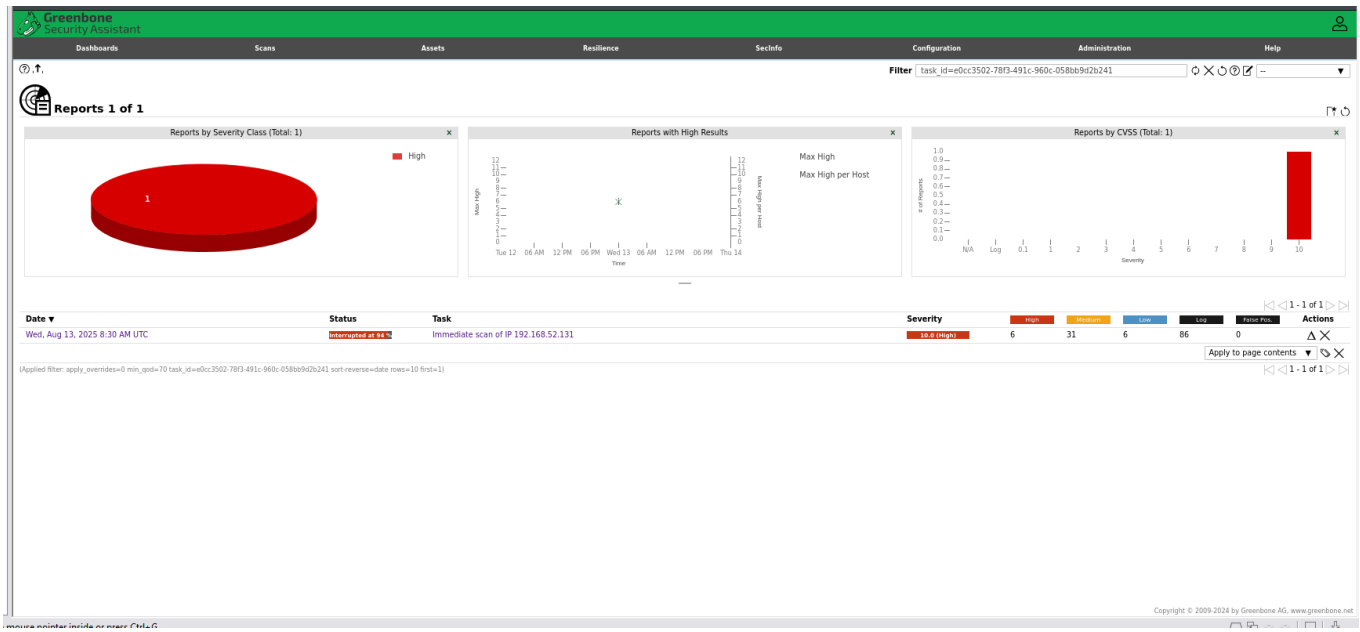
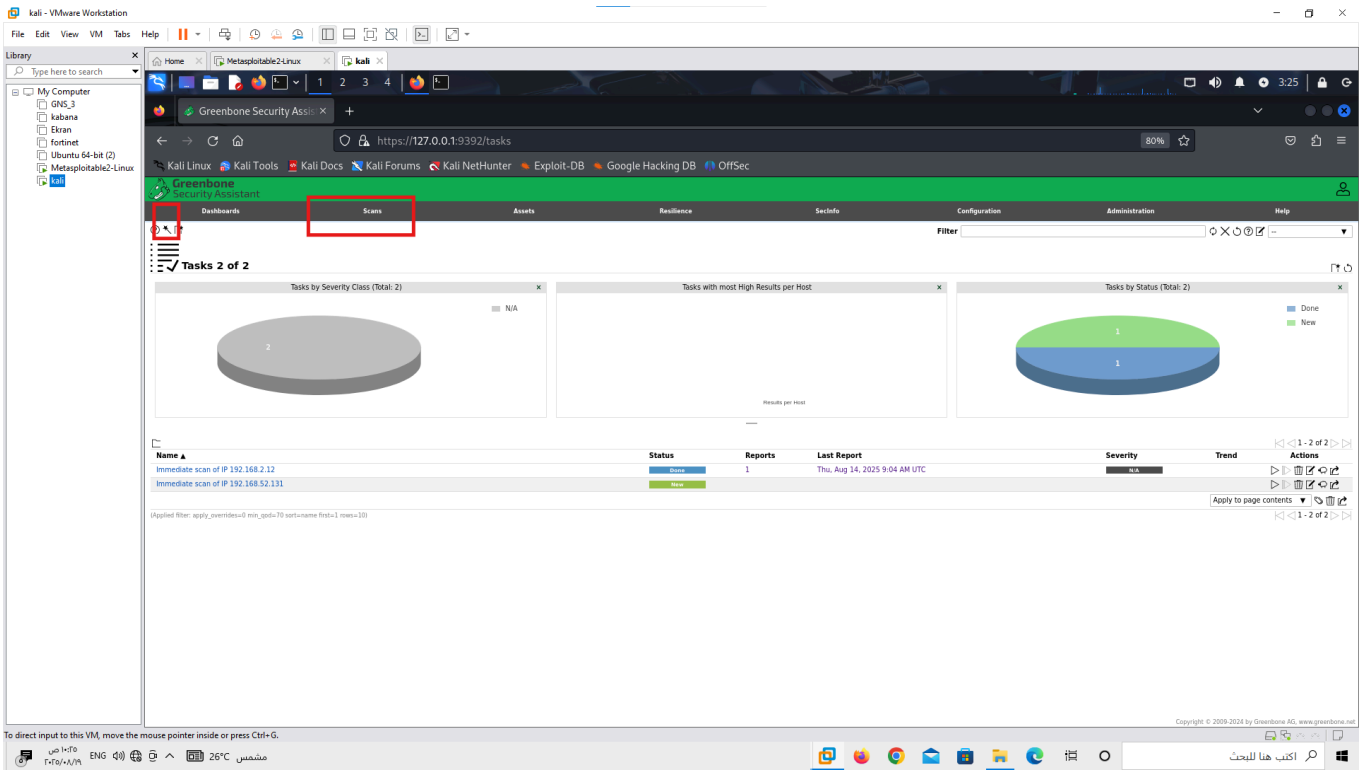
هنا استخدمنا اداة (OpenVAS) وهي تعمل على تحليل الانظمة للتعرف على انواع الثغرات والتهديدات الموجودة على النظام والبورتات المفتوحه ومالى ذالك.

