□□□□□□□□ □□□□□□□ □□ □□□□□□□ 4□ पर आक्रमण

यह मेरा तीसरा प्रयास है □□□□□□□□ को इंस्टॉल करने का। पहली बार 2019 में था, जब मैंने एक □□□□ पोर्ट का उपयोग करके कनेक्ट किया था। दूसरी बार, 2023 में, मैंने यहाँ वर्णित एक समान दूरस्थ विधि का उपयोग किया था।

एक्सप्लॉइट कोड को यहाँ से प्राप्त किया जा सकता है: □□□□□://□□□□□□□.□□□/□□□□□□□□□/□□□□□□□□□□□□□□□□□.

पहले, आवश्यकताओं को इंस्टॉल करें:

```
pip install -r requirements.txt --break-system-packages
```

एक्सप्लॉइट चलाने के बाद, आप राउटर के वेब इंटरफेस तक एक □□□ के साथ पहुंच सकते हैं जो इस जैसा है (□□□□ का मान बदल सकता है):

```
http://192.168.1.28/cgi-bin/luci/;stok=fe9b14c5c4dee48709fbdf00e048d5ec/web/home
```

```
lzwjava@anonymous OpenWRTInvasion % python remote_command_execution_vulnerability.py
Router IP address [press enter for using the default 'miwifi.com']: 192.168.1.28
Enter router admin password: ...
There two options to provide the files needed for invasion:
   1. Use a local TCP file server runing on random port to provide files in local directory `script_tools`.
   2. Download needed files from remote github repository. (choose this option only if github is accessable in
Which option do you prefer? (default: 1)1
****************
router_ip_address: 192.168.1.28
stok: 08f4f22fed20b94580cb8e70703c941c
file provider: local file server
****************
start uploading config file...
start exec command...
local file server is runing on 0.0.0.0:63067. root='script_tools'
local file server is getting 'busybox-mipsel' for 192.168.1.28.
local file server is getting 'dropbearStaticMipsel.tar.bz2' for 192.168.1.28.
done! Now you can connect to the router using several options: (user: root, password: root)
* telnet 192.168.1.28
* ssh -oKexAlgorithms=+diffie-hellman-group1-sha1 -oHostKeyAlgorithms=+ssh-rsa -c 3des-cbc -o UserKnownHostsFi
* ftp: using a program like cyberduck
```

```
root@XiaoQiang:/tmp# wget "https://downloads.openwrt.org/releases/24.10.0/targets/ramips/mt76x8/openwrt-24.10
ade.bin"
wget: not an http or ftp url: https://downloads.openwrt.org/releases/24.10.0/targets/ramips/mt76x8/openwrt-24
```

```
scp -oKexAlgorithms=+diffie-hellman-group1-sha1 -oHostKeyAlgorithms=+ssh-rsa -c 3des-cbc  openwrt-24.10.0-rami
ash: /usr/libexec/sftp-server: not found
```

```
scp: Connection closed
```

```
cat openwrt-24.10.0-ramips-mt76x8-xiaomi_mi-router-4c-squashfs-sysupgrade.bin | ssh -oKexAlgorithms=+diffie-he
```

```
root@XiaoQiang:/tmp# ls
2541.bootcheck.log                                                  oui
TZ                                                                  rc.done
appStoreRule.json                                                   rc.timing
arrays                                                              resolv.conf
authenfailed-cache                                                  resolv.conf.auto
busybox                                                             root
daemon                                                              rr
datalist                                                            run
dropbear                                                            script.sh
dropbear.tar.bz2                                                    speedtest_urls.xml
etc                                                                 spool
ftpd                                                                startscene_crontab.lua.PID
lock                                                                stat_points_privacy.log
log                                                                 stat_points_rom.log
logexec                                                             state
luci-indexcache                                                     sysapihttpd
luci-nonce                                                          sysapihttpdconf
luci-sessions                                                       sysinfo
messages                                                            syslog-ng.ctl
miqos.lock                                                          syslog-ng.pid
mnt                                                                 taskmonitor
mt76xx2.sh.log                                                      uci2dat_mt7628.log
network.env                                                         uploadfiles
nginx_check.log                                                     upnp.leases
ntp.status                                                          web_config_list
openwrt-24.10.0-ramips-mt76x8-xiaomi_mi-router-4c-squashfs-sysupgrade.bin  wifi_analysis.log
```

```
root@XiaoQiang:/tmp# mtd -r write openwrt-24.10.0-ramips-mt76x8-xiaomi_mi-router-4c-squashfs-sysupgrade.bin OS
Unlocking OS1 ...

Writing from openwrt-24.10.0-ramips-mt76x8-xiaomi_mi-router-4c-squashfs-sysupgrade.bin to OS1 ...  [w]
```

राउटर को एक वायर्ड कनेक्शन के माध्यम से कनेक्ट करें। फिर आप 192.168.1.1 पर वेब इंटरफेस तक पहुंच सकते हैं या `ssh root@192.168.1.1` चलाकर □□□ का उपयोग कर सकते हैं।