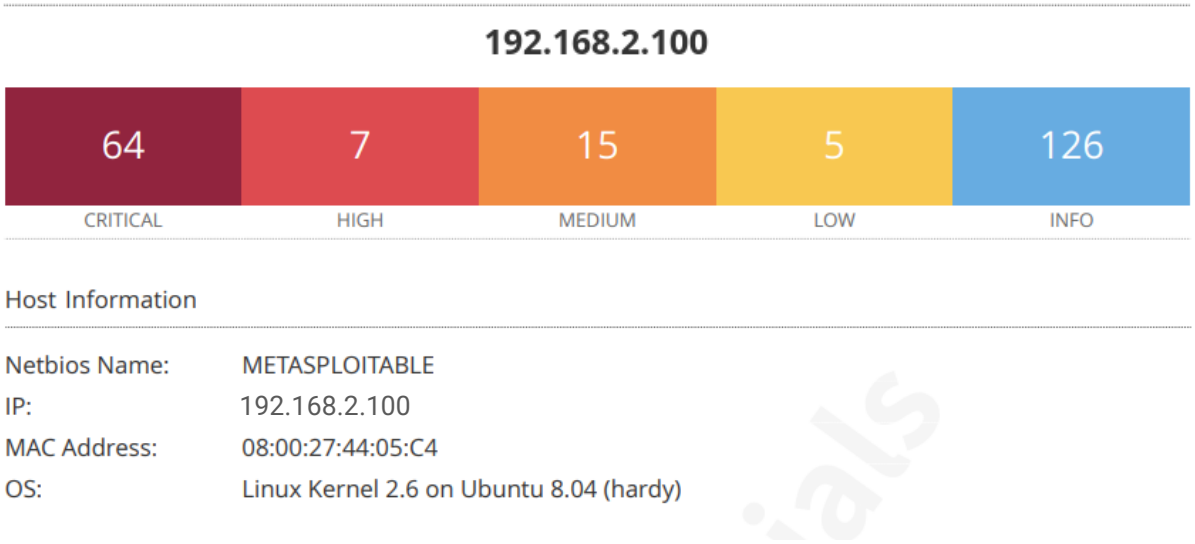
Report W12D4 – Scansione vulnerabilità Metasploitable (192.168.1.101) **Peppoli**

Per la scansione delle vulnerabilità di Metasploitable utilizzeremo Nessus, uno dei software più rinomati per la scansione e la valutazione della sicurezza informatica. È un potente strumento progettato per identificare vulnerabilità nei sistemi informatici, rilevare configurazioni non sicure e individuare potenziali minacce alla sicurezza. Nessus utilizza una vasta gamma di test e tecniche per esaminare reti, server, dispositivi e applicazioni alla ricerca di punti deboli che potrebbero essere sfruttati da attaccanti informatici. Il software fornisce report dettagliati e raccomandazioni per aiutare gli amministratori di sistema e i professionisti della sicurezza a mitigare i rischi e rafforzare la sicurezza delle infrastrutture IT.

Elenco delle vulnerabilità trovate:



Come si può notare abbiamo trovato:
Critiche: Queste sono le vulnerabilità più serie e potenzialmente dannose per un sistema. Possono consentire agli attaccanti di ottenere accesso completo al sistema o di eseguire codice dannoso senza autenticazione.

Alte: Le vulnerabilità considerate di gravità alta possono ancora costituire una minaccia significativa per la sicurezza dei sistemi. Possono consentire l'accesso non autorizzato o l'esecuzione di azioni dannose, anche se potrebbero richiedere condizioni specifiche per essere sfruttate.

Medie: Le vulnerabilità di gravità media rappresentano un rischio meno critico rispetto alle precedenti, ma possono comunque essere sfruttate dagli aggressori per compromettere la sicurezza dei sistemi.

Basse: Queste vulnerabilità sono considerate meno critiche e possono rappresentare un rischio limitato per la sicurezza. Tuttavia, è comunque consigliabile correggerle per mantenere un livello ottimale di sicurezza.

