Report Vulnerability Assessment

Indice

Vulnerability Scanning; identificazione delle vulnerabilità

Nell'ambito della computer security Nessus è un software proprietario di tipo client-server di scansione di tutti i tipi di vulnerabilità. Costituito da nessusd, il demone, che effettua la scansione, e da nessus, il client, il quale fornisce all'utente i risultati della scansione, tramite lo scan e l'abilitazione di plugin appositamente configurabili a seconda della tipologia di host e vulnerabilità che si andrà ad analizzare, rileva le vulnerabilità presenti suggerendo le possibili soluzioni attraverso report di facile analisi in vari formati. Tuttora Nessus con le sue tante opzioni per la scansione, la possibilità di scrivere plugin e per il tipo di reportistica prodotta rimane uno dei migliori strumenti per vulnerability assessment.
Tipicamente, Nessus inizialmente effettua una port scan con il suo portscanner interno (oppure talvolta utilizza Nmap[4]) per determinare quali porte sono aperte sull'obiettivo e poi tenta diversi exploit sulle porte aperte. I test di vulnerabilità, disponibili sotto forma di corposi plugin, sono scritti in NASL (Nessus Attack Scripting Language), un linguaggio di programmazione ottimizzato per l'interazione tra reti differenti.

La scansione effettuata ha avuto come target Metaspoitable (IP 192.168.1.99).

Ai fini del report sono state prese in considerazione solo le vulnerabilità con un livello di severity “critical”. Secondo il Common Vulnerability Scoring System (CVSS), che fornisce un modo per catturare le principali caratteristiche di una vulnerabilità e produrre un punteggio numerico che ne riflette la gravità, le vulnerabilità classificate come critiche sono quelle ricomprese tra un punteggio di 9.1 e 10.0.

Di seguito l'elenco delle vulnerabilità scansionate:

192.168.1.99

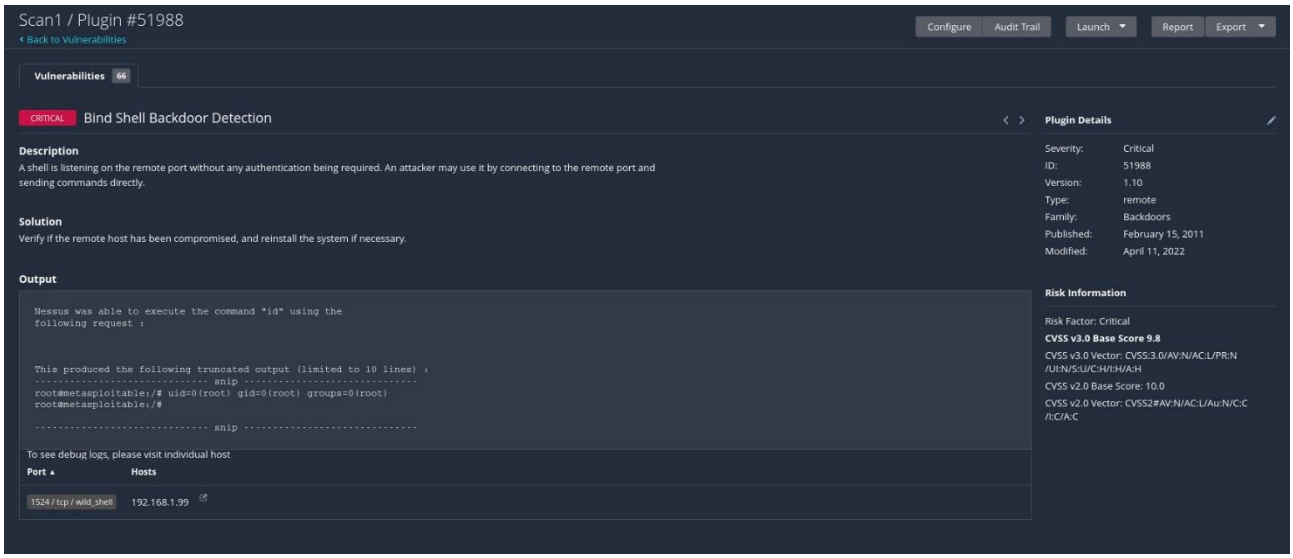
9	6	18	7	71
CRITICAL	HIGH	MEDIUM	LOW	INFO

