建立代理构建代理连从而入侵到核心系统



场景介绍

攻击流程图


DMZ网络入侵
通过入侵web服务器建立socks5代理入侵到办公网络
办公网络入侵
在办公网络进行扫描建立代理链入侵办入侵核心系统
核心网络入侵
核心系统存在weblogic等反序列化漏洞

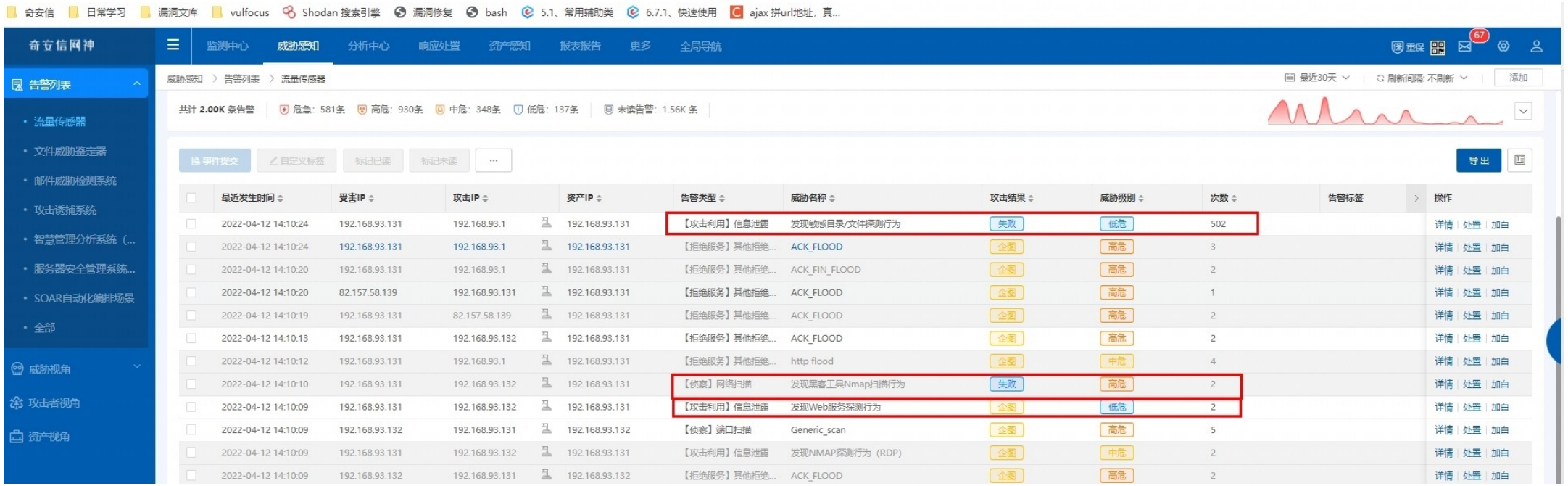
DMZ区域入侵

攻击-使用御剑进行目录扫描、nmap进行端口扫描


```
root@kali:~# nmap -sS -P0 -sV -O 192.168.93.131
Starting Nmap 7.80 ( https://nmap.org ) at 2022-04-12 02:07 EDT
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled.
Nmap scan report for 192.168.93.131
Host is up (0.0013s latency).
Not shown: 989 closed ports
PORT      STATE SERVICE            VERSION
80/tcp    open  http               Apache httpd 2.4.23 ((Win32) OpenSSL/1.0.2j PH
135/tcp   open  msrpc              Microsoft Windows RPC
139/tcp   open  netbios-ssn        Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds       Microsoft Windows Server 2008 R2 - 2012 micros
3306/tcp  open  mysql              MySQL (unauthorized)
3389/tcp  open  ssl/ms-wbt-server?
49152/tcp open  msrpc              Microsoft Windows RPC
49153/tcp open  msrpc              Microsoft Windows RPC
49154/tcp open  msrpc              Microsoft Windows RPC
49160/tcp open  msrpc              Microsoft Windows RPC
49163/tcp open  msrpc              Microsoft Windows RPC
MAC Address: 00:0C:29:40:9C:0E (VMware)
Device type: general purpose|media device
Running: Microsoft Windows 2008|10|7|8.1, Microsoft embedded
OS CPE: cpe:/o:microsoft:windows_server_2008::sp2 cpe:/o:microsoft:windows_10 cpe
:/o:microsoft:windows_8.1
OS details: Microsoft Windows Server 2008 SP2, Microsoft Windows Server 2008 SP2
8, or Windows 8.1 Update 1
Network Distance: 1 hop
Service Info: OSs: Windows, Windows Server 2008 R2 - 2012; CPE: cpe:/o:microsoft:
```

