S5L5,

BENVENUTI LUIGI

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.

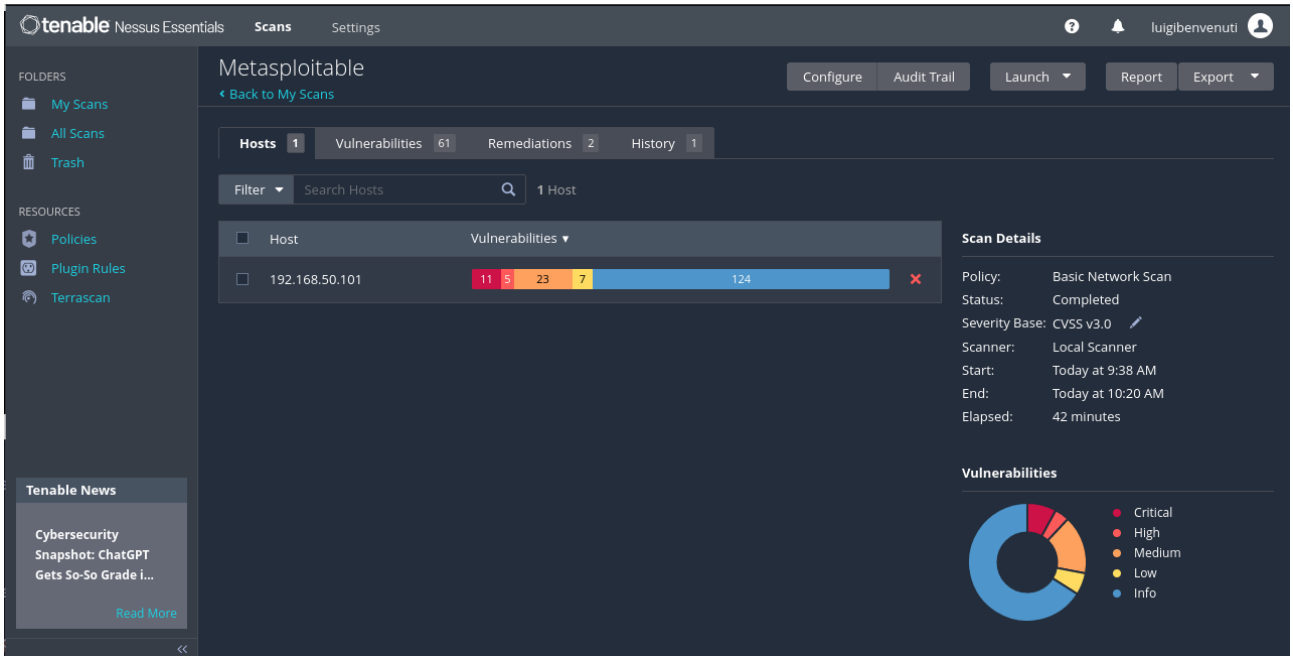
Per effettuare la scansione, utilizzeremo la macchina virtuale Kali Linux come client sul quale avviare il tool Nessus e la macchina Metasploitable 2 come target.

Avviamo il servizio Nessus su Kali ed accediamo alla sua interfaccia grafica da browser all'URL https://kali:8834.

Per avviare la scansione, selezioniamo la voce "Basic Network Scan", che ci fornisce una scansione con funzioni base di default, ed inseriamo come IP target quello della macchina Metasploitable.

Selezioniamo poi l'opzione <<port scan common ports>>, per andare a scansionare soltanto le porte più comuni.

Il risultato della scansione è il seguente:



Scarichiamo il report in formato PDF utilizzando la funzione <<Report>> in alto a destra.

