HackerFrogs Afterschool
Network Hacking – Session 9

Class:
Network Hacking

Workshop Number:
AS-NET-09

Document Version:
1.75

Special Requirements:
Registered account
at tryhackme.com

Welcome to HackerFrogs Afterschool!

This is the ninth session for network hacking!

Let's go over the concepts we covered in the previous session!

What are File Upload Attacks?

File Upload Attacks are a type of web app hack where malicious files can be uploaded to a web server and then accessed on the web app, executing the code within the uploaded malicious files

What are File Upload Attacks?

In order to perform a file upload attack, there are three conditions that must be met

1) There must be a way to upload files to a web-accessible location, via web app, or another service (e.g., FTP, SMB)

2) The upload location must be known to us

3) The app must be able to execute code: e.g., PHP or ASP

This Session's Topics

- What is Privilege Escalation (Priv Esc)?

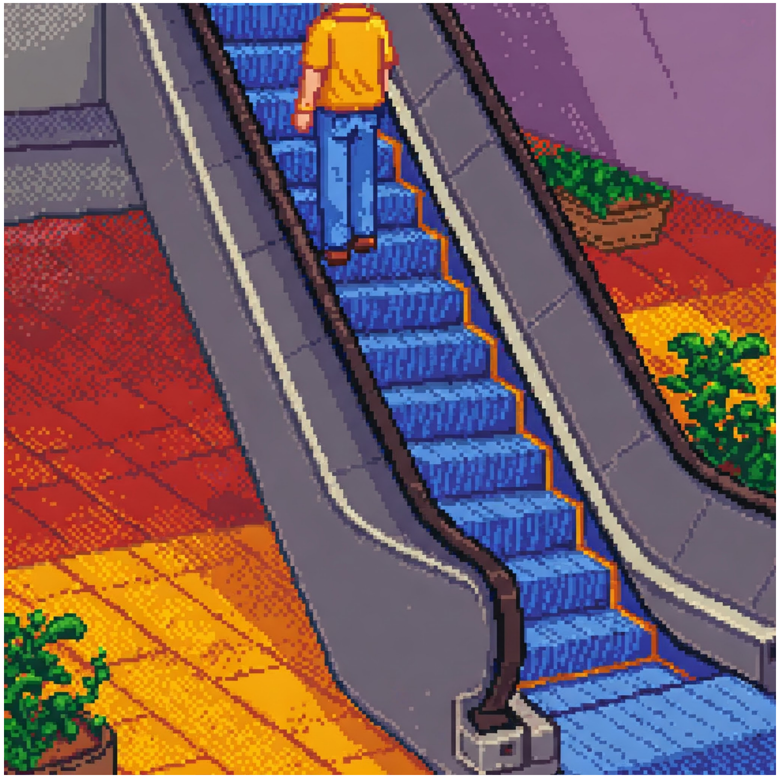
- Priv Esc via Sudo

- Priv Esc via SUID

- Priv Esc via Kernel Exploits

What is Privilege Escalation?

Privilege escalation (priv esc), is the act of upgrading the level of access on a system, typically through abusing insecure settings, capturing credentials

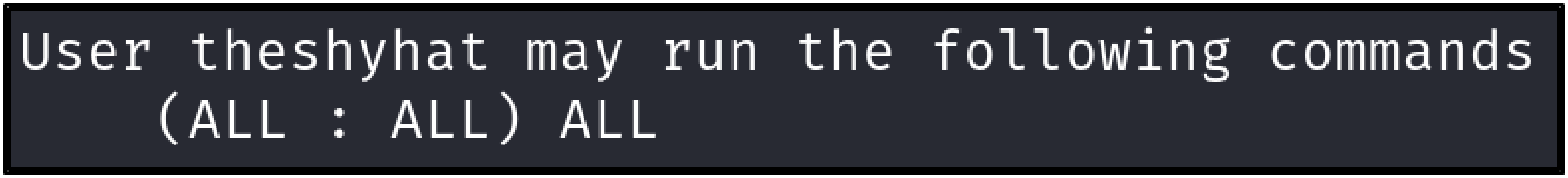


Accessing TryHackMe

Let's access this TryHackMe room to learn about privilege escalation:

