Lab01 Ethical Hacking

The task for the first lab was to gather information about a specified target using passive information gathering methods.

**Objectives included:**

* Learn to use passive recon tools
* Learn to gather information from openly available sources

**Scope:**

* Subdomain: wpk.tpu.fi
* All possible hosts of it \*.wpk.tpu.fi

**Tools and Methods:**

* Using only **passive** information gathering tools!
* Any tool or method that is suitable for **passive** recon.
* I chose several tools and methods that are listed below. There is also “Criticality-score” mentioned for each section.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Finding | Why important? | When found(date) | Tool/Method used | Criticality |
| 1. 7 hosts for wpk.tpu.fi | Narrowing the search | 25.1 | TheHarvester | High (Reveals network infrastructure and potential targets for attacks) |
| 2. SSL-certificates | Attacker can check for outdated SSL/TLS certificates | 25.1 | Crt.sh | Medium (Outdated certificates may lead to vulnerabilities, but not immediately critical for attack) |
| 3. Ip-address | Hacker can use IP-address to target an attack | 25.1 | TheHarvester | High (IP address is crucial for an attack) |
| 4. GeoLocations for wpk.tpu.fi’s IP address | Identifying geographical location helps plan physical attacks or determine origin of traffic | 25.1 | Censys/Shodan/ipinfo/curl | Medium (Geolocation helps identify the target but not directly for attacks) |
| 5. Email-address | Attacker can send malicious data to victim emails | 25.1 | TheHarvester | High (Phishing attacks are possible) |
| 6. Subdomains for tpu.fi and wpk.tpu.fi | Attacker can exploit data leaks from subdomains and find vulnerable systems | 25.1 | Sublist3r | High (Subdomains may reveal weak points or leaks) |
| 7. People | Attacker can use personal data for more aggressive attacks (phishing, social engineering) | 25.1 | Whois | High (Social engineering and attacks on personal data) |



  

