Progetto W5

Scansione vulnerabilità di Metasploitable con Nessus

Traccia

Effettuare una scansione completa sul target Metasploitable.

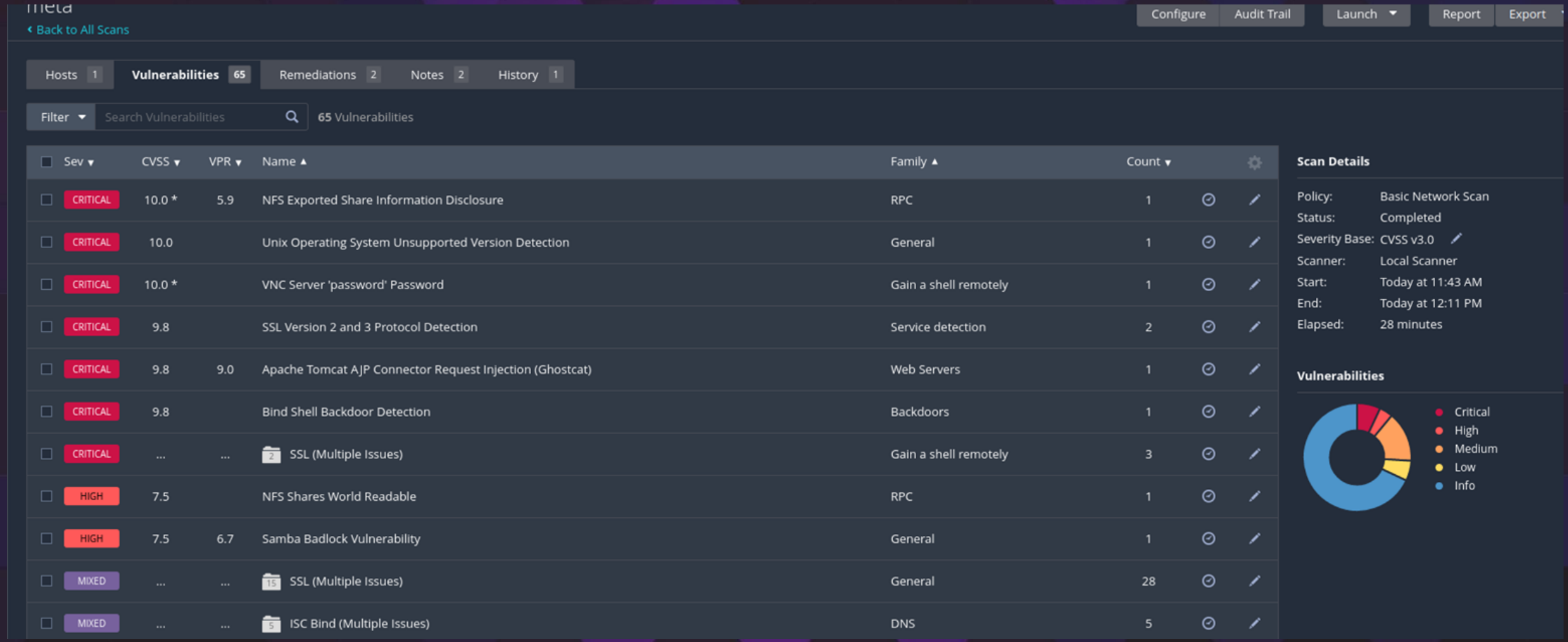
Scegliete da un minimo di 2 fino ad un massimo di 4 vulnerabilità critiche / high e provate ad implementare delle azioni di rimedio.

N.B. le azioni di rimedio, in questa fase, potrebbero anche essere delle regole firewall ben configurate in modo da limitare eventualmente le esposizioni dei servizi vulnerabili. Vi consigliamo tuttavia di utilizzare magari questo approccio per non più di una vulnerabilità.

Per dimostrare l'efficacia delle azioni di rimedio, eseguite nuovamente la scansione sul target e confrontate i risultati con quelli precedentemente ottenuti.