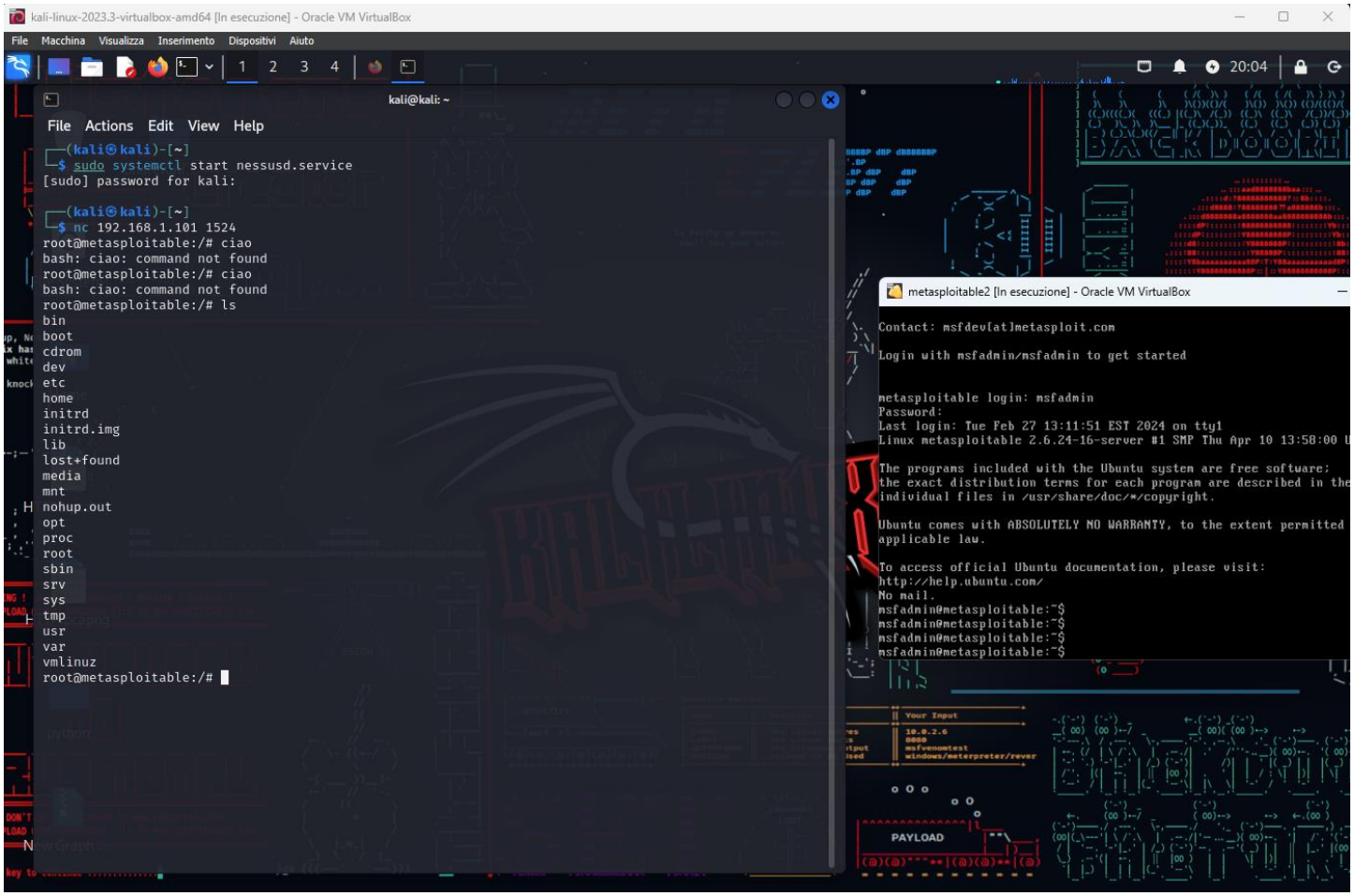
Informative (Info): Questo tipo di vulnerabilità fornisce informazioni aggiuntive sul sistema, come configurazioni non ottimali o informazioni sul software utilizzato. Anche se non rappresentano un rischio diretto per la sicurezza, possono essere utili per migliorare la configurazione e la gestione del sistema.

Vedremo 4 vulnerabilità critiche e il modo in cui risolverle:

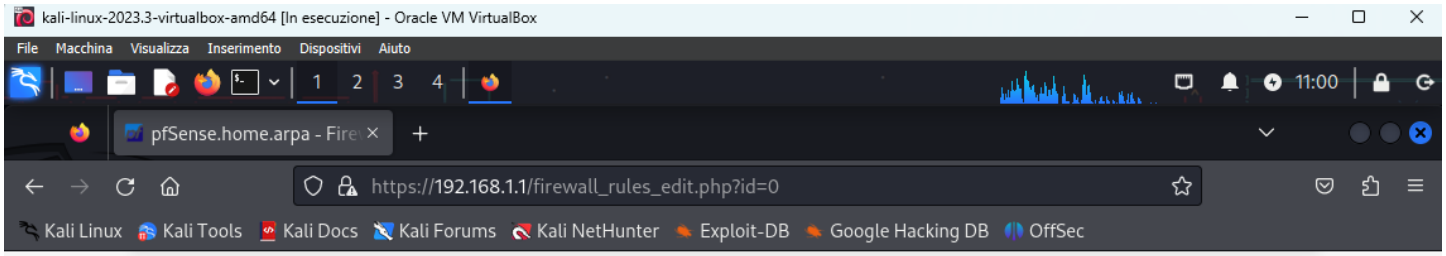
51988 - Bind Shell Backdoor Detection

Riepilogo	**Descrizione**	**Soluzione**
L'host remoto potrebbe essere stato compromesso.	Una shell è in ascolto sulla porta remota senza che sia richiesta alcuna autenticazione. Un utente malintenzionato può usarlo da collegandosi alla porta remota e inviando comandi direttamente.	Verificare se l'host remoto è stato compromesso e, se necessario, reinstallare il sistema.
Fattore di rischio critico	**CVSS v3.0 Base Score**: 9.8	**Plugin Output** tcp/1524/wild_shell

Notiamo come in plugin output nessus segnala una porta aperta 1524 in cui è installata una wild_shell, ossia una backdoor. Per avere la certezza bisogna tentare la connessione:



Per poter risolvere questo problema aggiungiamo una regola Firewall che blocca la connessione alla porta 1524. Per farlo utilizziamo pfsense. Aggiungiamo una nuova regola che impedisce la connessione da Kali 192.168.1.100 a Metasploitable 192.168.2.100 sulla porta che ci interessa.



Firewall / Rules / Edit

Edit Firewall Rule

Action Block

Choose what to do with packets that match the criteria specified below.
Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.

Disabled ☐ Disable this rule

Set this option to disable this rule without removing it from the list.

Interface LAN

Choose the interface from which packets must come to match this rule.

Address Family IPv4

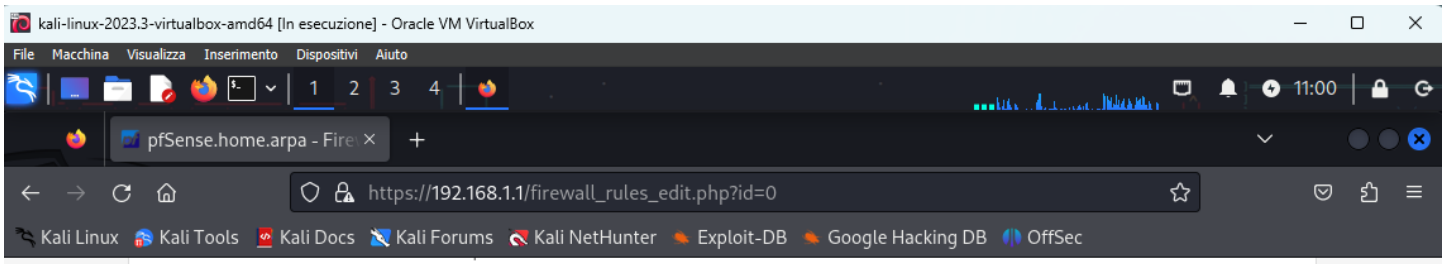
Select the Internet Protocol version this rule applies to.

Protocol TCP

Choose which IP protocol this rule should match.

Source

Source ☐ Invert match Address or Alias 192.168.1.100 /



Source

Source ☐ Invert match Address or Alias 192.168.1.100 /

Display Advanced

The **Source Port Range** for a connection is typically random and almost never equal to the destination port. In most cases this setting must remain at its default value, **any**.

Destination

Destination ☐ Invert match Address or Alias 192.168.2.100 /

Destination Port Range (other) 1524 (other) 1524

From Custom To Custom

Specify the destination port or port range for this rule. The "To" field may be left empty if only filtering a single port.

Extra Options

Log ☑ Log packets that are handled by this rule

Hint: the firewall has limited local log space. Don't turn on logging for everything. If doing a lot of logging, consider using a remote syslog server (see the Status: System Logs: Settings page).