Vulnerabilities — Total: 111

SEVERITY	CVSS V3.0	VPR SCORE	PLUGIN	NAME
CRITICAL	9.8	-	51988	Bind Shell Backdoor Detection
CRITICAL	9.8	-	20007	SSL Version 2 and 3 Protocol Detection
CRITICAL	9.1	-	33447	Multiple Vendor DNS Query ID Field Prediction Cache Poisoning
CRITICAL	10.0	-	33850	Unix Operating System Unsupported Version Detection
CRITICAL	10.0*	-	32314	Debian OpenSSH/OpenSSL Package Random Number Generator Weakness
CRITICAL	10.0*	-	32321	Debian OpenSSH/OpenSSL Package Random Number Generator Weakness (SSL check)
CRITICAL	10.0*	-	11356	NFS Exported Share Information Disclosure
CRITICAL	10.0*	-	46882	UnrealIRCd Backdoor Detection
CRITICAL	10.0*	-	61708	VNC Server 'password' Password

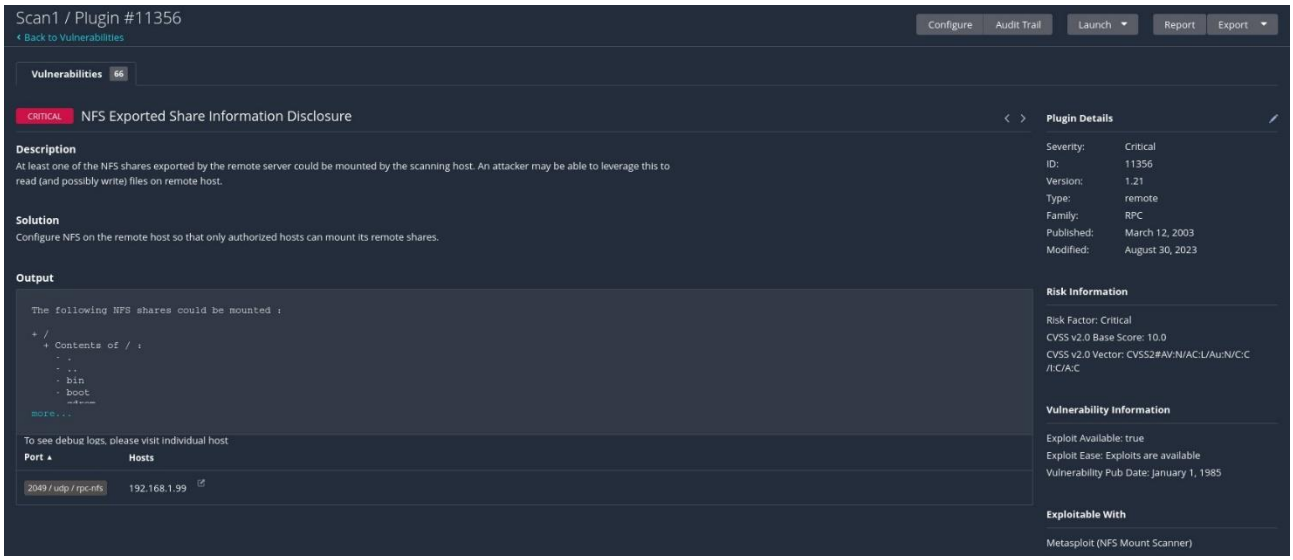
Sono state prese in esame tre tipologie di vulnerabilità: Bind Shell Backdoor Detection, NFS Exported Share Information Disclosure e VCN Server ‘password’ Password.