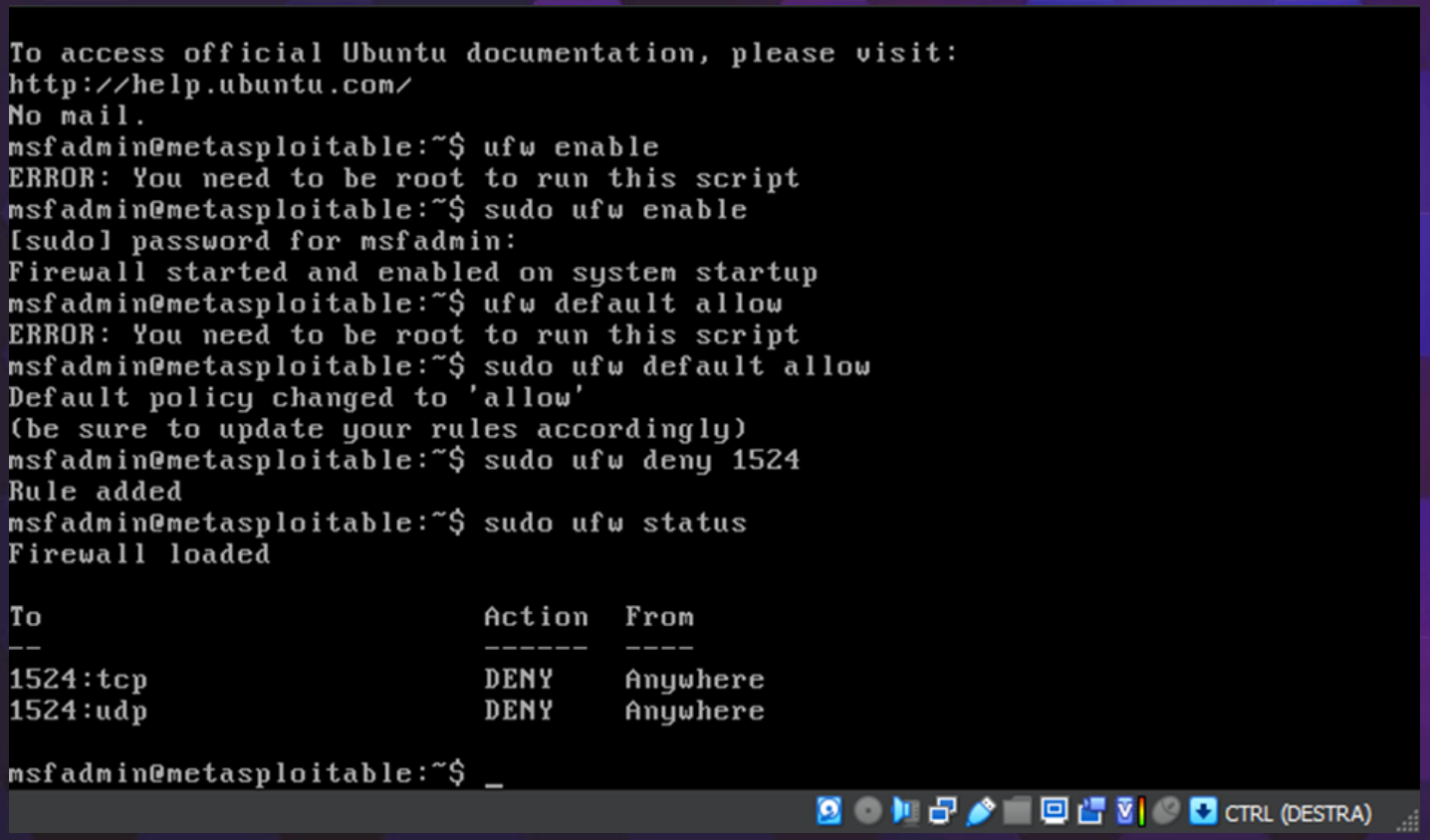
Dopo aver configurato Nessus, è stata avviata una scansione per individuare le vulnerabilità all'indirizzo di Metasploitable. Il risultato della scansione ha evidenziato numerose criticità, su cui è stato successivamente lavorato per cercare di risolverle.

