# ETHICAL HACKING COURSE

## MINOR PROJECT

## NMAP SCANNING AND FINDING VULNERABILITIES

SUBMITTED BY: ANWESHA GUPTA
SUBMITTED TO: MOHSIN QURESH

# SCOPES

- Setting Up the Labs

- N-map Scanning

- Checking the Vulnerability and Exploitation

# SETTING UP THE LAB

- For any penetration testing first of all we need to set a Lab

- The lab can be set in two modes.
  They are:
  (a) Live mode
  (b) Virtualization mode

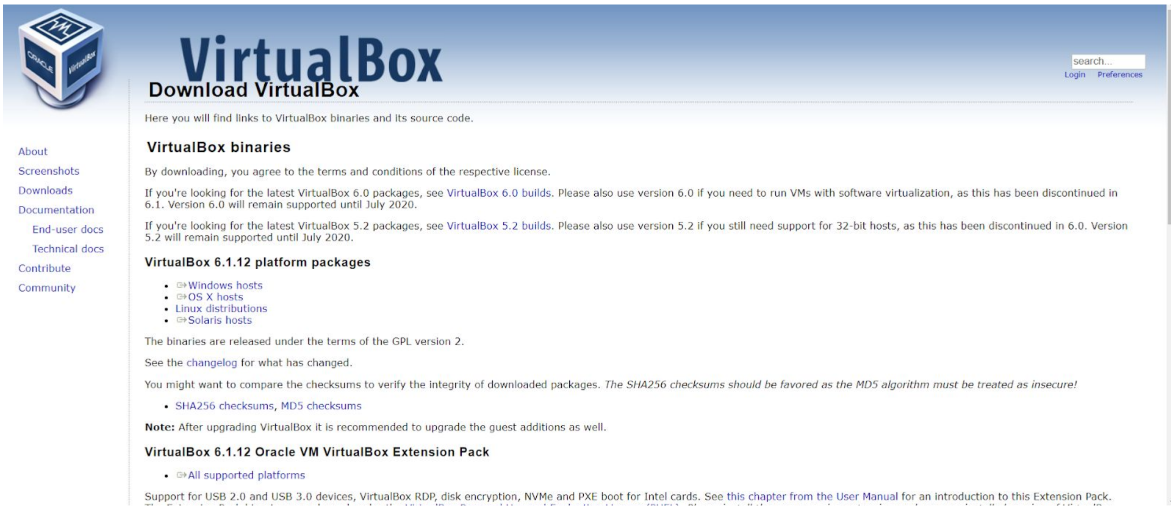
- In the case of the live mode the testing can be done by using the OS in live.

- In the Virtualization mode we have to install Virtual Box in the host machine. The Download Link is given below.

- Download link is: https://download.virtualbox.org/virtualbox/6.1.12/VirtualBox-6.1.12-139181-Win.exe

# STEPS TO SETUP LAB

## STEP 1: DOWNLOAD VIRTUAL BOX



### Download VirtualBox

Here you will find links to VirtualBox binaries and its source code.

### VirtualBox binaries

By downloading, you agree to the terms and conditions of the respective license.

If you're looking for the latest VirtualBox 6.0 packages, see VirtualBox 6.0 builds. Please also use version 6.0 if you need to run VMs with software virtualization, as this has been discontinued in 6.1. Version 6.0 will remain supported until July 2020.

If you're looking for the latest VirtualBox 5.2 packages, see VirtualBox 5.2 builds. Please also use version 5.2 if you still need support for 32-bit hosts, as this has been discontinued in 6.0. Version 5.2 will remain supported until July 2020.

### VirtualBox 6.1.12 platform packages

- Windows hosts
- OS X hosts
- Linux distributions
- Solaris hosts

The binaries are released under the terms of the GPL version 2.

See the changelog for what has changed.

You might want to compare the checksums to verify the integrity of downloaded packages. *The SHA256 checksums should be favored as the MD5 algorithm must be treated as insecure!*

- SHA256 checksums, MD5 checksums

**Note:** After upgrading VirtualBox it is recommended to upgrade the guest additions as well.

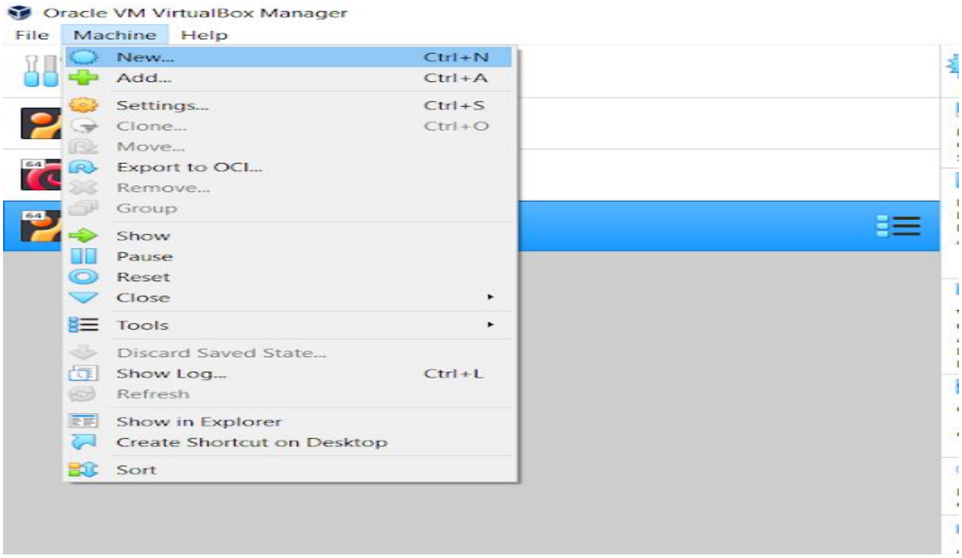
### VirtualBox 6.1.12 Oracle VM VirtualBox Extension Pack

- All supported platforms

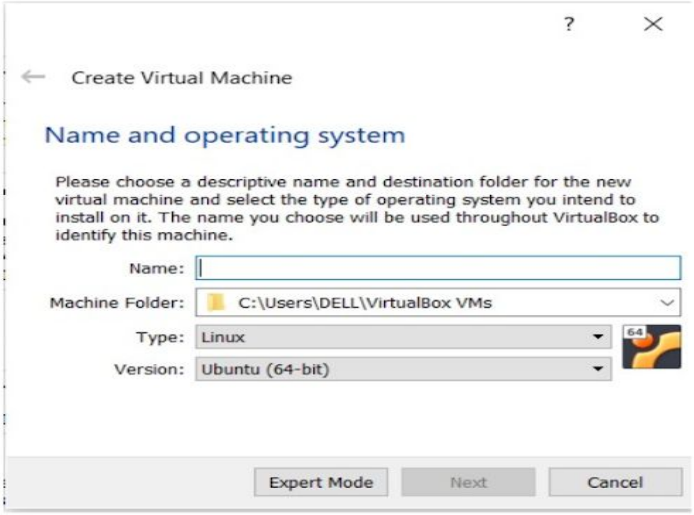
Support for USB 2.0 and USB 3.0 devices, VirtualBox RDP, disk encryption, NVMe and PXE boot for Intel cards. See this chapter from the User Manual for an introduction to this Extension Pack.