Description

A description may be entered here for administrative reference. A maximum of 52 characters will be used in the ruleset and

61708 - VNC Server 'password' Password

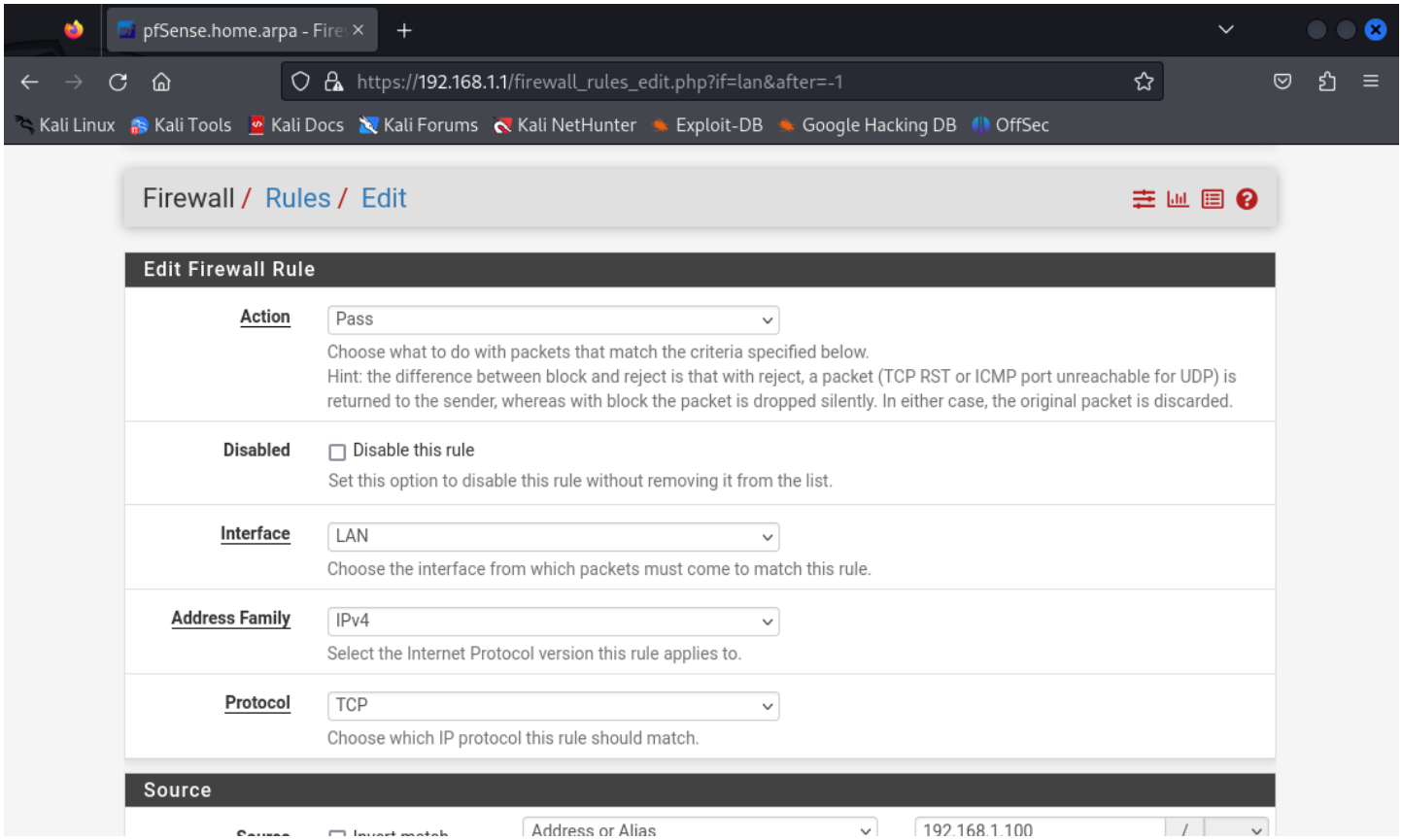
Riepilogo	Descrizione	Soluzione
Un server VNC in esecuzione sull'host remoto è protetto con una password debole.	Il server VNC in esecuzione sull'host remoto è protetto con una password debole. Nessus è riuscito ad accedere utilizzando l'autenticazione VNC e una password "password". Un utente malintenzionato remoto e non autenticato potrebbe sfruttare questo per prendere il controllo del sistema.	Mettere in sicurezza il servizio VNC con una password forte.
Fattore di rischio critico	**CVSS v2.0 Base Score**: 10.0	**Plugin Output** tcp/5900/vnc

