

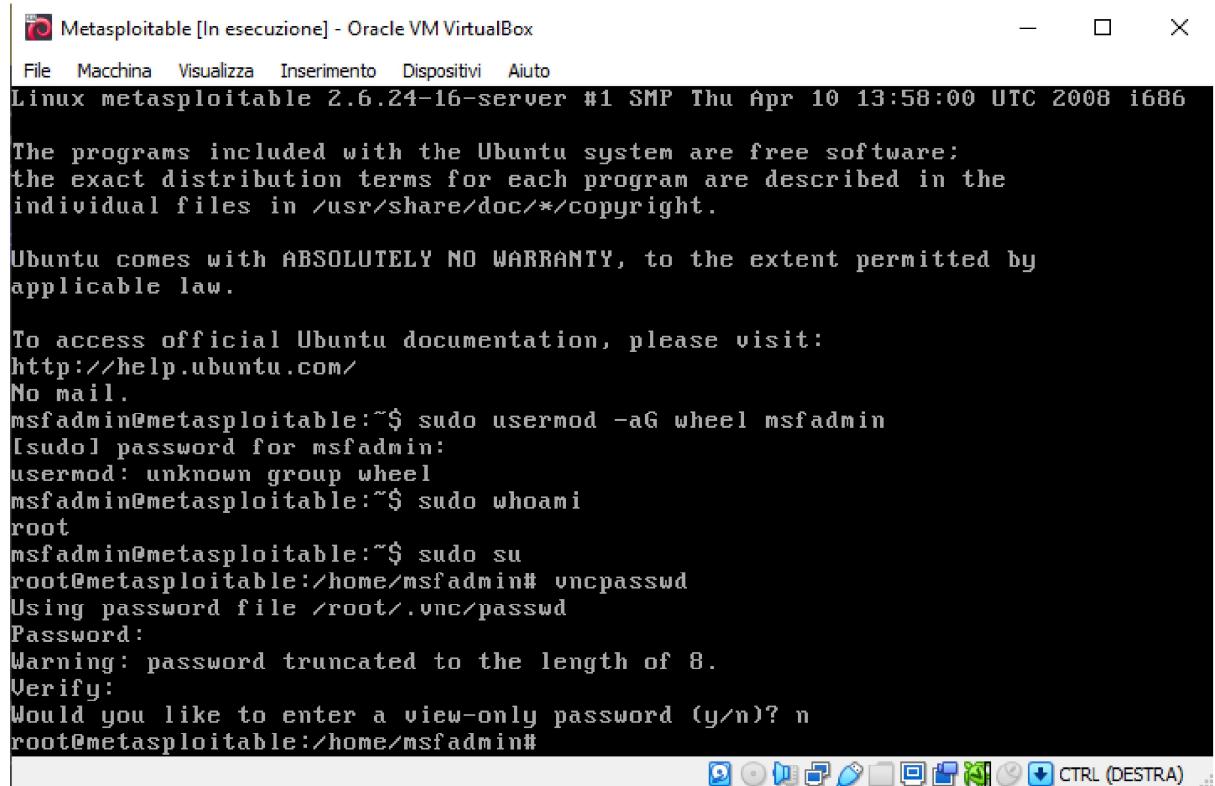
Report remediations

Vulnerabilità prima delle remediations

Vulnerabilities 60		
Hosts	1	Vulnerabilities
Filter	▼	Search Vulnerabilities
		60 Vulnerabilities
Sev ▾	Score ▾	Name ▲
<input type="checkbox"/> CRITICAL	10.0 *	NFS Exported Share Information Disclosure
<input type="checkbox"/> CRITICAL	10.0	Unix Operating System Unsupported Version Detection
<input type="checkbox"/> CRITICAL	10.0 *	VNC Server 'password' Password
<input type="checkbox"/> CRITICAL	9.8	Bind Shell Backdoor Detection
<input type="checkbox"/> CRITICAL	...	SSL (Multiple Issues)
<input type="checkbox"/> MIXED	...	SSL (Multiple Issues)
<input type="checkbox"/> MIXED	...	Apache Tomcat (Multiple Issues)
<input type="checkbox"/> HIGH	7.5	NFS Shares World Readable
<input type="checkbox"/> HIGH	7.5 *	rlogin Service Detection
<input type="checkbox"/> HIGH	7.5 *	rsh Service Detection
<input type="checkbox"/> HIGH	7.5	Samba Badlock Vulnerability

