Ahmed Emad Eldeen Abdelmoneam

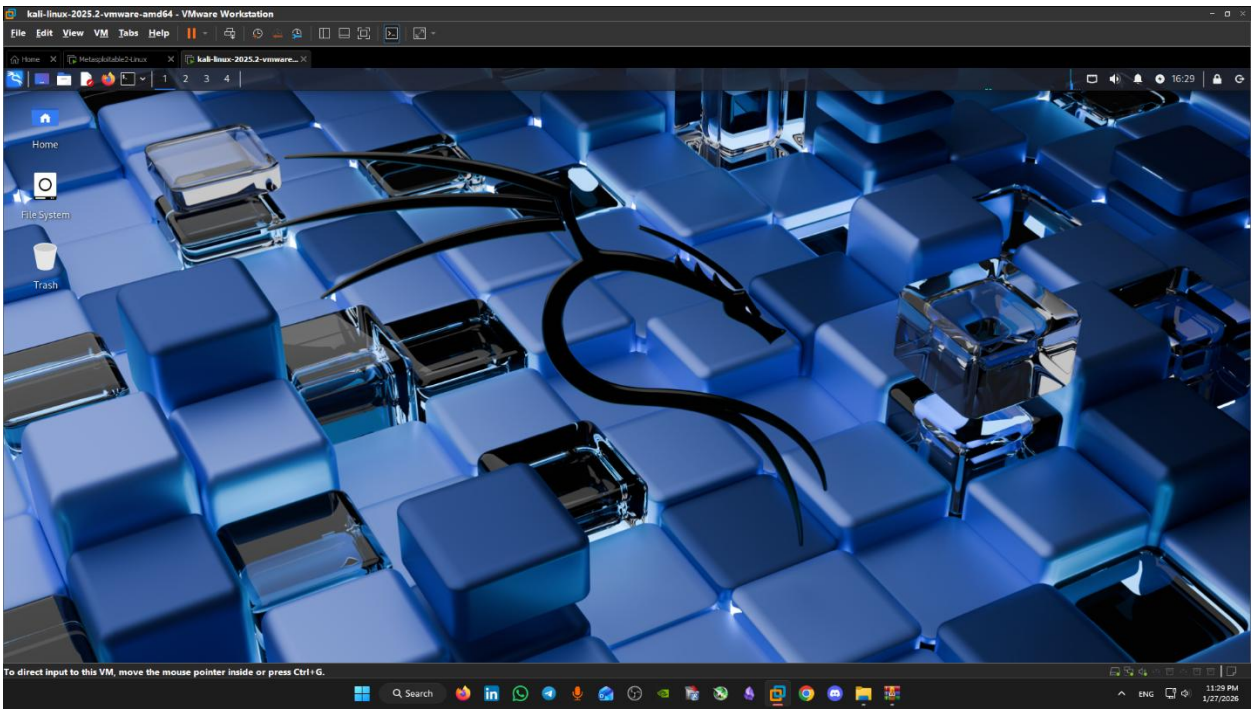
LinkedIn: https://www.linkedin.com/in/0x3omda/

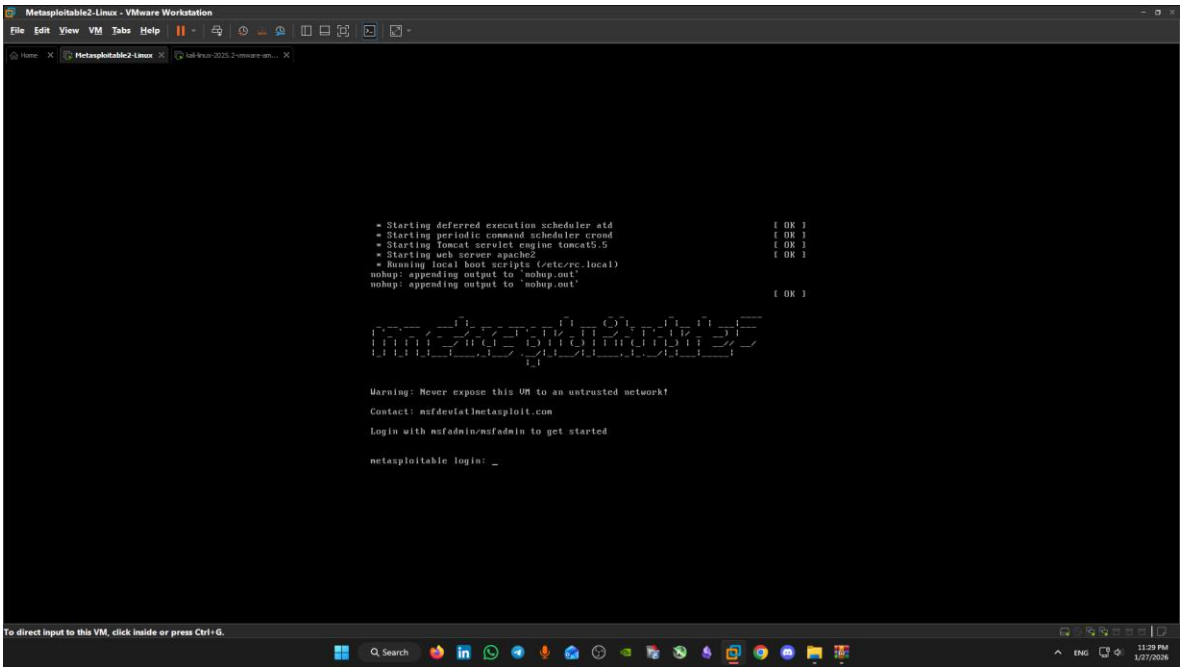
Portfolio : https://eng-ahmed-emad.github.io/AhmedEmad-Dev/

PostgreSQL Port : 5432

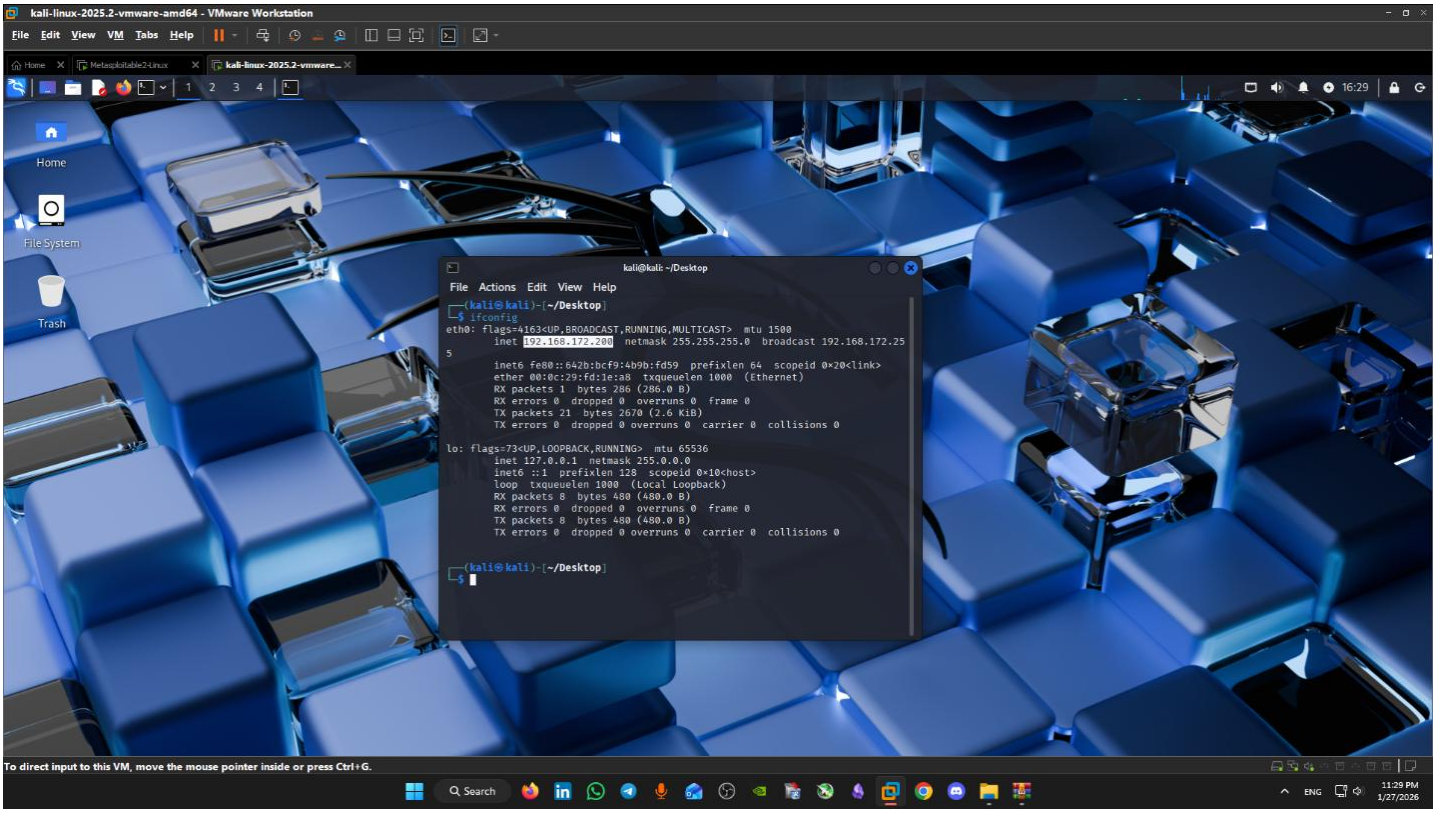
PostgreSQL is an open-source, object-relational database management system (ORDBMS) used to store and manage structured data.
It is widely adopted in enterprise and web applications due to its reliability, extensibility, and strong support for SQL standards.

First I Installed Kali Linux And Metasbolitable Machines





Second : I used **<u>ifconfig</u>** to know my ip and subnet (Target IP located: 192.168.172.129):



I Found Out It Was 192.168.172.0/24 so I used a simple <u>Nmap</u> Command On whole network and found out that machine has IP address of 192.168.172.129/24

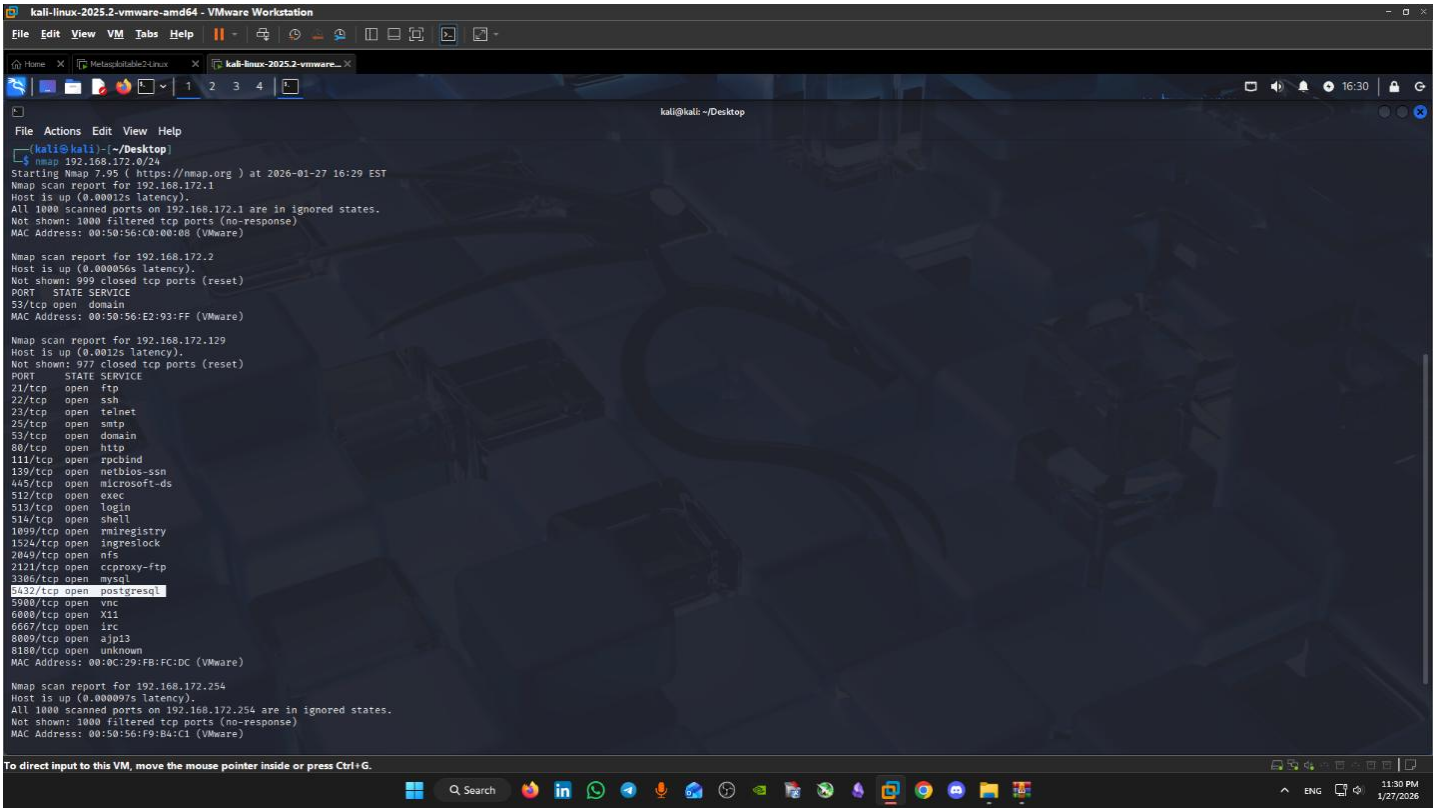
3. Port Scanning

Command:

Bash

nmap -p- 192.168.172.129

→ Port 5432 found open → service: postgresql



I found that the port I am curious about is open which is port **5432**

Fourth : I wanted to know the version so I used -A option which

4. Detailed Service & Version Fingerprinting

Command:

Bash

nmap -A -p 5432 192.168.172.129

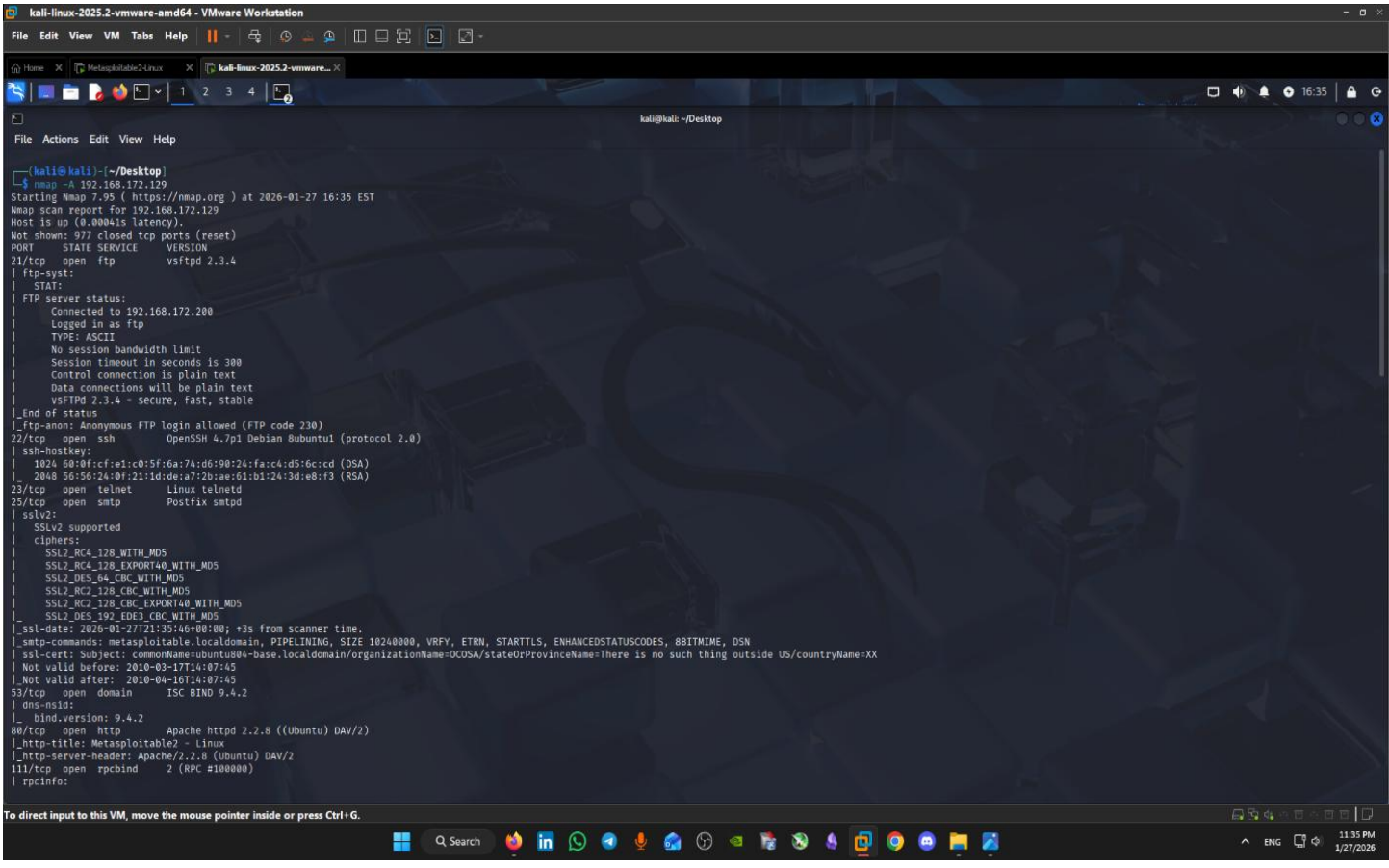
Result:

text

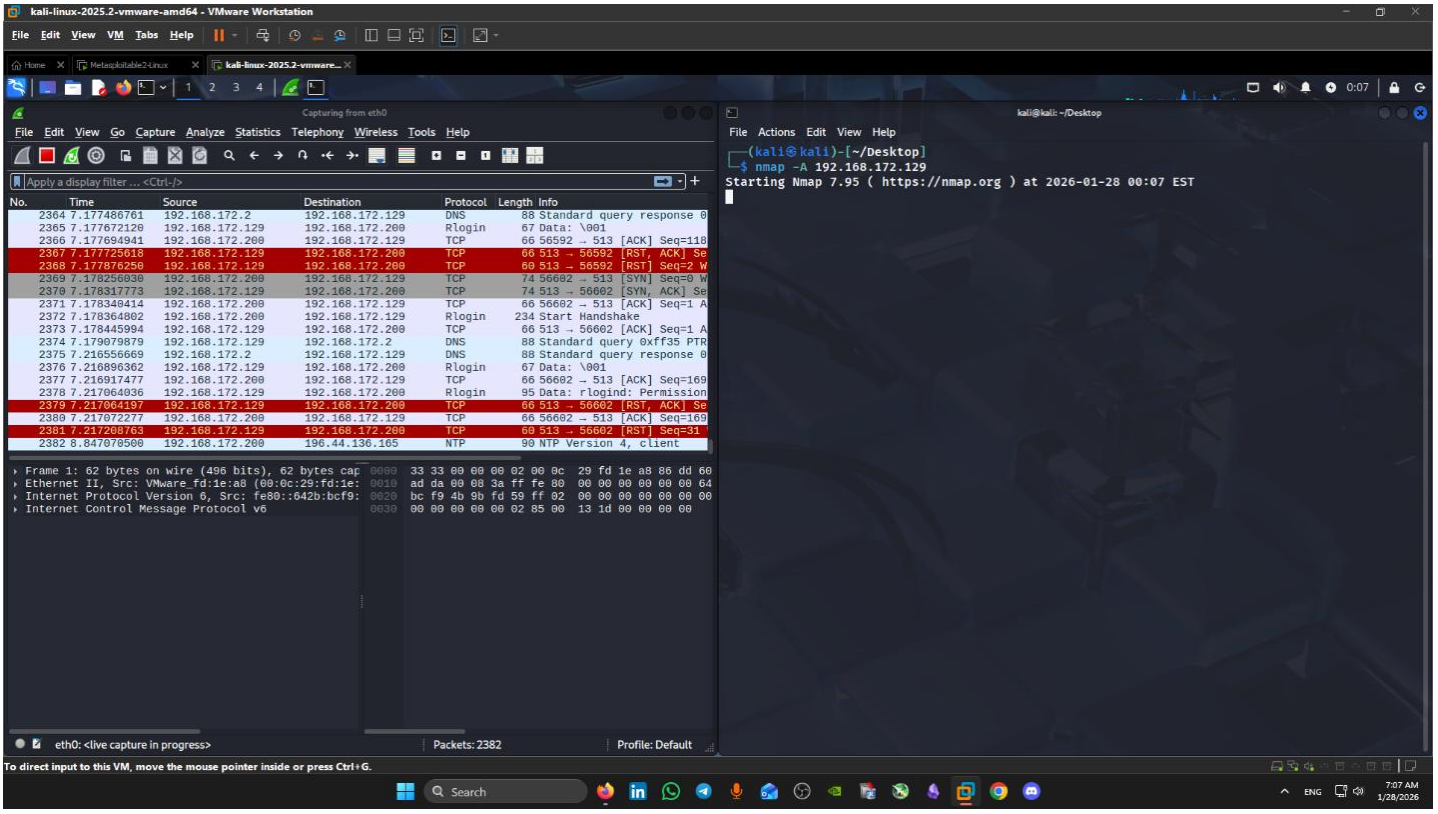
5432/tcp open postgresql PostgreSQL DB 8.3.0 - 8.3.7

Confirmed version: **PostgreSQL 8.3.0 – 8.3.7**

enables **aggressive scan mode**, which combines **OS detection, version detection, default scripts (NSE), and traceroute** in a single scan.



And this is how nmap scan appears in **Wireshark** which help me improve my Analysis Skills (Educational) 😊



I found out that the version is **PostgreSQL DB 8.3.0 - 8.3.7**

And I found 3 CVE's in NVD and and 1 in Exploit DB (CVE-2012-0868)

- **CVE-2012-0868**
- **CVE-2012-2655**
- **CVE-2010-4015**

NVD Report : https://nvd.nist.gov/vuln/detail/cve-2012-0868

VULNERABILITIES

CVE-2012-0868 Detail

DEFERRED

This CVE record is not being prioritized for NVD enrichment efforts due to resource or other concerns.

Description

CRLF injection vulnerability in pg_dump in PostgreSQL 8.3.x before 8.3.18, 8.4.x before 8.4.11, 9.0.x before 9.0.7, and 9.1.x before 9.1.3 allows user-assisted remote attackers to execute arbitrary SQL commands via a crafted file containing object names with newlines, which are inserted into an SQL script that is used when the database is restored.

QUICK INFO

CVE Dictionary Entry:
CVE-2012-0868
NVD Published Date:
07/18/2012
NVD Last Modified:
04/10/2025
Source:
Red Hat, Inc.

Metrics

CVSS Version 4.0 | CVSS Version 3.x | CVSS Version 2.0

NVD enrichment efforts reference publicly available information to associate vector strings. CVSS information contributed by other sources is also displayed.

CVSS 2.0 Severity and Vector Strings:

NIST: NVD **Base Score:** 6.8 MEDIUM **Vector:** (AV:N/AC:M/Au:N/C:P/I:P/A:P)

References to Advisories, Solutions, and Tools

By selecting these links, you will be leaving NIST webspace. We have provided these links to other web sites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other web sites that are more appropriate for your purpose. NIST does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, NIST does not endorse any commercial products that may be mentioned on these sites. Please address comments about this page to nvd@nist.gov.

6. Vulnerability Research

Searched National Vulnerability Database (NVD) and Exploit-DB for CVEs affecting PostgreSQL 8.3.x:

CVE ID	CVSS v2 Score	Vulnerability Type	Impact	Reference
CVE-2012-0868	6.8 (Medium)	SQL Injection via CRLF in pg_dump/restore	Arbitrary SQL execution during restore from crafted backup	https://nvd.nist.gov/vuln/detail/CVE-2012-0868
CVE-2012-2655	4.0 (Medium)	Denial of Service via SECURITY DEFINER functions	Authenticated users can crash the PostgreSQL server	NVD / PostgreSQL notes
CVE-2010-4015	6.5 (Medium)	Buffer overflow in intarray module (gettoken)	DoS + potential remote code execution (authenticated users)	NVD

VULNERABILITIES

CVE-2012-2655 Detail

DEFERRED

This CVE record is not being prioritized for NVD enrichment efforts due to resource or other concerns.

Description

PostgreSQL 8.3.x before 8.3.19, 8.4.x before 8.4.12, 9.0.x before 9.0.8, and 9.1.x before 9.1.4 allows remote authenticated users to cause a denial of service (server crash) by adding the (1) SECURITY DEFINER or (2) SET attributes to a procedural language's call handler.

Metrics

CVSS Version 4.0 | CVSS Version 3.x | CVSS Version 2.0

NVD enrichment efforts reference publicly available information to associate vector strings. CVSS information contributed by other sources is also displayed.

CVSS 2.0 Severity and Vector Strings:

NIST: NVD **Base Score:** 4.0 MEDIUM **Vector:** (AV:N/AC:L/Au:S/C:N/I:N/A:P)

References to Advisories, Solutions, and Tools

By selecting these links, you will be leaving NIST webspace. We have provided these links to other web sites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other web sites that are more appropriate for your purpose. NIST does not necessarily endorse the views expressed,

QUICK INFO

CVE Dictionary Entry:
CVE-2012-2655
NVD Published Date:
07/18/2012
NVD Last Modified:
04/10/2025
Source:
Red Hat, Inc.

Information Technology Laboratory
NATIONAL VULNERABILITY DATABASE
NIST NATIONAL VULNERABILITY DATABASE NVD

VULNERABILITIES

CVE-2010-4015 Detail

DEFERRED

This CVE record is not being prioritized for NVD enrichment efforts due to resource or other concerns.

Description

Buffer overflow in the gettoken function in contrib/intarray/_int_bool.c in the intarray array module in PostgreSQL 9.0.x before 9.0.3, 8.4.x before 8.4.7, 8.3.x before 8.3.14, and 8.2.x before 8.2.20 allows remote authenticated users to cause a denial of service (crash) and possibly execute arbitrary code via integers with a large number of digits to unspecified functions.

Metrics

CVSS Version 4.0 | CVSS Version 3.x | CVSS Version 2.0

NVD enrichment efforts reference publicly available information to associate vector strings. CVSS information contributed by other sources is also displayed.

CVSS 2.0 Severity and Vector Strings:

NIST: NVD **Base Score:** 6.5 MEDIUM **Vector:** (AV:N/AC:L/Au:S/C:P/I:P/A:P)

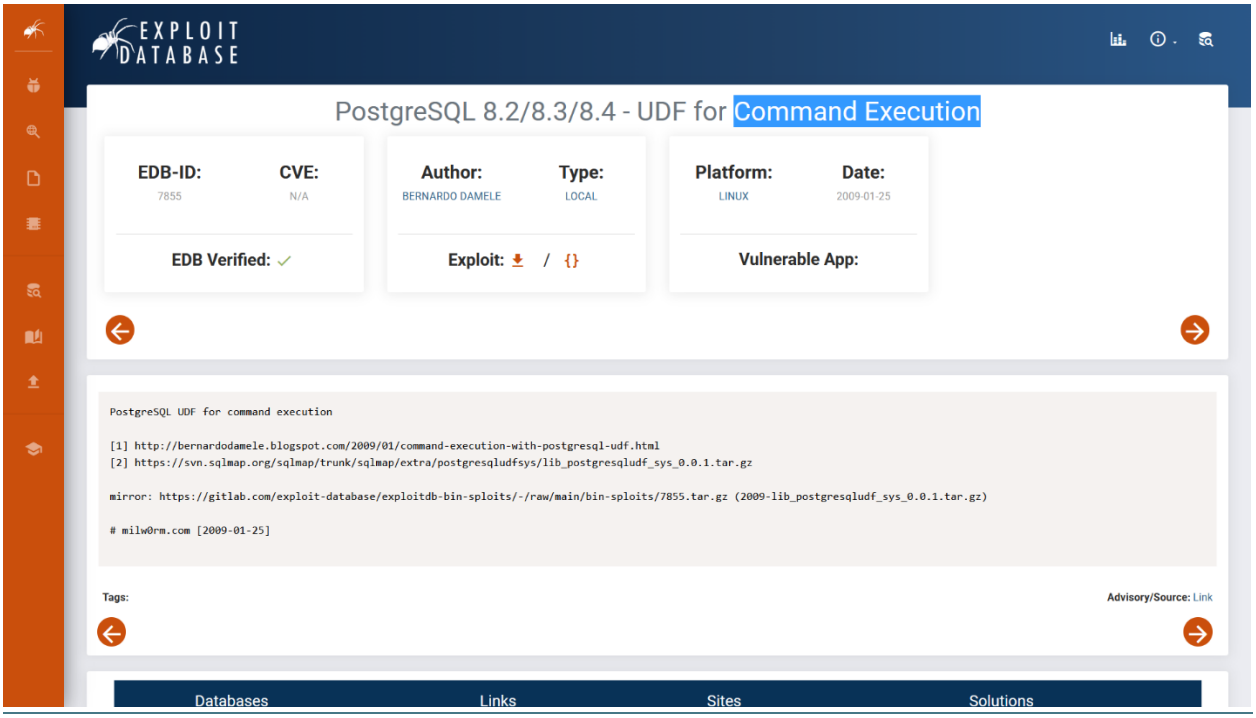
References to Advisories, Solutions, and Tools

By selecting these links, you will be leaving NIST webspace. We have provided these links to other web sites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this

QUICK INFO

CVE Dictionary Entry:
CVE-2010-4015
NVD Published Date:
02/01/2011
NVD Last Modified:
04/10/2025
Source:
Apple Inc.

ExploitDB : https://www.exploit-db.com/exploits/7855



Vulnerability Summary

CVE ID: CVE-2012-0868
Severity: Medium (CVSS v2.0: 6.8)
Type: SQL Injection via CRLF/Newline injection during backup restore
Impact: Execution of arbitrary SQL commands during the database restore process

CVE ID: CVE-2012-2655
Severity: Medium (CVSS v2.0: 4.0)
Type: Denial of Service due to improper handling of SECURITY DEFINER/SET in procedural language call handlers
Impact: Remote authenticated users can crash the PostgreSQL server, causing a denial of service

CVE ID: CVE-2010-4015
Severity: Medium (CVSS v2.0: 6.5)

Type: Buffer overflow in PostgreSQL intarray module (gettoken function)
Impact: Remote authenticated users can cause a denial of service and potentially execute arbitrary code

Additional Exploit Reference: Exploit-DB 7855 – PostgreSQL UDF code execution https://www.exploit-db.com/exploits/7855

Critical Note: PostgreSQL 8.3 branch is **End-of-Life** since 2013 → no security updates → highly vulnerable when network-accessible.

Conclusion

- Successfully identified PostgreSQL 8.3.0–8.3.7 on port 5432.
- Located multiple medium-severity vulnerabilities exploitable due to outdated software.
- Demonstrated complete reconnaissance workflow: network discovery → port scan → version detection → vulnerability enumeration.
-

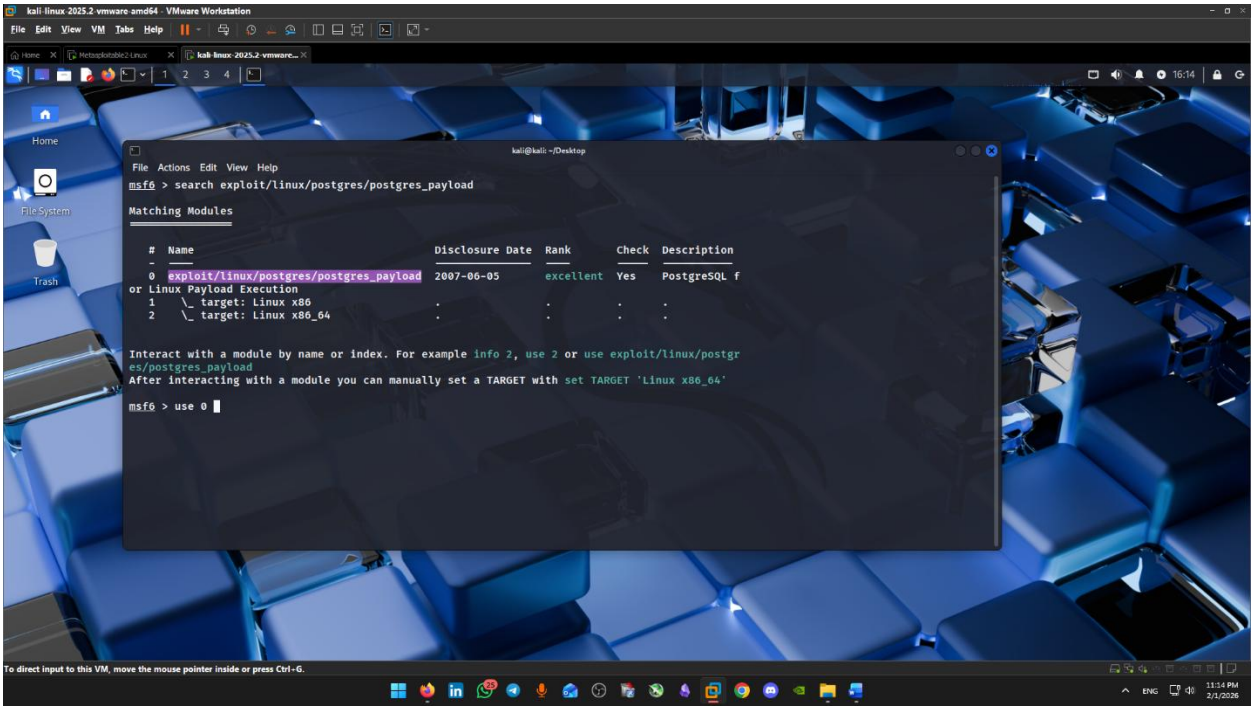
Tools & Resources Used

- ifconfig
- Nmap (-sn, -p-, -A)
- Wireshark
- NVD
- Exploit-DB
-

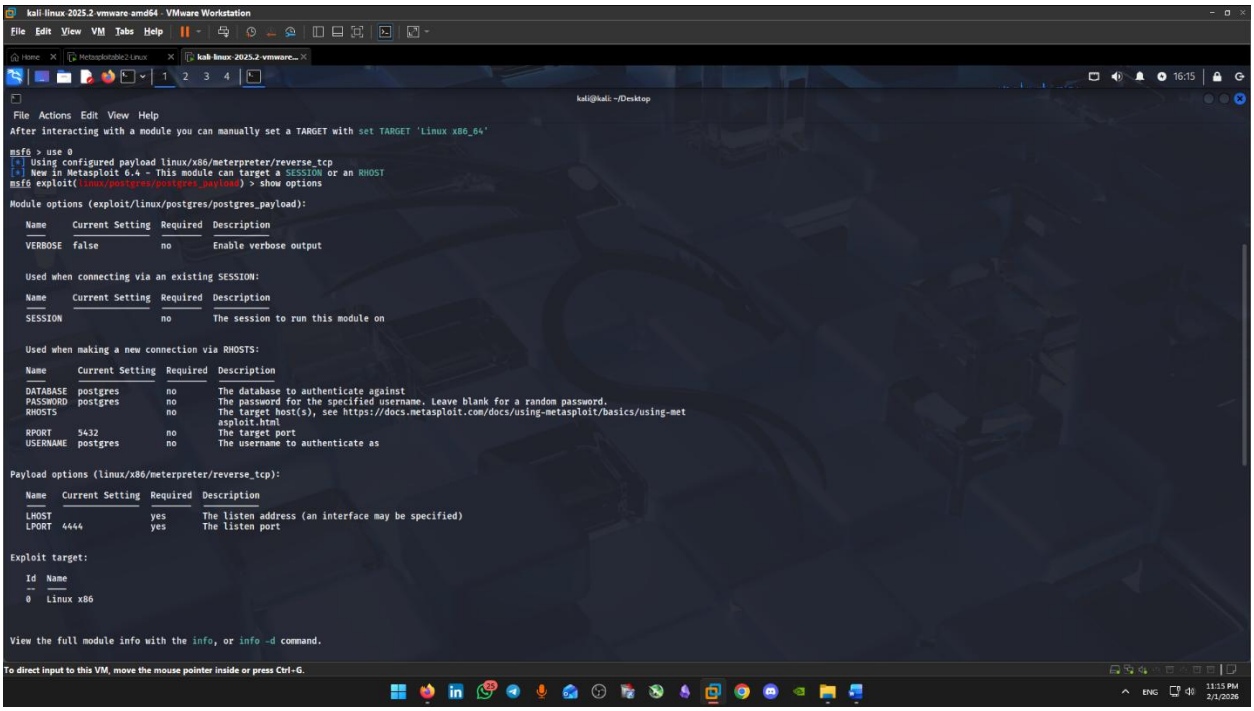
Prepared by: Ahmed Emad Eldeen Abdelmoneam
Benha – January 2026

NOW LETS EXPLOIIIIITTTTTTTTTTTTT 😊
First I used msfconsole command to open Metasploit

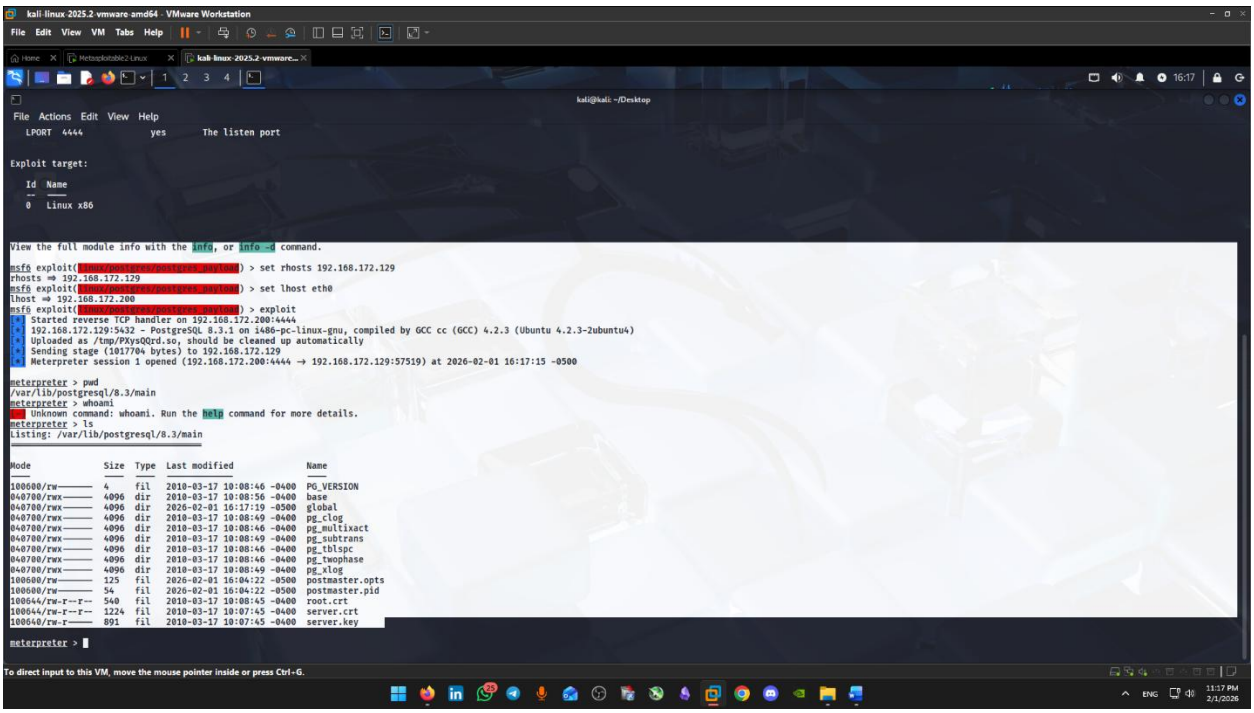
Second I searched for **PostgreSQL 8.3.0 – 8.3.7 modules using SEARCH command and I found the exact one I want and used USE (exploit/linux/postgres/postgres_payload)**



now I used SHOW OPTIONS command and I set RHOSTS to the target machine which is 192.168.172.129 and LHOSTS to ETH0



So All Things Now Are Ready I Used ***EXPLOIT*** command To Start Exploitation and It Succeesed and Opened A Reverse Shell And Now All Done 😊



How the Exploit Works

The exploit/linux/postgres/postgres_payload module exploits a vulnerability in PostgreSQL versions 8.3.0 through 8.3.7. Here's the technical breakdown of the exploitation process:

Exploitation Mechanism:

1. Vulnerability Identification

- The exploit targets a security weakness in PostgreSQL's pl/pgsql procedural language
- Affected versions: PostgreSQL 8.3.0 - 8.3.7
- The vulnerability allows arbitrary code execution through database functions

2. Payload Delivery

- Metasploit connects to the PostgreSQL service (default port 5432)
- Creates a malicious stored procedure using pl/pgsql
- The procedure contains the payload (reverse shell code)
- Executes the stored procedure to trigger the exploit

3. Reverse Shell Establishment

- Once executed, the payload initiates an outbound connection from the target server to the attacker's machine (LHOST)
- This is called a "reverse" shell because the target connects back to the attacker
- The connection bypasses most firewall rules since it's an outbound connection
- Upon successful connection, a command shell is established

4. Post-Exploitation Access

- The attacker gains interactive command-line access to the target system
- Commands can be executed with the privileges of the PostgreSQL service account
- Full system control may be achieved depending on the service account permissions

Why Reverse Shell?

A reverse shell is preferred in penetration testing because:

- Outbound connections are typically less restricted by firewalls
- NAT and firewall traversal is easier
- More reliable in real-world network environments