1-الطرثقة الاولى:الدخول للاداة عبر المتصفح عبر البورت (localhost 9392).

هذه الواجه الرئيسية ال (dashboards)للاداة

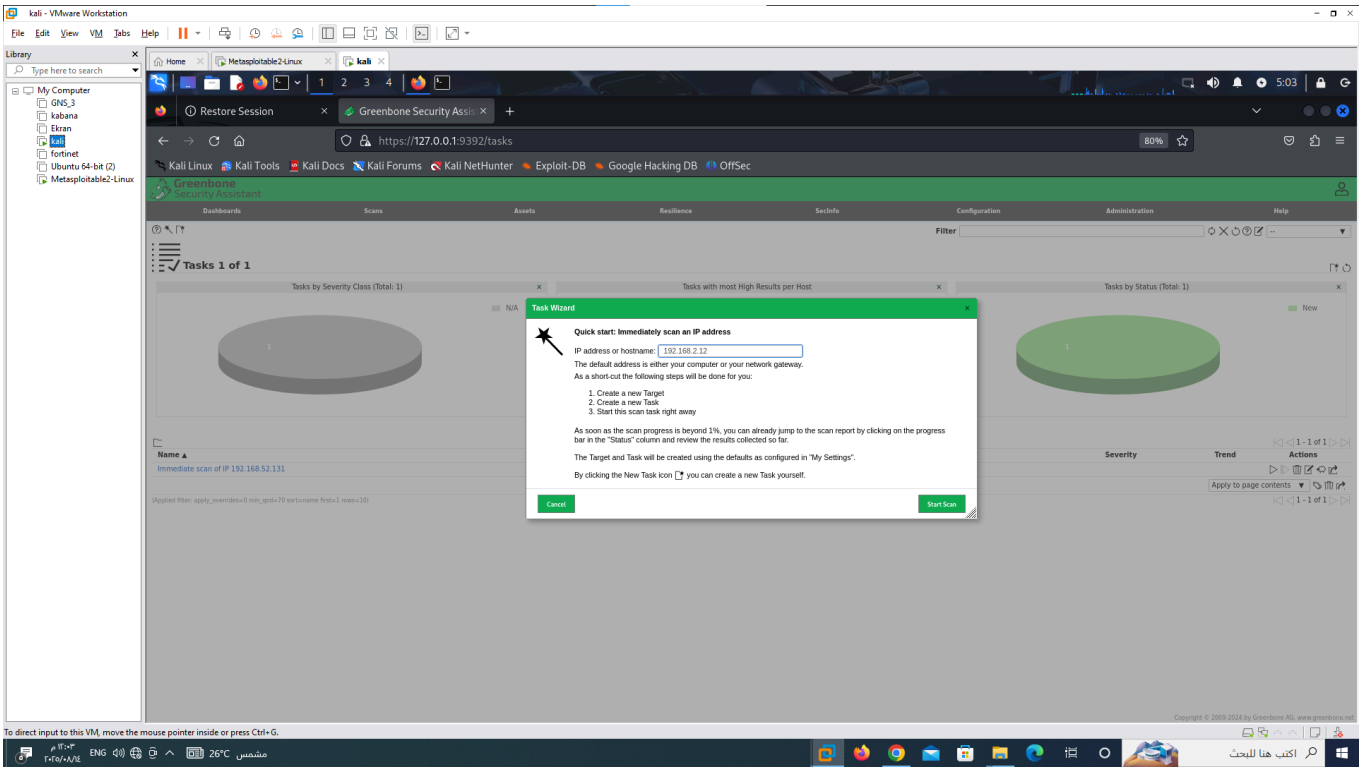


2-الطريقة الثانية :انشئ مهمة جديدة من خلال الضغط على (scan) ثم الضغط على السهم المشار اليه



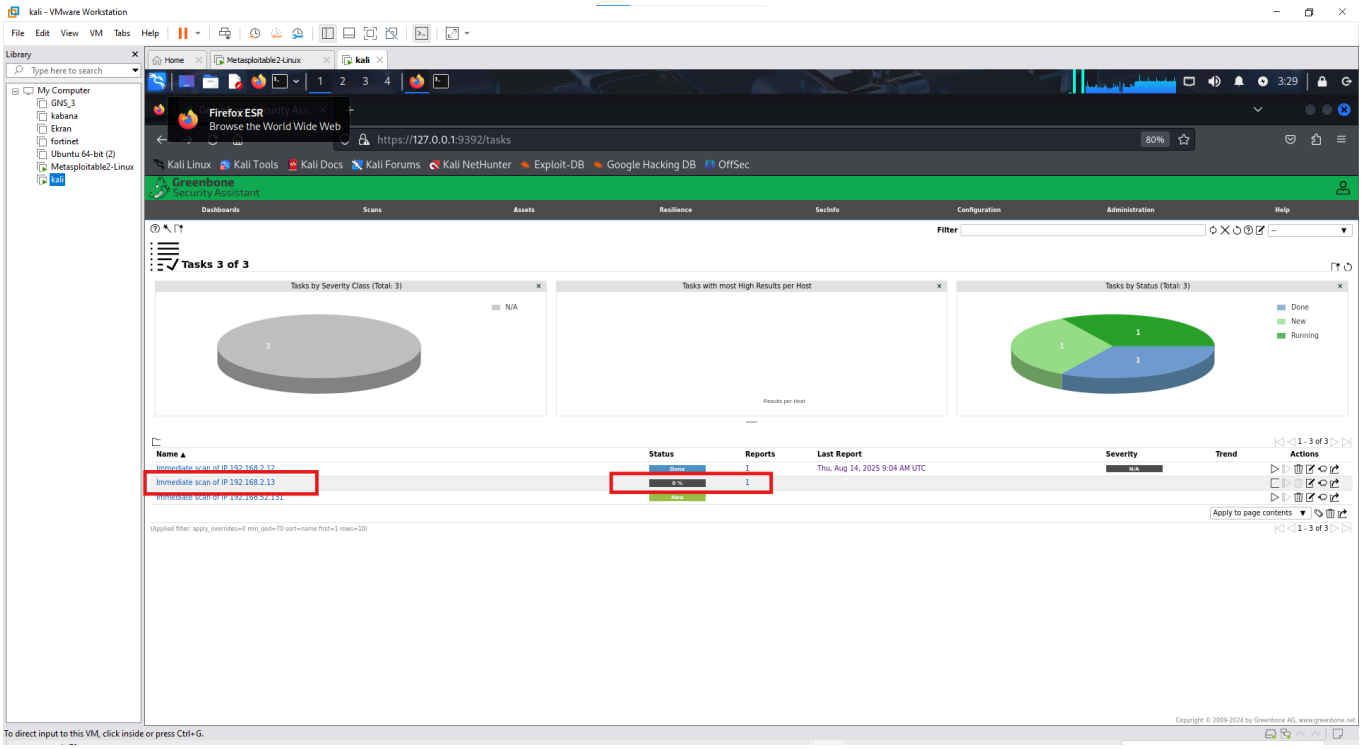
3-الطريقة الثالثة:

