**VMWare (ESX, VCenter...)**

## Enumeration

Copy

nmap -sV --script "http-vmware-path-vuln or vmware-version" -p <PORT> <IP>

msf> use auxiliary/scanner/vmware/esx\_fingerprint

msf> use auxiliary/scanner/http/ms15\_034\_http\_sys\_memory\_dump

## Bruteforce

Copy

msf> auxiliary/scanner/vmware/vmware\_http\_login

If you find valid credentials, you can use more metasploit scanner modules to obtain information.