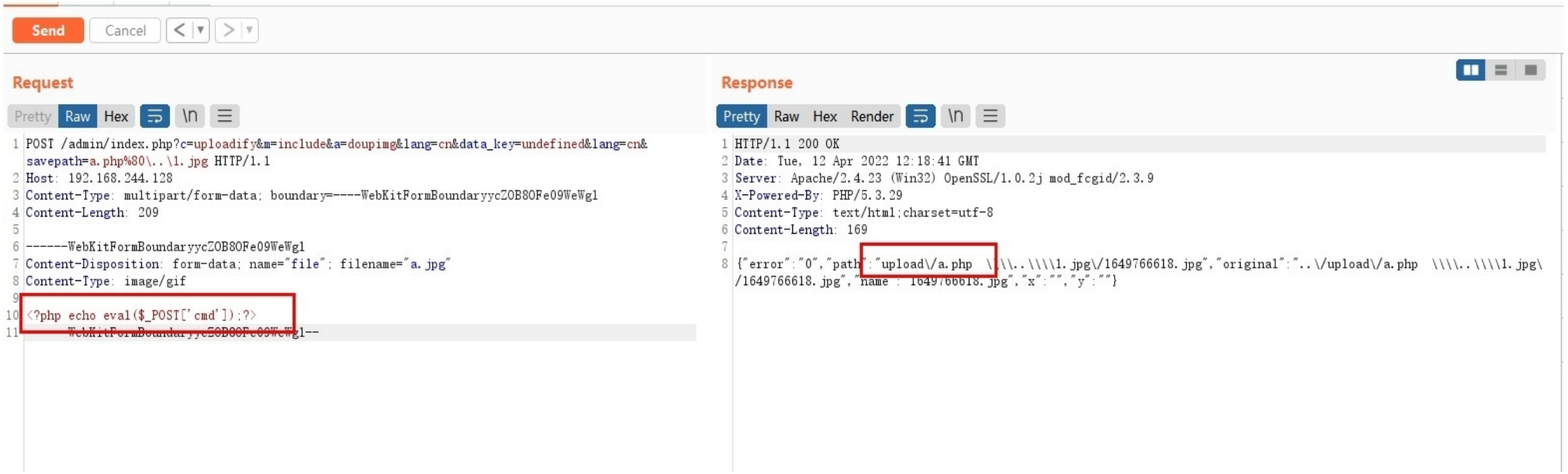
DMZ区域入侵

防守-查看分析平台有目录探测和NMAP扫描行为



DMZ区域入侵

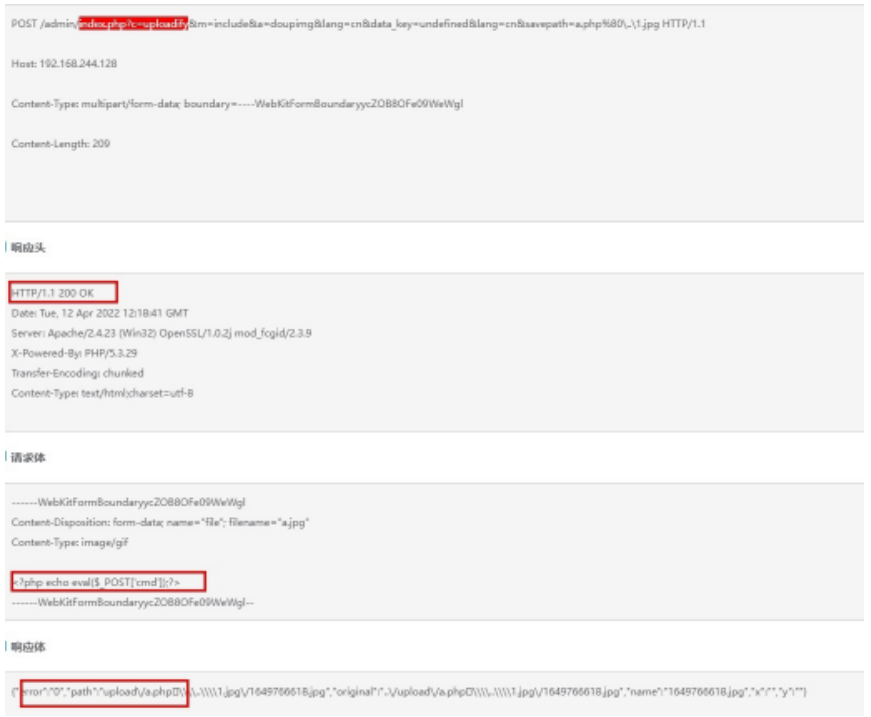
攻击-发现其使用metinfo框架，使用历史poc对服务器进行文件上传



DMZ区域入侵

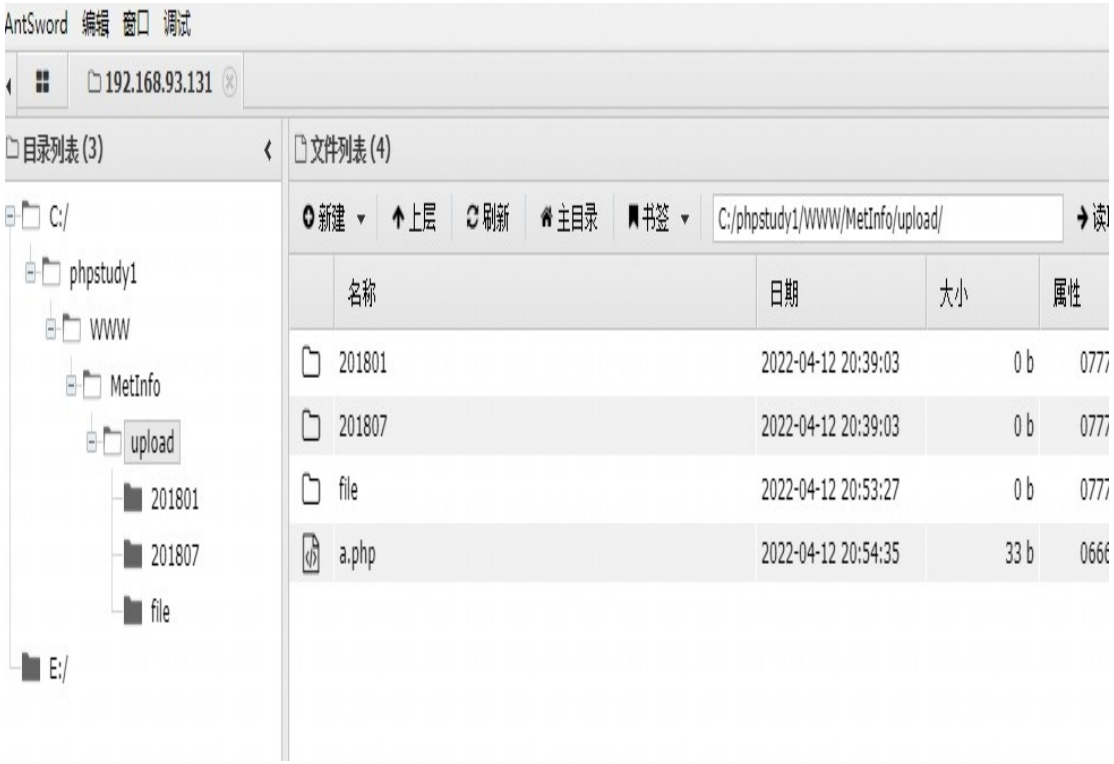
防守-在天眼分析文件上传的位置和溯源攻击

2022-04-12 20:20:33	192.168.93.131	192.168.93.1	【webshell上传】后门上传程序	发现PHP后门文件（机器学习）	企图	危急	2	详情 | 加白
2022-04-12 20:20:32	192.168.93.131	82.157.58.139	【网络攻击】拒绝服务	ACK_FLOOD	企图	高危	4	详情 | 加白
2022-04-12 20:20:32	192.168.93.131	192.168.93.1	【网页漏洞利用】文件上传	MetInfo <= 6.2.0前台任意文件上传漏洞	企图	高危	2	详情 | 加白



