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

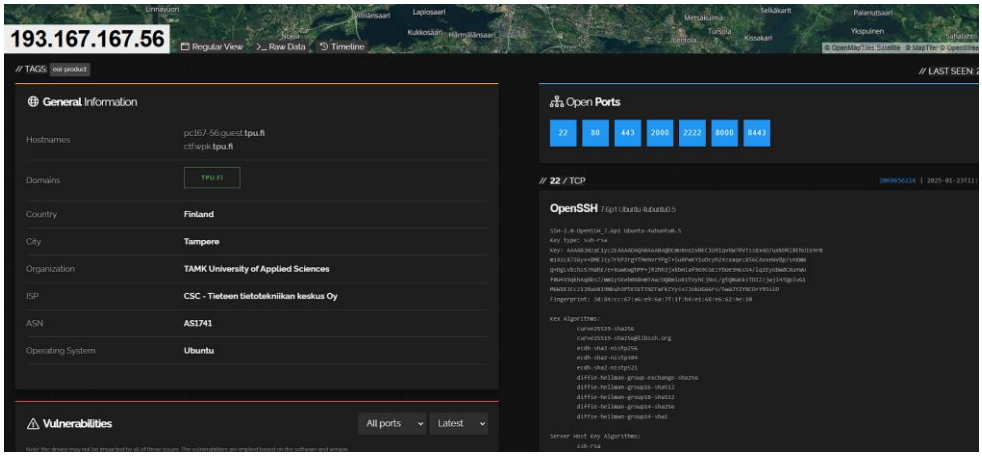
Scope:

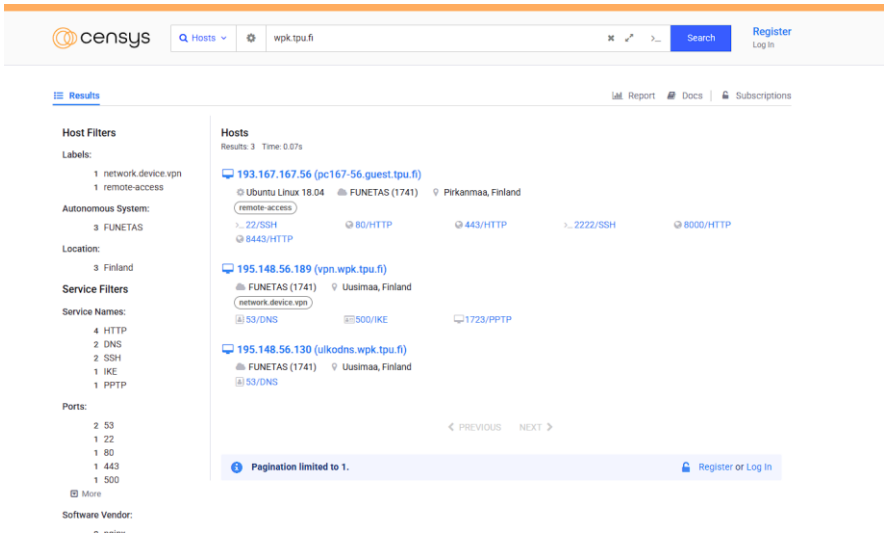
- Subdomain: wpk.tpu.fi
- All possible hosts of it *.wpk.tpu.fi

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 SSL-certificates	Attacker can check for outdated SSL/TLS certificates	25.1	Crt.sh	Medium (Outdated certificates may lead to vulnerabilities, but not immediately critical for attack)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)


193.167.167.56
Regular View
Raw Data
Timeline
TAGS
General Information
Hostnames
pc167-56.guest.tpu.fi
ctf.wpk.tpu.fi
Domains
TPU.FI
Country
Finland
City
Tampere
Organization
TAMK University of Applied Sciences
ISP
CSC - Tieteen tietotekniikan keskus Oy
ASN
AS1741
Operating System
Ubuntu
Vulnerabilities
All ports
Latest
Open Ports
22
80
443
2000
2222
8000
8443
22 / TCP
OpenSSH 7.6p1 Ubuntu-4ubuntu0.5