- BPFdoor



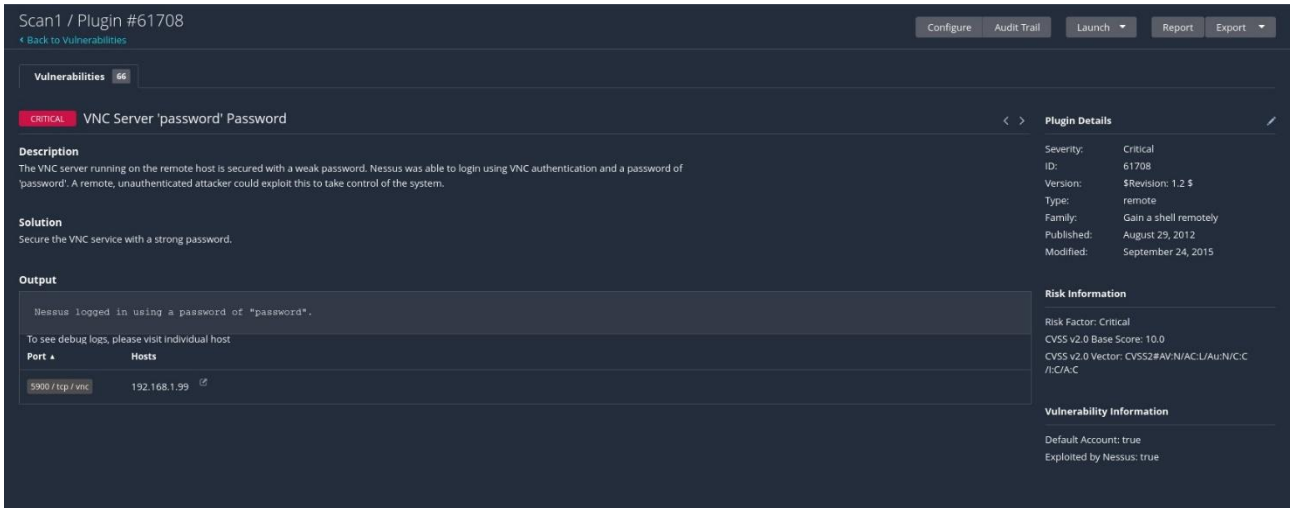
BPFdoor è un malware che bypassa i firewall per connettersi da remoto a una shell di Linux. Ha l’obiettivo di prendere il controllo completo del sistema sotto attacco, in maniera passiva e mettendosi in ascolto.
Sfruttando una funzione di sniffing, che opera nell’interfaccia al livello di rete, BPFdoor non è soggetto alle regole del firewall e resta in “ascolto” di pacchetti dalle porte ICMP, UDP e TCP. Tramite il rilevamento di specifici pacchetti, dotati di valori ben precisi e, nel caso di UDP/TDP, di una password, la backdoor si attiva eseguendo uno dei comandi supportati, ad esempio attivando una Reverse Shell.

- NFS Exported Share Information Disclosure



NFS è un protocollo di rete inizialmente sviluppato da Sun Microsystems nel 1984 che facilita la condivisione dei contenuti sulla rete. Le cartelle condivise risulteranno accessibile, anche in modalità remota, dai sistemi client così come se fossero disponibili in ambito locale.
Il protocollo NFS viene spesso utilizzato nelle reti in cui sono presenti sia sistemi Linux che Windows così da semplificare l'accesso alle risorse.
Supportando a sua volta il protocollo TCP, NFS può essere utilizzato per condividere file e cartelle tra sedi remote attraverso la rete Internet.
In presenza di un NFS Exported Share Information Disclosure si presuppone che almeno una delle condivisioni NFS esportate dal server remoto potrebbe essere montata dall'host di scansione. Un utente malintenzionato potrebbe essere in grado di sfruttare questo per leggere (ed eventualmente scrivere) file sull'host remoto.

- VCN Server 'password' Password



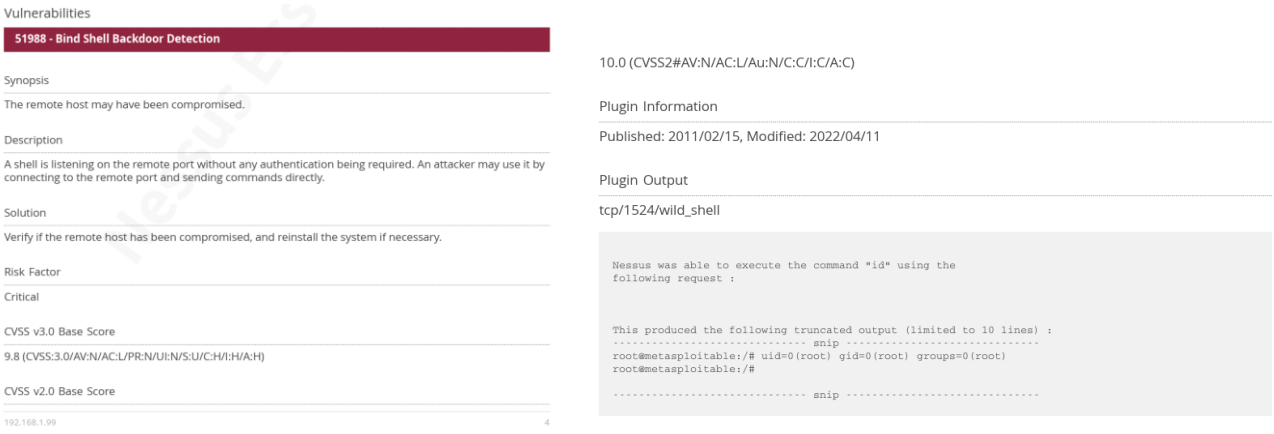
VCN è un servizio attivabile per fare in modo che il personal computer sul quale viene installato il server VNC sia sempre accessibile da remoto. Solitamente è necessario soltanto specificare una password. Tale password vi consentirà di amministrare, da remoto, il computer sul quale avete installato il server di VNC.
Attraverso questa finestra è possibile, eventualmente, attivare funzionalità avanzate, come la disabilitazione di tastiera/mouse locali/remoti.

Risoluzione delle vulnerabilità

La risoluzione delle vulnerabilità si riferisce al processo di identificazione e correzione delle vulnerabilità o dei punti deboli della sicurezza in software, sistemi o reti. Comporta l'analisi e la definizione delle priorità dei rischi per la sicurezza, l'applicazione di patch e aggiornamenti di sicurezza, l'implementazione di controlli di sicurezza e la verifica dell'efficacia delle misure di sicurezza.

