Reconnaissance Simulation Report (Simulation — Safe / No Scans Performed)

Includes: Python script, inline comments, explanation, and example output

Objective

Simulate the reconnaissance phase of a red team engagement to identify potential attack vectors. This is a SAFE simulation — no real network traffic or scans are performed. The PDF contains the code, comments, explanation, and example output.

Python Script (Simulation)

```
import os

# === CONFIGURATION ===
TARGET_DOMAIN = "fictionalcorp.com"
OUTPUT_DIR = "recon_results"
os.makedirs(OUTPUT_DIR, exist_ok=True)

def passive_recon(domain):
    """Simulates passive recon (subdomain enumeration)."""
    subdomains = [
        f"www.{domain}",
        f"mail.{domain}",
        f"dev.{domain}",
        f"vpn.{domain}"
    ]
    with open(f"{OUTPUT_DIR}/passive_recon.txt", "w") as f:
        for sub in subdomains:
            f.write(sub + "\n")
    return subdomains

def active_recon(subdomains):
    """Simulates active recon (port scanning) — FAKE results for safety."""
    scan_results = {
        "www.fictionalcorp.com": ["80/tcp open (HTTP)", "443/tcp open (HTTPS)"],
        "mail.fictionalcorp.com": ["25/tcp open (SMTP)", "993/tcp open (IMAPS)"],
        "dev.fictionalcorp.com": ["22/tcp open (SSH)", "8080/tcp open (HTTP-alt)"],
        "vpn.fictionalcorp.com": ["443/tcp open (HTTPS)", "500/udp open (IKE)"]
    }
    with open(f"{OUTPUT_DIR}/active_recon.txt", "w") as f:
        for host, ports in scan_results.items():
            f.write(f"{host}:\n")
            for port in ports:
                f.write(f"  - {port}\n")
    return scan_results

def analyze_findings(scan_results):
    """Analyzes results and flags potential attack vectors."""
    weaknesses = []
    for host, ports in scan_results.items():
        for port in ports:
            if "22/tcp" in port:
                weaknesses.append(f"{host} - SSH exposed (check for weak credentials).")
            if "8080/tcp" in port:
                weaknesses.append(f"{host} - Dev server on port 8080 may be vulnerable.")
            if "25/tcp" in port:
                weaknesses.append(f"{host} - SMTP open (possible spam relay).")
    with open(f"{OUTPUT_DIR}/analysis.txt", "w") as f:
        for weak in weaknesses:
            f.write(weak + "\n")
    return weaknesses
```

```
# === MAIN ===
print(f"=== Reconnaissance Simulation for {TARGET_DOMAIN} ===")
subs = passive_recon(TARGET_DOMAIN)
print("[PASSIVE] Subdomains found:", subs)
scan_data = active_recon(subs)
print("[ACTIVE] Simulated port scan results:")
for host, ports in scan_data.items():
    print(f"  {host}: {ports}")
weak_points = analyze_findings(scan_data)
print("[ANALYSIS] Potential weaknesses:")
for w in weak_points:
    print("  -", w)
print(f"\n[INFO] Detailed results saved in '{OUTPUT_DIR}' folder.")
```

Explanation

1. passive_recon() — simulates passive discovery of subdomains (what tools like Amass or Subfinder do).
2. active_recon() — provides fake port/ service results to model an Nmap scan (safe simulation).
3. analyze_findings() — flags services commonly associated with attack vectors (SSH, dev ports, SMTP).
4. Output files are written to 'recon_results/' to mirror real engagement deliverables.
Safety note: Do NOT run network scanning tools against systems you do not own or are not authorized to test.

Example Output

```
=== Reconnaissance Simulation for fictionalcorp.com ===
[PASSIVE] Subdomains found: ['www.fictionalcorp.com', 'mail.fictionalcorp.com',
'dev.fictionalcorp.com', 'vpn.fictionalcorp.com']
[ACTIVE] Simulated port scan results:
  www.fictionalcorp.com: ['80/tcp open (HTTP)', '443/tcp open (HTTPS)']
  mail.fictionalcorp.com: ['25/tcp open (SMTP)', '993/tcp open (IMAPS)']
  dev.fictionalcorp.com: ['22/tcp open (SSH)', '8080/tcp open (HTTP-alt)']
  vpn.fictionalcorp.com: ['443/tcp open (HTTPS)', '500/udp open (IKE)']
[ANALYSIS] Potential weaknesses:
  - mail.fictionalcorp.com - SMTP open (possible spam relay).
  - dev.fictionalcorp.com - SSH exposed (check for weak credentials).
  - dev.fictionalcorp.com - Dev server on port 8080 may be vulnerable.
[INFO] Detailed results saved in 'recon_results' folder.
```