## STEP 2:OPEN VIRTUAL BOX

## STEP 3: CLICK ON  MACHINE OPTION AND THEN SELECT NEW



STEP 4:Fill the name of lab .Then Select Linux in type and Ubuntu(64-Bit)in version and click on next.



Name and operating system

Please choose a descriptive name and destination folder for the new virtual machine and select the type of operating system you intend to install on it. The name you choose will be used throughout VirtualBox to identify this machine.

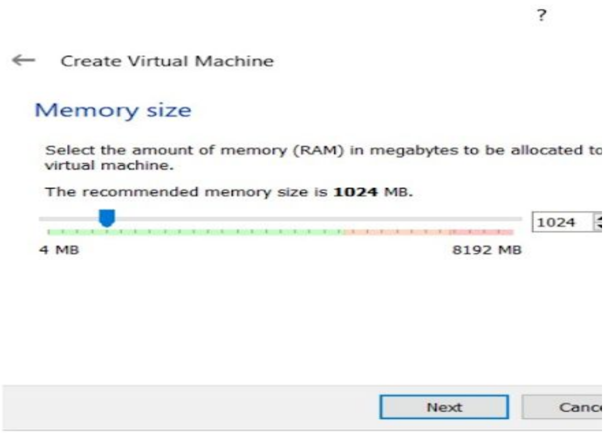
Name:

Machine Folder: C:\Users\DELL\VirtualBox VMs

Type: Linux

Version: Ubuntu (64-bit)

STEP 5: Allocate the memory (RAM) not less than 2GB and click Next.



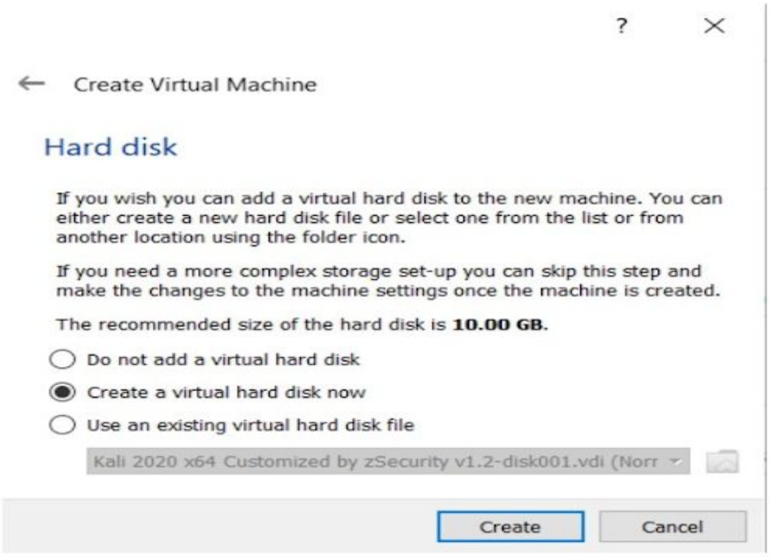
Memory size

Select the amount of memory (RAM) in megabytes to be allocated tc virtual machine.

The recommended memory size is **1024** MB.

1024

STEP 6: Then Select on create a virtual hard disk now and Click on Create.



Create Virtual Machine

Hard disk

If you wish you can add a virtual hard disk to the new machine. You can either create a new hard disk file or select one from the list or from another location using the folder icon.

If you need a more complex storage set-up you can skip this step and make the changes to the machine settings once the machine is created.

The recommended size of the hard disk is **10.00 GB**.

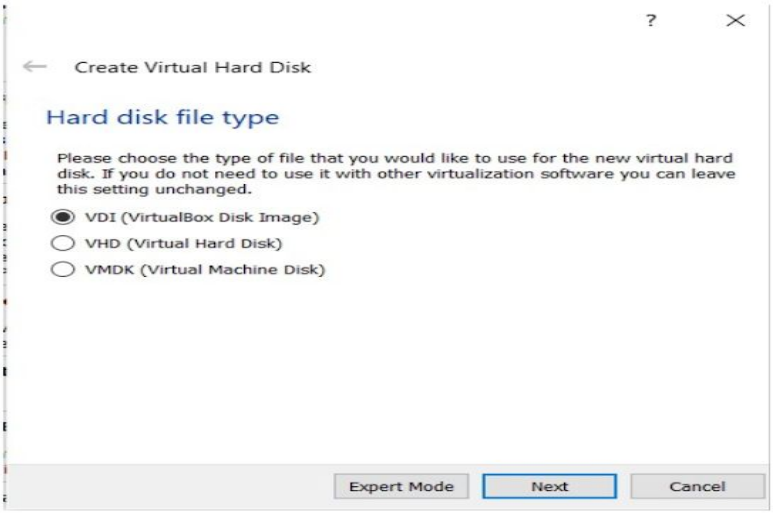
○ Do not add a virtual hard disk

● Create a virtual hard disk now

○ Use an existing virtual hard disk file

Kali 2020 x64 Customized by zSecurity v1.2-disk001.vdi (Norr

STEP 7:Click on VDI (Virtual Disk Image) and click next



Create Virtual Hard Disk

Hard disk file type

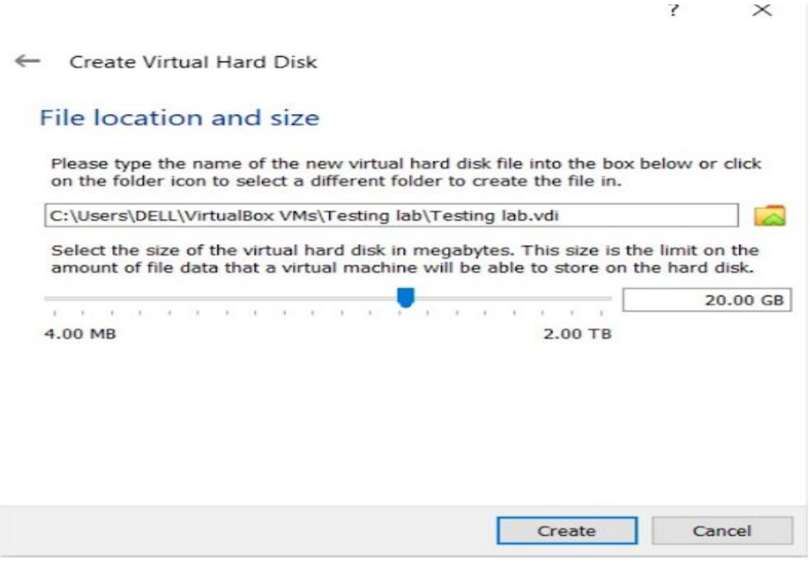
Please choose the type of file that you would like to use for the new virtual hard disk. If you do not need to use it with other virtualization software you can leave this setting unchanged.

● VDI (VirtualBox Disk Image)

○ VHD (Virtual Hard Disk)

○ VMDK (Virtual Machine Disk)

STEP 8: Then allocation of Size upto 20GB and Click On create.



