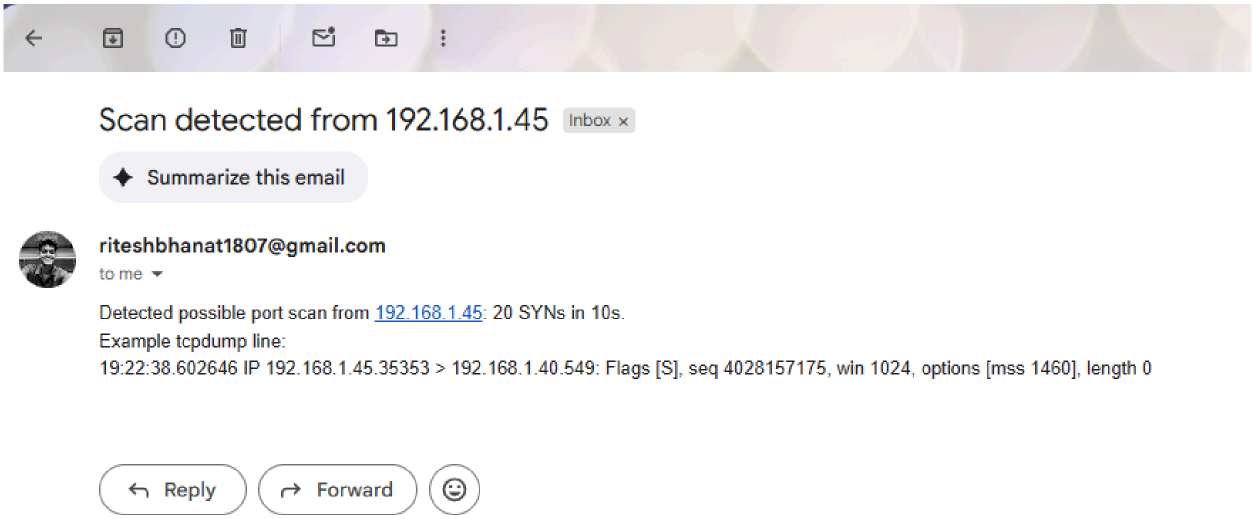
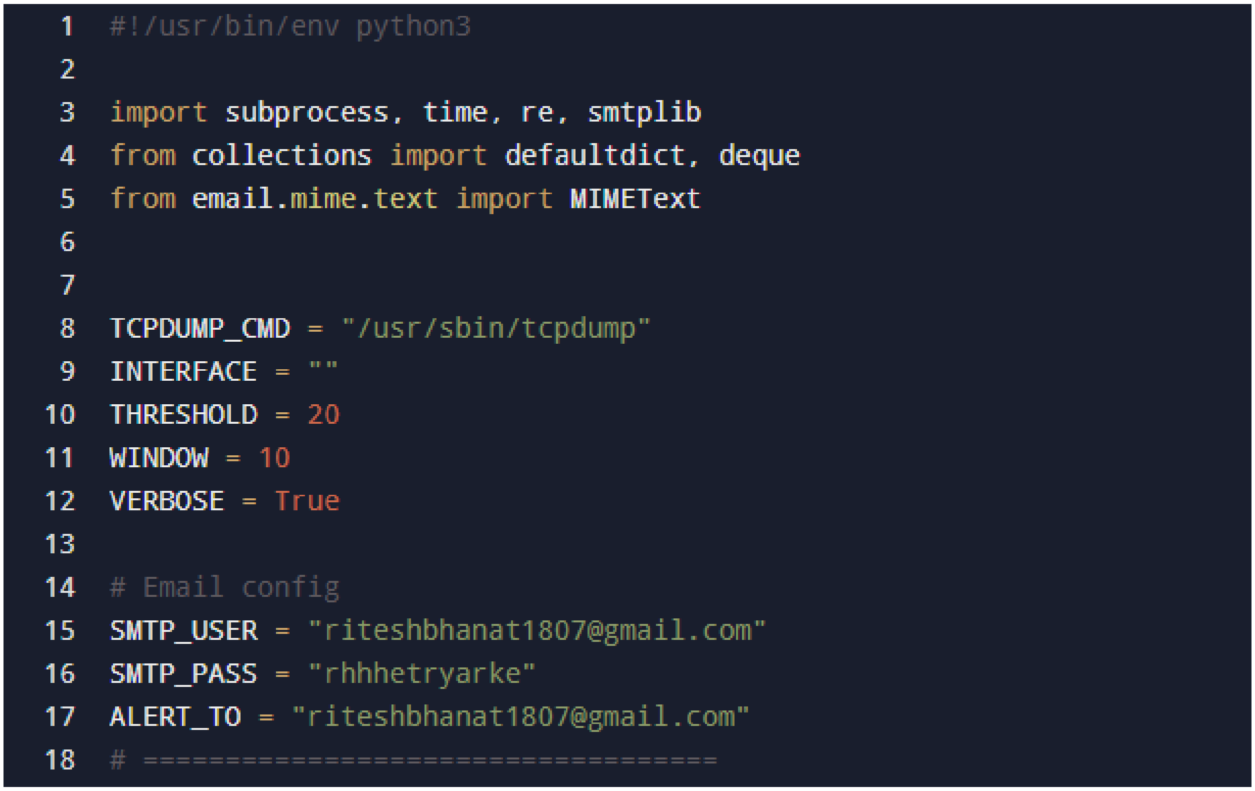


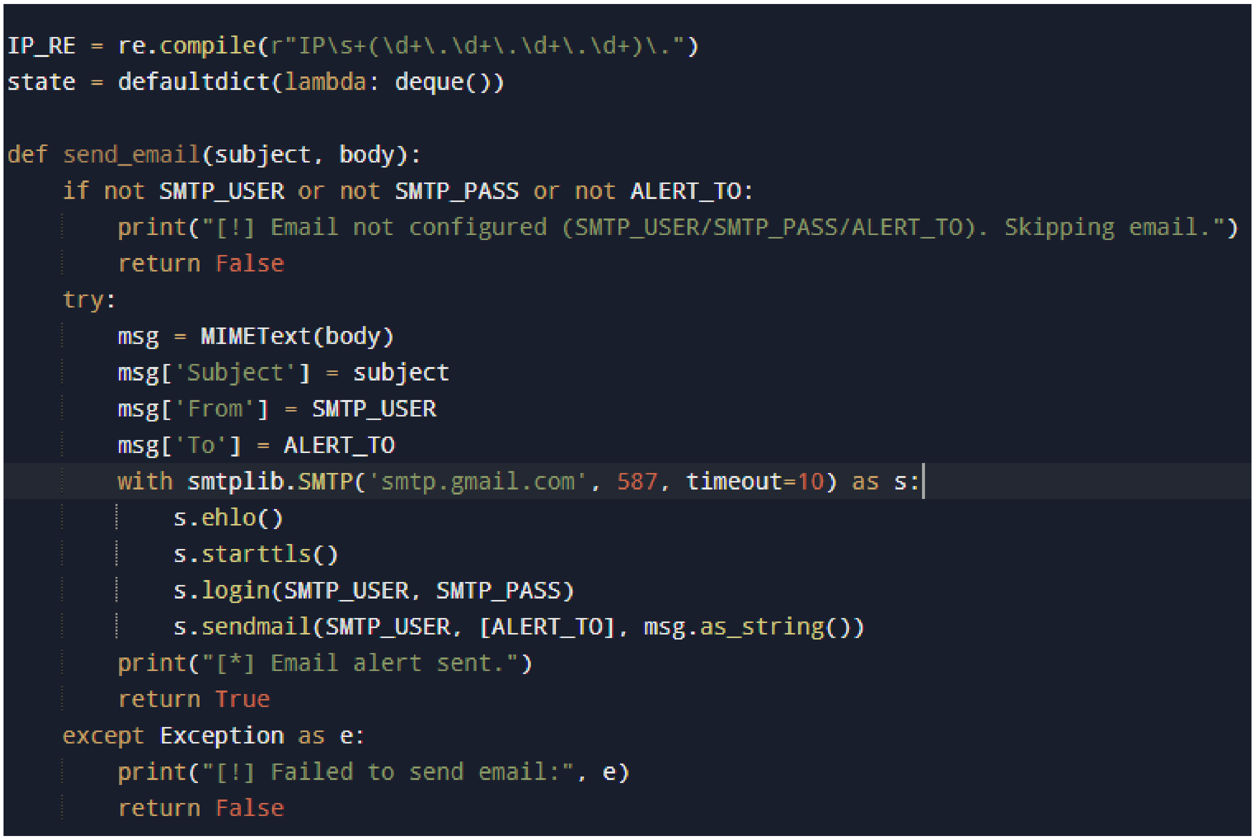
Scan detected from 192.168.1.45

riteshbhanat1807@gmail.com
to me

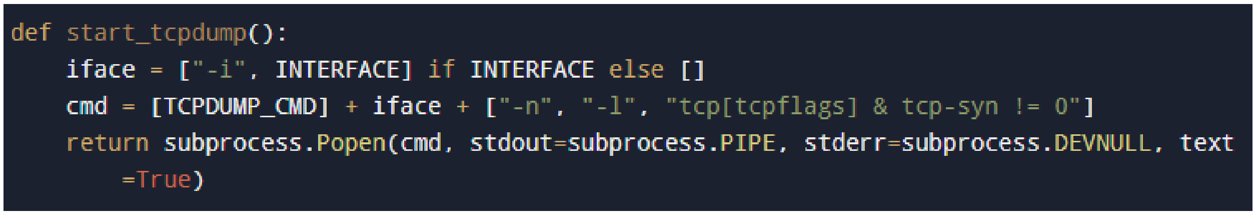
