

jalon 3

Copie d'écran de la fenêtre terminal « metasploit » avec la liste de l'ensemble des services identifiés suite à la commande 13 msf6 > services

```
tp@rt: ~  
Fichier  Edit  Affichage  Rechercher  Terminal  Aide  
Interact with a module by name or index. For example info 0, use 0 or use auxiliary/scanner/ssh/ssh version  
msf6 > services  
Services  
-----  
host      port  proto  name      state  info  
-----  
192.168.99.1 22    tcp    ssh       open  
192.168.99.1 53     tcp    dns       open  
192.168.99.1 53     udp    dns       open  
192.168.99.1 67     udp             open  
192.168.99.1 123    udp    ntp       open  
192.168.99.1 137    udp    netbios-ns open  
192.168.99.1 139    tcp    smb       open  
192.168.99.1 445    tcp    cifs      open  
192.168.99.1 901    tcp    SWAT      open  
192.168.99.1 5001   tcp    java-listener open  
192.168.99.1 8080   tcp    WWW       open  
192.168.99.7 22     tcp    ssh       open  
192.168.99.7 123    udp    ntp       open  
192.168.99.7 137    udp    netbios-ns open  
192.168.99.7 139    tcp    smb       open  
192.168.99.7 445    tcp    cifs      open  
192.168.99.7 901    tcp    SWAT      open  
192.168.99.7 5001   tcp    java-listener open  
192.168.99.7 8080   tcp    WWW       open  
192.168.99.10 22     tcp    ssh       open  
192.168.99.10 53     tcp    dns       open  
192.168.99.10 53     udp    dns       open  
192.168.99.10 80     tcp    WWW       open  
192.168.99.10 123    udp    ntp       open  
192.168.99.10 137    udp    netbios-ns open  
192.168.99.10 139    tcp    smb       open  
192.168.99.10 445    tcp    cifs      open  
192.168.99.10 901    tcp    SWAT      open  
192.168.99.10 5001   tcp    java-listener open  
192.168.99.10 8080   tcp    WWW       open  
192.168.99.13 22     tcp    ssh       open  
192.168.99.13 80     tcp    WWW       open  
192.168.99.13 123    udp    ntp       open  
192.168.99.13 137    udp    netbios-ns open  
192.168.99.13 139    tcp    smb       open
```

```
tp@rt: ~  
Fichier  Edit  Affichage  Rechercher  Terminal  Aide  
192.168.99.18 25     tcp    SMTP      open  
192.168.99.18 123    udp    ntp       open  
192.168.99.18 137    udp    netbios-ns open  
192.168.99.18 139    tcp    smb       open  
192.168.99.18 143    tcp    IMAP      open  
192.168.99.18 443    tcp    WWW       open  
192.168.99.18 445    tcp    cifs      open  
192.168.99.18 587    tcp    SMTP      open  
192.168.99.18 901    tcp    SWAT      open  
192.168.99.18 993    tcp    IMAP      open  
192.168.99.18 5001   tcp    java-listener open  
192.168.99.18 8080   tcp    WWW       open  
192.168.99.20 23     tcp    TELNET    open  
192.168.99.20 53     tcp    dns       open  
192.168.99.20 53     udp    dns       open  
192.168.99.20 80     tcp    WWW       open  
192.168.99.105 123    udp             open  
192.168.99.105 135    tcp    EPMAP     open  
192.168.99.105 137    udp             open  
192.168.99.105 138    udp             open  
192.168.99.105 139    tcp    smb       open  
192.168.99.105 445    tcp    cifs      open  
192.168.99.105 500    udp             open  
192.168.99.105 1900   udp             open  
192.168.99.105 4500   udp             open  
192.168.99.105 5040   tcp             open  
192.168.99.105 5050   udp             open  
192.168.99.105 5353   udp    MDNS      open  
192.168.99.105 5355   udp             open  
192.168.99.105 8834   tcp    WWW       open  
192.168.99.105 9012   tcp    WWW       open  
192.168.99.105 9013   tcp    WWW       open  
192.168.99.105 49664  tcp    DCE-RPC   open  
192.168.99.105 49665  tcp    DCE-RPC   open  
192.168.99.105 49670  tcp    DCE-RPC   open  
192.168.99.105 49671  tcp    DCE-RPC   open  
192.168.99.105 49672  tcp    DCE-RPC   open  
192.168.99.105 49683  tcp    DCE-RPC   open  
192.168.99.105 52952  udp             open  
192.168.99.105 61406  udp             open  
192.168.99.105 61407  udp             open  
192.168.99.105 65214  udp             open  
192.168.99.105 65215  udp             open  
192.168.99.105 65216  udp             open
```

```
tp@rt: ~  
Fichier  Editor  Affichage  Rechercher  Terminal  Aide  
192.168.99.18 5001 tcp java-listener open  
192.168.99.18 8080 tcp www open  
192.168.99.20 22 tcp telnet open  
192.168.99.20 53 tcp dns open  
192.168.99.20 53 udp dns open  
192.168.99.20 80 tcp www open  
192.168.99.105 123 udp open open  
192.168.99.105 135 tcp epmap open  
192.168.99.105 137 udp open open  
192.168.99.105 138 udp open open  
192.168.99.105 139 tcp smb open  
192.168.99.105 445 tcp cifs open  
192.168.99.105 500 udp open open  
192.168.99.105 1900 udp open open  
192.168.99.105 4500 udp open open  
192.168.99.105 5040 tcp open open  
192.168.99.105 5050 udp open open  
192.168.99.105 5353 udp mdns open  
192.168.99.105 5355 udp open open  
192.168.99.105 8834 tcp www open  
192.168.99.105 9012 tcp www open  
192.168.99.105 9013 tcp www open  
192.168.99.105 49664 tcp dce-rpc open  
192.168.99.105 49665 tcp dce-rpc open  
192.168.99.105 49670 tcp dce-rpc open  
192.168.99.105 49671 tcp dce-rpc open  
192.168.99.105 49672 tcp dce-rpc open  
192.168.99.105 49683 tcp dce-rpc open  
192.168.99.105 52952 udp open open  
192.168.99.105 61406 udp open open  
192.168.99.105 61407 udp open open  
192.168.99.105 65214 tcp open open  
192.168.99.105 65215 udp open open  
192.168.99.105 65216 udp open open  
192.168.99.105 65218 udp open open  
192.168.99.105 65219 udp open open  
192.168.99.105 65220 udp open open  
192.168.99.149 22 tcp ssh open  
192.168.99.185 22 tcp ssh open  
192.168.99.185 123 udp ntp open  
192.168.99.185 5353 udp mdns open  
msf6 > |
```

Copie d'écran de la fenêtre terminal « metasploit » avec la liste des cve du port 53 réaliser avec la commande search cve port:53

```
msf6 > search cve port:53  
Matching Modules  
=====
```

#	Name	Disclosure Date	Rank	Check	Description
0	auxiliary/dos/mdns/avahi_portzero	2008-11-14	normal	No	Avahi Source Port 0 DoS
1	auxiliary/dos/dns/bind_tkey	2015-07-28	normal	No	BIND TKEY Query Denial of Service
2	auxiliary/dos/dns/bind_tsig_badtime	2020-05-19	normal	No	BIND TSIG Badtime Query Denial of Service
3	auxiliary/dos/dns/bind_tsig	2016-09-27	normal	No	BIND TSIG Query Denial of Service
4	auxiliary/scanner/dns/dns_amp	.	normal	No	DNS Amplification Scanner
5	auxiliary/gather/enum_dns	.	normal	No	DNS Record Scanner and Enumerator
6	auxiliary/dos/hp/data_protector_rds	2011-01-08	normal	No	HP Data Protector Manager RDS DoS
7	exploit/windows/lotus/domino_sametime_stmux	2008-05-21	average	Yes	IBM Lotus Domino Sametime STmux.exe Stack Buffer Overflow
8	\ target: Lotus Sametime 7.5 on Windows Server 2000 SP4
9	\ target: Lotus Sametime 7.5 on Windows Server 2003 SP1
10	\ target: Lotus Sametime 7.5 on Windows Server 2003 SP2
11	\ target: Lotus Sametime 7.5.1 Windows Server 2003 SP2
12	\ target: Lotus Sametime 8.0.0 Windows Server 2003 SP2
13	exploit/windows/misc/landesk_aolnsrvr	2007-04-13	average	No	LANDesk Management Suite 8.7 Alert Service Buffer Overflow
14	\ target: Alerting Proxy 2000/2003/XP
15	\ target: Alerting Proxy 2003 SP1-2 (NX support)
16	\ target: Alerting Proxy XP SP2 (NX support)
17	auxiliary/dos/windows/llmnr/ms11_030_dnsapi	2011-04-12	normal	No	Microsoft Windows DNSAPI.dll LLMNR Buffer Underrun DoS
18	auxiliary/dos/windows/nat/nat_helper	2006-10-26	normal	No	Microsoft Windows NAT Helper Denial of Service

```
Interact with a module by name or index. For example info 16, use 18 or use auxiliary/dos/windows/nat/nat_helper  
msf6 > |
```

Copie d'écran de la fenêtre terminal « metasploit » avec la liste des exploits possibles en lien avec le ou les cve détectés.

commande search cve:2025-32728

```
msf6 > search cve:2025-32728  
[-] No results from search
```

La commande a retourné aucun résultat, ce qui signifie que, dans la version actuelle de Metasploit (msf6), il n'existe pas de module (exploit, scanner ou autre) associé à la CVE-2025-32728.

commande search cve:2008-5161

```
msf6 > search cve:2008-5161

Matching Modules
=====
#  Name                                     Disclosure Date  Rank  Check  Description
-  - - - - -                               - - - - -
0  auxiliary/scanner/ssh/ssh_version         .              normal No      SSH Version Scanner

Interact with a module by name or index. For example info 0, use 0 or use auxiliary/scanner/ssh/ssh_version
msf6 >
```

Résultat

Un seul module trouvé :

- auxiliary/scanner/ssh/ssh_version
 - Type : scanner
 - Rank : normal
 - Check intégré : non
 - Fonction : collecte la version SSH de la cible

Conclusion

Aucun module d'exploitation dédié à la CVE-2008-5161 n'est disponible dans Metasploit ; il faudra d'abord repérer manuellement les versions vulnérables via ce scanner, puis appliquer un exploit ou un PoC externe.