



TECHGUYS

# REPORT

## VULNERABILITY REMEDIATION

PROGETTO S5-L5

GIAN MARCO PELLEGRINO

[WWW.TECHGUYS.COM](http://WWW.TECHGUYS.COM)



# SVOLGIMENTO

**SCANSIONE  
NESSUS**



La prima fase vedrà come protagonista Nessus, vulnerability scanner. Dopo aver impostato IP target e le porte da scansionare, Nessus restituirà diversi risultati.

**REMEDIATION**

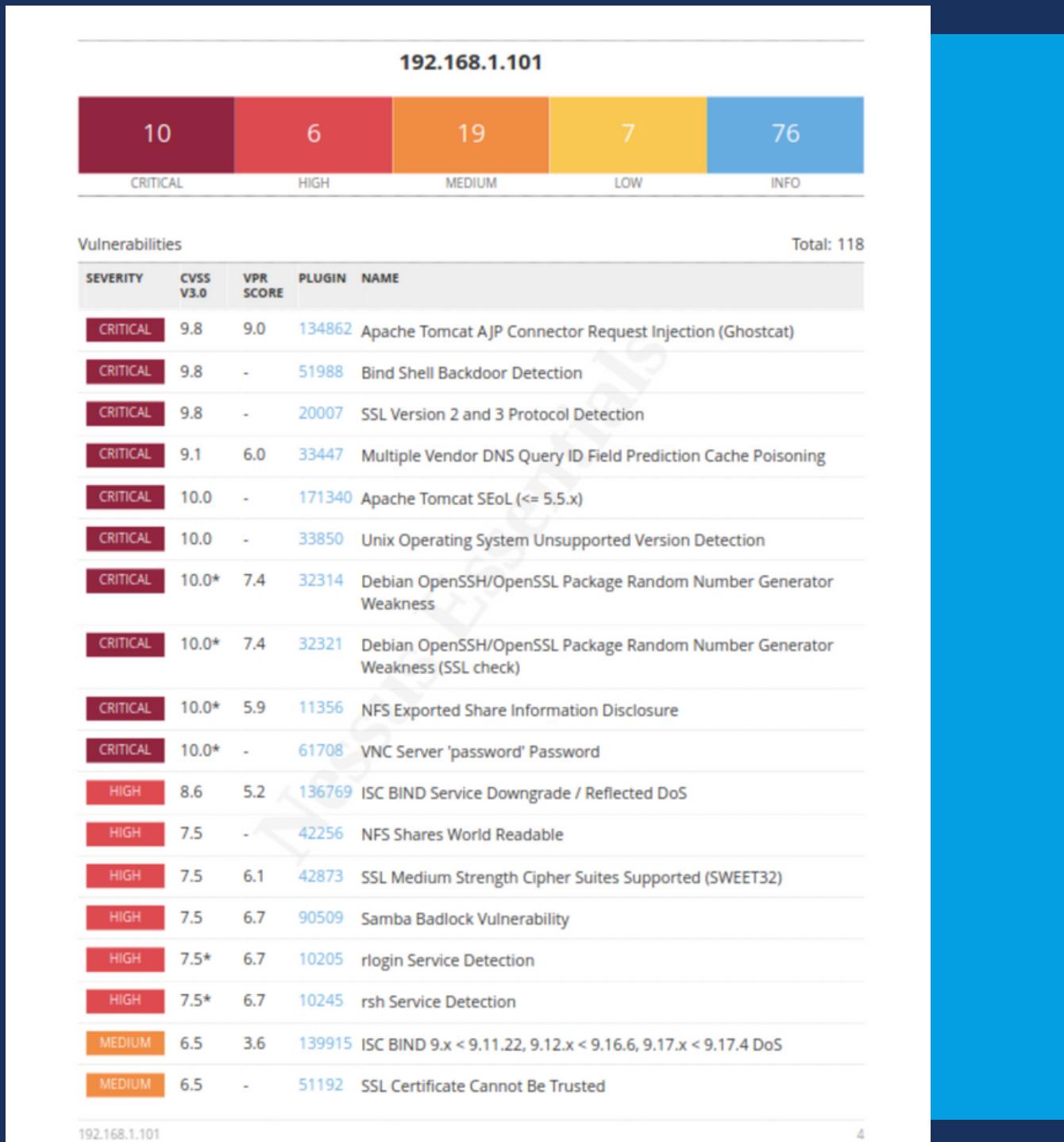


In base alla vulnerabilità trovata, Nessus fornisce delle istruzioni su come rimediare ai problemi riscontrati, i quali verranno risolti dall'utente, grazie anche all'implemento di ricerche online.

**SCANSIONE  
FINALE**



Dopo aver soddisfatto le condizioni, verrà avviata una scansione finale, la quale, se le risoluzioni sono andate a buon fine, restituirà un minor rischio generale.



# SCANSIONE NESSUS

Image 1  
from NESSUS



# VULNERABILITA'

CRITICAL 10.0\* - 61708 VNC Server 'password' Password

## VNC server password

Vulnerabilità critica trovata da Nessus utilizzando un attacco Brute Force sul server VNC, identificando la password come poco sicura.

CRITICAL 9.8 - 51988 Bind Shell Backdoor Detection

## BIND SHELL backdoor

Rilevata una backdoor in ascolto sulla porta 1524 senza autorizzazione. Potrebbe essere sfruttata da un attaccante.

CRITICAL 10.0\* 5.9 11356 NFS Exported Share Information Disclosure

## NFS exported Share

Vulnerabilità critica basata sulla possibilità, da parte di un black hat, di attaccare almeno uno dei pacchetti NFS Shares e avere modo di leggere e modificare file da remoto.

CRITICAL 9.8 - 20007 SSL Version 2 and 3 Protocol Detection

## Version SSL 2 e 3 (non completato)

Le versioni SSL 2 e 3 sono obsolete e possono essere sfruttate da malintenzionati.



# VNC SERVER PASSWORD

VNC, Virtual Network Computing, è un software che permette di condividere e controllare il desktop da remoto.

La soluzione per questa vulnerabilità consisteva nel cambiare la password al server VNC, essendo la precedente semplicemente “password”.

Con il comando sudo su è possibile avere i permessi di super-user, così da poter modificare la password del server, usando il comando `vncpasswd`.

Image 2  
from [METASPLOITABLE](#)

```
root@metasploitable:/home/msfadmin# vncpasswd
Using password file /root/.vnc/passwd
Password:
Verify:
Would you like to enter a view-only password (y/n)? n
root@metasploitable:/home/msfadmin#
```



# NFS EXPORTED SHARE

Il NFS, Network file system, permette a client e server di condividere file e directory su una rete.

In questo caso è stato necessario modificare tre file:

- **/etc(exports**; le esportazioni erano abilitate di default a tutte le possibili connessioni. Aggiunto l'IP della macchina Kali.

- **/etc/hosts.allow**; file che mette in lista chiunque sia abilitato alla connessione.

- **/etc/hosts.deny**; file che impedisce le connessioni, restrizione impostata su ALL tranne per macchina Kali.

Modificando i permessi di lettura e scrittura, i quali non avevano restrizioni, e abilitandoli solo all'IP collegato alla macchina kali. è stato possibile risolvere il problema.

```
## /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)
##
## /          192.168.1.100(rw,sync,no_root_squash,no_subtree_check)
```

```
## /etc/hosts.allow: list of hosts that are allowed to access the system.
## See the manual pages hosts_access(5) and hosts_options(5).
##
## Example:    ALL: LOCAL @some_netgroup
##              ALL: .foobar.edu EXCEPT terminalserver.foobar.edu
##
## If you're going to protect the portmapper use the name "portmap" for the
## daemon name. Remember that you can only use the keyword "ALL" and IP
## addresses (NOT host or domain names) for the portmapper, as well as for
## rpc.mountd (the NFS mount daemon). See portmap(8) and rpc.mountd(8)
## for further information.
##
ALL:192.168.1.100
ALL:192.168.1.101
```

```
# for further information.
#
# The PARANOID wildcard matches any host whose name does not match its
# address.
#
# You may wish to enable this to ensure any programs that don't
# validate looked up hostnames still leave understandable logs. In past
# versions of Debian this has been the default.
# ALL: PARANOID
#
ALL:ALL
ALL EXCEPT:192.168.1.100, 192.168.1.101
```



# BIND SHELL BACKDOOR

Per impedire la connessione alla backdoor in ascolto sulla porta 1524 è stato abilitato il firewall ufw (uncomplicated firewall) e impostata la regola che impedisce tutte le connessioni sulla porta 1524. E' stata attuata questa soluzione poichè una formattazione e installazione del sistema operativo non erano un'opzione.

```
Commands:
  enable          Enables the firewall
  disable         Disables the firewall
  default ARG    set default policy to ALLOW or DENY
  logging ARG    set logging to ON or OFF
  allow/deny RULE allow or deny RULE
  delete allow/deny RULE delete the allow/deny RULE
  status          show firewall status
  version         display version information

root@metasploitable:~# ufw enable
Firewall started and enabled on system startup
root@metasploitable:~# ufw status
Firewall loaded

To                         Action  From
--                         ----   ---
1524/tcp                   DENY    Anywhere
1524/udp                   DENY    Anywhere

root@metasploitable:~#
```

Image 4  
from METASPLOITABLE

La riuscita dell'impostazione è stata confermata anche usando Nmap, il quale restituisce il feedback "filtered" alla porta invece che "open".

```
[root@kali)-[/home/gimp] you
# nmap -sV -p 1524 192.168.1.101
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-27 14:07 CEST
Nmap scan report for 192.168.1.101
Host is up (0.00068s latency).Please manager, use the line for
sources.list as given below:
PORT      STATE     SERVICE      VERSION
1524/tcp  filtered  ingreslock
MAC Address: 08:00:27:59:30:75 (Oracle VirtualBox virtual NIC)
```

Image 5
from KALI



```
# SSL Cipher Suite:  
# List the ciphers that the client is permitted to negotiate. See the  
# ciphers(1) man page from the openssl package for list of all available  
# options.  
# Enable only secure ciphers:  
SSLCipherSuite HIGH:!aNULL  
  
# SSL server cipher order preference:  
# Use server priorities for cipher algorithm choice.  
# Clients may prefer lower grade encryption. You should enable this  
# option if you want to enforce stronger encryption, and can afford  
# the CPU cost, and did not override SSLCipherSuite in a way that puts  
# insecure ciphers first.  
# Default: Off  
#SSLHonorCipherOrder on  
  
# The protocols to enable.  
# Available values: all, SSLv3, TLSv1, TLSv1.1, TLSv1.2  
# SSL v2 is no longer supported  
SSLProtocol all -SSLv3 +TLSv1.2
```

Image 6  
from KALI

## VERSION SSL 2 E 3

Per risolvere questa vulnerabilità si è cercato di disabilitare i protocolli SSL obsoleti ed attivare TLSv1.2.

Dopo essersi spostati nella directory /etc/apache2 e aperto il file mods-available/ssl.conf tramite editor di testo, si è andato a cercare la riga "SSLProtocol". Si è poi abilitato TLSv1.2 e disattivato SSLv3.

La procedura però non ha funzionato. Il problema potrebbe trovarsi nella ChiperSuite.

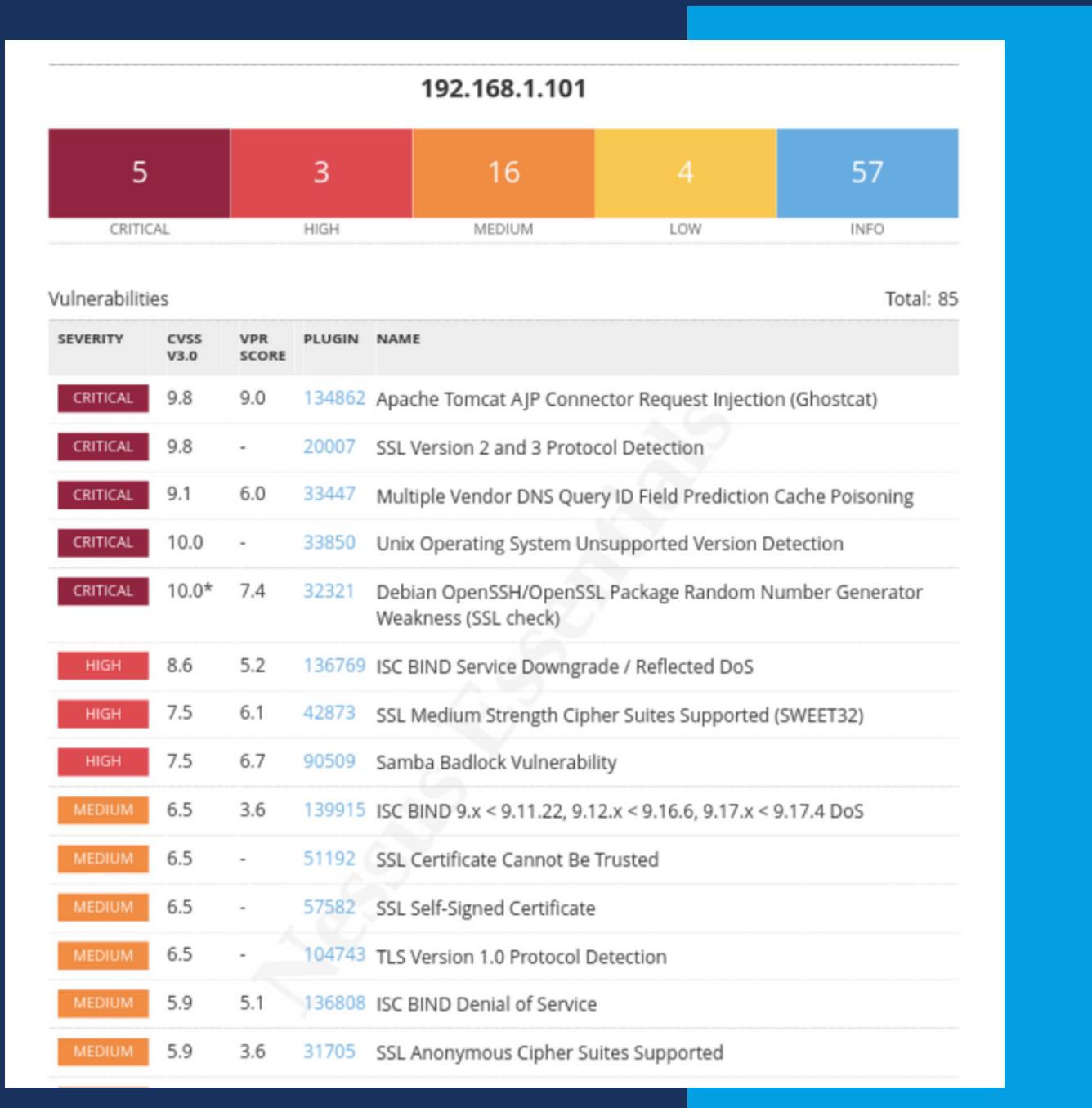


Image 7  
from [NESSUS](#)

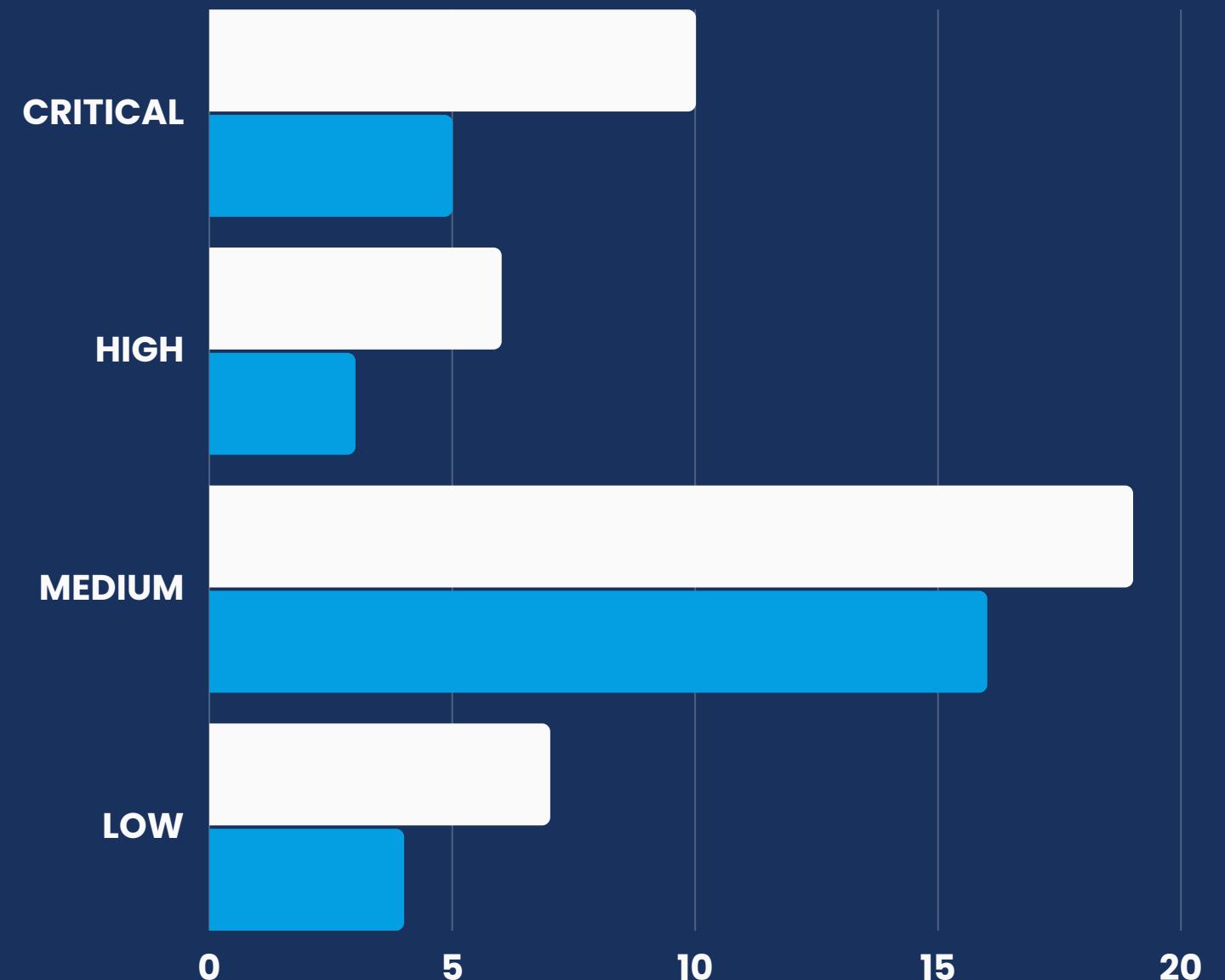
## SCANSIONE FINALE

Come è possibile osservare dal report, le criticità totali sono diminuite di molto.

Si può affermare quindi che la maggior parte dei processi di risoluzione abbiano funzionato e si sia riusciti ad abbassare di molto il fattore di rischio.

## RISULTATI COLLATERALI

Sono state risolte anche molte criticità le quali non erano però target delle risoluzioni. Per questo motivo non sono state inserite nel report, poiché la loro risoluzione è legata alla riuscita di misure di sicurezza implementate su altri target.



## MIGLIORAMENTO

1

CRITICITA' 1° SCAN

2

CRITICITA' FINAL SCAN



TECHGUYS

WWW.TECHGUYS.COM

**G R A Z I E**  
PER L'ATTENZIONE

[www.techguys.com](http://www.techguys.com)

[GianMarcoPellegrino@techguys.com](mailto:GianMarcoPellegrino@techguys.com)

123-456-7890