https://tryhackme.com/room/linprivesc

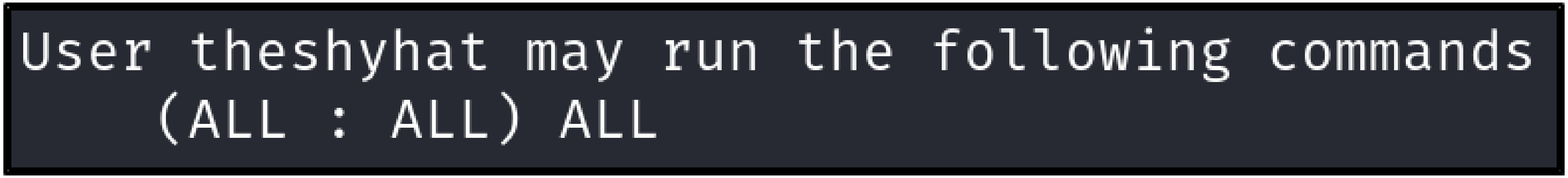
Priv Esc via Sudo



```
User theshyhat may run the following commands
    (ALL : ALL) ALL
```

If a user has access sudo (root) access with any command, there is the possibility of abusing that command for privilege escalation

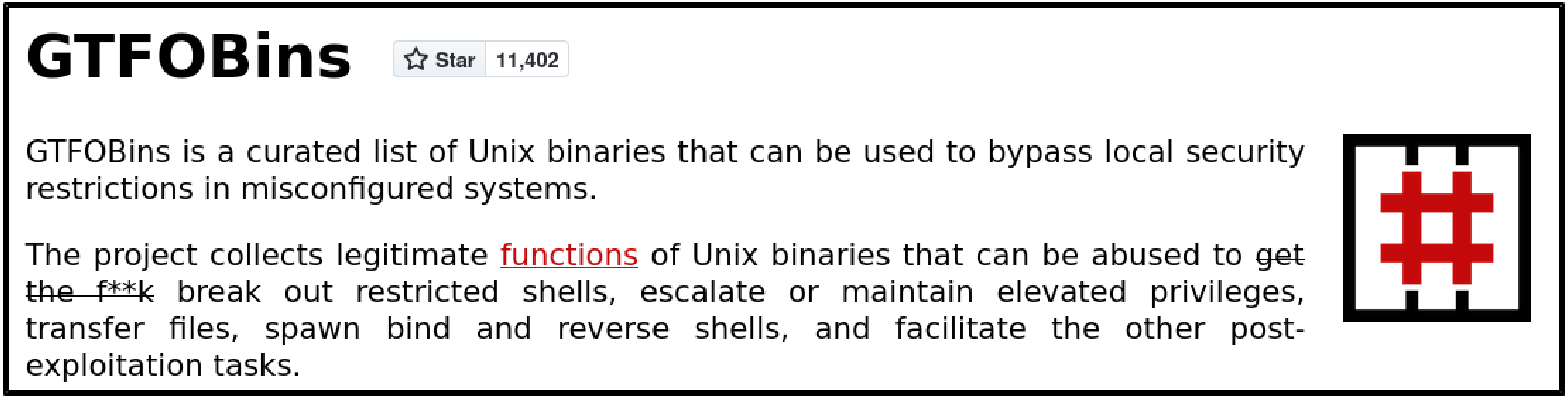
Priv Esc via Sudo



```
User theshyhat may run the following commands
    (ALL : ALL) ALL
```

We can list our sudo permissions in Linux with the `sudo -l` command. In the above example, the user can run as all users, and all groups, any command

Priv Esc via Sudo



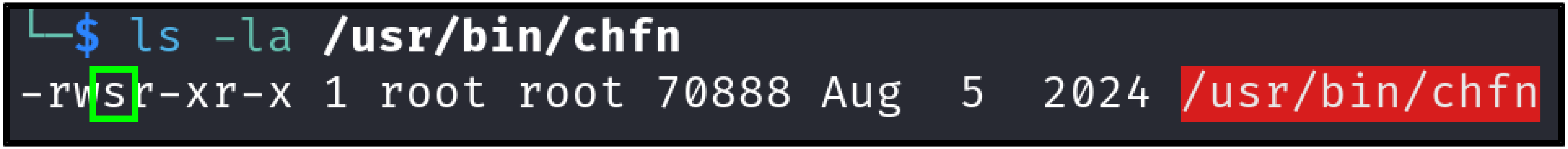
GTFOBins

GTFOBins is a curated list of Unix binaries that can be used to bypass local security restrictions in misconfigured systems.

The project collects legitimate functions of Unix binaries that can be abused to ~~get the f**k~~ break out restricted shells, escalate or maintain elevated privileges, transfer files, spawn bind and reverse shells, and facilitate the other post-exploitation tasks.

There's a popular website called GTFOBins which can be used to lookup whether a Linux command can be used for privilege escalation or not

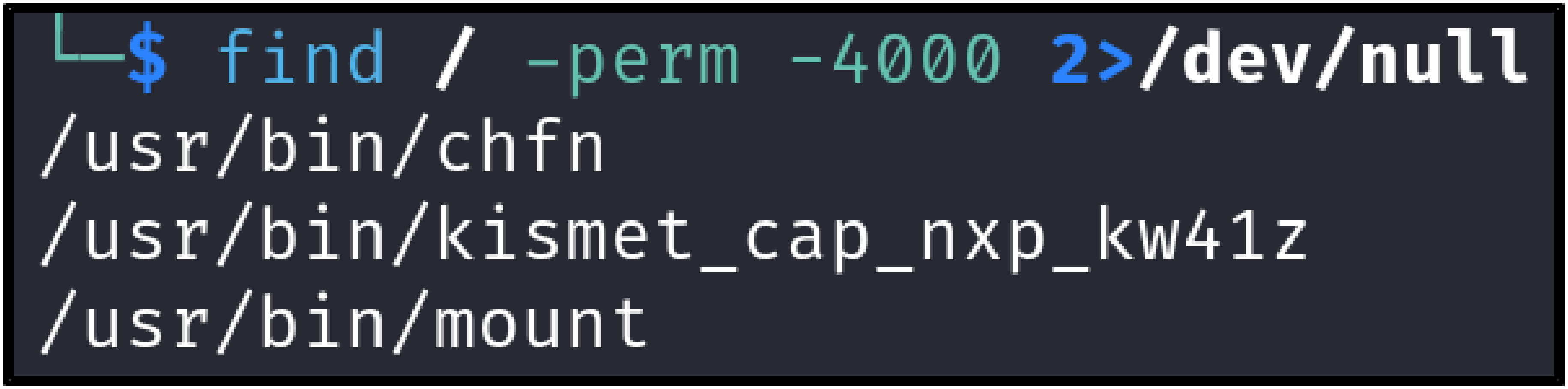
Priv Esc via SUID



```
└─$ ls -la /usr/bin/chfn
-rwsr-xr-x 1 root root 70888 Aug  5  2024 /usr/bin/chfn
```

SUID binaries are commands that are run in the context of the file's owner by default. Most SUID binaries are owned by the **root** user, and certain SUID binaries can be used for privilege escalation