Create Virtual Hard Disk

File location and size

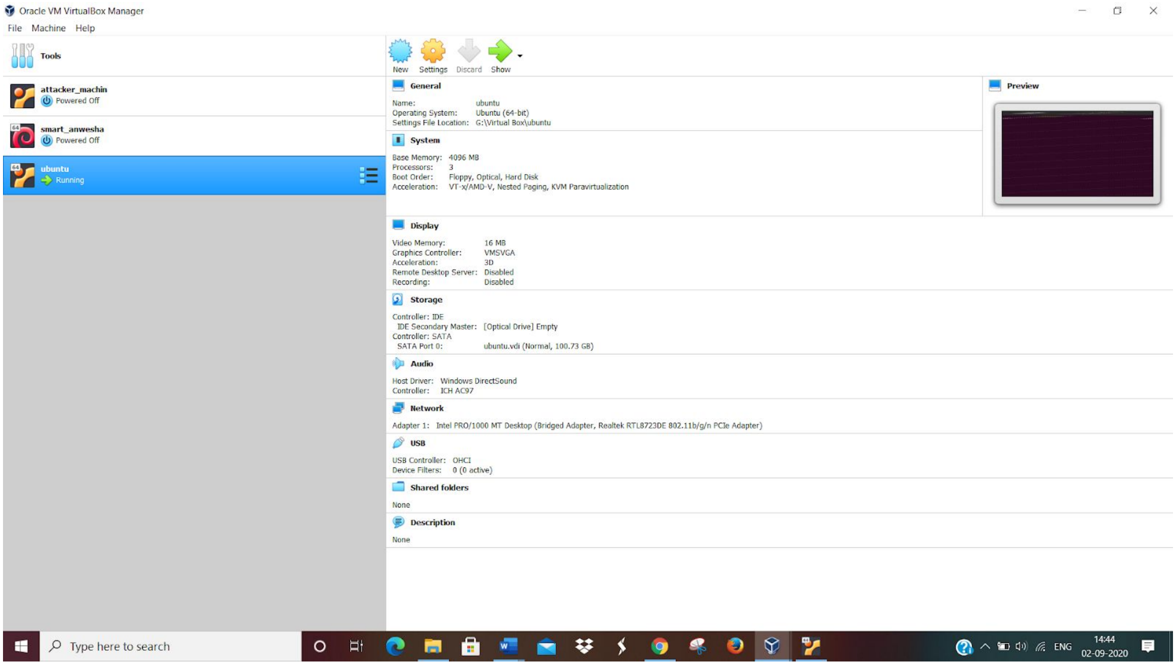
Please type the name of the new virtual hard disk file into the box below or click on the folder icon to select a different folder to create the file in.

C:\Users\DELL\VirtualBox VMs\Testing lab\Testing lab.vdi

Select the size of the virtual hard disk in megabytes. This size is the limit on the amount of file data that a virtual machine will be able to store on the hard disk.

20.00 GB

STEP 9:Hence Lab is created , now add ISO file in that and configure it.



**General**

Name: ubuntu
Operating System: Ubuntu (64-bit)
Settings File Location: G:\Virtual Box\ubuntu

**System**

Base Memory: 4096 MB
Processors: 3
Boot Order: Floppy, Optical, Hard Disk
Acceleration: VT-x/AMD-V, Nested Paging, KVM Paravirtualization

**Display**

Video Memory: 16 MB
Graphics Controller: VMSVGA
Acceleration: 3D
Remote Desktop Server: Disabled
Recording: Disabled

**Storage**

Controller: IDE
IDE Secondary Master: [Optical Drive] Empty
Controller: SATA
SATA Port 0: ubuntu.vdi (Normal, 100.73 GB)

**Audio**

Host Driver: Windows DirectSound
Controller: ICH AC97

**Network**

Adapter 1: Intel PRO/1000 MT Desktop (Bridged Adapter, Realtek RTL8723DE 802.11b/g/n PCIe Adapter)

**USB**

USB Controller: OHCI
Device Filters: 0 (0 active)

**Shared folders**

None

**Description**

None

# NMAP SCANNING

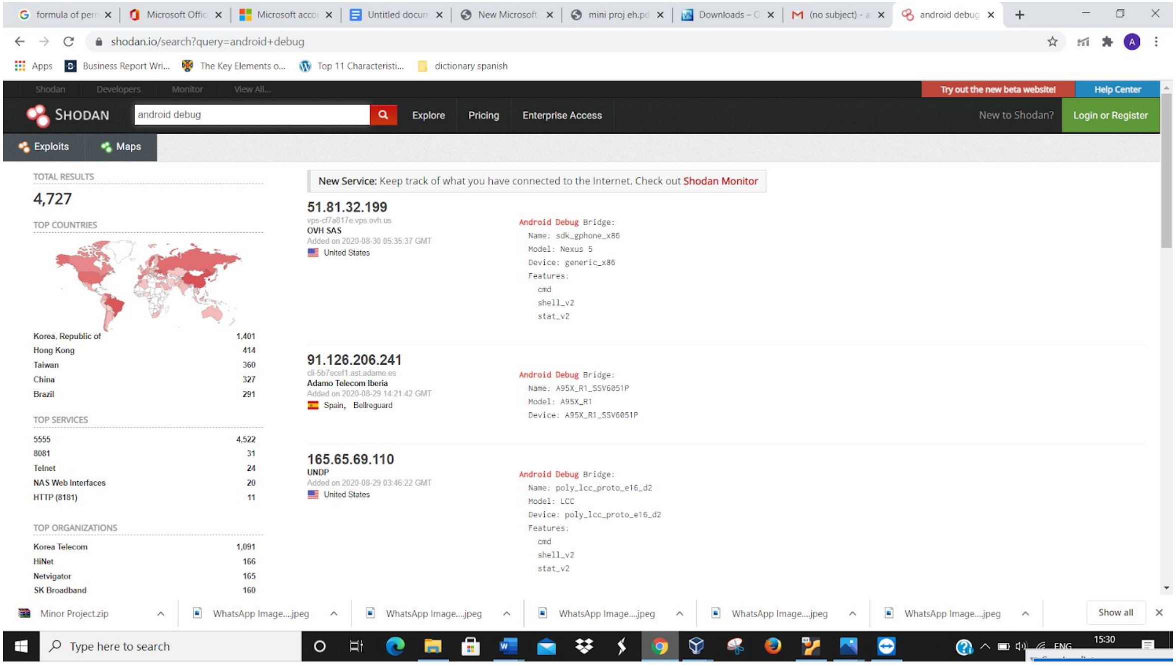
STEP 1: Open the ubuntu setup from virtual box and then open its teriminal.

STEP 2: To get root access use the command “sudo passwd” and then type your login password there. Then set new password for the root access . Then use the command “su” and then type the password set above to get the root access.

STEP 3: Update the machine using “apt update”.

STEP 4: Then install nmap using command “apt install nmap”

STEP 5: Then we have to find a suitable IP address for scanning and then finding the vulnerabilities.



TOTAL RESULTS

4,727

TOP COUNTRIES

| | |
|---|---|
| Korea, Republic of | 1,401 |
| Hong Kong | 414 |
| Taiwan | 360 |
| China | 327 |
| Brazil | 291 |

TOP SERVICES

| | |
|---|---|
| 5555 | 4,522 |
| 8081 | 31 |
| Telnet | 24 |
| NAS Web Interfaces | 20 |
| HTTP (8181) | 11 |

TOP ORGANIZATIONS

| | |
|---|---|
| Korea Telecom | 1,091 |
| HiNet | 166 |
| Netvigator | 165 |
| SK Broadband | 160 |

New Service: Keep track of what you have connected to the Internet. Check out Shodan Monitor

51.81.32.199
vps-cf7a817e.vps.ovh.us
OVH SAS
Added on 2020-08-30 05:35:37 GMT
United States

```
Android Debug Bridge:
  Name: sdk_gphone_x86
  Model: Nexus 5
  Device: generic_x86
  Features:
    cmd
    shell_v2
    stat_v2
```

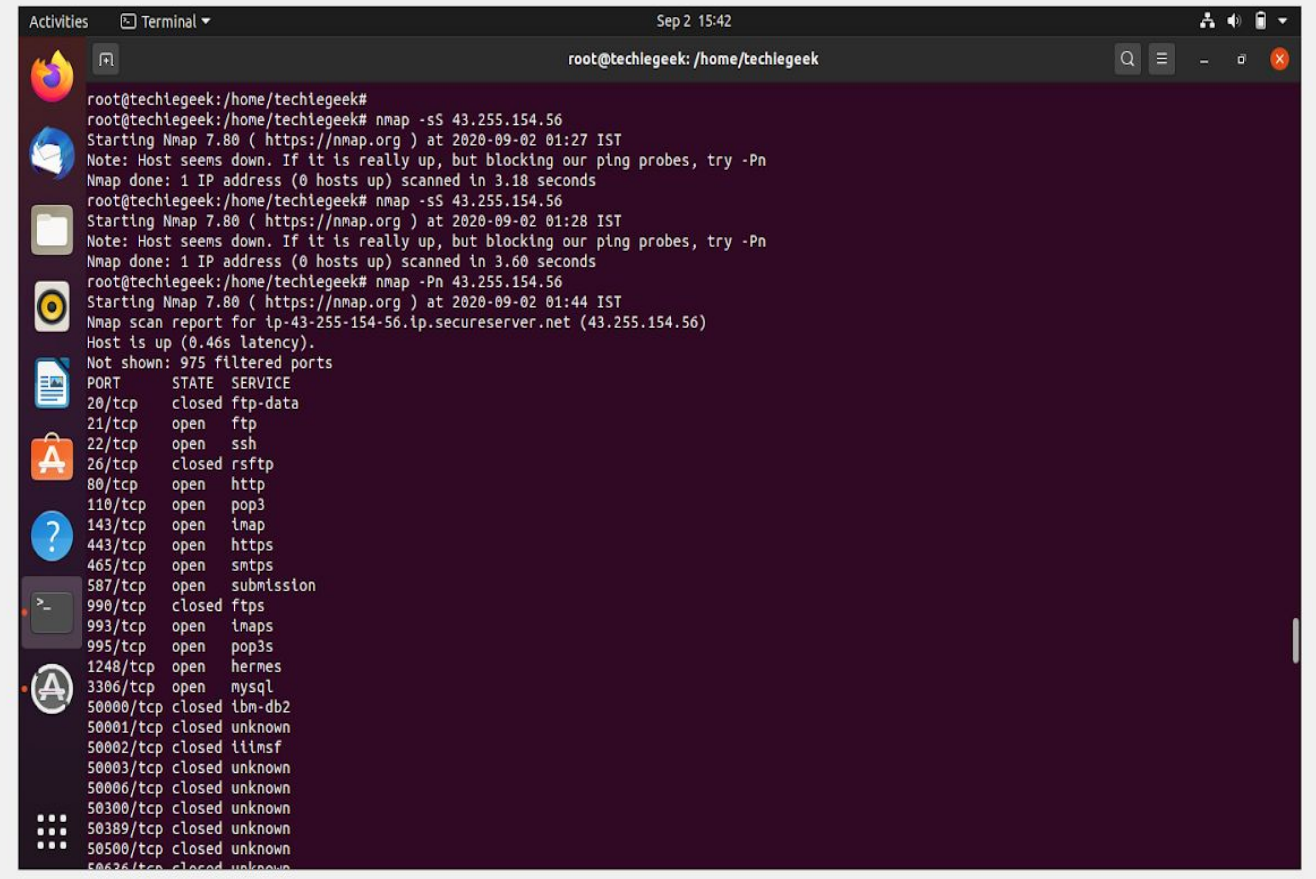
91.126.206.241
cli-5b7ecef1.ast.adamo.es
Adamo Telecom Iberia
Added on 2020-08-29 14:21:42 GMT
Spain, Bellreguard

```
Android Debug Bridge:
  Name: A95X_R1_SSV6051P
  Model: A95X_R1
  Device: A95X_R1_SSV6051P
```

165.65.69.110
UNDP
Added on 2020-08-29 03:46:22 GMT
United States

```
Android Debug Bridge:
  Name: poly_lcc_proto_e16_d2
  Model: LCC
  Device: poly_lcc_proto_e16_d2
  Features:
    cmd
    shell_v2
    stat_v2
```

STEP 6: Now for scanning use the command “ nmap -sS 43.255.154.56 “ .



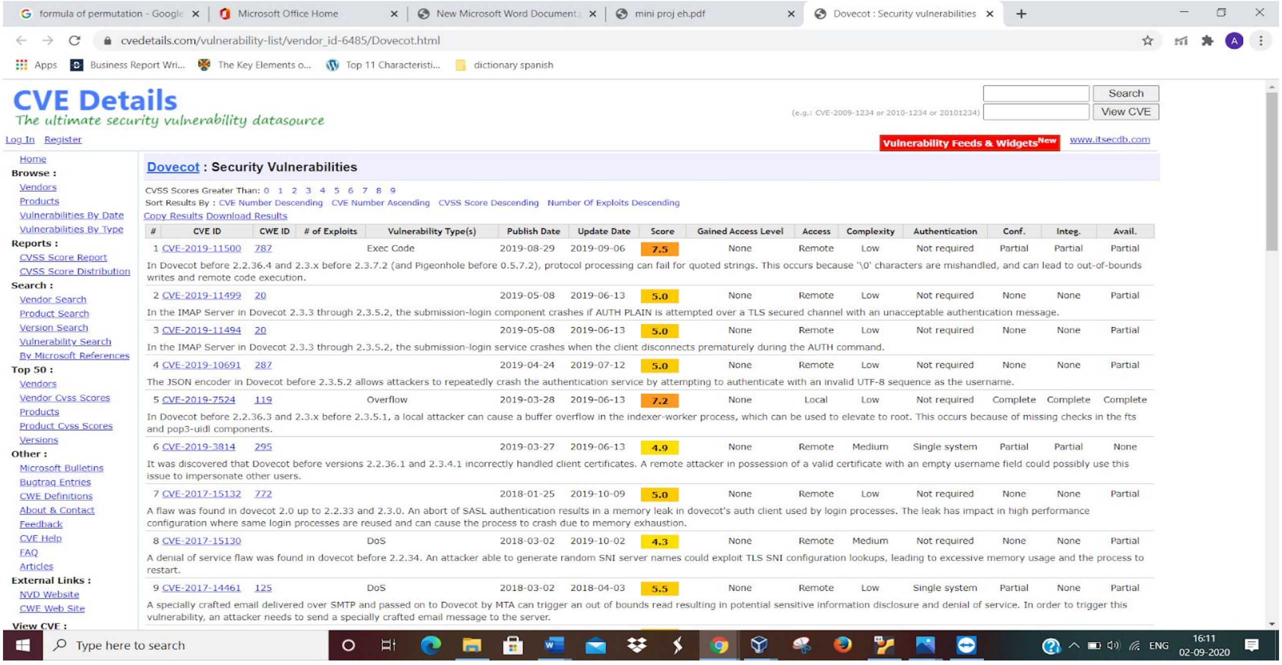
```
root@techiegeek:/home/techiegeek#
root@techiegeek:/home/techiegeek# nmap -sS 43.255.154.56
Starting Nmap 7.80 ( https://nmap.org ) at 2020-09-02 01:27 IST
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 3.18 seconds
root@techiegeek:/home/techiegeek# nmap -sS 43.255.154.56
Starting Nmap 7.80 ( https://nmap.org ) at 2020-09-02 01:28 IST
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 3.60 seconds
root@techiegeek:/home/techiegeek# nmap -Pn 43.255.154.56
Starting Nmap 7.80 ( https://nmap.org ) at 2020-09-02 01:44 IST
Nmap scan report for ip-43-255-154-56.ip.secureserver.net (43.255.154.56)
Host is up (0.46s latency).
Not shown: 975 filtered ports
PORT      STATE  SERVICE
20/tcp    closed ftp-data
21/tcp    open   ftp
22/tcp    open   ssh
26/tcp    closed rsftp
80/tcp    open   http
110/tcp   open   pop3
143/tcp   open   imap
443/tcp   open   https
465/tcp   open   smtps
587/tcp   open   submission
990/tcp   closed ftps
993/tcp   open   imaps
995/tcp   open   pop3s
1248/tcp  open   hermes
3306/tcp  open   mysql
50000/tcp closed ibm-db2
50001/tcp closed unknown
50002/tcp closed iiimsf
50003/tcp closed unknown
50006/tcp closed unknown
50300/tcp closed unknown
50389/tcp closed unknown
50500/tcp closed unknown
50636/tcp closed unknown
```