192.168.50.101

9	4	17	6	70
CRITICAL	HIGH	MEDIUM	LOW	INFO

Vulnerabilities — Total: 106

SEVERITY	CVSS V3.0	VPR SCORE	PLUGIN	NAME
CRITICAL	9.8	-	134862	Apache Tomcat AJP Connector Request Injection (Ghostcat)
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*	-	61708	VNC Server 'password' Password
HIGH	8.6	-	136769	ISC BIND Service Downgrade / Reflected DoS
HIGH	7.5	-	42256	NFS Shares World Readable

Nella prima parte del report generato, ci vengono ricapitolate le vulnerabilità rilevate sulla macchina scansionata.

Vediamo nel dettaglio il significato di alcune voci:

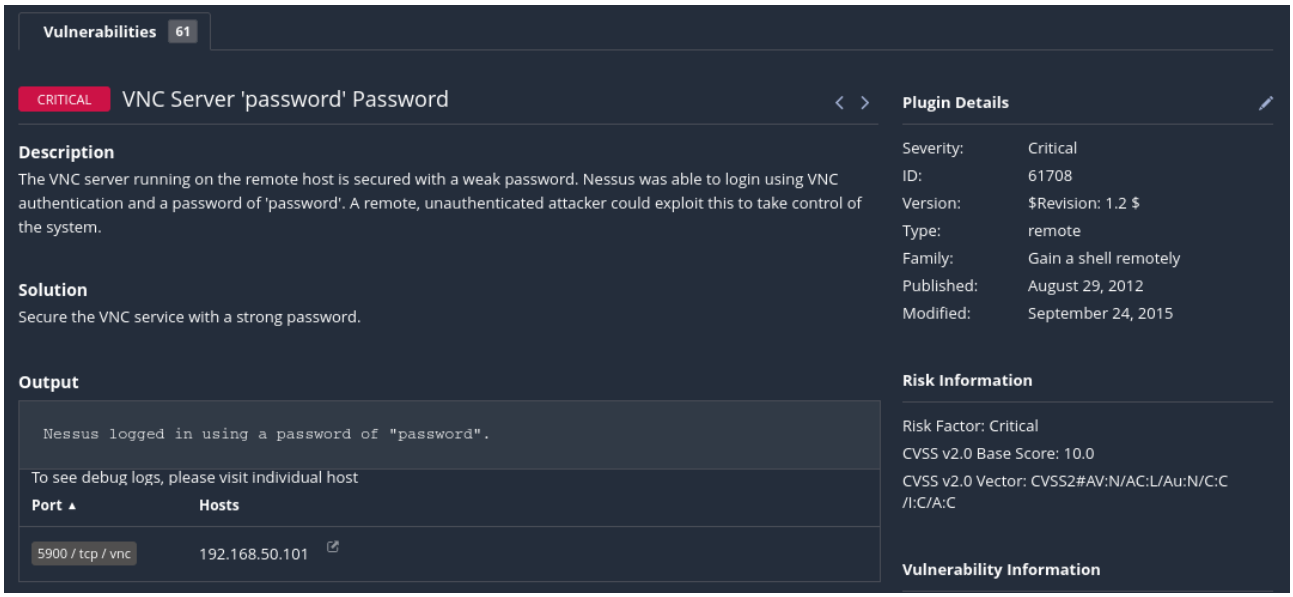
- Severity: indica il grado di pericolosità di una vulnerabilità, ed ha 5 voci. Oltre a critical, high, medium e low, fornisce una voce info, che sta ad indicare che la macchina espone alcune possibili informazioni interessanti per un eventuale attaccante.
- CVSS: Common Vulnerability Scoring System, metodo standard di valutazione della gravità di una vulnerabilità.
- VPR score: Vulnerability Priority Rating, è uno score fornito direttamente da Nessus che consiglia un indice di priorità nell'applicazione delle patch.
- Plugin: indica l'ID plugin di Nessus che ha scovato la vulnerabilità.
- Name: indica il nome della vulnerabilità rilevata.

Ci concentreremo principalmente su 2 applicazioni critiche:

1- VNC Server ‘password’ Password

Prendiamo in esame la criticità con pericolosità Critical di nome “VNC Server Password password”; Questa vulnerabilità ha CVSS 10, quindi massimo. Essa sta ad indicare che una virtual network computing app ha come password di accesso “password”, facilmente reperibile da un potenziale attaccante. Si potrebbe sfruttare la vulnerabilità per lanciare una shell e prendere il comando del server (indicato nella voce Family).