ادخل العنوان تبع الظام الذي تريد فحصة



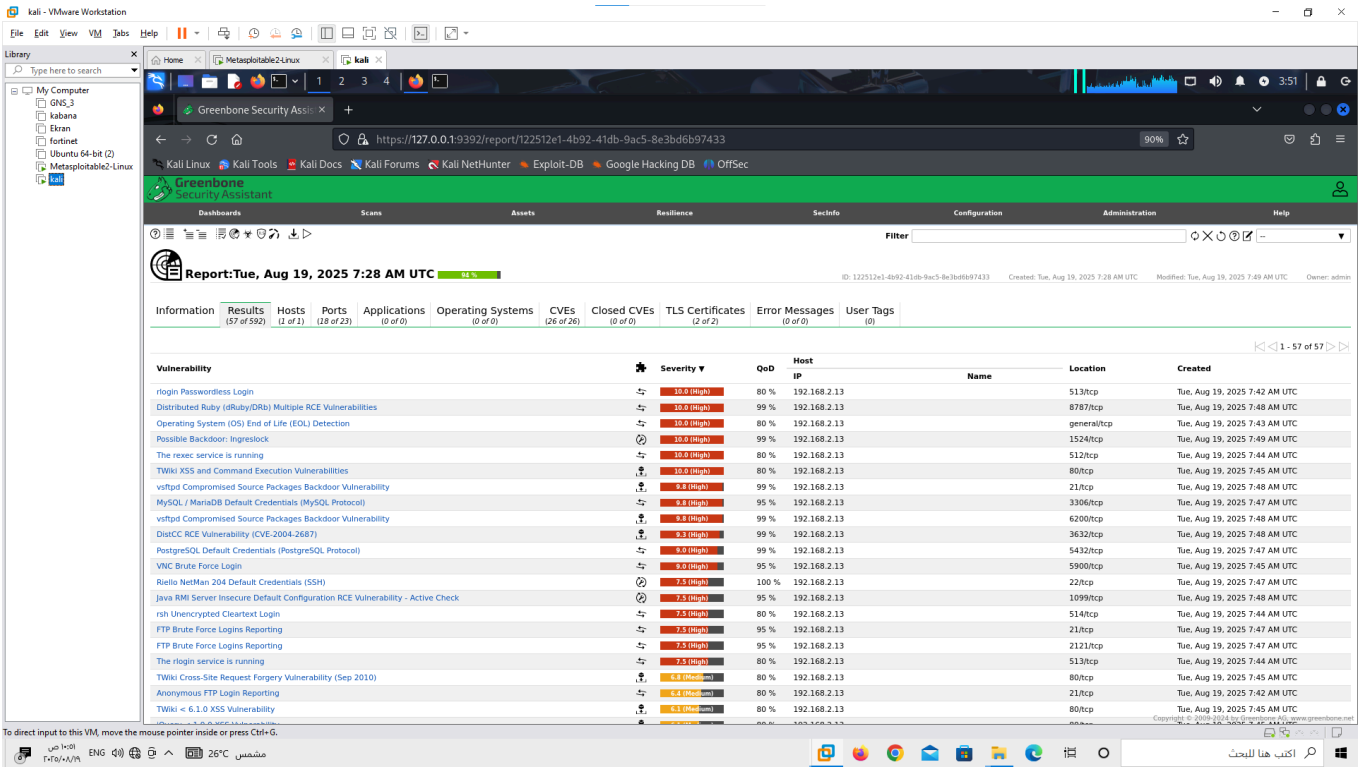
4-الطريقة الرابعة:

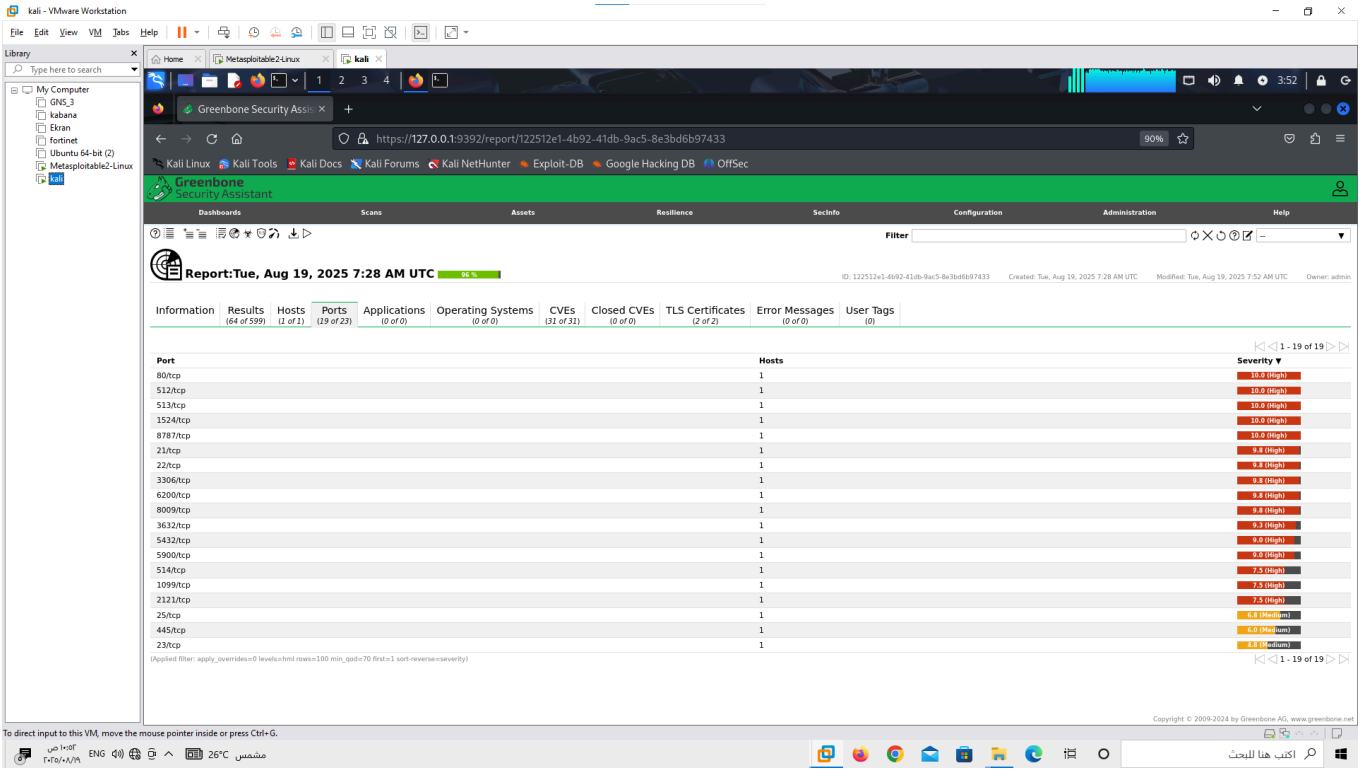
هنا يظهر عنوان النظام الذي قمنا بتحديدة ومقابله عداد الفحص المشار اليه بالصوره ادناه

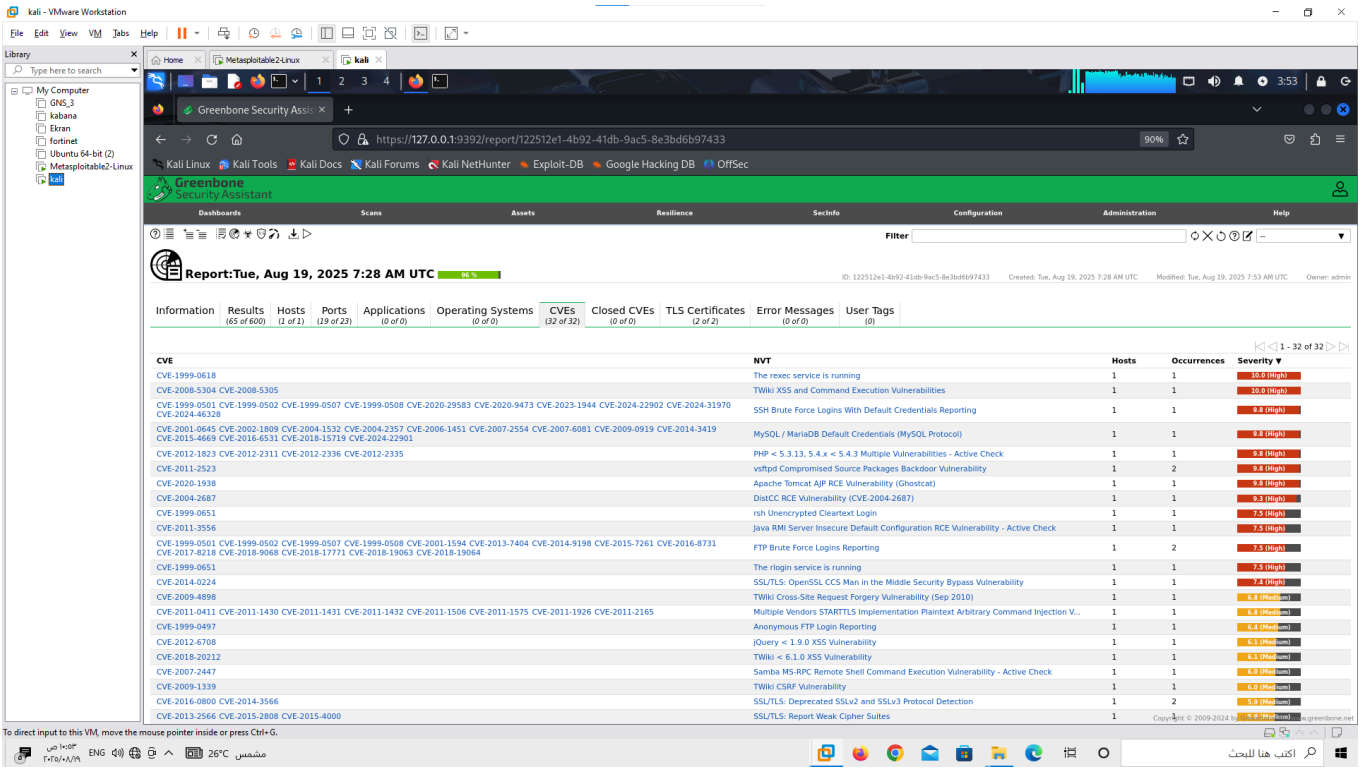


5-الطريقة الخامسة:

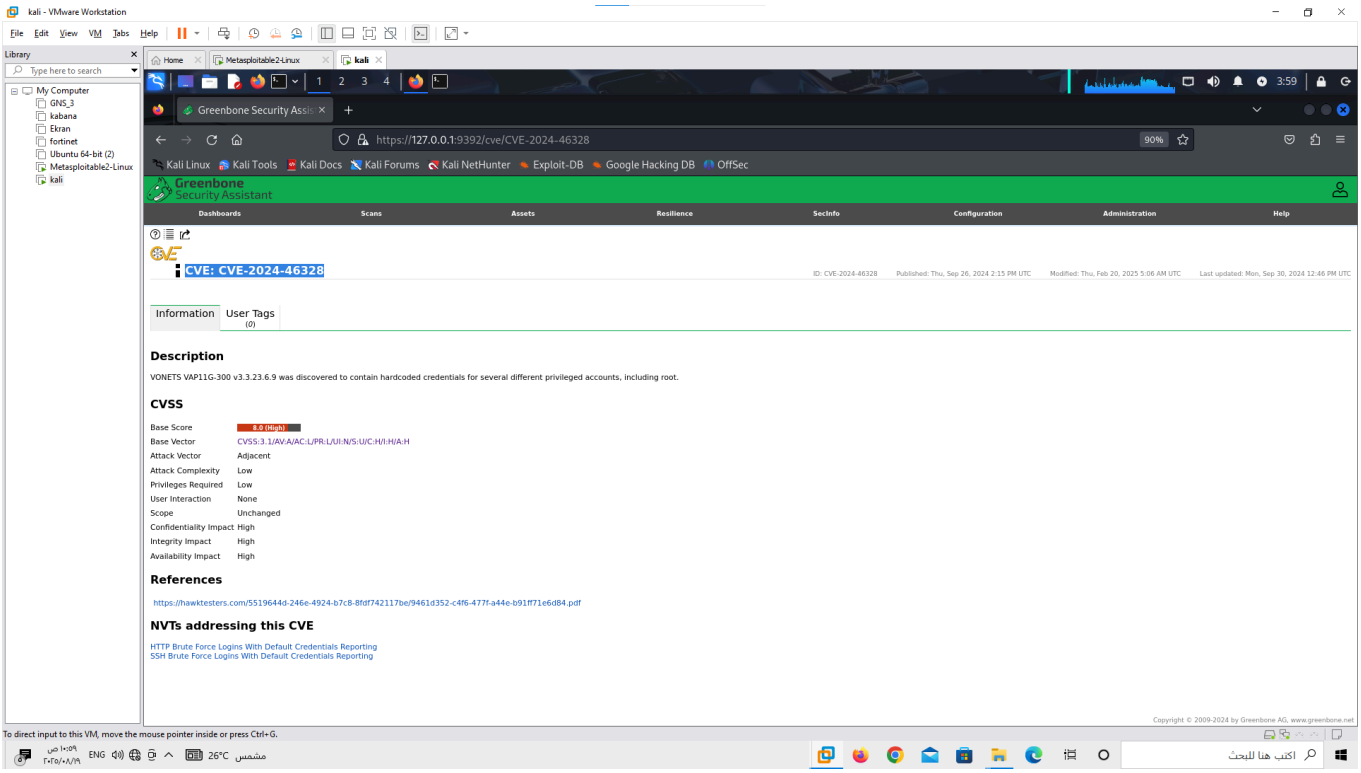
هذه نتائج الفحص من ثغرات ومن بورتات وانواع اخرى تدل على تهديدات في النظام

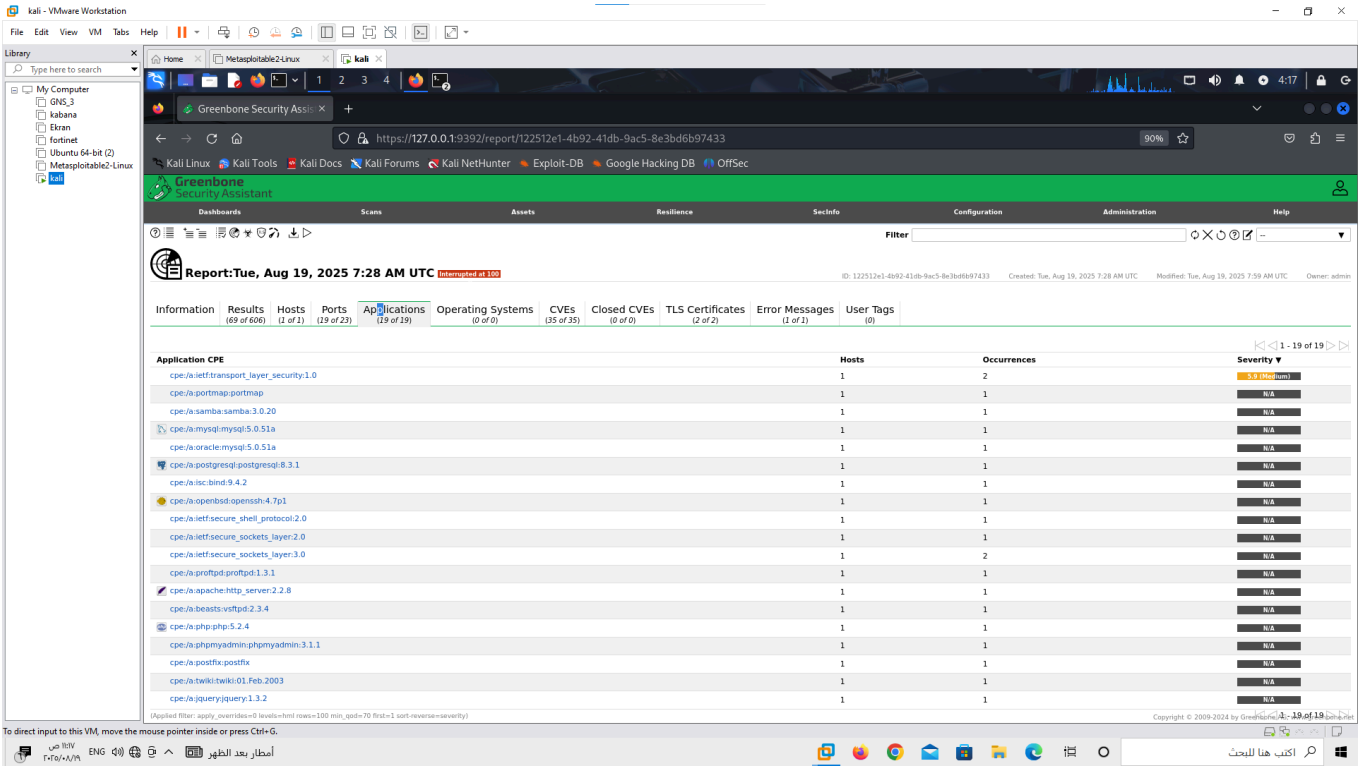

kali - VMware Workstation
https://127.0.0.1:9392/report/122512e1-4b92-41db-9ac5-8e3bd6b97433
Greenbone Security Assistant
Report:Tue, Aug 19, 2025 7:28 AM UTC
Information Results (57 of 592) Hosts (1 of 1) Ports (18 of 23) Applications (0 of 0) Operating Systems (0 of 0) CVEs (26 of 26) Closed CVEs (0 of 0) TLS Certificates (2 of 2) Error Messages (0 of 0) User Tags (0)
1 - 57 of 57
Vulnerability | Severity | QoD | Host IP | Name | Location | Created
rlogin Passwordless Login | 10.0 (High) | 80 % | 192.168.2.13 | 513/tcp | Tue, Aug 19, 2025 7:42 AM UTC
Distributed Ruby (dRuby/DRb) Multiple RCE Vulnerabilities | 10.0 (High) | 99 % | 192.168.2.13 | 8787/tcp | Tue, Aug 19, 2025 7:48 AM UTC
Operating System (OS) End of Life (EOL) Detection | 10.0 (High) | 80 % | 192.168.2.13 | general/tcp | Tue, Aug 19, 2025 7:43 AM UTC
Possible Backdoor: Ingreslock | 10.0 (High) | 99 % | 192.168.2.13 | 1524/tcp | Tue, Aug 19, 2025 7:49 AM UTC
The rexec service is running | 10.0 (High) | 80 % | 192.168.2.13 | 512/tcp | Tue, Aug 19, 2025 7:44 AM UTC
TWiki XSS and Command Execution Vulnerabilities | 10.0 (High) | 80 % | 192.168.2.13 | 80/tcp | Tue, Aug 19, 2025 7:45 AM UTC
vsftpd Compromised Source Packages Backdoor Vulnerability | 9.8 (High) | 99 % | 192.168.2.13 | 21/tcp | Tue, Aug 19, 2025 7:48 AM UTC
MySQL / MariaDB Default Credentials (MySQL Protocol) | 9.8 (High) | 95 % | 192.168.2.13 | 3306/tcp | Tue, Aug 19, 2025 7:47 AM UTC
vsftpd Compromised Source Packages Backdoor Vulnerability | 9.8 (High) | 99 % | 192.168.2.13 | 6200/tcp | Tue, Aug 19, 2025 7:48 AM UTC
DistCC RCE Vulnerability (CVE-2004-2687) | 9.3 (High) | 99 % | 192.168.2.13 | 3632/tcp | Tue, Aug 19, 2025 7:48 AM UTC
PostgreSQL Default Credentials (PostgreSQL Protocol) | 9.0 (High) | 99 % | 192.168.2.13 | 5432/tcp | Tue, Aug 19, 2025 7:47 AM UTC
VNC Brute Force Login | 9.0 (High) | 95 % | 192.168.2.13 | 5900/tcp | Tue, Aug 19, 2025 7:45 AM UTC
Rlello NetMan 204 Default Credentials (SSH) | 7.5 (High) | 100 % | 192.168.2.13 | 22/tcp | Tue, Aug 19, 2025 7:47 AM UTC
Java RMI Server Insecure Default Configuration RCE Vulnerability - Active Check | 7.5 (High) | 95 % | 192.168.2.13 | 1099/tcp | Tue, Aug 19, 2025 7:48 AM UTC
rsh Unencrypted Cleartext Login | 7.5 (High) | 80 % | 192.168.2.13 | 514/tcp | Tue, Aug 19, 2025 7:44 AM UTC
FTP Brute Force Logins Reporting | 7.5 (High) | 95 % | 192.168.2.13 | 21/tcp | Tue, Aug 19, 2025 7:47 AM UTC
FTP Brute Force Logins Reporting | 7.5 (High) | 95 % | 192.168.2.13 | 2121/tcp | Tue, Aug 19, 2025 7:47 AM UTC
The rlogin service is running | 7.5 (High) | 80 % | 192.168.2.13 | 513/tcp | Tue, Aug 19, 2025 7:44 AM UTC
TWiki Cross-Site Request Forgery Vulnerability (Sep 2010) | 6.8 (Medium) | 80 % | 192.168.2.13 | 80/tcp | Tue, Aug 19, 2025 7:45 AM UTC
Anonymous FTP Login Reporting | 6.4 (Medium) | 80 % | 192.168.2.13 | 21/tcp | Tue, Aug 19, 2025 7:42 AM UTC
TWiki < 6.1.0 XSS Vulnerability | 6.1 (Medium) | 80 % | 192.168.2.13 | 80/tcp | Tue, Aug 19, 2025 7:45 AM UTC
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.


kali - VMware Workstation
https://127.0.0.1:9392/report/122512e1-4b92-41db-9ac5-8e3bd6b97433
Greenbone Security Assistant
Report:Tue, Aug 19, 2025 7:28 AM UTC
Information Results (64 of 599) Hosts (1 of 1) Ports (19 of 23) Applications (0 of 0) Operating Systems (0 of 0) CVEs (31 of 31) Closed CVEs (0 of 0) TLS Certificates (2 of 2) Error Messages (0 of 0) User Tags (0)
1 - 19 of 19
Port | Hosts | Severity
80/tcp | 1 | 10.0 (High)
512/tcp | 1 | 10.0 (High)
513/tcp | 1 | 10.0 (High)
1524/tcp | 1 | 10.0 (High)
8787/tcp | 1 | 10.0 (High)
21/tcp | 1 | 9.8 (High)
22/tcp | 1 | 9.8 (High)
3306/tcp | 1 | 9.8 (High)
6200/tcp | 1 | 9.8 (High)
8009/tcp | 1 | 9.8 (High)
3632/tcp | 1 | 9.3 (High)
5432/tcp | 1 | 9.0 (High)
5900/tcp | 1 | 9.0 (High)
514/tcp | 1 | 7.5 (High)
1099/tcp | 1 | 7.5 (High)
2121/tcp | 1 | 7.5 (High)
25/tcp | 1 | 6.8 (Medium)
445/tcp | 1 | 6.0 (Medium)
23/tcp | 1 | 4.8 (Medium)
(Applied filter: apply_overrides=0 levels=hml rows=100 min_qod=70 first=1 sort-reverse=severity)
1 - 19 of 19
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.



هذه تفاصيل حول ثغرة معينة من الثغرات الموجودة على النظام




kali - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
GNS_3
kabana
Ekran
fortinet
Ubuntu 64-bit (2)
Metasploitable2-Linux
kali
Home
Metasploitable2-Linux
kali
Greenbone Security Assis
https://127.0.0.1:9392/report/122512e1-4b92-41db-9ac5-8e3bd6b97433
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
Greenbone Security Assistant
Dashboards Scans Assets Resilience SecInfo Configuration Administration Help
Filter
Report:Tue, Aug 19, 2025 7:28 AM UTC Interrupted at 100
Information Results (69 of 606) Hosts (1 of 1) Ports (19 of 23) Applications (19 of 19) Operating Systems (0 of 0) CVEs (35 of 35) Closed CVEs (0 of 0) TLS Certificates (2 of 2) Error Messages (1 of 1) User Tags (0)
1 - 19 of 19
Application CPE Hosts Occurrences Severity
cpe:/a:ietf:transport_layer_security:1.0 1 2 5.9 (Medium)
cpe:/a:portmap:portmap 1 1 N/A
cpe:/a:samba:samba:3.0.20 1 1 N/A
cpe:/a:mysql:mysql:5.0.51a 1 1 N/A
cpe:/a:oracle:mysql:5.0.51a 1 1 N/A
cpe:/a:postgresql:postgresql:8.3.1 1 1 N/A
cpe:/a:isc:bind:9.4.2 1 1 N/A
cpe:/a:openbsd:openssh:4.7p1 1 1 N/A
cpe:/a:ietf:secure_shell_protocol:2.0 1 1 N/A
cpe:/a:ietf:secure_sockets_layer:2.0 1 1 N/A
cpe:/a:ietf:secure_sockets_layer:3.0 1 2 N/A
cpe:/a:proftpd:proftpd:1.3.1 1 1 N/A
cpe:/a:apache:http_server:2.2.8 1 1 N/A
cpe:/a:beasts:vsftpd:2.3.4 1 1 N/A
cpe:/a:php:php:5.2.4 1 1 N/A
cpe:/a:phpmyadmin:phpmyadmin:3.1.1 1 1 N/A
cpe:/a:postfix:postfix 1 1 N/A
cpe:/a:twiki:twiki:01.Feb.2003 1 1 N/A
cpe:/a:jquery:jquery:1.3.2 1 1 N/A
1 - 19 of 19
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
أمطار بعد الظهر
ENG
اكتب هنا للبحث