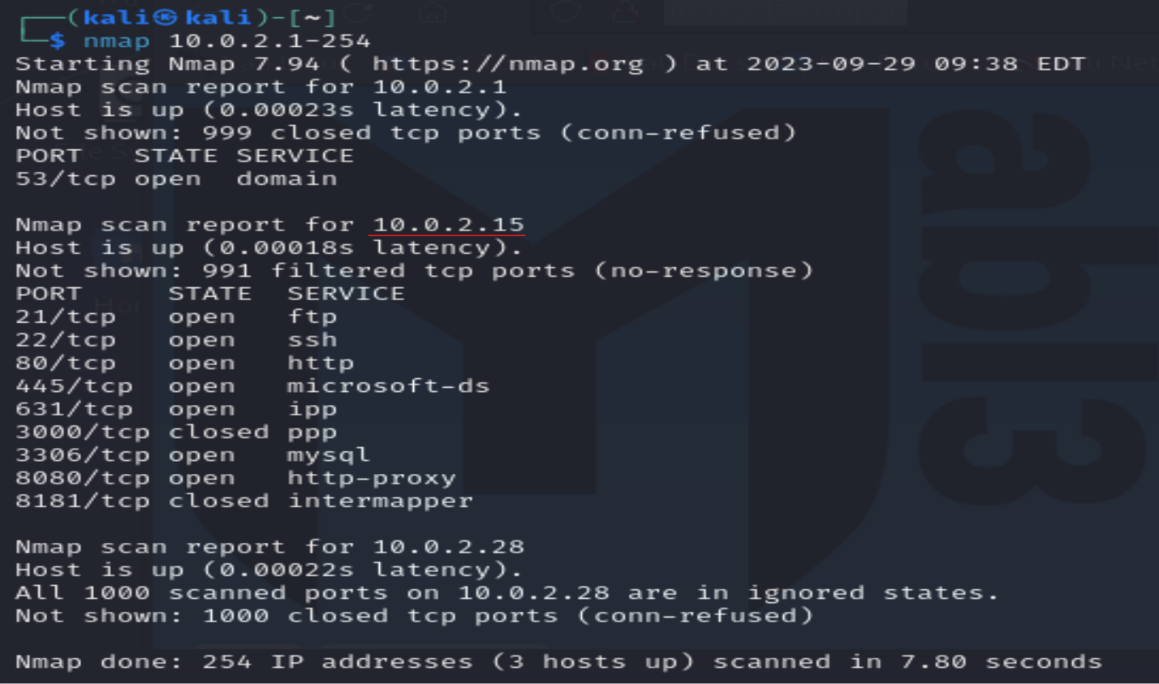
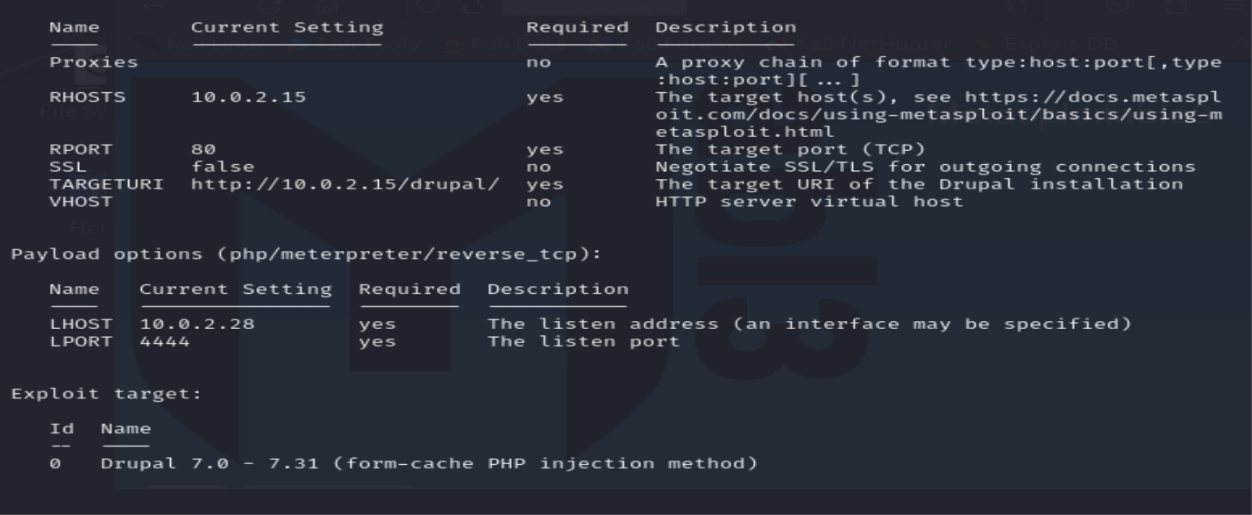
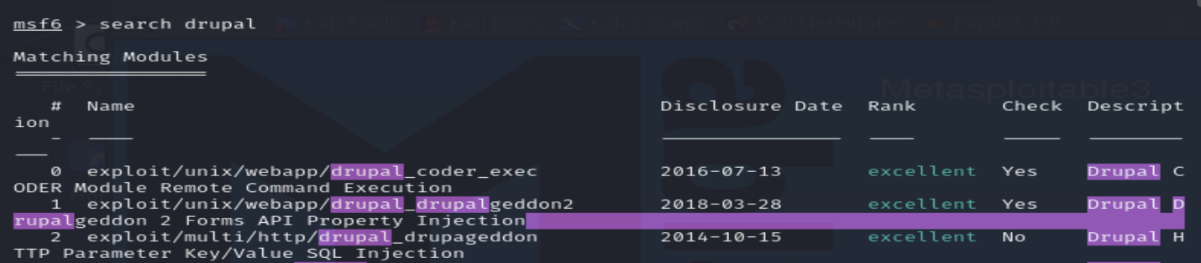
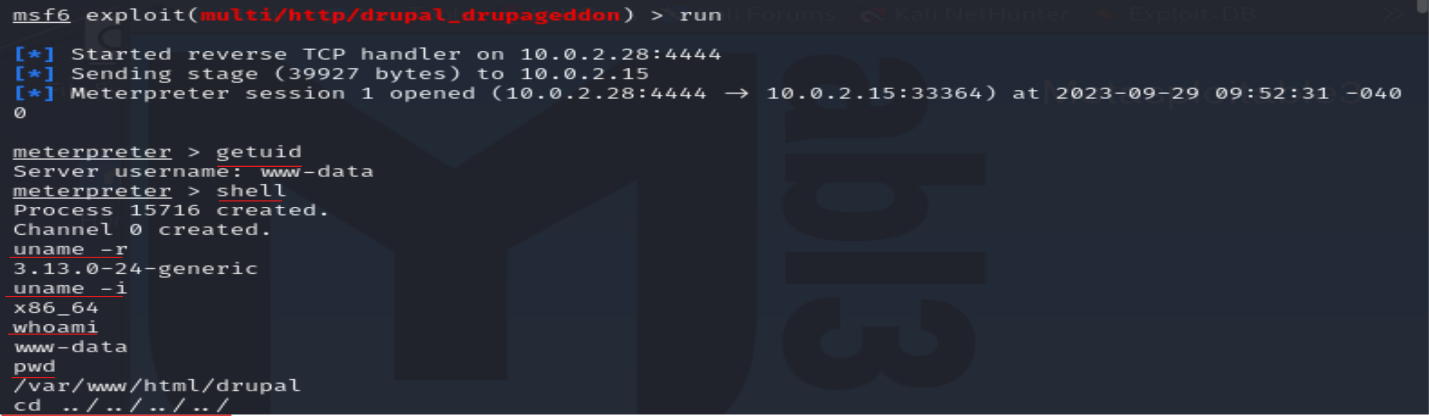
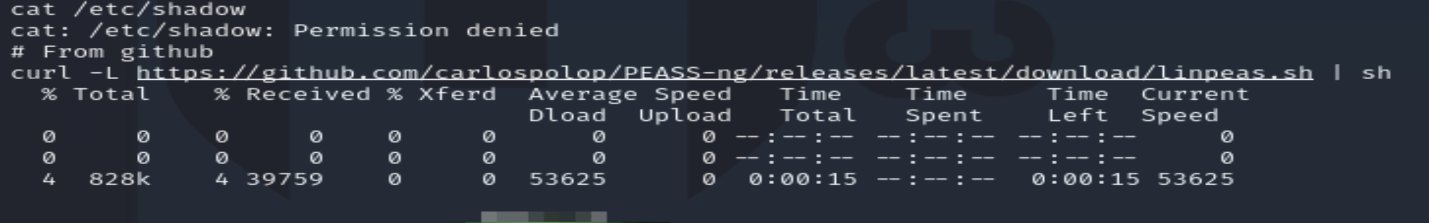
I began by conducting an Nmap scan to pinpoint the IP addresses of both the target (10.0.2.15) and the host (10.0.2.28). My focus was on identifying open ports, specifically highlighting port 22 (SSH) and port 80 (HTTP), which serve as potential entry points for exploiting vulnerabilities or services. Delving deeper into these services and ports is vital for achieving initial access to the Ubuntu machine and then proceeding to explore potential avenues for privilege escalation.

Utilizing Metasploit to search for potential vulnerabilities related to Drupal, a popular web application. Module 2, tailored to exploit HTTP, is an ideal option for targeting Drupal via its web interface.

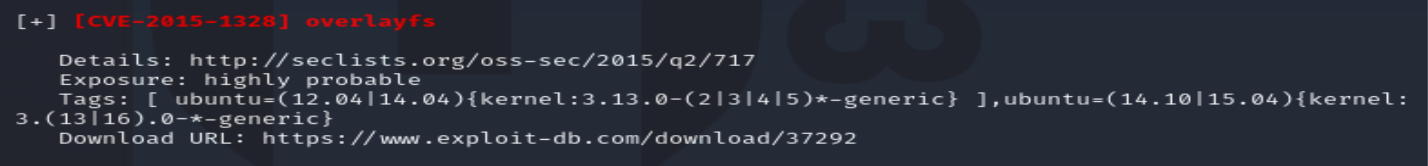
Configuring RHOSTS with the target IP (10.0.2.15) and specifying the TARGETURI as http://10.0.2.15/drupal/ is a vital step, honing the exploit towards the particular Drupal instance being targeted. It's essential to thoroughly configure all other parameters and options before initiating the exploit. 

The information I've gathered indicates that the system is running the Linux kernel version 3.13.0-24-generic on an x86\_64 architecture, and I am are currently operating as the www-data user.

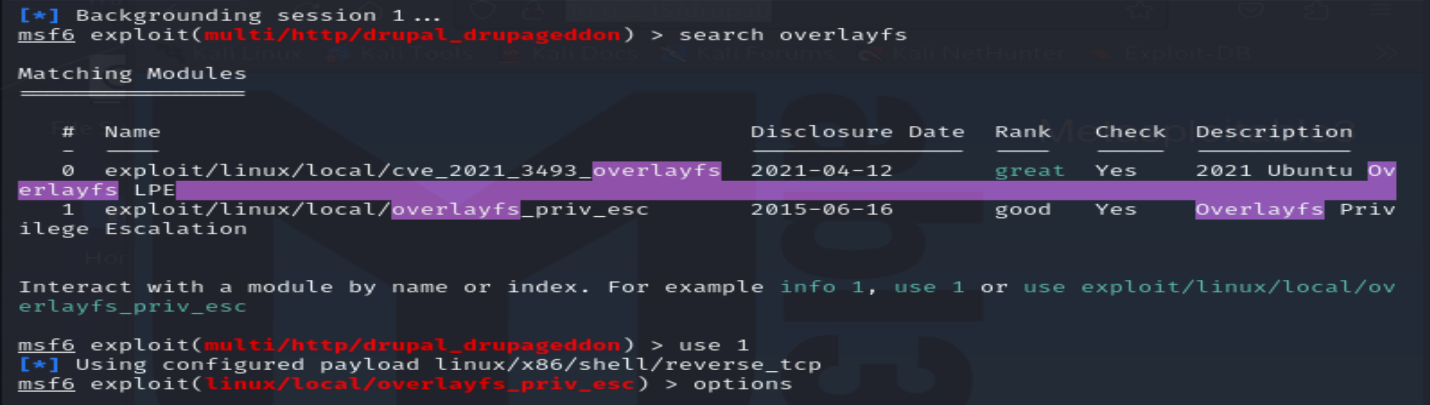
However, my attempt to read the /etc/shadow file resulted in a "Permission denied" error. This is because the /etc/shadow file is typically only readable by the root user for security reasons. As the www-data user, I lack the necessary permissions to access it directly.

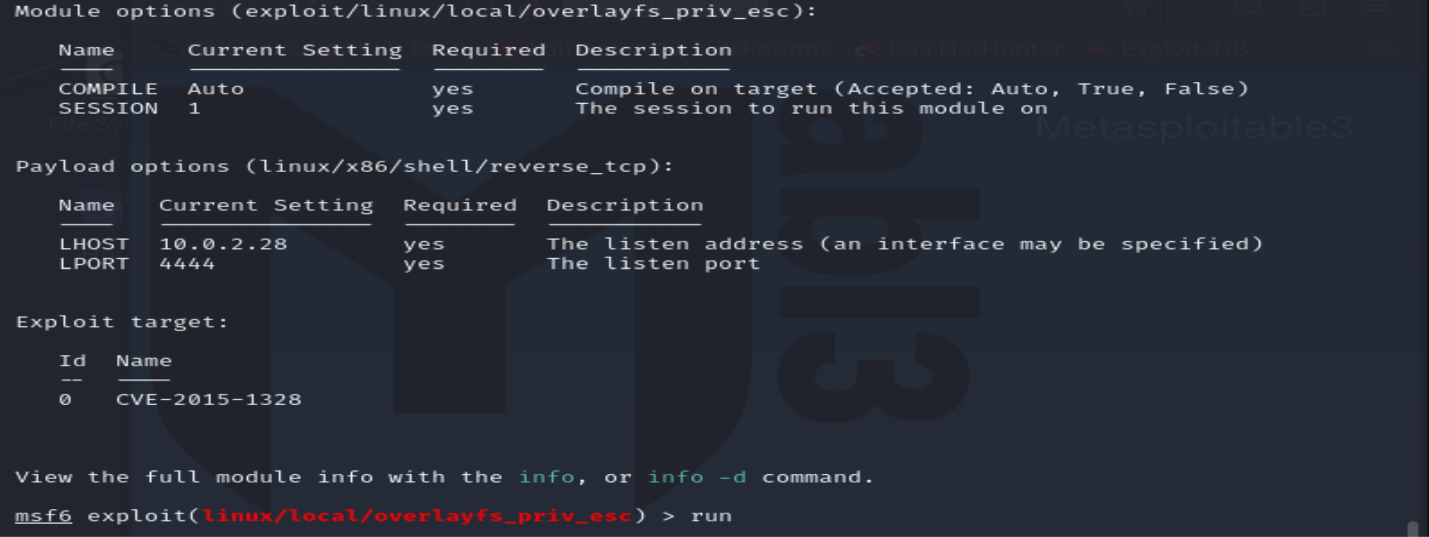


I've identified a potential privilege escalation vulnerability CVE-2015-1328 related to the OverlayFS filesystem. This vulnerability could allow me to escalate my privileges from the www-data user to root if it's successfully exploited.



I placed the Meterpreter session in the background, which allows me to run other Metasploit modules. I used the search command in Metasploit to look for the OverlayFS privilege escalation module.



It appears you've set up the exploit module with the appropriate session, LHOST (local host), and target (CVE-2015-1328). With these settings in place, I can proceed to run the exploit by executing the exploit command within Metasploit. This will attempt to exploit the CVE-2015-1328 vulnerability on the target system and, if successful, grant me elevated privileges, potentially allowing my to become the root user.

It seems that the exploit was effective in granting me root access to the target system. The warning regarding an incompatible session architecture likely stems from the module I utilized, which was designed for a different architecture (possibly PHP), than the initial Meterpreter session. However, this discrepancy didn't hinder me from achieving root access.

I've managed to successfully acquire the /etc/shadow file, which holds password hashes for various user accounts on the system. The discovery of a user named "Leia Organa" and what appears to be a hashed password is a significant finding. In the realm of ethical hacking or penetration testing, obtaining password hashes holds great value, as it opens the door to potential password cracking and other password-centric attacks, thereby enabling further access or privileges on the target system.

To kick off the process, I initiated an Nmap scan to uncover open ports and services. Notably, ports 22 (SSH) and 80 (HTTP) stood out as potential entry points. I proceeded to investigate the Drupal application running on port 80 and leveraged Metasploit to exploit a known vulnerability (CVE-2015-1328) associated with OverlayFS. This allowed me to gain initial access to the system, assuming the identity of the "www-data" user. Subsequently, I escalated my privileges using the same vulnerability, elevating my status to that of the root user and granting me complete control over the target system. From there, I proceeded to access sensitive files like /etc/shadow, where I identified a user and their associated password hash.