Vediamo le specifiche della voce fornite da Nessus:



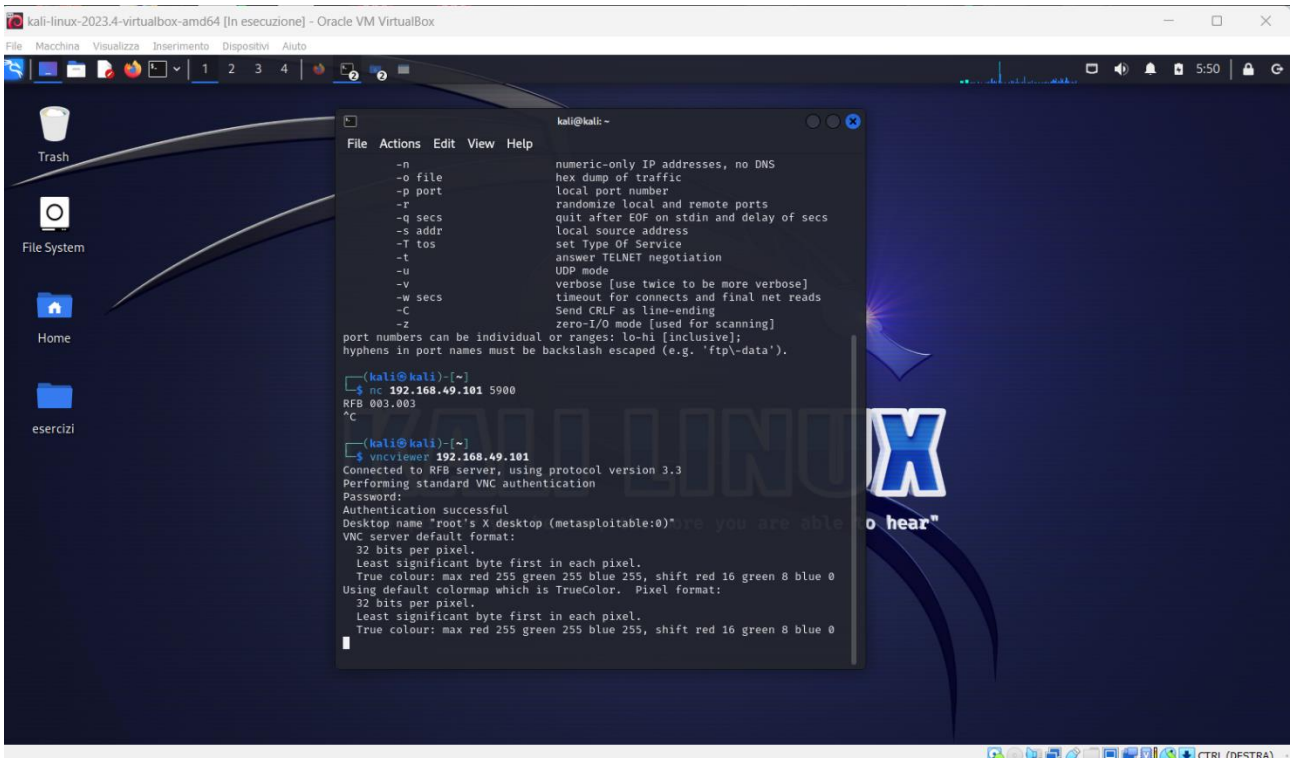
Il web server attivo sulla porta 5900 di Metasploitable è dunque accessibile tramite VNC authentication utilizzando semplicemente una password ‘password’.

