## **使用diff和patch工具打补丁**

### **3.1 问题**

本案例要求优化提升常见网络服务的安全性，主要完成以下任务操作：

1. 使用diff对比文件差异
2. 使用diff生成补丁文件
3. 使用patch命令为旧版本打补丁

### **3.2 方案**

程序是人设计出来的，总是会有这样那样的问题与漏洞，目前的主流解决方法就是为有问题的程序打补丁，升级新版本。

在Linux系统中diff命令可以为我们生成补丁文件，然后使用patch命令为有问题的程序代码打补丁。

### **3.3 步骤**

实现此案例需要按照如下步骤进行。

步骤一：对比单个文件差异

1） 编写两个版本的脚本，一个为v1版本，一个为v2版本。

[copytextpop-up](http://tts.tmooc.cn/ttsPage/LINUX/NSDTN202001/SECURITY/DAY05/CASE/01/index.html)

1. [root@proxy ~]# cat test1.sh                                //v1版本脚本
2. #!/bin/bash
3. echo "hello wrld"
5. [root@proxy ~]# cat test2.sh                                //v2版本脚本
6. #!/bin/bash
7. echo "hello the world"
8. echo "test file"

[root@proxy ~]# cat test1.sh //v1版本脚本

#!/bin/bash

echo "hello wrld"

[root@proxy ~]# cat test2.sh //v2版本脚本

#!/bin/bash

echo "hello the world"

echo "test file"

2） 使用diff命令语法

使用diff命令查看不同版本文件的差异。

[copytextpop-up](http://tts.tmooc.cn/ttsPage/LINUX/NSDTN202001/SECURITY/DAY05/CASE/01/index.html)

1. [root@proxy ~]# diff test1.sh test2.sh                     //查看文件差异
2. @@ -1,3 +1,3 @@
3. #!/bin/bash
4. -echo "hello world"
5. -echo "test"
6. +echo "hello the world"
7. +echo "test file"
9. [root@proxy ~]# diff -u test1.sh test2.sh                 //查看差异，包含头部信息
10. --- test1.sh    2018-02-07 22:20:02.723971251 +0800
11. +++ test2.sh    2018-02-07 22:20:13.358760687 +0800
12. @@ -1,3 +1,3 @@
13. #!/bin/bash
14. -echo "hello world"
15. -echo "test"
16. +echo "hello the world"
17. +echo "test file"

[root@proxy ~]# diff test1.sh test2.sh //查看文件差异

@@ -1,3 +1,3 @@

#!/bin/bash

-echo "hello world"

-echo "test"

+echo "hello the world"

+echo "test file"

[root@proxy ~]# diff -u test1.sh test2.sh //查看差异，包含头部信息

--- test1.sh 2018-02-07 22:20:02.723971251 +0800

+++ test2.sh 2018-02-07 22:20:13.358760687 +0800

@@ -1,3 +1,3 @@

#!/bin/bash

-echo "hello world"

-echo "test"

+echo "hello the world"

+echo "test file"

diff制作补丁文件的原理：告诉我们怎么修改第一个文件后能得到第二个文件。

这样如果第一个版本的脚本有漏洞，我们不需要将整个脚本都替换，仅需要修改有问题的一小部分代码即可，diff刚好可以满足这个需求！

像Linux内核这样的大块头，一旦发现有一个小漏洞，我们不可能把整个内核都重新下载，全部替换一遍，而仅需要更新有问题的那一小部分代码即可！

diff命令常用选项：

-u 输出统一内容的头部信息（打补丁使用），计算机知道是哪个文件需要修改

-r 递归对比目录中的所有资源（可以对比目录）

-a 所有文件视为文本（包括二进制程序）

-N 无文件视为空文件（空文件怎么变成第二个文件）

-N选项备注说明：

A目录下没有txt文件，B目录下有txt文件

diff比较两个目录时，默认会提示txt仅在B目录有（无法对比差异，修复文件）

diff比较时使用N选项，则diff会拿B下的txt与A下的空文件对比，补丁信息会明确说明如何从空文件修改后变成txt文件，打补丁即可成功！

步骤二：使用patch命令对单文件代码打补丁

1）准备实验环境

[copytextpop-up](http://tts.tmooc.cn/ttsPage/LINUX/NSDTN202001/SECURITY/DAY05/CASE/01/index.html)

1. [root@proxy ~]# cd demo
2. [root@proxy demo]# vim test1.sh
3. #!/bin/bash
4. echo "hello world"
5. echo "test"
6. [root@proxy demo]# vim test2.sh
7. #!/bin/bash
8. echo "hello the world"
9. echo "test file"

[root@proxy ~]# cd demo

[root@proxy demo]# vim test1.sh

#!/bin/bash

echo "hello world"

echo "test"

[root@proxy demo]# vim test2.sh

#!/bin/bash

echo "hello the world"

echo "test file"

2) 生成补丁文件

[copytextpop-up](http://tts.tmooc.cn/ttsPage/LINUX/NSDTN202001/SECURITY/DAY05/CASE/01/index.html)

1. [root@proxy demo]# diff -u test1.sh test2.sh > test.patch

[root@proxy demo]# diff -u test1.sh test2.sh > test.patch

3）使用patch命令打补丁

在代码相同目录下为代码打补丁

[copytextpop-up](http://tts.tmooc.cn/ttsPage/LINUX/NSDTN202001/SECURITY/DAY05/CASE/01/index.html)

1. [root@proxy demo]# yum -y install patch
2. [root@proxy demo]# patch -p0 < test.patch                    //打补丁
3. patching file test1.sh
4. //patch -pnum（其中num为数字，指定删除补丁文件中多少层路径前缀）
5. //如原始路径为/u/howard/src/blurfl/blurfl.c
6. //-p0则整个路径不变
7. //-p1则修改路径为u/howard/src/blurfl/blurfl.c
8. //-p4则修改路径为blurfl/blurfl.c
9. //-R(reverse)反向修复，-E修复后如果文件为空，则删除该文件
10. [root@proxy demo]# patch -RE < test.patch                     //还原旧版本，反向修复

[root@proxy demo]# yum -y install patch

[root@proxy demo]# patch -p0 < test.patch //打补丁

patching file test1.sh

//patch -pnum（其中num为数字，指定删除补丁文件中多少层路径前缀）

//如原始路径为/u/howard/src/blurfl/blurfl.c

//-p0则整个路径不变

//-p1则修改路径为u/howard/src/blurfl/blurfl.c

//-p4则修改路径为blurfl/blurfl.c

//-R(reverse)反向修复，-E修复后如果文件为空，则删除该文件

[root@proxy demo]# patch -RE < test.patch //还原旧版本，反向修复

步骤三：对比目录中所有文件的差异

1） 准备实验环境

[copytextpop-up](http://tts.tmooc.cn/ttsPage/LINUX/NSDTN202001/SECURITY/DAY05/CASE/01/index.html)

1. [root@proxy ~]# mkdir demo
2. [root@proxy ~]# cd demo
3. [root@proxy demo]# mkdir {source1,source2}
5. [root@proxy demo]# echo "hello world" > source1/test.sh
6. [root@proxy demo]# cp /bin/find source1/
7. [root@proxy demo]# tree source1/                        //source1目录下2个文件
8. |-- find
9. `-- test.sh
11. [root@proxy demo]# echo "hello the world" > source2/test.sh
12. [root@proxy demo]# echo "test" > source2/tmp.txt
13. [root@proxy demo]# cp /bin/find source2/
14. [root@proxy demo]# echo "1" >> source2/find
15. [root@proxy demo]# tree source2/                        //source1目录下3个文件
16. |-- find
17. |-- test.sh
18. `-- tmp.txt
19. //注意：两个目录下find和test.sh文件内容不同，source2有tmp.txt而source1没有该文件

