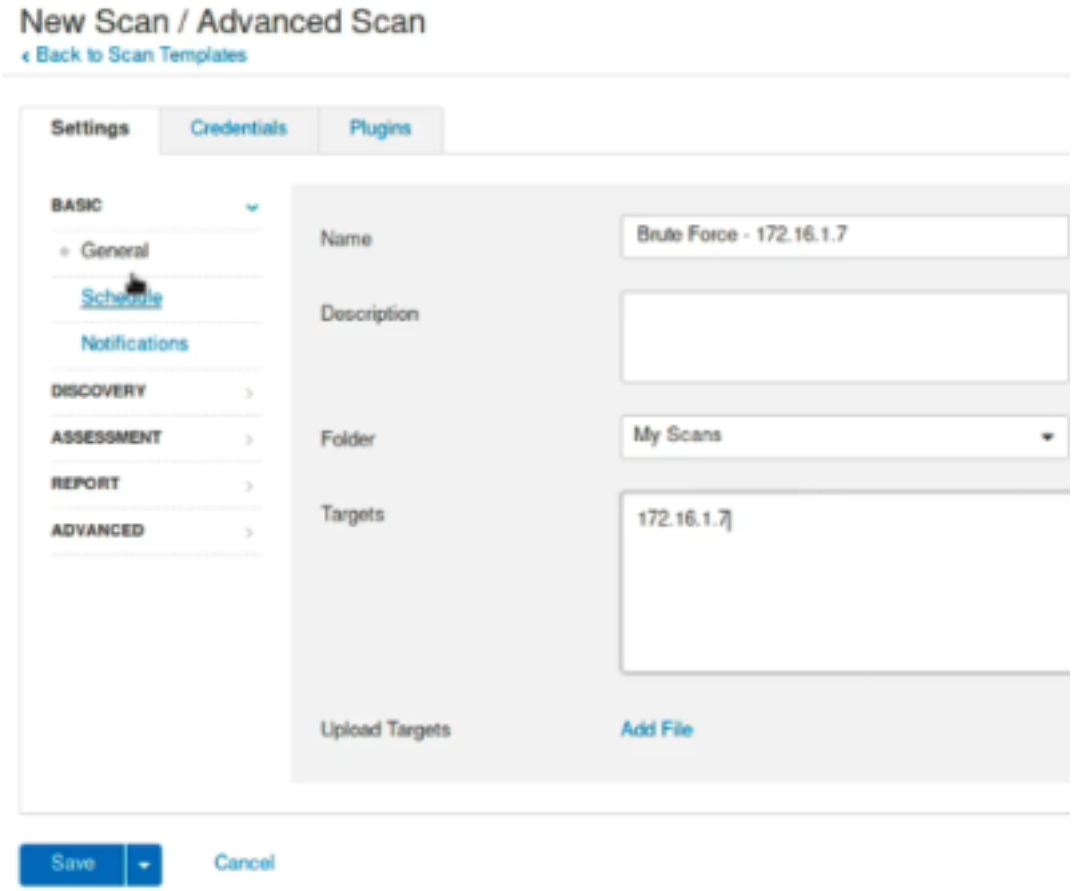
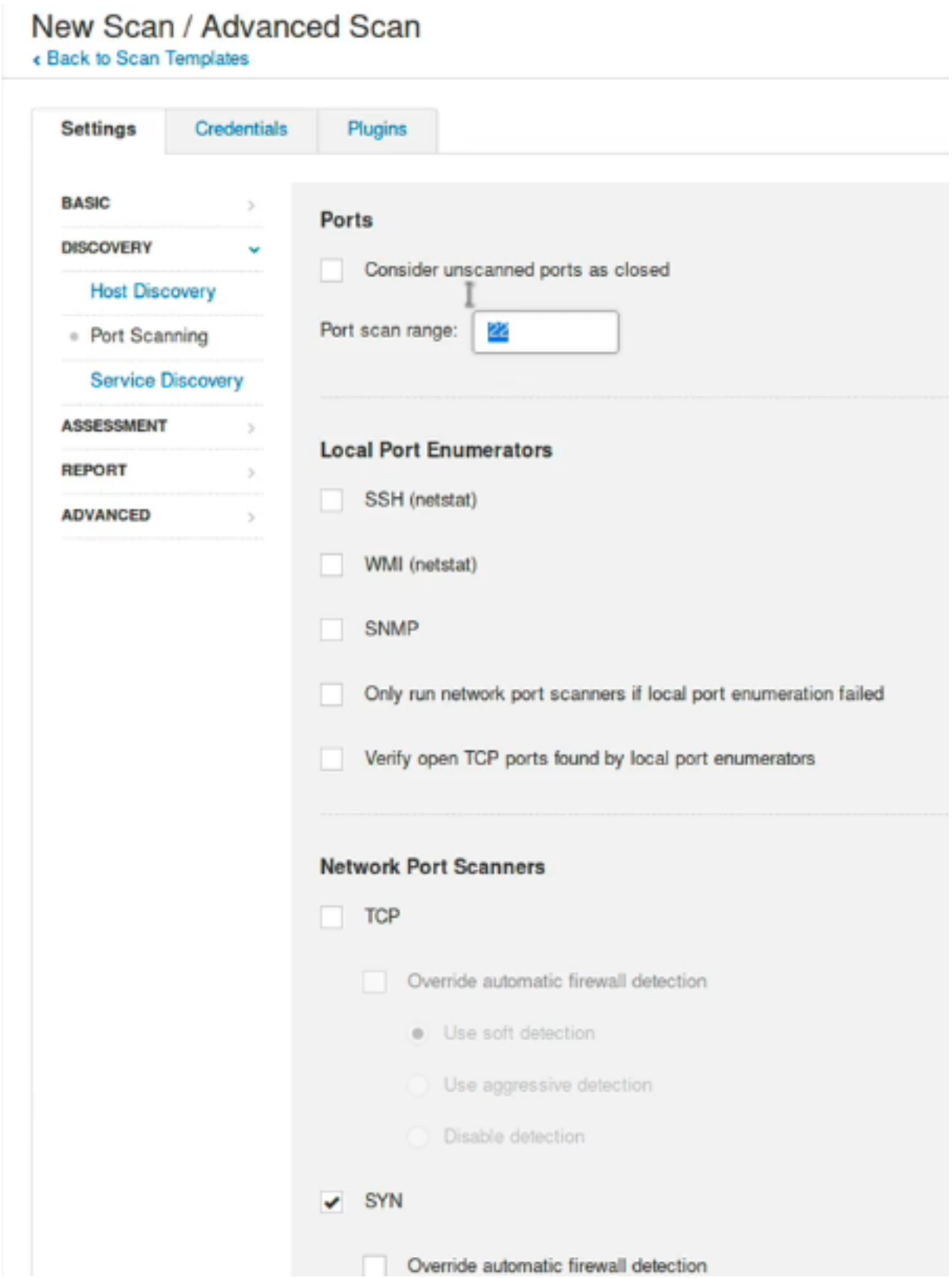
Realizando Testes de Força Bruta

+ Usaremos agora o Advanced Scan

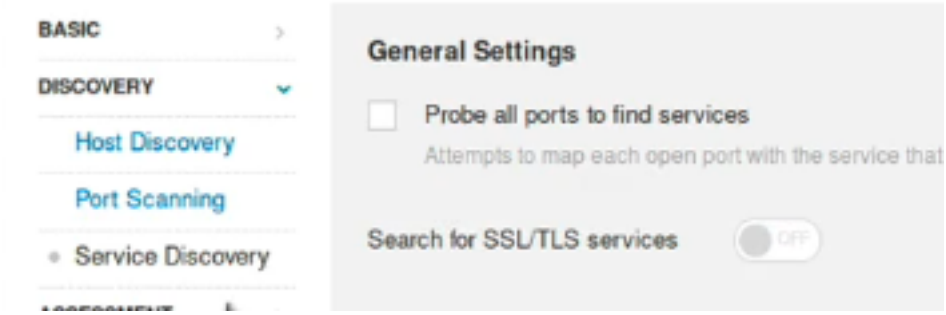
+ Modo de uso:



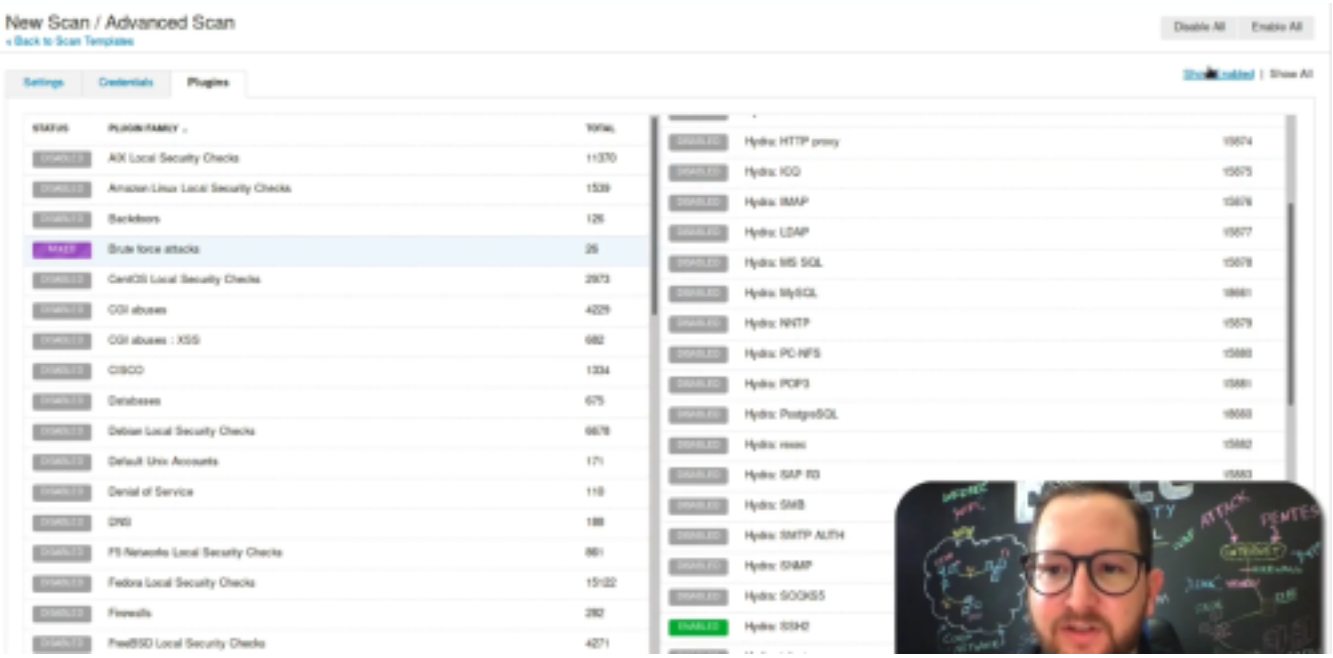
→ Não precisamos agendar
→ Em Host Discovery, vamos desabilitar o ping
→ Em Port Scanning, desabilitamos as enumerções e habilitamos somente a opção mais básica (supondo que queremos um brute force no ssh)



→ Quanto menos parâmetros habilitados, mais rápida será a execução da nossa ferramenta
→ Em Service Discovery, desabilitamos tudo também:



→ No Assessment, vamos habilitar o Hydra e adicionar os arquivos com possíveis users e passwords
→ Desabilitamos as outras ferramentas e deixamos da seguinte maneira:



+No final, ele exibiu o user e a senha encontrados:

CRITICAL **Hydra: SSH2**

Description

This plugin runs Hydra to find SSH2 accounts and passwords by brute

To use this plugin, enter the 'Logins file' and the 'Passwords file' under t

Solution

Change the passwords for the affected accounts.

Output

```
Hydra discovered the following SSH credentials :
username: ti    password: security
```