DMZ区域入侵

攻击-蚁剑连接webshell进行命令执行和代理文件的上传



DMZ区域入侵

防守-在天眼分析上传的文件和执行的命令

最近发生时间	受害IP	攻击IP	告警类型	威胁名称	攻击结果	威胁级别	次数	操作
2022-04-12 20:57:52	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
2022-04-12 20:57:52	192.168.93.131	192.168.93.1	【网页漏洞利用】代码执行	PHP代码执行漏洞(成功)(机器学习)	成功	危急	1	详情 | 加白
2022-04-12 20:57:51	192.168.93.131	192.168.93.1	【网络攻击】拒绝服务	ACK_FLOOD	企图	高危	4	详情 | 加白
2022-04-12 20:57:51	192.168.93.131	82.157.58.139	【网络攻击】拒绝服务	ACK_FLOOD	企图	高危	5	详情 | 加白
2022-04-12 20:57:51	192.168.93.131	情报查询	【网页漏洞利用】webshell利用	发现利用中国蚁剑连接后门行为	企图	危急	1	详情 | 加白
2022-04-12 20:57:51	192.168.93.131	192.168.93.1	【网页漏洞利用】webshell利用	发现利用中国蚁剑连接后门行为(v2.1)	失陷	危急	6	详情 | 加白
2022-04-12 20:57:51	192.168.93.131	192.168.93.1	【网页漏洞利用】命令执行	发现隐匿命令执行攻击行为	成功	危急	1	详情 | 加白
2022-04-12 20:57:51	192.168.93.131	192.168.93.1	【网页漏洞利用】webshell利用	发现利用中国蚁剑连接后门行为（企图）	企图	高危	1	详情 | 加白