STEP 7: To get the version of the ports that are open use the command " nmap -sS 43.255.154.56 ".

| PORT | STATE | VERSION |
|---|---|---|
| 21/tcp | open | Pure -FTPd h |
| 22 /tcp | open | ssh OpenSSH 5.3 |
| 80/tcp | open | http Apache httpd |
| 110/tcp | open | pop3 Dovecot pop3d |

STEP 8: Now for checking vulnerabilities go to website " https://www.cvedetails.com/ ". Type the version and then search.

I have checked of port 110/tcp pop3 Dovecot pop3d



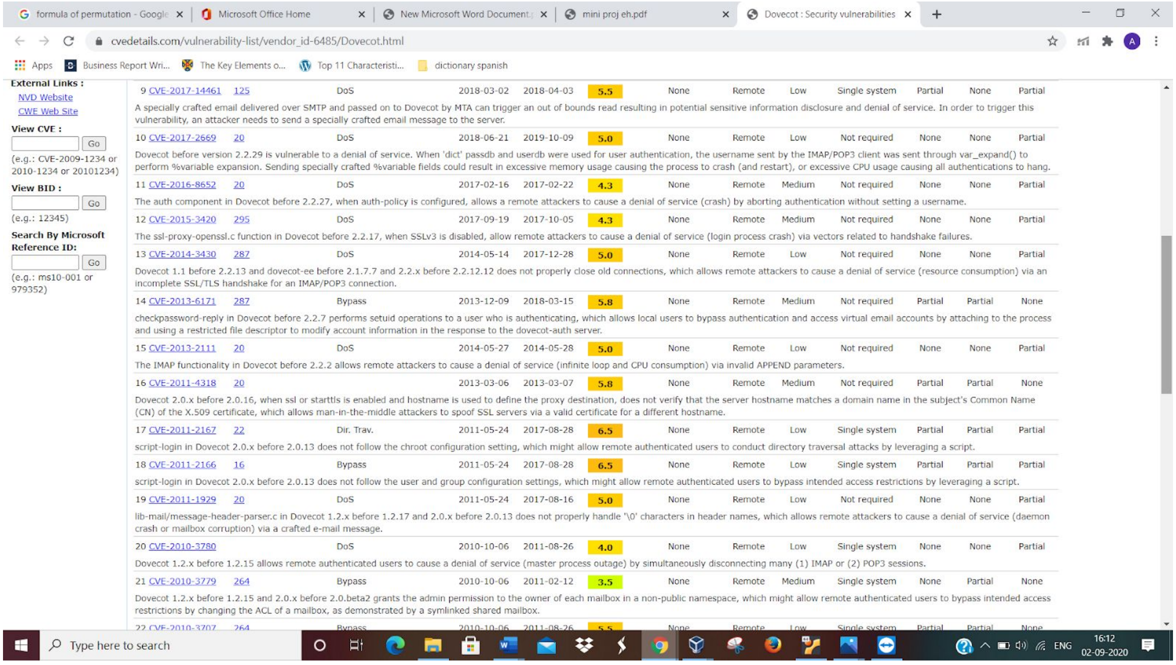
Dovecot : Security Vulnerabilities

CVSS Scores Greater Than: 0 1 2 3 4 5 6 7 8 9

Sort Results By : CVE Number Descending CVE Number Ascending CVSS Score Descending Number Of Exploits Descending

