



1.1_Descubrimiento en NMAP

Hosts activos

Dirección IP: 192.168.56.104 - *Dirección MAC:* 08:00:27:F2:C3:90



1.2_Escaneo-de-puertos-sin-utilizar-ICMP

Dirección IP:

192.168.56.104

```
| Port | State | Service |
|-----|-----|-----|
| 1099/tcp | open | rmiregistry |
| 111/tcp | open | rpcbind |
| 139/tcp | open | netbios-ssn |
| 1524/tcp | open | ingreslock |
| 2049/tcp | open | nfs |
| 21/tcp | open | ftp |
| 2121/tcp | open | ccproxy-ftp |
| 22/tcp | open | ssh |
| 23/tcp | open | telnet |
| 25/tcp | open | smtp |
| 3306/tcp | open | mysql |
| 445/tcp | open | microsoft-ds |
| 512/tcp | open | exec |
| 513/tcp | open | login |
| 514/tcp | open | shell |
| 53/tcp | open | domain |
| 5432/tcp | open | postgresql |
| 5900/tcp | open | vnc |
| 6000/tcp | open | X11 |
| 6667/tcp | open | irc |
| 80/tcp | open | http |
| 8009/tcp | open | ajp13 |
| 8180/tcp | open | unknown |
```

(end of excerpt)



1.2_Obtención-de-puertos-TCP-abiertos

Direcciones:

IP: 192.168.56.104 - ipv4

Física: mac - 08:00:27:F2:C3:90

Puertos:

Los 977 puertos escaneados pero no presentados, estan en estado: closed

Los 977 puertos respondieron con: reset

=====
192.168.56.104

```
| Port | State | Service |  
|-----|-----|-----|  
| 1099/tcp | open | rmiregistry |  
| 111/tcp | open | rpcbind |  
| 139/tcp | open | netbios-ssn |  
| 1524/tcp | open | ingreslock |  
| 2049/tcp | open | nfs |  
| 21/tcp | open | ftp |  
| 2121/tcp | open | ccproxy-ftp |  
| 22/tcp | open | ssh |  
| 23/tcp | open | telnet |  
| 25/tcp | open | smtp |  
| 3306/tcp | open | mysql |  
| 445/tcp | open | microsoft-ds |  
| 512/tcp | open | exec |  
| 513/tcp | open | login |  
| 514/tcp | open | shell |  
| 53/tcp | open | domain |  
| 5432/tcp | open | postgresql |  
| 5900/tcp | open | vnc |  
| 6000/tcp | open | X11 |  
| 6667/tcp | open | irc |  
| 80/tcp | open | http |  
| 8009/tcp | open | ajp13 |  
| 8180/tcp | open | unknown |
```

(end of excerpt)

=====



1.3_Vulnerabilidades-mediante-puertos-TCP

Dirección IP:

```
# Nmap 7.93 scan initiated Tue Jan 31 02:00:16 2023 as: nmap -v -sS --script=vuln
--stylesheet=https://svn.nmap.org/nmap/docs/nmap.xml -oA /src/archivos/hosts/fase_3/192.168.56.104vunlnmaptcp
192.168.56.104
Nmap scan report for 192.168.56.104
Host is up (0.00029s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
| 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://www.securityfocus.com/bid/48539
| https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2523
| https://github.com/rapid7/metasploit-framework/blob/master/modules/exploits/unix/ftp/vsftpd_234_backdoor.rb
| http://scarybeastsecurity.blogspot.com/2011/07/alert-vsftpd-download-backdoored.html
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
| ssl-poodle:
| VULNERABLE:
| SSL POODLE information leak
| State: VULNERABLE
| IDs: CVE:CVE-2014-3566 BID:70574
| 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://www.imperialviolet.org/2014/10/14/poodle.html
| https://www.securityfocus.com/bid/70574
| https://www.openssl.org/~bodo/ssl-poodle.pdf
| https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-3566
| ssl-dh-params:
```



1.3_Vulnerabilidades-mediante-puertos-TCP

| 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_EXPORT_WITH_RC4_40_MD5
| Modulus Type: Safe prime
| Modulus Source: Unknown/Custom-generated
| Modulus Length: 512
| Generator Length: 8
| Public Key Length: 512
| References:
| <https://www.ietf.org/rfc/rfc2246.txt>
|
| Transport Layer Security (TLS) Protocol DHE_EXPORT Ciphers Downgrade MitM (Logjam)
| State: VULNERABLE
| IDs: CVE:CVE-2015-4000 BID:74733
| 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
| to downgrade the security of a TLS session to 512-bit export-grade
| 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://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-4000>
| <https://weakdh.org>