Fase di exploit:

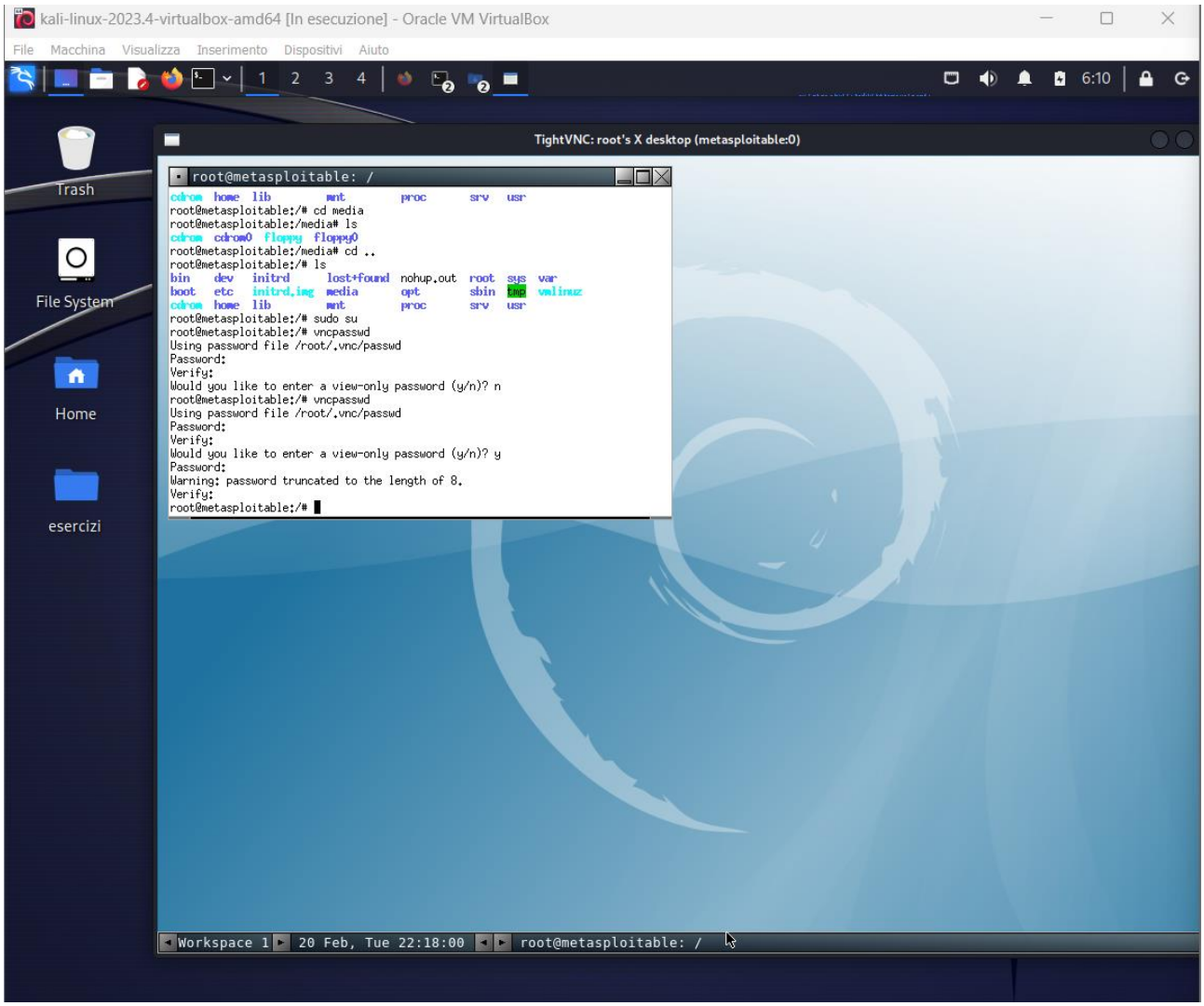
Tentiamo dunque l’accesso al servizio dalla macchina Metasploitable.

Il comando necessario è: vncviewer ip_target

La porta utilizzata sarà di default la 5900.