Copy Results Download Results

<table>
<tr><th>#</th><th>CVE ID</th><th>CWE ID</th><th># of Exploits</th><th>Vulnerability Type(s)</th><th>Publish Date</th><th>Update Date</th><th>Score</th><th>Gained Access Level</th><th>Access</th><th>Complexity</th><th>Authentication</th><th>Conf.</th><th>Integ.</th><th>Avail.</th></tr>
<tr><td>1</td><td>CVE-2019-11500</td><td>787</td><td></td><td>Exec Code</td><td>2019-08-29</td><td>2019-09-06</td><td>7.5</td><td>None</td><td>Remote</td><td>Low</td><td>Not required</td><td>Partial</td><td>Partial</td><td>Partial</td></tr>
<tr><td colspan="15">In Dovecot before 2.2.36.4 and 2.3.x before 2.3.7.2 (and Pigeonhole before 0.5.7.2), protocol processing can fail for quoted strings. This occurs because '\0' characters are mishandled, and can lead to out-of-bounds writes and remote code execution.</td></tr>
<tr><td>2</td><td>CVE-2019-11499</td><td>20</td><td></td><td></td><td>2019-05-08</td><td>2019-06-13</td><td>5.0</td><td>None</td><td>Remote</td><td>Low</td><td>Not required</td><td>None</td><td>None</td><td>Partial</td></tr>
<tr><td colspan="15">In the IMAP Server in Dovecot 2.3.3 through 2.3.5.2, the submission-login component crashes if AUTH PLAIN is attempted over a TLS secured channel with an unacceptable authentication message.</td></tr>
<tr><td>3</td><td>CVE-2019-11494</td><td>20</td><td></td><td></td><td>2019-05-08</td><td>2019-06-13</td><td>5.0</td><td>None</td><td>Remote</td><td>Low</td><td>Not required</td><td>None</td><td>None</td><td>Partial</td></tr>
<tr><td colspan="15">In the IMAP Server in Dovecot 2.3.3 through 2.3.5.2, the submission-login service crashes when the client disconnects prematurely during the AUTH command.</td></tr>
<tr><td>4</td><td>CVE-2019-10691</td><td>287</td><td></td><td></td><td>2019-04-24</td><td>2019-07-12</td><td>5.0</td><td>None</td><td>Remote</td><td>Low</td><td>Not required</td><td>None</td><td>None</td><td>Partial</td></tr>
<tr><td colspan="15">The JSON encoder in Dovecot before 2.3.5.2 allows attackers to repeatedly crash the authentication service by attempting to authenticate with an invalid UTF-8 sequence as the username.</td></tr>
<tr><td>5</td><td>CVE-2019-7524</td><td>119</td><td></td><td>Overflow</td><td>2019-03-28</td><td>2019-06-13</td><td>7.2</td><td>None</td><td>Local</td><td>Low</td><td>Not required</td><td>Complete</td><td>Complete</td><td>Complete</td></tr>
<tr><td colspan="15">In Dovecot before 2.2.36.3 and 2.3.x before 2.3.5.1, a local attacker can cause a buffer overflow in the indexer-worker process, which can be used to elevate to root. This occurs because of missing checks in the fts and pop3-uidl components.</td></tr>
<tr><td>6</td><td>CVE-2019-3814</td><td>295</td><td></td><td></td><td>2019-03-27</td><td>2019-06-13</td><td>4.9</td><td>None</td><td>Remote</td><td>Medium</td><td>Single system</td><td>Partial</td><td>Partial</td><td>None</td></tr>
<tr><td colspan="15">It was discovered that Dovecot before versions 2.2.36.1 and 2.3.4.1 incorrectly handled client certificates. A remote attacker in possession of a valid certificate with an empty username field could possibly use this issue to impersonate other users.</td></tr>
<tr><td>7</td><td>CVE-2017-15132</td><td>772</td><td></td><td></td><td>2018-01-25</td><td>2019-10-09</td><td>5.0</td><td>None</td><td>Remote</td><td>Low</td><td>Not required</td><td>None</td><td>None</td><td>Partial</td></tr>
<tr><td colspan="15">A flaw was found in dovecot 2.0 up to 2.2.33 and 2.3.0. An abort of SASL authentication results in a memory leak in dovecot's auth client used by login processes. The leak has impact in high performance configuration where same login processes are reused and can cause the process to crash due to memory exhaustion.</td></tr>
<tr><td>8</td><td>CVE-2017-15130</td><td></td><td></td><td>DoS</td><td>2018-03-02</td><td>2019-10-02</td><td>4.3</td><td>None</td><td>Remote</td><td>Medium</td><td>Not required</td><td>None</td><td>None</td><td>Partial</td></tr>
<tr><td colspan="15">A denial of service flaw was found in dovecot before 2.2.34. An attacker able to generate random SNI server names could exploit TLS SNI configuration lookups, leading to excessive memory usage and the process to restart.</td></tr>
<tr><td>9</td><td>CVE-2017-14461</td><td>125</td><td></td><td>DoS</td><td>2018-03-02</td><td>2018-04-03</td><td>5.5</td><td>None</td><td>Remote</td><td>Low</td><td>Single system</td><td>Partial</td><td>None</td><td>Partial</td></tr>
<tr><td colspan="15">A specially crafted email delivered over SMTP and passed on to Dovecot by MTA can trigger an out of bounds read resulting in potential sensitive information disclosure and denial of service. In order to trigger this vulnerability, an attacker needs to send a specially crafted email message to the server.</td></tr>
</table>



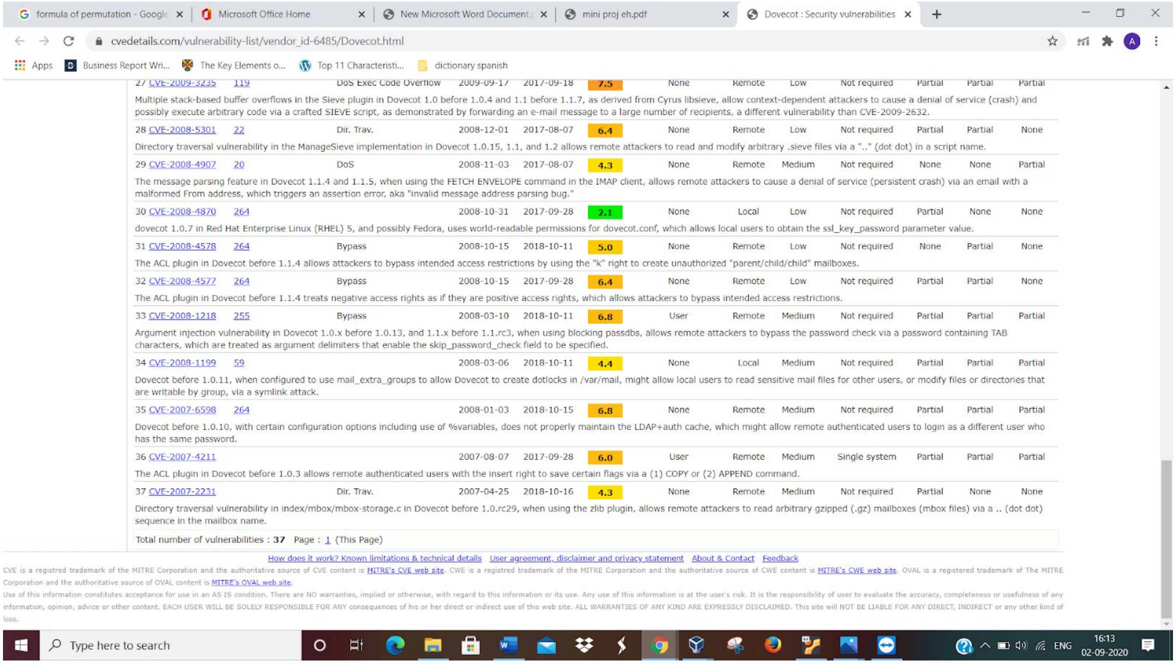
**External Links :**
NVD Website
CWE Web Site

