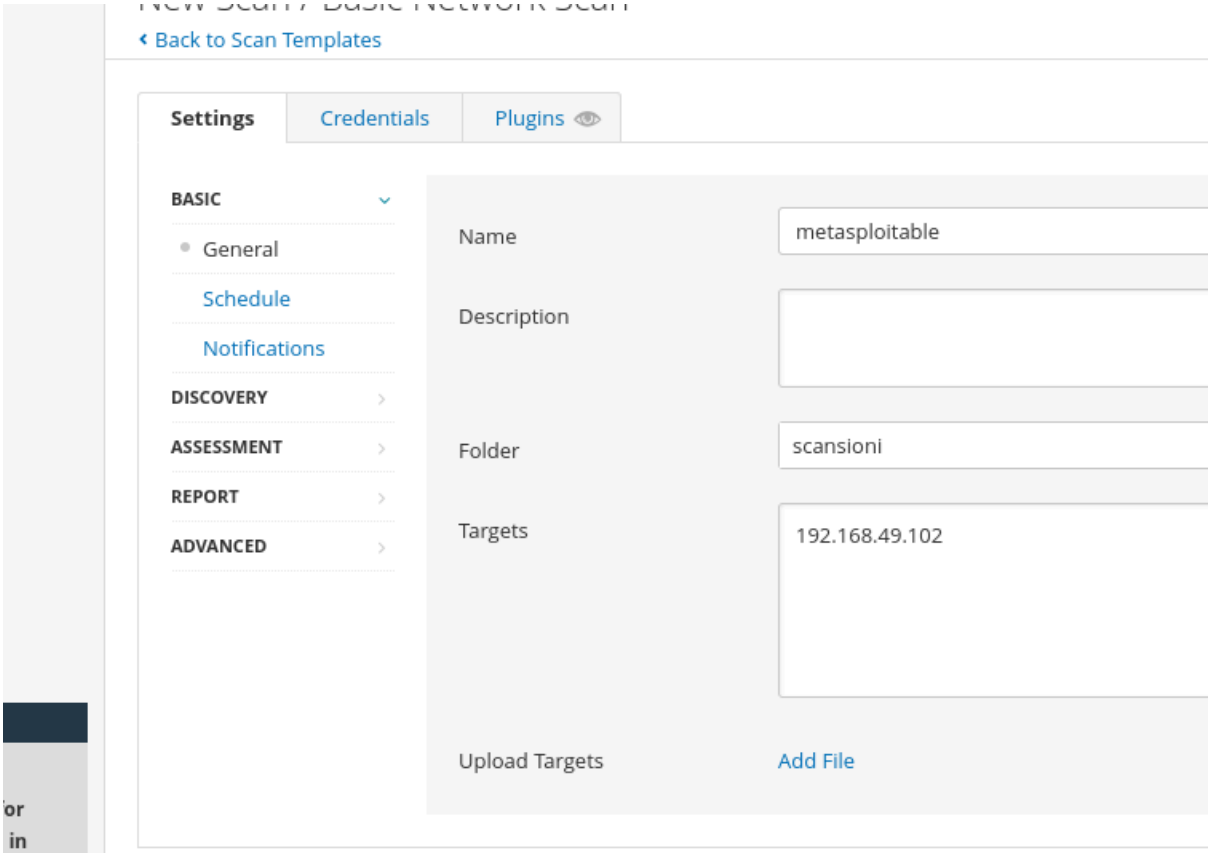
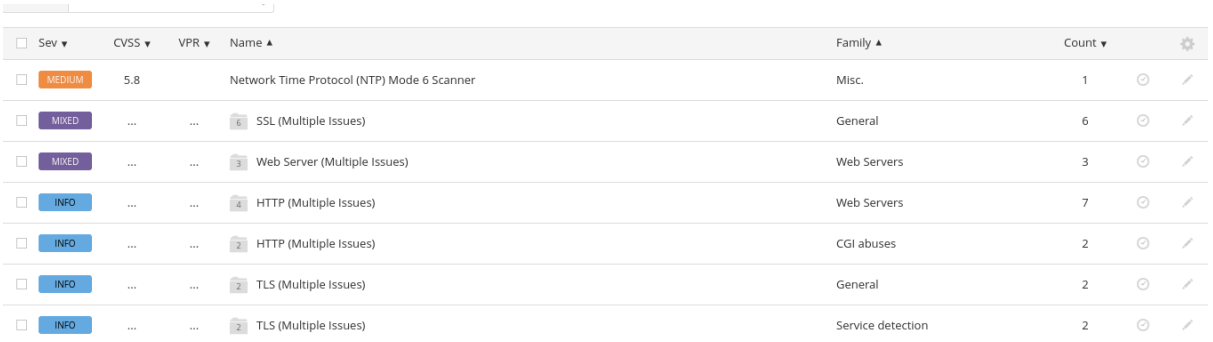
L’esercizio di oggi consisteva nel usare nessus per fare una scansione verso metasploitable nella foto qui sotto è  la pagina iniziale di nessus per fare una scansione dove si inserisce il nome(va bene qualsiasi nome) e il target (può essere più d'uno contemporaneamente)




Dopo aver messo il nome e il target si imposta le porte tramite discovery e le vulnerabilità tramite assessment, dopo aver lanciato la scansione se procede tutto bene apparirà lo schermo come la foto sotto indicando le vulnerabilità trovato e quanto sono serie in questo caso la vulnerabilità è medium e il modo per risolvere questa è limitare la rete



| Sev | CVSS | VPR | Name | Family | Count |
|---|---|---|---|---|---|
| MEDIUM | 5.8 | | Network Time Protocol (NTP) Mode 6 Scanner | Misc. | 1 |
| MIXED | ... | ... | SSL (Multiple Issues) | General | 6 |
| MIXED | ... | ... | Web Server (Multiple Issues) | Web Servers | 3 |
| INFO | ... | ... | HTTP (Multiple Issues) | Web Servers | 7 |
| INFO | ... | ... | HTTP (Multiple Issues) | CGI abuses | 2 |
| INFO | ... | ... | TLS (Multiple Issues) | General | 2 |
| INFO | ... | ... | TLS (Multiple Issues) | Service detection | 2 |