



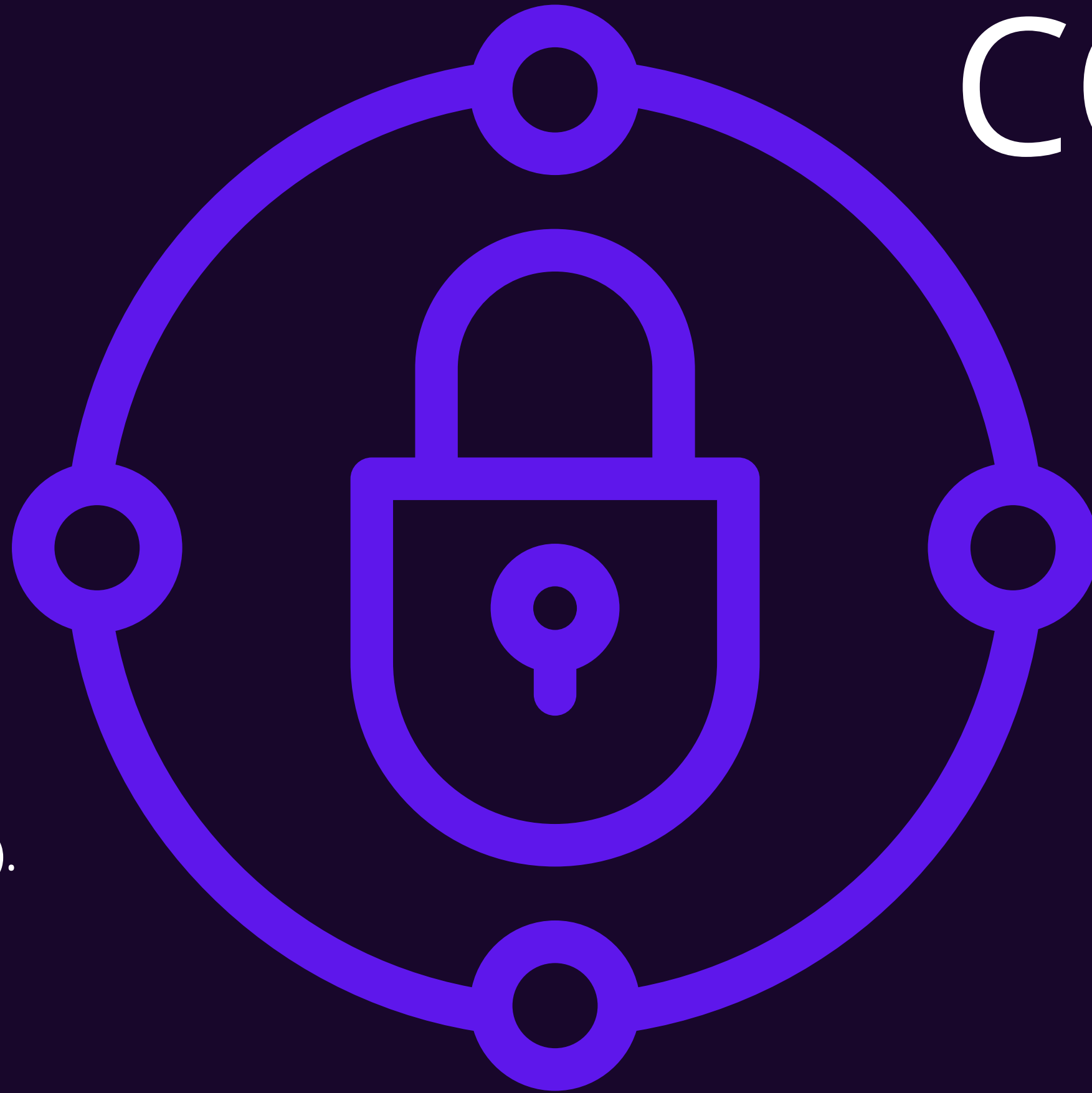
**Nessus**<sup>®</sup>  
vulnerability scanner



# COS'E'?

E' un vulnerability scanner, un software che esegue scansioni alla ricerca di vulnerabilità conosciute.

Grazie al confronto con un database online o offline (meno aggiornato).





# 3 Fasi principali:

Invia un pacchetto: scopre che S.O. c'è e scansiona i programmi.



Li confronta e dà una valutazione.




3) E' la parte attiva: simula attacchi.




























# Panoramica delle scannerizzazioni



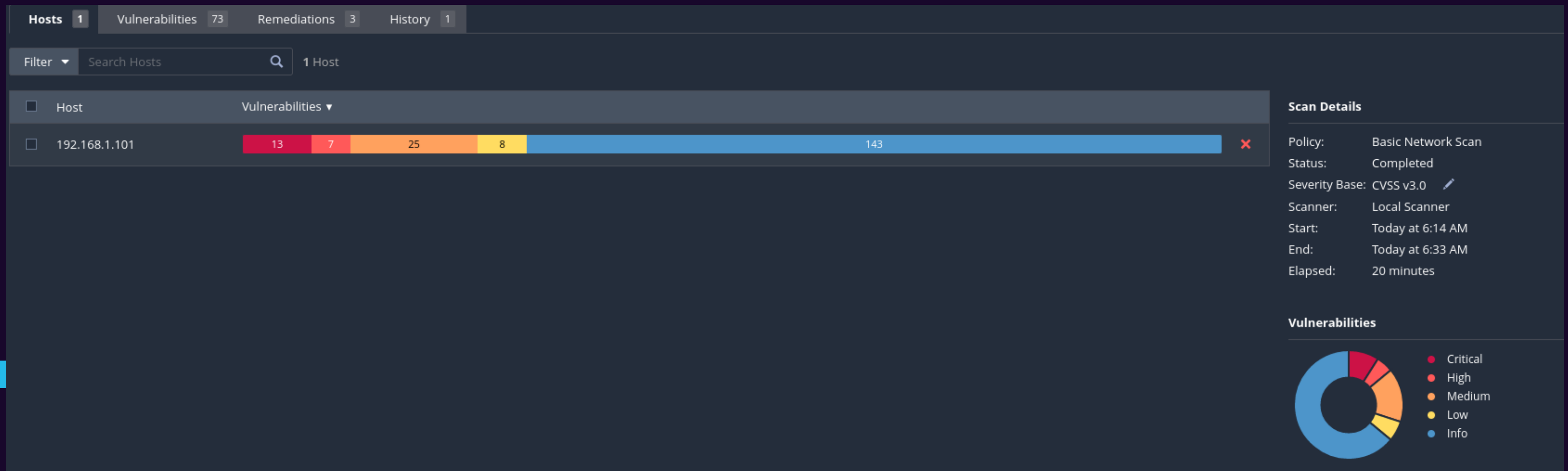
**Host Discovery**  
A simple scan to discover live hosts and open ports.

### VULNERABILITIES

 <p><b>Basic Network Scan</b> A full system scan suitable for any host.</p>	 <p><b>Advanced Scan</b> Configure a scan without using any recommendations.</p>	 <p><b>Advanced Dynamic Scan</b> Configure a dynamic plugin scan without recommendations.</p>	 <p><b>Malware Scan</b> Scan for malware on Windows and Unix systems.</p>	 <p><b>Mobile Device Scan</b> Assess mobile devices via Microsoft Exchange or an MDM.</p>	 <p><b>Web Application Tests</b> Scan for published and unknown web vulnerabilities using Nessus Scanner.</p>	 <p><b>Credentialed Patch Audit</b> Authenticate to hosts and enumerate missing updates.</p>
 <p><b>Intel AMT Security Bypass</b> Remote and local checks for CVE-2017-5689.</p>	 <p><b>Spectre and Meltdown</b> Remote and local checks for CVE-2017-5753, CVE-2017-5715, and CVE-2017-5754.</p>	 <p><b>WannaCry Ransomware</b> Remote and local checks for MS17-010.</p>	 <p><b>Ripple20 Remote Scan</b> A remote scan to fingerprint hosts potentially running the Treck stack in the network.</p>	 <p><b>Zerologon Remote Scan</b> A remote scan to detect Microsoft Netlogon Elevation of Privilege (Zerologon).</p>	 <p><b>Solorigate</b> Remote and local checks to detect SolarWinds Solorigate vulnerabilities.</p>	 <p><b>ProxyLogon : MS Exchange</b> Remote and local checks to detect Exchange vulnerabilities targeted by HAFNIUM.</p>
 <p><b>PrintNightmare</b> Local checks to detect the PrintNightmare Vulnerability in Windows Print Spooler.</p>	 <p><b>Active Directory Starter Scan</b> Look for misconfigurations in Active Directory.</p>	 <p><b>Log4Shell</b> Detection of Apache Log4j CVE-2021-44228</p>	 <p><b>Log4Shell Remote Checks</b> Detection of Apache Log4j CVE-2021-44228 via Remote Direct Checks</p>	 <p><b>Log4Shell Vulnerability Ecosystem</b> Detection of Log4Shell Vulnerabilities</p>	 <p><b>CISA Alerts AA22-011A and AA22-047A</b> Detection of vulnerabilities from recent CISA alerts.</p>	 <p><b>ContiLeaks</b> Detection of vulnerabilities revealed in the ContiLeaks chats.</p>
 <p><b>Ransomware Ecosystem</b> Vulnerabilities used by ransomware groups and affiliates.</p>	 <p><b>2022 Threat Landscape Report (TLR)</b> A scan to detect vulnerabilities featured in our End of Year report.</p>					



# Faremo una scannerizzazione di rete





# Nel dettaglio...

<input type="checkbox"/>	CRITICAL	10.0 *	5.9	NFS Exported Share Information Disclosure	RPC
<input type="checkbox"/>	CRITICAL	10.0		Unix Operating System Unsupported Version Detection	General
<input type="checkbox"/>	CRITICAL	10.0 *	7.4	UnrealIRCd Backdoor Detection	Backdoors
<input type="checkbox"/>	CRITICAL	10.0 *		VNC Server 'password' Password	Gain a shell remotely
<input type="checkbox"/>	CRITICAL	9.8		SSL Version 2 and 3 Protocol Detection	Service detection
<input type="checkbox"/>	CRITICAL	9.8		Bind Shell Backdoor Detection	Backdoors
<input type="checkbox"/>	HIGH	7.5		NFS Shares World Readable	RPC
<input type="checkbox"/>	HIGH	7.5 *	6.7	rlogin Service Detection	Service detection
<input type="checkbox"/>	HIGH	7.5 *	6.7	rsh Service Detection	Service detection
<input type="checkbox"/>	HIGH	7.5	6.7	Samba Badlock Vulnerability	General
<input type="checkbox"/>	MEDIUM	6.5		TLS Version 1.0 Protocol Detection	Service detection
<input type="checkbox"/>	MEDIUM	6.5		Unencrypted Telnet Server	Misc.
<input type="checkbox"/>	MEDIUM	5.9	3.6	SSL Anonymous Cipher Suites Supported	Service detection
<input type="checkbox"/>	MEDIUM	5.9	4.4	SSL DROWN Attack Vulnerability (Decrypting RSA with Obsolete and Weakened eNcryption)	Misc.
<input type="checkbox"/>	MEDIUM	5.3	4.0	HTTP TRACE / TRACK Methods Allowed	Web Servers
<input type="checkbox"/>	LOW	3.7	4.5	SSL/TLS Diffie-Hellman Modulus <= 1024 Bits (Logjam)	Misc.
<input type="checkbox"/>	LOW	2.6 *		X Server Detection	Service detection

<input type="checkbox"/>	INFO			Nessus SYN scanner	Port scanners
<input type="checkbox"/>	INFO			RPC Services Enumeration	Service detection
<input type="checkbox"/>	INFO			Service Detection	Service detection
<input type="checkbox"/>	INFO			IRC Daemon Version Detection	Service detection
<input type="checkbox"/>	INFO			OpenSSL Detection	Service detection
<input type="checkbox"/>	INFO			RMI Registry Detection	Service detection
<input type="checkbox"/>	INFO			Service Detection (GET request)	Service detection
<input type="checkbox"/>	INFO			Unknown Service Detection: Banner Retrieval	Service detection
<input type="checkbox"/>	INFO			AJP Connector Detection	Service detection
<input type="checkbox"/>	INFO			Backported Security Patch Detection (FTP)	General
<input type="checkbox"/>	INFO			Backported Security Patch Detection (WWW)	General
<input type="checkbox"/>	INFO			Common Platform Enumeration (CPE)	General
<input type="checkbox"/>	INFO			Device Type	General
<input type="checkbox"/>	INFO			Ethernet Card Manufacturer Detection	Misc.
<input type="checkbox"/>	INFO			Ethernet MAC Addresses	General
<input type="checkbox"/>	INFO			ICMP Timestamp Request Remote Date Disclosure	General

Plugin ID: 10719



Si passa alla risoluzione dei  
problemi.

Ecco alcuni esempi:



Il server VNC (condivisione remota) in esecuzione è protetto da una password debole. Nessus è stato in grado di accedere utilizzando l'autenticazione VNC i 'password'. Un utente malintenzionato remoto e non autenticato potrebbe sfruttare questa situazione.

**CRITICAL** VNC Server 'password' Password

**Description**

The VNC server running on the remote host is secured with a weak password. Nessus was able to login using VNC authentication and a password of 'password'. A remote, unauthenticated attacker could exploit this to take control of the system.

**Solution**

Secure the VNC service with a strong password.

**Output**

```
Nessus logged in using a password of "password".
```

To see debug logs, please visit individual host

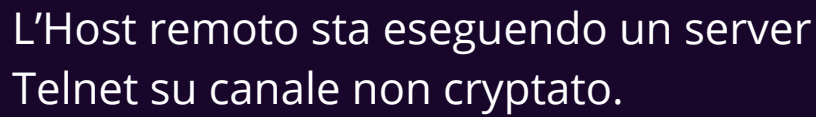
Port ▲	Hosts
5900 / tcp / vnc	192.168.1.101 <a href="#">🔗</a>

Il server VNC è configurato per supportare TLS per la comunicazione sicura. TLS è dunque un protocollo di sicurezza che fornisce crittografia e autenticazione dei dati trasmessi su una rete. Nell'ambito di VNC, l'uso di TLS aggiunge un livello di sicurezza crittografica alla connessione VNC, impedendo a terzi di intercettare o modificare il traffico di dati tra il client e il server.

eseguire in root `/etc/vnc.conf` o `/etc/vnc/vncserver.conf`.  
e scrivere `SecurityTypes = TLSVnc` :

```
MetaSploit [In esecuzione] - Oracle VM VirtualBox
File  Macchina  Visualizza  Inserimento  Dispositivi  Aiuto
GNU nano 2.0.7      File: /etc/vnc.conf
SecurityTypes=UncAuth,TLSVnc
```





Telnet è un protocollo di rete utilizzato per consentire la comunicazione remota tra computer su una rete.

Apro il file di configurazione col comando `sudo nano /etc/inetd.conf`  
Cerco la riga che fa riferimento al Telnet e la commento aggiungendo `#`

Metasploit [in esecuzione] - Oracle VM VirtualBox

File Macchina Visualizza Inserimento Dispositivi Aiuto

GNU nano 2.0.7 File: /etc/ssh/sshd\_config

```
# Package generated configuration file
# See the sshd(8) manpage for details

# What ports, IPs and protocols we listen for
Port 22
# Use these options to restrict which interfaces/protocols sshd will bind to
#ListenAddress ::
#ListenAddress 0.0.0.0
Protocol 2
# HostKeys for protocol version 2
HostKey /etc/ssh/ssh_host_rsa_key
HostKey /etc/ssh/ssh_host_dsa_key
#Privilege Separation is turned on for security
UsePrivilegeSeparation yes

# Lifetime and size of ephemeral version 1 server key
KeyRegenerationInterval 3600
ServerKeyBits 768

# Logging
```

[ Read 77 lines ]

Get Help WriteOut Read File Prev Page Cut Text Cur Pos  
Exit Justify Where Is Next Page UnCut Text To Spell



Almeno una delle condivisioni NFS esportate dal server remoto può essere montata dall'host di scansione. Un utente malintenzionato potrebbe essere in grado di sfruttare questa funzionalità per leggere (ed eventualmente scrivere) file su un host remoto.

Configurare NFS sull'host remoto in modo che solo gli host autorizzati possano montare le condivisioni remote.

Nella directory si modifica l'ultima linea aggiungendo #

**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.

**Output**

```
The following NFS shares could be mounted :  
  
+ /  
+ Contents of / :  
- .  
- ..  
- bin  
- boot  
- cdrom  
more...
```

To see debug logs, please visit individual host

Port ▲	Hosts
2049 / udp / rpc-nfs	192.168.1.101

```
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)

^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
```



# Report dopo la risoluzione delle vulnerabilità

Sev ▼	CVSS ▼	VPR ▼	Name ▲	Family ▲
CRITICAL	10.0		Unix Operating System Unsupported Version Detection	General
CRITICAL	10.0 *	7.4	UnrealIRCd Backdoor Detection	Backdoors
CRITICAL	9.8		SSL Version 2 and 3 Protocol Detection	Service detection
CRITICAL	9.8		Bind Shell Backdoor Detection	Backdoors
MIXED	...	...	4 DNS (Multiple Issues)	DNS
CRITICAL	...	...	2 SSL (Multiple Issues)	Gain a shell remotely
MIXED	...	...	3 Apache Tomcat (Multiple Issues)	Web Servers
HIGH	7.5 *	6.7	rlogin Service Detection	Service detection
HIGH	7.5 *	6.7	rsh Service Detection	Service detection
HIGH	7.5	6.7	Samba Badlock Vulnerability	General
MIXED	...	...	15 SSL (Multiple Issues)	General
MIXED	...	...	5 ISC Bind (Multiple Issues)	DNS
MEDIUM	6.5		TLS Version 1.0 Protocol Detection	Service detection
MEDIUM	6.5		Unencrypted Telnet Server	Misc.
MEDIUM	5.9	3.6	SSL Anonymous Cipher Suites Supported	Service detection

MIXED	...	...	2 SMB (Multiple Issues)	Misc.
MIXED	...	...	2 TLS (Multiple Issues)	Misc.
MIXED	...	...	2 TLS (Multiple Issues)	SMTP problems
LOW	3.7	4.5	SSL/TLS Diffie-Hellman Modulus <= 1024 Bits (Logjam)	Misc.
LOW	2.6 *		X Server Detection	Service detection
INFO	...	...	6 SMB (Multiple Issues)	Windows
INFO	...	...	2 HTTP (Multiple Issues)	Web Servers
INFO	...	...	2 TLS (Multiple Issues)	General
INFO	...	...	2 FTP (Multiple Issues)	Service detection
INFO	...	...	3 VNC (Multiple Issues)	Service detection
INFO	...	...	2 Apache HTTP Server (Multiple Issues)	Web Servers
INFO	...	...	2 PHP (Multiple Issues)	Web Servers
INFO	...	...	2 RPC (Multiple Issues)	RPC
INFO	...	...	2 SSH (Multiple Issues)	General
INFO	...	...	2 SSH (Multiple Issues)	Service detection

Web Server (Multiple Issues)