**View CVE :**
Go
(e.g.: CVE-2009-1234 or 2010-1234 or 20101234)

**View BID :**
Go
(e.g.: 12345)

**Search By Microsoft Reference ID:**
Go
(e.g.: ms10-001 or 979352)

| | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 9 | CVE-2017-14461 | 125 | DoS | 2018-03-02 | 2018-04-03 | 5.5 | None | Remote | Low | Single system | Partial | None | Partial |
| A specially crafted email delivered over SMTP and passed on to Dovecot by MTA can trigger an out of bounds read resulting in potential sensitive information disclosure and denial of service. In order to trigger this vulnerability, an attacker needs to send a specially crafted email message to the server. | | | | | | | | | | | | | |
| 10 | CVE-2017-2669 | 20 | DoS | 2018-06-21 | 2019-10-09 | 5.0 | None | Remote | Low | Not required | None | None | Partial |
| Dovecot before version 2.2.29 is vulnerable to a denial of service. When 'dict' passdb and userdb were used for user authentication, the username sent by the IMAP/POP3 client was sent through var_expand() to perform %variable expansion. Sending specially crafted %variable fields could result in excessive memory usage causing the process to crash (and restart), or excessive CPU usage causing all authentications to hang. | | | | | | | | | | | | | |
| 11 | CVE-2016-8652 | 20 | DoS | 2017-02-16 | 2017-02-22 | 4.3 | None | Remote | Medium | Not required | None | None | Partial |
| The auth component in Dovecot before 2.2.27, when auth-policy is configured, allows a remote attackers to cause a denial of service (crash) by aborting authentication without setting a username. | | | | | | | | | | | | | |
| 12 | CVE-2015-3420 | 295 | DoS | 2017-09-19 | 2017-10-05 | 4.3 | None | Remote | Medium | Not required | None | None | Partial |
| The ssl-proxy-openssl.c function in Dovecot before 2.2.17, when SSLv3 is disabled, allow remote attackers to cause a denial of service (login process crash) via vectors related to handshake failures. | | | | | | | | | | | | | |
| 13 | CVE-2014-3430 | 287 | DoS | 2014-05-14 | 2017-12-28 | 5.0 | None | Remote | Low | Not required | None | None | Partial |
| Dovecot 1.1 before 2.2.13 and dovecot-ee before 2.1.7.7 and 2.2.x before 2.2.12.12 does not properly close old connections, which allows remote attackers to cause a denial of service (resource consumption) via an incomplete SSL/TLS handshake for an IMAP/POP3 connection. | | | | | | | | | | | | | |
| 14 | CVE-2013-6171 | 287 | Bypass | 2013-12-09 | 2018-03-15 | 5.8 | None | Remote | Medium | Not required | Partial | Partial | None |
| checkpassword-reply in Dovecot before 2.2.7 performs setuid operations to a user who is authenticating, which allows local users to bypass authentication and access virtual email accounts by attaching to the process and using a restricted file descriptor to modify account information in the response to the dovecot-auth server. | | | | | | | | | | | | | |
| 15 | CVE-2013-2111 | 20 | DoS | 2014-05-27 | 2014-05-28 | 5.0 | None | Remote | Low | Not required | None | None | Partial |
| The IMAP functionality in Dovecot before 2.2.2 allows remote attackers to cause a denial of service (infinite loop and CPU consumption) via invalid APPEND parameters. | | | | | | | | | | | | | |
| 16 | CVE-2011-4318 | 20 | | 2013-03-06 | 2013-03-07 | 5.8 | None | Remote | Medium | Not required | Partial | Partial | None |
| Dovecot 2.0.x before 2.0.16, when ssl or starttls is enabled and hostname is used to define the proxy destination, does not verify that the server hostname matches a domain name in the subject's Common Name (CN) of the X.509 certificate, which allows man-in-the-middle attackers to spoof SSL servers via a valid certificate for a different hostname. | | | | | | | | | | | | | |
| 17 | CVE-2011-2167 | 22 | Dir. Trav. | 2011-05-24 | 2017-08-28 | 6.5 | None | Remote | Low | Single system | Partial | Partial | Partial |
| script-login in Dovecot 2.0.x before 2.0.13 does not follow the chroot configuration setting, which might allow remote authenticated users to conduct directory traversal attacks by leveraging a script. | | | | | | | | | | | | | |
| 18 | CVE-2011-2166 | 16 | Bypass | 2011-05-24 | 2017-08-28 | 6.5 | None | Remote | Low | Single system | Partial | Partial | Partial |
| script-login in Dovecot 2.0.x before 2.0.13 does not follow the user and group configuration settings, which might allow remote authenticated users to bypass intended access restrictions by leveraging a script. | | | | | | | | | | | | | |
| 19 | CVE-2011-1929 | 20 | DoS | 2011-05-24 | 2017-08-16 | 5.0 | None | Remote | Low | Not required | None | None | Partial |
| lib-mail/message-header-parser.c in Dovecot 1.2.x before 1.2.17 and 2.0.x before 2.0.13 does not properly handle '\0' characters in header names, which allows remote attackers to cause a denial of service (daemon crash or mailbox corruption) via a crafted e-mail message. | | | | | | | | | | | | | |
| 20 | CVE-2010-3780 | | DoS | 2010-10-06 | 2011-08-26 | 4.0 | None | Remote | Low | Single system | None | None | Partial |
| Dovecot 1.2.x before 1.2.15 allows remote authenticated users to cause a denial of service (master process outage) by simultaneously disconnecting many (1) IMAP or (2) POP3 sessions. | | | | | | | | | | | | | |
| 21 | CVE-2010-3779 | 264 | Bypass | 2010-10-06 | 2011-02-12 | 3.5 | None | Remote | Medium | Single system | None | Partial | None |
| Dovecot 1.2.x before 1.2.15 and 2.0.x before 2.0.beta2 grants the admin permission to the owner of each mailbox in a non-public namespace, which might allow remote authenticated users to bypass intended access restrictions by changing the ACL of a mailbox, as demonstrated by a symlinked shared mailbox. | | | | | | | | | | | | | |
| 22 | CVE-2010-3707 | 264 | Bypass | 2010-10-06 | 2011-08-26 | 5.5 | None | Remote | Low | Single system | Partial | Partial | None |



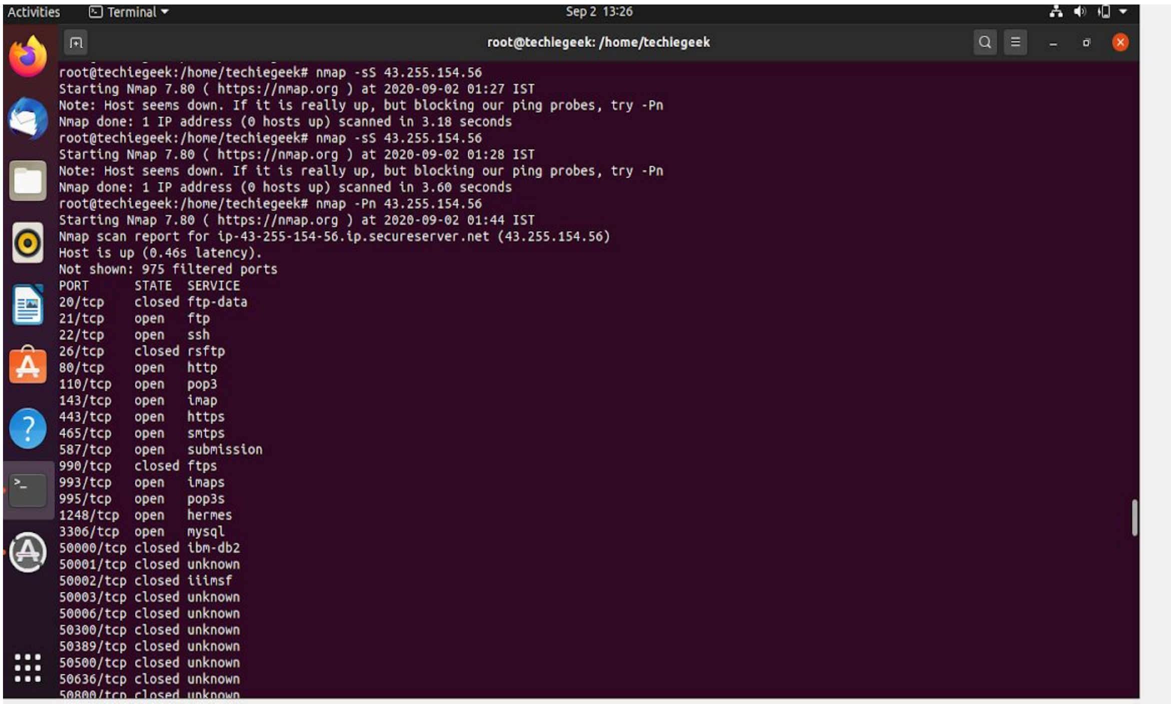
| | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 27 | CVE-2009-3235 | 119 | DoS Exec Code Overflow | 2009-09-17 | 2017-09-18 | 7.5 | None | Remote | Low | Not required | Partial | Partial | Partial |
| Multiple stack-based buffer overflows in the Sieve plugin in Dovecot 1.0 before 1.0.4 and 1.1 before 1.1.7, as derived from Cyrus libsieve, allow context-dependent attackers to cause a denial of service (crash) and possibly execute arbitrary code via a crafted SIEVE script, as demonstrated by forwarding an e-mail message to a large number of recipients, a different vulnerability than CVE-2009-2632. | | | | | | | | | | | | | |
| 28 | CVE-2008-5301 | 22 | Dir. Trav. | 2008-12-01 | 2017-08-07 | 6.4 | None | Remote | Low | Not required | Partial | Partial | None |
| Directory traversal vulnerability in the ManageSieve implementation in Dovecot 1.0.15, 1.1, and 1.2 allows remote attackers to read and modify arbitrary .sieve files via a ".." (dot dot) in a script name. | | | | | | | | | | | | | |
| 29 | CVE-2008-4907 | 20 | DoS | 2008-11-03 | 2017-08-07 | 4.3 | None | Remote | Medium | Not required | None | None | Partial |
| The message parsing feature in Dovecot 1.1.4 and 1.1.5, when using the FETCH ENVELOPE command in the IMAP client, allows remote attackers to cause a denial of service (persistent crash) via an email with a malformed From address, which triggers an assertion error, aka "invalid message address parsing bug." | | | | | | | | | | | | | |
| 30 | CVE-2008-4870 | 264 | | 2008-10-31 | 2017-09-28 | 2.1 | None | Local | Low | Not required | Partial | None | None |
| dovecot 1.0.7 in Red Hat Enterprise Linux (RHEL) 5, and possibly Fedora, uses world-readable permissions for dovecot.conf, which allows local users to obtain the ssl_key_password parameter value. | | | | | | | | | | | | | |
| 31 | CVE-2008-4578 | 264 | Bypass | 2008-10-15 | 2018-10-11 | 5.0 | None | Remote | Low | Not required | None | Partial | None |
| The ACL plugin in Dovecot before 1.1.4 allows attackers to bypass intended access restrictions by using the "k" right to create unauthorized "parent/child/child" mailboxes. | | | | | | | | | | | | | |
| 32 | CVE-2008-4577 | 264 | Bypass | 2008-10-15 | 2017-09-28 | 6.4 | None | Remote | Low | Not required | Partial | Partial | None |
| The ACL plugin in Dovecot before 1.1.4 treats negative access rights as if they are positive access rights, which allows attackers to bypass intended access restrictions. | | | | | | | | | | | | | |
| 33 | CVE-2008-1218 | 255 | Bypass | 2008-03-10 | 2018-10-11 | 6.8 | User | Remote | Medium | Not required | Partial | Partial | Partial |
| Argument injection vulnerability in Dovecot 1.0.x before 1.0.13, and 1.1.x before 1.1.rc3, when using blocking passdbs, allows remote attackers to bypass the password check via a password containing TAB characters, which are treated as argument delimiters that enable the skip_password_check field to be specified. | | | | | | | | | | | | | |
| 34 | CVE-2008-1199 | 59 | | 2008-03-06 | 2018-10-11 | 4.4 | None | Local | Medium | Not required | Partial | Partial | Partial |
| Dovecot before 1.0.11, when configured to use mail_extra_groups to allow Dovecot to create dotlocks in /var/mail, might allow local users to read sensitive mail files for other users, or modify files or directories that are writable by group, via a symlink attack. | | | | | | | | | | | | | |
| 35 | CVE-2007-6598 | 264 | | 2008-01-03 | 2018-10-15 | 6.8 | None | Remote | Medium | Not required | Partial | Partial | Partial |
| Dovecot before 1.0.10, with certain configuration options including use of %variables, does not properly maintain the LDAP+auth cache, which might allow remote authenticated users to login as a different user who has the same password. | | | | | | | | | | | | | |
| 36 | CVE-2007-4211 | | | 2007-08-07 | 2017-09-28 | 6.0 | User | Remote | Medium | Single system | Partial | Partial | Partial |
| The ACL plugin in Dovecot before 1.0.3 allows remote authenticated users with the insert right to save certain flags via a (1) COPY or (2) APPEND command. | | | | | | | | | | | | | |
| 37 | CVE-2007-2231 | | Dir. Trav. | 2007-04-25 | 2018-10-16 | 4.3 | None | Remote | Medium | Not required | Partial | None | None |
| Directory traversal vulnerability in index/mbox/mbox-storage.c in Dovecot before 1.0.rc29, when using the zlib plugin, allows remote attackers to read arbitrary gzipped (.gz) mailboxes (mbox files) via a .. (dot dot) sequence in the mailbox name. | | | | | | | | | | | | | |

Total number of vulnerabilities : **37** Page : 1 (This Page)

How does it work? Known limitations & technical details User agreement, disclaimer and privacy statement About & Contact Feedback

CVE is a registred trademark of the MITRE Corporation and the authoritative source of CVE content is MITRE's CVE web site. CWE is a registred trademark of the MITRE Corporation and the authoritative source of CWE content is MITRE's CWE web site. OVAL is a registered trademark of The MITRE Corporation and the authoritative source of OVAL content is MITRE's OVAL web site.

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.



```
root@techiegeek:/home/techiegeek# nmap -sS 43.255.154.56
Starting Nmap 7.80 ( https://nmap.org ) at 2020-09-02 01:27 IST
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 3.18 seconds
root@techiegeek:/home/techiegeek# nmap -sS 43.255.154.56
Starting Nmap 7.80 ( https://nmap.org ) at 2020-09-02 01:28 IST
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 3.60 seconds
root@techiegeek:/home/techiegeek# nmap -Pn 43.255.154.56
Starting Nmap 7.80 ( https://nmap.org ) at 2020-09-02 01:44 IST
Nmap scan report for ip-43-255-154-56.ip.secureserver.net (43.255.154.56)
Host is up (0.46s latency).
Not shown: 975 filtered ports
PORT      STATE  SERVICE
20/tcp    closed ftp-data
21/tcp    open   ftp
22/tcp    open   ssh
26/tcp    closed rsftp
80/tcp    open   http
110/tcp   open   pop3
143/tcp   open   imap
443/tcp   open   https
465/tcp   open   smtps
587/tcp   open   submission
990/tcp   closed ftps
993/tcp   open   imaps
995/tcp   open   pop3s
1248/tcp  open   hermes
3306/tcp  open   mysql
50000/tcp closed ibm-db2
50001/tcp closed unknown
50002/tcp closed iiimsf
50003/tcp closed unknown
50006/tcp closed unknown
50300/tcp closed unknown
50389/tcp closed unknown
50500/tcp closed unknown
50636/tcp closed unknown
50800/tcp closed unknown
```