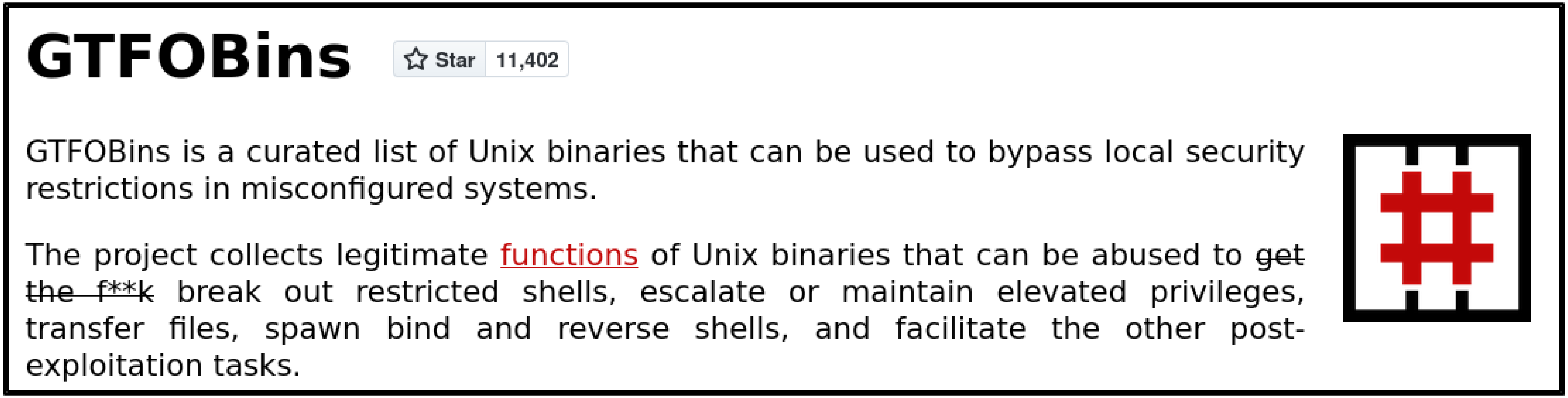
Priv Esc via SUID



```
└─$ find / -perm -4000 2>/dev/null
/usr/bin/chfn
/usr/bin/kismet_cap_nxp_kw41z
/usr/bin/mount
```

We can determine which SUID binaries exist on a system with the example `find` command above

Priv Esc via Sudo



GTFOBins

GTFOBins is a curated list of Unix binaries that can be used to bypass local security restrictions in misconfigured systems.

The project collects legitimate functions of Unix binaries that can be abused to ~~get the f**k~~ break out restricted shells, escalate or maintain elevated privileges, transfer files, spawn bind and reverse shells, and facilitate the other post-exploitation tasks.

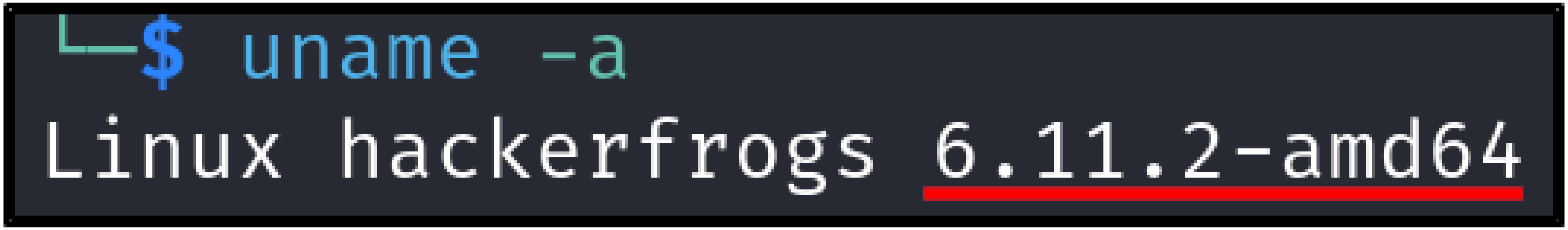
Like with sudo commands, the GTFOBins website can be used to search for SUID commands that can be used for privilege escalation

Priv Esc via Kernel Exploits

Kernel exploits are hacks that target the lowest level of operations in an operating system

Typically, older versions of operating systems are vulnerable to kernel exploits

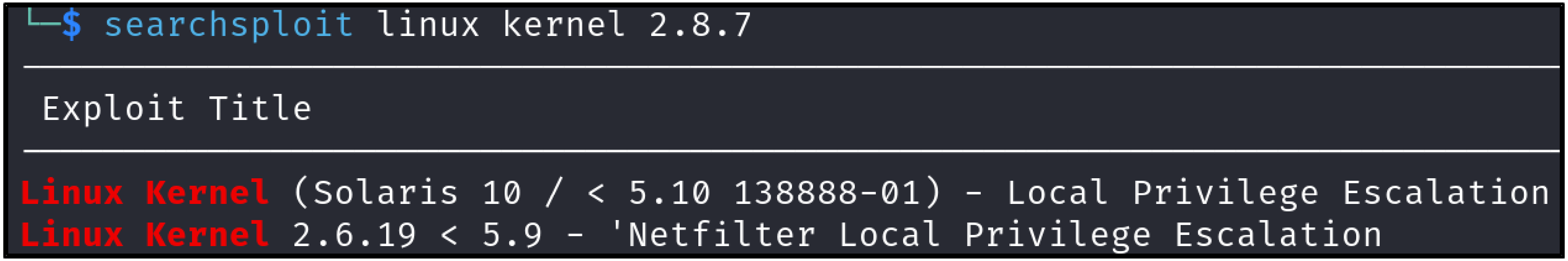
Priv Esc via Kernel Exploits



```
└─$ uname -a
Linux hackerfrogs 6.11.2-amd64
```

We can use the `uname -a` command to return the OS version for a computer

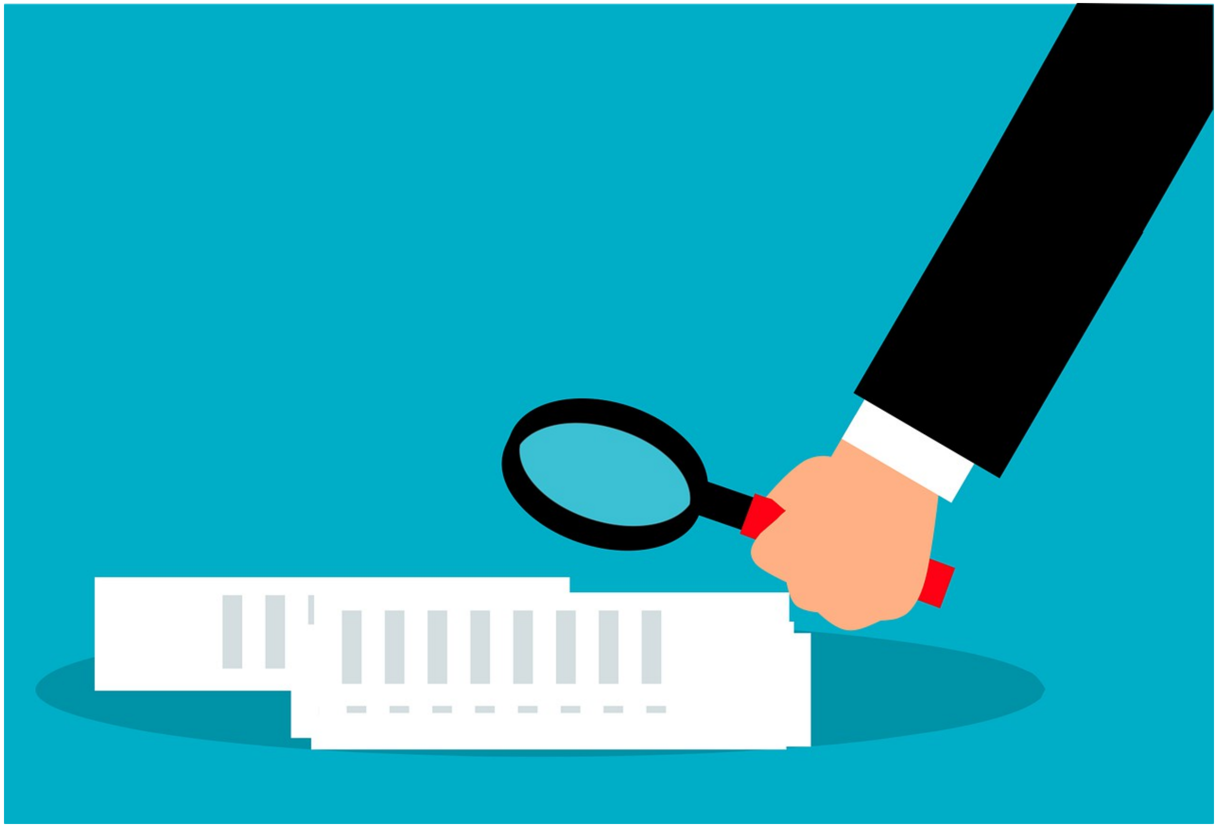
Priv Esc via Kernel Exploits



```
└─$ searchsploit linux kernel 2.8.7
---------------------------------------------------------------------------
 Exploit Title
---------------------------------------------------------------------------
Linux Kernel (Solaris 10 / < 5.10 138888-01) - Local Privilege Escalation
Linux Kernel 2.6.19 < 5.9 - 'Netfilter Local Privilege Escalation
```

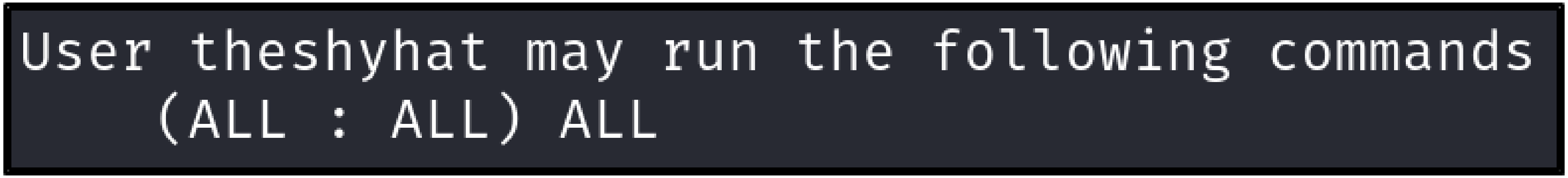
We can research whether a particular version of an OS is vulnerable by using the searchsploit command or using a search engine

Summary



Let's review the network hacking concepts we learned in this workshop:

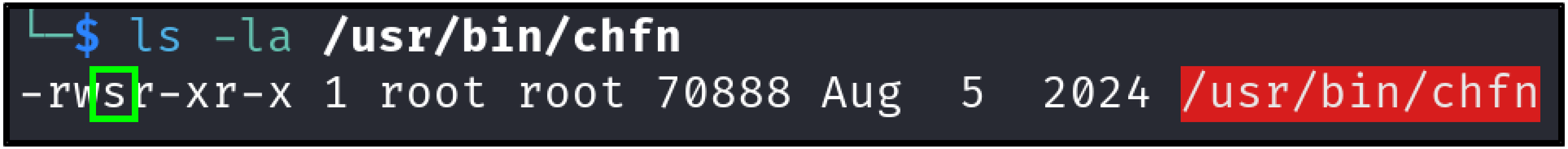
Priv Esc via Sudo



```
User theshyhat may run the following commands
    (ALL : ALL) ALL
```

If a user has access sudo (root) access with any command, there is the possibility of abusing that command for privilege escalation

Priv Esc via SUID



```
└─$ ls -la /usr/bin/chfn
-rwsr-xr-x 1 root root 70888 Aug  5  2024 /usr/bin/chfn
```

SUID binaries are commands that are run in the context of the file's owner by default. Most SUID binaries are owned by the **root** user, and certain SUID binaries can be used for privilege escalation

Priv Esc via Kernel Exploits

Kernel exploits are hacks that target the lowest level of operations in an operating system

Typically, older versions of operating systems are vulnerable to kernel exploits

What's Next?

In the next HackerFrogs Afterschool Network Hacking workshop, we'll be finishing our look at Linux privilege escalation!