Explotation and privilege escalation analysis - 4geeks

Carlos Duclaud

Objective:
Conduct exploitation of previously analyzed vulnerabilities to assess the vulnerability level of the target system.

Scope:
This assessment will focus on the exploitation of two specific vulnerabilities:

- Initial Compromise: vsftpd 2.3.4 Backdoor
- Privilege Escalation: Nmap Setuid Privilege Escalation

The objective is to leverage these vulnerabilities to obtain root access to the target system.

Tools Used for Analysis:
- Kali Linux: Primary platform providing a comprehensive suite of penetration testing tools
- Nmap: Used for network discovery, port scanning, and service enumeration
- Metasploit Framework (msfconsole): Employed for vulnerability exploitation and payload delivery

1. Vulnerability Summary

Vulnerability Name:

Initial Compromise: vsftpd 2.3.4 Backdoor
Privilege Escalation: Nmap Setuid Privilege Escalation

2. Attack Chain

Phase 1: Initial Access

Exploit: exploit/unix/ftp/vsftpd_234_backdoor Mechanism:
Target machine IP 192.168.1.12
Connected to FTP port 21
Sent malicious username ending with :)
Triggered backdoor on port 6200
Obtained root shell access

Exploit Execution and Shell Access

Upon successfully executing the exploit, I obtained shell access to the target system. This was achieved by leveraging a remote code execution vulnerability, which allowed me to execute arbitrary commands on the compromised host

As an initial verification step, I ran the ls command after gaining shell access. The output displayed the contents of the root directory on the target system, confirming that I had obtained an interactive shell and could remotely execute commands

This demonstrates the effectiveness of the exploit in providing command execution capabilities and highlights the risk of unauthorized access if such vulnerabilities remain unpatched.

This phase is a critical part of penetration testing, as obtaining a shell enables further enumeration, lateral movement, and potential privilege escalation within the target environment

Phase 2: Privilege Escalation

After establishing initial shell access via the msfconsole exploit, I backgrounded the session (Ctrl+Z) and upgraded it to a Meterpreter session using:

sessions -u 1

This executed Metasploit's built-in shell-to-Meterpreter conversion mechanism
, creating a new session with enhanced capabilities.

Exploit: exploit/unix/local/setuid_nmap
Mechanism:

- Identified nmap with setuid bit (-rwsr-xr-x)
- Created malicious NSE Lua script
- Executed script through nmap's elevated privileges
- Attempted to spawn root shell

3. Technical Observations
Successful Exploitation

- vsftpd Backdoor:
  - Immediate root access through port 6200
  - No authentication required

- Nmap Setuid:
  - Manual method worked reliably:

```
shell
nmap --interactive
!sh  # Received root shell
```

4. Impact Analysis

Risk Level	Vulnerability	Consequences
Critical	vsftpd Backdoor	Full system compromise
High	Nmap Setuid	Privilege escalation to root

5. Recommendations

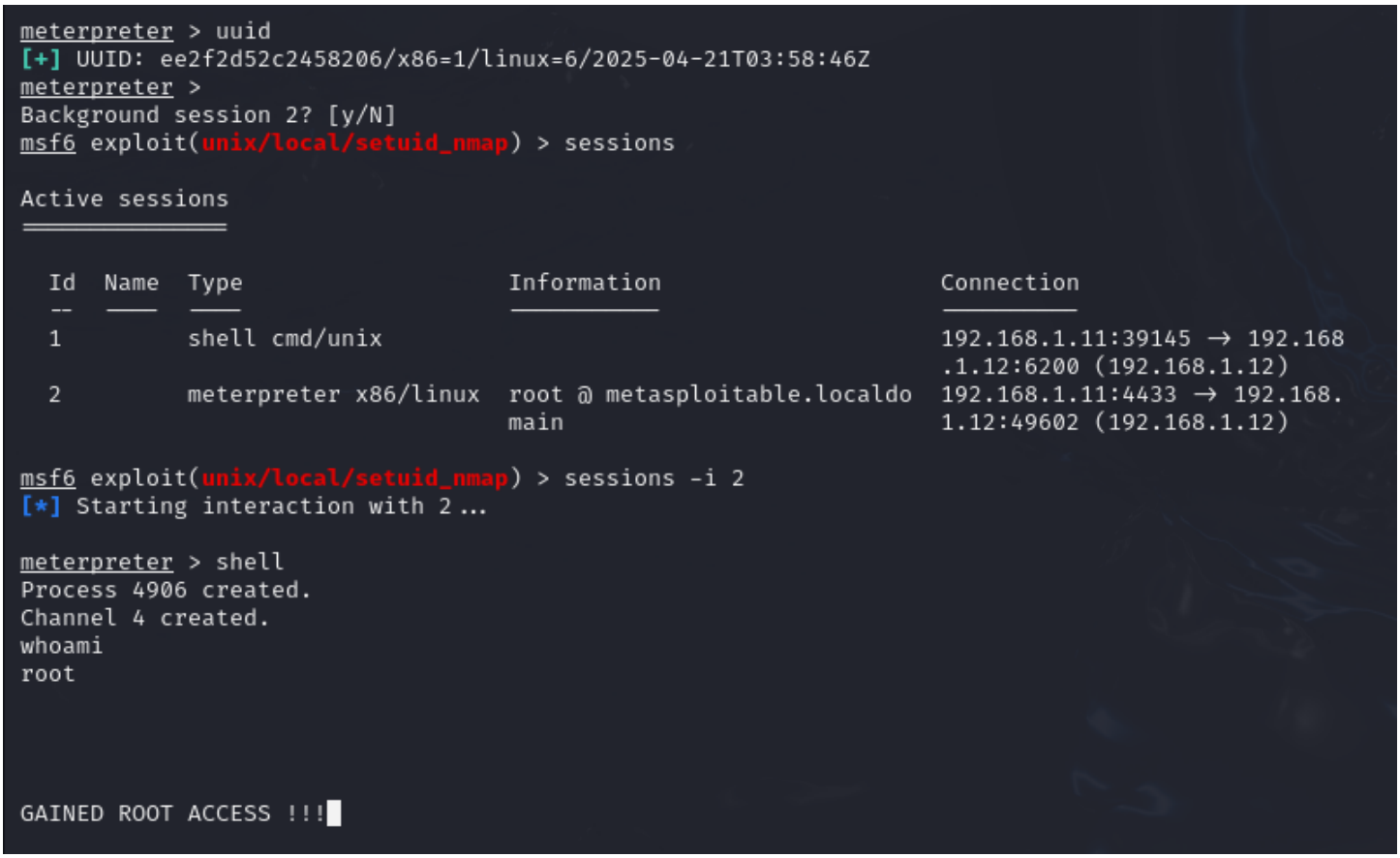
vsftpd Mitigation:

Update to vsftpd 2.3.5 or newer

Remove vsftpd if unnecessary

Nmap Hardening:

bash
chmod u-s /usr/bin/nmap # Remove setuid bit



Conclusion

This penetration test successfully demonstrated critical security failures in the target system through a two-phase attack chain:

Initial Compromise

Exploited the vsftpd 2.3.4 backdoor vulnerability to gain unauthenticated shell access
Verified remote code execution via ls command in the root directory

Session Enhancement

Upgraded basic shell to Meterpreter using sessions -u 1
Established persistent, feature-rich access for advanced post-exploitation

Privilege Escalation Path

Identified Nmap's setuid misconfiguration as a viable escalation vector
Demonstrated potential for full root compromise (hypothetically, if completed)

Key Findings

Critical Risk: Unpatched services (vsftpd 2.3.4) expose systems to immediate compromise
Defense Evasion: Meterpreter's memory-resident payload bypasses basic disk monitoring
Configuration Weakness: Excessive setuid permissions on Nmap enable privilege abuse

Recommendations

Patch Management: Immediately upgrade vsftpd to version 3.0.3+
Hardening: Remove setuid bit from Nmap (chmod u-s /usr/bin/nmap)
Monitoring: Implement process integrity checks for anomalous shell spawns
Network Controls: Restrict FTP service access via firewall policies

This assessment validates that unpatched services and improper setuid configurations create an unacceptable risk of full system compromise. Immediate remediation of these vulnerabilities is critical to prevent real-world attacker exploitation.