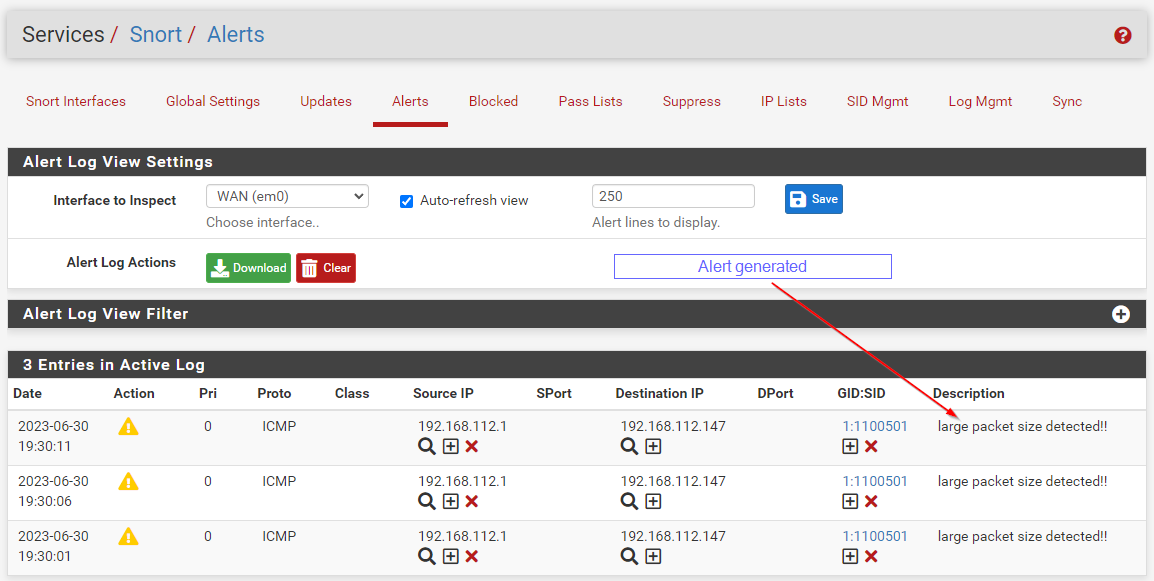
Assignment 4:

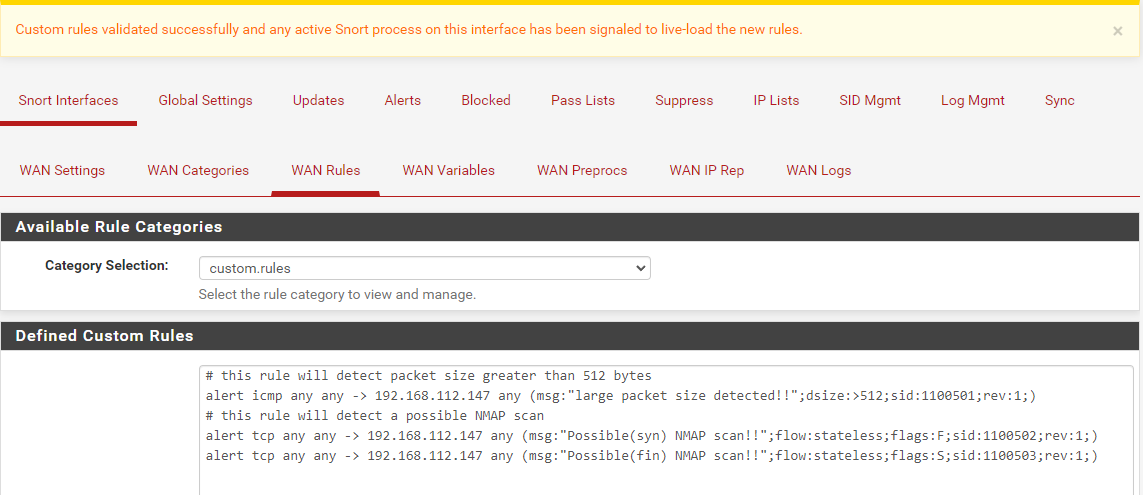
-> detect ping for packet greater than 512 bytes

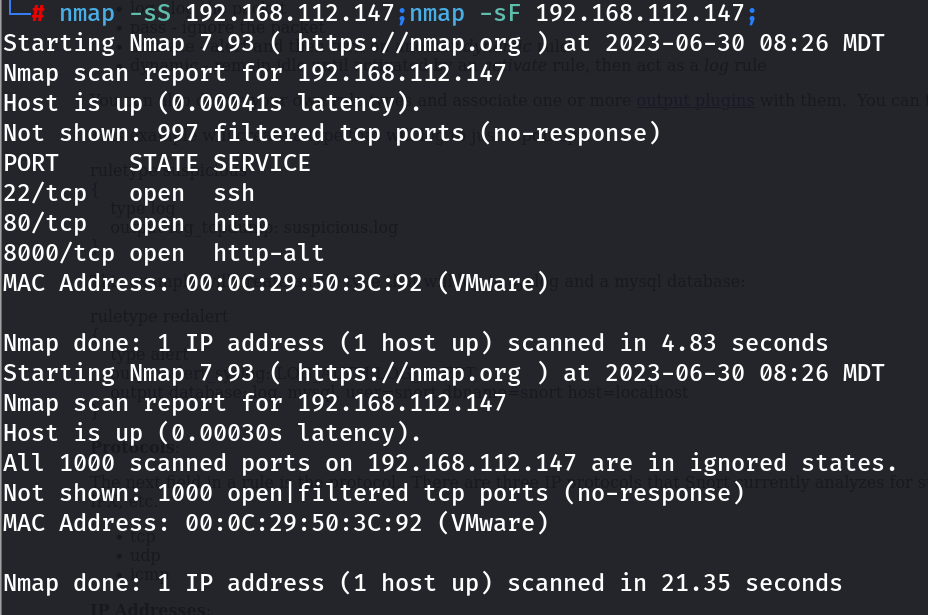


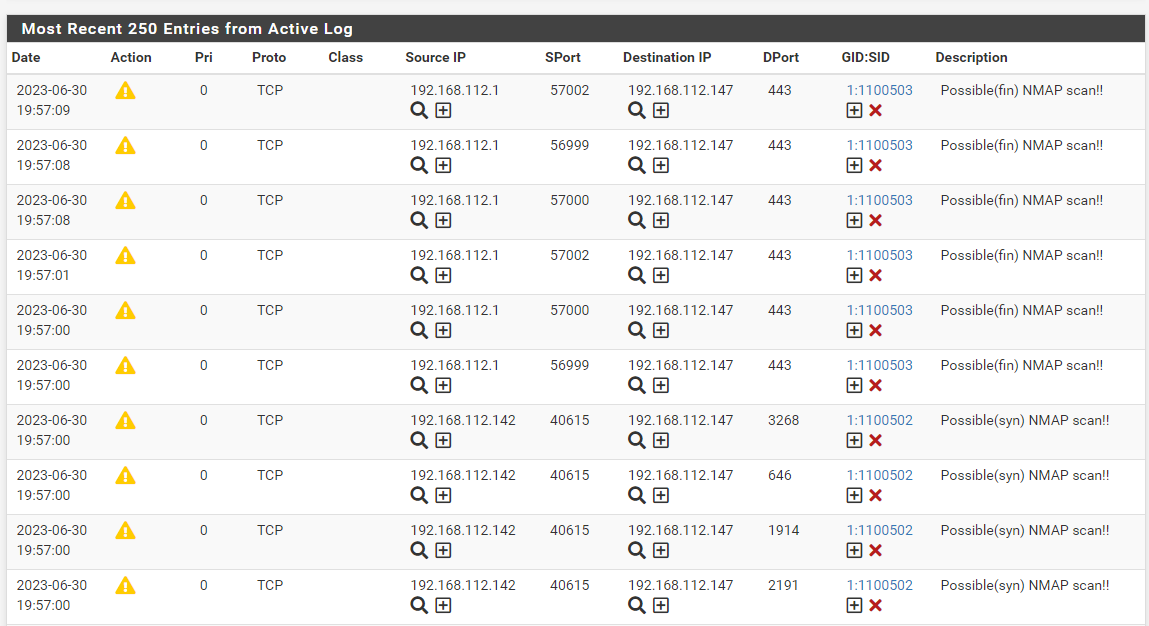




-> detect nmap scan -sF -sS

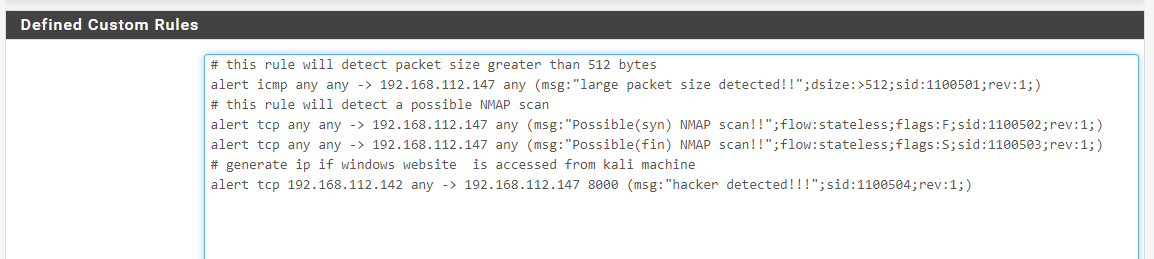


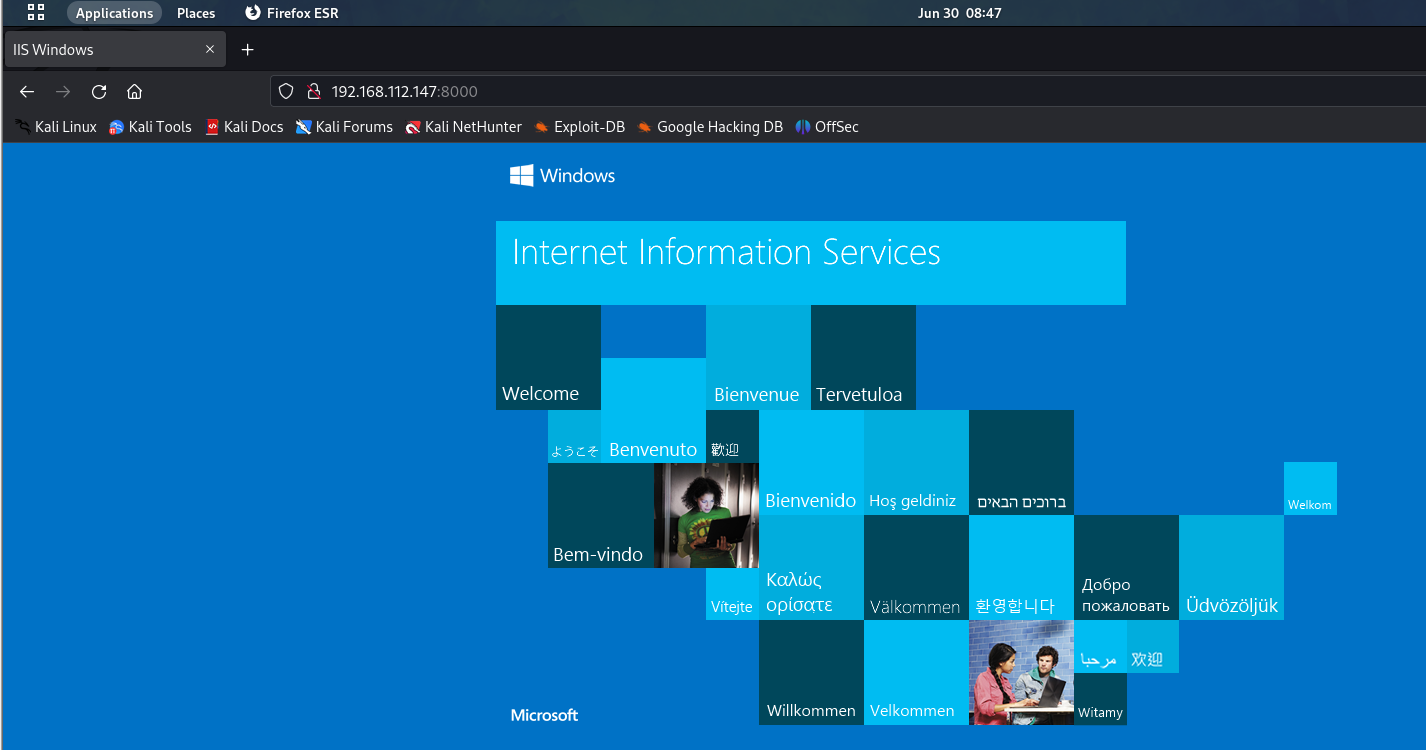


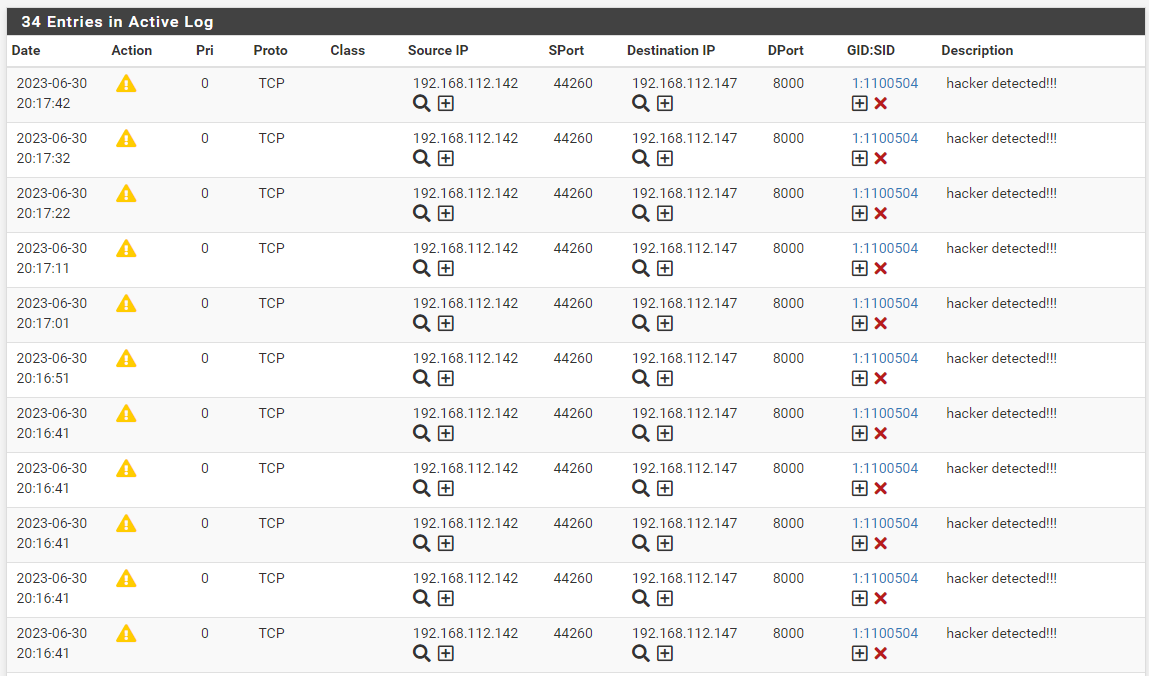


-> detect if windows website is accessed from kali linux generate alert

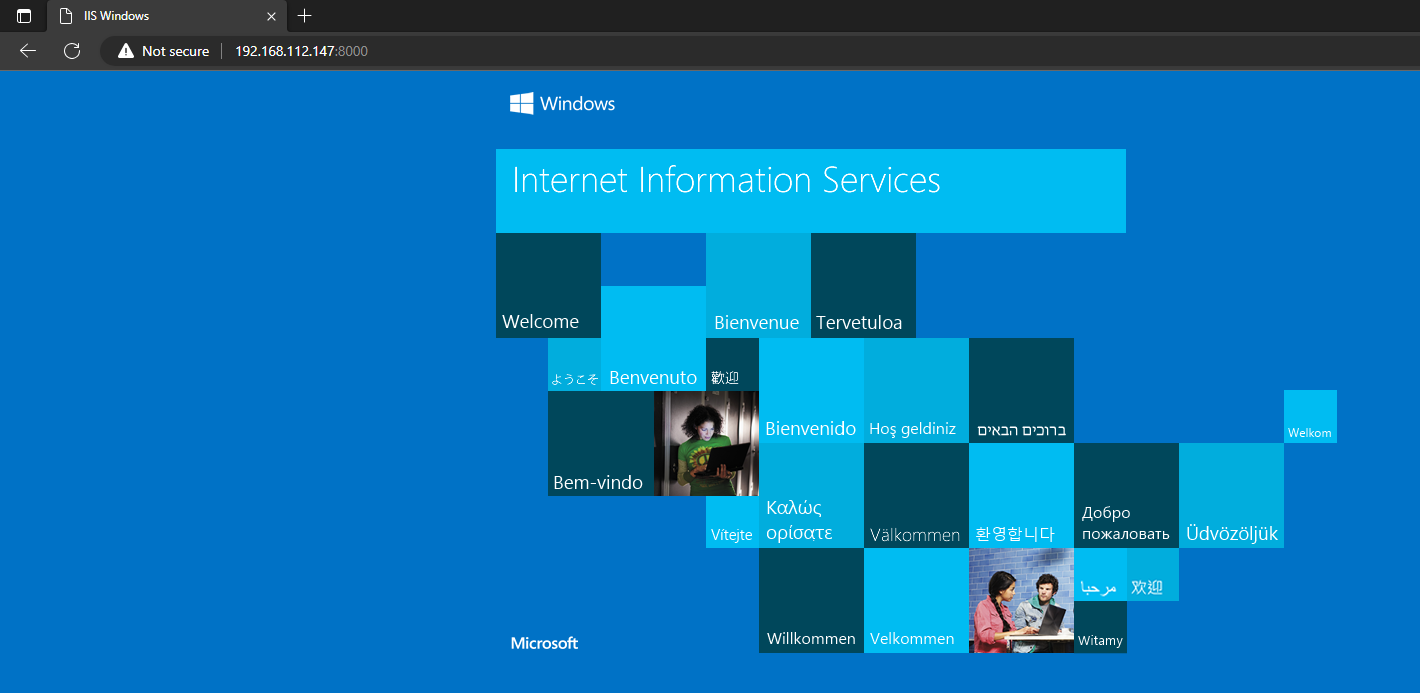
& if it is accessed from base machine no alert

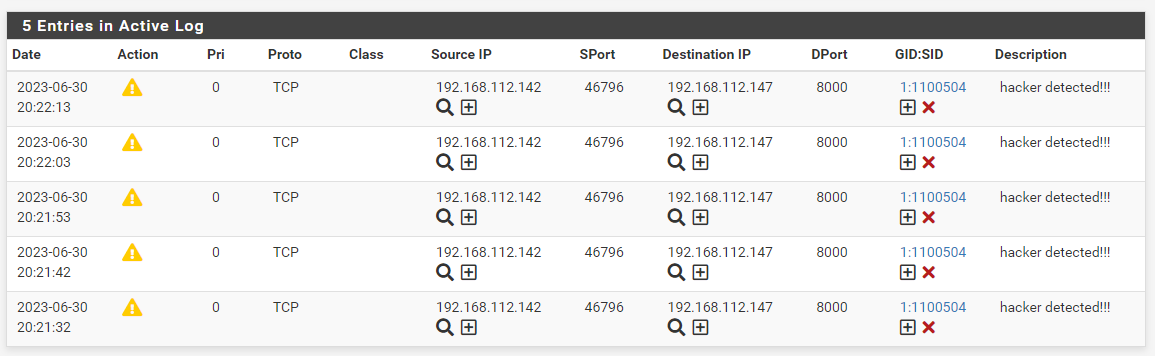


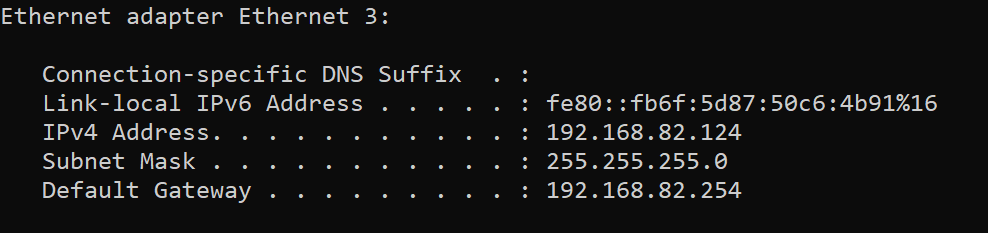




# accessed from base windows machine

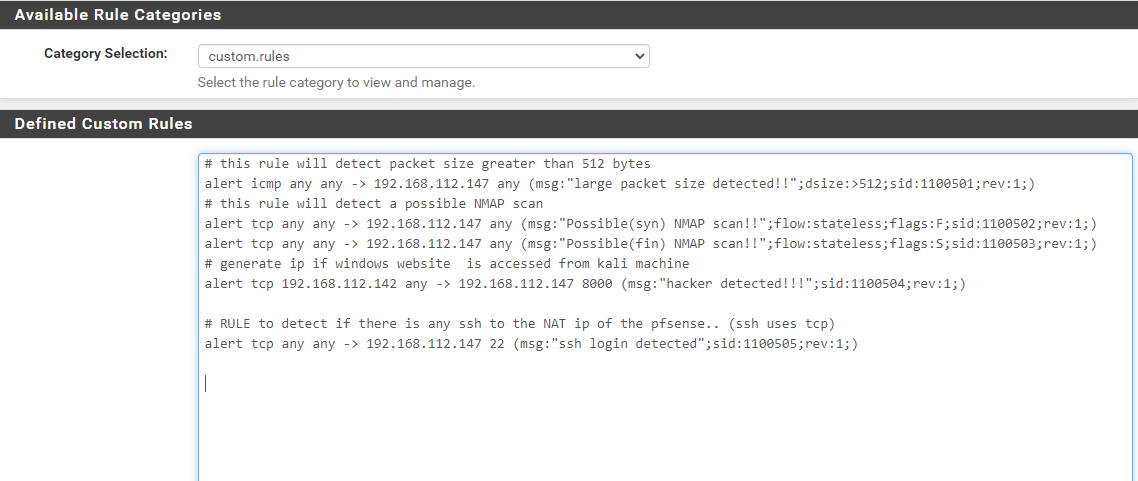


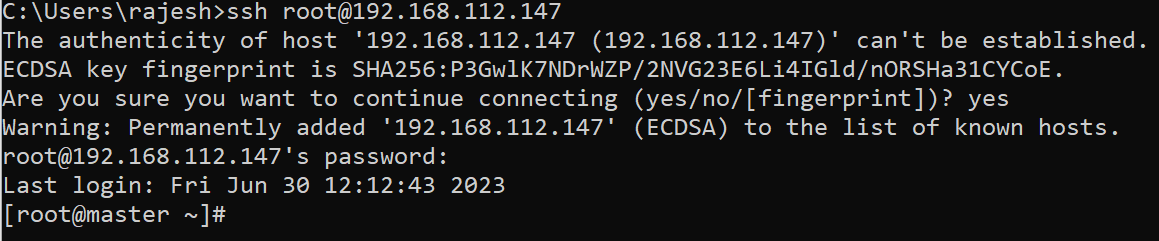


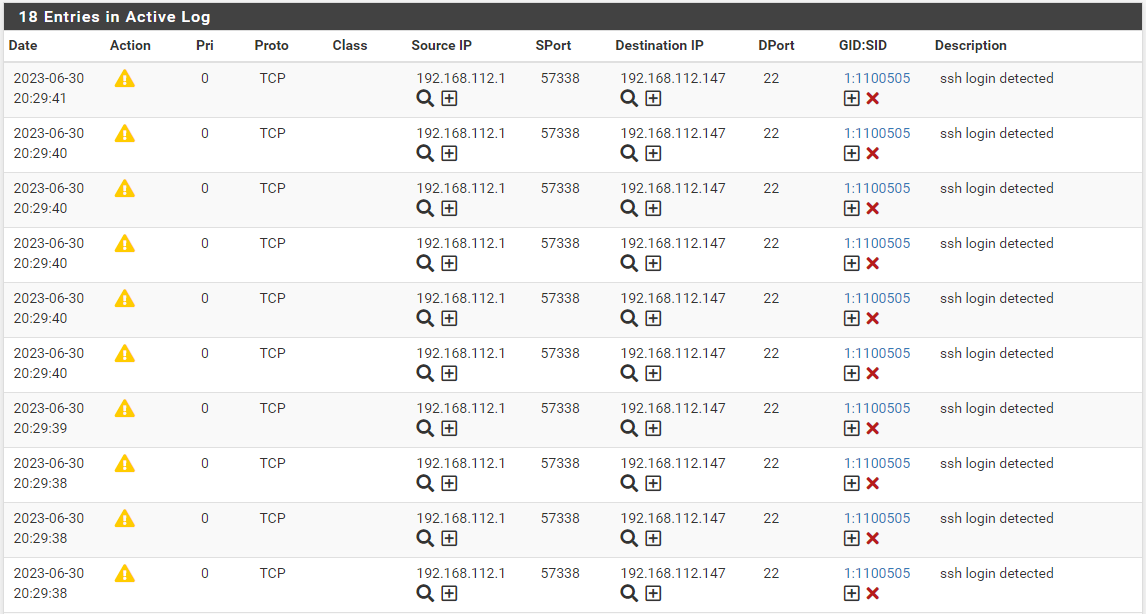


no base machine ip(192.168.82.124) found in logs, which means no log is generated for base machine access for windows website

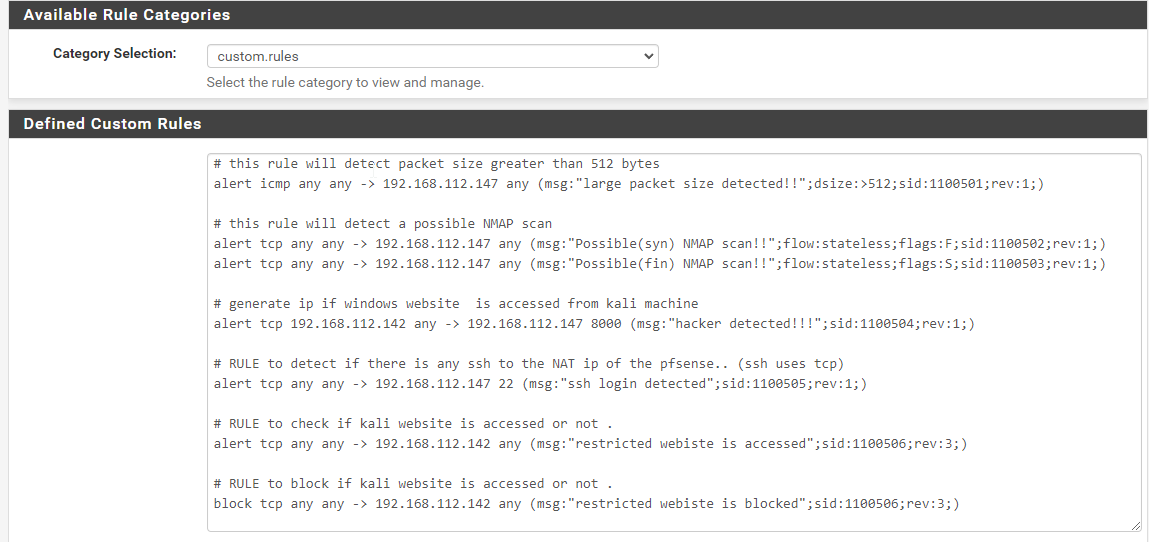
-> detect if ssh to nat ip is done

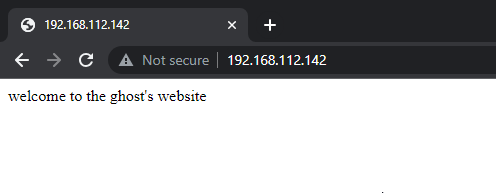


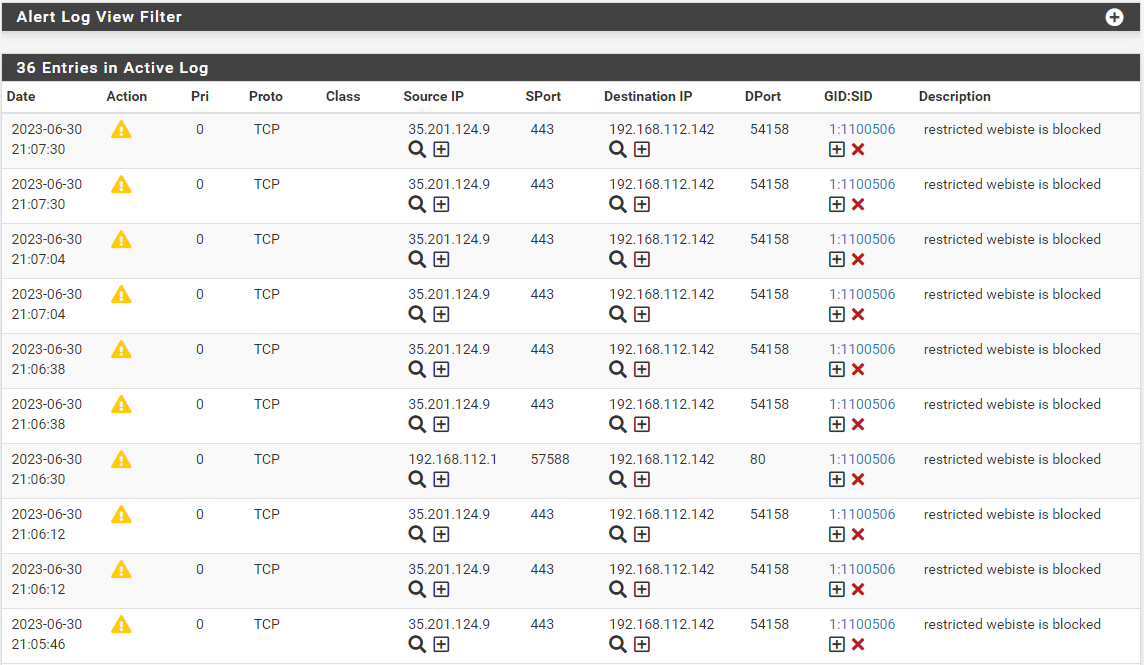




-> create a website on kali linux write a rule to detect if website is accessed (try drop action to check if access is blocked)







-> create a folder web2

-> create a index.html inside web2