DC -1 Machine

DC-1 CTF Challenge Overview

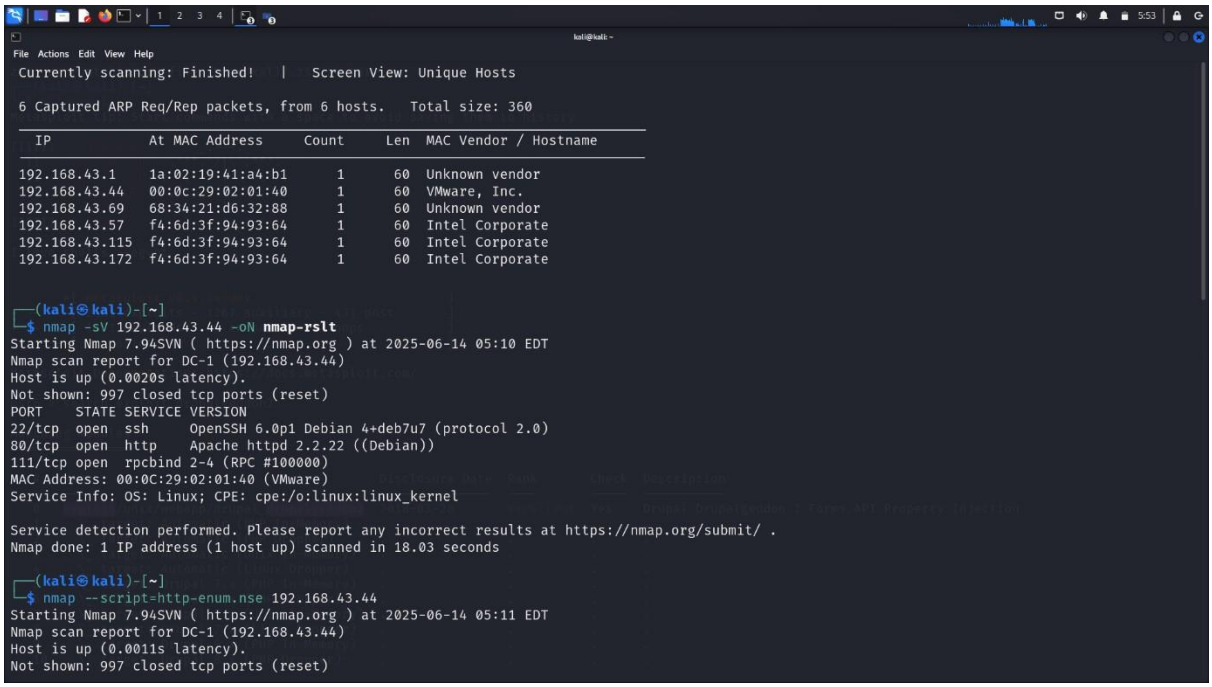
- **Platform**: VulnHub
- **Objective**: Capture the flag by gaining root access (`root.txt`)
- **Challenge Type**: Boot2Root | CTF | Beginner-friendly

Step 1:-

A lightweight network reconnaissance tool commonly used to identify active hosts in a network.

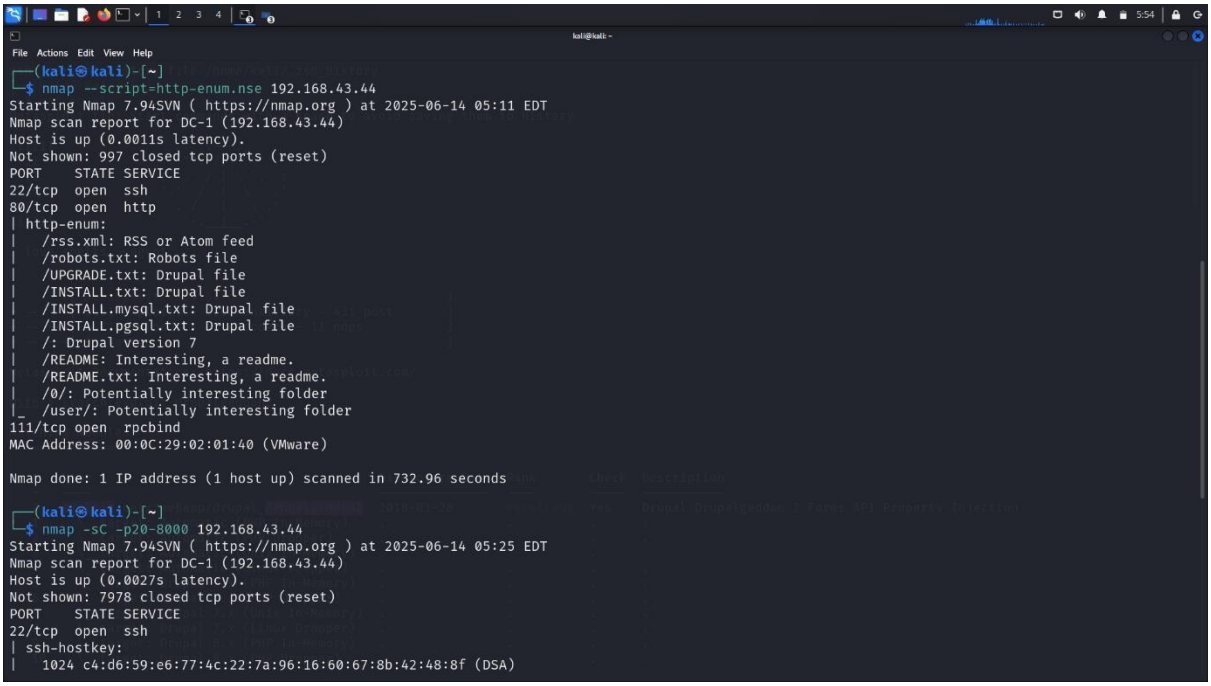
It's Netdiscover is a simple tool, particularly useful in Local Area Networks (LANs). It works by sending

ARP (Address Resolution Protocol) requests and listens for ARP replies to map live systems in a subnet.



Step 2:-

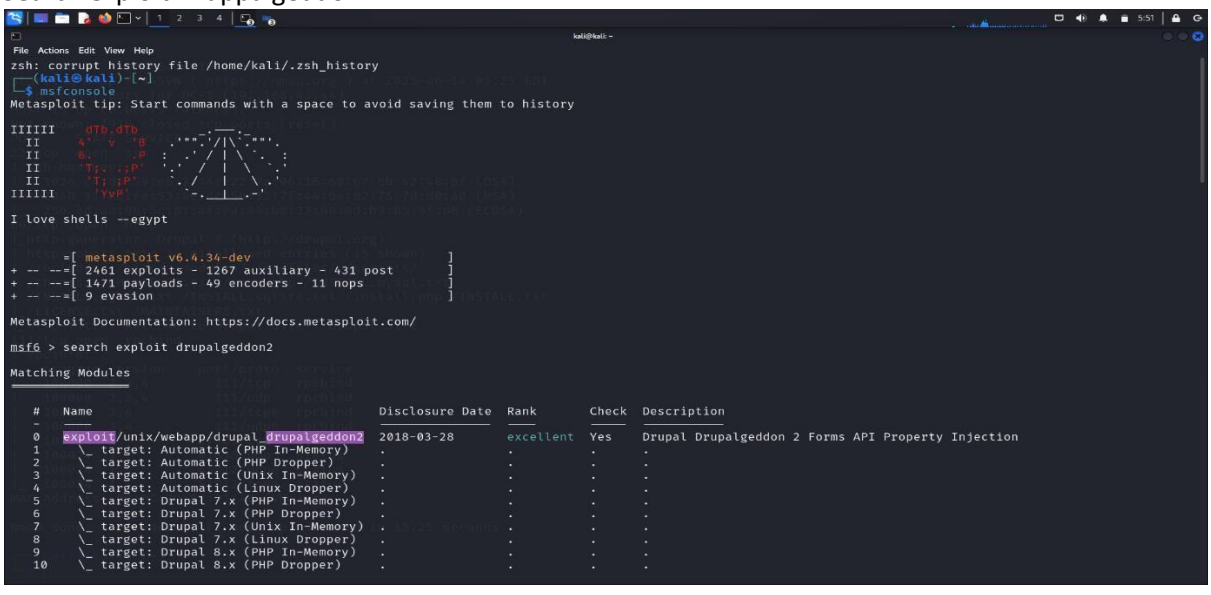
Nmap is a powerful, open-source tool used for network discovery and security auditing.It is widely used by network administrators and penetration testers to map networks, identify devices, scan for open ports, and detect vulnerabilities.



Step-3:-

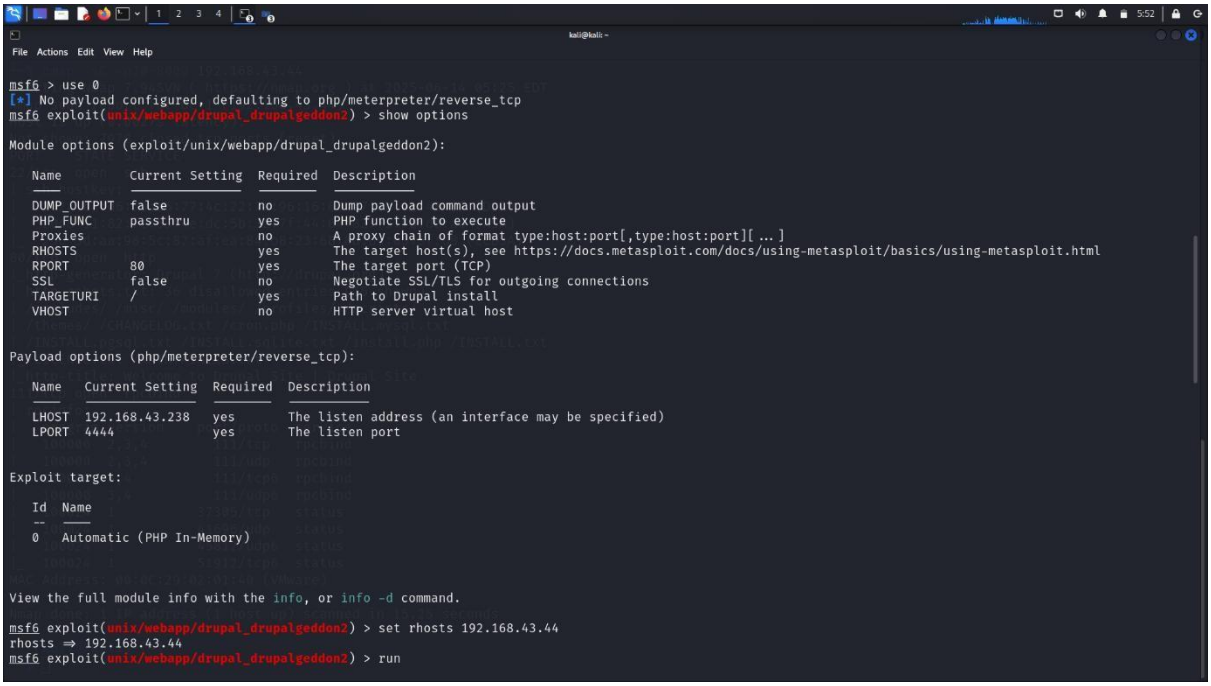
Msfconsoleis the command-line interface for the Metasploit Framework, a widely used opensource tool for penetration testing, exploit development, and vulnerability research. Metasploit is used to test security defenses by simulating attacks, exploiting vulnerabilities, and verifying security mitigations.

Search exploit Druppalgeddon -2



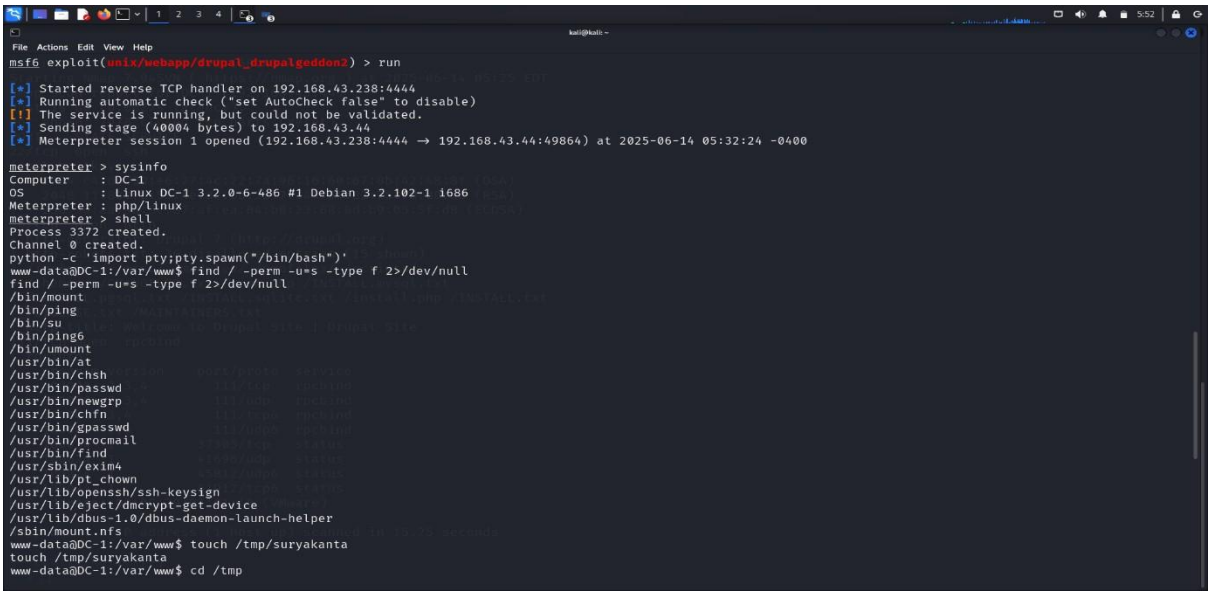
Step -4 :-

Then use 0 for attack the machine and show options and set the RHOSTS, LHOST.



Step-5 :-

Set RHOSTS(victim IP) & set LHOST (listening IP) and then exploit.



Step -6 :- use the sysinfo for next session

Step 7: use python script for shell

Step 8: find command use for permission the files and 2>/dev/null for error

Step 9: touch command use for create a directory

Step 10: then execute the file name we create

Step 11: then execute the file /bin/bash and then we crack the machine