[root@proxy ~]# mkdir demo

[root@proxy ~]# cd demo

[root@proxy demo]# mkdir {source1,source2}

[root@proxy demo]# echo "hello world" > source1/test.sh

[root@proxy demo]# cp /bin/find source1/

[root@proxy demo]# tree source1/ //source1目录下2个文件

|-- find

`-- test.sh

[root@proxy demo]# echo "hello the world" > source2/test.sh

[root@proxy demo]# echo "test" > source2/tmp.txt

[root@proxy demo]# cp /bin/find source2/

[root@proxy demo]# echo "1" >> source2/find

[root@proxy demo]# tree source2/ //source1目录下3个文件

|-- find

|-- test.sh

`-- tmp.txt

//注意：两个目录下find和test.sh文件内容不同，source2有tmp.txt而source1没有该文件

2）制作补丁文件

[copytextpop-up](http://tts.tmooc.cn/ttsPage/LINUX/NSDTN202001/SECURITY/DAY05/CASE/01/index.html)

1. [root@proxy demo]# diff -u source1/ source2/
2. //仅对比了文本文件test.sh；二进制文件、tmp都没有对比差异，仅提示，因为没有-a和-N选项
3. [root@proxy demo]# diff -Nu source1/ source2/
4. //对比了test.sh，并且使用source2目录的tmp.txt与source1的空文件对比差异。
5. [root@proxy demo]# diff -Nua source1/ source2/
6. //对比了test.sh、tmp.txt、find(程序)。

[root@proxy demo]# diff -u source1/ source2/

//仅对比了文本文件test.sh；二进制文件、tmp都没有对比差异，仅提示，因为没有-a和-N选项

[root@proxy demo]# diff -Nu source1/ source2/

//对比了test.sh，并且使用source2目录的tmp.txt与source1的空文件对比差异。

[root@proxy demo]# diff -Nua source1/ source2/

//对比了test.sh、tmp.txt、find(程序)。

步骤四：使用patch命令对目录下的所有代码打补丁

1）使用前面创建的source1和source2目录下的代码为素材，生成补丁文件

[copytextpop-up](http://tts.tmooc.cn/ttsPage/LINUX/NSDTN202001/SECURITY/DAY05/CASE/01/index.html)

1. [root@proxy ~]# cd demo
2. [root@proxy demo]# diff -Nuar source1/ source2/ > source.patch

[root@proxy ~]# cd demo

[root@proxy demo]# diff -Nuar source1/ source2/ > source.patch

2）使用patch命令为代码打补丁

[copytextpop-up](http://tts.tmooc.cn/ttsPage/LINUX/NSDTN202001/SECURITY/DAY05/CASE/01/index.html)

1. [root@proxy demo]# ls
2. source1 source2 source.patch
3. [root@proxy demo]# cat source.patch                //对比的文件有路径信息
4. --- source1/test.sh 2018-02-07 22:51:33.034879417 +0800
5. +++ source2/test.sh 2018-02-07 22:47:32.531754268 +0800
6. @@ -1 +1 @@
7. -hello world
8. +hello the world
9. [root@proxy demo]# cd source1
10. [root@proxy source1]# patch -p1 < ../source.patch

diff和patch使用总结

·使用diff 对比文件差异

Diff 旧文件/目录 新文件/目录

·生成diff 补丁文件

Diff -Nuar 旧文件/目录 新文件/目录 > 补丁文件名（任意）.diff

diff命令常用选项：

-u 输出统一内容的头部信息（打补丁使用），计算机知道是哪个文件需要修改

-r 递归对比目录中的所有资源（可以对比目录）

-a 所有文件视为文本（包括二进制程序）

-N 无文件视为空文件（空文件怎么变成第二个文件）

-N选项备注说明：

A目录下没有txt文件，B目录下有txt文件

diff比较两个目录时，默认会提示txt仅在B目录有（无法对比差异，修复文件）

diff比较时使用N选项，则diff会拿B下的txt与A下的空文件对比，

补丁信息会明确说明如何从空文件修改后变成txt文件，打补丁即可成功！

·使用patch命令对单文件打补丁

软件包 patch

Patch -p0 < 补丁名字.diff

1. //patch -pnum（其中num为数字，指定删除补丁文件中多少层路径前缀）
2. //如原始路径为/u/howard/src/blurfl/blurfl.c
3. //-p0则整个路径不变
4. //-p1则修改路径为u/howard/src/blurfl/blurfl.c 和当前自己坐在位置有关系
5. //-p4则修改路径为blurfl/blurfl.c
6. //-R(reverse)反向修复，-E修复后如果文件为空，则删除该文件
7. root@proxy demo]# patch -RE < test.patch