ELENCO remediations:

server VNC password:

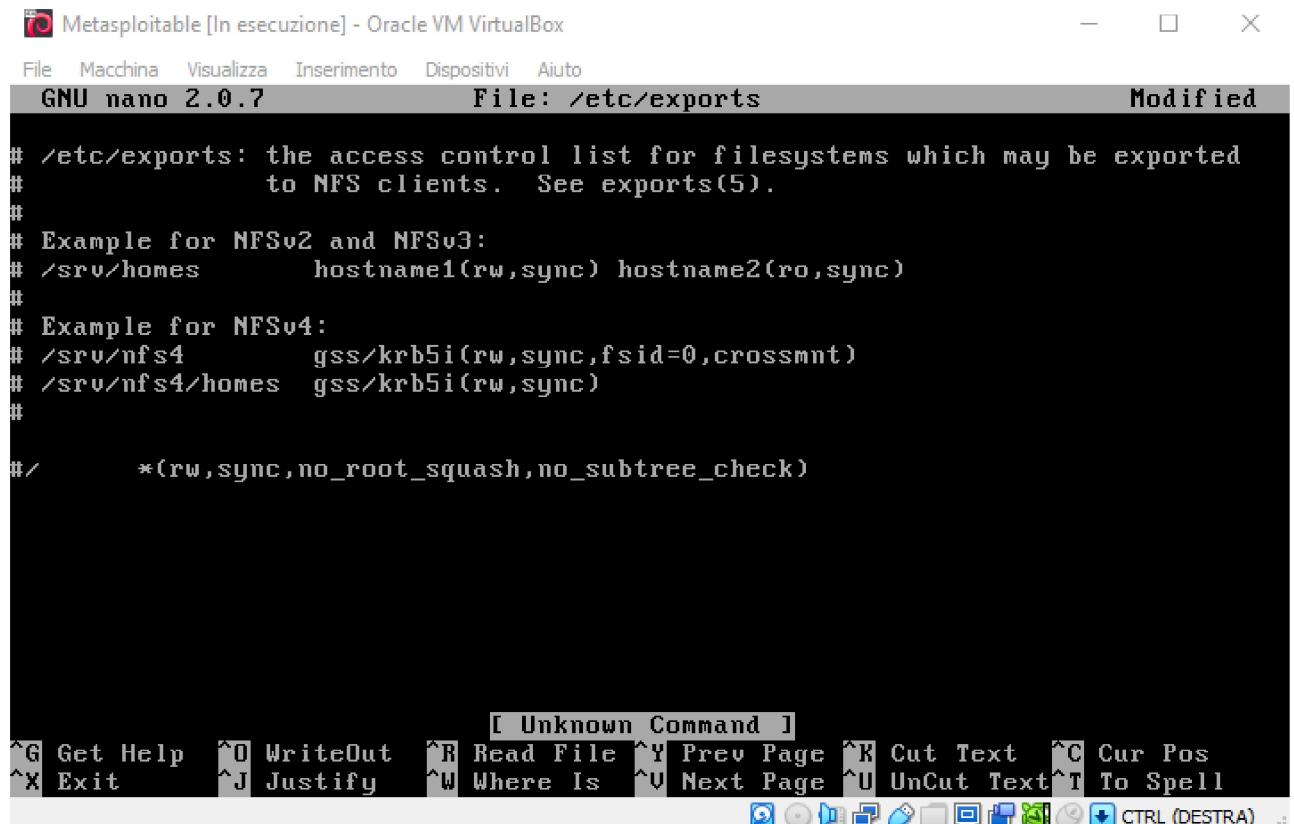


```
Metasploitable [In esecuzione] - Oracle VM VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686
The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

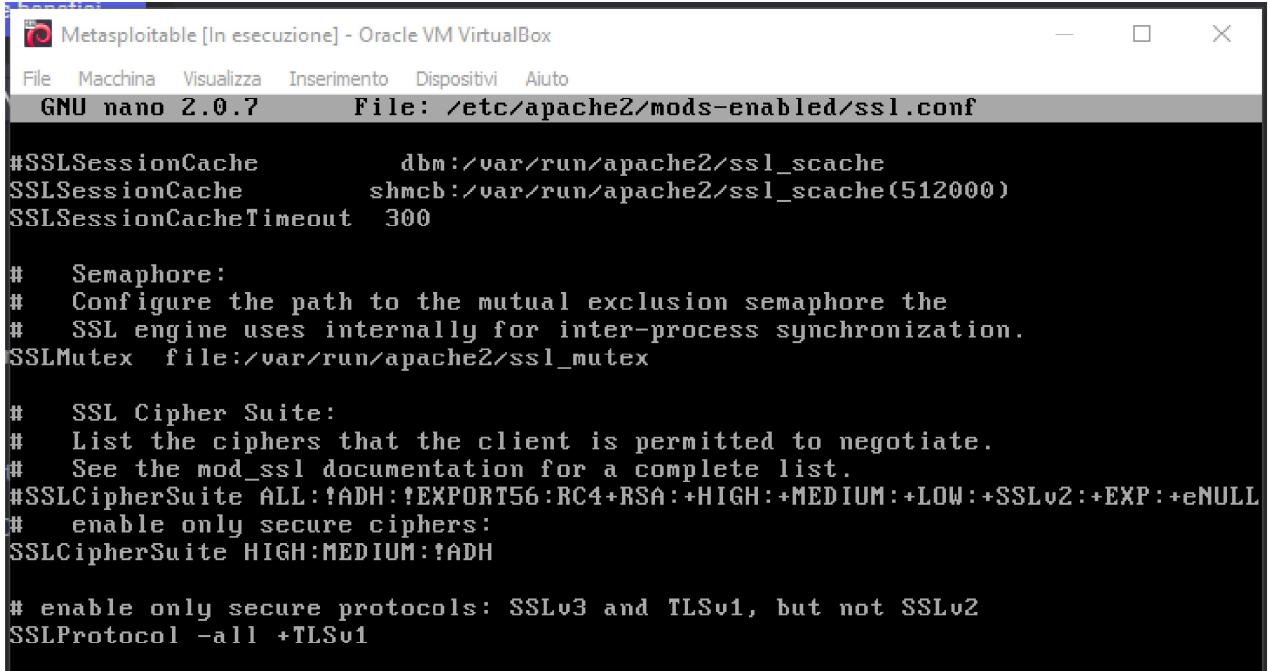
To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ sudo usermod -aG wheel msfadmin
[sudo] password for msfadmin:
usermod: unknown group wheel
msfadmin@metasploitable:~$ sudo whoami
root
msfadmin@metasploitable:~$ sudo su
root@metasploitable:/home/msfadmin# vncpasswd
Using password file /root/.vnc/passwd
Password:
Warning: password truncated to the length of 8.
Verify:
Would you like to enter a view-only password (y/n)? n
root@metasploitable:/home/msfadmin#
```

Rimuovo la cartella root / dal file export per risolvere la vuln di NFS:



```
Metasploitable [In esecuzione] - Oracle VM VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto
GNU nano 2.0.7 File: /etc/exports Modified
# /etc/exports: the access control list for filesystems which may be exported
#           to NFS clients. See exports(5).
#
# Example for NFSv2 and NFSv3:
# /srv/homes      hostname1(rw,sync) hostname2(ro,sync)
#
# Example for NFSv4:
# /srv/nfs4        gss/krb5i(rw,sync,fsid=0,crossmnt)
# /srv/nfs4/homes  gss/krb5i(rw,sync)
#
#*(rw,sync,no_root_squash,no_subtree_check)
```

Protocolli SSL non sicuri



```
Metasploitable [In esecuzione] - Oracle VM VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto
GNU nano 2.0.7          File: /etc/apache2/mods-enabled/ssl.conf

#SSLSessionCache          dbm:/var/run/apache2/ssl_scache
SSLSessionCache          shmc:/var/run/apache2/ssl_scache(512000)
SSLSessionCacheTimeout   300

#  Semaphore:
#  Configure the path to the mutual exclusion semaphore the
#  SSL engine uses internally for inter-process synchronization.
SSLMutex    file:/var/run/apache2/ssl_mutex

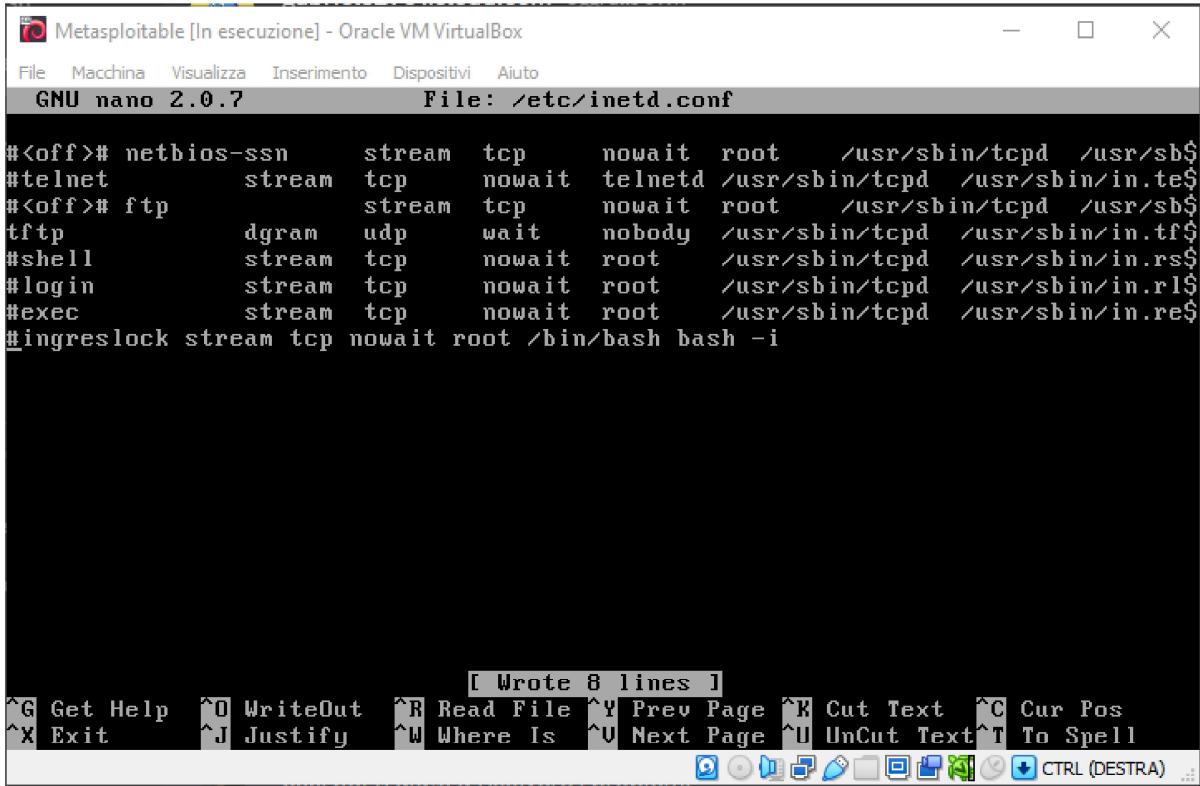
#  SSL Cipher Suite:
#  List the ciphers that the client is permitted to negotiate.
#  See the mod_ssl documentation for a complete list.
#SSLCipherSuite ALL:!ADH:!EXPORT56:RC4+RSA:+HIGH:+MEDIUM:+LOW:+SSLv2:+EXP:+eNULL
#  enable only secure ciphers:
SSLCipherSuite HIGH:MEDIUM:!ADH

# enable only secure protocols: SSLv3 and TLSv1, but not SSLv2
SSLProtocol -all +TLSv1
```

Poi lancio il comando a2enmod ssl come root

Non è comunque sicuro ma è il massimo che è possibile fare senza aggiornare apache2

Disattivo alcuni servizi in ascolto



```
Metasploitable [In esecuzione] - Oracle VM VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto
GNU nano 2.0.7          File: /etc/inetd.conf

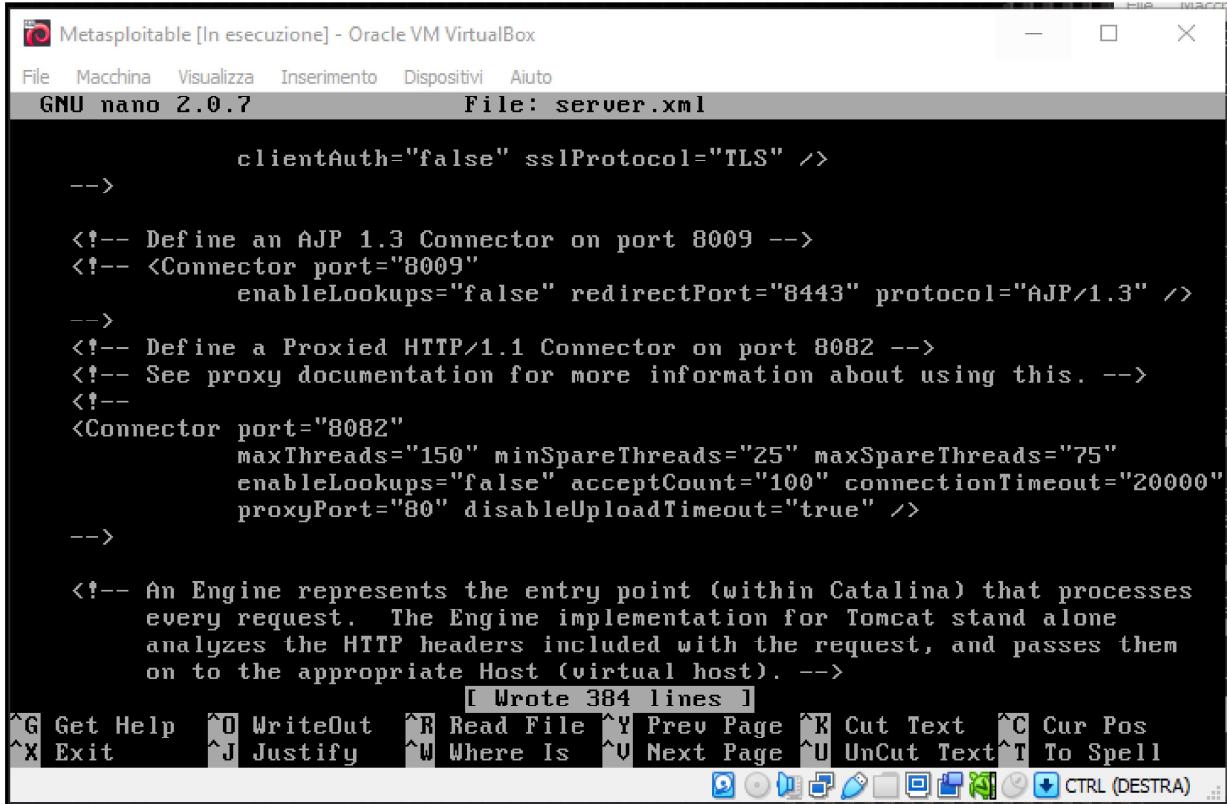
#<off># netbios-ssn    stream  tcp     nowait  root    /usr/sbin/tcpd /usr/sbin/tcpd
#telnet      stream  tcp     nowait  telnetd /usr/sbin/tcpd /usr/sbin/in.telnetd
#<off># ftp       stream  tcp     nowait  root    /usr/sbin/tcpd /usr/sbin/tcpd
tftp        dgram   udp     wait    nobody  /usr/sbin/tcpd /usr/sbin/tcpd
#shell      stream  tcp     nowait  root    /usr/sbin/tcpd /usr/sbin/in.rshd
#login      stream  tcp     nowait  root    /usr/sbin/tcpd /usr/sbin/in.rlogind
#exec       stream  tcp     nowait  root    /usr/sbin/tcpd /usr/sbin/in.rexecd
#ingreslock stream  tcp     nowait  root    /bin/bash bash -i

[Wrote 8 lines]
^G Get Help  ^O WriteOut  ^R Read File  ^Y Prev Page  ^E Cut Text  ^C Cur Pos
^X Exit      ^J Justify   ^W Where Is   ^V Next Page  ^U UnCut Text ^T To Spell
                                         CTRL (DESTRA) ...
```

In questo modo risolvo alcune delle backdoor

AJP connector su Tomcat

Vado su /etc/tomcat5.5 e modifco il file:



```
clientAuth="false" sslProtocol="TLS" />
-->

<!-- Define an AJP 1.3 Connector on port 8009 -->
<!-- <Connector port="8009"
    enableLookups="false" redirectPort="8443" protocol="AJP/1.3" />
-->
<!-- Define a Proxied HTTP/1.1 Connector on port 8082 -->
<!-- See proxy documentation for more information about using this. -->
<!--
<Connector port="8082"
    maxThreads="150" minSpareThreads="25" maxSpareThreads="75"
    enableLookups="false" acceptCount="100" connectionTimeout="20000"
    proxyPort="80" disableUploadTimeout="true" />
-->

<!-- An Engine represents the entry point (within Catalina) that processes
     every request. The Engine implementation for Tomcat stand alone
     analyzes the HTTP headers included with the request, and passes them
     on to the appropriate Host (virtual host). -->
[ Wrote 384 lines ]
^G Get Help ^O WriteOut ^R Read File ^Y Prev Page ^K Cut Text ^C Cur Pos
^X Exit ^J Justify ^W Where Is ^V Next Page ^U UnCut Text ^T To Spell
                                          CTRL (DESTRA)
```

Lo commento per disattivarlo

IRC backdoor



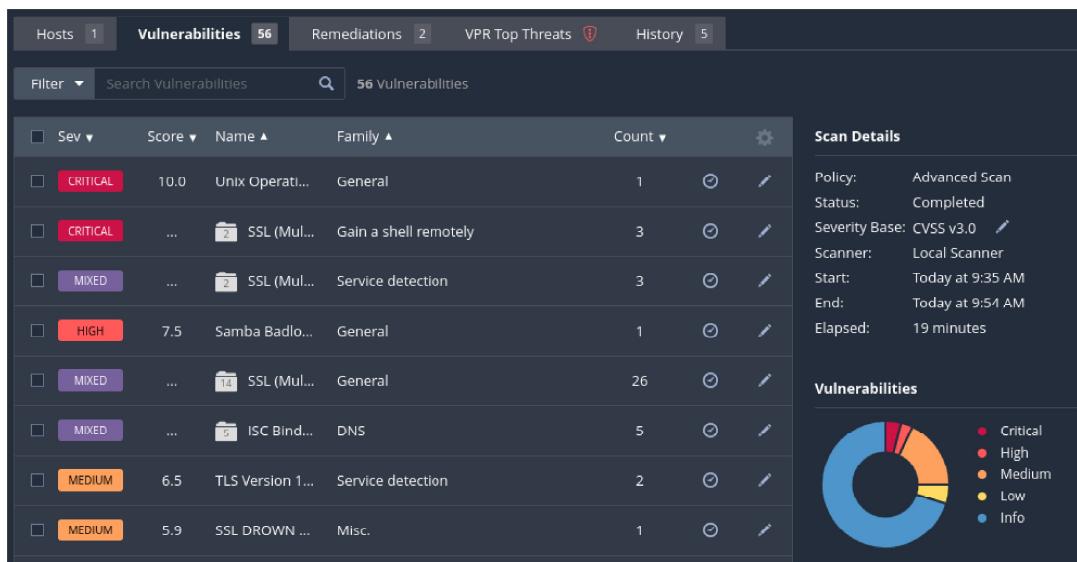
Permetto solo agli utenti della rete locale di connettersi impostando la regola da pfSense

Ho provato con iptables ma al riavvio le regole si resettavano

Anche qui, è comunque vulnerabile da utenti che si trovano nella rete, ma senza aggiornare l'unica altra soluzione sarebbe rimuovere il servizio

Vulnerabilità residue dopo le remediations:

Host	Vulnerabilities ▾		
192.168.49.101	6	4	25



Sono state risolte 4 vulnerabilità critiche e 3 high