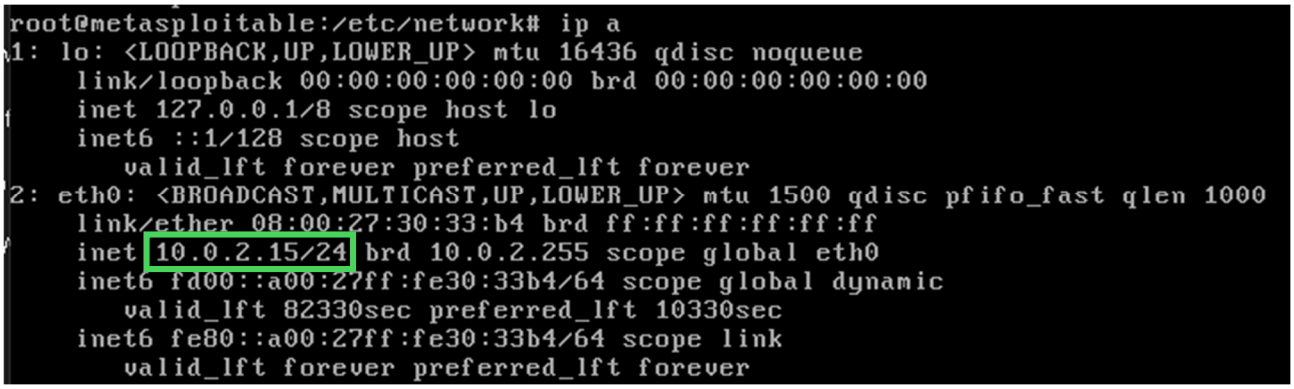
La consegna chiedeva di configurare il firewall in maniera tale che venisse bloccato l'accesso alla DVWA su metasploitable da parte della machina con Kali Linux facente parte di un'altra rete.

Configurazione degli IP

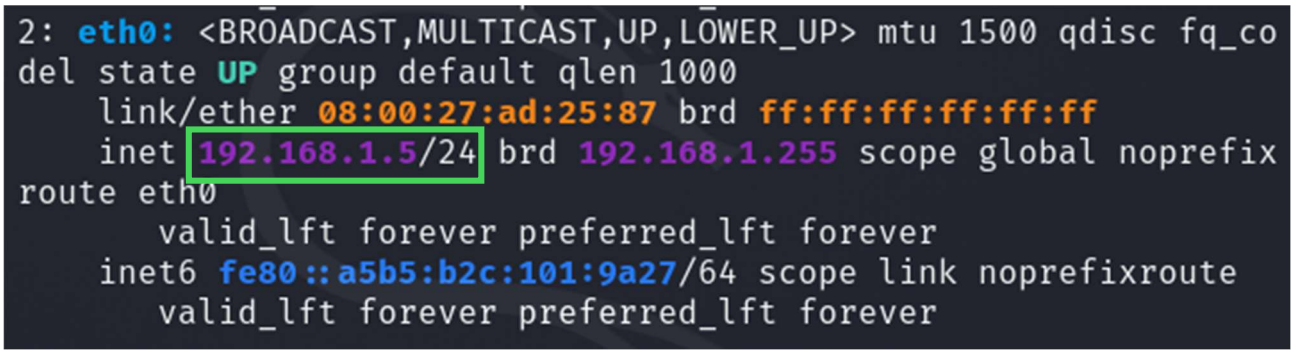
Per prima cosa ho impostato i vari indirizzi IP sulle macchine mettendo 192.168.1.2 a metasploitable e 192.168.2.5 a Kali Linux.

L'indirizzo IP di Kali Linux lo cambierò dopo aver fatto tutte le configurazioni perché inizialmente mi servirà per la configurazione del firewall e della DVWA.

