Lab 1 - CTF.WPK.TPU.FI

Passive recon tools used

Lab 1 - CTF.WPK.TPU.FI
- Nslookup
- Whois
- Dig
- Spiderfoot
- Recon-ng
- Enumeration
- Shodan
- TLDR

Nslookup

The nslookup tool was able to find ip address for the target ctf.wpk.tpu.fi and also some information about mail servers

```
┌──(kali㉿Kali)-[~]
└─$ nslookup ctf.wpk.tpu.fi
Server:         192.168.1.1
Address:        192.168.1.1#53

Non-authoritative answer:
Name:   ctf.wpk.tpu.fi
Address: 193.167.167.56
```

Name server lookup

```
┌──(kali㉿Kali)-[~]
└─$ nslookup -q=ns ctf.wpk.tpu.fi
Server:         192.168.1.1
Address:        192.168.1.1#53

Non-authoritative answer:
*** Can't find ctf.wpk.tpu.fi: No answer
```

Authoritative answers can be found from:
wpk.tpu.fi
origin = **ulkodns.wpk.tpu.fi**
mail addr = **hostmaster.wpk.tpu.fi**
serial = 235
refresh = 900
retry = 600
expire = 86400
minimum = 3600

Reverse nslookup
```
┌──(kali㉿Kali)-[~]
└─$ nslookup 193.167.167.56
```
56.167.167.193.in-addr.arpa name = **pc167-56.guest.tpu.fi.**

Whois

From whois more information like the country and and address of the target were discovered along with 2 people who are in charge of the target.

inetnum: **193.167.163.0 - 193.167.167.255**
netname: TPU-WS-NET
descr: TAMK University of Applied Sciences
descr: Tampere, Finland
country: FI

organisation: ORG-TAMK1-RIPE
org-name: Tampere University of Applied Sciences (TAMK)
org-type: OTHER
address: Kuntokatu 3
address: FI-33520 Tampere
address: Finland

person: **Jarmo Sorvari**
address: TAMK University of Applied Sciences
address: Kuntokatu 3
address: FI-33520 Tampere
address: FINLAND
phone: +358 3 254 2111
fax-no: +358 3 254 2222

person: **Marko Jauhiainen**

```
address:        TAMK University of Applied Sciences
address:        Kuntokatu 3
address:        FI-33520 Tampere
address:        Finland
phone:          +358 3 245 2111
fax-no:         +358 3 245 2222
% Information related to '193.166.0.0/15AS1741'

route:          193.166.0.0/15
descr:          FUNET-BLOCK
origin:         AS1741
mnt-by:         AS1741-MNT
created:        1970-01-01T00:00:00Z
last-modified:  2001-09-22T09:33:14Z
source:         RIPE # Filtered
```

Dig

Dig returned similar ip address thus confirming nslookup

```
┌──(kali㉿Kali)-[~]
└─$ dig ctf.wpk.tpu.fi

;; ANSWER SECTION:
ctf.wpk.tpu.fi.         3600    IN      A       193.167.167.56
```

Reverse dns lookup

```
;; QUESTION SECTION:
;56.167.167.193.in-addr.arpa.   IN      PTR

;; ANSWER SECTION:
56.167.167.193.in-addr.arpa. 8942 IN    PTR     pc167-56.guest.tpu.fi.
```

Spiderfoot

Running all passive scan on spiderfoot gave a lot of information which is exported to this csv sheet -

https://docs.google.com/spreadsheets/d/1S9EpHJaY28DTPb7X6ZYP7XPjdcEPiGPNzAjB3Glzg0s/edit#gid=2042033834

Updated	Type	Module	Source	F/P	Data	
2023-10-20 7:39:36	AFFILIATE_IPADDR	sfp_dnsresolve	ns-secondary.funet.fi	0	128.214.248.132	
2023-10-20 7:39:09	BGP_AS_MEMBER	sfp_ripe	193.166.0.0/15	0	1741	
2023-10-20 7:38:57	BGP_AS_MEMBER	sfp_bgpview	193.167.167.56	0	1741	
2023-10-20 7:38:54	NETBLOCK_MEMBER	sfp_ripe	193.167.167.56	0	193.166.0.0/15	
2023-10-20 7:38:57	NETBLOCK_MEMBER	sfp_bgpview	193.167.167.56	0	193.166.0.0/15	
2023-10-20 7:39:34	AFFILIATE_IPADDR	sfp_dnsresolve	mail1.tuni.fi	0	193.166.164.156	
2023-10-20 7:39:22	AFFILIATE_IPADDR	sfp_dnsresolve	mail.tuni.fi	0	193.166.164.156	
2023-10-20 7:39:22	AFFILIATE_IPADDR	sfp_dnsresolve	mail.tuni.fi	0	193.166.164.157	
2023-10-20 7:39:30	AFFILIATE_IPADDR	sfp_dnsresolve	mail2.tuni.fi	0	193.166.164.157	
2023-10-20 7:39:21	AFFILIATE_IPADDR	sfp_dnsresolve	ns1.tuni.fi	0	193.166.164.164	
2023-10-20 7:39:39	AFFILIATE_IPADDR	sfp_dnsresolve	ns2.tuni.fi	0	193.166.164.165	
2023-10-20 7:38:36	IP_ADDRESS	sfp_dnsresolve	ctf.wpk.tpu.fi	0	193.167.167.56	
2023-10-20 7:39:36	AFFILIATE_IPV6_ADDRESS	sfp_dnsresolve	ns-secondary.funet.fi	0	2001:708:10:55::53	

Recon-ng

With recon-ng I was able to find more hostnames and even some exposed services via the modules hackertarget and shodan_net

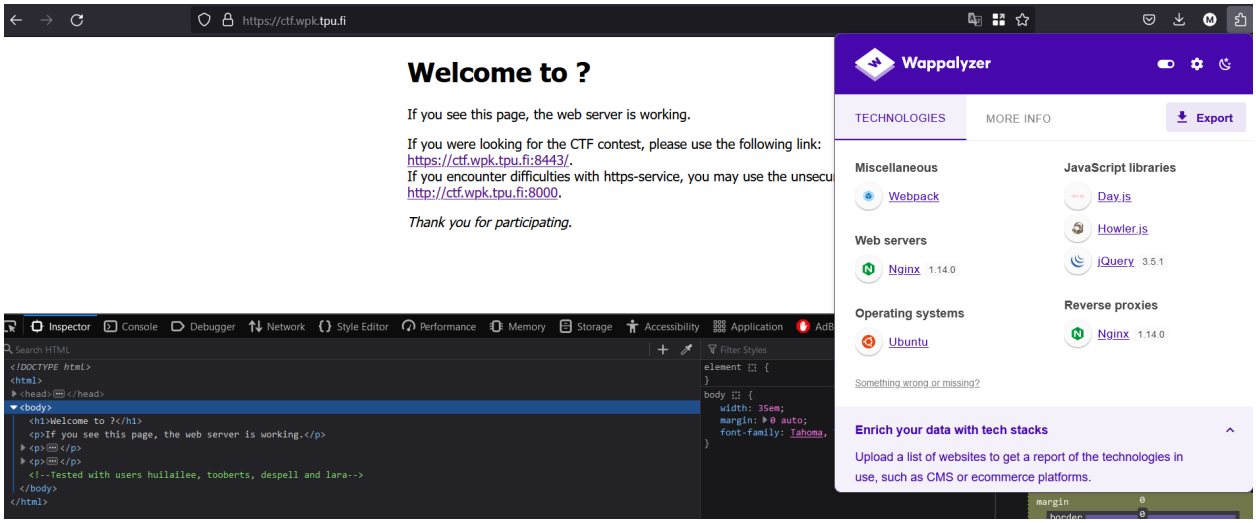
```
[recon-ng][L1-ctf.wpk][shodan_hostname] > db
delete  insert  notes   query   schema
[recon-ng][L1-ctf.wpk][shodan_hostname] > show ports

  +-----------------------------------------------------------------------------------------------------+
  | rowid |   ip_address    |          host          | port | protocol | banner | notes |      module      |
  +-----------------------------------------------------------------------------------------------------+
  | 1     | 193.167.167.56 | pc167-56.guest.tpu.fi | 8443 | tcp      |        |       | shodan_hostname |
  | 2     | 193.167.167.56 | ctf.wpk.tpu.fi        | 8443 | tcp      |        |       | shodan_hostname |
  | 3     | 193.167.167.56 | pc167-56.guest.tpu.fi | 443  | tcp      |        |       | shodan_hostname |
  | 4     | 193.167.167.56 | ctf.wpk.tpu.fi        | 443  | tcp      |        |       | shodan_hostname |
  +-----------------------------------------------------------------------------------------------------+
```

Enumeration

This led to the webserver running on target where I could find leaked usernames(?) in the comments on the html page.

Also some info about the webserver running what web stack from Wappalyzer.



Shodan

Open ports and vulnerabilities from shodan web

Open Ports

22 80 443 2000 2222 8000 8443

Vulnerabilities

Note: the device may not be impacted by all of these issues. The vulnerabilities are implied based on the software and version.

CVE-2021-3618 5.8 ALPACA is an application layer protocol content confusion attack, exploiting TLS servers implementing different protocols but using compatible certificates, such as multi-domain or wildcard certificates. A MiTM attacker having access to victim's traffic at the TCP/IP layer can redirect traffic from one subdomain to another, resulting in a valid TLS session. This breaks the authentication of TLS and cross-protocol attacks may be possible where the behavior of one protocol service may compromise the other at the application layer.

CVE-2019-20372	4.3 NGINX before 1.17.7, with certain error_page configurations, allows HTTP request smuggling, as demonstrated by the ability of an attacker to read unauthorized web pages in environments where NGINX is being fronted by a load balancer.
CVE-2018-16845	5.8 nginx before versions 1.15.6, 1.14.1 has a vulnerability in the ngx_http_mp4_module, which might allow an attacker to cause infinite loop in a worker process, cause a worker process crash, or might result in worker process memory disclosure by using a specially crafted mp4 file. The issue only affects nginx if it is built with the ngx_http_mp4_module (the module is not built by default) and the .mp4. directive is used in the configuration file. Further, the attack is only possible if an attacker is able to trigger processing of a specially crafted mp4 file with the ngx_http_mp4_module.
CVE-2018-16844	7.8 nginx before versions 1.15.6 and 1.14.1 has a vulnerability in the implementation of HTTP/2 that can allow for excessive CPU usage. This issue affects nginx compiled with the ngx_http_v2_module (not compiled by default) if the 'http2' option of the 'listen' directive is used in a configuration file.
CVE-2018-16843	7.8 nginx before versions 1.15.6 and 1.14.1 has a vulnerability in the implementation of HTTP/2 that can allow for excessive memory consumption. This issue affects nginx compiled with the ngx_http_v2_module (not compiled by default) if the 'http2' option of the 'listen' directive is used in a configuration file.

TLDR

Crucial information that was found from passive recon

Target IP - 193.167.167.56
IP range - **193.167.163.0 - 193.167.167.255**
People of interest - **Jarmo Sorvari** and **Marko Jauhiainen**
Email from Hunter.io

Target is running a webserver which hosts ctf competition - needs credentials and registration code to look further in
Webserver is nginx

Browse / Web Server

	Data Element	Sou
	gunicorn/20.0.4	{" t- 69
	nginx/1.14.0 (Ubuntu)	{" "I e"

(May have been done by active scan on spiderfoot :D)

SSH is open on 22 and 2222 port