连接特定的 DNS 后缀 . . . . . : localdomain

本地链接 IPv6 地址. . . . . : fe80::38b4:3112:feab:bc4e%12

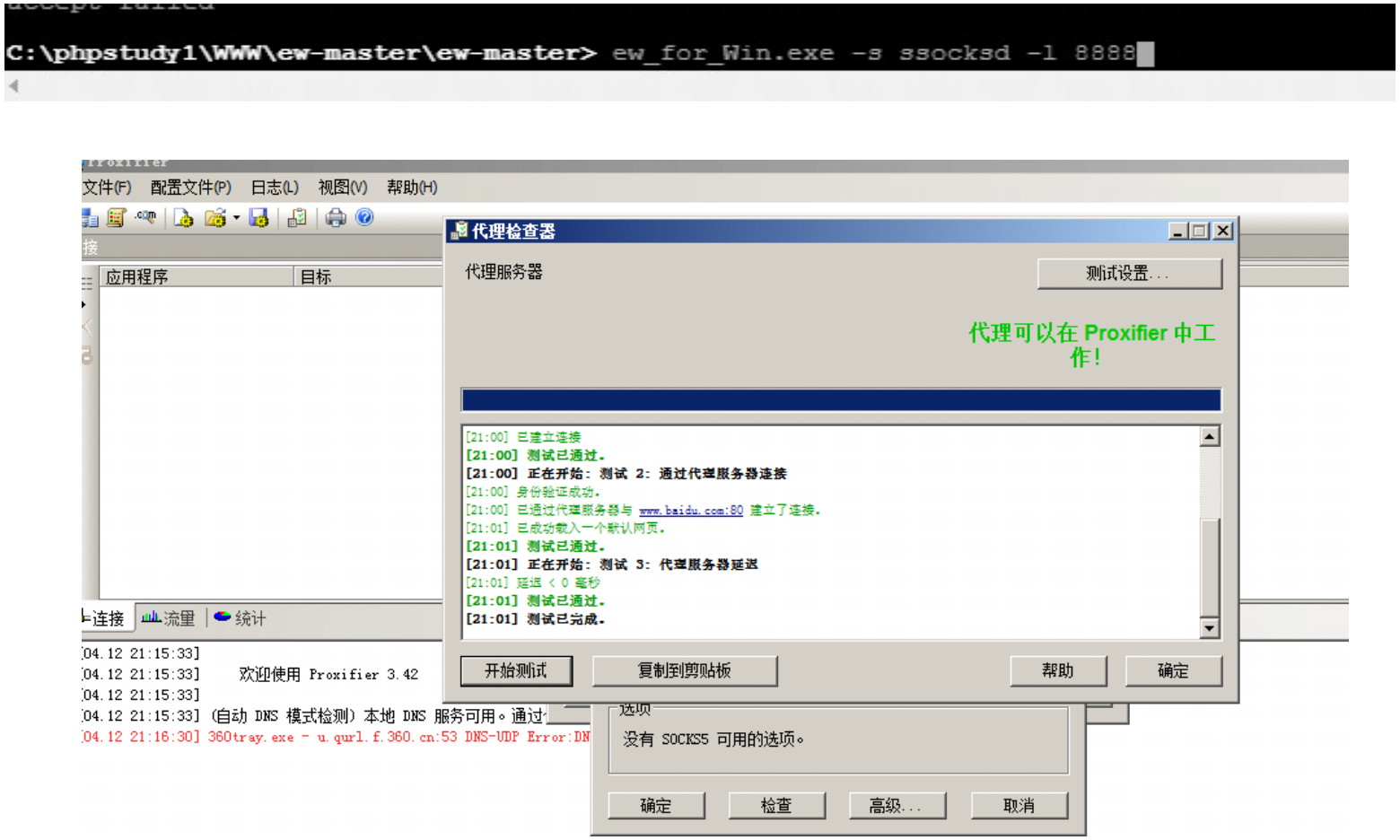
IPv4 地址 . . . . . : 192.168.93.131

子网掩码 . . . . . : 255.255.255.0

默认网关. . . . . : 192.168.93.2

DMZ区域入侵

攻击-使用socks5代理将流量代理出来



DMZ区域入侵

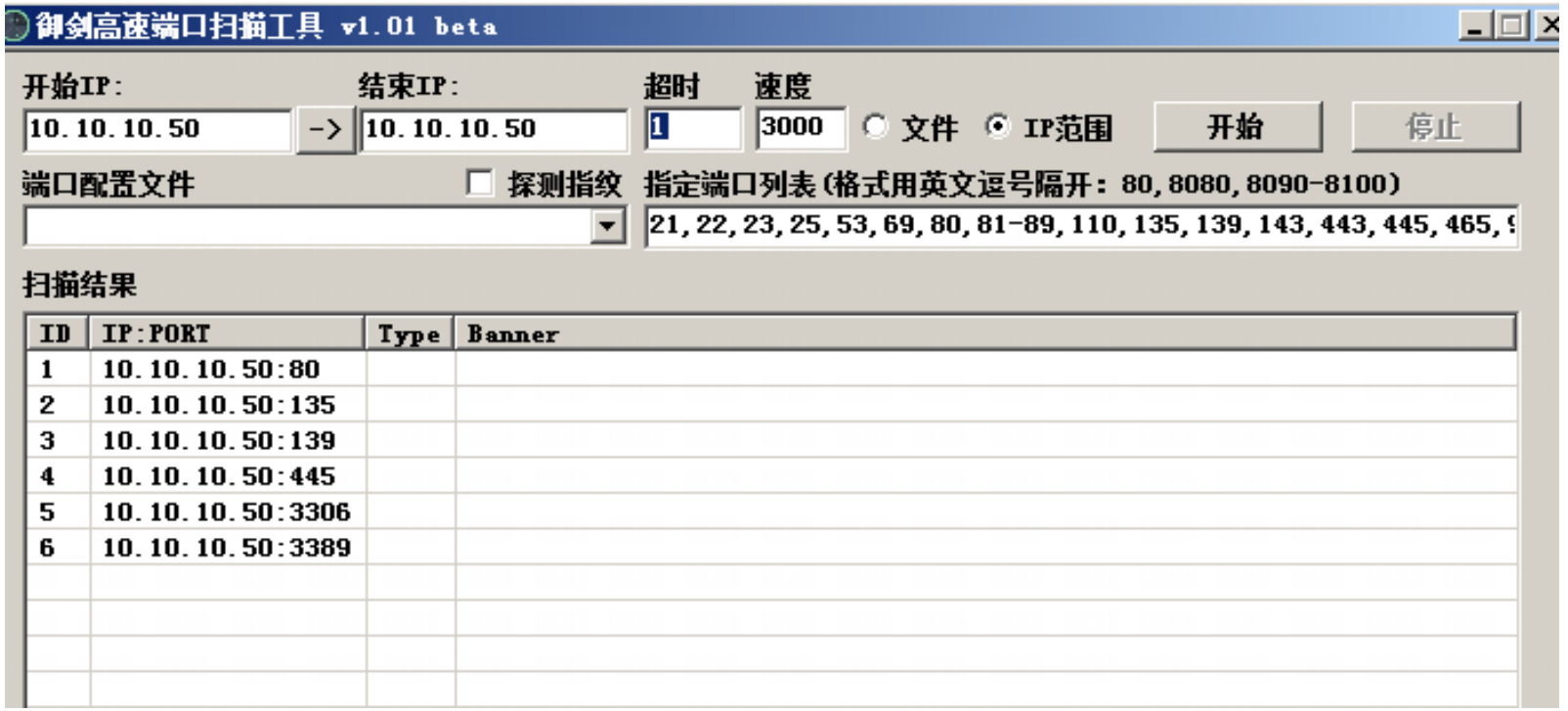
防守-在天眼看到攻击者使用socks5代理，分析代理端口,并且在服务器进行排查

2022-04-13 11:09:51	192.168.93.140	192.168.93.131	【网络攻击】其他	发现使用Socks代理	成功	中危	2	详情 | 加白
2022-04-13 11:09:51	192.168.93.131	192.168.93.140	【网络攻击】黑市工具	发现黑客工具-EarthWorm内网穿透工具	失陷	高危	2	详情 | 加白

```
TCP    192.168.93.131:139     0.0.0.0:0              LISTENING       4
TCP    192.168.93.131:8888    192.168.93.140:49187   TIME_WAIT       0
TCP    192.168.93.131:8888    192.168.93.140:49190   TIME_WAIT       0
TCP    192.168.93.131:8888    192.168.93.140:49193   TIME_WAIT       0
TCP    192.168.93.131:8888    192.168.93.140:49196   ESTABLISHED     3460
TCP    192.168.93.131:8888    192.168.93.140:49199   TIME_WAIT       0
TCP    192.168.93.131:8888    192.168.93.140:49202   TIME_WAIT       0
TCP    192.168.93.131:8888    192.168.93.140:49205   TIME_WAIT       0
TCP    192.168.93.131:49486   82.157.58.139:7902     CLOSE_WAIT      1204
TCP    192.168.93.131:49748   82.157.58.139:443      TIME_WAIT       0
TCP    192.168.93.131:49751   82.157.58.139:443      TIME_WAIT       0
TCP    192.168.93.131:49752   82.157.58.139:443      TIME_WAIT       0