Visualizzo l'IP della metasploitable:

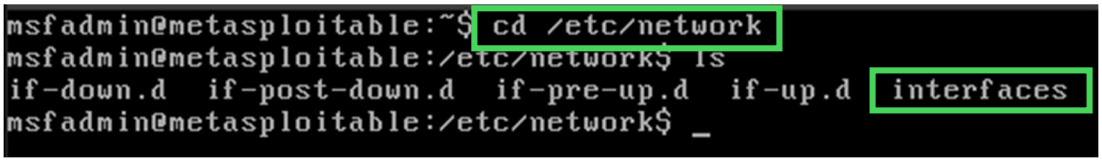


E l'indirizzo IP di Kali:

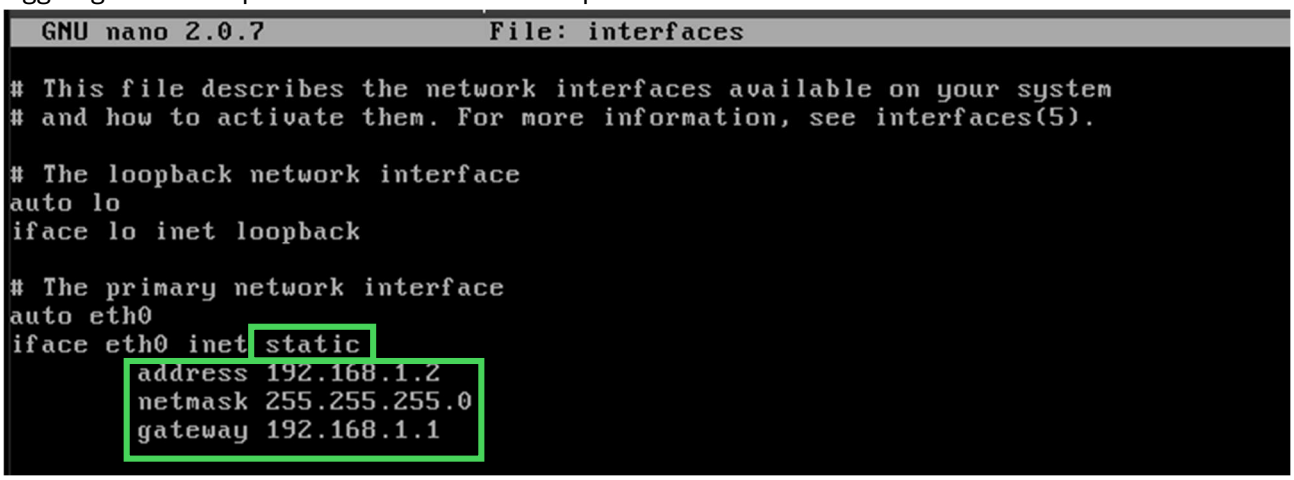


Adeso modifico l'indirizzo IP di metasploitable così da avere tutto sotto la stessa rete.

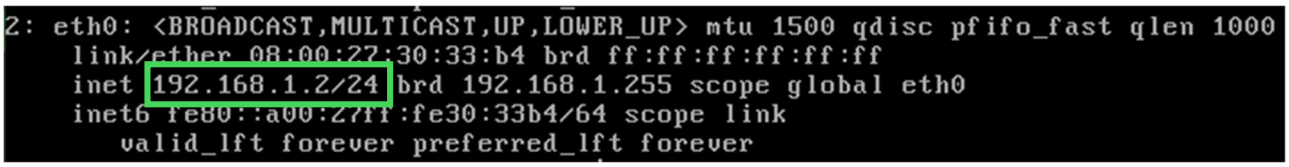
Per poterlo fare devo andare a modificar, usando "nano" con diritti da super user, il file "interface" presente al percorso "/etc/network/":



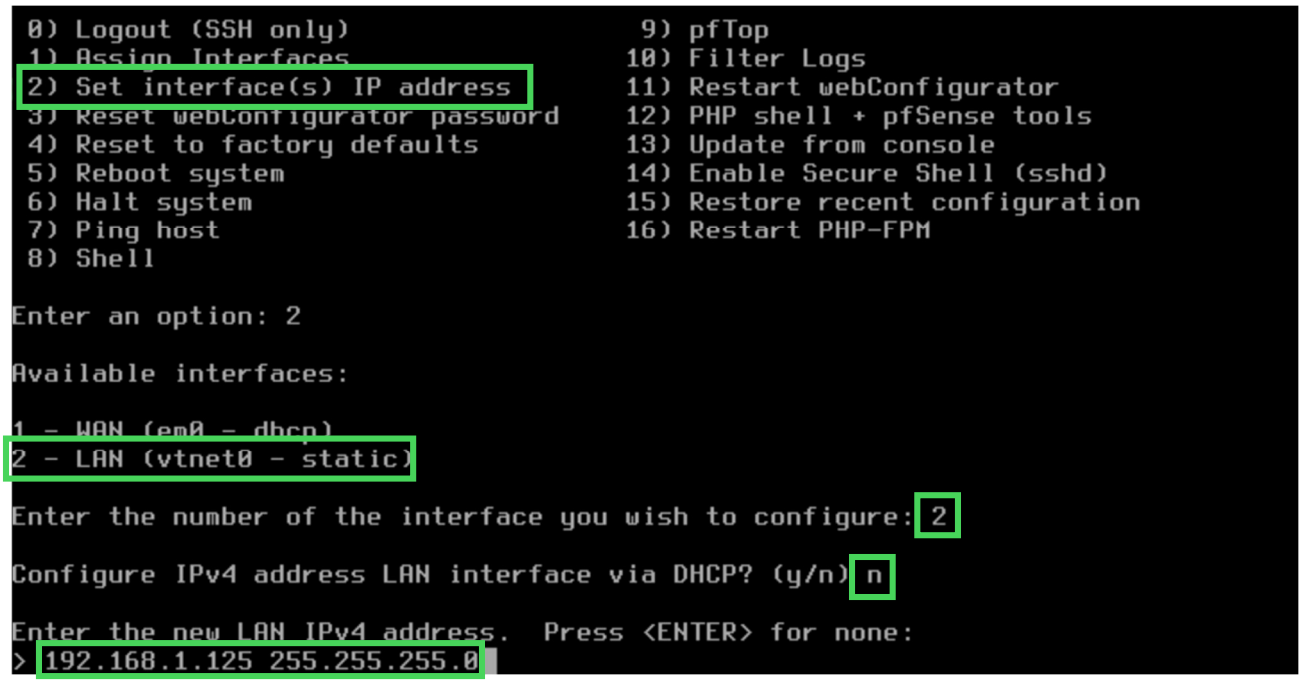
Aggiungendo i dati per l'IP e modificando "dhcp" in "static":



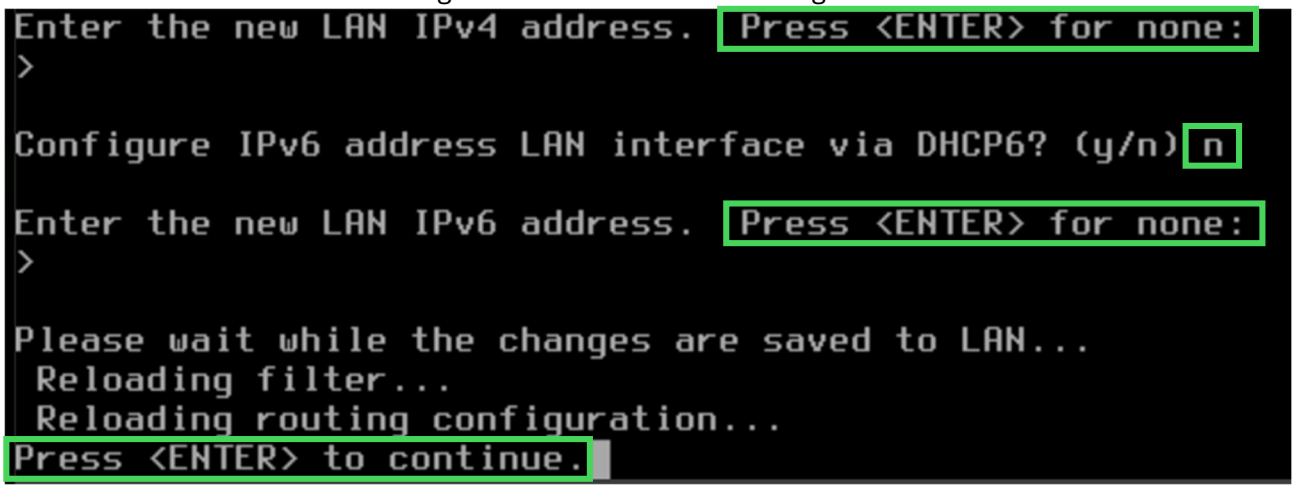
Adesso visualizza l'avvenuto cambio di IP:



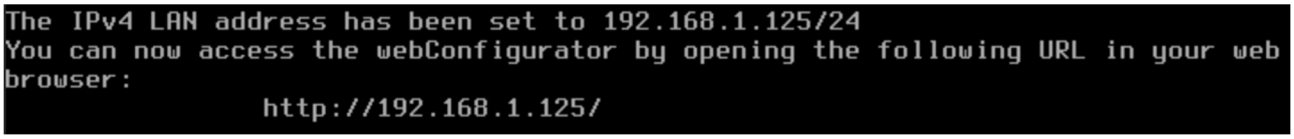
Ora configuro l'IP del firewall dando il comando numero 2 presente nel menu di pfsense che dice "Set interface(s) IP address", successivamente dando il comando 2 che dice di configurare l'interfaccia di rete di tipo LAN e negando la richiesta di configurare via DHCP, scrivo l'IP "192.168.1.125"e la Subnet mask "255.255.255.0:



E successivamente vado avanti negando la sua richiesta di configurare un IPv6:

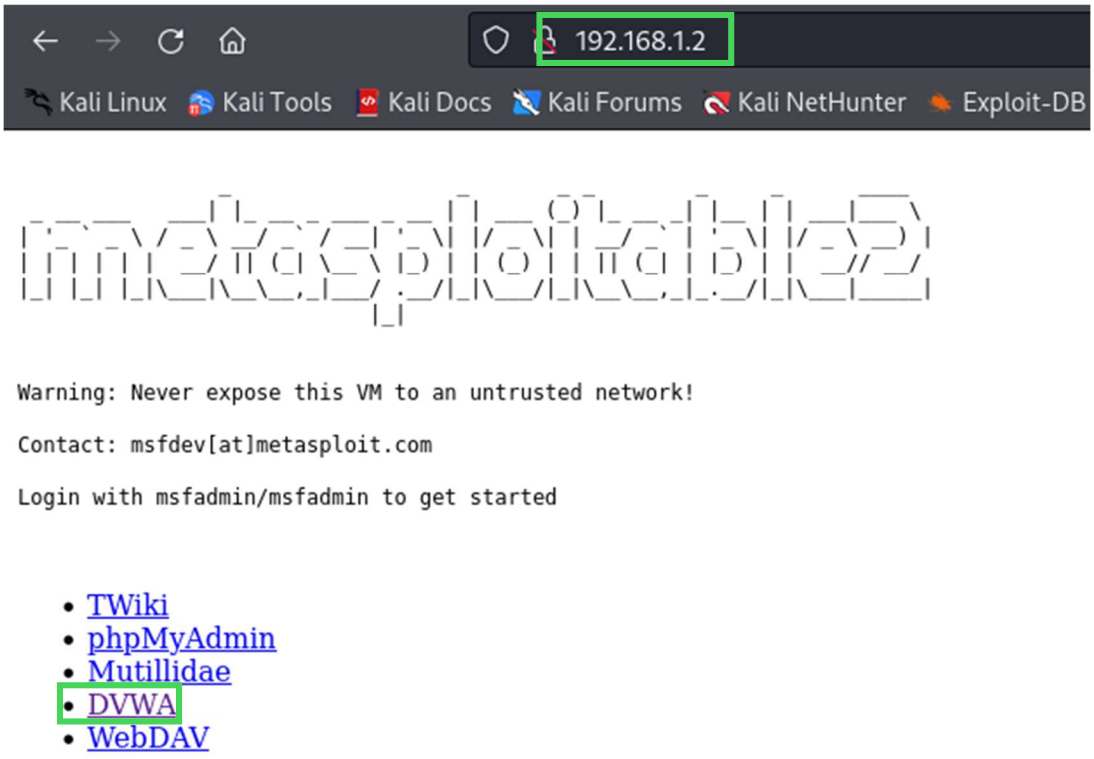


Configurazione avvenuta con successo:

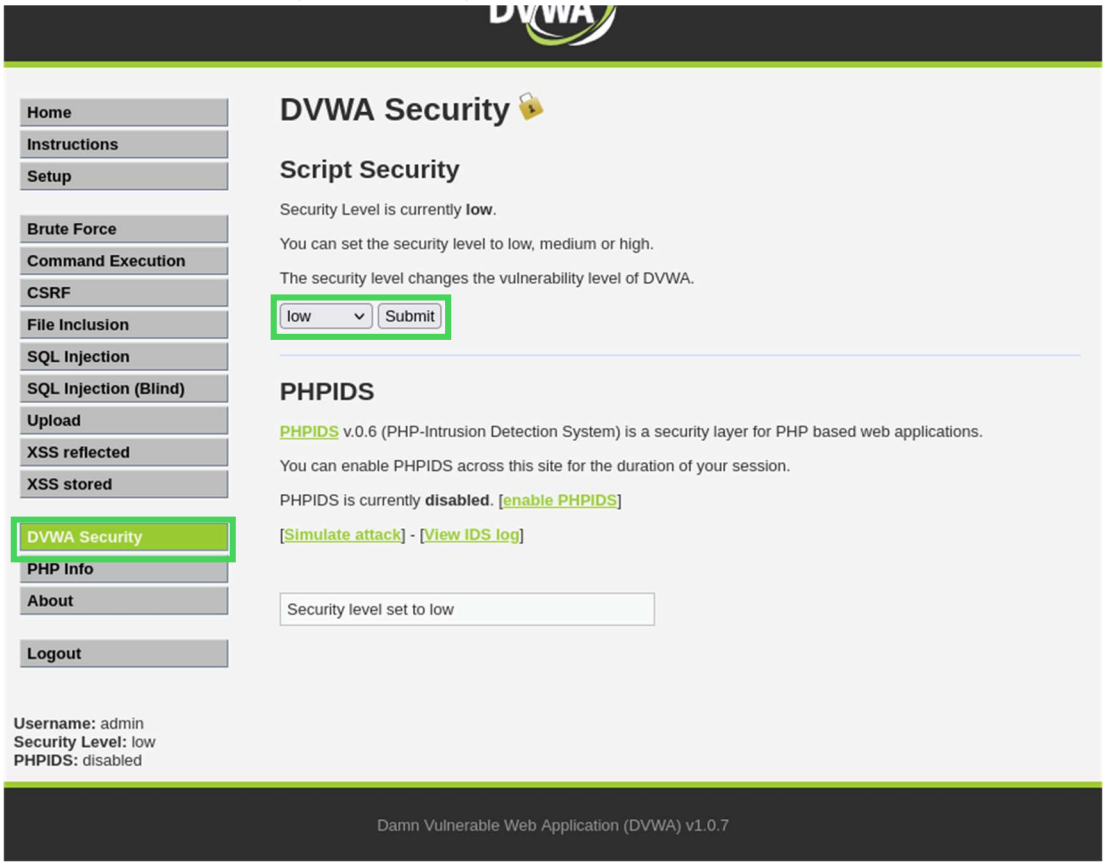


Configurazione DVWA

Adesso, avendo momentaneamente Kali nella stessa rete, cerco dal browser l'IP di metasploitable che darà a schermo la pagina di configurazione dové presente il collegamento per accedere a DVWA già installata su metasploitable:

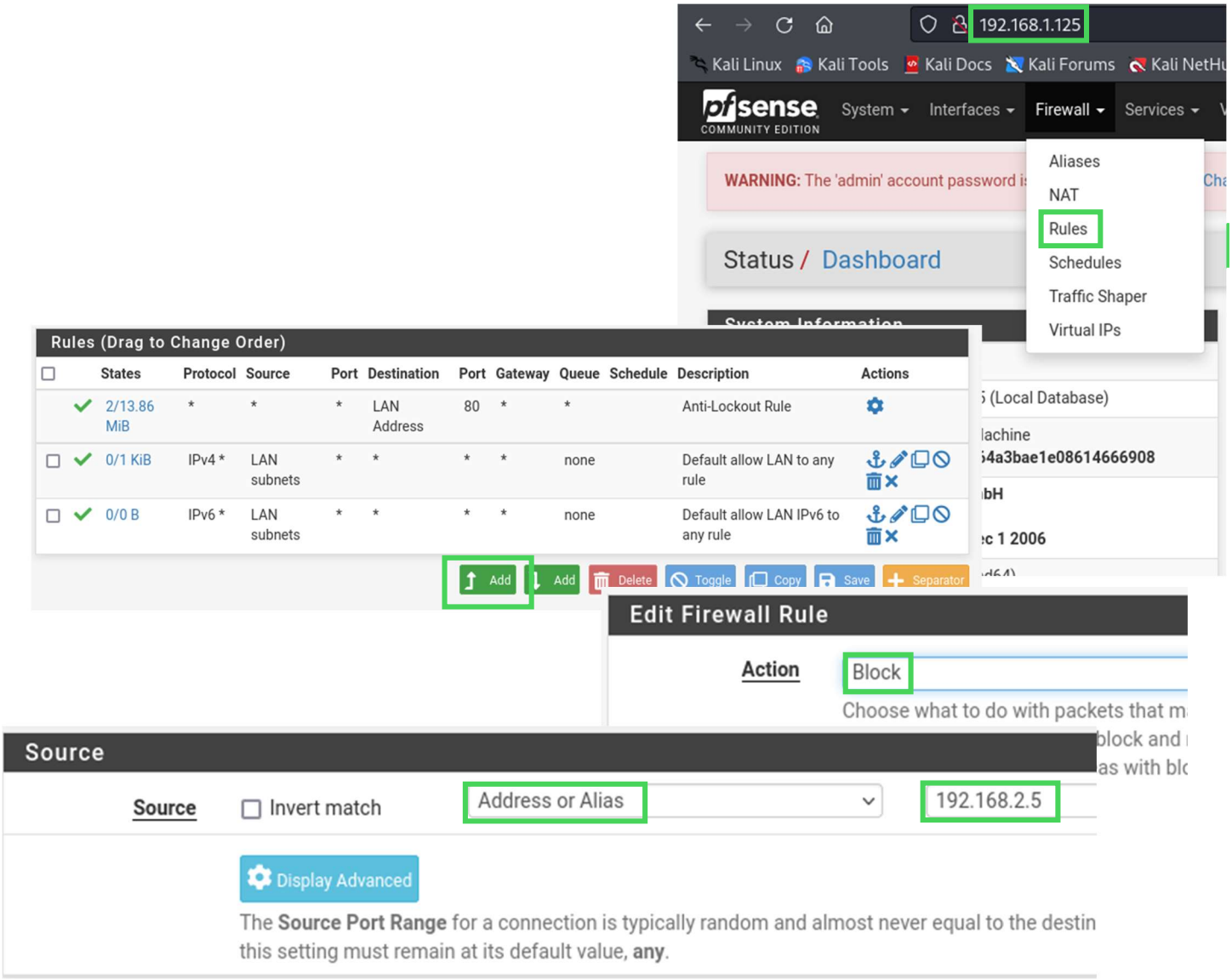


Facendo l'accesso, inserendo "admin" e "password" nelle credenziali, avremo accesso alla pagina di configurazione di DVWA nella quale vado impostare un basso livello di sicurezza:



Configurazione firewall pfsense

Adesso accedo alla pagina di configurazione del firewall tramite Kali.
Cerco da browser l'IP "192.168.1.125" di pfsense e successivamente farò l'accesso usando "admin" e "pfsense" come credenziali.
Sulla schermata di configurazione, vado ad impostare delle regole al firewall, aggiungendone una in cima alla lista, così che verrà eseguita per prima, che blocca i pacchetti provenienti dall'IP "192.168.2.5" che sarà il successivo indirizzo IP di Kali:

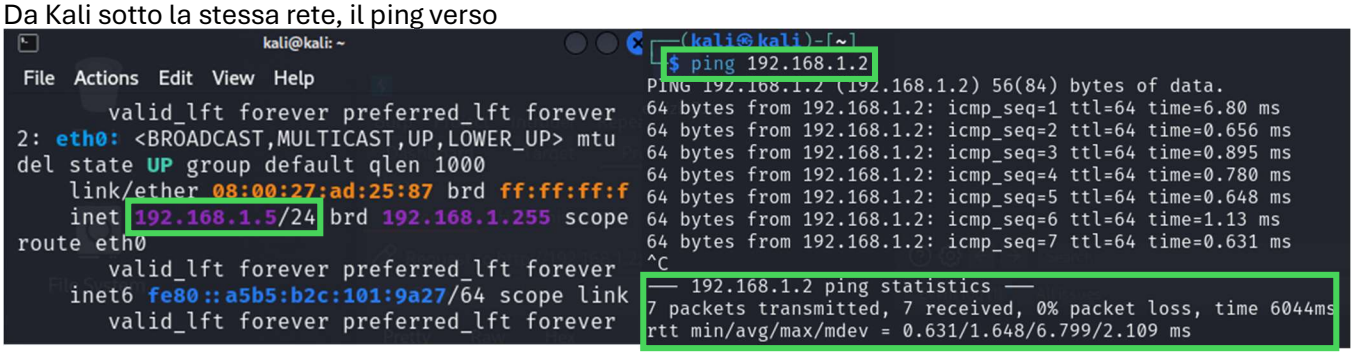


Per completare la configurazione salvo e applico i cambiamenti.

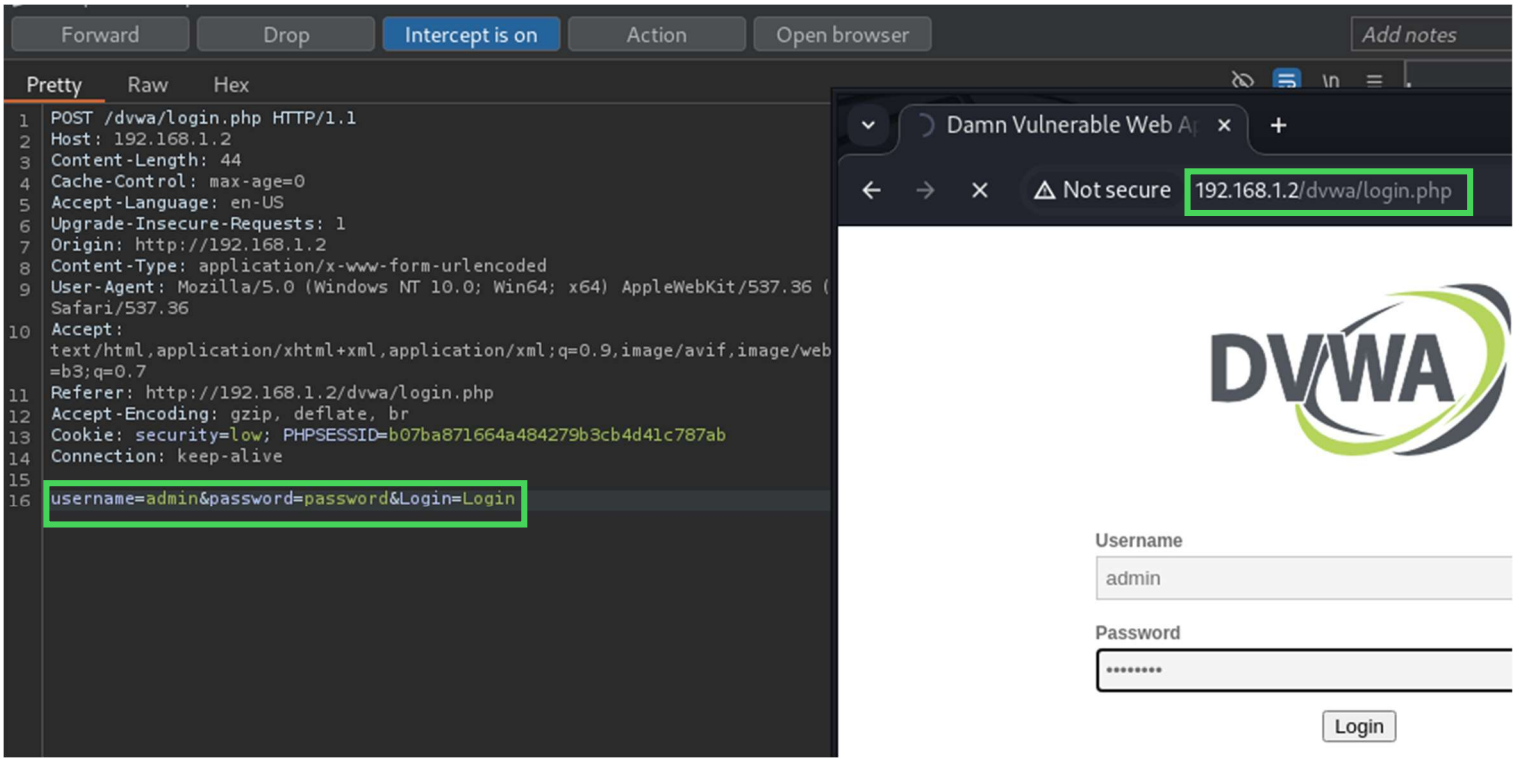
Test

Adesso effettuo dei test, prima provo a scansionare sia con un ping sia con BurpSuite DVWA da Kali sulla stessa rete e successivamente ripeterò l'operazione cambiando l'IP di Kali e impostandolo in una rete diversa.

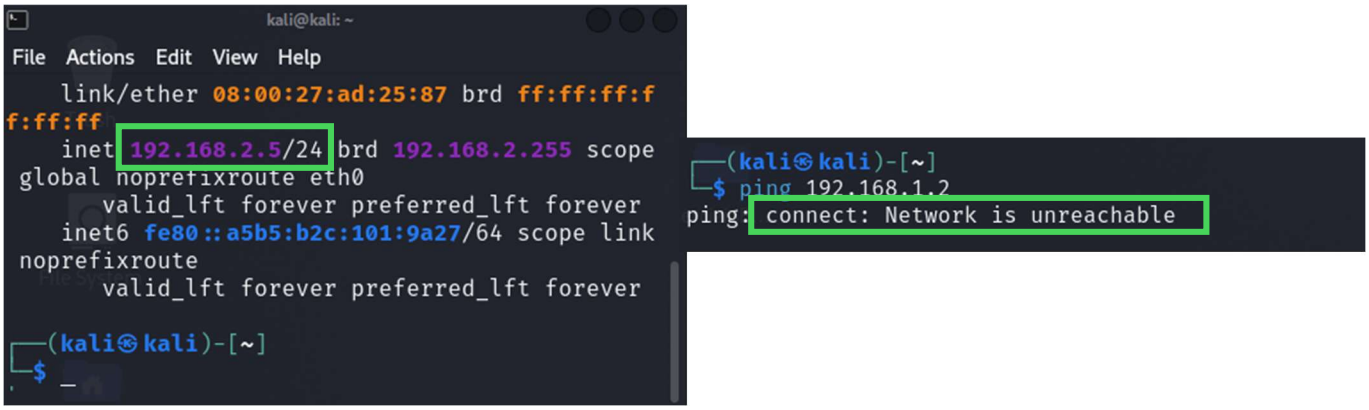
Da Kali sotto la stessa rete, il ping verso



Successivamente, con BurpSuite, le credenziali vengono intercettate senza problemi:



Adesso, modificando l'IP di Kali, possiamo notare che il ping non riesce a raggiungere metasploitable:



E usando il browser di BurpSuite, la pagina non viene raggiunta: