Phase 2: Scanning & Enumeration Report

1. Objective

The primary objective of scanning and enumeration is to gather detailed information about target systems,networks,open ports and running services to identify potential vulnerabilities, understand the attack surface, and assess security posture.

2. Process Flow :

- Scanning : Initial phase to discover targets,open ports,services.

- Enumeration: Deeper dive to gather specifics about identified elements.

- Analysis: Assess findings for vulnerabilities and exploitation.

3. Tools Used

- Nmap
- Netcat
- Enum4linux
- SNMPwalk
- Nikto
- Dirb

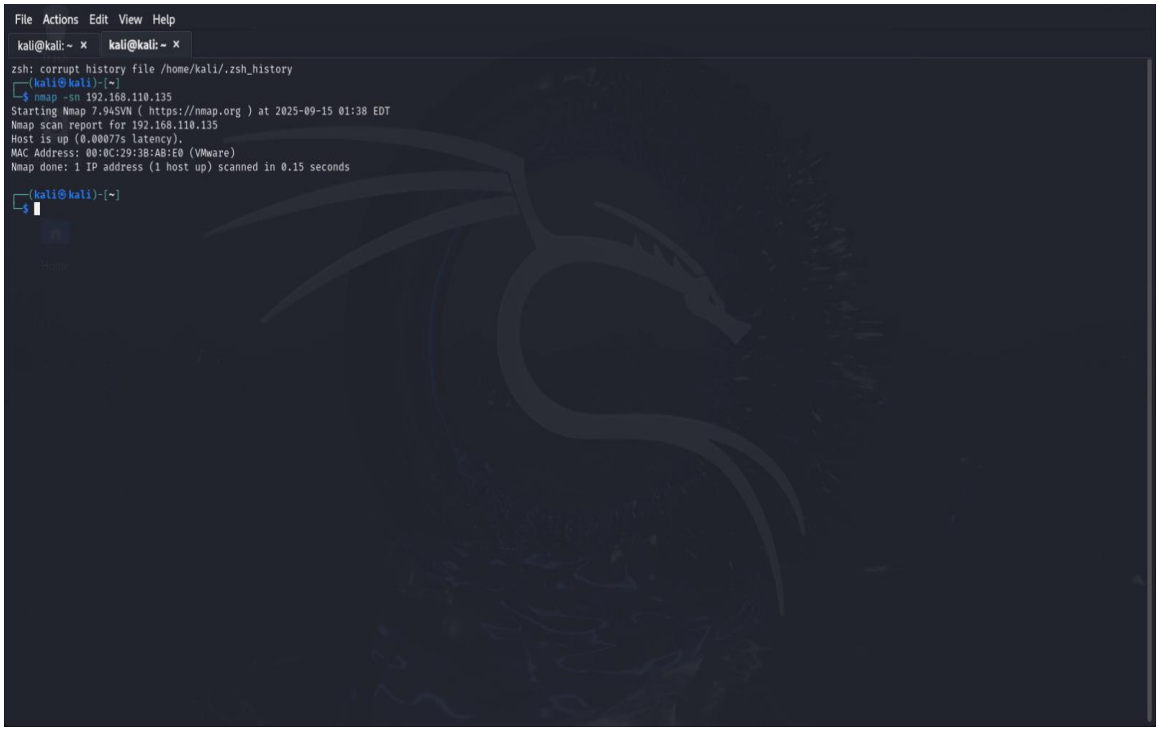
4. Target IP

Example: 192.168.110.135(Metasploitable2 IP)

5. Host Discovery

We performed a host discovery scan using Nmap with the -sn flag to identify live hosts within the local subnet. This type of scan sends ICMP echo requests and ARP packets (on LAN) to detect which machines are active. The scan confirmed the presence of the target system (Metasploitable2), which will be used for further enumeration.

Command:
nmap -sn 192.168.110.135



6.Port Scanning (TCP SYN Scan)

A full TCP SYN scan was conducted using nmap -sS -p-, which scans all 65,535 TCP ports. This helps identify which services are accessible externally. Multiple open ports such as 21 (FTP), 22 (SSH), 23 (Telnet), 80 (HTTP), and 445 (SMB) were discovered. These ports indicate available attack surfaces.

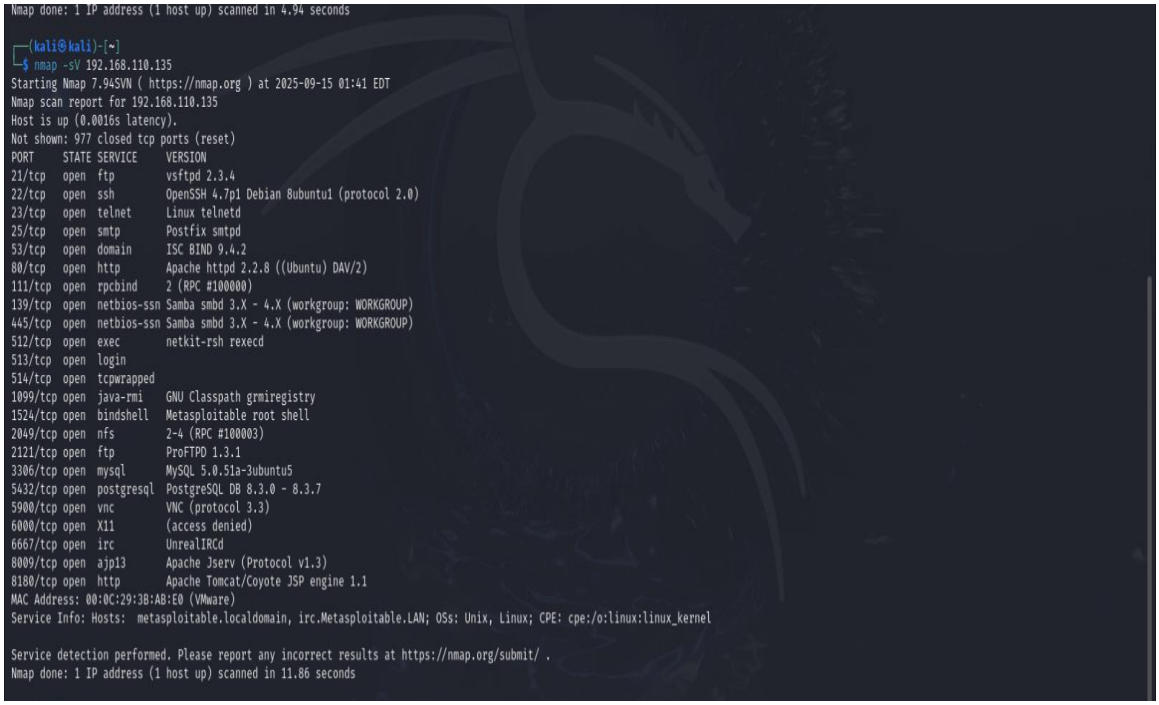
Command :

nmap -sS -p- 192.168.110.135

7. Service Version Detection

Using nmap -sV, we scanned the open ports to detect running services and their version numbers. This information is critical in identifying known vulnerabilities in outdated software. Services such as Apache 2.2.8, OpenSSH 4.7p1, and vsftpd 2.3.4 were discovered, which are known to be vulnerable in specific configurations.

Command:
nmap -sV 192.168.110.135



8. OS Detection

The nmap -O flag was used to perform OS fingerprinting. This technique analyzes TCP/IP stack behavior to determine the operating system of the target. The result indicated that the machine is running a Linux-based OS, specifically Ubuntu, which matches with the known configuration of Metasploitable2.

Command:
nmap -O 192.168.110.135

9. Banner Grabbing

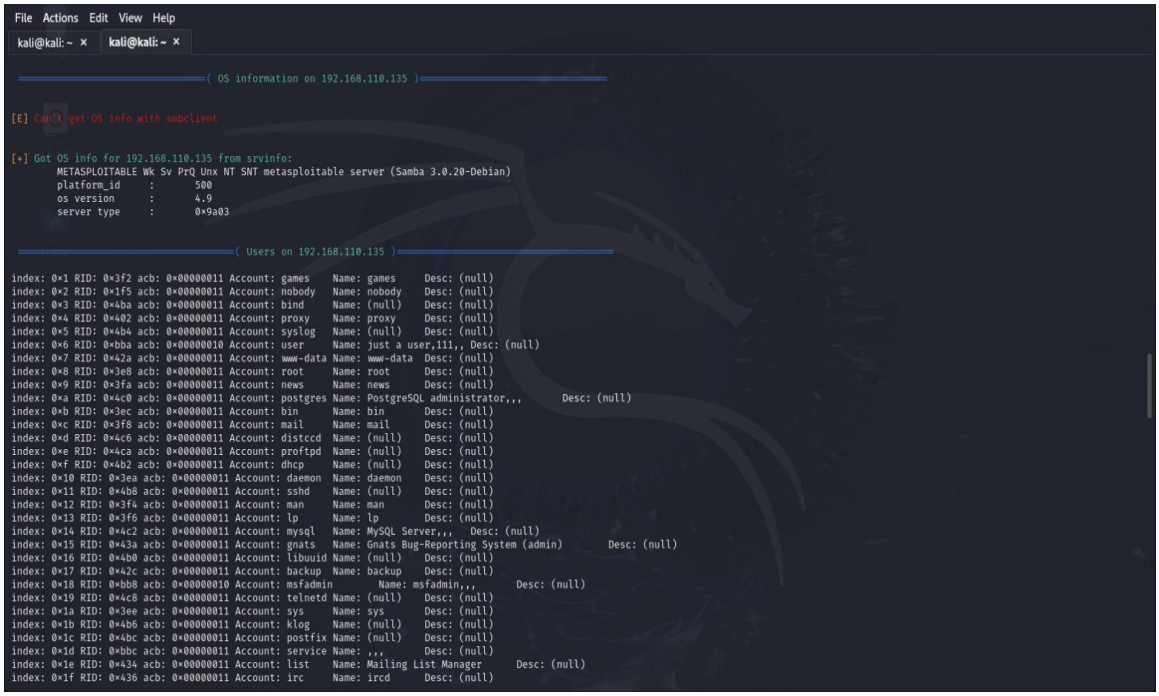
We connected to the target's HTTP service on port 80 using Netcat and manually sent a HEAD / HTTP/1.0 request. The server responded with an HTML error message that included a banner disclosing the web server's details. The banner revealed that Apache 2.2.8 is running on Ubuntu, confirming the software and environment.

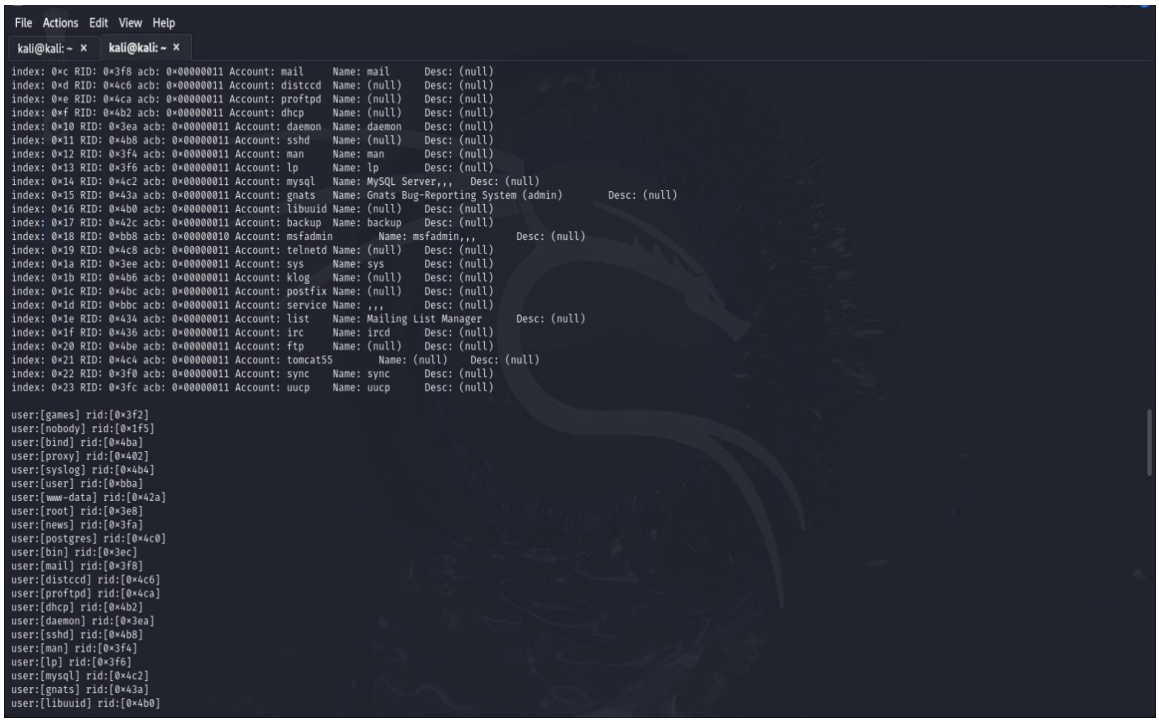
Command:
nc 192.168.110.135
Then type:
HEAD / HTTP/1.0

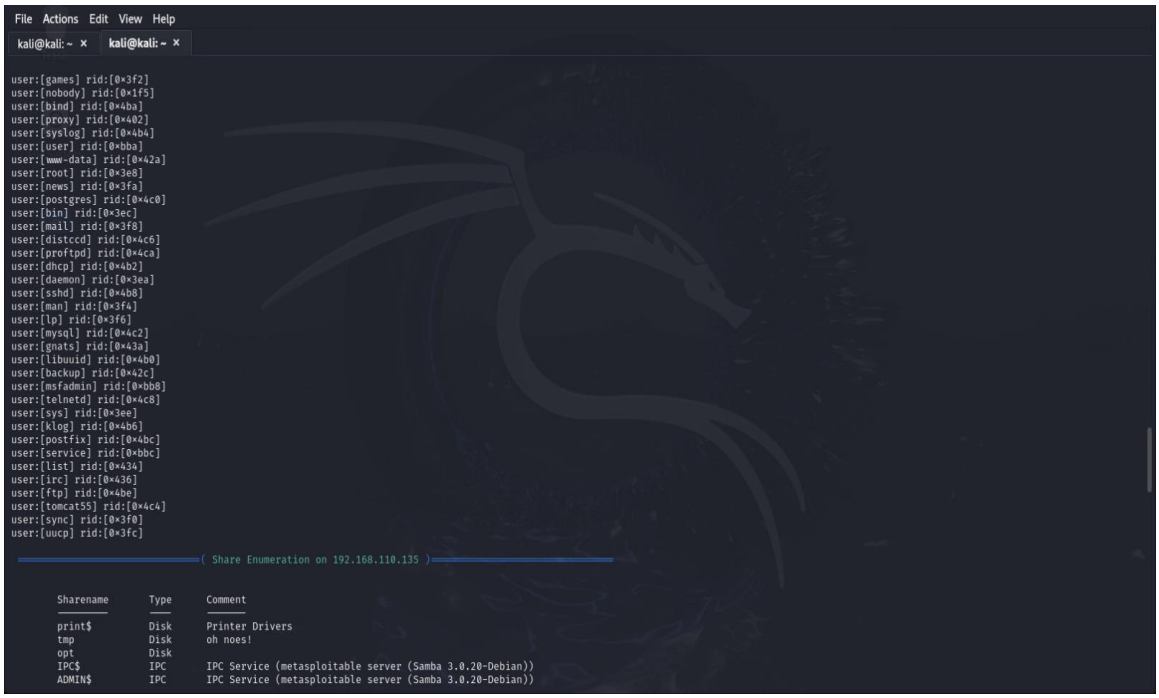
10. SMB Enumeration

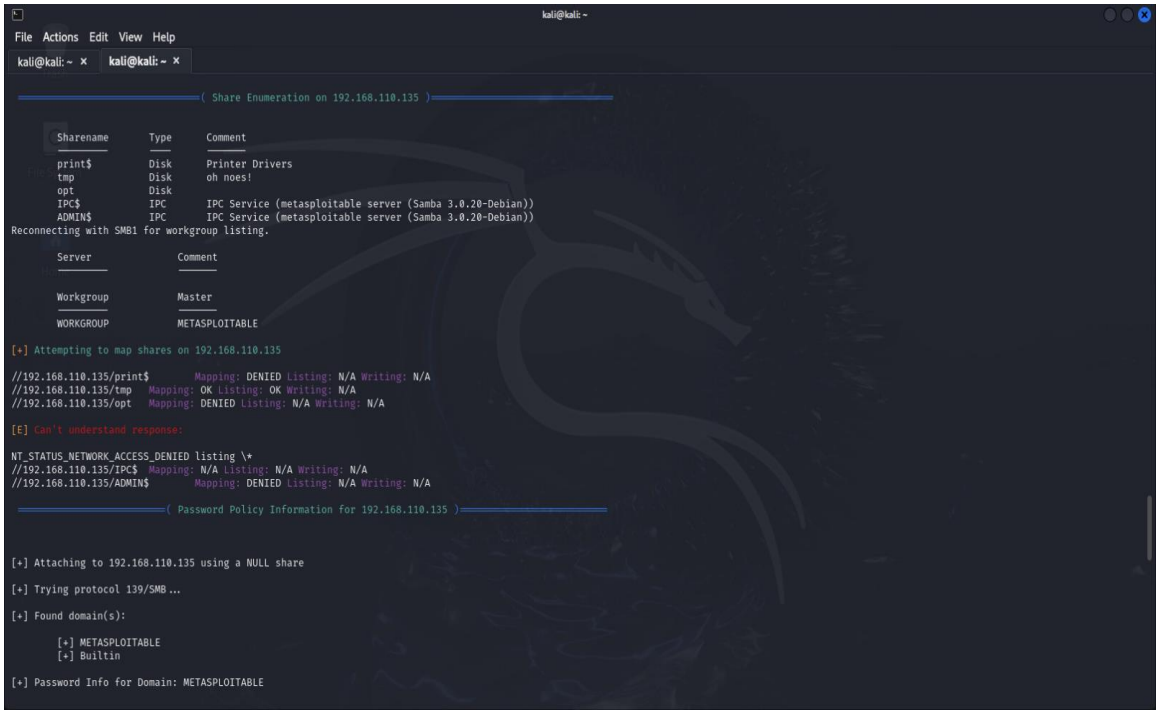
Using enum4linux, we performed enumeration on the SMB (port 445) service. This tool extracted information such as available shares, domain/workgroup details, and usernames. The scan revealed several users and open shares, indicating potential misconfigurations and insecure access.

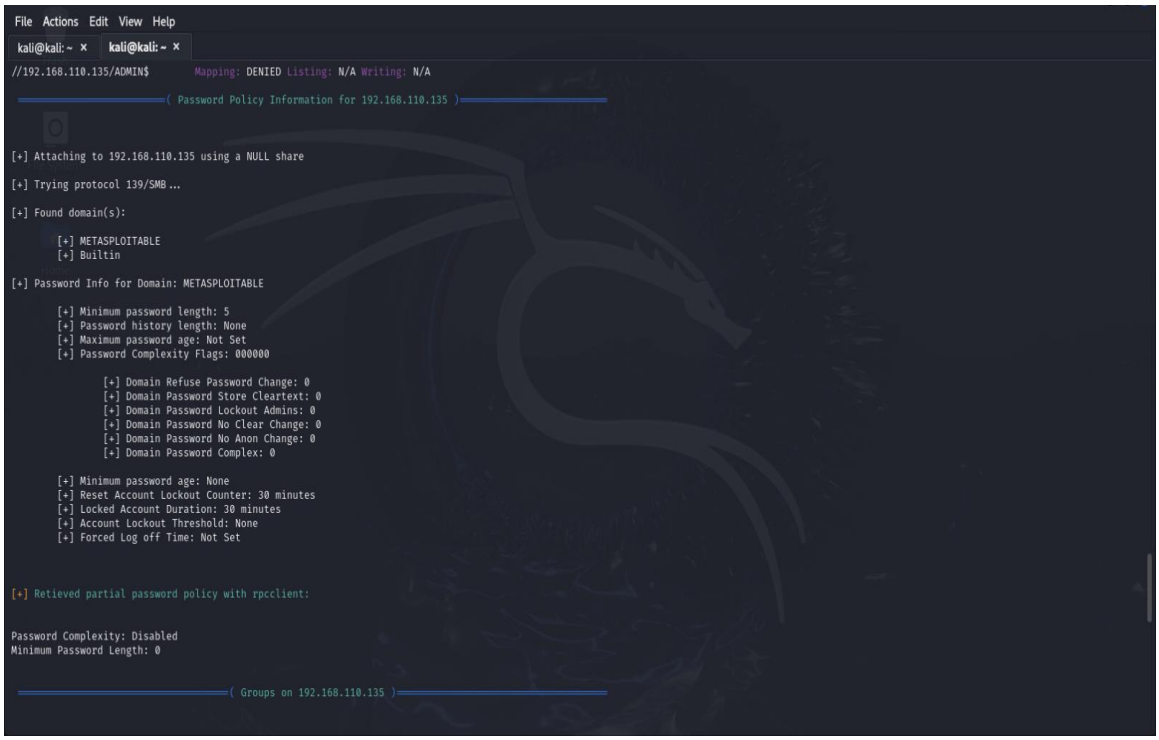
Command:
enum4linux -a 192.168.110.135

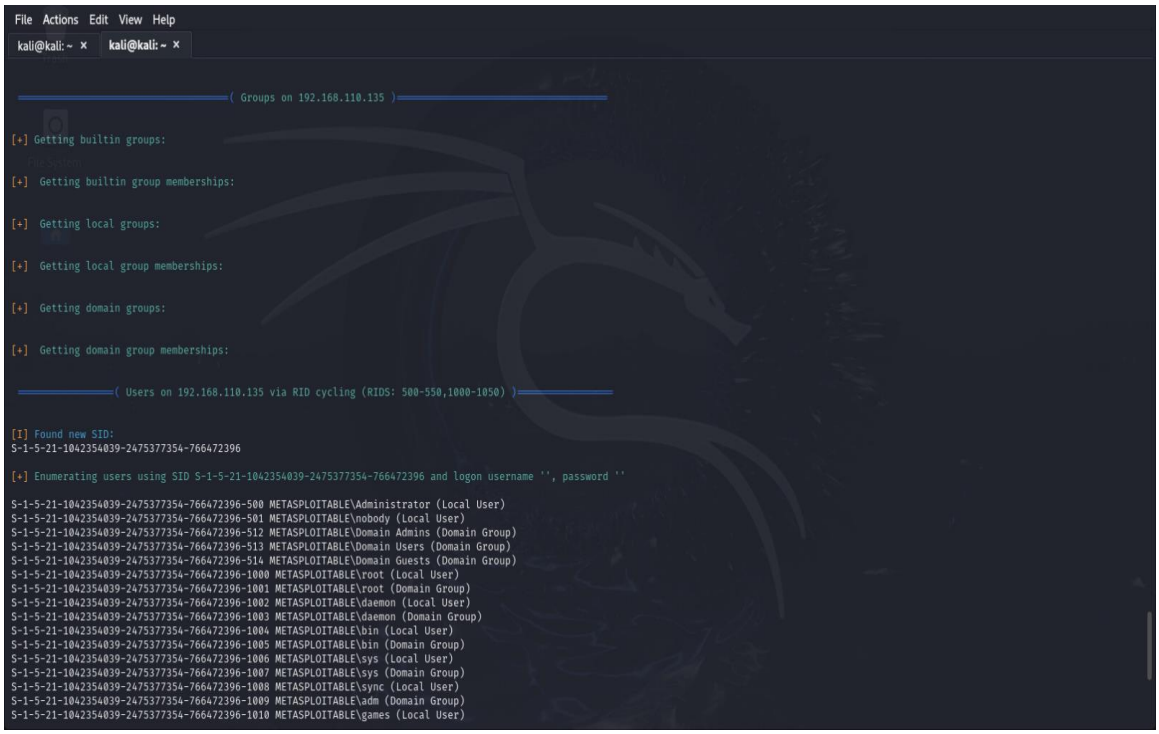

File Actions Edit View Help
kali@kali: ~
kali@kali: ~
(OS information on 192.168.110.135)
[E] Can't get OS info with smbclient
[+] Got OS info for 192.168.110.135 from srvinfo:
METASPLOITABLE Wk Sv PrQ Unx NT SNT metasploitable server (Samba 3.0.20-Debian)
platform_id : 500
os version : 4.9
server type : 0x9a03
(Users on 192.168.110.135)
index: 0x1 RID: 0x3f2 acb: 0x00000011 Account: games Name: games Desc: (null)
index: 0x2 RID: 0x1f5 acb: 0x00000011 Account: nobody Name: nobody Desc: (null)
index: 0x3 RID: 0x4ba acb: 0x00000011 Account: bind Name: (null) Desc: (null)
index: 0x4 RID: 0x402 acb: 0x00000011 Account: proxy Name: proxy Desc: (null)
index: 0x5 RID: 0x4b4 acb: 0x00000011 Account: syslog Name: (null) Desc: (null)
index: 0x6 RID: 0xbba acb: 0x00000010 Account: user Name: just a user,111,, Desc: (null)
index: 0x7 RID: 0x42a acb: 0x00000011 Account: www-data Name: www-data Desc: (null)
index: 0x8 RID: 0x3e8 acb: 0x00000011 Account: root Name: root Desc: (null)
index: 0x9 RID: 0x3fa acb: 0x00000011 Account: news Name: news Desc: (null)
index: 0xa RID: 0x4c0 acb: 0x00000011 Account: postgres Name: PostgreSQL administrator,,, Desc: (null)
index: 0xb RID: 0x3ec acb: 0x00000011 Account: bin Name: bin Desc: (null)
index: 0xc RID: 0x3f8 acb: 0x00000011 Account: mail Name: mail Desc: (null)
index: 0xd RID: 0x4c6 acb: 0x00000011 Account: distccd Name: (null) Desc: (null)
index: 0xe RID: 0x4ca acb: 0x00000011 Account: proftpd Name: (null) Desc: (null)
index: 0xf RID: 0x4b2 acb: 0x00000011 Account: dhcp Name: (null) Desc: (null)
index: 0x10 RID: 0x3ea acb: 0x00000011 Account: daemon Name: daemon Desc: (null)
index: 0x11 RID: 0x4b8 acb: 0x00000011 Account: sshd Name: (null) Desc: (null)
index: 0x12 RID: 0x3f4 acb: 0x00000011 Account: man Name: man Desc: (null)
index: 0x13 RID: 0x3f6 acb: 0x00000011 Account: lp Name: lp Desc: (null)
index: 0x14 RID: 0x4c2 acb: 0x00000011 Account: mysql Name: MySQL Server,,, Desc: (null)
index: 0x15 RID: 0x43a acb: 0x00000011 Account: gnats Name: Gnats Bug-Reporting System (admin) Desc: (null)
index: 0x16 RID: 0x4b0 acb: 0x00000011 Account: libuuid Name: (null) Desc: (null)
index: 0x17 RID: 0x42c acb: 0x00000011 Account: backup Name: backup Desc: (null)
index: 0x18 RID: 0xbb8 acb: 0x00000010 Account: msfadmin Name: msfadmin,,, Desc: (null)
index: 0x19 RID: 0x4c8 acb: 0x00000011 Account: telnetd Name: (null) Desc: (null)
index: 0x1a RID: 0x3ee acb: 0x00000011 Account: sys Name: sys Desc: (null)
index: 0x1b RID: 0x4b6 acb: 0x00000011 Account: klog Name: (null) Desc: (null)
index: 0x1c RID: 0x4bc acb: 0x00000011 Account: postfix Name: (null) Desc: (null)
index: 0x1d RID: 0xbbc acb: 0x00000011 Account: service Name: ,,, Desc: (null)
index: 0x1e RID: 0x434 acb: 0x00000011 Account: list Name: Mailing List Manager Desc: (null)
index: 0x1f RID: 0x436 acb: 0x00000011 Account: irc Name: ircd Desc: (null)

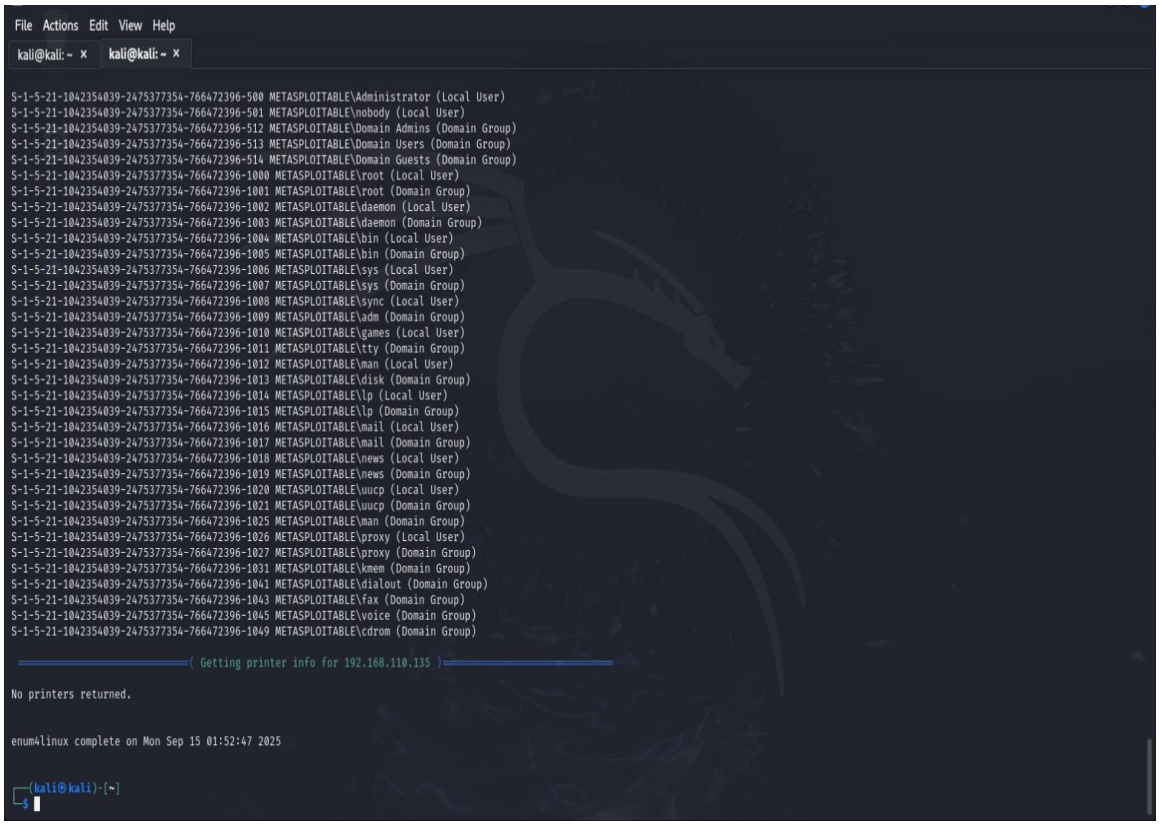

File Actions Edit View Help
kali@kali: ~
kali@kali: ~
index: 0xc RID: 0x3f8 acb: 0x00000011 Account: mail Name: mail Desc: (null)
index: 0xd RID: 0x4c6 acb: 0x00000011 Account: distccd Name: (null) Desc: (null)
index: 0xe RID: 0x4ca acb: 0x00000011 Account: proftpd Name: (null) Desc: (null)
index: 0xf RID: 0x4b2 acb: 0x00000011 Account: dhcp Name: (null) Desc: (null)
index: 0x10 RID: 0x3ea acb: 0x00000011 Account: daemon Name: daemon Desc: (null)
index: 0x11 RID: 0x4b8 acb: 0x00000011 Account: sshd Name: (null) Desc: (null)
index: 0x12 RID: 0x3f4 acb: 0x00000011 Account: man Name: man Desc: (null)
index: 0x13 RID: 0x3f6 acb: 0x00000011 Account: lp Name: lp Desc: (null)
index: 0x14 RID: 0x4c2 acb: 0x00000011 Account: mysql Name: MySQL Server,,, Desc: (null)
index: 0x15 RID: 0x43a acb: 0x00000011 Account: gnats Name: Gnats Bug-Reporting System (admin) Desc: (null)
index: 0x16 RID: 0x4b0 acb: 0x00000011 Account: libuuid Name: (null) Desc: (null)
index: 0x17 RID: 0x42c acb: 0x00000011 Account: backup Name: backup Desc: (null)
index: 0x18 RID: 0xbb8 acb: 0x00000010 Account: msfadmin Name: msfadmin,,, Desc: (null)
index: 0x19 RID: 0x4c8 acb: 0x00000011 Account: telnetd Name: (null) Desc: (null)
index: 0x1a RID: 0x3ee acb: 0x00000011 Account: sys Name: sys Desc: (null)
index: 0x1b RID: 0x4b6 acb: 0x00000011 Account: klog Name: (null) Desc: (null)
index: 0x1c RID: 0x4bc acb: 0x00000011 Account: postfix Name: (null) Desc: (null)
index: 0x1d RID: 0xbbc acb: 0x00000011 Account: service Name: ,,, Desc: (null)
index: 0x1e RID: 0x434 acb: 0x00000011 Account: list Name: Mailing List Manager Desc: (null)
index: 0x1f RID: 0x436 acb: 0x00000011 Account: irc Name: ircd Desc: (null)
index: 0x20 RID: 0x4be acb: 0x00000011 Account: ftp Name: (null) Desc: (null)
index: 0x21 RID: 0x4c4 acb: 0x00000011 Account: tomcat55 Name: (null) Desc: (null)
index: 0x22 RID: 0x3f0 acb: 0x00000011 Account: sync Name: sync Desc: (null)
index: 0x23 RID: 0x3fc acb: 0x00000011 Account: uucp Name: uucp Desc: (null)
user:[games] rid:[0x3f2]
user:[nobody] rid:[0x1f5]
user:[bind] rid:[0x4ba]
user:[proxy] rid:[0x402]
user:[syslog] rid:[0x4b4]
user:[user] rid:[0xbba]
user:[www-data] rid:[0x42a]
user:[root] rid:[0x3e8]
user:[news] rid:[0x3fa]
user:[postgres] rid:[0x4c0]
user:[bin] rid:[0x3ec]
user:[mail] rid:[0x3f8]
user:[distccd] rid:[0x4c6]
user:[proftpd] rid:[0x4ca]
user:[dhcp] rid:[0x4b2]
user:[daemon] rid:[0x3ea]
user:[sshd] rid:[0x4b8]
user:[man] rid:[0x3f4]
user:[lp] rid:[0x3f6]
user:[mysql] rid:[0x4c2]
user:[gnats] rid:[0x43a]
user:[libuuid] rid:[0x4b0]


File Actions Edit View Help
kali@kali: ~
kali@kali: ~
user:[games] rid:[0×3f2]
user:[nobody] rid:[0×1f5]
user:[bind] rid:[0×4ba]
user:[proxy] rid:[0×402]
user:[syslog] rid:[0×4b4]
user:[user] rid:[0×bba]
user:[www-data] rid:[0×42a]
user:[root] rid:[0×3e8]
user:[news] rid:[0×3fa]
user:[postgres] rid:[0×4c0]
user:[bin] rid:[0×3ec]
user:[mail] rid:[0×3f8]
user:[distccd] rid:[0×4c6]
user:[proftpd] rid:[0×4ca]
user:[dhcp] rid:[0×4b2]
user:[daemon] rid:[0×3ea]
user:[sshd] rid:[0×4b8]
user:[man] rid:[0×3f4]
user:[lp] rid:[0×3f6]
user:[mysql] rid:[0×4c2]
user:[gnats] rid:[0×43a]
user:[libuuid] rid:[0×4b0]
user:[backup] rid:[0×42c]
user:[msfadmin] rid:[0×bb8]
user:[telnetd] rid:[0×4c8]
user:[sys] rid:[0×3ee]
user:[klog] rid:[0×4b6]
user:[postfix] rid:[0×4bc]
user:[service] rid:[0×bbc]
user:[list] rid:[0×434]
user:[irc] rid:[0×436]
user:[ftp] rid:[0×4be]
user:[tomcat55] rid:[0×4c4]
user:[sync] rid:[0×3f0]
user:[uucp] rid:[0×3fc]
(Share Enumeration on 192.168.110.135)
Sharename Type Comment
print$ Disk Printer Drivers
tmp Disk oh noes!
opt Disk
IPC$ IPC IPC Service (metasploitable server (Samba 3.0.20-Debian))
ADMIN$ IPC IPC Service (metasploitable server (Samba 3.0.20-Debian))


kali@kali: ~
File Actions Edit View Help
kali@kali: ~
kali@kali: ~
(Share Enumeration on 192.168.110.135)
Sharename Type Comment
print$ Disk Printer Drivers
tmp Disk oh noes!
opt Disk
IPC$ IPC IPC Service (metasploitable server (Samba 3.0.20-Debian))
ADMIN$ IPC IPC Service (metasploitable server (Samba 3.0.20-Debian))
Reconnecting with SMB1 for workgroup listing.
Server Comment
Workgroup Master
WORKGROUP METASPLOITABLE
[+] Attempting to map shares on 192.168.110.135
//192.168.110.135/print$ Mapping: DENIED Listing: N/A Writing: N/A
//192.168.110.135/tmp Mapping: OK Listing: OK Writing: N/A
//192.168.110.135/opt Mapping: DENIED Listing: N/A Writing: N/A
[E] Can't understand response:
NT_STATUS_NETWORK_ACCESS_DENIED listing *
//192.168.110.135/IPC$ Mapping: N/A Listing: N/A Writing: N/A
//192.168.110.135/ADMIN$ Mapping: DENIED Listing: N/A Writing: N/A
(Password Policy Information for 192.168.110.135)
[+] Attaching to 192.168.110.135 using a NULL share
[+] Trying protocol 139/SMB ...
[+] Found domain(s):
[+] METASPLOITABLE
[+] Builtin
[+] Password Info for Domain: METASPLOITABLE


File Actions Edit View Help
kali@kali: ~
kali@kali: ~
//192.168.110.135/ADMIN$ Mapping: DENIED Listing: N/A Writing: N/A
(Password Policy Information for 192.168.110.135)
[+] Attaching to 192.168.110.135 using a NULL share
[+] Trying protocol 139/SMB ...
[+] Found domain(s):
[+] METASPLOITABLE
[+] Builtin
[+] Password Info for Domain: METASPLOITABLE
[+] Minimum password length: 5
[+] Password history length: None
[+] Maximum password age: Not Set
[+] Password Complexity Flags: 000000
[+] Domain Refuse Password Change: 0
[+] Domain Password Store Cleartext: 0
[+] Domain Password Lockout Admins: 0
[+] Domain Password No Clear Change: 0
[+] Domain Password No Anon Change: 0
[+] Domain Password Complex: 0
[+] Minimum password age: None
[+] Reset Account Lockout Counter: 30 minutes
[+] Locked Account Duration: 30 minutes
[+] Account Lockout Threshold: None
[+] Forced Log off Time: Not Set
[+] Retieved partial password policy with rpcclient:
Password Complexity: Disabled
Minimum Password Length: 0
(Groups on 192.168.110.135)


File Actions Edit View Help
kali@kali: ~
kali@kali: ~
(Groups on 192.168.110.135)
[+] Getting builtin groups:
[+] Getting builtin group memberships:
[+] Getting local groups:
[+] Getting local group memberships:
[+] Getting domain groups:
[+] Getting domain group memberships:
(Users on 192.168.110.135 via RID cycling (RIDS: 500-550,1000-1050))
[I] Found new SID:
S-1-5-21-1042354039-2475377354-766472396
[+] Enumerating users using SID S-1-5-21-1042354039-2475377354-766472396 and logon username '', password ''
S-1-5-21-1042354039-2475377354-766472396-500 METASPLOITABLE\Administrator (Local User)
S-1-5-21-1042354039-2475377354-766472396-501 METASPLOITABLE\nobody (Local User)
S-1-5-21-1042354039-2475377354-766472396-512 METASPLOITABLE\Domain Admins (Domain Group)
S-1-5-21-1042354039-2475377354-766472396-513 METASPLOITABLE\Domain Users (Domain Group)
S-1-5-21-1042354039-2475377354-766472396-514 METASPLOITABLE\Domain Guests (Domain Group)
S-1-5-21-1042354039-2475377354-766472396-1000 METASPLOITABLE\root (Local User)
S-1-5-21-1042354039-2475377354-766472396-1001 METASPLOITABLE\root (Domain Group)
S-1-5-21-1042354039-2475377354-766472396-1002 METASPLOITABLE\daemon (Local User)
S-1-5-21-1042354039-2475377354-766472396-1003 METASPLOITABLE\daemon (Domain Group)
S-1-5-21-1042354039-2475377354-766472396-1004 METASPLOITABLE\bin (Local User)
S-1-5-21-1042354039-2475377354-766472396-1005 METASPLOITABLE\bin (Domain Group)
S-1-5-21-1042354039-2475377354-766472396-1006 METASPLOITABLE\sys (Local User)
S-1-5-21-1042354039-2475377354-766472396-1007 METASPLOITABLE\sys (Domain Group)
S-1-5-21-1042354039-2475377354-766472396-1008 METASPLOITABLE\sync (Local User)
S-1-5-21-1042354039-2475377354-766472396-1009 METASPLOITABLE\adm (Domain Group)
S-1-5-21-1042354039-2475377354-766472396-1010 METASPLOITABLE\games (Local User)


File Actions Edit View Help
kali@kali: ~
kali@kali: ~
S-1-5-21-1042354039-2475377354-766472396-500 METASPLOITABLE\Administrator (Local User)
S-1-5-21-1042354039-2475377354-766472396-501 METASPLOITABLE\nobody (Local User)
S-1-5-21-1042354039-2475377354-766472396-512 METASPLOITABLE\Domain Admins (Domain Group)
S-1-5-21-1042354039-2475377354-766472396-513 METASPLOITABLE\Domain Users (Domain Group)
S-1-5-21-1042354039-2475377354-766472396-514 METASPLOITABLE\Domain Guests (Domain Group)
S-1-5-21-1042354039-2475377354-766472396-1000 METASPLOITABLE\root (Local User)
S-1-5-21-1042354039-2475377354-766472396-1001 METASPLOITABLE\root (Domain Group)
S-1-5-21-1042354039-2475377354-766472396-1002 METASPLOITABLE\daemon (Local User)
S-1-5-21-1042354039-2475377354-766472396-1003 METASPLOITABLE\daemon (Domain Group)
S-1-5-21-1042354039-2475377354-766472396-1004 METASPLOITABLE\bin (Local User)
S-1-5-21-1042354039-2475377354-766472396-1005 METASPLOITABLE\bin (Domain Group)
S-1-5-21-1042354039-2475377354-766472396-1006 METASPLOITABLE\sys (Local User)
S-1-5-21-1042354039-2475377354-766472396-1007 METASPLOITABLE\sys (Domain Group)
S-1-5-21-1042354039-2475377354-766472396-1008 METASPLOITABLE\sync (Local User)
S-1-5-21-1042354039-2475377354-766472396-1009 METASPLOITABLE\adm (Domain Group)
S-1-5-21-1042354039-2475377354-766472396-1010 METASPLOITABLE\games (Local User)
S-1-5-21-1042354039-2475377354-766472396-1011 METASPLOITABLE\tty (Domain Group)
S-1-5-21-1042354039-2475377354-766472396-1012 METASPLOITABLE\man (Local User)
S-1-5-21-1042354039-2475377354-766472396-1013 METASPLOITABLE\disk (Domain Group)
S-1-5-21-1042354039-2475377354-766472396-1014 METASPLOITABLE\lp (Local User)
S-1-5-21-1042354039-2475377354-766472396-1015 METASPLOITABLE\lp (Domain Group)
S-1-5-21-1042354039-2475377354-766472396-1016 METASPLOITABLE\mail (Local User)
S-1-5-21-1042354039-2475377354-766472396-1017 METASPLOITABLE\mail (Domain Group)
S-1-5-21-1042354039-2475377354-766472396-1018 METASPLOITABLE\news (Local User)
S-1-5-21-1042354039-2475377354-766472396-1019 METASPLOITABLE\news (Domain Group)
S-1-5-21-1042354039-2475377354-766472396-1020 METASPLOITABLE\uucp (Local User)
S-1-5-21-1042354039-2475377354-766472396-1021 METASPLOITABLE\uucp (Domain Group)
S-1-5-21-1042354039-2475377354-766472396-1025 METASPLOITABLE\man (Domain Group)
S-1-5-21-1042354039-2475377354-766472396-1026 METASPLOITABLE\proxy (Local User)
S-1-5-21-1042354039-2475377354-766472396-1027 METASPLOITABLE\proxy (Domain Group)
S-1-5-21-1042354039-2475377354-766472396-1031 METASPLOITABLE\kmem (Domain Group)
S-1-5-21-1042354039-2475377354-766472396-1041 METASPLOITABLE\dialout (Domain Group)
S-1-5-21-1042354039-2475377354-766472396-1043 METASPLOITABLE\fax (Domain Group)
S-1-5-21-1042354039-2475377354-766472396-1045 METASPLOITABLE\voice (Domain Group)
S-1-5-21-1042354039-2475377354-766472396-1049 METASPLOITABLE\cdrom (Domain Group)
(Getting printer info for 192.168.110.135)
No printers returned.
enum4linux complete on Mon Sep 15 01:52:47 2025
(kali㉿kali)-[~]
$

11. SNMP Enumeration

SNMP enumeration was attempted using snmpwalk, but the target did not respond on port 161/UDP. This indicates that the SNMP service was either not active or the port was filtered. Therefore, SNMP enumeration was skipped for this phase.

Command:
snmpwalk -v1 -c public 192.168.110.135

12. Web Server Scanning

A vulnerability scan of the target's web server was conducted using Nikto. The tool discovered several known vulnerabilities, including outdated server software, exposed directories, and potentially dangerous HTTP methods. These findings provide insight into possible attack vectors in the web layer.

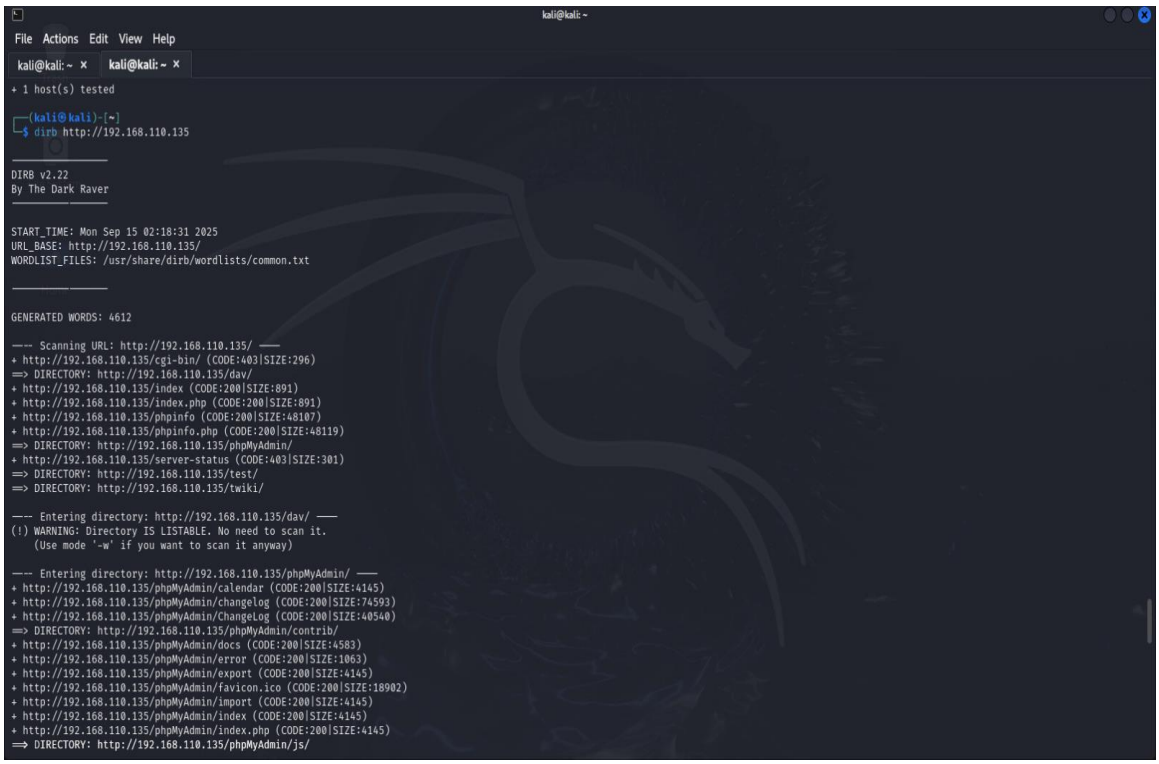
Command:
nikto -h http://192.168.110.135

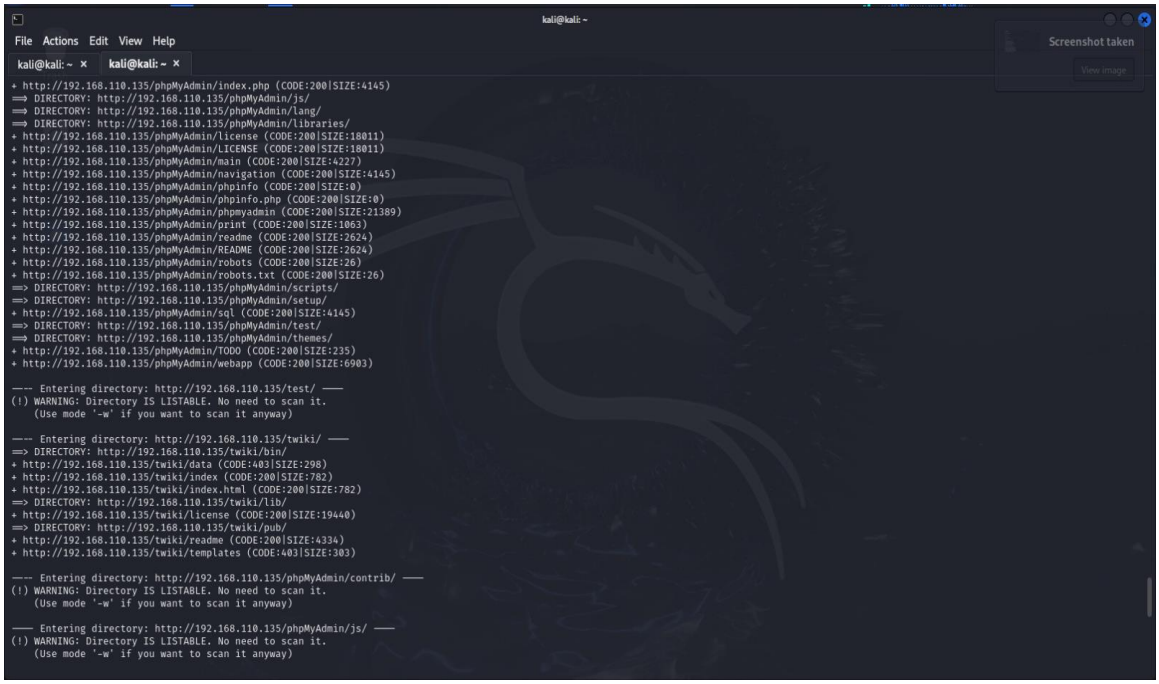

kali@kali: ~
File Actions Edit View Help
kali@kali: ~
kali@kali: ~
┌──(kali㉿kali)-[~]
└─$ nikto -h http://192.168.110.135
- Nikto v2.5.0
+ Target IP: 192.168.110.135
+ Target Hostname: 192.168.110.135
+ Target Port: 80
+ Start Time: 2025-09-15 02:17:32 (GMT-4)
+ Server: Apache/2.2.8 (Ubuntu) DAV/2
+ /: Retrieved x-powered-by header: PHP/5.2.4-2ubuntu5.10.
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
+ Apache/2.2.8 appears to be outdated (current is at least Apache/2.4.54). Apache 2.2.34 is the EOL for the 2.x branch.
+ /index: Uncommon header 'tcn' found, with contents: list.
+ /index: Apache mod_negotiation is enabled with MultiViews, which allows attackers to easily brute force file names. The following alternatives for 'index' were found: index.php. See: http://www.wisec.it/sectou.php?id=4698ebdc59d15,https://exchange.xforce.ibmcloud.com/vulnerabilities/8275
+ /: Web Server returns a valid response with junk HTTP methods which may cause false positives.
+ /: HTTP TRACE method is active which suggests the host is vulnerable to XST. See: https://owasp.org/www-community/attacks/Cross_Site_Tracing
+ /phpinfo.php: Output from the phpinfo() function was found.
+ /doc/: Directory indexing found.
+ /doc/: The /doc/ directory is browsable. This may be /usr/doc. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-0678
+ /?=PHPB8B5F2A0-3C92-11d3-A3A9-4C7B08C10000: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings. See: OSVDB-12184
+ /?=PHPE9568F36-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings. See: OSVDB-12184
+ /?=PHPE9568F34-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings. See: OSVDB-12184
+ /?=PHPE9568F35-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings. See: OSVDB-12184
+ /phpMyAdmin/changelog.php: phpMyAdmin is for managing MySQL databases, and should be protected or limited to authorized hosts.
+ /phpMyAdmin/ChangeLog: Server may leak inodes via ETags, header found with file /phpMyAdmin/ChangeLog, inode: 92462, size: 40540, mtime: Tue Dec 9 12:24:00 2008. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2003-1418
+ /phpMyAdmin/ChangeLog: phpMyAdmin is for managing MySQL databases, and should be protected or limited to authorized hosts.
+ /test/: Directory indexing found.
+ /test/: This might be interesting.
+ /phpinfo.php: PHP is installed, and a test script which runs phpinfo() was found. This gives a lot of system information. See: CWE-552
+ /icons/: Directory indexing found.
+ /icons/README: Apache default file found. See: https://www.vntweb.co.uk/apache-restricting-access-to-iconsreadme/
+ /phpMyAdmin/: phpMyAdmin directory found.
+ /phpMyAdmin/Documentation.html: phpMyAdmin is for managing MySQL databases, and should be protected or limited to authorized hosts.
+ /phpMyAdmin/README: phpMyAdmin is for managing MySQL databases, and should be protected or limited to authorized hosts. See: https://typo3.org/
+ /#wp-config.php#: #wp-config.php# file found. This file contains the credentials.
+ 8910 requests: 0 error(s) and 27 item(s) reported on remote host
+ End Time: 2025-09-15 02:17:54 (GMT-4) (22 seconds)
+ 1 host(s) tested
┌──(kali㉿kali)-[~]
└─$

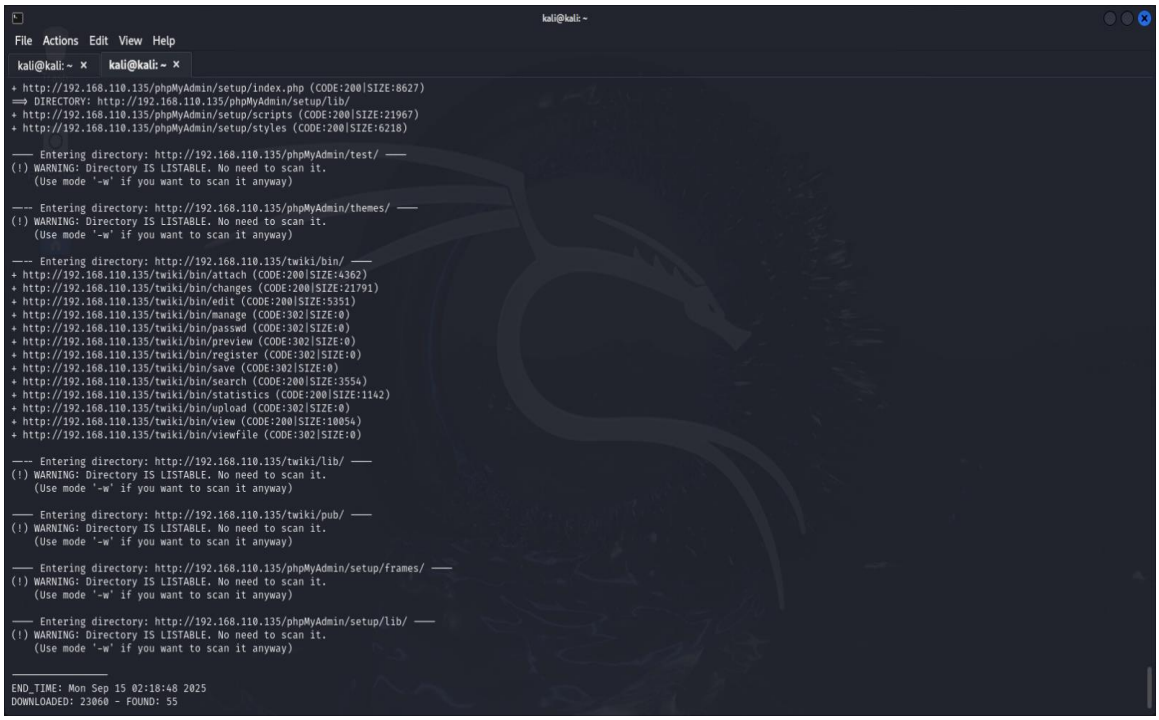
13. Directory Brute Forcing

We used dirb to brute-force hidden web directories on the target's HTTP service. This revealed folders such as /admin, /phpmyadmin, and /backup, which may contain sensitive or exploitable resources if accessible. Directory enumeration is critical for discovering unlinked and sensitive backend content.

Command:
dirb http://192.168.110.135




kali@kali: ~
File Actions Edit View Help
kali@kali: ~ ×
kali@kali: ~ ×
+ http://192.168.110.135/phpMyAdmin/index.php (CODE:200|SIZE:4145)
==> DIRECTORY: http://192.168.110.135/phpMyAdmin/js/
==> DIRECTORY: http://192.168.110.135/phpMyAdmin/lang/
==> DIRECTORY: http://192.168.110.135/phpMyAdmin/libraries/
+ http://192.168.110.135/phpMyAdmin/license (CODE:200|SIZE:18011)
+ http://192.168.110.135/phpMyAdmin/LICENSE (CODE:200|SIZE:18011)
+ http://192.168.110.135/phpMyAdmin/main (CODE:200|SIZE:4227)
+ http://192.168.110.135/phpMyAdmin/navigation (CODE:200|SIZE:4145)
+ http://192.168.110.135/phpMyAdmin/phpinfo (CODE:200|SIZE:0)
+ http://192.168.110.135/phpMyAdmin/phpinfo.php (CODE:200|SIZE:0)
+ http://192.168.110.135/phpMyAdmin/phpmyadmin (CODE:200|SIZE:21389)
+ http://192.168.110.135/phpMyAdmin/print (CODE:200|SIZE:1063)
+ http://192.168.110.135/phpMyAdmin/readme (CODE:200|SIZE:2624)
+ http://192.168.110.135/phpMyAdmin/README (CODE:200|SIZE:2624)
+ http://192.168.110.135/phpMyAdmin/robots (CODE:200|SIZE:26)
+ http://192.168.110.135/phpMyAdmin/robots.txt (CODE:200|SIZE:26)
==> DIRECTORY: http://192.168.110.135/phpMyAdmin/scripts/
==> DIRECTORY: http://192.168.110.135/phpMyAdmin/setup/
+ http://192.168.110.135/phpMyAdmin/sql (CODE:200|SIZE:4145)
==> DIRECTORY: http://192.168.110.135/phpMyAdmin/test/
==> DIRECTORY: http://192.168.110.135/phpMyAdmin/themes/
+ http://192.168.110.135/phpMyAdmin/TODO (CODE:200|SIZE:235)
+ http://192.168.110.135/phpMyAdmin/webapp (CODE:200|SIZE:6903)
—— Entering directory: http://192.168.110.135/test/ ——
(!) WARNING: Directory IS LISTABLE. No need to scan it.
(Use mode '-w' if you want to scan it anyway)
—— Entering directory: http://192.168.110.135/twiki/ ——
==> DIRECTORY: http://192.168.110.135/twiki/bin/
+ http://192.168.110.135/twiki/data (CODE:403|SIZE:298)
+ http://192.168.110.135/twiki/index (CODE:200|SIZE:782)
+ http://192.168.110.135/twiki/index.html (CODE:200|SIZE:782)
==> DIRECTORY: http://192.168.110.135/twiki/lib/
+ http://192.168.110.135/twiki/license (CODE:200|SIZE:19440)
==> DIRECTORY: http://192.168.110.135/twiki/pub/
+ http://192.168.110.135/twiki/readme (CODE:200|SIZE:4334)
+ http://192.168.110.135/twiki/templates (CODE:403|SIZE:303)
—— Entering directory: http://192.168.110.135/phpMyAdmin/contrib/ ——
(!) WARNING: Directory IS LISTABLE. No need to scan it.
(Use mode '-w' if you want to scan it anyway)
—— Entering directory: http://192.168.110.135/phpMyAdmin/js/ ——
(!) WARNING: Directory IS LISTABLE. No need to scan it.
(Use mode '-w' if you want to scan it anyway)
Screenshot taken
View image


kali@kali: ~
File Actions Edit View Help
kali@kali: ~ ×
kali@kali: ~ ×
+ http://192.168.110.135/phpMyAdmin/setup/index.php (CODE:200|SIZE:8627)
==> DIRECTORY: http://192.168.110.135/phpMyAdmin/setup/lib/
+ http://192.168.110.135/phpMyAdmin/setup/scripts (CODE:200|SIZE:21967)
+ http://192.168.110.135/phpMyAdmin/setup/styles (CODE:200|SIZE:6218)
—— Entering directory: http://192.168.110.135/phpMyAdmin/test/ ——
(!) WARNING: Directory IS LISTABLE. No need to scan it.
(Use mode '-w' if you want to scan it anyway)
—— Entering directory: http://192.168.110.135/phpMyAdmin/themes/ ——
(!) WARNING: Directory IS LISTABLE. No need to scan it.
(Use mode '-w' if you want to scan it anyway)
—— Entering directory: http://192.168.110.135/twiki/bin/ ——
+ http://192.168.110.135/twiki/bin/attach (CODE:200|SIZE:4362)
+ http://192.168.110.135/twiki/bin/changes (CODE:200|SIZE:21791)
+ http://192.168.110.135/twiki/bin/edit (CODE:200|SIZE:5351)
+ http://192.168.110.135/twiki/bin/manage (CODE:302|SIZE:0)
+ http://192.168.110.135/twiki/bin/passwd (CODE:302|SIZE:0)
+ http://192.168.110.135/twiki/bin/preview (CODE:302|SIZE:0)
+ http://192.168.110.135/twiki/bin/register (CODE:302|SIZE:0)
+ http://192.168.110.135/twiki/bin/save (CODE:302|SIZE:0)
+ http://192.168.110.135/twiki/bin/search (CODE:200|SIZE:3554)
+ http://192.168.110.135/twiki/bin/statistics (CODE:200|SIZE:1142)
+ http://192.168.110.135/twiki/bin/upload (CODE:302|SIZE:0)
+ http://192.168.110.135/twiki/bin/view (CODE:200|SIZE:10054)
+ http://192.168.110.135/twiki/bin/viewfile (CODE:302|SIZE:0)
—— Entering directory: http://192.168.110.135/twiki/lib/ ——
(!) WARNING: Directory IS LISTABLE. No need to scan it.
(Use mode '-w' if you want to scan it anyway)
—— Entering directory: http://192.168.110.135/twiki/pub/ ——
(!) WARNING: Directory IS LISTABLE. No need to scan it.
(Use mode '-w' if you want to scan it anyway)
—— Entering directory: http://192.168.110.135/phpMyAdmin/setup/frames/ ——
(!) WARNING: Directory IS LISTABLE. No need to scan it.
(Use mode '-w' if you want to scan it anyway)
—— Entering directory: http://192.168.110.135/phpMyAdmin/setup/lib/ ——
(!) WARNING: Directory IS LISTABLE. No need to scan it.
(Use mode '-w' if you want to scan it anyway)
END_TIME: Mon Sep 15 02:18:48 2025
DOWNLOADED: 23060 - FOUND: 55

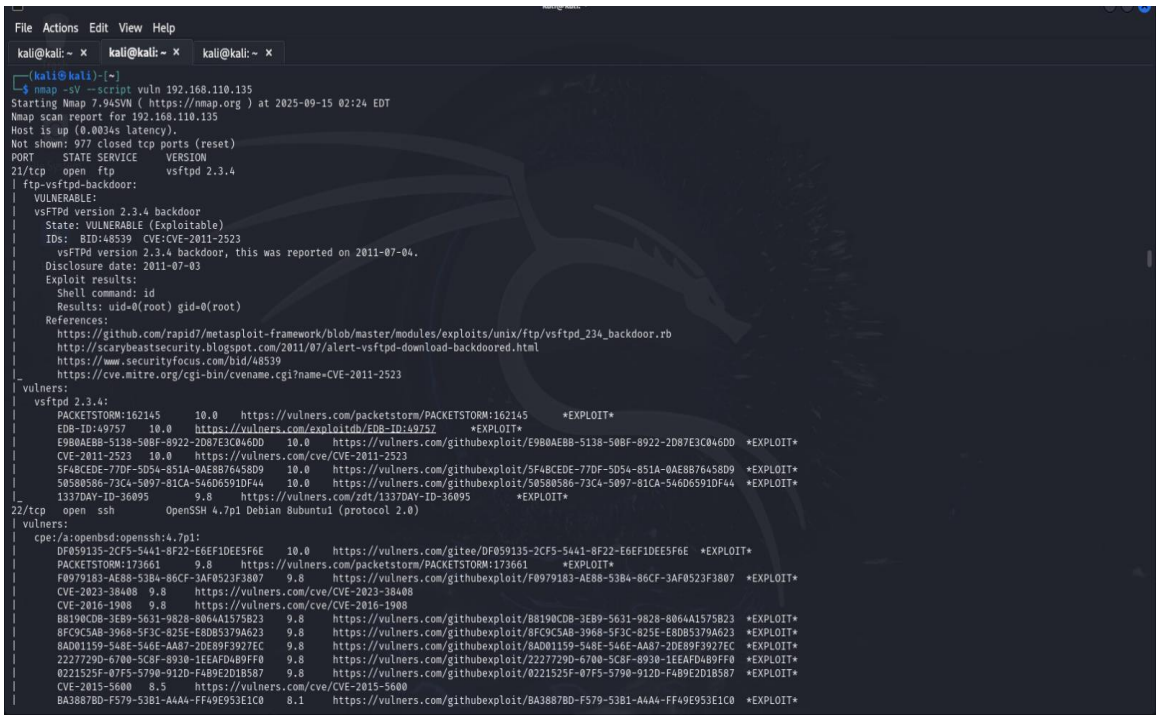
14. Vulnerability Scanning (Optional)

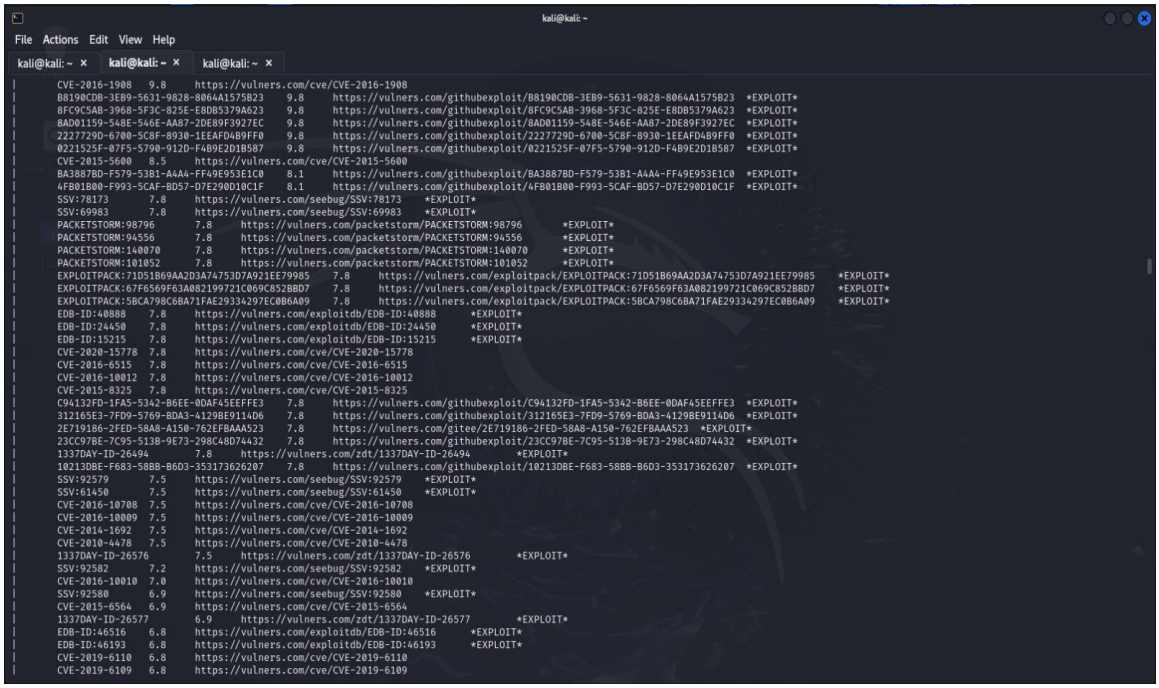
A full vulnerability assessment was performed using Nessus (or OpenVAS). The scan identified multiple high and medium severity vulnerabilities mapped to known CVEs. This step ties together all enumeration findings and presents actionable insights for exploitation or mitigation planning.

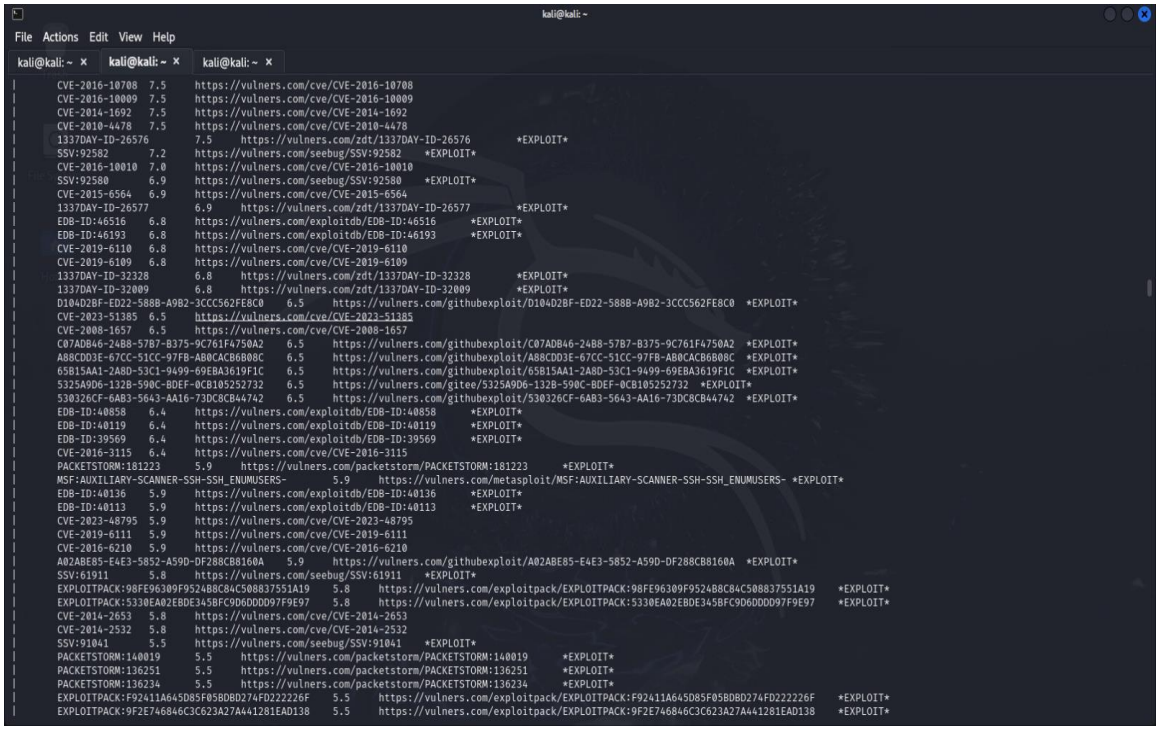
Tool: Nessus or OpenVAS (GUI-based)

Command:

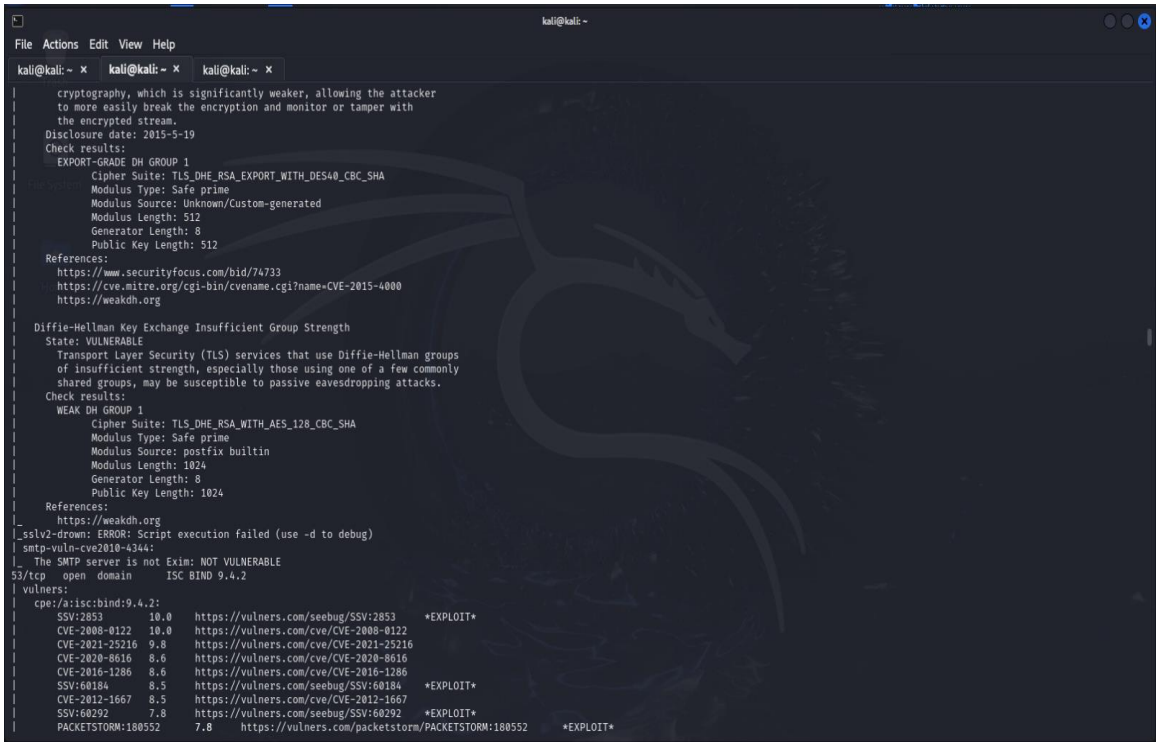
nmap -sV --script vuln 192.168.110.135

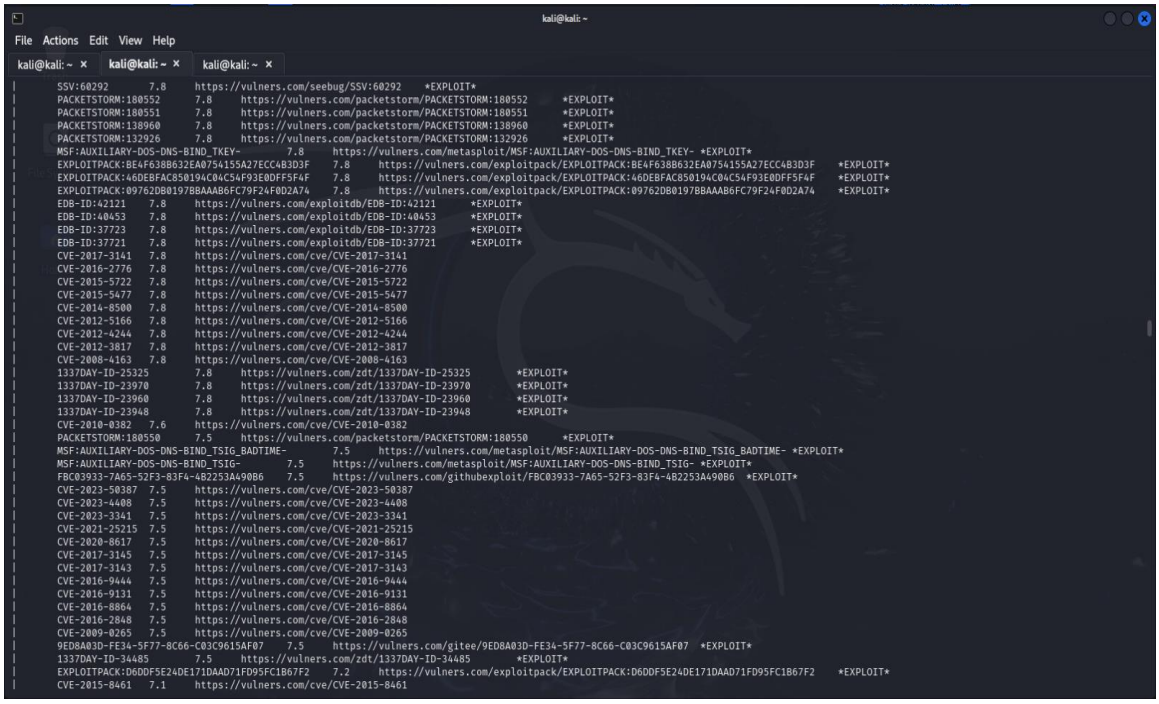


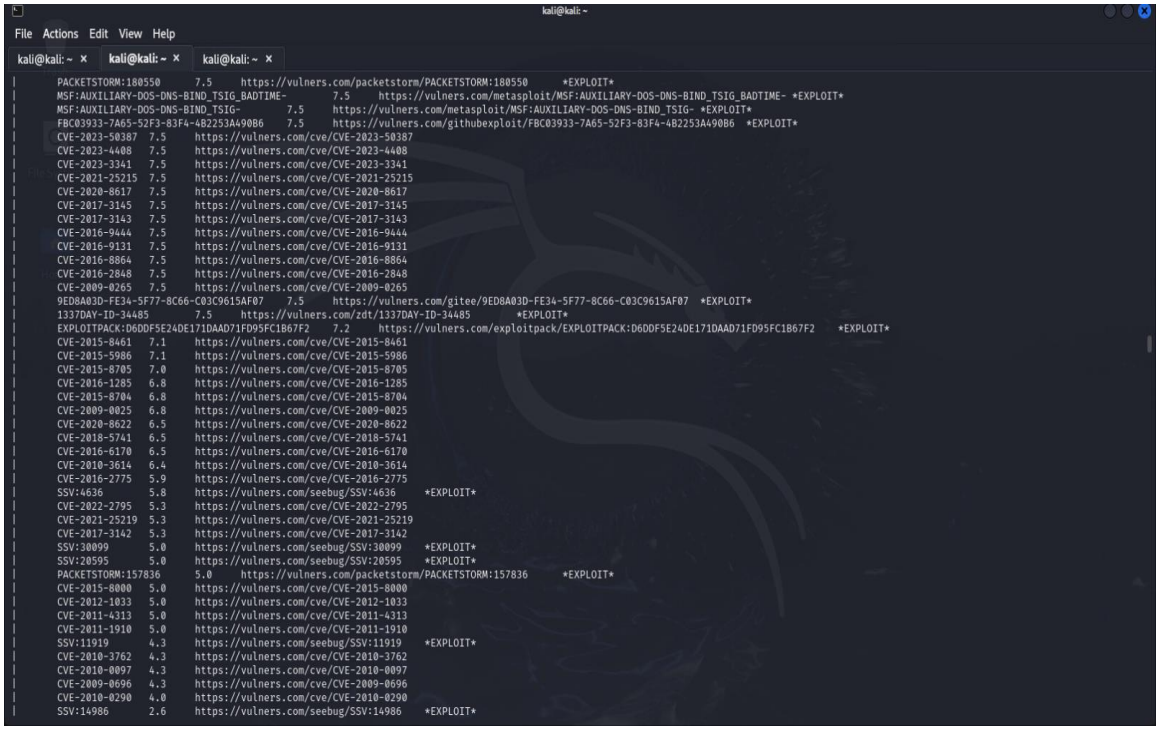

kali@kali: ~
File Actions Edit View Help
kali@kali: ~
kali@kali: ~
kali@kali: ~
CVE-2016-1908 9.8 https://vulners.com/cve/CVE-2016-1908
B8190CDB-3EB9-5631-9828-8064A1575B23 9.8 https://vulners.com/githubexploit/B8190CDB-3EB9-5631-9828-8064A1575B23 *EXPLOIT*
8FC9C5AB-3968-5F3C-825E-E8DB5379A623 9.8 https://vulners.com/githubexploit/8FC9C5AB-3968-5F3C-825E-E8DB5379A623 *EXPLOIT*
8AD01159-548E-546E-AA87-2DE89F3927EC 9.8 https://vulners.com/githubexploit/8AD01159-548E-546E-AA87-2DE89F3927EC *EXPLOIT*
2227729D-6700-5C8F-8930-1EEAFD4B9FF0 9.8 https://vulners.com/githubexploit/2227729D-6700-5C8F-8930-1EEAFD4B9FF0 *EXPLOIT*
0221525F-07F5-5790-912D-F4B9E2D1B587 9.8 https://vulners.com/githubexploit/0221525F-07F5-5790-912D-F4B9E2D1B587 *EXPLOIT*
CVE-2015-5600 8.5 https://vulners.com/cve/CVE-2015-5600
BA3887BD-F579-53B1-A4A4-FF49E953E1C0 8.1 https://vulners.com/githubexploit/BA3887BD-F579-53B1-A4A4-FF49E953E1C0 *EXPLOIT*
4FB01B00-F993-5CAF-BD57-D7E290D10C1F 8.1 https://vulners.com/githubexploit/4FB01B00-F993-5CAF-BD57-D7E290D10C1F *EXPLOIT*
SSV:78173 7.8 https://vulners.com/seebug/SSV:78173 *EXPLOIT*
SSV:69983 7.8 https://vulners.com/seebug/SSV:69983 *EXPLOIT*
PACKETSTORM:98796 7.8 https://vulners.com/packetstorm/PACKETSTORM:98796 *EXPLOIT*
PACKETSTORM:94556 7.8 https://vulners.com/packetstorm/PACKETSTORM:94556 *EXPLOIT*
PACKETSTORM:140070 7.8 https://vulners.com/packetstorm/PACKETSTORM:140070 *EXPLOIT*
PACKETSTORM:101052 7.8 https://vulners.com/packetstorm/PACKETSTORM:101052 *EXPLOIT*
EXPLOITPACK:71D51B69AA2D3A74753D7A921EE79985 7.8 https://vulners.com/exploitpack/EXPLOITPACK:71D51B69AA2D3A74753D7A921EE79985 *EXPLOIT*
EXPLOITPACK:67F6569F63A082199721C069C852BBD7 7.8 https://vulners.com/exploitpack/EXPLOITPACK:67F6569F63A082199721C069C852BBD7 *EXPLOIT*
EXPLOITPACK:5BCA798C6BA71FAE29334297EC0B6A09 7.8 https://vulners.com/exploitpack/EXPLOITPACK:5BCA798C6BA71FAE29334297EC0B6A09 *EXPLOIT*
EDB-ID:40888 7.8 https://vulners.com/exploitdb/EDB-ID:40888 *EXPLOIT*
EDB-ID:24450 7.8 https://vulners.com/exploitdb/EDB-ID:24450 *EXPLOIT*
EDB-ID:15215 7.8 https://vulners.com/exploitdb/EDB-ID:15215 *EXPLOIT*
CVE-2020-15778 7.8 https://vulners.com/cve/CVE-2020-15778
CVE-2016-6515 7.8 https://vulners.com/cve/CVE-2016-6515
CVE-2016-10012 7.8 https://vulners.com/cve/CVE-2016-10012
CVE-2015-8325 7.8 https://vulners.com/cve/CVE-2015-8325
C94132FD-1FA5-5342-B6EE-0DAF45EEFFE3 7.8 https://vulners.com/githubexploit/C94132FD-1FA5-5342-B6EE-0DAF45EEFFE3 *EXPLOIT*
312165E3-7FD9-5769-BDA3-4129BE9114D6 7.8 https://vulners.com/githubexploit/312165E3-7FD9-5769-BDA3-4129BE9114D6 *EXPLOIT*
2E719186-2FED-58A8-A150-762EFBAAA523 7.8 https://vulners.com/gitee/2E719186-2FED-58A8-A150-762EFBAAA523 *EXPLOIT*
23CC97BE-7C95-513B-9E73-298C48D74432 7.8 https://vulners.com/githubexploit/23CC97BE-7C95-513B-9E73-298C48D74432 *EXPLOIT*
1337DAY-ID-26494 7.8 https://vulners.com/zdt/1337DAY-ID-26494 *EXPLOIT*
10213DBE-F683-58BB-B6D3-353173626207 7.8 https://vulners.com/githubexploit/10213DBE-F683-58BB-B6D3-353173626207 *EXPLOIT*
SSV:92579 7.5 https://vulners.com/seebug/SSV:92579 *EXPLOIT*
SSV:61450 7.5 https://vulners.com/seebug/SSV:61450 *EXPLOIT*
CVE-2016-10708 7.5 https://vulners.com/cve/CVE-2016-10708
CVE-2016-10009 7.5 https://vulners.com/cve/CVE-2016-10009
CVE-2014-1692 7.5 https://vulners.com/cve/CVE-2014-1692
CVE-2010-4478 7.5 https://vulners.com/cve/CVE-2010-4478
1337DAY-ID-26576 7.5 https://vulners.com/zdt/1337DAY-ID-26576 *EXPLOIT*
SSV:92582 7.2 https://vulners.com/seebug/SSV:92582 *EXPLOIT*
CVE-2016-10010 7.0 https://vulners.com/cve/CVE-2016-10010
SSV:92580 6.9 https://vulners.com/seebug/SSV:92580 *EXPLOIT*
CVE-2015-6564 6.9 https://vulners.com/cve/CVE-2015-6564
1337DAY-ID-26577 6.9 https://vulners.com/zdt/1337DAY-ID-26577 *EXPLOIT*
EDB-ID:46516 6.8 https://vulners.com/exploitdb/EDB-ID:46516 *EXPLOIT*
EDB-ID:46193 6.8 https://vulners.com/exploitdb/EDB-ID:46193 *EXPLOIT*
CVE-2019-6110 6.8 https://vulners.com/cve/CVE-2019-6110
CVE-2019-6109 6.8 https://vulners.com/cve/CVE-2019-6109

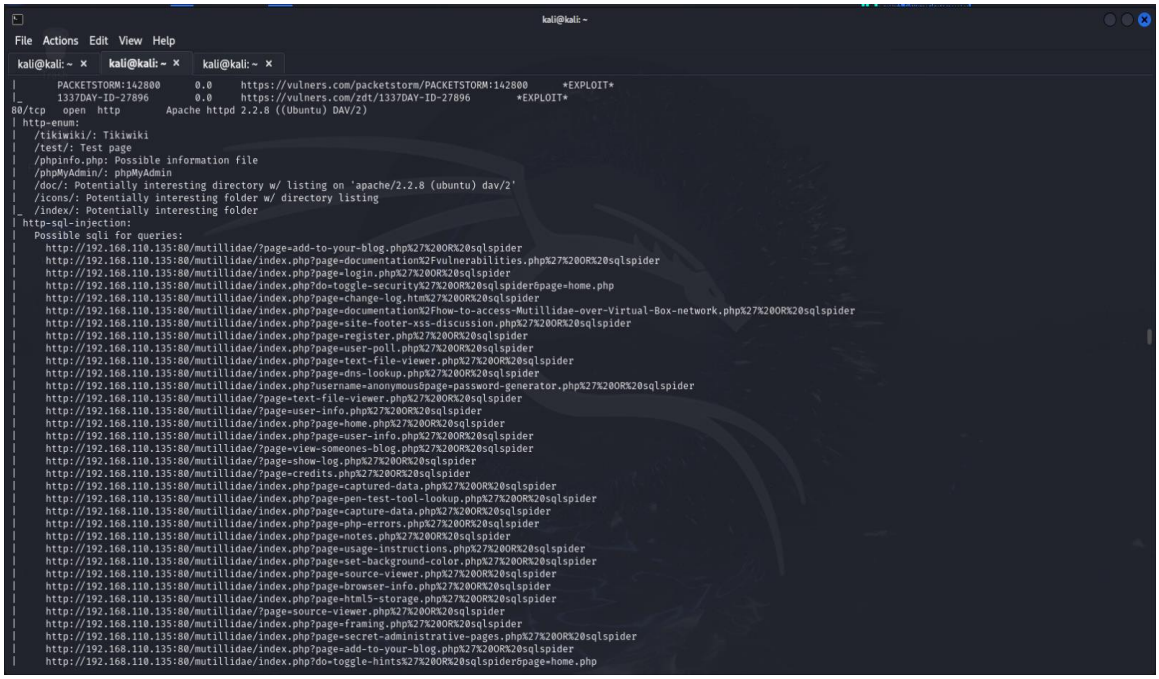

kali@kali: ~
File Actions Edit View Help
kali@kali: ~
kali@kali: ~
kali@kali: ~
CVE-2016-10708 7.5 https://vulners.com/cve/CVE-2016-10708
CVE-2016-10009 7.5 https://vulners.com/cve/CVE-2016-10009
CVE-2014-1692 7.5 https://vulners.com/cve/CVE-2014-1692
CVE-2010-4478 7.5 https://vulners.com/cve/CVE-2010-4478
1337DAY-ID-26576 7.5 https://vulners.com/zdt/1337DAY-ID-26576 *EXPLOIT*
SSV:92582 7.2 https://vulners.com/seebug/SSV:92582 *EXPLOIT*
CVE-2016-10010 7.0 https://vulners.com/cve/CVE-2016-10010
SSV:92580 6.9 https://vulners.com/seebug/SSV:92580 *EXPLOIT*
CVE-2015-6564 6.9 https://vulners.com/cve/CVE-2015-6564
1337DAY-ID-26577 6.9 https://vulners.com/zdt/1337DAY-ID-26577 *EXPLOIT*
EDB-ID:46516 6.8 https://vulners.com/exploitdb/EDB-ID:46516 *EXPLOIT*
EDB-ID:46193 6.8 https://vulners.com/exploitdb/EDB-ID:46193 *EXPLOIT*
CVE-2019-6110 6.8 https://vulners.com/cve/CVE-2019-6110
CVE-2019-6109 6.8 https://vulners.com/cve/CVE-2019-6109
1337DAY-ID-32328 6.8 https://vulners.com/zdt/1337DAY-ID-32328 *EXPLOIT*
1337DAY-ID-32009 6.8 https://vulners.com/zdt/1337DAY-ID-32009 *EXPLOIT*
D104D2BF-ED22-588B-A9B2-3CCC562FE8C0 6.5 https://vulners.com/githubexploit/D104D2BF-ED22-588B-A9B2-3CCC562FE8C0 *EXPLOIT*
CVE-2023-51385 6.5 https://vulners.com/cve/CVE-2023-51385
CVE-2008-1657 6.5 https://vulners.com/cve/CVE-2008-1657
C07ADB46-24B8-57B7-B375-9C761F4750A2 6.5 https://vulners.com/githubexploit/C07ADB46-24B8-57B7-B375-9C761F4750A2 *EXPLOIT*
A88CDD3E-67CC-51CC-97FB-AB0CACB6B08C 6.5 https://vulners.com/githubexploit/A88CDD3E-67CC-51CC-97FB-AB0CACB6B08C *EXPLOIT*
65B15AA1-2A8D-53C1-9499-69EBA3619F1C 6.5 https://vulners.com/githubexploit/65B15AA1-2A8D-53C1-9499-69EBA3619F1C *EXPLOIT*
5325A9D6-132B-590C-BDEF-0CB105252732 6.5 https://vulners.com/gitee/5325A9D6-132B-590C-BDEF-0CB105252732 *EXPLOIT*
530326CF-6AB3-5643-AA16-73DC8CB44742 6.5 https://vulners.com/githubexploit/530326CF-6AB3-5643-AA16-73DC8CB44742 *EXPLOIT*
EDB-ID:40858 6.4 https://vulners.com/exploitdb/EDB-ID:40858 *EXPLOIT*
EDB-ID:40119 6.4 https://vulners.com/exploitdb/EDB-ID:40119 *EXPLOIT*
EDB-ID:39569 6.4 https://vulners.com/exploitdb/EDB-ID:39569 *EXPLOIT*
CVE-2016-3115 6.4 https://vulners.com/cve/CVE-2016-3115
PACKETSTORM:181223 5.9 https://vulners.com/packetstorm/PACKETSTORM:181223 *EXPLOIT*
MSF:AUXILIARY-SCANNER-SSH-SSH_ENUMUSERS- 5.9 https://vulners.com/metasploit/MSF:AUXILIARY-SCANNER-SSH-SSH_ENUMUSERS- *EXPLOIT*
EDB-ID:40136 5.9 https://vulners.com/exploitdb/EDB-ID:40136 *EXPLOIT*
EDB-ID:40113 5.9 https://vulners.com/exploitdb/EDB-ID:40113 *EXPLOIT*
CVE-2023-48795 5.9 https://vulners.com/cve/CVE-2023-48795
CVE-2019-6111 5.9 https://vulners.com/cve/CVE-2019-6111
CVE-2016-6210 5.9 https://vulners.com/cve/CVE-2016-6210
A02ABE85-E4E3-5852-A59D-DF288CB8160A 5.9 https://vulners.com/githubexploit/A02ABE85-E4E3-5852-A59D-DF288CB8160A *EXPLOIT*
SSV:61911 5.8 https://vulners.com/seebug/SSV:61911 *EXPLOIT*
EXPLOITPACK:98FE96309F9524B8C84C508837551A19 5.8 https://vulners.com/exploitpack/EXPLOITPACK:98FE96309F9524B8C84C508837551A19 *EXPLOIT*
EXPLOITPACK:5330EA02EBDE345BFC9D6DDDD97F9E97 5.8 https://vulners.com/exploitpack/EXPLOITPACK:5330EA02EBDE345BFC9D6DDDD97F9E97 *EXPLOIT*
CVE-2014-2653 5.8 https://vulners.com/cve/CVE-2014-2653
CVE-2014-2532 5.8 https://vulners.com/cve/CVE-2014-2532
SSV:91041 5.5 https://vulners.com/seebug/SSV:91041 *EXPLOIT*
PACKETSTORM:140019 5.5 https://vulners.com/packetstorm/PACKETSTORM:140019 *EXPLOIT*
PACKETSTORM:136251 5.5 https://vulners.com/packetstorm/PACKETSTORM:136251 *EXPLOIT*
PACKETSTORM:136234 5.5 https://vulners.com/packetstorm/PACKETSTORM:136234 *EXPLOIT*
EXPLOITPACK:F92411A645D85F05BDBD274FD222226F 5.5 https://vulners.com/exploitpack/EXPLOITPACK:F92411A645D85F05BDBD274FD222226F *EXPLOIT*
EXPLOITPACK:9F2E746846C3C623A27A441281EAD138 5.5 https://vulners.com/exploitpack/EXPLOITPACK:9F2E746846C3C623A27A441281EAD138 *EXPLOIT*

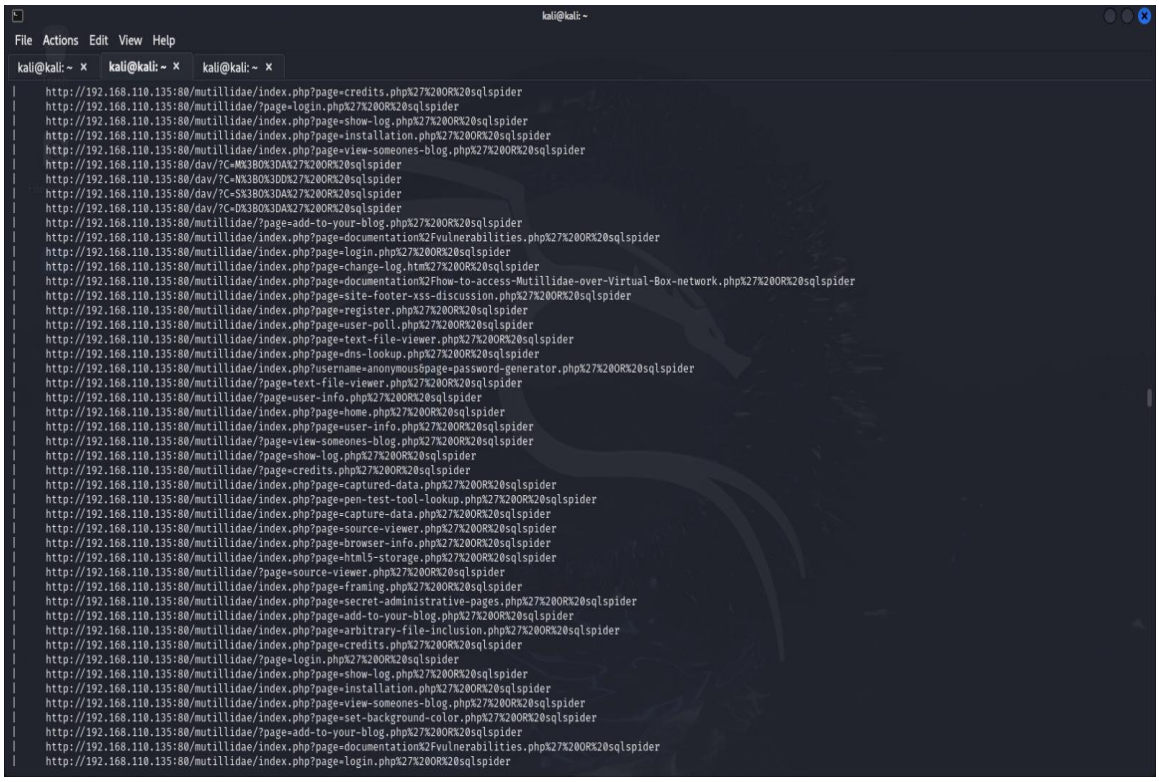

kali@kali: ~
File Actions Edit View Help
kali@kali: ~
kali@kali: ~
kali@kali: ~
| 1337DAY-ID-20301 0.0 https://vulners.com/zdt/1337DAY-ID-20301 *EXPLOIT*
| 1337DAY-ID-14373 0.0 https://vulners.com/zdt/1337DAY-ID-14373 *EXPLOIT*
23/tcp open telnet Linux telnetd
25/tcp open smtp Postfix smtpd
| ssl-poodle:
| VULNERABLE:
| SSL POODLE information leak
| State: VULNERABLE
| IDs: BID:70574 CVE:CVE-2014-3566
| The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and other
| products, uses nondeterministic CBC padding, which makes it easier
| for man-in-the-middle attackers to obtain cleartext data via a
| padding-oracle attack, aka the "POODLE" issue.
| Disclosure date: 2014-10-14
| Check results:
| TLS_RSA_WITH_AES_128_CBC_SHA
| References:
| https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-3566
| https://www.securityfocus.com/bid/70574
| https://www.imperialviolet.org/2014/10/14/poodle.html
| https://www.openssl.org/~bodo/ssl-poodle.pdf
| ssl-dh-params:
| VULNERABLE:
| Anonymous Diffie-Hellman Key Exchange MitM Vulnerability
| State: VULNERABLE
| Transport Layer Security (TLS) services that use anonymous
| Diffie-Hellman key exchange only provide protection against passive
| eavesdropping, and are vulnerable to active man-in-the-middle attacks
| which could completely compromise the confidentiality and integrity
| of any data exchanged over the resulting session.
| Check results:
| ANONYMOUS DH GROUP 1
| Cipher Suite: TLS_DH_anon_WITH_AES_128_CBC_SHA
| Modulus Type: Safe prime
| Modulus Source: postfix builtin
| Modulus Length: 1024
| Generator Length: 8
| Public Key Length: 1024
| References:
| https://www.ietf.org/rfc/rfc2246.txt
|
| Transport Layer Security (TLS) Protocol DHE_EXPORT Ciphers Downgrade MitM (Logjam)
| State: VULNERABLE
| IDs: BID:74733 CVE:CVE-2015-4000
| The Transport Layer Security (TLS) protocol contains a flaw that is
| triggered when handling Diffie-Hellman key exchanges defined with
| the DHE_EXPORT cipher. This may allow a man-in-the-middle attacker

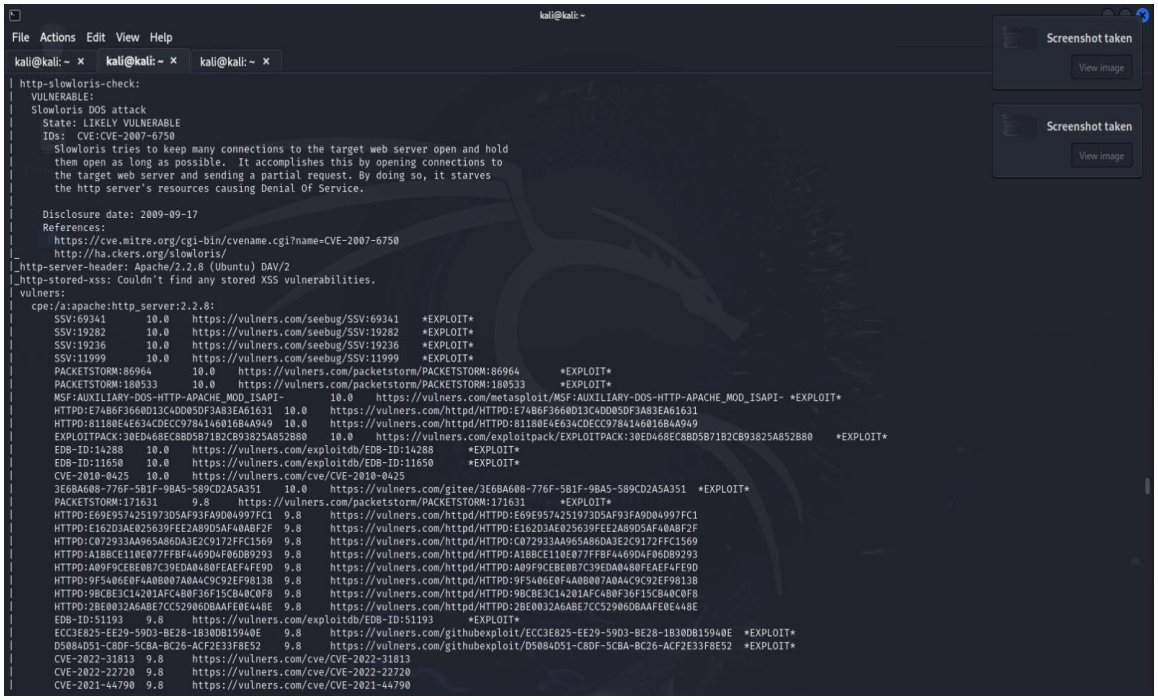

kali@kali: ~
File Actions Edit View Help
kali@kali: ~
kali@kali: ~
kali@kali: ~
| cryptography, which is significantly weaker, allowing the attacker
| to more easily break the encryption and monitor or tamper with
| the encrypted stream.
| Disclosure date: 2015-5-19
| Check results:
| EXPORT-GRADE DH GROUP 1
| Cipher Suite: TLS_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA
| Modulus Type: Safe prime
| Modulus Source: Unknown/Custom-generated
| Modulus Length: 512
| Generator Length: 8
| Public Key Length: 512
| References:
| https://www.securityfocus.com/bid/74733
| https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-4000
| https://weakdh.org
|
| Diffie-Hellman Key Exchange Insufficient Group Strength
| State: VULNERABLE
| Transport Layer Security (TLS) services that use Diffie-Hellman groups
| of insufficient strength, especially those using one of a few commonly
| shared groups, may be susceptible to passive eavesdropping attacks.
| Check results:
| WEAK DH GROUP 1
| Cipher Suite: TLS_DHE_RSA_WITH_AES_128_CBC_SHA
| Modulus Type: Safe prime
| Modulus Source: postfix builtin
| Modulus Length: 1024
| Generator Length: 8
| Public Key Length: 1024
| References:
| https://weakdh.org
|_sslv2-drown: ERROR: Script execution failed (use -d to debug)
| smtp-vuln-cve2010-4344:
|_ The SMTP server is not Exim: NOT VULNERABLE
53/tcp open domain ISC BIND 9.4.2
| vulners:
| cpe:/a:isc:bind:9.4.2:
| SSV:2853 10.0 https://vulners.com/seebug/SSV:2853 *EXPLOIT*
| CVE-2008-0122 10.0 https://vulners.com/cve/CVE-2008-0122
| CVE-2021-25216 9.8 https://vulners.com/cve/CVE-2021-25216
| CVE-2020-8616 8.6 https://vulners.com/cve/CVE-2020-8616
| CVE-2016-1286 8.6 https://vulners.com/cve/CVE-2016-1286
| SSV:60184 8.5 https://vulners.com/seebug/SSV:60184 *EXPLOIT*
| CVE-2012-1667 8.5 https://vulners.com/cve/CVE-2012-1667
| SSV:60292 7.8 https://vulners.com/seebug/SSV:60292 *EXPLOIT*
| PACKETSTORM:180552 7.8 https://vulners.com/packetstorm/PACKETSTORM:180552 *EXPLOIT*


kali@kali: ~
File Actions Edit View Help
kali@kali: ~ ×
kali@kali: ~ ×
kali@kali: ~ ×
SSV:60292 7.8 https://vulners.com/seebug/SSV:60292 *EXPLOIT*
PACKETSTORM:180552 7.8 https://vulners.com/packetstorm/PACKETSTORM:180552 *EXPLOIT*
PACKETSTORM:180551 7.8 https://vulners.com/packetstorm/PACKETSTORM:180551 *EXPLOIT*
PACKETSTORM:138960 7.8 https://vulners.com/packetstorm/PACKETSTORM:138960 *EXPLOIT*
PACKETSTORM:132926 7.8 https://vulners.com/packetstorm/PACKETSTORM:132926 *EXPLOIT*
MSF:AUXILIARY-DOS-DNS-BIND_TKEY- 7.8 https://vulners.com/metasploit/MSF:AUXILIARY-DOS-DNS-BIND_TKEY- *EXPLOIT*
EXPLOITPACK:BE4F638B632EA0754155A27ECC4B3D3F 7.8 https://vulners.com/exploitpack/EXPLOITPACK:BE4F638B632EA0754155A27ECC4B3D3F *EXPLOIT*
EXPLOITPACK:46DEBFAC850194C04C54F93E0DFF5F4F 7.8 https://vulners.com/exploitpack/EXPLOITPACK:46DEBFAC850194C04C54F93E0DFF5F4F *EXPLOIT*
EXPLOITPACK:09762DB0197BBAAAB6FC79F24F0D2A74 7.8 https://vulners.com/exploitpack/EXPLOITPACK:09762DB0197BBAAAB6FC79F24F0D2A74 *EXPLOIT*
EDB-ID:42121 7.8 https://vulners.com/exploitdb/EDB-ID:42121 *EXPLOIT*
EDB-ID:40453 7.8 https://vulners.com/exploitdb/EDB-ID:40453 *EXPLOIT*
EDB-ID:37723 7.8 https://vulners.com/exploitdb/EDB-ID:37723 *EXPLOIT*
EDB-ID:37721 7.8 https://vulners.com/exploitdb/EDB-ID:37721 *EXPLOIT*
CVE-2017-3141 7.8 https://vulners.com/cve/CVE-2017-3141
CVE-2016-2776 7.8 https://vulners.com/cve/CVE-2016-2776
CVE-2015-5722 7.8 https://vulners.com/cve/CVE-2015-5722
CVE-2015-5477 7.8 https://vulners.com/cve/CVE-2015-5477
CVE-2014-8500 7.8 https://vulners.com/cve/CVE-2014-8500
CVE-2012-5166 7.8 https://vulners.com/cve/CVE-2012-5166
CVE-2012-4244 7.8 https://vulners.com/cve/CVE-2012-4244
CVE-2012-3817 7.8 https://vulners.com/cve/CVE-2012-3817
CVE-2008-4163 7.8 https://vulners.com/cve/CVE-2008-4163
1337DAY-ID-25325 7.8 https://vulners.com/zdt/1337DAY-ID-25325 *EXPLOIT*
1337DAY-ID-23970 7.8 https://vulners.com/zdt/1337DAY-ID-23970 *EXPLOIT*
1337DAY-ID-23960 7.8 https://vulners.com/zdt/1337DAY-ID-23960 *EXPLOIT*
1337DAY-ID-23948 7.8 https://vulners.com/zdt/1337DAY-ID-23948 *EXPLOIT*
CVE-2010-0382 7.6 https://vulners.com/cve/CVE-2010-0382
PACKETSTORM:180550 7.5 https://vulners.com/packetstorm/PACKETSTORM:180550 *EXPLOIT*
MSF:AUXILIARY-DOS-DNS-BIND_TSIG_BADTIME- 7.5 https://vulners.com/metasploit/MSF:AUXILIARY-DOS-DNS-BIND_TSIG_BADTIME- *EXPLOIT*
MSF:AUXILIARY-DOS-DNS-BIND_TSIG- 7.5 https://vulners.com/metasploit/MSF:AUXILIARY-DOS-DNS-BIND_TSIG- *EXPLOIT*
FBC03933-7A65-52F3-83F4-4B2253A490B6 7.5 https://vulners.com/githubexploit/FBC03933-7A65-52F3-83F4-4B2253A490B6 *EXPLOIT*
CVE-2023-50387 7.5 https://vulners.com/cve/CVE-2023-50387
CVE-2023-4408 7.5 https://vulners.com/cve/CVE-2023-4408
CVE-2023-3341 7.5 https://vulners.com/cve/CVE-2023-3341
CVE-2021-25215 7.5 https://vulners.com/cve/CVE-2021-25215
CVE-2020-8617 7.5 https://vulners.com/cve/CVE-2020-8617
CVE-2017-3145 7.5 https://vulners.com/cve/CVE-2017-3145
CVE-2017-3143 7.5 https://vulners.com/cve/CVE-2017-3143
CVE-2016-9444 7.5 https://vulners.com/cve/CVE-2016-9444
CVE-2016-9131 7.5 https://vulners.com/cve/CVE-2016-9131
CVE-2016-8864 7.5 https://vulners.com/cve/CVE-2016-8864
CVE-2016-2848 7.5 https://vulners.com/cve/CVE-2016-2848
CVE-2009-0265 7.5 https://vulners.com/cve/CVE-2009-0265
9ED8A03D-FE34-5F77-8C66-C03C9615AF07 7.5 https://vulners.com/gitee/9ED8A03D-FE34-5F77-8C66-C03C9615AF07 *EXPLOIT*
1337DAY-ID-34485 7.5 https://vulners.com/zdt/1337DAY-ID-34485 *EXPLOIT*
EXPLOITPACK:D6DDF5E24DE171DAAD71FD95FC1B67F2 7.2 https://vulners.com/exploitpack/EXPLOITPACK:D6DDF5E24DE171DAAD71FD95FC1B67F2 *EXPLOIT*
CVE-2015-8461 7.1 https://vulners.com/cve/CVE-2015-8461

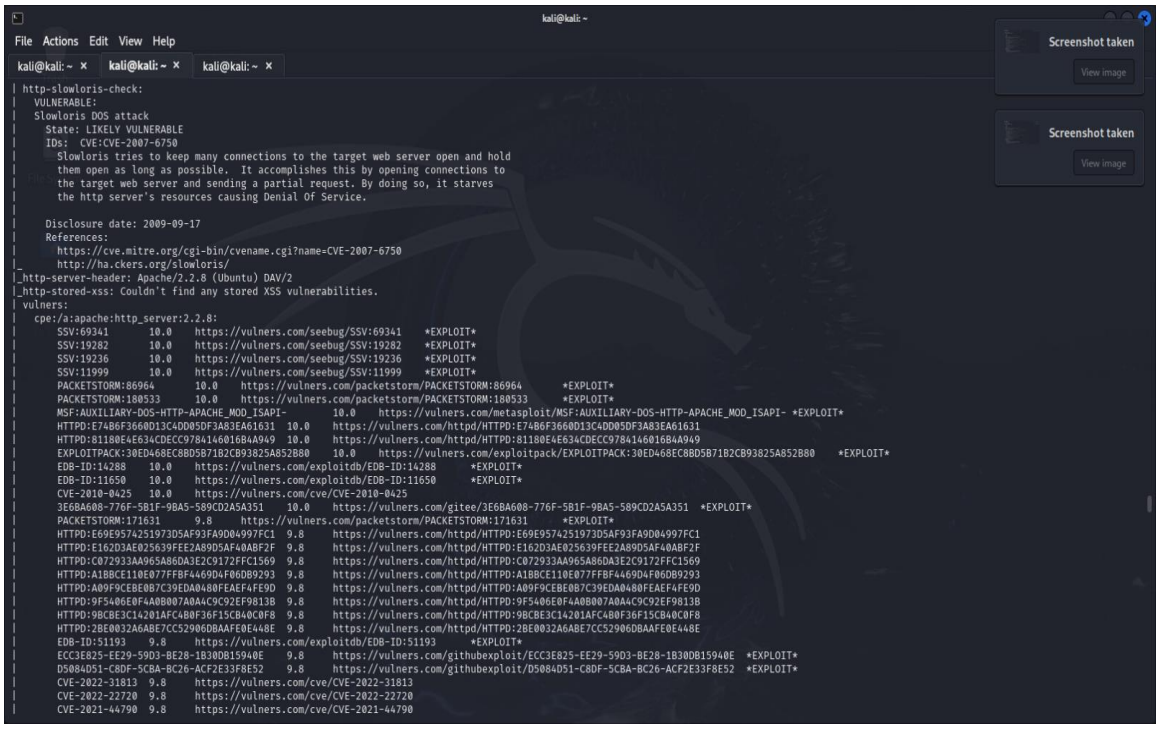

kali@kali: ~
File Actions Edit View Help
kali@kali: ~ ×
kali@kali: ~ ×
kali@kali: ~ ×
PACKETSTORM:180550 7.5 https://vulners.com/packetstorm/PACKETSTORM:180550 *EXPLOIT*
MSF:AUXILIARY-DOS-DNS-BIND_TSIG_BADTIME- 7.5 https://vulners.com/metasploit/MSF:AUXILIARY-DOS-DNS-BIND_TSIG_BADTIME- *EXPLOIT*
MSF:AUXILIARY-DOS-DNS-BIND_TSIG- 7.5 https://vulners.com/metasploit/MSF:AUXILIARY-DOS-DNS-BIND_TSIG- *EXPLOIT*
FBC03933-7A65-52F3-83F4-4B2253A490B6 7.5 https://vulners.com/githubexploit/FBC03933-7A65-52F3-83F4-4B2253A490B6 *EXPLOIT*
CVE-2023-50387 7.5 https://vulners.com/cve/CVE-2023-50387
CVE-2023-4408 7.5 https://vulners.com/cve/CVE-2023-4408
CVE-2023-3341 7.5 https://vulners.com/cve/CVE-2023-3341
CVE-2021-25215 7.5 https://vulners.com/cve/CVE-2021-25215
CVE-2020-8617 7.5 https://vulners.com/cve/CVE-2020-8617
CVE-2017-3145 7.5 https://vulners.com/cve/CVE-2017-3145
CVE-2017-3143 7.5 https://vulners.com/cve/CVE-2017-3143
CVE-2016-9444 7.5 https://vulners.com/cve/CVE-2016-9444
CVE-2016-9131 7.5 https://vulners.com/cve/CVE-2016-9131
CVE-2016-8864 7.5 https://vulners.com/cve/CVE-2016-8864
CVE-2016-2848 7.5 https://vulners.com/cve/CVE-2016-2848
CVE-2009-0265 7.5 https://vulners.com/cve/CVE-2009-0265
9ED8A03D-FE34-5F77-8C66-C03C9615AF07 7.5 https://vulners.com/gitee/9ED8A03D-FE34-5F77-8C66-C03C9615AF07 *EXPLOIT*
1337DAY-ID-34485 7.5 https://vulners.com/zdt/1337DAY-ID-34485 *EXPLOIT*
EXPLOITPACK:D6DDF5E24DE171DAAD71FD95FC1B67F2 7.2 https://vulners.com/exploitpack/EXPLOITPACK:D6DDF5E24DE171DAAD71FD95FC1B67F2 *EXPLOIT*
CVE-2015-8461 7.1 https://vulners.com/cve/CVE-2015-8461
CVE-2015-5986 7.1 https://vulners.com/cve/CVE-2015-5986
CVE-2015-8705 7.0 https://vulners.com/cve/CVE-2015-8705
CVE-2016-1285 6.8 https://vulners.com/cve/CVE-2016-1285
CVE-2015-8704 6.8 https://vulners.com/cve/CVE-2015-8704
CVE-2009-0025 6.8 https://vulners.com/cve/CVE-2009-0025
CVE-2020-8622 6.5 https://vulners.com/cve/CVE-2020-8622
CVE-2018-5741 6.5 https://vulners.com/cve/CVE-2018-5741
CVE-2016-6170 6.5 https://vulners.com/cve/CVE-2016-6170
CVE-2010-3614 6.4 https://vulners.com/cve/CVE-2010-3614
CVE-2016-2775 5.9 https://vulners.com/cve/CVE-2016-2775
SSV:4636 5.8 https://vulners.com/seebug/SSV:4636 *EXPLOIT*
CVE-2022-2795 5.3 https://vulners.com/cve/CVE-2022-2795
CVE-2021-25219 5.3 https://vulners.com/cve/CVE-2021-25219
CVE-2017-3142 5.3 https://vulners.com/cve/CVE-2017-3142
SSV:30099 5.0 https://vulners.com/seebug/SSV:30099 *EXPLOIT*
SSV:20595 5.0 https://vulners.com/seebug/SSV:20595 *EXPLOIT*
PACKETSTORM:157836 5.0 https://vulners.com/packetstorm/PACKETSTORM:157836 *EXPLOIT*
CVE-2015-8000 5.0 https://vulners.com/cve/CVE-2015-8000
CVE-2012-1033 5.0 https://vulners.com/cve/CVE-2012-1033
CVE-2011-4313 5.0 https://vulners.com/cve/CVE-2011-4313
CVE-2011-1910 5.0 https://vulners.com/cve/CVE-2011-1910
SSV:11919 4.3 https://vulners.com/seebug/SSV:11919 *EXPLOIT*
CVE-2010-3762 4.3 https://vulners.com/cve/CVE-2010-3762
CVE-2010-0097 4.3 https://vulners.com/cve/CVE-2010-0097
CVE-2009-0696 4.3 https://vulners.com/cve/CVE-2009-0696
CVE-2010-0290 4.0 https://vulners.com/cve/CVE-2010-0290
SSV:14986 2.6 https://vulners.com/seebug/SSV:14986 *EXPLOIT*


kali@kali: ~
File Actions Edit View Help
kali@kali: ~ ×
kali@kali: ~ ×
kali@kali: ~ ×
| PACKETSTORM:142800 0.0 https://vulners.com/packetstorm/PACKETSTORM:142800 *EXPLOIT*
|_ 1337DAY-ID-27896 0.0 https://vulners.com/zdt/1337DAY-ID-27896 *EXPLOIT*
80/tcp open http Apache httpd 2.2.8 ((Ubuntu) DAV/2)
| http-enum:
| /tikiwiki/: Tikiwiki
| /test/: Test page
| /phpinfo.php: Possible information file
| /phpMyAdmin/: phpMyAdmin
| /doc/: Potentially interesting directory w/ listing on 'apache/2.2.8 (ubuntu) dav/2'
| /icons/: Potentially interesting folder w/ directory listing
|_ /index/: Potentially interesting folder
| http-sql-injection:
| Possible sqli for queries:
| http://192.168.110.135:80/mutillidae/?page=add-to-your-blog.php%27%20OR%20sqlspider
| http://192.168.110.135:80/mutillidae/index.php?page=documentation%2Fvulnerabilities.php%27%20OR%20sqlspider
| http://192.168.110.135:80/mutillidae/index.php?page=login.php%27%20OR%20sqlspider
| http://192.168.110.135:80/mutillidae/index.php?do=toggle-security%27%20OR%20sqlspider&page=home.php
| http://192.168.110.135:80/mutillidae/index.php?page=change-log.htm%27%20OR%20sqlspider
| http://192.168.110.135:80/mutillidae/index.php?page=documentation%2Fhow-to-access-Mutillidae-over-Virtual-Box-network.php%27%20OR%20sqlspider
| http://192.168.110.135:80/mutillidae/index.php?page=site-footer-xss-discussion.php%27%20OR%20sqlspider
| http://192.168.110.135:80/mutillidae/index.php?page=register.php%27%20OR%20sqlspider
| http://192.168.110.135:80/mutillidae/index.php?page=user-poll.php%27%20OR%20sqlspider
| http://192.168.110.135:80/mutillidae/index.php?page=text-file-viewer.php%27%20OR%20sqlspider
| http://192.168.110.135:80/mutillidae/index.php?page=dns-lookup.php%27%20OR%20sqlspider
| http://192.168.110.135:80/mutillidae/index.php?username=anonymous&page=password-generator.php%27%20OR%20sqlspider
| http://192.168.110.135:80/mutillidae/?page=text-file-viewer.php%27%20OR%20sqlspider
| http://192.168.110.135:80/mutillidae/?page=user-info.php%27%20OR%20sqlspider
| http://192.168.110.135:80/mutillidae/index.php?page=home.php%27%20OR%20sqlspider
| http://192.168.110.135:80/mutillidae/index.php?page=user-info.php%27%20OR%20sqlspider
| http://192.168.110.135:80/mutillidae/?page=view-someones-blog.php%27%20OR%20sqlspider
| http://192.168.110.135:80/mutillidae/?page=show-log.php%27%20OR%20sqlspider
| http://192.168.110.135:80/mutillidae/?page=credits.php%27%20OR%20sqlspider
| http://192.168.110.135:80/mutillidae/index.php?page=captured-data.php%27%20OR%20sqlspider
| http://192.168.110.135:80/mutillidae/index.php?page=pen-test-tool-lookup.php%27%20OR%20sqlspider
| http://192.168.110.135:80/mutillidae/index.php?page=capture-data.php%27%20OR%20sqlspider
| http://192.168.110.135:80/mutillidae/index.php?page=php-errors.php%27%20OR%20sqlspider
| http://192.168.110.135:80/mutillidae/index.php?page=notes.php%27%20OR%20sqlspider
| http://192.168.110.135:80/mutillidae/index.php?page=usage-instructions.php%27%20OR%20sqlspider
| http://192.168.110.135:80/mutillidae/index.php?page=set-background-color.php%27%20OR%20sqlspider
| http://192.168.110.135:80/mutillidae/index.php?page=source-viewer.php%27%20OR%20sqlspider
| http://192.168.110.135:80/mutillidae/index.php?page=browser-info.php%27%20OR%20sqlspider
| http://192.168.110.135:80/mutillidae/index.php?page=html5-storage.php%27%20OR%20sqlspider
| http://192.168.110.135:80/mutillidae/?page=source-viewer.php%27%20OR%20sqlspider
| http://192.168.110.135:80/mutillidae/index.php?page=framing.php%27%20OR%20sqlspider
| http://192.168.110.135:80/mutillidae/index.php?page=secret-administrative-pages.php%27%20OR%20sqlspider
| http://192.168.110.135:80/mutillidae/index.php?page=add-to-your-blog.php%27%20OR%20sqlspider
| http://192.168.110.135:80/mutillidae/index.php?do=toggle-hints%27%20OR%20sqlspider&page=home.php

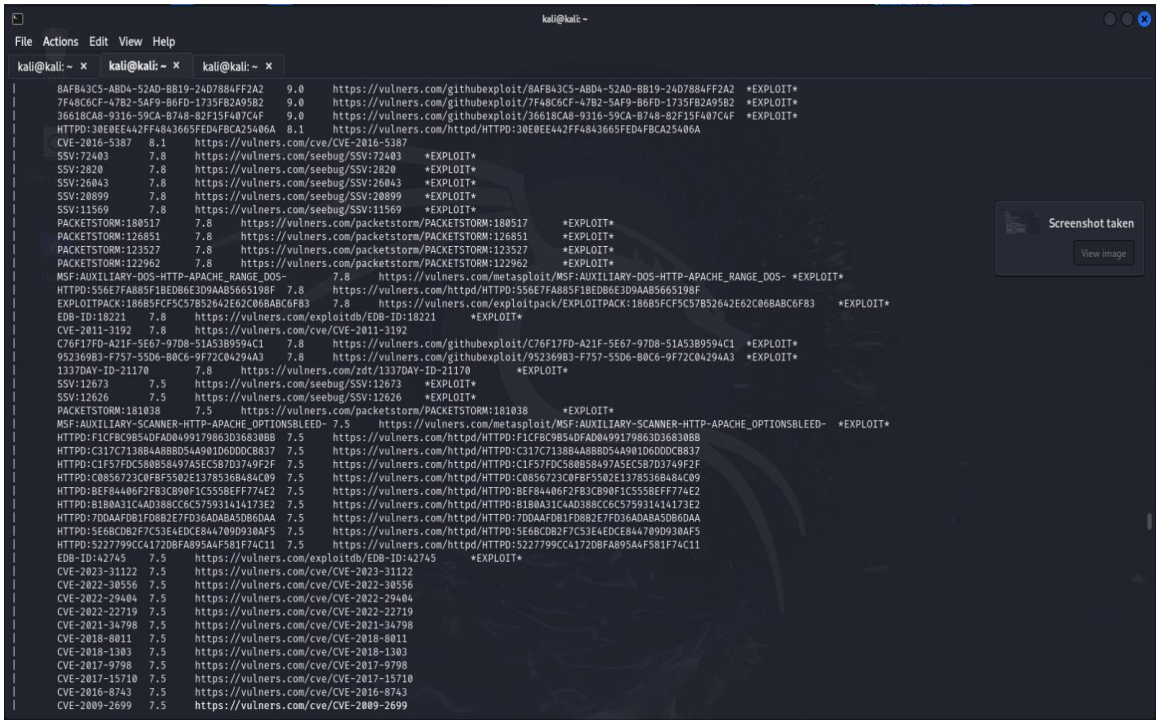

kali@kali: ~
File Actions Edit View Help
kali@kali: ~ ×
kali@kali: ~ ×
kali@kali: ~ ×
| http://192.168.110.135:80/mutillidae/index.php?page=credits.php%27%20OR%20sqlspider
| http://192.168.110.135:80/mutillidae/?page=login.php%27%20OR%20sqlspider
| http://192.168.110.135:80/mutillidae/index.php?page=show-log.php%27%20OR%20sqlspider
| http://192.168.110.135:80/mutillidae/index.php?page=installation.php%27%20OR%20sqlspider
| http://192.168.110.135:80/mutillidae/index.php?page=view-someones-blog.php%27%20OR%20sqlspider
| http://192.168.110.135:80/dav/?C=M%3BO%3DA%27%20OR%20sqlspider
| http://192.168.110.135:80/dav/?C=N%3BO%3DD%27%20OR%20sqlspider
| http://192.168.110.135:80/dav/?C=S%3BO%3DA%27%20OR%20sqlspider
| http://192.168.110.135:80/dav/?C=D%3BO%3DA%27%20OR%20sqlspider
| http://192.168.110.135:80/mutillidae/?page=add-to-your-blog.php%27%20OR%20sqlspider
| http://192.168.110.135:80/mutillidae/index.php?page=documentation%2Fvulnerabilities.php%27%20OR%20sqlspider
| http://192.168.110.135:80/mutillidae/index.php?page=login.php%27%20OR%20sqlspider
| http://192.168.110.135:80/mutillidae/index.php?page=change-log.htm%27%20OR%20sqlspider
| http://192.168.110.135:80/mutillidae/index.php?page=documentation%2Fhow-to-access-Mutillidae-over-Virtual-Box-network.php%27%20OR%20sqlspider
| http://192.168.110.135:80/mutillidae/index.php?page=site-footer-xss-discussion.php%27%20OR%20sqlspider
| http://192.168.110.135:80/mutillidae/index.php?page=register.php%27%20OR%20sqlspider
| http://192.168.110.135:80/mutillidae/index.php?page=user-poll.php%27%20OR%20sqlspider
| http://192.168.110.135:80/mutillidae/index.php?page=text-file-viewer.php%27%20OR%20sqlspider
| http://192.168.110.135:80/mutillidae/index.php?page=dns-lookup.php%27%20OR%20sqlspider
| http://192.168.110.135:80/mutillidae/index.php?username=anonymous&page=password-generator.php%27%20OR%20sqlspider
| http://192.168.110.135:80/mutillidae/?page=text-file-viewer.php%27%20OR%20sqlspider
| http://192.168.110.135:80/mutillidae/?page=user-info.php%27%20OR%20sqlspider
| http://192.168.110.135:80/mutillidae/index.php?page=home.php%27%20OR%20sqlspider
| http://192.168.110.135:80/mutillidae/index.php?page=user-info.php%27%20OR%20sqlspider
| http://192.168.110.135:80/mutillidae/?page=view-someones-blog.php%27%20OR%20sqlspider
| http://192.168.110.135:80/mutillidae/?page=show-log.php%27%20OR%20sqlspider
| http://192.168.110.135:80/mutillidae/?page=credits.php%27%20OR%20sqlspider
| http://192.168.110.135:80/mutillidae/index.php?page=captured-data.php%27%20OR%20sqlspider
| http://192.168.110.135:80/mutillidae/index.php?page=pen-test-tool-lookup.php%27%20OR%20sqlspider
| http://192.168.110.135:80/mutillidae/index.php?page=capture-data.php%27%20OR%20sqlspider
| http://192.168.110.135:80/mutillidae/index.php?page=source-viewer.php%27%20OR%20sqlspider
| http://192.168.110.135:80/mutillidae/index.php?page=browser-info.php%27%20OR%20sqlspider
| http://192.168.110.135:80/mutillidae/index.php?page=html5-storage.php%27%20OR%20sqlspider
| http://192.168.110.135:80/mutillidae/?page=source-viewer.php%27%20OR%20sqlspider
| http://192.168.110.135:80/mutillidae/index.php?page=framing.php%27%20OR%20sqlspider
| http://192.168.110.135:80/mutillidae/index.php?page=secret-administrative-pages.php%27%20OR%20sqlspider
| http://192.168.110.135:80/mutillidae/index.php?page=add-to-your-blog.php%27%20OR%20sqlspider
| http://192.168.110.135:80/mutillidae/index.php?page=arbitrary-file-inclusion.php%27%20OR%20sqlspider
| http://192.168.110.135:80/mutillidae/index.php?page=credits.php%27%20OR%20sqlspider
| http://192.168.110.135:80/mutillidae/?page=login.php%27%20OR%20sqlspider
| http://192.168.110.135:80/mutillidae/index.php?page=show-log.php%27%20OR%20sqlspider
| http://192.168.110.135:80/mutillidae/index.php?page=installation.php%27%20OR%20sqlspider
| http://192.168.110.135:80/mutillidae/index.php?page=view-someones-blog.php%27%20OR%20sqlspider
| http://192.168.110.135:80/mutillidae/index.php?page=set-background-color.php%27%20OR%20sqlspider
| http://192.168.110.135:80/mutillidae/?page=add-to-your-blog.php%27%20OR%20sqlspider
| http://192.168.110.135:80/mutillidae/index.php?page=documentation%2Fvulnerabilities.php%27%20OR%20sqlspider
| http://192.168.110.135:80/mutillidae/index.php?page=login.php%27%20OR%20sqlspider

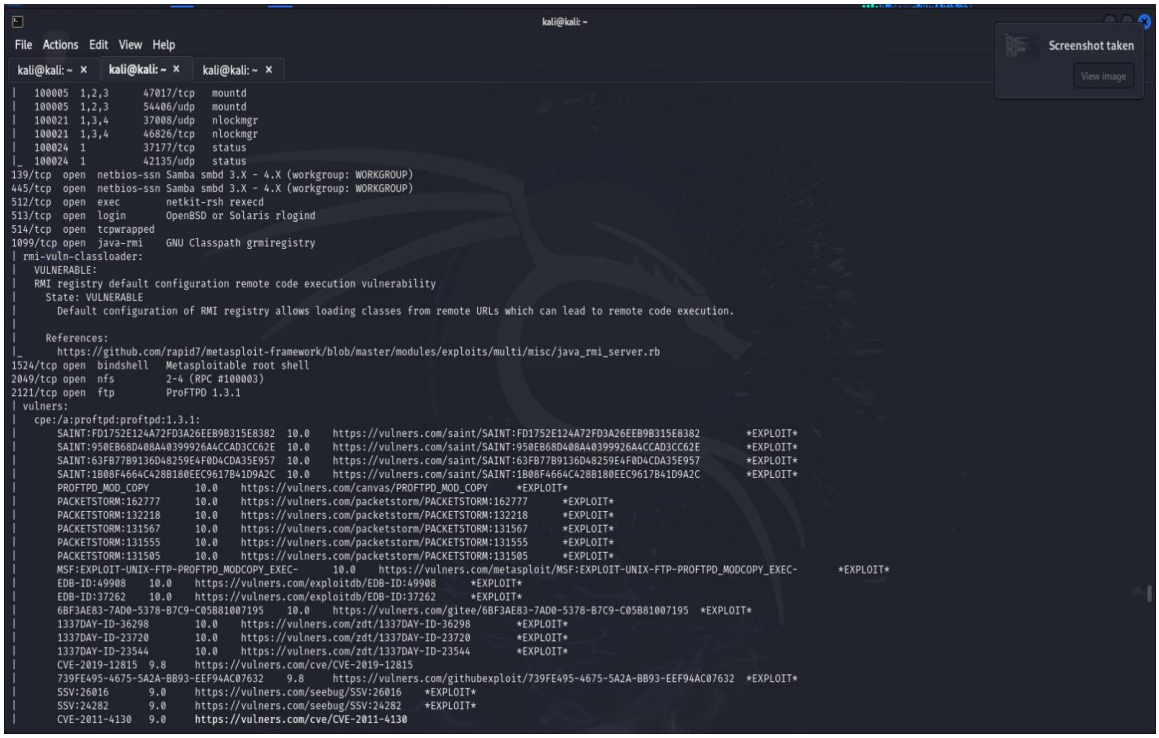


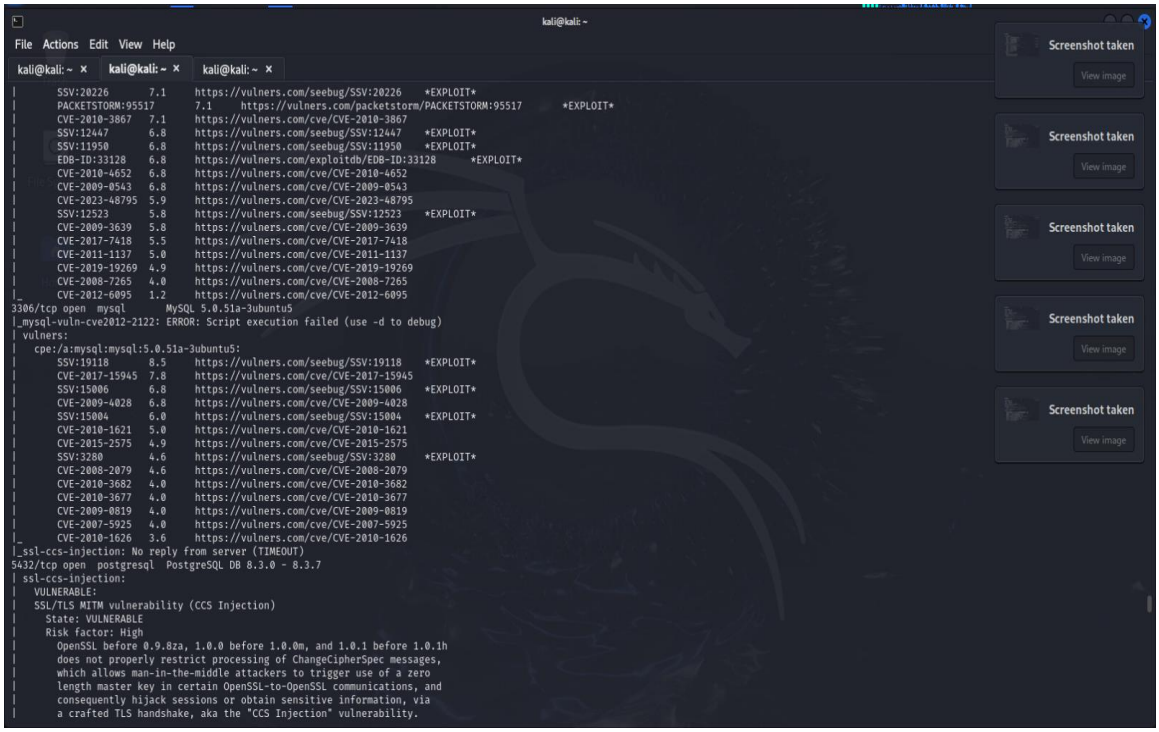

```
| http-slowloris-check:
|   VULNERABLE:
|   Slowloris DOS attack
|     State: LIKELY VULNERABLE
|     IDs:  CVE:CVE-2007-6750
|       Slowloris tries to keep many connections to the target web server open and hold
|       them open as long as possible.  It accomplishes this by opening connections to
|       the target web server and sending a partial request. By doing so, it starves
|       the http server's resources causing Denial Of Service.
|
|     Disclosure date: 2009-09-17
|     References:
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-6750
|_      http://ha.ckers.org/slowloris/
|_http-server-header: Apache/2.2.8 (Ubuntu) DAV/2
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
| vulners:
|   cpe:/a:apache:http_server:2.2.8:
|       SSV:69341       10.0    https://vulners.com/seebug/SSV:69341    *EXPLOIT*
|       SSV:19282       10.0    https://vulners.com/seebug/SSV:19282    *EXPLOIT*
|       SSV:19236       10.0    https://vulners.com/seebug/SSV:19236    *EXPLOIT*
|       SSV:11999       10.0    https://vulners.com/seebug/SSV:11999    *EXPLOIT*
|       PACKETSTORM:86964       10.0    https://vulners.com/packetstorm/PACKETSTORM:86964       *EXPLOIT*
|       PACKETSTORM:180533      10.0    https://vulners.com/packetstorm/PACKETSTORM:180533      *EXPLOIT*
|       MSF:AUXILIARY-DOS-HTTP-APACHE_MOD_ISAPI-       10.0    https://vulners.com/metasploit/MSF:AUXILIARY-DOS-HTTP-APACHE_MOD_ISAPI- *EXPLOIT*
|       HTTPD:E74B6F3660D13C4DD05DF3A83EA61631  10.0    https://vulners.com/httpd/HTTPD:E74B6F3660D13C4DD05DF3A83EA61631
|       HTTPD:81180E4E634CDECC9784146016B4A949  10.0    https://vulners.com/httpd/HTTPD:81180E4E634CDECC9784146016B4A949
|       EXPLOITPACK:30ED468EC8BD5B71B2CB93825A852B80    10.0    https://vulners.com/exploitpack/EXPLOITPACK:30ED468EC8BD5B71B2CB93825A852B80    *EXPLOIT*
|       EDB-ID:14288    10.0    https://vulners.com/exploitdb/EDB-ID:14288      *EXPLOIT*
|       EDB-ID:11650    10.0    https://vulners.com/exploitdb/EDB-ID:11650      *EXPLOIT*
|       CVE-2010-0425   10.0    https://vulners.com/cve/CVE-2010-0425
|       3E6BA608-776F-5B1F-9BA5-589CD2A5A351    10.0    https://vulners.com/gitee/3E6BA608-776F-5B1F-9BA5-589CD2A5A351  *EXPLOIT*
|       PACKETSTORM:171631      9.8     https://vulners.com/packetstorm/PACKETSTORM:171631      *EXPLOIT*
|       HTTPD:E69E9574251973D5AF93FA9D04997FC1  9.8     https://vulners.com/httpd/HTTPD:E69E9574251973D5AF93FA9D04997FC1
|       HTTPD:E162D3AE025639FEE2A89D5AF40ABF2F  9.8     https://vulners.com/httpd/HTTPD:E162D3AE025639FEE2A89D5AF40ABF2F
|       HTTPD:C072933AA965A86DA3E2C9172FFC1569  9.8     https://vulners.com/httpd/HTTPD:C072933AA965A86DA3E2C9172FFC1569
|       HTTPD:A1BBCE110E077FFBF4469D4F06DB9293  9.8     https://vulners.com/httpd/HTTPD:A1BBCE110E077FFBF4469D4F06DB9293
|       HTTPD:A09F9CEBE0B7C39EDA0480FEAEF4FE9D  9.8     https://vulners.com/httpd/HTTPD:A09F9CEBE0B7C39EDA0480FEAEF4FE9D
|       HTTPD:9F5406E0F4A0B007A0A4C9C92EF9813B  9.8     https://vulners.com/httpd/HTTPD:9F5406E0F4A0B007A0A4C9C92EF9813B
|       HTTPD:9BCBE3C14201AFC4B0F36F15CB40C0F8  9.8     https://vulners.com/httpd/HTTPD:9BCBE3C14201AFC4B0F36F15CB40C0F8
|       HTTPD:2BE0032A6ABE7CC52906DBAAFE0E448E  9.8     https://vulners.com/httpd/HTTPD:2BE0032A6ABE7CC52906DBAAFE0E448E
|       EDB-ID:51193    9.8     https://vulners.com/exploitdb/EDB-ID:51193      *EXPLOIT*
|       ECC3E825-EE29-59D3-BE28-1B30DB15940E    9.8     https://vulners.com/githubexploit/ECC3E825-EE29-59D3-BE28-1B30DB15940E  *EXPLOIT*
|       D5084D51-C8DF-5CBA-BC26-ACF2E33F8E52    9.8     https://vulners.com/githubexploit/D5084D51-C8DF-5CBA-BC26-ACF2E33F8E52  *EXPLOIT*
|       CVE-2022-31813  9.8     https://vulners.com/cve/CVE-2022-31813
|       CVE-2022-22720  9.8     https://vulners.com/cve/CVE-2022-22720
|       CVE-2021-44790  9.8     https://vulners.com/cve/CVE-2021-44790
```

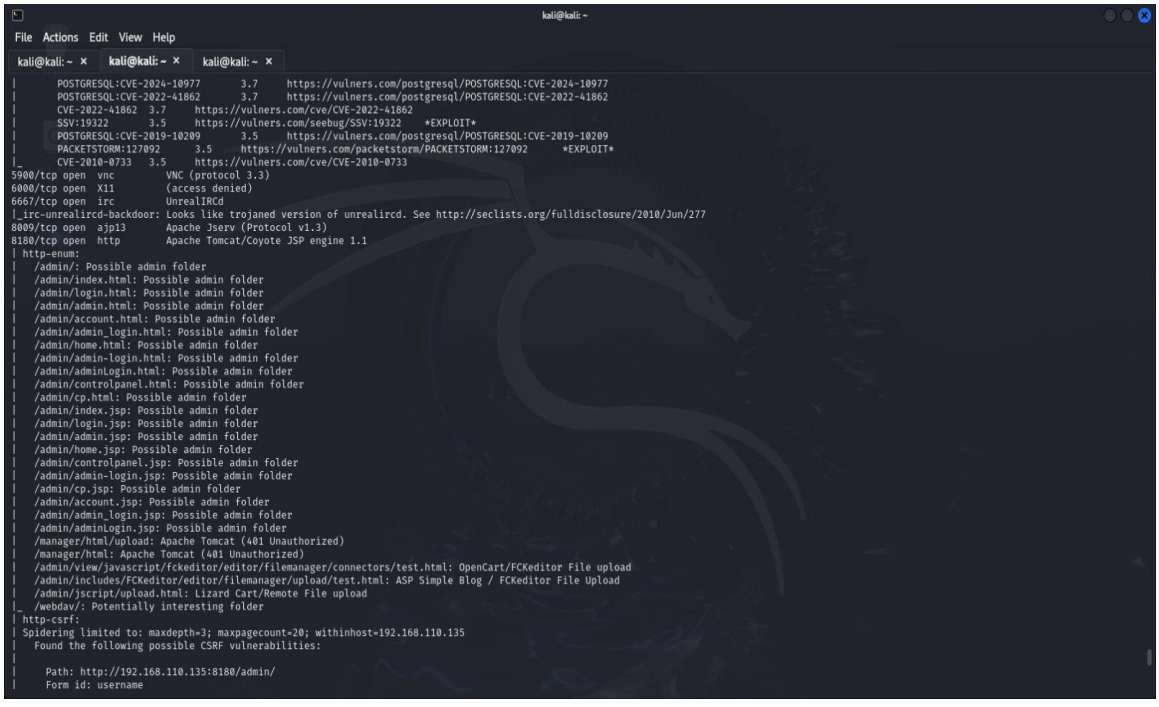



```
| http-slowloris-check:
|   VULNERABLE:
|   Slowloris DOS attack
|     State: LIKELY VULNERABLE
|     IDs:  CVE:CVE-2007-6750
|       Slowloris tries to keep many connections to the target web server open and hold
|       them open as long as possible.  It accomplishes this by opening connections to
|       the target web server and sending a partial request. By doing so, it starves
|       the http server's resources causing Denial Of Service.
|
|     Disclosure date: 2009-09-17
|     References:
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-6750
|_      http://ha.ckers.org/slowloris/
|_http-server-header: Apache/2.2.8 (Ubuntu) DAV/2
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
| vulners:
|   cpe:/a:apache:http_server:2.2.8:
|       SSV:69341       10.0    https://vulners.com/seebug/SSV:69341    *EXPLOIT*
|       SSV:19282       10.0    https://vulners.com/seebug/SSV:19282    *EXPLOIT*
|       SSV:19236       10.0    https://vulners.com/seebug/SSV:19236    *EXPLOIT*
|       SSV:11999       10.0    https://vulners.com/seebug/SSV:11999    *EXPLOIT*
|       PACKETSTORM:86964       10.0    https://vulners.com/packetstorm/PACKETSTORM:86964       *EXPLOIT*
|       PACKETSTORM:180533      10.0    https://vulners.com/packetstorm/PACKETSTORM:180533      *EXPLOIT*
|       MSF:AUXILIARY-DOS-HTTP-APACHE_MOD_ISAPI-       10.0    https://vulners.com/metasploit/MSF:AUXILIARY-DOS-HTTP-APACHE_MOD_ISAPI- *EXPLOIT*
|       HTTPD:E74B6F3660D13C4DD05DF3A83EA61631  10.0    https://vulners.com/httpd/HTTPD:E74B6F3660D13C4DD05DF3A83EA61631
|       HTTPD:81180E4E634CDECC9784146016B4A949  10.0    https://vulners.com/httpd/HTTPD:81180E4E634CDECC9784146016B4A949
|       EXPLOITPACK:30ED468EC8BD5B71B2CB93825A852B80    10.0    https://vulners.com/exploitpack/EXPLOITPACK:30ED468EC8BD5B71B2CB93825A852B80    *EXPLOIT*
|       EDB-ID:14288    10.0    https://vulners.com/exploitdb/EDB-ID:14288      *EXPLOIT*
|       EDB-ID:11650    10.0    https://vulners.com/exploitdb/EDB-ID:11650      *EXPLOIT*
|       CVE-2010-0425   10.0    https://vulners.com/cve/CVE-2010-0425
|       3E6BA608-776F-5B1F-9BA5-589CD2A5A351    10.0    https://vulners.com/gitee/3E6BA608-776F-5B1F-9BA5-589CD2A5A351  *EXPLOIT*
|       PACKETSTORM:171631      9.8     https://vulners.com/packetstorm/PACKETSTORM:171631      *EXPLOIT*
|       HTTPD:E69E9574251973D5AF93FA9D04997FC1  9.8     https://vulners.com/httpd/HTTPD:E69E9574251973D5AF93FA9D04997FC1
|       HTTPD:E162D3AE025639FEE2A89D5AF40ABF2F  9.8     https://vulners.com/httpd/HTTPD:E162D3AE025639FEE2A89D5AF40ABF2F
|       HTTPD:C072933AA965A86DA3E2C9172FFC1569  9.8     https://vulners.com/httpd/HTTPD:C072933AA965A86DA3E2C9172FFC1569
|       HTTPD:A1BBCE110E077FFBF4469D4F06DB9293  9.8     https://vulners.com/httpd/HTTPD:A1BBCE110E077FFBF4469D4F06DB9293
|       HTTPD:A09F9CEBE0B7C39EDA0480FEAEF4FE9D  9.8     https://vulners.com/httpd/HTTPD:A09F9CEBE0B7C39EDA0480FEAEF4FE9D
|       HTTPD:9F5406E0F4A0B007A0A4C9C92EF9813B  9.8     https://vulners.com/httpd/HTTPD:9F5406E0F4A0B007A0A4C9C92EF9813B
|       HTTPD:9BCBE3C14201AFC4B0F36F15CB40C0F8  9.8     https://vulners.com/httpd/HTTPD:9BCBE3C14201AFC4B0F36F15CB40C0F8
|       HTTPD:2BE0032A6ABE7CC52906DBAAFE0E448E  9.8     https://vulners.com/httpd/HTTPD:2BE0032A6ABE7CC52906DBAAFE0E448E
|       EDB-ID:51193    9.8     https://vulners.com/exploitdb/EDB-ID:51193      *EXPLOIT*
|       ECC3E825-EE29-59D3-BE28-1B30DB15940E    9.8     https://vulners.com/githubexploit/ECC3E825-EE29-59D3-BE28-1B30DB15940E  *EXPLOIT*
|       D5084D51-C8DF-5CBA-BC26-ACF2E33F8E52    9.8     https://vulners.com/githubexploit/D5084D51-C8DF-5CBA-BC26-ACF2E33F8E52  *EXPLOIT*
|       CVE-2022-31813  9.8     https://vulners.com/cve/CVE-2022-31813
|       CVE-2022-22720  9.8     https://vulners.com/cve/CVE-2022-22720
|       CVE-2021-44790  9.8     https://vulners.com/cve/CVE-2021-44790
```

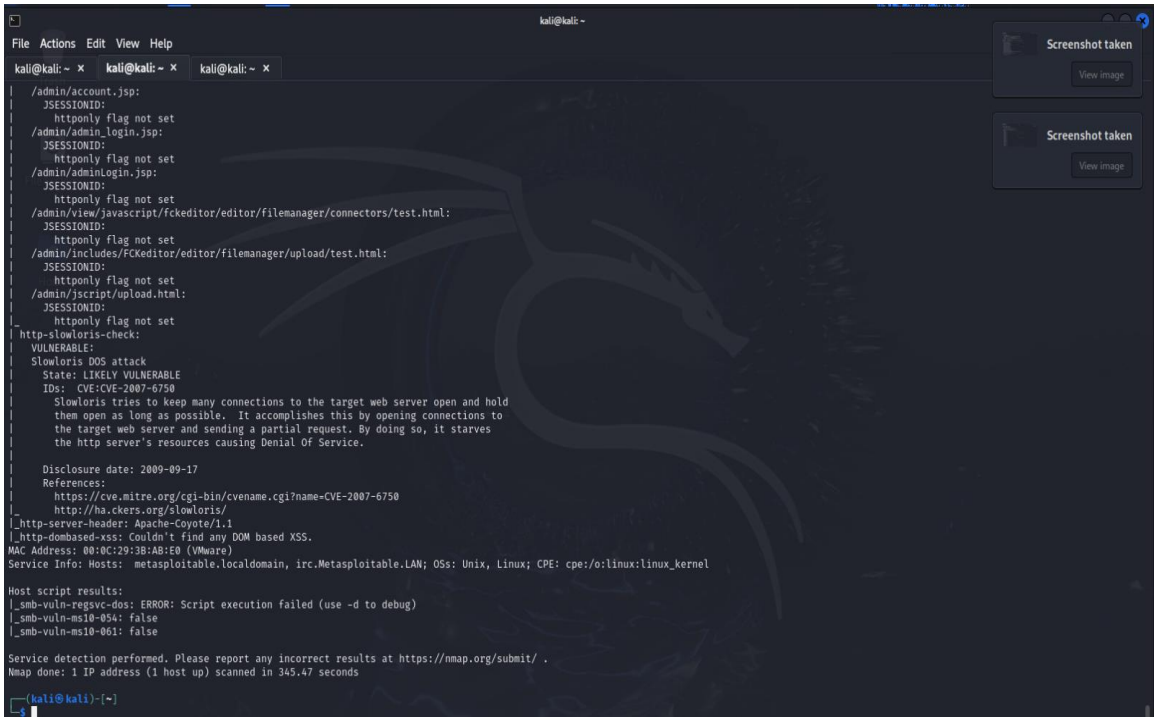

kali@kali: ~
File Actions Edit View Help
kali@kali: ~
kali@kali: ~
kali@kali: ~
8AFB43C5-ABD4-52AD-BB19-24D7884FF2A2 9.0 https://vulners.com/githubexploit/8AFB43C5-ABD4-52AD-BB19-24D7884FF2A2 *EXPLOIT*
7F48C6CF-47B2-5AF9-B6FD-1735FB2A95B2 9.0 https://vulners.com/githubexploit/7F48C6CF-47B2-5AF9-B6FD-1735FB2A95B2 *EXPLOIT*
36618CA8-9316-59CA-B748-82F15F407C4F 9.0 https://vulners.com/githubexploit/36618CA8-9316-59CA-B748-82F15F407C4F *EXPLOIT*
HTTPD:30E0EE442FF4843665FED4FBCA25406A 8.1 https://vulners.com/httpd/HTTPD:30E0EE442FF4843665FED4FBCA25406A
CVE-2016-5387 8.1 https://vulners.com/cve/CVE-2016-5387
SSV:72403 7.8 https://vulners.com/seebug/SSV:72403 *EXPLOIT*
SSV:2820 7.8 https://vulners.com/seebug/SSV:2820 *EXPLOIT*
SSV:26043 7.8 https://vulners.com/seebug/SSV:26043 *EXPLOIT*
SSV:20899 7.8 https://vulners.com/seebug/SSV:20899 *EXPLOIT*
SSV:11569 7.8 https://vulners.com/seebug/SSV:11569 *EXPLOIT*
PACKETSTORM:180517 7.8 https://vulners.com/packetstorm/PACKETSTORM:180517 *EXPLOIT*
PACKETSTORM:126851 7.8 https://vulners.com/packetstorm/PACKETSTORM:126851 *EXPLOIT*
PACKETSTORM:123527 7.8 https://vulners.com/packetstorm/PACKETSTORM:123527 *EXPLOIT*
PACKETSTORM:122962 7.8 https://vulners.com/packetstorm/PACKETSTORM:122962 *EXPLOIT*
MSF:AUXILIARY-DOS-HTTP-APACHE_RANGE_DOS- 7.8 https://vulners.com/metasploit/MSF:AUXILIARY-DOS-HTTP-APACHE_RANGE_DOS- *EXPLOIT*
HTTPD:556E7FA885F1BED86E3D9AAB5665198F 7.8 https://vulners.com/httpd/HTTPD:556E7FA885F1BED86E3D9AAB5665198F
EXPLOITPACK:18685FCF5C57B52642E62C06BABC6F83 7.8 https://vulners.com/exploitpack/EXPLOITPACK:18685FCF5C57B52642E62C06BABC6F83 *EXPLOIT*
EDB-ID:18221 7.8 https://vulners.com/exploitdb/EDB-ID:18221 *EXPLOIT*
CVE-2011-3192 7.8 https://vulners.com/cve/CVE-2011-3192
C76F17FD-A21F-5E67-97D8-51A53B9594C1 7.8 https://vulners.com/githubexploit/C76F17FD-A21F-5E67-97D8-51A53B9594C1 *EXPLOIT*
952369B3-F757-55D6-B0C6-9F72C04294A3 7.8 https://vulners.com/githubexploit/952369B3-F757-55D6-B0C6-9F72C04294A3 *EXPLOIT*
1337DAY-ID-21170 7.8 https://vulners.com/zdt/1337DAY-ID-21170 *EXPLOIT*
SSV:12673 7.5 https://vulners.com/seebug/SSV:12673 *EXPLOIT*
SSV:12626 7.5 https://vulners.com/seebug/SSV:12626 *EXPLOIT*
PACKETSTORM:181038 7.5 https://vulners.com/packetstorm/PACKETSTORM:181038 *EXPLOIT*
MSF:AUXILIARY-SCANNER-HTTP-APACHE_OPTIONSBLEED- 7.5 https://vulners.com/metasploit/MSF:AUXILIARY-SCANNER-HTTP-APACHE_OPTIONSBLEED- *EXPLOIT*
HTTPD:F1CFBC9B54DFAD0499179863D36830BB 7.5 https://vulners.com/httpd/HTTPD:F1CFBC9B54DFAD0499179863D36830BB
HTTPD:C317C7138B4A8BBD54A901D6DDDCB837 7.5 https://vulners.com/httpd/HTTPD:C317C7138B4A8BBD54A901D6DDDCB837
HTTPD:C1F57FDC580B58497A5EC5B7D3749F2F 7.5 https://vulners.com/httpd/HTTPD:C1F57FDC580B58497A5EC5B7D3749F2F
HTTPD:C0856723C0FBF5502E1378536B484C09 7.5 https://vulners.com/httpd/HTTPD:C0856723C0FBF5502E1378536B484C09
HTTPD:BEF84406F2FB3CB90F1C555BEFF774E2 7.5 https://vulners.com/httpd/HTTPD:BEF84406F2FB3CB90F1C555BEFF774E2
HTTPD:B1B0A31C4AD388CC6C5759314141173E2 7.5 https://vulners.com/httpd/HTTPD:B1B0A31C4AD388CC6C5759314141173E2
HTTPD:7DDAAFDB1FD8B2E7FD36ADABA5DB6DAA 7.5 https://vulners.com/httpd/HTTPD:7DDAAFDB1FD8B2E7FD36ADABA5DB6DAA
HTTPD:5E6BCDB2F7C53E4EDCE844709D930AF5 7.5 https://vulners.com/httpd/HTTPD:5E6BCDB2F7C53E4EDCE844709D930AF5
HTTPD:5227799CC4172DBFA895A4F581F74C11 7.5 https://vulners.com/httpd/HTTPD:5227799CC4172DBFA895A4F581F74C11
EDB-ID:42745 7.5 https://vulners.com/exploitdb/EDB-ID:42745 *EXPLOIT*
CVE-2023-31122 7.5 https://vulners.com/cve/CVE-2023-31122
CVE-2022-30556 7.5 https://vulners.com/cve/CVE-2022-30556
CVE-2022-29404 7.5 https://vulners.com/cve/CVE-2022-29404
CVE-2022-22719 7.5 https://vulners.com/cve/CVE-2022-22719
CVE-2021-34798 7.5 https://vulners.com/cve/CVE-2021-34798
CVE-2018-8011 7.5 https://vulners.com/cve/CVE-2018-8011
CVE-2018-1303 7.5 https://vulners.com/cve/CVE-2018-1303
CVE-2017-9798 7.5 https://vulners.com/cve/CVE-2017-9798
CVE-2017-15710 7.5 https://vulners.com/cve/CVE-2017-15710
CVE-2016-8743 7.5 https://vulners.com/cve/CVE-2016-8743
CVE-2009-2699 7.5 https://vulners.com/cve/CVE-2009-2699
Screenshot taken
View image


kali@kali: ~
File Actions Edit View Help
kali@kali: ~
kali@kali: ~
kali@kali: ~
100005 1,2,3 47017/tcp mountd
100005 1,2,3 54406/udp mountd
100021 1,3,4 37008/udp nlockmgr
100021 1,3,4 46826/tcp nlockmgr
100024 1 37177/tcp status
100024 1 42135/udp status
139/tcp open netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp open netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp open exec netkit-rsh rexecd
513/tcp open login OpenBSD or Solaris rlogind
514/tcp open tcpwrapped
1099/tcp open java-rmi GNU Classpath grmiregistry
rmi-vuln-classloader:
VULNERABLE:
RMI registry default configuration remote code execution vulnerability
State: VULNERABLE
Default configuration of RMI registry allows loading classes from remote URLs which can lead to remote code execution.
References:
https://github.com/rapid7/metasploit-framework/blob/master/modules/exploits/multi/misc/java_rmi_server.rb
1524/tcp open bindshell Metasploitable root shell
2049/tcp open nfs 2-4 (RPC #100003)
2121/tcp open ftp ProFTPD 1.3.1
vulners:
cpe:/a:proftpd:proftpd:1.3.1:
SAINT:FD1752E124A72FD3A26EEB9B315E8382 10.0 https://vulners.com/saint/SAINT:FD1752E124A72FD3A26EEB9B315E8382 *EXPLOIT*
SAINT:950EB68D408A40399926A4CCAD3CC62E 10.0 https://vulners.com/saint/SAINT:950EB68D408A40399926A4CCAD3CC62E *EXPLOIT*
SAINT:63FB77B9136D48259E4F0D4CDA35E957 10.0 https://vulners.com/saint/SAINT:63FB77B9136D48259E4F0D4CDA35E957 *EXPLOIT*
SAINT:1B08F4664C428B180EEC9617B41D9A2C 10.0 https://vulners.com/saint/SAINT:1B08F4664C428B180EEC9617B41D9A2C *EXPLOIT*
PROFTPD_MOD_COPY 10.0 https://vulners.com/canvas/PROFTPD_MOD_COPY *EXPLOIT*
PACKETSTORM:162777 10.0 https://vulners.com/packetstorm/PACKETSTORM:162777 *EXPLOIT*
PACKETSTORM:132218 10.0 https://vulners.com/packetstorm/PACKETSTORM:132218 *EXPLOIT*
PACKETSTORM:131567 10.0 https://vulners.com/packetstorm/PACKETSTORM:131567 *EXPLOIT*
PACKETSTORM:131555 10.0 https://vulners.com/packetstorm/PACKETSTORM:131555 *EXPLOIT*
PACKETSTORM:131505 10.0 https://vulners.com/packetstorm/PACKETSTORM:131505 *EXPLOIT*
MSF:EXPLOIT-UNIX-FTP-PROFTPD_MODCOPY_EXEC- 10.0 https://vulners.com/metasploit/MSF:EXPLOIT-UNIX-FTP-PROFTPD_MODCOPY_EXEC- *EXPLOIT*
EDB-ID:49908 10.0 https://vulners.com/exploitdb/EDB-ID:49908 *EXPLOIT*
EDB-ID:37262 10.0 https://vulners.com/exploitdb/EDB-ID:37262 *EXPLOIT*
6BF3AE83-7AD0-5378-B7C9-C05B81007195 10.0 https://vulners.com/gitee/6BF3AE83-7AD0-5378-B7C9-C05B81007195 *EXPLOIT*
1337DAY-ID-36298 10.0 https://vulners.com/zdt/1337DAY-ID-36298 *EXPLOIT*
1337DAY-ID-23720 10.0 https://vulners.com/zdt/1337DAY-ID-23720 *EXPLOIT*
1337DAY-ID-23544 10.0 https://vulners.com/zdt/1337DAY-ID-23544 *EXPLOIT*
CVE-2019-12815 9.8 https://vulners.com/cve/CVE-2019-12815
739FE495-4675-5A2A-BB93-EEF94AC07632 9.8 https://vulners.com/githubexploit/739FE495-4675-5A2A-BB93-EEF94AC07632 *EXPLOIT*
SSV:26016 9.0 https://vulners.com/seebug/SSV:26016 *EXPLOIT*
SSV:24282 9.0 https://vulners.com/seebug/SSV:24282 *EXPLOIT*
CVE-2011-4130 9.0 https://vulners.com/cve/CVE-2011-4130
Screenshot taken
View image


kali@kali: ~
File Actions Edit View Help
kali@kali: ~
kali@kali: ~
kali@kali: ~
| SSV:20226 7.1 https://vulners.com/seebug/SSV:20226 *EXPLOIT*
| PACKETSTORM:95517 7.1 https://vulners.com/packetstorm/PACKETSTORM:95517 *EXPLOIT*
| CVE-2010-3867 7.1 https://vulners.com/cve/CVE-2010-3867
| SSV:12447 6.8 https://vulners.com/seebug/SSV:12447 *EXPLOIT*
| SSV:11950 6.8 https://vulners.com/seebug/SSV:11950 *EXPLOIT*
| EDB-ID:33128 6.8 https://vulners.com/exploitdb/EDB-ID:33128 *EXPLOIT*
| CVE-2010-4652 6.8 https://vulners.com/cve/CVE-2010-4652
| CVE-2009-0543 6.8 https://vulners.com/cve/CVE-2009-0543
| CVE-2023-48795 5.9 https://vulners.com/cve/CVE-2023-48795
| SSV:12523 5.8 https://vulners.com/seebug/SSV:12523 *EXPLOIT*
| CVE-2009-3639 5.8 https://vulners.com/cve/CVE-2009-3639
| CVE-2017-7418 5.5 https://vulners.com/cve/CVE-2017-7418
| CVE-2011-1137 5.0 https://vulners.com/cve/CVE-2011-1137
| CVE-2019-19269 4.9 https://vulners.com/cve/CVE-2019-19269
| CVE-2008-7265 4.0 https://vulners.com/cve/CVE-2008-7265
|_ CVE-2012-6095 1.2 https://vulners.com/cve/CVE-2012-6095
3306/tcp open mysql MySQL 5.0.51a-3ubuntu5
|_mysql-vuln-cve2012-2122: ERROR: Script execution failed (use -d to debug)
| vulners:
| cpe:/a:mysql:mysql:5.0.51a-3ubuntu5:
| SSV:19118 8.5 https://vulners.com/seebug/SSV:19118 *EXPLOIT*
| CVE-2017-15945 7.8 https://vulners.com/cve/CVE-2017-15945
| SSV:15006 6.8 https://vulners.com/seebug/SSV:15006 *EXPLOIT*
| CVE-2009-4028 6.8 https://vulners.com/cve/CVE-2009-4028
| SSV:15004 6.0 https://vulners.com/seebug/SSV:15004 *EXPLOIT*
| CVE-2010-1621 5.0 https://vulners.com/cve/CVE-2010-1621
| CVE-2015-2575 4.9 https://vulners.com/cve/CVE-2015-2575
| SSV:3280 4.6 https://vulners.com/seebug/SSV:3280 *EXPLOIT*
| CVE-2008-2079 4.6 https://vulners.com/cve/CVE-2008-2079
| CVE-2010-3682 4.0 https://vulners.com/cve/CVE-2010-3682
| CVE-2010-3677 4.0 https://vulners.com/cve/CVE-2010-3677
| CVE-2009-0819 4.0 https://vulners.com/cve/CVE-2009-0819
| CVE-2007-5925 4.0 https://vulners.com/cve/CVE-2007-5925
|_ CVE-2010-1626 3.6 https://vulners.com/cve/CVE-2010-1626
|_ssl-ccs-injection: No reply from server (TIMEOUT)
5432/tcp open postgresql PostgreSQL DB 8.3.0 - 8.3.7
| ssl-ccs-injection:
| VULNERABLE:
| SSL/TLS MITM vulnerability (CCS Injection)
| State: VULNERABLE
| Risk factor: High
| OpenSSL before 0.9.8za, 1.0.0 before 1.0.0m, and 1.0.1 before 1.0.1h
| does not properly restrict processing of ChangeCipherSpec messages,
| which allows man-in-the-middle attackers to trigger use of a zero
| length master key in certain OpenSSL-to-OpenSSL communications, and
| consequently hijack sessions or obtain sensitive information, via
| a crafted TLS handshake, aka the "CCS Injection" vulnerability.
Screenshot taken
View image
Screenshot taken
View image
Screenshot taken
View image
Screenshot taken
View image
Screenshot taken
View image


kali@kali: ~
File Actions Edit View Help
kali@kali: ~
kali@kali: ~
kali@kali: ~
| POSTGRESQL:CVE-2024-10977 3.7 https://vulners.com/postgresql/POSTGRESQL:CVE-2024-10977
| POSTGRESQL:CVE-2022-41862 3.7 https://vulners.com/postgresql/POSTGRESQL:CVE-2022-41862
| CVE-2022-41862 3.7 https://vulners.com/cve/CVE-2022-41862
| SSV:19322 3.5 https://vulners.com/seebug/SSV:19322 *EXPLOIT*
| POSTGRESQL:CVE-2019-10209 3.5 https://vulners.com/postgresql/POSTGRESQL:CVE-2019-10209
| PACKETSTORM:127092 3.5 https://vulners.com/packetstorm/PACKETSTORM:127092 *EXPLOIT*
|_ CVE-2010-0733 3.5 https://vulners.com/cve/CVE-2010-0733
5900/tcp open vnc VNC (protocol 3.3)
6000/tcp open X11 (access denied)
6667/tcp open irc UnrealIRCd
|_irc-unrealircd-backdoor: Looks like trojaned version of unrealircd. See http://seclists.org/fulldisclosure/2010/Jun/277
8009/tcp open ajp13 Apache Jserv (Protocol v1.3)
8180/tcp open http Apache Tomcat/Coyote JSP engine 1.1
| http-enum:
| /admin/: Possible admin folder
| /admin/index.html: Possible admin folder
| /admin/login.html: Possible admin folder
| /admin/admin.html: Possible admin folder
| /admin/account.html: Possible admin folder
| /admin/admin_login.html: Possible admin folder
| /admin/home.html: Possible admin folder
| /admin/admin-login.html: Possible admin folder
| /admin/adminLogin.html: Possible admin folder
| /admin/controlpanel.html: Possible admin folder
| /admin/cp.html: Possible admin folder
| /admin/index.jsp: Possible admin folder
| /admin/login.jsp: Possible admin folder
| /admin/admin.jsp: Possible admin folder
| /admin/home.jsp: Possible admin folder
| /admin/controlpanel.jsp: Possible admin folder
| /admin/admin-login.jsp: Possible admin folder
| /admin/cp.jsp: Possible admin folder
| /admin/account.jsp: Possible admin folder
| /admin/admin_login.jsp: Possible admin folder
| /admin/adminLogin.jsp: Possible admin folder
| /manager/html/upload: Apache Tomcat (401 Unauthorized)
| /manager/html: Apache Tomcat (401 Unauthorized)
| /admin/view/javascript/fckeditor/editor/filemanager/connectors/test.html: OpenCart/FCKeditor File upload
| /admin/includes/FCKeditor/editor/filemanager/upload/test.html: ASP Simple Blog / FCKeditor File Upload
| /admin/jscript/upload.html: Lizard Cart/Remote File upload
|_ /webdav/: Potentially interesting folder
| http-csrf:
| Spidering limited to: maxdepth=3; maxpagecount=20; withinhost=192.168.110.135
| Found the following possible CSRF vulnerabilities:
|
| Path: http://192.168.110.135:8180/admin/
| Form id: username


kali@kali: ~
File Actions Edit View Help
kali@kali: ~ ×
kali@kali: ~ ×
kali@kali: ~ ×
Screenshot taken
View image
| Path: http://192.168.110.135:8180/admin/
| Form id: username
| Form action: j_security_check;jsessionid=1C84FD9A13B2295BDBDD290E957A211C
|
| Path: http://192.168.110.135:8180/admin/login.jsp
| Form id: username
|_ Form action: j_security_check;jsessionid=0E93BB07FB50503D159C80658A1F3D15
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
| http-cookie-flags:
| /admin/:
| JSESSIONID:
| httponly flag not set
| /admin/index.html:
| JSESSIONID:
| httponly flag not set
| /admin/login.html:
| JSESSIONID:
| httponly flag not set
| /admin/admin.html:
| JSESSIONID:
| httponly flag not set
| /admin/account.html:
| JSESSIONID:
| httponly flag not set
| /admin/admin_login.html:
| JSESSIONID:
| httponly flag not set
| /admin/home.html:
| JSESSIONID:
| httponly flag not set
| /admin/admin-login.html:
| JSESSIONID:
| httponly flag not set
| /admin/adminLogin.html:
| JSESSIONID:
| httponly flag not set
| /admin/controlpanel.html:
| JSESSIONID:
| httponly flag not set
| /admin/cp.html:
| JSESSIONID:
| httponly flag not set
| /admin/index.jsp:
| JSESSIONID:
| httponly flag not set
| /admin/login.jsp:
| JSESSIONID:


kali@kali: ~
File Actions Edit View Help
kali@kali: ~ ×
kali@kali: ~ ×
kali@kali: ~ ×
Screenshot taken
View image
Screenshot taken
View image
| /admin/account.jsp:
| JSESSIONID:
| httponly flag not set
| /admin/admin_login.jsp:
| JSESSIONID:
| httponly flag not set
| /admin/adminLogin.jsp:
| JSESSIONID:
| httponly flag not set
| /admin/view/javascript/fckeditor/editor/filemanager/connectors/test.html:
| JSESSIONID:
| httponly flag not set
| /admin/includes/FCKeditor/editor/filemanager/upload/test.html:
| JSESSIONID:
| httponly flag not set
| /admin/jscript/upload.html:
| JSESSIONID:
|_ httponly flag not set
| http-slowloris-check:
| VULNERABLE:
| Slowloris DOS attack
| State: LIKELY VULNERABLE
| IDs: CVE:CVE-2007-6750
| Slowloris tries to keep many connections to the target web server open and hold
| them open as long as possible. It accomplishes this by opening connections to
| the target web server and sending a partial request. By doing so, it starves
| the http server's resources causing Denial Of Service.
|
| Disclosure date: 2009-09-17
| References:
| https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-6750
|_ http://ha.ckers.org/slowloris/
|_http-server-header: Apache-Coyote/1.1
|_http-dombased-xss: Couldn't find any DOM based XSS.
MAC Address: 00:0C:29:3B:AB:E0 (VMware)
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
Host script results:
|_smb-vuln-regsvc-dos: ERROR: Script execution failed (use -d to debug)
|_smb-vuln-ms10-054: false
|_smb-vuln-ms10-061: false
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 345.47 seconds
┌──(kali㉿kali)-[~]
└─$

15.Conclusion

Scanning and enumeration revealed the system's surface area and running services. This information will assist in identifying vulnerabilities and preparing for exploitation in the next phase.