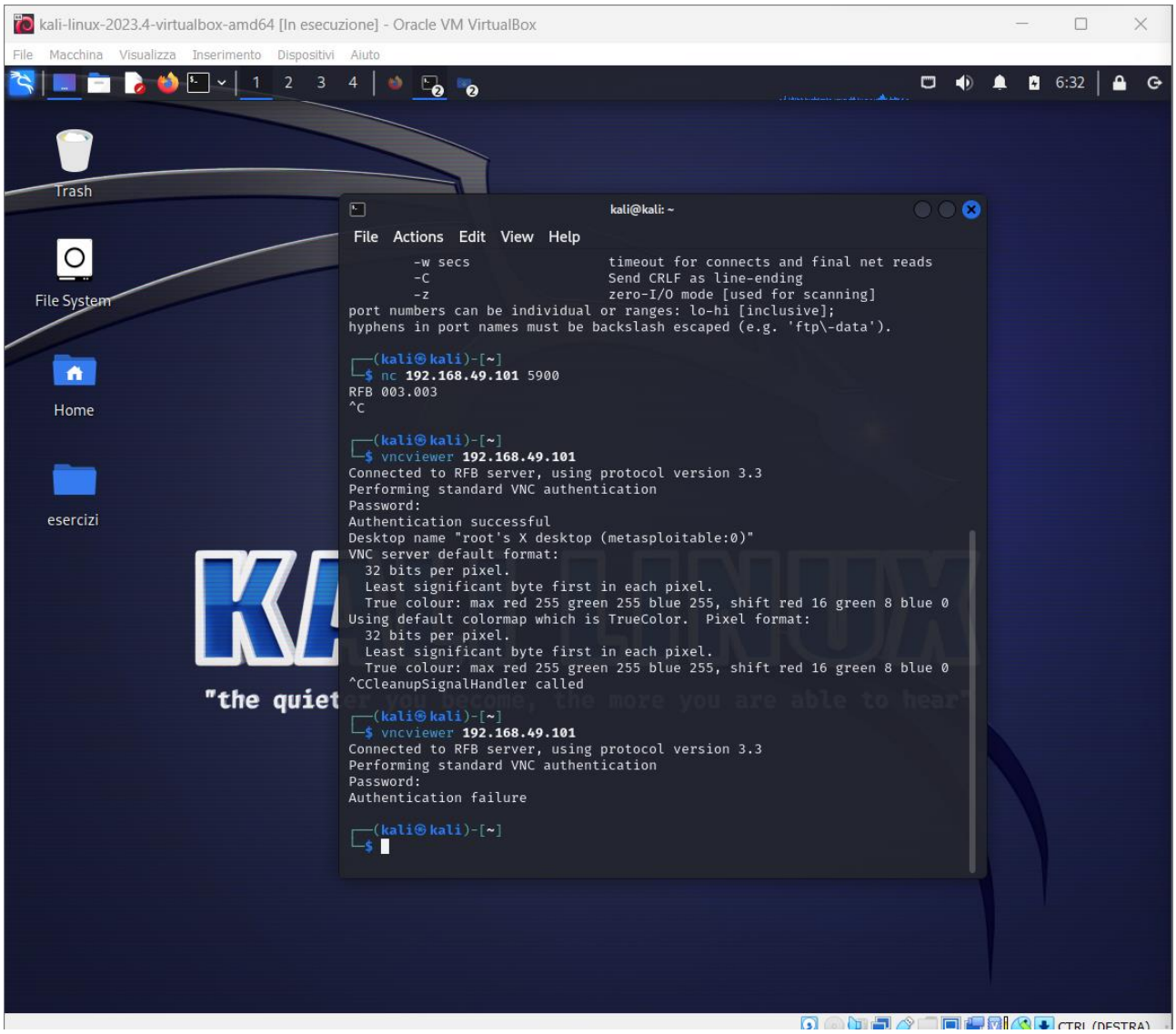
Inseriamo come richiesto la password ‘password’, e riusciamo correttamente ad autenticarci sull’interfaccia grafica del RFB server (remote framebuffer, protocollo client-server di connessione ad interfaccia remota). Abbiamo dunque guadagnato una via di configurazione all’interno del web server.



Vulnerability fixing:

A questo punto, ottenuto l'accesso, andiamo a sfruttarlo per eseguire le patch di correzione. Scegliamo una nuova password complessa ed inseriamo una view-only password per consultare (senza modificare) la configurazione del web server.

Verifichiamo che le correzioni siano state effettuate con successo:



L'autenticazione con password 'password' non è più attiva.

2- NFS exported share information disclosure

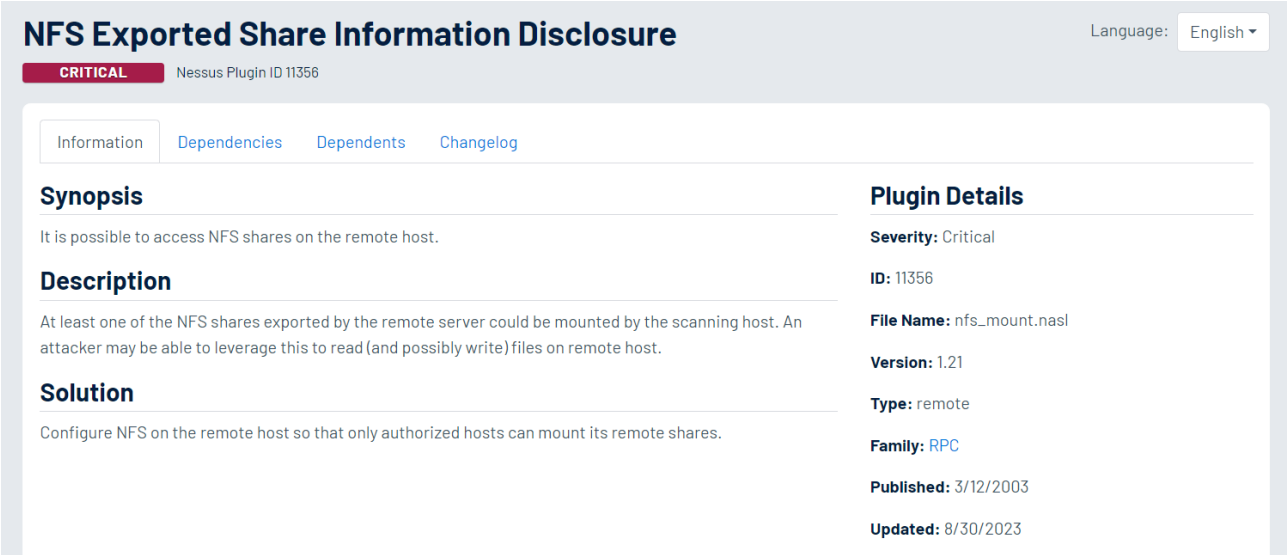
Il secondo caso critico preso in esame è quello relativo alla vulnerabilità **NFS exported share information disclosure**.

Esso fa riferimento ad un servizio attivo solitamente sulle porte 111 (RPC) o sulla porta 2049 (NFS).

Fa parte delle vulnerabilità della famiglia **RPC** (Remote Procedure Call), ovvero delle attivazioni di procedura da un host diverso da quello dove il programma viene eseguito.

NFS (Network File Sharing) è un protocollo che permette la condivisione di cartelle e file sulla rete attraverso sistemi operativi diversi, e permette inoltre di accedere localmente ai sistemi remoti nel caso in cui le condivisioni siano "mounted" (comando mount Linux).

Vediamo la descrizione Nessus della criticità:



Lo scanning host ritiene dunque possibile eseguire il mount su una o più cartelle del remote server. Questo potrebbe permettere ad un potenziale attaccante di leggere o addirittura scrivere file sul remote host.

Fase di exploit:

Per prima cosa, utilizziamo Nmap per verificare lo stato dettagliato delle porte 111 e 2049: