

# Realizando Testes de Força Bruta

+ Usaremos agora o Advanced Scan

+ Modo de uso:

## New Scan / Advanced Scan

[← Back to Scan Templates](#)

Settings Credentials Plugins

**BASIC**

- General
- Schedule**
- Notifications

**DISCOVERY**

**ASSESSMENT**

**REPORT**

**ADVANCED**

Name: Brute Force - 172.16.1.7

Description:

Folder: My Scans

Targets: 172.16.1.7

Upload Targets Add File

Save Cancel

→ Não precisamos agendar

→ Em Host Discovery, vamos desabilitar o ping

→ Em Port Scanning, desabilitamos as enumerações e habilitamos somente a opção mais básica (supondo que queremos um brute force no ssh)

## New Scan / Advanced Scan

[← Back to Scan Templates](#)

**Settings** | Credentials | Plugins

**BASIC** >  
**DISCOVERY** ▾  
Host Discovery  
• Port Scanning  
Service Discovery  
**ASSESSMENT** >  
**REPORT** >  
**ADVANCED** >

**Ports**  
☐ Consider unscanned ports as closed  
Port scan range:   
**Local Port Enumerators**  
☐ SSH (netstat)  
☐ WMI (netstat)  
☐ SNMP  
☐ Only run network port scanners if local port enumeration failed  
☐ Verify open TCP ports found by local port enumerators  
**Network Port Scanners**  
☐ TCP  
☐ Override automatic firewall detection  
• Use soft detection  
○ Use aggressive detection  
○ Disable detection  
☒ SYN  
☐ Override automatic firewall detection

→ Quanto menos parâmetros habilitados, mais rápida será a execução da nossa ferramenta

→ Em Service Discovery, desabilitamos tudo também:

**BASIC** >  
**DISCOVERY** ▾  
Host Discovery  
Port Scanning  
• Service Discovery

**General Settings**  
☐ Probe all ports to find services  
Attempts to map each open port with the service that  
Search for SSL/TLS services ☐ OFF

→ No Assessment, vamos habilitar o Hydra e adicionar os arquivos com possíveis users e passwords

→ Desabilitamos as outras ferramentas e deixamos da seguinte maneira:

Settings	Credentials	Plugins
Show 1 loaded   Show All		
STATUS	PLUGIN FAMILY	PORT
DISABLED	All Local Security Checks	11370
DISABLED	Amazon Linux Local Security Checks	1539
DISABLED	Backdoors	126
ENABLED	Brute force attacks	26
DISABLED	CentOS Local Security Checks	2973
DISABLED	CGI abuses	4229
DISABLED	CGI abuses : XSS	682
DISABLED	CISCO	1334
DISABLED	Databases	675
DISABLED	Debian Local Security Checks	9678
DISABLED	Default Unix Accounts	171
DISABLED	Denial of Service	118
DISABLED	DNS	188
DISABLED	FS Networks Local Security Checks	861
DISABLED	Fedora Local Security Checks	15122
DISABLED	Firewalls	282
DISABLED	FreeBSD Local Security Checks	4271
DISABLED	Hydra: HTTP proxy	15674
DISABLED	Hydra: IGD	15675
DISABLED	Hydra: IMAP	15676
DISABLED	Hydra: LDAP	15677
DISABLED	Hydra: MS SQL	15678
DISABLED	Hydra: MySQL	18681
DISABLED	Hydra: NNTP	15679
DISABLED	Hydra: PC NFS	15680
DISABLED	Hydra: POP3	15681
DISABLED	Hydra: PostgreSQL	18683
DISABLED	Hydra: rexec	15682
DISABLED	Hydra: SAP SD	15683
DISABLED	Hydra: SMB	
DISABLED	Hydra: SMTP AUTH	
DISABLED	Hydra: SNMP	
DISABLED	Hydra: SOCKS5	
ENABLED	Hydra: SSH2	



+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 force.

To use this plugin, enter the 'Logins file' and the 'Passwords file' under the 'SSH2' section.

### Solution

Change the passwords for the affected accounts.

### Output

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