RECON

Fast TCP port scanner + basic service probe

Python script:

```
#!/usr/bin/env python3
"""
Simple TCP port scanner + banner probe.
Usage: python3 recon.py <target_ip> [start_port] [end_port]
Example: python3 recon.py 192.168.56.101 1 1024
"""

import socket
import sys
import concurrent.futures
from datetime import datetime

TARGET = sys.argv[1] if len(sys.argv) > 1 else None
START = int(sys.argv[2]) if len(sys.argv) > 2 else 1
END = int(sys.argv[3]) if len(sys.argv) > 3 else 1024
TIMEOUT = 1.0

if not TARGET:
    print("Usage: python3 recon.py <target_ip> [start_port] [end_port]")
    sys.exit(1)

open_ports = []

def probe_port(port):
    try:
        with socket.socket(socket.AF_INET, socket.SOCK_STREAM) as s:
            s.settimeout(TIMEOUT)
            r = s.connect_ex((TARGET, port))
            if r == 0:
                try:
                    s.send(b'HEAD / HTTP/1.0\r\n\r\n')
                    banner = s.recv(1024).decode(errors='ignore').strip()
```

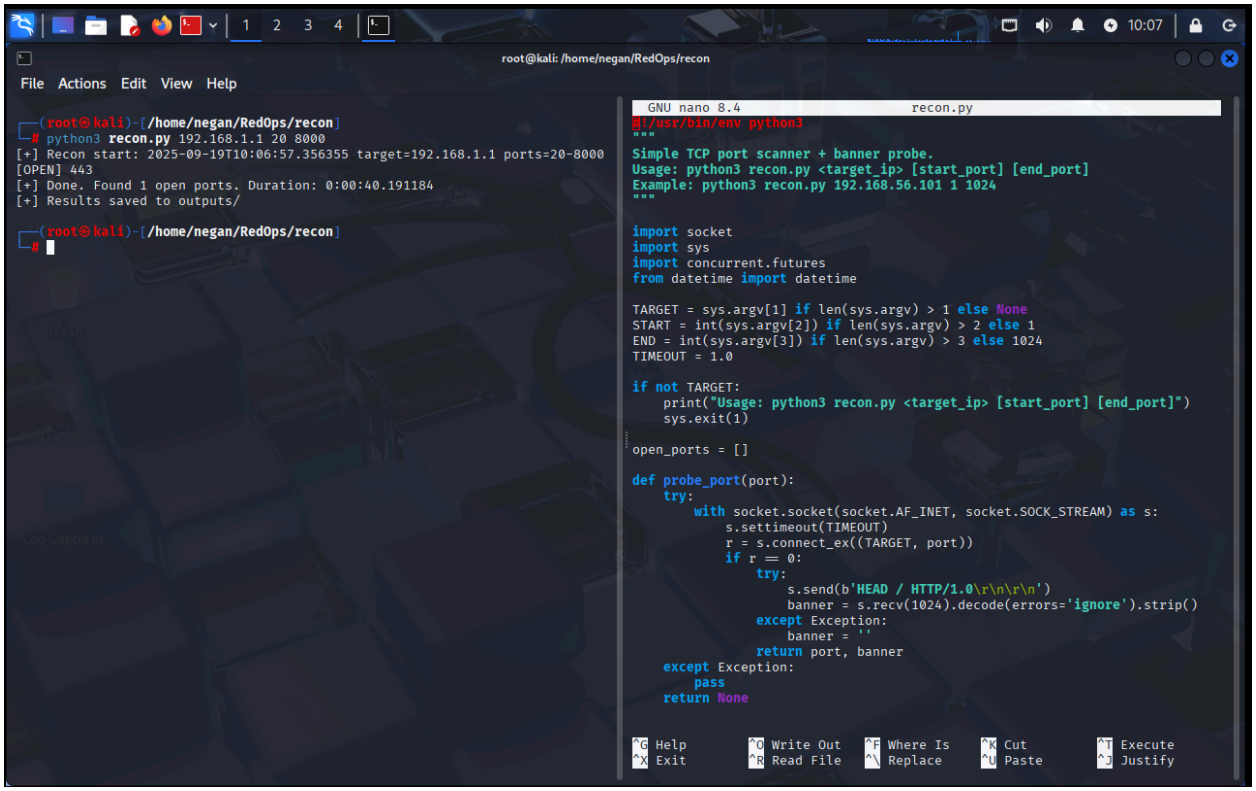
```
            except Exception:
                banner = ''
            return port, banner
    except Exception:
        pass
    return None

start = datetime.now()
print(f"[+] Recon start: {start.isoformat()} target={TARGET} ports={START}-{END}")

with concurrent.futures.ThreadPoolExecutor(max_workers=200) as ex:
    futures = {ex.submit(probe_port, p): p for p in range(START, END+1)}
    for fut in concurrent.futures.as_completed(futures):
        res = fut.result()
        if res:
            port, banner = res
            open_ports.append((port, banner))
            print(f"[OPEN] {port} {banner}")

end = datetime.now()
print(f"[+] Done. Found {len(open_ports)} open ports. Duration: {end-start}")
# Save to outputs
import json, os
os.makedirs("../outputs", exist_ok=True)
with open("../outputs/recon_{}.json".format(TARGET), "w") as f:
    json.dump({"target": TARGET, "ports": open_ports, "scanned_range": [START, END],
"started": start.isoformat()}, f, indent=2)
print("[+] Results saved to outputs/")
```

Working :



Jayesh R. Yadav

Output :

```
┌──(root㉿kali)-[/home/negan/RedOps/recon]
└─# python3 recon.py 192.168.1.1 20 8000
[+] Recon start: 2025-09-19T10:06:57.356355 target=192.168.1.1 ports=20-8000
[OPEN] 443
[+] Done. Found 1 open ports. Duration: 0:00:40.191184
[+] Results saved to outputs/

┌──(root㉿kali)-[/home/negan/RedOps/recon]
└─# ls
recon.py

┌──(root㉿kali)-[/home/negan/RedOps/recon]
└─# cd ..

┌──(root㉿kali)-[/home/negan/RedOps]
└─# ls
outputs  recon

┌──(root㉿kali)-[/home/negan/RedOps]
└─# outputs/

┌──(root㉿kali)-[/home/negan/RedOps/outputs]
└─# ls
recon_192.168.1.1.json

┌──(root㉿kali)-[/home/negan/RedOps/outputs]
└─#
```