censys
Hosts
wpk.tpu.fi
Search
Register
Log In
Results
Report
Docs
Subscriptions
Host Filters
Labels:
1 network.device.vpn
1 remote-access
Autonomous System:
3 FUNETAS
Location:
3 Finland
Service Filters
Service Names:
4 HTTP
2 DNS
2 SSH
1 IKE
1 PPTP
Ports:
2 53
1 22
1 80
1 443
1 500
More
Software Vendor:
Hosts
Results: 3 Time: 0.07s
193.167.167.56 (pc167-56.guest.tpu.fi)
Ubuntu Linux 18.04
FUNETAS (1741)
Pirkanmaa, Finland
remote-access
22/SSH
80/HTTP
443/HTTP
2222/SSH
8000/HTTP
8443/HTTP
195.148.56.189 (vpn.wpk.tpu.fi)
FUNETAS (1741)
Uusimaa, Finland
network.device.vpn
53/DNS
500/IKE
1723/PPTP
195.148.56.130 (ulkodns.wpk.tpu.fi)
FUNETAS (1741)
Uusimaa, Finland
53/DNS
PREVIOUS
NEXT
Pagination limited to 1.
Register or Log In


kali@kali: ~
File Actions Edit View Help
└─$ sublist3r -d tpu.fi
Coded By Ahmed Aboul-Ela - @aboul3la
[-] Enumerating subdomains now for tpu.fi
[-] Searching now in Baidu..
[-] Searching now in Yahoo..
[-] Searching now in Google..
[-] Searching now in Bing..
[-] Searching now in Ask..
[-] Searching now in Netcraft..
[-] Searching now in DNSdumpster..
[-] Searching now in Virustotal..
[-] Searching now in ThreatCrowd..
[-] Searching now in SSL Certificates..
[-] Searching now in PassiveDNS..
[!] Error: Virustotal probably now is blocking our requests
Process DNSdumpster-8:
Traceback (most recent call last):
File "/usr/lib/python3.12/multiprocessing/process.py", line 314, in _bootstrap
self.run()
File "/usr/lib/python3/dist-packages/sublist3r.py", line 269, in run
domain_list = self.enumerate()
File "/usr/lib/python3/dist-packages/sublist3r.py", line 649, in enumerate
token = self.get_csrftoken(resp)
File "/usr/lib/python3/dist-packages/sublist3r.py", line 644, in get_csrftoken
token = csrf_regex.findall(resp)[0]
IndexError: list index out of range
[-] Total Unique Subdomains Found: 4
cal.tpu.fi
intra.tpu.fi
sync.tpu.fi
ctf.wpk.tpu.fi
┌──(kali㉿kali)-[~]
└─$

```
[*] LinkedIn Links found: 0
──────────────────────

[*] IPs found: 1
──────────────────────
193.167.167.56

[*] Emails found: 1
──────────────────────
helpdesk@wpk.tpu.fi

[*] Hosts found: 7
──────────────────────
ctf.wpk.tpu.fi
ctf.wpk.tpu.fi:193.167.167.56
pate.wpk.tpu.fi
ulkodns.wpk.tpu.fi
ulkodns.wpk.tpu.fi:195.148.56.130
vpn.wpk.tpu.fi
vpn.wpk.tpu.fi:195.148.56.189
```

```
┌──(kali㉿kali)-[~]
└─$ whois 193.167.167.56
% This is the RIPE Database query service.
% The objects are in RPSL format.
%
% The RIPE Database is subject to Terms and Conditions.
% See https://docs.db.ripe.net/terms-conditions.html

% Note: this output has been filtered.
%       To receive output for a database update, use the "-B" flag.

% Information related to '193.167.163.0 - 193.167.167.255'

% Abuse contact for '193.167.163.0 - 193.167.167.255' is 'abuse@tamk.fi'

inetnum:        193.167.163.0 - 193.167.167.255
netname:        TPU-WS-NET
descr:          TAMK University of Applied Sciences
descr:          Tampere, Finland
country:        FI
admin-c:        JS14064-RIPE
tech-c:         MJ68-RIPE
status:         ASSIGNED PA
mnt-by:         AS1741-MNT
mnt-lower:      AS1741-MNT
org:            ORG-TAMK1-RIPE
created:        1970-01-01T00:00:00Z
last-modified:  2015-01-21T12:56:11Z
source:         RIPE # Filtered

organisation:   ORG-TAMK1-RIPE
org-name:       Tampere University of Applied Sciences (TAMK)
org-type:       OTHER
address:        Kuntokatu 3
address:        FI-33520 Tampere
address:        Finland
abuse-c:        AR31320-RIPE
mnt-ref:        AS1741-MNT
mnt-by:         AS1741-MNT
created:        2015-01-21T12:47:35Z
last-modified:  2015-01-21T12:48:39Z
source:         RIPE # Filtered
```

```
┌──(kali㉿kali)-[~]
└─$ curl ipinfo.io/193.167.167.56
{
  "ip": "193.167.167.56",
  "hostname": "pc167-56.guest.tpu.fi",
  "city": "Tampere",
  "region": "Pirkanmaa",
  "country": "FI",
  "loc": "61.4991,23.7871",
  "org": "AS1741 CSC - Tieteen tietotekniikan keskus Oy",
  "postal": "33100",
  "timezone": "Europe/Helsinki",
  "readme": "https://ipinfo.io/missingauth"
}
```

crt.sh Identity Search

Group by Issuer

Criteria	Type: Identity Match: ILIKE Search: 'wpk.tpu.fi'

Certificates

crt.sh ID	Logged At ⇧	Not Before	Not After	Common Name	Matching Identities	Issuer Name
15517402185	2024-11-27	2024-11-27	2025-02-25	ctf.wpk.tpu.fi	ctf.wpk.tpu.fi	C=US, O=Let's Encrypt, CN=R10
15521992263	2024-11-27	2024-11-27	2025-02-25	ctf.wpk.tpu.fi	ctf.wpk.tpu.fi	C=US, O=Let's Encrypt, CN=R10
14711004267	2024-09-27	2024-09-27	2024-12-26	ctf.wpk.tpu.fi	ctf.wpk.tpu.fi	C=US, O=Let's Encrypt, CN=R10
14711001280	2024-09-27	2024-09-27	2024-12-26	ctf.wpk.tpu.fi	ctf.wpk.tpu.fi	C=US, O=Let's Encrypt, CN=R10
13939025687	2024-07-29	2024-07-29	2024-10-27	ctf.wpk.tpu.fi	ctf.wpk.tpu.fi	C=US, O=Let's Encrypt, CN=R10
13938508089	2024-07-29	2024-07-29	2024-10-27	ctf.wpk.tpu.fi	ctf.wpk.tpu.fi	C=US, O=Let's Encrypt, CN=R10
12965488312	2024-05-06	2024-05-06	2024-08-04	ctf.wpk.tpu.fi	ctf.wpk.tpu.fi	C=US, O=Let's Encrypt, CN=R3
12965483518	2024-05-06	2024-05-06	2024-08-04	ctf.wpk.tpu.fi	ctf.wpk.tpu.fi	C=US, O=Let's Encrypt, CN=R3
12296759346	2024-03-06	2024-03-06	2024-06-04	ctf.wpk.tpu.fi	ctf.wpk.tpu.fi	C=US, O=Let's Encrypt, CN=R3
12296757336	2024-03-06	2024-03-06	2024-06-04	ctf.wpk.tpu.fi	ctf.wpk.tpu.fi	C=US, O=Let's Encrypt, CN=R3
11657652007	2024-01-06	2024-01-06	2024-04-05	ctf.wpk.tpu.fi	ctf.wpk.tpu.fi	C=US, O=Let's Encrypt, CN=R3
11657647587	2024-01-06	2024-01-06	2024-04-05	ctf.wpk.tpu.fi	ctf.wpk.tpu.fi	C=US, O=Let's Encrypt, CN=R3
11024493465	2023-11-07	2023-11-07	2024-02-05	ctf.wpk.tpu.fi	ctf.wpk.tpu.fi	C=US, O=Let's Encrypt, CN=R3
11024487128	2023-11-07	2023-11-07	2024-02-05	ctf.wpk.tpu.fi	ctf.wpk.tpu.fi	C=US, O=Let's Encrypt, CN=R3