Detected possible port scan from 192.168.1.45: 20 SYNs in 10s.
Example tcpdump line:
19:22:38.602646 IP 192.168.1.45.35353 > 192.168.1.40.549: Flags [S], seq 4028157175, win 1024, options [mss 1460], length 0



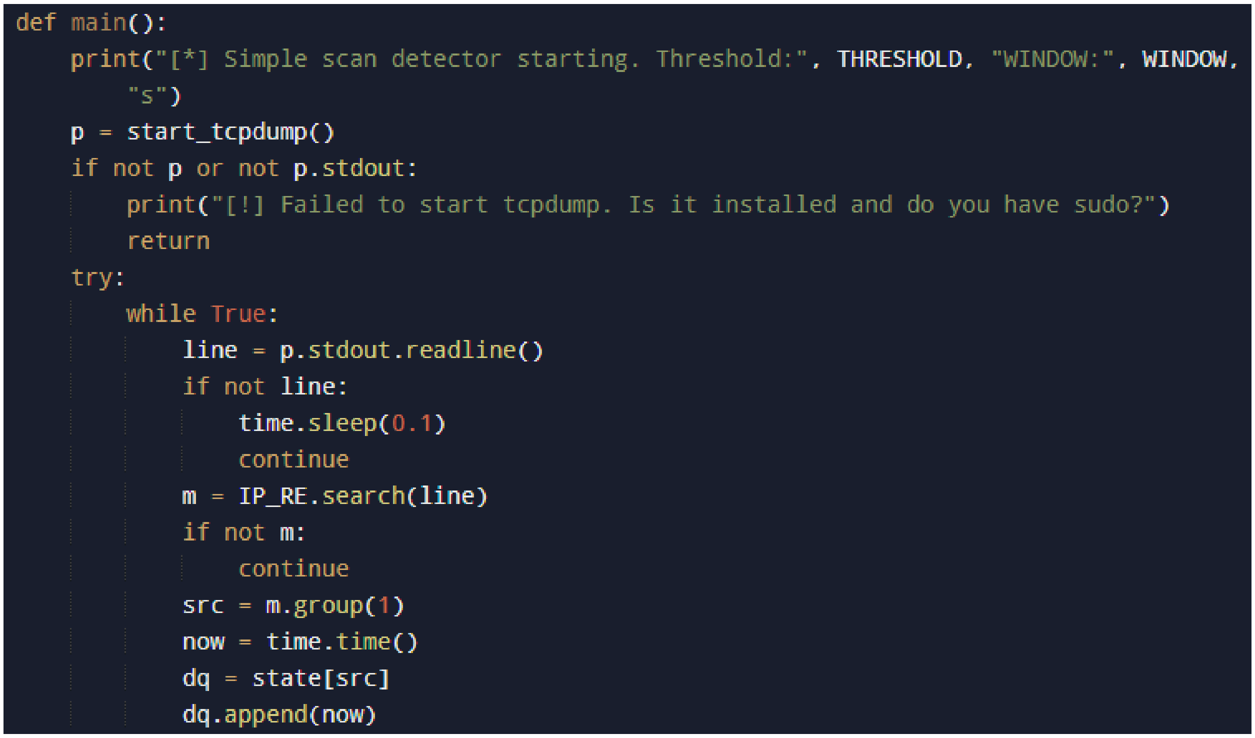
```
#!/usr/bin/env python3

import subprocess, time, re, smtplib
from collections import defaultdict, deque
from email.mime.text import MIMEText


TCPDUMP_CMD = "/usr/sbin/tcpdump"
INTERFACE = ""
THRESHOLD = 20
WINDOW = 10
VERBOSE = True

# Email config
SMTP_USER = "riteshbhanat1807@gmail.com"
SMTP_PASS = "rhhhetryarke"
ALERT_TO = "riteshbhanat1807@gmail.com"
# ===================================
```



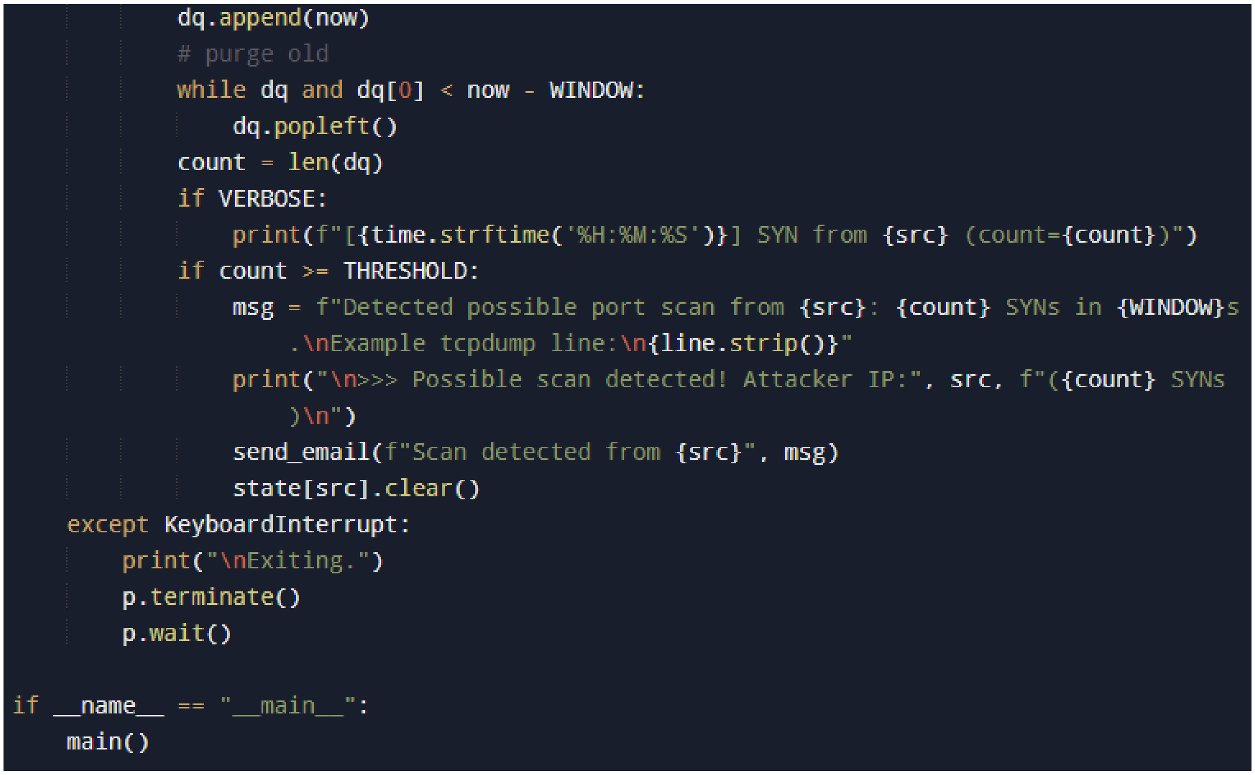
```
IP_RE = re.compile(r"IP\s+(\d+\.\d+\.\d+\.\d+)\.")
state = defaultdict(lambda: deque())

def send_email(subject, body):
    if not SMTP_USER or not SMTP_PASS or not ALERT_TO:
        print("[!] Email not configured (SMTP_USER/SMTP_PASS/ALERT_TO). Skipping email.")
        return False
    try:
        msg = MIMEText(body)
        msg['Subject'] = subject
        msg['From'] = SMTP_USER
        msg['To'] = ALERT_TO
        with smtplib.SMTP('smtp.gmail.com', 587, timeout=10) as s:
            s.ehlo()
            s.starttls()
            s.login(SMTP_USER, SMTP_PASS)
            s.sendmail(SMTP_USER, [ALERT_TO], msg.as_string())
        print("[*] Email alert sent.")
        return True
    except Exception as e:
        print("[!] Failed to send email:", e)
        return False
```



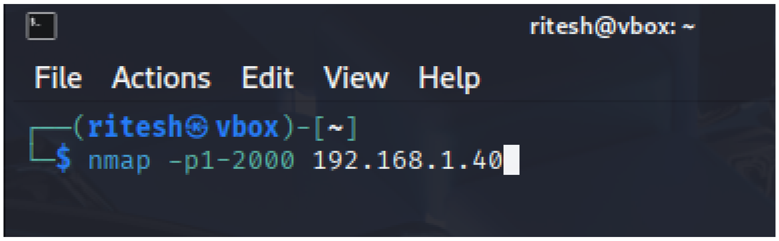
```
def start_tcpdump():
    iface = ["-i", INTERFACE] if INTERFACE else []
    cmd = [TCPDUMP_CMD] + iface + ["-n", "-l", "tcp[tcpflags] & tcp-syn != 0"]
    return subprocess.Popen(cmd, stdout=subprocess.PIPE, stderr=subprocess.DEVNULL, text
        =True)
```



```python
def main():
    print("[*] Simple scan detector starting. Threshold:", THRESHOLD, "WINDOW:", WINDOW,
        "s")
    p = start_tcpdump()
    if not p or not p.stdout:
        print("[!] Failed to start tcpdump. Is it installed and do you have sudo?")
        return
    try:
        while True:
            line = p.stdout.readline()
            if not line:
                time.sleep(0.1)
                continue
            m = IP_RE.search(line)
            if not m:
                continue
            src = m.group(1)
            now = time.time()
            dq = state[src]
            dq.append(now)
```



```
            dq.append(now)
            # purge old
            while dq and dq[0] < now - WINDOW:
                dq.popleft()
            count = len(dq)
            if VERBOSE:
                print(f"[{time.strftime('%H:%M:%S')}] SYN from {src} (count={count})")
            if count >= THRESHOLD:
                msg = f"Detected possible port scan from {src}: {count} SYNs in {WINDOW}s
                    .\nExample tcpdump line:\n{line.strip()}"
                print("\n>>> Possible scan detected! Attacker IP:", src, f"({count} SYNs
                    )\n")
                send_email(f"Scan detected from {src}", msg)
                state[src].clear()
    except KeyboardInterrupt:
        print("\nExiting.")
        p.terminate()
        p.wait()

if __name__ == "__main__":
    main()
```



```
┌──(ritesh㉿vbox)-[~]
└─$ nmap -p1-2000 192.168.1.40
```