TCP    192.168.93.131:49753   82.157.58.139:443      TIME_WAIT       0
TCP    192.168.93.131:49754   82.157.58.139:443      TIME_WAIT       0
TCP    192.168.93.131:49755   82.157.58.139:443      TIME_WAIT       0
TCP    192.168.93.131:49756   82.157.58.139:443      TIME_WAIT       0
```

办公区域入侵

攻击-首先在内网进行一个扫描发现办公区区域存活的机器有哪些,可以看到10.10.10.50存活并且开放80端口



办公区域入侵

攻击-访问发现是dede，使用弱口令进行后台登录并且上传webshell

办公区域入侵

防守-在天眼发现dede弱口令登录，并且发现一句话木马上传

最近发生时间	受害IP	攻击IP	告警类型	威胁名称	攻击结果	威胁级别	次数	操作
2022-04-13 11:48:09	10.10.10.50	10.10.10.90	【网页漏洞利用】其他	发现明文口令传输	成功	中危	2	详情|加白
2022-04-13 11:48:09	10.10.10.50	10.10.10.90	【网页漏洞利用】弱口令	Dedecms系统弱口令登录	成功	高危	2	详情|加白
2022-04-13 11:48:09	192.168.93.131	192.168.93.140	【网页漏洞利用】其他	发现明文口令传输	成功	中危	2	详情|加白
2022-04-13 11:48:09	192.168.93.131	192.168.93.140	【网页漏洞利用】弱口令	Dedecms系统弱口令登录	成功	高危	2	详情|加白
2022-04-13 11:48:09	10.10.10.50	10.10.10.90	【网页漏洞利用】弱口令	Web弱口令登录	成功	高危	2	详情|加白
2022-04-13 11:48:09	192.168.93.131	192.168.93.140	【网页漏洞利用】弱口令	Web弱口令登录	成功	高危	2	详情|加白

2022-04-13 11:45:29	10.10.10.50	10.10.10.90	【webshell上传】后门上传程序	发现PHP后门文件（机器学习）	企图	危急	1	详情|加白
2022-04-13 11:45:29	10.10.10.50	10.10.10.90	【webshell上传】中国菜刀变形	中国菜刀变形.A	企图	危急	1	详情|加白
2022-04-13 11:45:29	192.168.93.131	192.168.93.140	【webshell上传】后门上传程序	发现PHP后门文件（机器学习）	企图	危急	1	详情|加白
2022-04-13 11:45:29	192.168.93.131	192.168.93.140	【webshell上传】中国菜刀变形	中国菜刀变形.A	企图	危急	1	详情|加白

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/156052151011010121