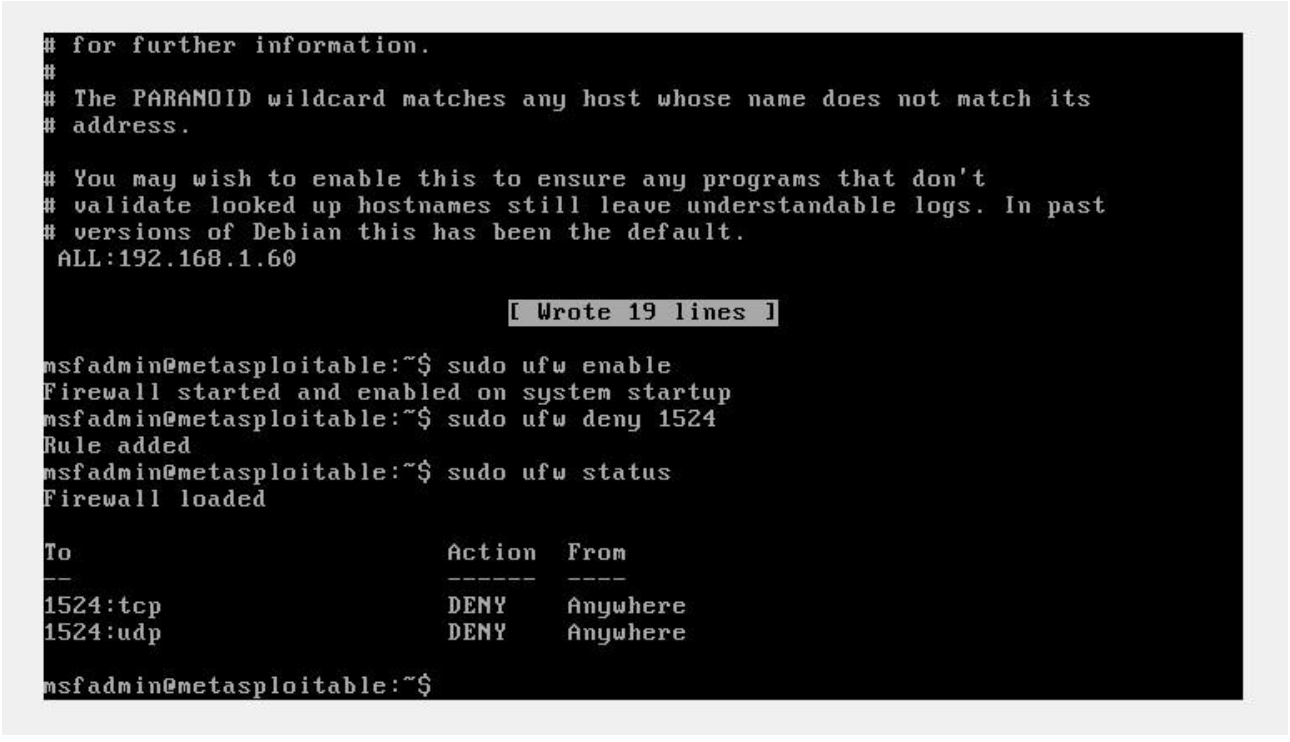
L’obiettivo del processo di risoluzione delle vulnerabilità è ridurre il rischio di attacchi informatici, proteggere le risorse digitali e mantenere la riservatezza, l’integrità e la disponibilità delle informazioni.

Si è proceduto con la risoluzione della prima vulnerabilità ‘Bind Shell Backdoor Detection’.



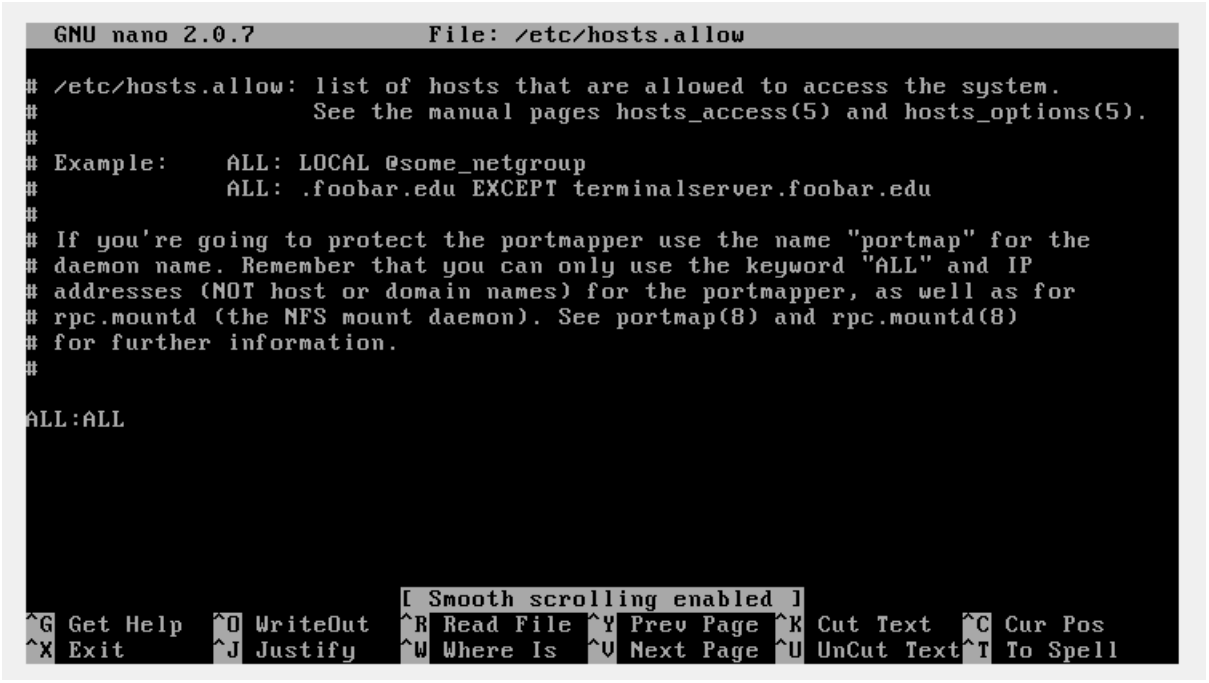
Nessus ha rilevato una backdoor (remote shell) sulla porta 1524.

Con il comando *sudo ufw enable* è stato attivato il firewall e, successivamente, con *sudo ufw deny 1524* è stata applicata una regola che negasse qualsiasi azione sulla porta 1524.

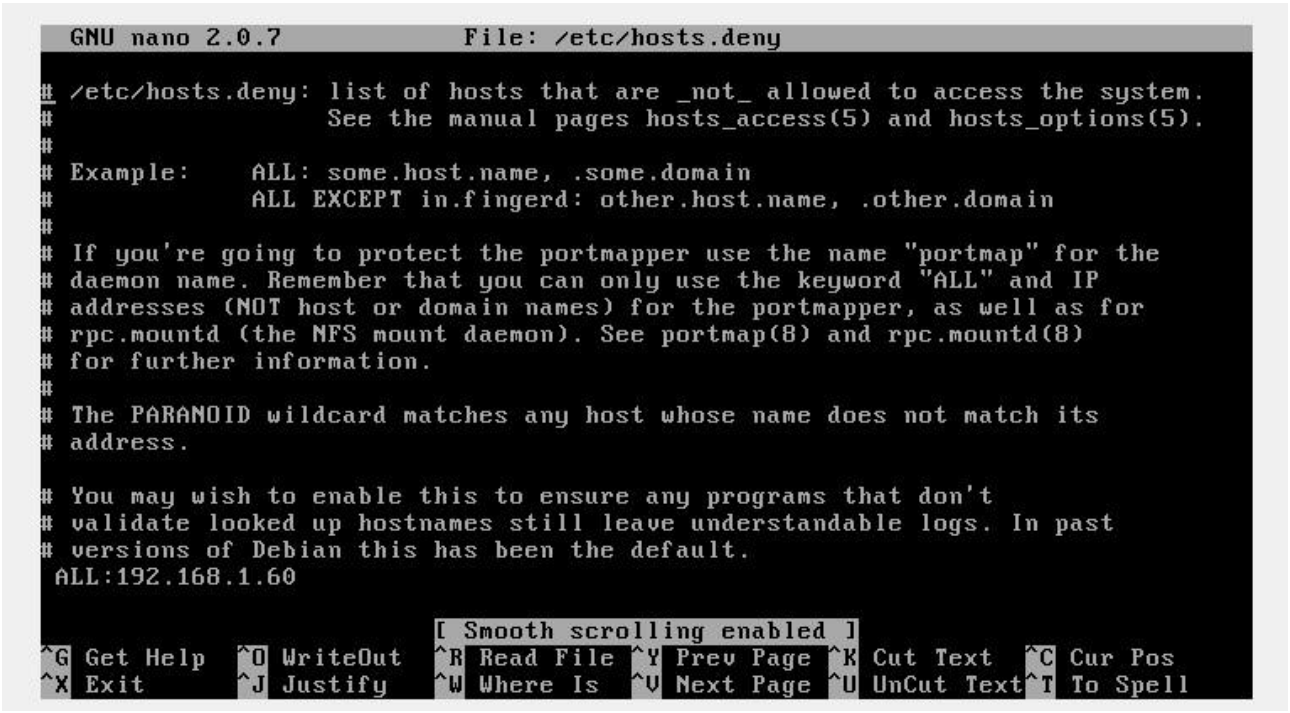


La seconda vulnerabilità NFS Exported Share Information Disclosure è dovuta alla configurazione su Metaspoitable che consente l'accesso a tutte le share condivisibili. Tramite il comando */etc/exports* è possibile visualizzare la lista delle cartelle condivisibili, mentre con *sudo nano /etc/hosts.allow* si può specificare quali computer sulla rete posso accedere alle directory condivise e con *sudo nano /etc/hosts.deny* quali, invece, non possono.

Con il comando allow è stata decommentata la riga ALL:ALL



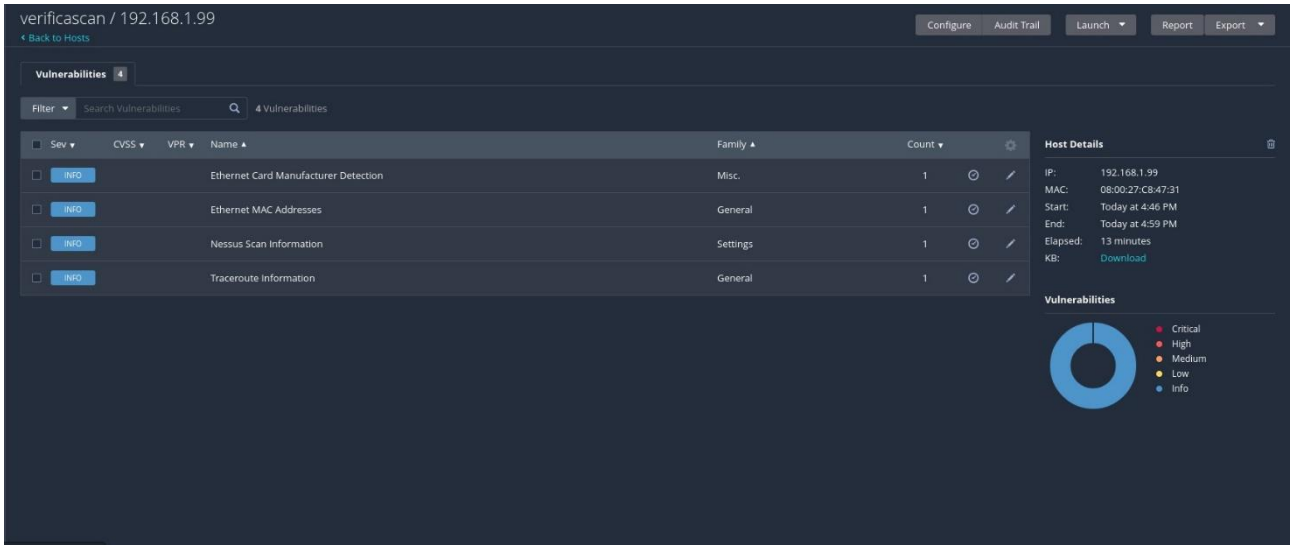
Con il comando deny è stata modificata la riga ALL:192.168.1.60, quindi inserendo l'IP di Kali.



Infine, la terza vulnerabilità, VCN Server ‘password’ Password, è stata risolta inserendo una password che rispecchi criteri tali da garantire un alto livello di sicurezza, difficile da scoprire con attacchi come Brute Force.

Rivalutazione

Quando le vulnerabilità vengono risolte, viene sempre eseguita una nuova valutazione delle vulnerabilità per assicurarsi che le attività di correzione abbiano funzionato e che non abbiano introdotto nuove vulnerabilità.



La posizione di sicurezza complessiva risulta, ora, ottimale.