路由器漏洞复现 -环境搭建

- gdbserve7.12-mips的下载
- gdb7.12的下载编译
- 把gdbserve传到路由器上
- 还有如何通过uart口连接到路由器 并拿到shell

gdbserve的下载

因为gdb太大，无法直接放到路由器上，我们选择gdbserve+gdb。gdbserve放在路由器上运行。所以我们需要一个能在mips架构上运行的gdbserve。可以选择自己下载源码然后编译，也可以选择网上现成编译好的。

https://github.com/mzpqnxow/embedded-toolkit/tree/master/prebuilt*static*bins/gdbserver

gdb下载编译

gdb需要自己编译 host=linux target=mips。源码从官网上就可以下载。 7.12的gdbserve配7.12gdb。

把gdbserve传到路由器

我目前在用的路由器是 d-link dir822. 只支持 wget。

作为菜鸟，我一开始在ubuntu上搭建ftp，但是就是 wget不下来？？？！！！ 总是会出现错误 提示 cannot open file？？ `wget ftp://anonymous@ip/路径`

实在是不知道为什么，后来换了http ，大神告诉我 python可以快速搭建服务器

```
python -m SimpleHTTPServer 8088
```

```
wget http://ip/路径
```

但是出现404错误。

于是我终于知道刚才为什么ftp就不行，因为文件名打错了！！！！！

很气～浪费了很久的时间