1.3_Vulnerabilidades-mediante-puertos-TCP

```
| https://www.securityfocus.com/bid/74733
|
| 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_DES_CBC_SHA
|   Modulus Type: Safe prime
|   Modulus Source: postfix builtin
|   Modulus Length: 1024
|   Generator Length: 8
|   Public Key Length: 1024
| References:
|_ https://weakdh.org
| smtp-vuln-cve2010-4344:
|_ The SMTP server is not Exim: NOT VULNERABLE
|_ sslv2-drown: ERROR: Script execution failed (use -d to debug)
53/tcp open domain
80/tcp open http
|_ http-trace: TRACE is enabled
| http-csrf:
| Spidering limited to: maxdepth=3; maxpagecount=20; withinhost=192.168.56.104
| Found the following possible CSRF vulnerabilities:
|
| Path: http://192.168.56.104:80/dvwa/
| Form id:
| Form action: login.php
|
| Path: http://192.168.56.104:80/dvwa/login.php
| Form id:
| Form action: login.php
|
| Path: http://192.168.56.104:80/twiki/TWikiDocumentation.html
| Form id:
| Form action: http://TWiki.org/cgi-bin/passwd/TWiki/WebHome
|
| Path: http://192.168.56.104:80/twiki/TWikiDocumentation.html
| Form id:
```



1.3_Vulnerabilidades-mediante-puertos-TCP

```
| Form action: http://TWiki.org/cgi-bin/passwd/Main/WebHome
|
| Path: http://192.168.56.104:80/twiki/TWikiDocumentation.html
| Form id:
| Form action: http://TWiki.org/cgi-bin/edit/TWiki/
|
| Path: http://192.168.56.104:80/twiki/TWikiDocumentation.html
| Form id:
| Form action: http://TWiki.org/cgi-bin/view/TWiki/TWikiSkins
|
| Path: http://192.168.56.104:80/twiki/TWikiDocumentation.html
| Form id:
|_ Form action: http://TWiki.org/cgi-bin/manage/TWiki/ManagingWebs
|_ http-vuln-cve2017-1001000: ERROR: Script execution failed (use -d to debug)
|_ http-stored-xss: Couldn't find any stored XSS vulnerabilities.
| 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-dombased-xss: Couldn't find any DOM based XSS.
| http-fileupload-exploiter:
|
|_ Couldn't find a file-type field.
| http-sql-injection:
| Possible sqli for queries:
| http://192.168.56.104:80/dav/?C=M%3BO%3DA%27%20OR%20sqlspider
| http://192.168.56.104:80/dav/?C=S%3BO%3DA%27%20OR%20sqlspider
| http://192.168.56.104:80/dav/?C=D%3BO%3DA%27%20OR%20sqlspider
| http://192.168.56.104:80/dav/?C=N%3BO%3DD%27%20OR%20sqlspider
| http://192.168.56.104:80/mutillidae/index.php?page=change-log.htm%27%20OR%20sqlspider
| http://192.168.56.104:80/mutillidae/index.php?page=notes.php%27%20OR%20sqlspider
| http://192.168.56.104:80/mutillidae/index.php?page=documentation%2Fvulnerabilities.php%27%20OR%20sqlspider
| http://192.168.56.104:80/mutillidae/index.php?page=add-to-your-blog.php%27%20OR%20sqlspider
| http://192.168.56.104:80/mutillidae/index.php?page=user-info.php%27%20OR%20sqlspider
| http://192.168.56.104:80/mutillidae/?page=show-log.php%27%20OR%20sqlspider
| http://192.168.56.104:80/mutillidae/index.php?page=home.php%27%20OR%20sqlspider
|
```



1.3_Vulnerabilidades-mediante-puertos-TCP

<http://192.168.56.104:80/mutillidae/index.php?page=password-generator.php%27%20OR%20sqlspider&username=anonymous>

| <http://192.168.56.104:80/mutillidae/index.php?page=credits.php%27%20OR%20sqlspider>

| <http://192.168.56.104:80/mutillidae/?page=add-to-your-blog.php%27%20OR%20sqlspider>

| <http://192.168.56.104:80/mutillidae/index.php?page=text-file-viewer.php%27%20OR%20sqlspider>

| <http://192.168.56.104:80/mutillidae/index.php?page=html5-storage.php%27%20OR%20sqlspider>

| <http://192.168.56.104:80/mutillidae/?page=text-file-viewer.php%27%20OR%20sqlspider>

| <http://192.168.56.104:80/mutillidae/index.php?page=pen-test-tool-lookup.php%27%20OR%20sqlspider>

| <http://192.168.56.104:80/mutillidae/index.php?do=toggle-security%27%20OR%20sqlspider&page=home.php>

| <http://192.168.56.104:80/mutillidae/?page=view-someones-blog.php%27%20OR%20sqlspider>

| <http://192.168.56.104:80/mutillidae/?page=user-info.php%27%20OR%20sqlspider>

| <http://192.168.56.104:80/mutillidae/index.php?page=php-errors.php%27%20OR%20sqlspider>

| <http://192.168.56.104:80/mutillidae/index.php?page=captured-data.php%27%20OR%20sqlspider>

| <http://192.168.56.104:80/mutillidae/index.php?page=capture-data.php%27%20OR%20sqlspider>

| <http://192.168.56.104:80/mutillidae/index.php?page=usage-instructions.php%27%20OR%20sqlspider>

| <http://192.168.56.104:80/mutillidae/index.php?page=site-footer-xss-discussion.php%27%20OR%20sqlspider>

| <http://192.168.56.104:80/mutillidae/index.php?page=show-log.php%27%20OR%20sqlspider>

| <http://192.168.56.104:80/mutillidae/index.php?page=dns-lookup.php%27%20OR%20sqlspider>

| <http://192.168.56.104:80/mutillidae/index.php?page=source-viewer.php%27%20OR%20sqlspider>

| <http://192.168.56.104:80/mutillidae/index.php?page=installation.php%27%20OR%20sqlspider>

| <http://192.168.56.104:80/mutillidae/index.php?do=toggle-hints%27%20OR%20sqlspider&page=home.php>

| <http://192.168.56.104:80/mutillidae/index.php?page=framing.php%27%20OR%20sqlspider>

| <http://192.168.56.104:80/mutillidae/?page=source-viewer.php%27%20OR%20sqlspider>

| <http://192.168.56.104:80/mutillidae/?page=credits.php%27%20OR%20sqlspider>

| <http://192.168.56.104:80/mutillidae/index.php?page=login.php%27%20OR%20sqlspider>

<http://192.168.56.104:80/mutillidae/index.php?page=documentation%2Fhow-to-access-Mutillidae-over-Virtual-Box-network.php%27%20OR%20sqlspider>

| <http://192.168.56.104:80/mutillidae/?page=login.php%27%20OR%20sqlspider>

| <http://192.168.56.104:80/mutillidae/index.php?page=set-background-color.php%27%20OR%20sqlspider>

| <http://192.168.56.104:80/mutillidae/index.php?page=secret-administrative-pages.php%27%20OR%20sqlspider>

| <http://192.168.56.104:80/mutillidae/index.php?page=arbitrary-file-inclusion.php%27%20OR%20sqlspider>

| <http://192.168.56.104:80/mutillidae/index.php?page=browser-info.php%27%20OR%20sqlspider>

| <http://192.168.56.104:80/mutillidae/index.php?page=register.php%27%20OR%20sqlspider>

| <http://192.168.56.104:80/mutillidae/index.php?page=user-poll.php%27%20OR%20sqlspider>

| <http://192.168.56.104:80/mutillidae/index.php?page=view-someones-blog.php%27%20OR%20sqlspider>

| <http://192.168.56.104:80/dav/?C=M%3BO%3DD%27%20OR%20sqlspider>

| <http://192.168.56.104:80/dav/?C=S%3BO%3DA%27%20OR%20sqlspider>

| <http://192.168.56.104:80/dav/?C=D%3BO%3DA%27%20OR%20sqlspider>

| <http://192.168.56.104:80/dav/?C=N%3BO%3DA%27%20OR%20sqlspider>

| <http://192.168.56.104:80/dav/?C=M%3BO%3DA%27%20OR%20sqlspider>



1.3_Vulnerabilidades-mediante-puertos-TCP

| <http://192.168.56.104:80/dav/?C=N%3BO%3DA%27%20OR%20sqlspider>
| <http://192.168.56.104:80/dav/?C=S%3BO%3DD%27%20OR%20sqlspider>
| <http://192.168.56.104:80/dav/?C=D%3BO%3DA%27%20OR%20sqlspider>
| <http://192.168.56.104:80/dav/?C=M%3BO%3DA%27%20OR%20sqlspider>
| <http://192.168.56.104:80/dav/?C=N%3BO%3DA%27%20OR%20sqlspider>
| <http://192.168.56.104:80/dav/?C=S%3BO%3DA%27%20OR%20sqlspider>
| <http://192.168.56.104:80/dav/?C=D%3BO%3DD%27%20OR%20sqlspider>
| <http://192.168.56.104:80/dav/?C=M%3BO%3DA%27%20OR%20sqlspider>
| <http://192.168.56.104:80/dav/?C=N%3BO%3DA%27%20OR%20sqlspider>
| <http://192.168.56.104:80/dav/?C=S%3BO%3DA%27%20OR%20sqlspider>
| <http://192.168.56.104:80/dav/?C=D%3BO%3DA%27%20OR%20sqlspider>
| <http://192.168.56.104:80/rdiff/TWiki/TWikiHistory?rev1=1.9%27%20OR%20sqlspider&rev2=1.8>
| <http://192.168.56.104:80/rdiff/TWiki/TWikiHistory?rev1=1.9&rev2=1.8%27%20OR%20sqlspider>
| <http://192.168.56.104:80/view/TWiki/TWikiHistory?rev=1.9%27%20OR%20sqlspider>
| <http://192.168.56.104:80/view/TWiki/TWikiHistory?rev=1.7%27%20OR%20sqlspider>
| <http://192.168.56.104:80/oops/TWiki/TWikiHistory?template=oopsrev%27%20OR%20sqlspider¶m1=1.10>
| <http://192.168.56.104:80/oops/TWiki/TWikiHistory?template=oopsrev¶m1=1.10%27%20OR%20sqlspider>
| <http://192.168.56.104:80/view/TWiki/TWikiHistory?rev=1.8%27%20OR%20sqlspider>
| <http://192.168.56.104:80/rdiff/TWiki/TWikiHistory?rev1=1.10%27%20OR%20sqlspider&rev2=1.9>
| <http://192.168.56.104:80/rdiff/TWiki/TWikiHistory?rev1=1.10&rev2=1.9%27%20OR%20sqlspider>
| <http://192.168.56.104:80/rdiff/TWiki/TWikiHistory?rev1=1.8%27%20OR%20sqlspider&rev2=1.7>
| <http://192.168.56.104:80/rdiff/TWiki/TWikiHistory?rev1=1.8&rev2=1.7%27%20OR%20sqlspider>
| <http://192.168.56.104:80/rdiff/TWiki/TWikiHistory?rev1=1.9%27%20OR%20sqlspider&rev2=1.8>
| <http://192.168.56.104:80/rdiff/TWiki/TWikiHistory?rev1=1.9&rev2=1.8%27%20OR%20sqlspider>
| <http://192.168.56.104:80/view/TWiki/TWikiHistory?rev=1.9%27%20OR%20sqlspider>
| <http://192.168.56.104:80/view/TWiki/TWikiHistory?rev=1.7%27%20OR%20sqlspider>
| <http://192.168.56.104:80/oops/TWiki/TWikiHistory?template=oopsrev%27%20OR%20sqlspider¶m1=1.10>
| <http://192.168.56.104:80/oops/TWiki/TWikiHistory?template=oopsrev¶m1=1.10%27%20OR%20sqlspider>
| <http://192.168.56.104:80/view/TWiki/TWikiHistory?rev=1.8%27%20OR%20sqlspider>
| <http://192.168.56.104:80/rdiff/TWiki/TWikiHistory?rev1=1.10%27%20OR%20sqlspider&rev2=1.9>
| <http://192.168.56.104:80/rdiff/TWiki/TWikiHistory?rev1=1.10&rev2=1.9%27%20OR%20sqlspider>
| <http://192.168.56.104:80/rdiff/TWiki/TWikiHistory?rev1=1.8%27%20OR%20sqlspider&rev2=1.7>
| <http://192.168.56.104:80/rdiff/TWiki/TWikiHistory?rev1=1.8&rev2=1.7%27%20OR%20sqlspider>
| <http://192.168.56.104:80/mutillidae/index.php?page=change-log.htm%27%20OR%20sqlspider>
| <http://192.168.56.104:80/mutillidae/index.php?page=documentation%2Fvulnerabilities.php%27%20OR%20sqlspider>
| <http://192.168.56.104:80/mutillidae/index.php?page=add-to-your-blog.php%27%20OR%20sqlspider>
| <http://192.168.56.104:80/mutillidae/index.php?do=toggle-hints%27%20OR%20sqlspider&page=change-log.htm>
| <http://192.168.56.104:80/mutillidae/?page=show-log.php%27%20OR%20sqlspider>
| <http://192.168.56.104:80/mutillidae/index.php?page=home.php%27%20OR%20sqlspider>
| <http://192.168.56.104:80/mutillidae/index.php?page=password-generator.php%27%20OR%20sqlspider&username=ano>



1.3_Vulnerabilidades-mediante-puertos-TCP

nymous

| <http://192.168.56.104:80/mutillidae/index.php?page=credits.php%27%20OR%20sqlspider>
| <http://192.168.56.104:80/mutillidae/index.php?do=toggle-security%27%20OR%20sqlspider&page=change-log.htm>
| <http://192.168.56.104:80/mutillidae/?page=add-to-your-blog.php%27%20OR%20sqlspider>
| <http://192.168.56.104:80/mutillidae/index.php?page=text-file-viewer.php%27%20OR%20sqlspider>
| <http://192.168.56.104:80/mutillidae/index.php?page=html5-storage.php%27%20OR%20sqlspider>
| <http://192.168.56.104:80/mutillidae/?page=text-file-viewer.php%27%20OR%20sqlspider>
| <http://192.168.56.104:80/mutillidae/index.php?page=pen-test-tool-lookup.php%27%20OR%20sqlspider>
| <http://192.168.56.104:80/mutillidae/?page=view-someones-blog.php%27%20OR%20sqlspider>
| <http://192.168.56.104:80/mutillidae/?page=user-info.php%27%20OR%20sqlspider>
| <http://192.168.56.104:80/mutillidae/index.php?page=view-someones-blog.php%27%20OR%20sqlspider>
| <http://192.168.56.104:80/mutillidae/index.php?page=captured-data.php%27%20OR%20sqlspider>
| <http://192.168.56.104:80/mutillidae/index.php?page=capture-data.php%27%20OR%20sqlspider>
| <http://192.168.56.104:80/mutillidae/index.php?page=show-log.php%27%20OR%20sqlspider>
| <http://192.168.56.104:80/mutillidae/index.php?page=dns-lookup.php%27%20OR%20sqlspider>
| <http://192.168.56.104:80/mutillidae/index.php?page=browser-info.php%27%20OR%20sqlspider>
| <http://192.168.56.104:80/mutillidae/index.php?page=installation.php%27%20OR%20sqlspider>
| <http://192.168.56.104:80/mutillidae/index.php?page=framing.php%27%20OR%20sqlspider>
| <http://192.168.56.104:80/mutillidae/?page=source-viewer.php%27%20OR%20sqlspider>
| <http://192.168.56.104:80/mutillidae/?page=credits.php%27%20OR%20sqlspider>
| <http://192.168.56.104:80/mutillidae/?page=login.php%27%20OR%20sqlspider>
| <http://192.168.56.104:80/mutillidae/index.php?page=login.php%27%20OR%20sqlspider>
|
<http://192.168.56.104:80/mutillidae/index.php?page=documentation%2Fhow-to-access-Mutillidae-over-Virtual-Box-network.php%27%20OR%20sqlspider>
| <http://192.168.56.104:80/mutillidae/index.php?page=source-viewer.php%27%20OR%20sqlspider>
| <http://192.168.56.104:80/mutillidae/index.php?page=set-background-color.php%27%20OR%20sqlspider>
| <http://192.168.56.104:80/mutillidae/index.php?page=secret-administrative-pages.php%27%20OR%20sqlspider>
| <http://192.168.56.104:80/mutillidae/index.php?page=arbitrary-file-inclusion.php%27%20OR%20sqlspider>
| <http://192.168.56.104:80/mutillidae/index.php?page=register.php%27%20OR%20sqlspider>
| <http://192.168.56.104:80/mutillidae/index.php?page=site-footer-xss-discussion.php%27%20OR%20sqlspider>
| <http://192.168.56.104:80/mutillidae/index.php?page=user-poll.php%27%20OR%20sqlspider>
| <http://192.168.56.104:80/mutillidae/index.php?page=user-info.php%27%20OR%20sqlspider>
| <http://192.168.56.104:80/mutillidae/index.php?page=change-log.htm%27%20OR%20sqlspider>
| <http://192.168.56.104:80/mutillidae/index.php?page=documentation%2Fvulnerabilities.php%27%20OR%20sqlspider>
| <http://192.168.56.104:80/mutillidae/index.php?page=add-to-your-blog.php%27%20OR%20sqlspider>
| <http://192.168.56.104:80/mutillidae/index.php?page=user-info.php%27%20OR%20sqlspider>
| <http://192.168.56.104:80/mutillidae/?page=show-log.php%27%20OR%20sqlspider>
| <http://192.168.56.104:80/mutillidae/index.php?page=home.php%27%20OR%20sqlspider>
|
<http://192.168.56.104:80/mutillidae/index.php?page=password-generator.php%27%20OR%20sqlspider&username=ano>



1.3_Vulnerabilidades-mediante-puertos-TCP

nymous

| <http://192.168.56.104:80/mutillidae/index.php?page=credits.php%27%20OR%20sqlspider>
| <http://192.168.56.104:80/mutillidae/?page=add-to-your-blog.php%27%20OR%20sqlspider>
| <http://192.168.56.104:80/mutillidae/index.php?page=text-file-viewer.php%27%20OR%20sqlspider>
| <http://192.168.56.104:80/mutillidae/index.php?page=html5-storage.php%27%20OR%20sqlspider>
| <http://192.168.56.104:80/mutillidae/?page=text-file-viewer.php%27%20OR%20sqlspider>
| <http://192.168.56.104:80/mutillidae/index.php?page=pen-test-tool-lookup.php%27%20OR%20sqlspider>
| <http://192.168.56.104:80/mutillidae/index.php?page=view-someones-blog.php%27%20OR%20sqlspider>
| <http://192.168.56.104:80/mutillidae/?page=view-someones-blog.php%27%20OR%20sqlspider>
| <http://192.168.56.104:80/mutillidae/?page=user-info.php%27%20OR%20sqlspider>
| <http://192.168.56.104:80/mutillidae/index.php?page=captured-data.php%27%20OR%20sqlspider>
| <http://192.168.56.104:80/mutillidae/index.php?page=capture-data.php%27%20OR%20sqlspider>
| <http://192.168.56.104:80/mutillidae/index.php?page=show-log.php%27%20OR%20sqlspider>
| <http://192.168.56.104:80/mutillidae/index.php?page=dns-lookup.php%27%20OR%20sqlspider>
| <http://192.168.56.104:80/mutillidae/index.php?page=browser-info.php%27%20OR%20sqlspider>
| <http://192.168.56.104:80/mutillidae/index.php?page=installation.php%27%20OR%20sqlspider>
| <http://192.168.56.104:80/mutillidae/index.php?page=framing.php%27%20OR%20sqlspider>
| <http://192.168.56.104:80/mutillidae/?page=source-viewer.php%27%20OR%20sqlspider>
| <http://192.168.56.104:80/mutillidae/?page=credits.php%27%20OR%20sqlspider>
| <http://192.168.56.104:80/mutillidae/?page=login.php%27%20OR%20sqlspider>
| <http://192.168.56.104:80/mutillidae/index.php?page=login.php%27%20OR%20sqlspider>
|
<http://192.168.56.104:80/mutillidae/index.php?page=documentation%2Fhow-to-access-Mutillidae-over-Virtual-Box-netw>
<ork.php%27%20OR%20sqlspider>
| <http://192.168.56.104:80/mutillidae/index.php?page=source-viewer.php%27%20OR%20sqlspider>
| <http://192.168.56.104:80/mutillidae/index.php?page=set-background-color.php%27%20OR%20sqlspider>
| <http://192.168.56.104:80/mutillidae/index.php?page=secret-administrative-pages.php%27%20OR%20sqlspider>
| <http://192.168.56.104:80/mutillidae/index.php?page=arbitrary-file-inclusion.php%27%20OR%20sqlspider>
| <http://192.168.56.104:80/mutillidae/index.php?page=register.php%27%20OR%20sqlspider>
| <http://192.168.56.104:80/mutillidae/index.php?page=user-poll.php%27%20OR%20sqlspider>
| <http://192.168.56.104:80/mutillidae/index.php?page=site-footer-xss-discussion.php%27%20OR%20sqlspider>
| <http://192.168.56.104:80/mutillidae/index.php?page=change-log.htm%27%20OR%20sqlspider>
| <http://192.168.56.104:80/mutillidae/index.php?page=add-to-your-blog.php%27%20OR%20sqlspider>
| <http://192.168.56.104:80/mutillidae/index.php?page=user-info.php%27%20OR%20sqlspider>
| <http://192.168.56.104:80/mutillidae/?page=show-log.php%27%20OR%20sqlspider>
| <http://192.168.56.104:80/mutillidae/index.php?page=home.php%27%20OR%20sqlspider>
|
<http://192.168.56.104:80/mutillidae/index.php?page=password-generator.php%27%20OR%20sqlspider&username=ano>
<nymous>
| <http://192.168.56.104:80/mutillidae/index.php?page=credits.php%27%20OR%20sqlspider>
| <http://192.168.56.104:80/mutillidae/?page=add-to-your-blog.php%27%20OR%20sqlspider>



1.3_Vulnerabilidades-mediante-puertos-TCP

```
| http://192.168.56.104:80/mutillidae/index.php?page=text-file-viewer.php%27%20OR%20sqlspider
| http://192.168.56.104:80/mutillidae/index.php?page=html5-storage.php%27%20OR%20sqlspider
| http://192.168.56.104:80/mutillidae/?page=text-file-viewer.php%27%20OR%20sqlspider
| http://192.168.56.104:80/mutillidae/index.php?page=pen-test-tool-lookup.php%27%20OR%20sqlspider
| http://192.168.56.104:80/mutillidae/?page=view-someones-blog.php%27%20OR%20sqlspider
| http://192.168.56.104:80/mutillidae/?page=user-info.php%27%20OR%20sqlspider
| http://192.168.56.104:80/mutillidae/index.php?page=captured-data.php%27%20OR%20sqlspider
| http://192.168.56.104:80/mutillidae/index.php?page=capture-data.php%27%20OR%20sqlspider
| http://192.168.56.104:80/mutillidae/index.php?page=browser-info.php%27%20OR%20sqlspider
| http://192.168.56.104:80/mutillidae/index.php?page=site-footer-xss-discussion.php%27%20OR%20sqlspider
| http://192.168.56.104:80/mutillidae/index.php?page=show-log.php%27%20OR%20sqlspider
| http://192.168.56.104:80/mutillidae/index.php?page=dns-lookup.php%27%20OR%20sqlspider
| http://192.168.56.104:80/mutillidae/index.php?page=documentation%2Fvulnerabilities.php%27%20OR%20sqlspider
| http://192.168.56.104:80/mutillidae/index.php?page=installation.php%27%20OR%20sqlspider
| http://192.168.56.104:80/mutillidae/index.php?page=framing.php%27%20OR%20sqlspider
| http://192.168.56.104:80/mutillidae/?page=source-viewer.php%27%20OR%20sqlspider
| http://192.168.56.104:80/mutillidae/?page=credits.php%27%20OR%20sqlspider
| http://192.168.56.104:80/mutillidae/?page=login.php%27%20OR%20sqlspider
| http://192.168.56.104:80/mutillidae/index.php?page=login.php%27%20OR%20sqlspider
|
http://192.168.56.104:80/mutillidae/index.php?page=documentation%2Fhow-to-access-Mutillidae-over-Virtual-Box-netw
ork.php%27%20OR%20sqlspider
| http://192.168.56.104:80/mutillidae/index.php?page=source-viewer.php%27%20OR%20sqlspider
| http://192.168.56.104:80/mutillidae/index.php?page=set-background-color.php%27%20OR%20sqlspider
| http://192.168.56.104:80/mutillidae/index.php?page=secret-administrative-pages.php%27%20OR%20sqlspider
| http://192.168.56.104:80/mutillidae/index.php?page=arbitrary-file-inclusion.php%27%20OR%20sqlspider
| http://192.168.56.104:80/mutillidae/index.php?page=register.php%27%20OR%20sqlspider
| http://192.168.56.104:80/mutillidae/index.php?page=user-poll.php%27%20OR%20sqlspider
| http://192.168.56.104:80/mutillidae/index.php?page=view-someones-blog.php%27%20OR%20sqlspider
111/tcp open rpcbind
139/tcp open netbios-ssn
445/tcp open microsoft-ds
512/tcp open exec
513/tcp open login
514/tcp open shell
1099/tcp open rmiregistry
| 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
```




1.3_Vulnerabilidades-mediante-puertos-TCP

execution.

|

| References:

| https://github.com/rapid7/metasploit-framework/blob/master/modules/exploits/multi/misc/java_rmi_server.rb

| 1524/tcp open ingreslock

| 2049/tcp open nfs

| 2121/tcp open ccproxy-ftp

| 3306/tcp open mysql

| _ssl-ccs-injection: No reply from server (TIMEOUT)

| 5432/tcp open postgresql

| ssl-dh-params:

| VULNERABLE:

| 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_3DES_EDE_CBC_SHA

| Modulus Type: Safe prime

| Modulus Source: Unknown/Custom-generated

| Modulus Length: 1024

| Generator Length: 8

| Public Key Length: 1024

| References:

| <https://weakdh.org>

| _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.

|

| References:

| <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0224>



1.3_Vulnerabilidades-mediante-puertos-TCP

```
| http://www.cvedetails.com/cve/2014-0224
|_ http://www.openssl.org/news/secadv_20140605.txt
| ssl-poodle:
| VULNERABLE:
| SSL POODLE information leak
| State: VULNERABLE
| IDs: CVE:CVE-2014-3566 BID:70574
| 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://www.imperialviolet.org/2014/10/14/poodle.html
| https://www.securityfocus.com/bid/70574
| https://www.openssl.org/~bodo/ssl-poodle.pdf
|_ https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-3566
5900/tcp open vnc
6000/tcp open X11
6667/tcp open irc
|_irc-unrealircd-backdoor: Looks like trojaned version of unrealircd. See http://seclists.org/fulldisclosure/2010/Jun/277
8009/tcp open ajp13
8180/tcp open unknown
| 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
```



1.3_Vulnerabilidades-mediante-puertos-TCP

- | /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-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:



1.3_Vulnerabilidades-mediante-puertos-TCP

```
| 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:  
|    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
```




1.3_Vulnerabilidades-mediante-puertos-TCP

```
| /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:
| http://ha.ckers.org/slowloris/
|_ https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-6750
MAC Address: 08:00:27:F2:C3:90 (Oracle VirtualBox virtual NIC)
```

Host script results:

```
_smb-vuln-ms10-061: false
_smb-vuln-regsvc-dos: ERROR: Script execution failed (use -d to debug)
_smb-vuln-ms10-054: false
```

Read data files from: /usr/bin/./share/nmap

Nmap done at Tue Jan 31 02:05:30 2023 -- 1 IP address (1 host up) scanned in 313.69 seconds

(end of excerpt)



1.3_Escaneo-de-vulnerabilidades-utilizando-servicios-obtenidos-con-NMAP

Dirección IP:

```
# Nmap 7.93 scan initiated Tue Jan 31 02:05:30 2023 as: nmap -sV --script=vulners --script-args mincvss=7.5
--stylesheet=https://svn.nmap.org/nmap/docs/nmap.xsl -oA
/src/archivos/hosts/fase_3/192.168.56.104vulners_nmap_serv 192.168.56.104
Nmap scan report for 192.168.56.104
Host is up (0.00026s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE  VERSION
21/tcp    open  ftp      vsftpd 2.3.4
22/tcp    open  ssh      OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp    open  telnet   Linux telnetd
25/tcp    open  smtp     Postfix smtpd
53/tcp    open  domain   ISC BIND 9.4.2
80/tcp    open  http     Apache httpd 2.2.8 ((Ubuntu) DAV/2)
|_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      38100/tcp  mountd
|  100005 1,2,3      40615/udp  mountd
|  100021 1,3,4      44943/udp  nlockmgr
|  100021 1,3,4      56517/tcp  nlockmgr
|  100024 1          43932/tcp  status
|_ 100024 1          44439/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  shell     Netkit rshd
1099/tcp  open  java-rmi   GNU Classpath grmiregistry
1524/tcp  open  bindshell  Metasploitable root shell
2049/tcp  open  nfs       2-4 (RPC #100003)
2121/tcp  open  ftp       ProFTPD 1.3.1
3306/tcp  open  mysql     MySQL 5.0.51a-3ubuntu5
5432/tcp  open  postgresql PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp  open  vnc       VNC (protocol 3.3)
6000/tcp  open  X11       (access denied)
6667/tcp  open  irc       UnrealIRCd
8009/tcp  open  ajp13     Apache Jserv (Protocol v1.3)
8180/tcp  open  http      Apache Tomcat/Coyote JSP engine 1.1
|_http-server-header: Apache-Coyote/1.1
```



1.3_Escaneo-de-vulnerabilidades-utilizando-servicios-obtenidos-con-NMAP

MAC Address: 08:00:27:F2:C3:90 (Oracle VirtualBox virtual NIC)

Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at <https://nmap.org/submit/>.

Nmap done at Tue Jan 31 02:05:43 2023 -- 1 IP address (1 host up) scanned in 12.65 seconds

(end of excerpt)