Risultato scansione iniziale



Bind Shell Backdoor Detection

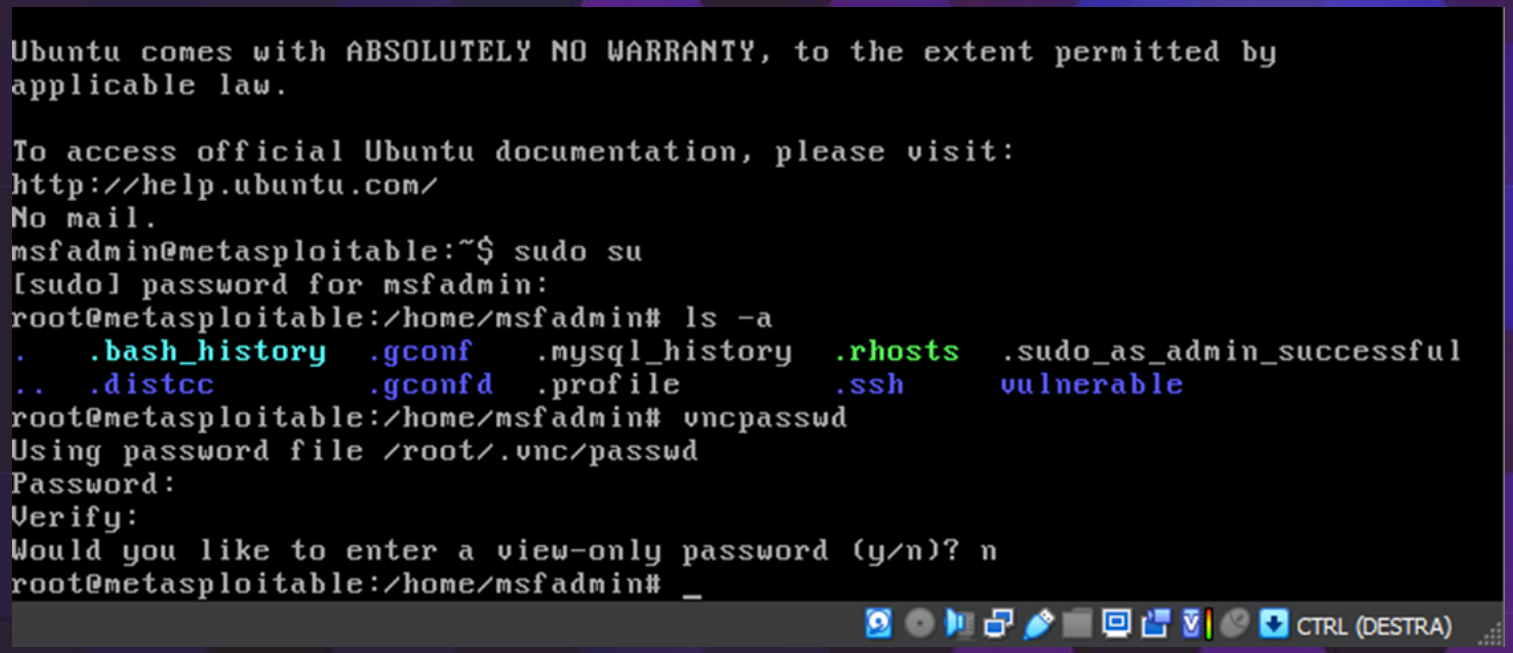
Dopo aver ricevuto segnalazioni di una possibile presenza di backdoor sulla porta 1524, è stato necessario intervenire regolando le impostazioni del firewall. Le regole di default sono state configurate per la porta al fine di mitigare il rischio segnalato.



Una backdoor è un metodo nascosto per accedere in modo non autorizzato a un sistema informatico, consentendo a un attaccante di bypassare le normali procedure di autenticazione e ottenere un accesso segreto e non autorizzato.

VNC Server <password> Password

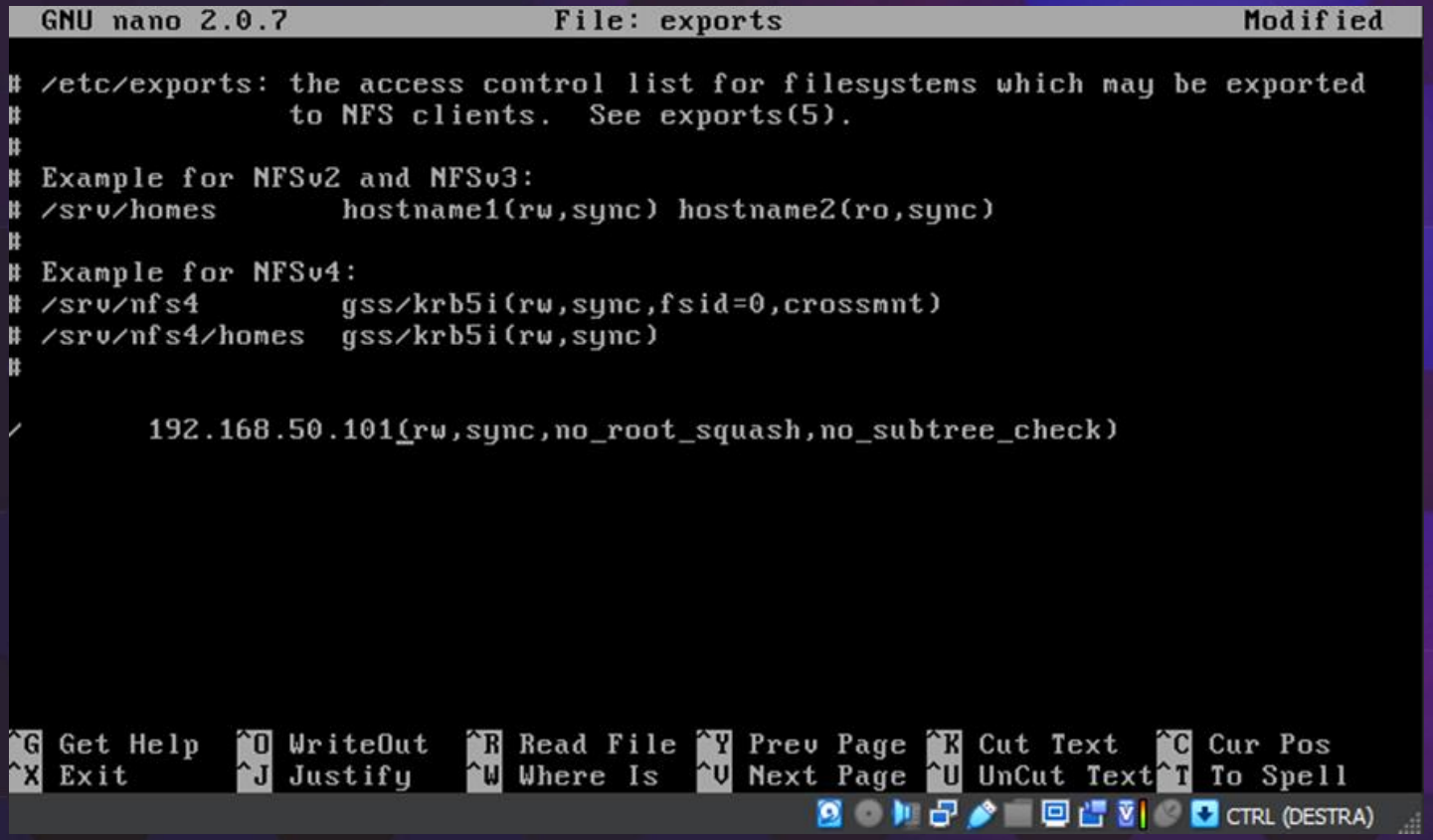
È stata rilevata una password troppo debole per il server VNC. È stato quindi necessario intervenire per inserire una password più sicura, utilizzando caratteri alfanumerici per garantire maggiore protezione.



Un server VNC è un software che consente agli utenti di controllare un computer remoto attraverso una connessione di rete. Utilizzando il protocollo VNC (Virtual Network Computing), gli utenti possono visualizzare e interagire con l'interfaccia grafica del computer remoto come se fossero fisicamente presenti di fronte ad esso.

NFS Exported Share Information Disclosure

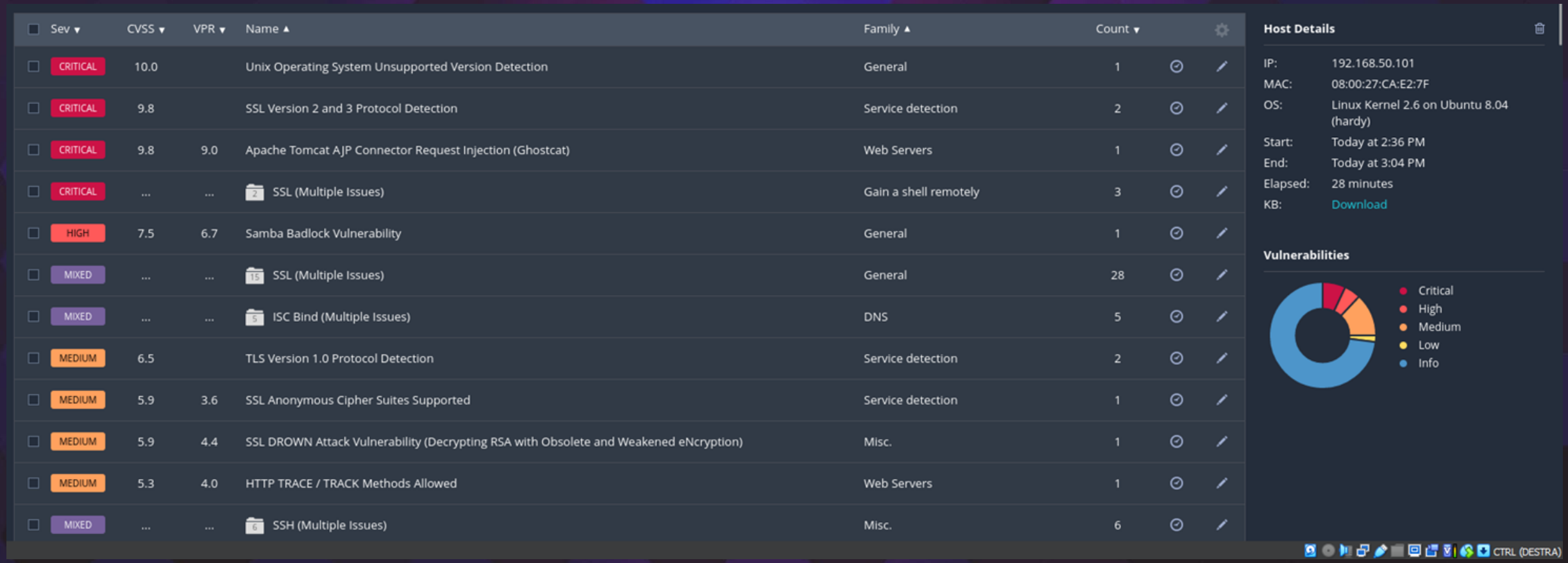
È stata rilevata una vulnerabilità nell'accesso al NFS. È stato necessario intervenire modificando gli accessi consentiti solo alla macchina Linux, apportando modifiche al file exports per aumentare la sicurezza del sistema.



NFS (Network File System) è un protocollo di rete che consente ai sistemi di memorizzazione di condividere file e risorse su una rete. Consente agli utenti di accedere e montare file e directory remote come se fossero locali sul proprio sistema.

Scansione dopo le modifiche

È evidente che i tre problemi critici individuati sono stati risolti durante l'ultima scansione delle vulnerabilità, migliorando così la sicurezza complessiva del sistema.



Sev	CVSS	VPR	Name	Family	Count
CRITICAL	10.0		Unix Operating System Unsupported Version Detection	General	1
CRITICAL	9.8		SSL Version 2 and 3 Protocol Detection	Service detection	2
CRITICAL	9.8	9.0	Apache Tomcat AJP Connector Request Injection (Ghostcat)	Web Servers	1
CRITICAL	...	...	SSL (Multiple Issues)	Gain a shell remotely	3
HIGH	7.5	6.7	Samba Badlock Vulnerability	General	1
MIXED	...	...	SSL (Multiple Issues)	General	28
MIXED	...	...	ISC Bind (Multiple Issues)	DNS	5
MEDIUM	6.5		TLS Version 1.0 Protocol Detection	Service detection	2
MEDIUM	5.9	3.6	SSL Anonymous Cipher Suites Supported	Service detection	1
MEDIUM	5.9	4.4	SSL DROWN Attack Vulnerability (Decrypting RSA with Obsolete and Weakened eNcryption)	Misc.	1
MEDIUM	5.3	4.0	HTTP TRACE / TRACK Methods Allowed	Web Servers	1
MIXED	...	...	SSH (Multiple Issues)	Misc.	6

Host Details

IP:	192.168.50.101
MAC:	08:00:27:CA:E2:7F
OS:	Linux Kernel 2.6 on Ubuntu 8.04 (hardy)
Start:	Today at 2:36 PM
End:	Today at 3:04 PM
Elapsed:	28 minutes
KB:	Download

Vulnerabilities

CTRL (DESTRA)

Fine della presentazione

Amedeo Natalizi