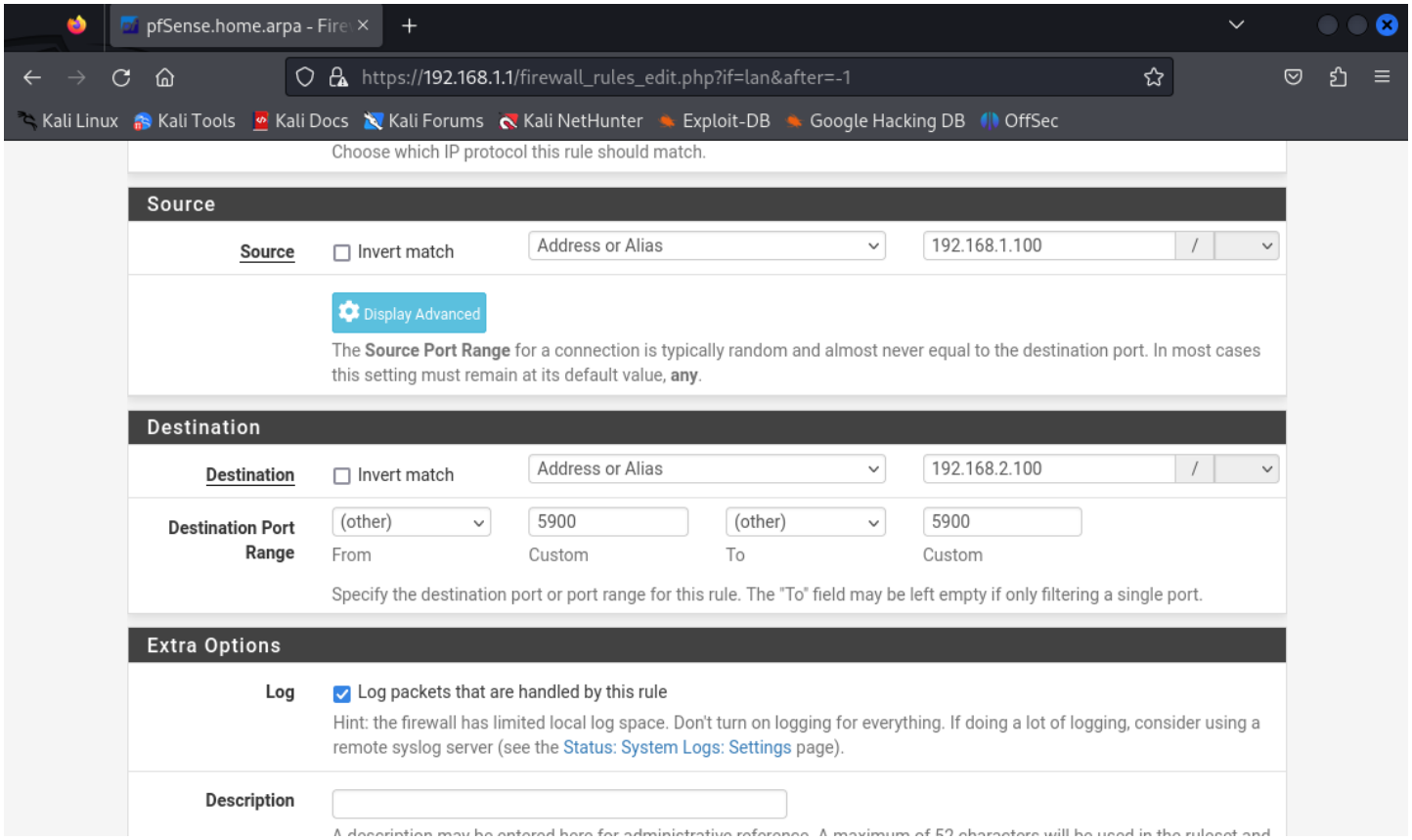
Sulla macchina metasploitable è attivo un servizio VNC utilizzato per l'accesso e il controllo remoto.

Il problema segnalato da nessus è la password troppo debole.

Per prima cosa cambiamo la password del servizio con il comando vncpasswd.

Come secondo passaggio limitiamo il traffico verso la porta in questione: 5900





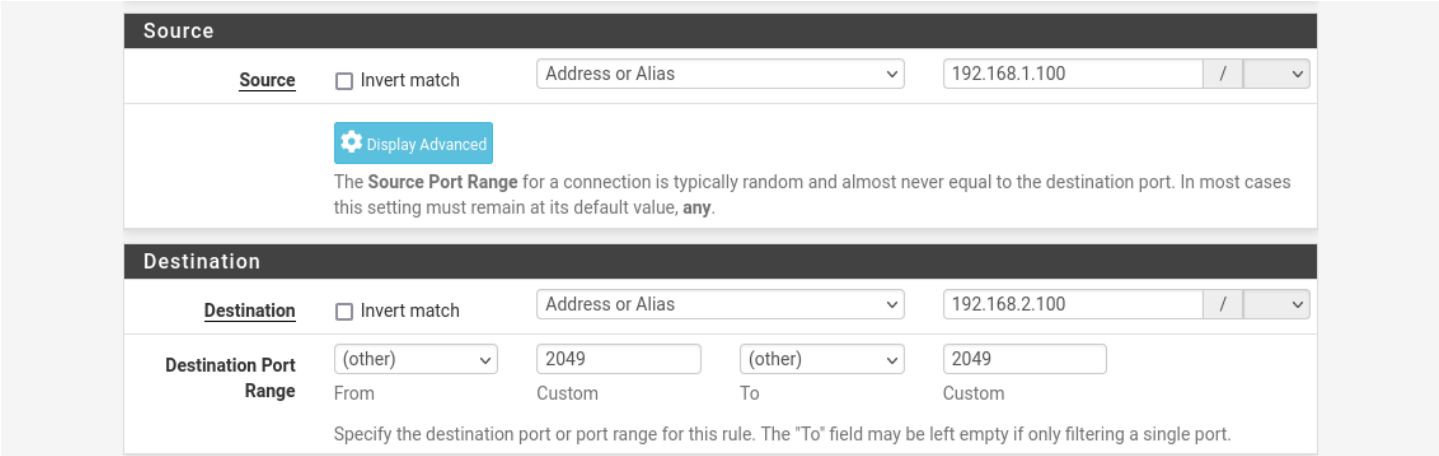
In questo modo Kali si potrà connettere a Metasploitable sulla porta 5900, ma la connessione sarà controllata dal Log.

11356 - NFS Exported Share Information Disclosure

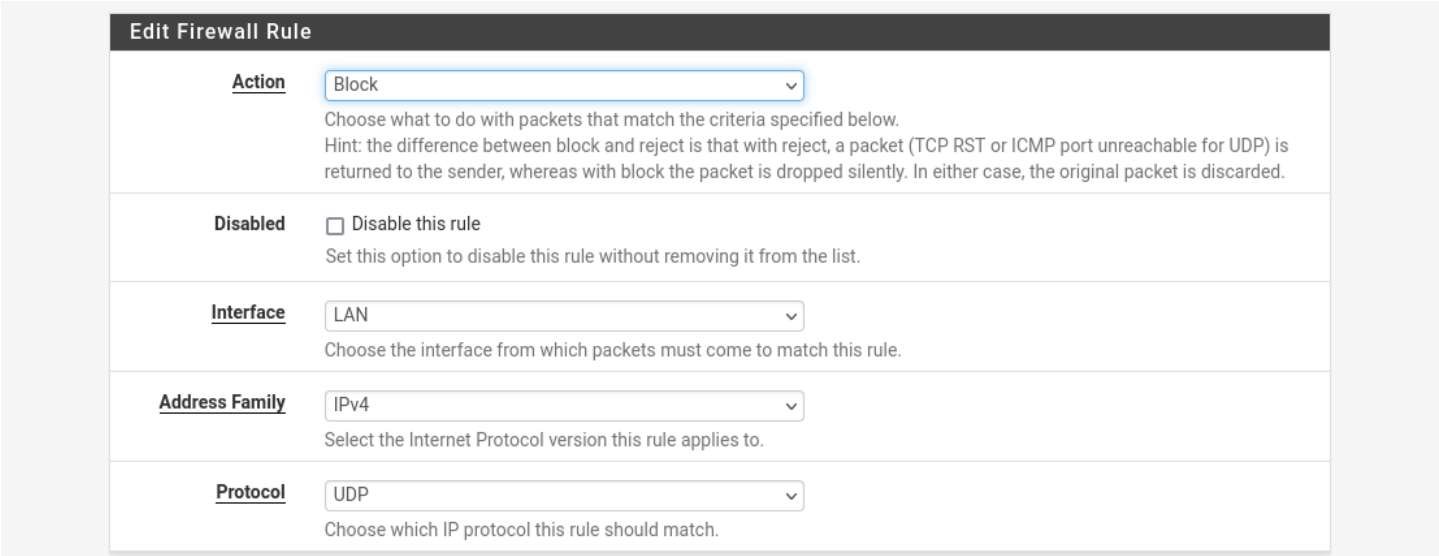
Riepilogo	**Descrizione**	**Soluzione**
È possibile accedere alle condivisioni NFS sull'host remoto.	Almeno una delle condivisioni NFS esportate dal server remoto potrebbe essere montata dall'host di scansione. L'attaccante potrebbe essere in grado di sfruttare questo per leggere (ed eventualmente scrivere) file sull'host remoto.	Configura NFS sull'host remoto in modo che solo gli host autorizzati possano montare le sue condivisioni remote.
Fattore di rischio critico	**CVSS v2.0 Base Score**: 10.0	**Plugin Output** udp/2049/rpc-nfs

Il report di nessus segnala che sulla porta 2049 è attivo un servizio NFS non configurato correttamente a cui chiunque può accedere.

Modifichiamo i file /etc/hosts.allow e /etc/hosts.deny assicurandoci di bloccare l'accesso a dispositivi non necessari. Dunque, togliamo l'accesso ALL e limitiamo le cartelle condivisibili.



Aggiungiamo su pfsense una regola di controllo che ci permette di bloccare il traffico sulla porta.



33850 - Unix Operating System Unsupported Version Detection

Riepilogo	**Descrizione**	**Soluzione**
Il sistema operativo in esecuzione sull'host remoto non è più supportato.	Secondo il numero di versione riportato, il sistema operativo Unix in esecuzione sull'host remoto è il n più supportato. La mancanza di supporto implica che il fornitore non rilascerà alcuna nuova patch di sicurezza per il prodotto. Di conseguenza, è probabile che contenga vulnerabilità di sicurezza.	Esegui l'upgrade a una versione del sistema operativo Unix attualmente supportata.
Fattore di rischio critico	**CVSS v3.0 Base Score**: 10.0	**Plugin Output** tcp/0

Per risolvere il problema della versione non supportata del sistema operativo su Metasploitable, bisogna aggiornare il sistema alla versione più recente che è compatibile e sicura. Rimuovere vecchi

software che potrebbero essere vulnerabili e controlla regolarmente il sistema per correggere eventuali altri problemi di sicurezza. Assicurarsi di mantenere sempre il sistema aggiornato e di monitorare attentamente qualsiasi attività strana.

32314 - Debian OpenSSH/OpenSSL Package Random Number Generator Weakness

Riepilogo	**Descrizione**	**Soluzione**
Le chiavi dell'host SSH remoto sono deboli.	La chiave host SSH remota è stata generata su un sistema Debian o Ubuntu che contiene un bug nel file generatore di numeri casuali della sua libreria OpenSSL. Il problema è dovuto al fatto che un packager Debian ha rimosso quasi tutte le fonti di entropia nella versione remota di OpenSSL. Un utente malintenzionato può facilmente ottenere la parte privata della chiave remota e utilizzarla per configurare la decifrazione del telecomando sessione o impostare un uomo al centro dell'attacco.	Considerare indovinabile tutto il materiale crittografico generato sull'host remoto. In particolare, tutti gli SSH. Il materiale delle chiavi SSL e OpenVPN deve essere rigenerato.
Fattore di rischio critico	**CVSS v2.0 Base Score**: 10.0	**Plugin Output** tcp/22/ssh

Per aggiornare i pacchetti OpenSSH e OpernSSL alla versione più recente, digitiamo i comandi:

Per OpenSSH: sudo apt-get update && sudo apt-get install openssh-server

Per OpenSSL: sudo apt-get update && sudo apt-get install openssl

In una macchina non pensata per essere vulnerabile, questi due comandi avrebbero permesso l'aggiornamento, mentre su metasploitable lo possiamo solo svolgere teoricamente.

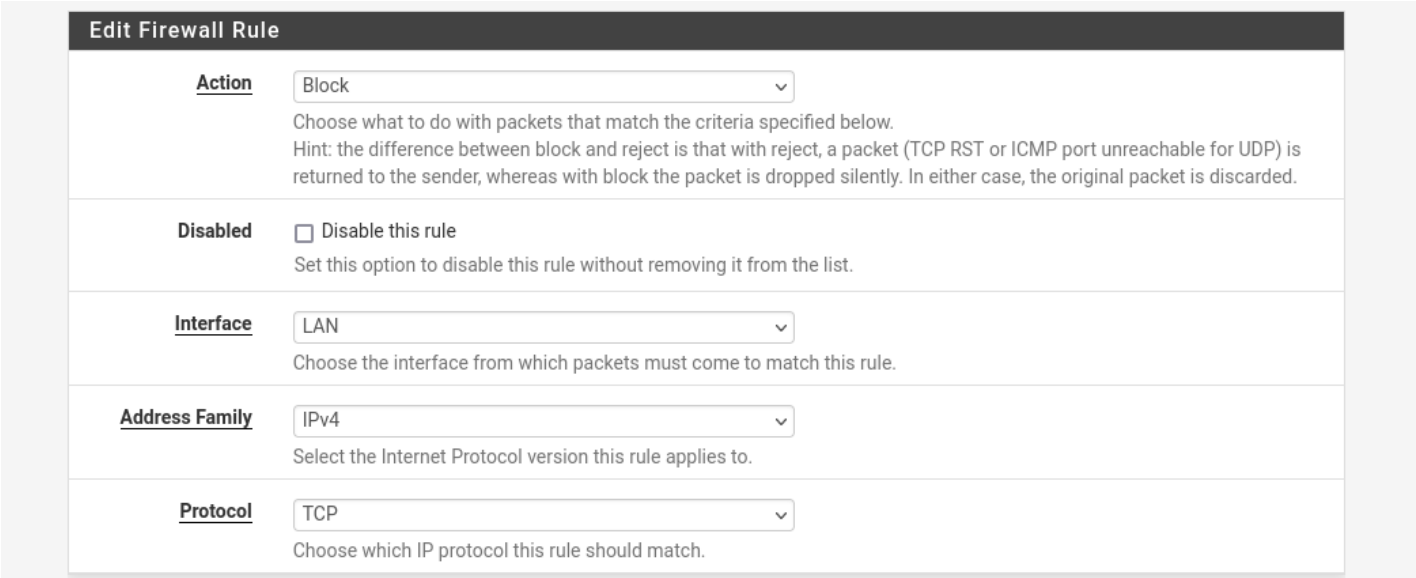
Verifichiamo di aver aggiornato correttamente con i comandi:

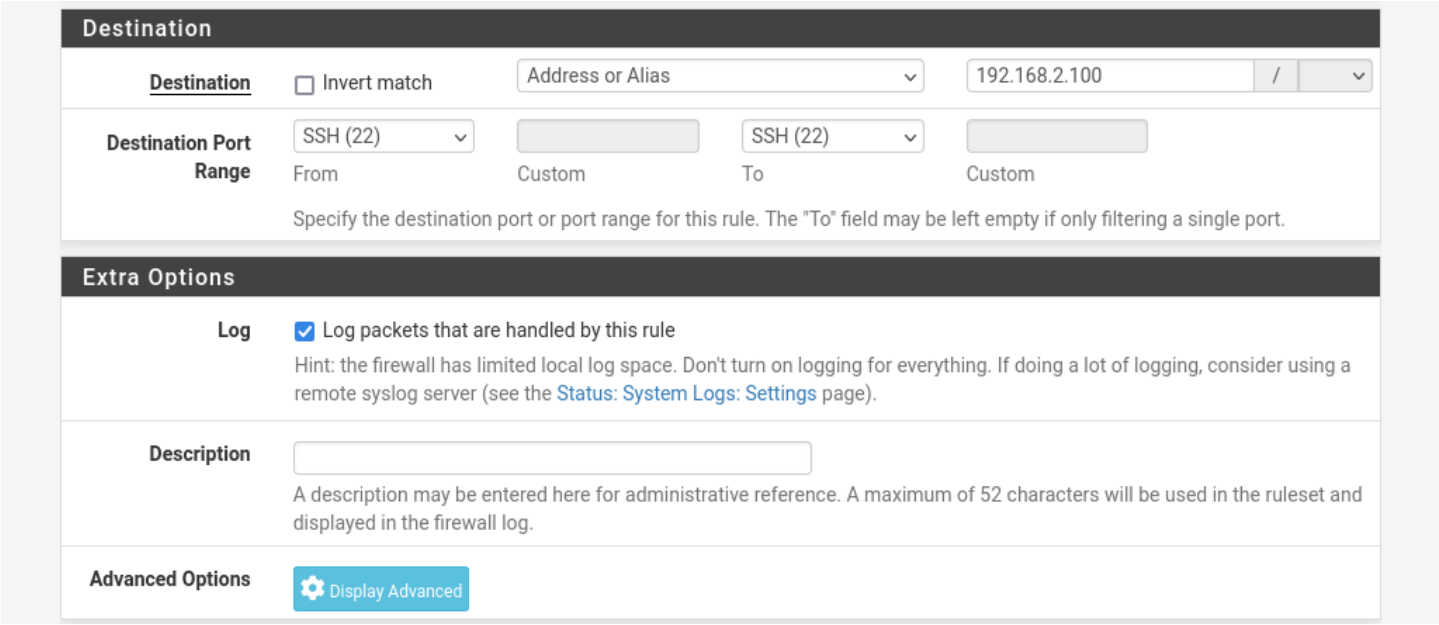
Per OpenSSH: ssh -V e per OpenSSL: openssl version

Controlliamo siano presenti le patch di sicurezza con i comandi:

Per OpenSSH: dpkg -l | grep openssh-server e per OpenSSL: dpkg -l | grep openssl

Aggiungiamo una regola firewall per bloccare la connessione da kali:





Infine bloccando con il firewall di kali le porte esaminate il risultato sarà simile a questo: