Lab 2 - CTF.WPK.TPU.FI and IP range

Active Recon tools used

Nmap, shodan, spiderfoot, recon-ng, google, dirbuster, ffuf, gobuster?

NMAP

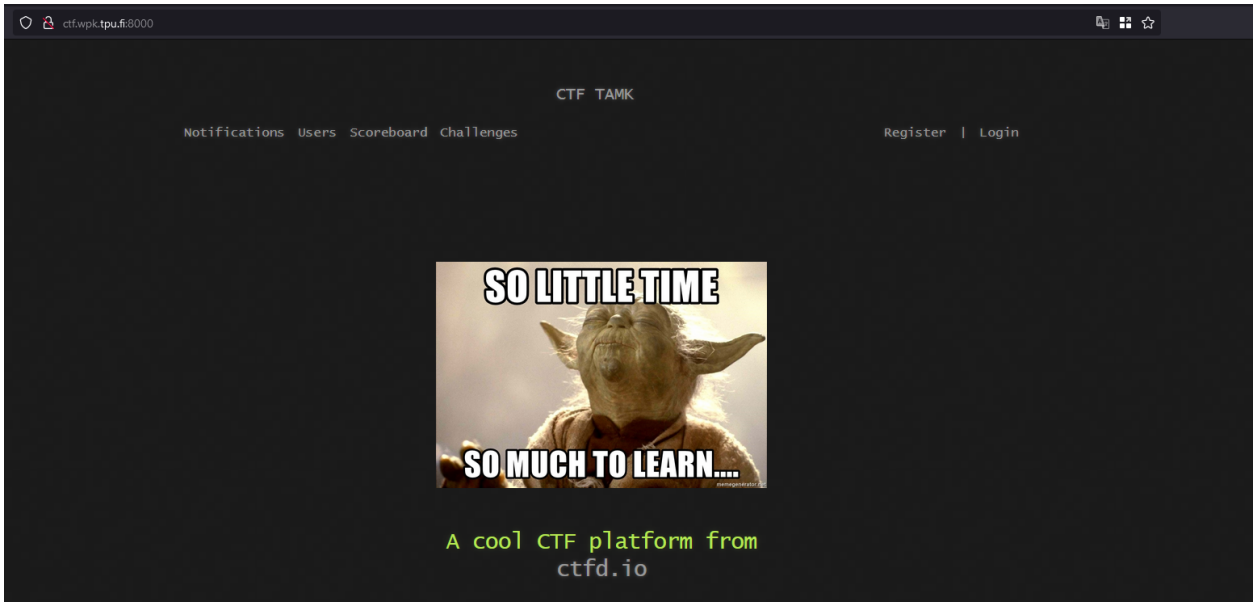
Target - 193.167.167.56

Our target ctf.wpk.tpu.fi has the public IP - 193.167.167.56 which we found from passive recon in the last lab, running nmap on target
Command - nmap -sV -sC -oA lab2_scan.txt -p- 193.167.167.56
sV - Version detection
sC - Run basic nmap scripts for well known vulnerabilities
oA - output file name
-p- scan all ports not just the top 1000

```
PORT     STATE    SERVICE    VERSION
22/tcp   open     ssh        OpenSSH 7.6p1 Ubuntu 4ubuntu0.5 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 3d:84:cc:67:a6:e9:6a:7f:1f:b4:e1:68:e6:62:4e:10 (RSA)
|   256 03:e2:28:46:ac:e7:b0:f7:91:3e:0d:d0:6a:51:46:a3 (ECDSA)
|_  256 b8:9c:95:c6:8c:5a:c6:ac:20:f5:74:da:eb:db:ad:cc (ED25519)
25/tcp   filtered smtp
80/tcp   open     http       nginx 1.14.0 (Ubuntu)
|_http-server-header: nginx/1.14.0 (Ubuntu)
|_http-title: Welcome to ?
443/tcp  open     ssl/http   nginx 1.14.0 (Ubuntu)
|_ssl-date: TLS randomness does not represent time
|_http-server-header: nginx/1.14.0 (Ubuntu)
|_http-title: Welcome to ?
| ssl-cert: Subject: commonName=ctf.wpk.tpu.fi
| Subject Alternative Name: DNS:ctf.wpk.tpu.fi
| Not valid before: 2023-09-07T17:40:30
|_Not valid after:  2023-12-06T17:40:29
2000/tcp open     tcpwrapped
2222/tcp open     ssh        OpenSSH 7.6p1 Ubuntu 4ubuntu0.5 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 3d:84:cc:67:a6:e9:6a:7f:1f:b4:e1:68:e6:62:4e:10 (RSA)
|   256 03:e2:28:46:ac:e7:b0:f7:91:3e:0d:d0:6a:51:46:a3 (ECDSA)
|_  256 b8:9c:95:c6:8c:5a:c6:ac:20:f5:74:da:eb:db:ad:cc (ED25519)
5060/tcp open     tcpwrapped
8000/tcp open     tcpwrapped
|_http-server-header: gunicorn/20.0.4
|_http-title: CTF TAMK
8443/tcp open     ssl/http   nginx 1.17.10
|_ssl-date: TLS randomness does not represent time
| tls-alpn:
|_  http/1.1
|_http-server-header: nginx/1.17.10
| tls-nextprotoneg:
|_  http/1.1
| ssl-cert: Subject: commonName=ctf.wpk.tpu.fi
| Subject Alternative Name: DNS:ctf.wpk.tpu.fi
| Not valid before: 2023-03-11T08:27:29
|_Not valid after:  2023-06-09T08:27:28
|_http-title: CTF TAMK
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

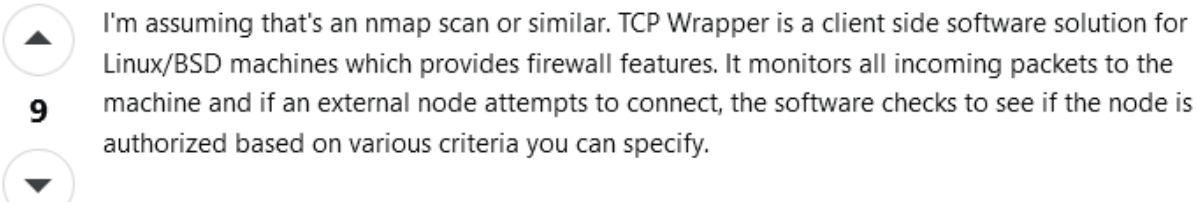
From the nmap result we can gather the info that

Port **22 and 2222 have SSH running** which also gives us some OS info that the target is probably running **Ubuntu**
We already found out the nginx webserver running on port 80, 443 in the last lab and now we know its version 1.14.0 (also already known)
Webserver on 8000 and 8443 is the one that hosts the ctf



Funny meme on the page - probably nothing to look at (heh)

There are however a couple of ports with tcpwrapper Service which looks interesting
From a quick google and stackoverflow answers it looks like there is some firewall preventing service detection for these ports



https://superuser.com/questions/84421/what-does-it-mean-when-a-portscan-shows-a-port-as-tcpwrapped

Well we can still work some nmap magic

```
┌──(kali㉿Kali)-[~/Templates/ethical-hacking]
└─$ sudo nmap -sF -p 2000,5060,8000 -T1  193.167.167.56
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-24 16:08 UTC
Nmap scan report for pc167-56.guest.tpu.fi (193.167.167.56)
Host is up (0.11s latency).

PORT     STATE         SERVICE
2000/tcp open|filtered cisco-sccp
5060/tcp open|filtered sip
8000/tcp open|filtered http-alt

Nmap done: 1 IP address (1 host up) scanned in 121.36 seconds
```

So
2000 is running some cisco service it is used for VoIP
5060 is running sip ; now what is SIP

8000 is running http-alt which is just redirecting the http server.

Running nmap on the IP range given

First we do host enumeration to find out what devices are online and using this IP range

```
# Nmap 7.94 scan initiated Tue Oct 24 09:22:41 2023 as: nmap -sn -oN lab2_host_discovery.txt 195.148.56.130-190
Nmap scan report for pc56-137.tpu.fi (195.148.56.137)
Host is up (0.013s latency).
Nmap scan report for pc56-151.tpu.fi (195.148.56.151)
Host is up (0.011s latency).
Nmap scan report for pc56-154.tpu.fi (195.148.56.154)
Host is up (0.010s latency).
# Nmap done at Tue Oct 24 09:22:42 2023 -- 61 IP addresses (3 hosts up) scanned in 1.73 seconds
```

So we get 3 hits ie 3 servers in this IP range

195.148.56.137	pc56-137.tpu.fi

195.148.56.151	pc56-151.tpu.fi
195.148.56.154	pc56-154.tpu.fi

Running nmap on all 3 of them one by one

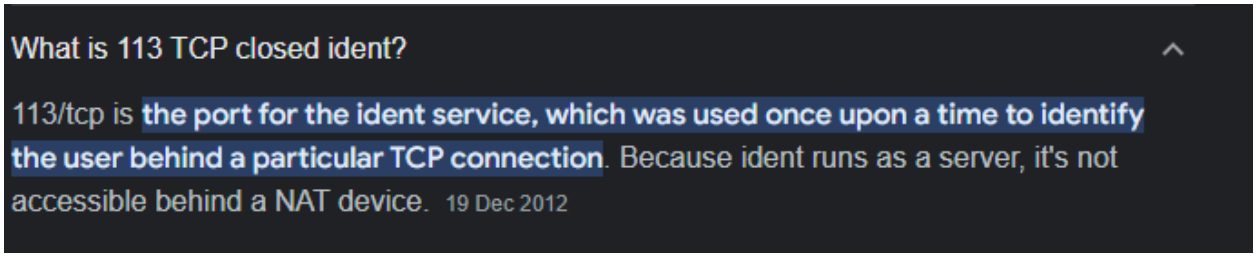
Host 1 - 195.148.56.137

Nothing special there just a port 22 for SSH

```
# Nmap 7.94 scan initiated Tue Oct 24 14:17:40 2023 as: nmap -sV -sC -p- -O -oN nmap_scans/lab2_host1_scan.txt 195.148.56.137
Nmap scan report for pc56-137.tpu.fi (195.148.56.137)
Host is up (0.0094s latency).
Not shown: 65039 filtered tcp ports (no-response), 495 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 6.0p1 Debian 4+deb7u2 (protocol 2.0)
| ssh-hostkey:
|   2048 ab:40:0c:24:48:57:f6:66:5c:fd:45:23:55:bd:9e:21 (RSA)
|   256 ea:46:34:0a:3b:78:a9:5f:55:c7:4d:76:95:3f:78:68 (ECDSA)
|_  256 c3:24:29:0c:6f:93:1c:93:86:2b:e0:bb:3a:7c:d8:74 (ED25519)
Device type: general purpose
Running (JUST GUESSING): Linux 4.X|2.6.X|3.X (91%)
OS CPE: cpe:/o:linux:linux_kernel:4.0 cpe:/o:linux:linux_kernel:2.6.32 cpe:/o:linux:linux_kernel:3.10
Aggressive OS guesses: Linux 4.0 (91%), Linux 2.6.32 (89%), Linux 4.4 (89%), Linux 2.6.32 or 3.10 (87%), Linux 2.6.32 - 2.6.35 (86%), Linux 2.6.32 - 2.6.39 (85%
)
No exact OS matches for host (test conditions non-ideal).
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Host 2 - 195.148.56.151

Not much here either except port 443 configured for SSL from the looks of it and port 113 which is closed but a quick google says that



```
# Nmap 7.94 scan initiated Tue Oct 24 14:25:22 2023 as: nmap -sV -sC -p- -O -oN nmap_scans/lab2_host2_scan.txt 195.148.56.151
Nmap scan report for pc56-151.tpu.fi (195.148.56.151)
Host is up (0.0089s latency).
Not shown: 65533 filtered tcp ports (no-response)
PORT    STATE  SERVICE   VERSION
113/tcp closed ident
443/tcp open   ssl/https
| ssl-cert: Subject: commonName=terasmies-rzggzkpjdv.dynamic-m.com/organizationName=Cisco Systems Inc./stateOrProvinceName=California/countryName=US
| Subject Alternative Name: DNS:terasmies-rzggzkpjdv.dynamic-m.com
| Not valid before: 2023-09-14T20:38:34
|_Not valid after:  2023-12-13T20:37:34
|_http-title: Site doesn't have a title (text/html).
| fingerprint-strings:
|   FourOhFourRequest:
|     HTTP/1.0 200 OK
|     Content-Type: text/html
|     Cache-Control: no-cache
|     Pragma: no-cache
|     Connection: Keep-Alive
|     Date: Tue, 24 Oct 2023 14:27:34 GMT
|     X-Frame-Options: SAMEORIGIN
|     X-Transcend-Version:1
|     Strict-Transport-Security: max-age=31536000; includeSubDomains
|     X-Content-Type-Options: nosniff
|     X-XSS-Protection: 1; mode=block
|   GetRequest:
|     HTTP/1.0 200 OK
|     Content-Type: text/html
|     Cache-Control: no-cache
|     Pragma: no-cache
|     Connection: Keep-Alive
|     Date: Tue, 24 Oct 2023 14:27:28 GMT
|     X-Frame-Options: SAMEORIGIN
|     X-Transcend-Version:1
|     Strict-Transport-Security: max-age=31536000; includeSubDomains
|     X-Content-Type-Options: nosniff
|_    X-XSS-Protection: 1; mode=block
```

And finally

Host 3 - 195.148.56.154

Finally some services to look into!
We have
21 FTP but no anonymous login because -sC checks for that

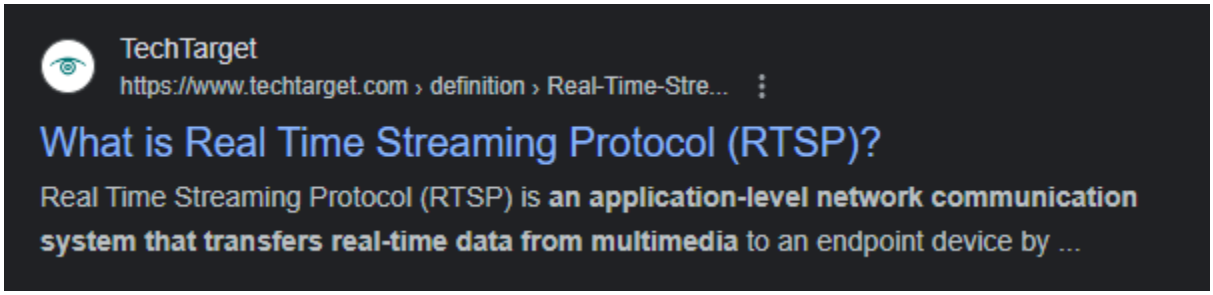
Tried some basic username:passwd combos and **root** is a valid username but lets see about password soon.

```
┌──(kali㉿Kali)-[~/ethical-hacking]
└─$ ftp 195.148.56.154
Connected to 195.148.56.154.
220 AXIS M1011-W Network Camera 5.20.1 (Oct 25 2010) ready.
Name (195.148.56.154:kali): root
331 User name okay, need password.
Password:
530 Login incorrect.
ftp: Login failed
ftp>
```

Additional info from shodan

23 Telnet but its filtered so not sure if its up and running
25 smtp also filtered
80 **http** With a robots.txt disallowing all user agents
554 rtsp Looks like its some service for a camera

```
# Nmap 7.94 scan initiated Tue Oct 24 14:30:07 2023 as: nmap -sV -sC -p- -O -oN nmap_scans/lab2_host3_scan.txt 195.148.56.154
Nmap scan report for pc56-154.tpu.fi (195.148.56.154)
Host is up (0.012s latency).
Not shown: 65530 closed tcp ports (reset)
PORT    STATE    SERVICE VERSION
21/tcp  open     ftp     Axis M1011-W Network Camera ftpd 5.20.1 (Oct 25 2010)
23/tcp  filtered telnet
25/tcp  filtered smtp
80/tcp  open     http    Boa httpd
| http-robots.txt: 1 disallowed entry
|_/
|_http-title: Index page
554/tcp open     rtsp    Axis M1054 or P3364 Network Camera rtspd
|_rtsp-methods: DESCRIBE, GET_PARAMETER, PAUSE, PLAY, SETUP, SET_PARAMETER, TEARDOWN
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.32 - 2.6.33
Network Distance: 14 hops
Service Info: Device: webcam; CPE: cpe:/h:axis:m1011-w_network_camera
```



RTSP is a streaming protocol so the Network camera probably streams using this port
And we also get supported methods for the rtsp protocol

|_rtsp-methods: DESCRIBE, GET_PARAMETER, PAUSE, PLAY, SETUP, SET_PARAMETER, TEARDOWN

So we already have quite a lot of info for all the devices but lets look deeper into these webservers and try some enumeration for them.

Spiderfoot

This time running spiderfoot with Footprint option reveals a lot of information but most of it is what we have already gathered, still spiderfoot provides it in a better tabular form.

Type	Unique Data Elements	Total Data Elements	Last Data Element
Affiliate - Domain Name	3	9	2023-10-24 16:14:53
Affiliate - Email Address	4	5	2023-10-24 16:14:47
Affiliate - IP Address	20	22	2023-10-24 16:14:53
Affiliate - IPv6 Address	1	1	2023-10-24 16:14:51
Affiliate - Internet Name	21	27	2023-10-24 16:14:57
BGP AS Membership	1	2	2023-10-24 16:14:04
Co-Hosted Site	1	1	2023-10-24 16:13:08
Co-Hosted Site - Domain Name	1	1	2023-10-24 16:14:47
Country Name	1	5	2023-10-24 16:14:52
DNS SPF Record	1	1	2023-10-24 16:13:57
DNS TXT Record	1	1	2023-10-24 16:13:57
Domain Name (Parent)	1	1	2023-10-24 16:11:27
Email Gateway (DNS MX Records)	3	3	2023-10-24 16:13:57

<and so on CSV file can be requested if needed>

Disbuster

Running dirbuster on ctf.wpk.tpu.fi

```
DirBuster 1.0-RC1 - Report
http://www.owasp.org/index.php/Category:OWASP_DirBuster_Project
Report produced on Tue Oct 24 15:16:34 UTC 2023
--------------------------------

http://ctf.wpk.tpu.fi:8000
--------------------------------
Directories found during testing:

Dirs found with a 200 response:

/

Dirs found with a 301 response:

/files/
/files/bacee6dbbac752c2ebc9663a6a7d530f/
/themes/
/themes/hacker-theme/
/themes/hacker-theme/static/
/themes/hacker-theme/static/js/
/themes/hacker-theme/static/js/pages/


--------------------------------
Files found during testing:

Files found with a 301 responce:

/notifications
/users
/scoreboard
/challenges
/register
/login
/themes/hacker-theme/static/js/vendor.bundle.min.js
/themes/hacker-theme/static/js/core.min.js
/themes/hacker-theme/static/js/helpers.min.js
/themes/hacker-theme/static/js/pages/main.min.js


--------------------------------
```

Also running dirbuster on Host 3

DirBusterReport-195.148.56.154-80.txt

```
SDirBuster 1.0-RC1 - Report
http://www.owasp.org/index.php/Category:OWASP_DirBuster_Project
Report produced on Tue Oct 24 20:28:50 UTC 2023
--------------------------------

http://195.148.56.154:80
--------------------------------
Directories found during testing:

Dirs found with a 200 response:

/
/view/
/admin/
/view/view/

Dirs found with a 401 response:

/help/
/view/help/
/admin/help/

Dirs found with a 403 response:

/pub/
/pics/
/view/pub/


--------------------------------
--------------------------------
```

Dirbuster wasnt able to find much but we still get some idea about the dir layout of the webservers.

Tried running FFUF too but the list was too big and taking too long, need to learn more about those tools.

GVM

Vulnerability		Severity ▼	QoD	Host	
				IP	Name
Missing 'Secure' Cookie Attribute (HTTP)		6.4 (Medium)	80 %	193.167.167.56	pc167-56.guest.tpu.fi

Summary

The remote HTTP web server / application is missing to set the 'Secure' cookie attribute for one or more sent HTTP cookie.

Detection Result

```
The cookies:

Set-Cookie: session=09966919-754b-447a-8091-2b9992ffe8ff.QgvA-nzQoSseLnS21fSWc59LxYY; HttpOnly; Path=/; SameSite=Lax

are missing the "Secure" cookie attribute.
```

Insight

The flaw exists if a cookie is not using the 'Secure' cookie attribute and is sent over a SSL/TLS connection.

This allows a cookie to be passed to the server by the client over non-secure channels (HTTP) and subsequently allows an attacker to e.g. conduct session hijacking attacks.

Detection Method

Checks all cookies sent by the remote HTTP web server / application over a SSL/TLS connection for a missing 'Secure' cookie attribute.

Details: Missing 'Secure' Cookie Attribute (HTTP) OID: 1.3.6.1.4.1.25623.1.0.902661

Version used: 2023-01-17T10:10:58Z

GVM found a couple of vulns for ctf.wpk.tpu.fi

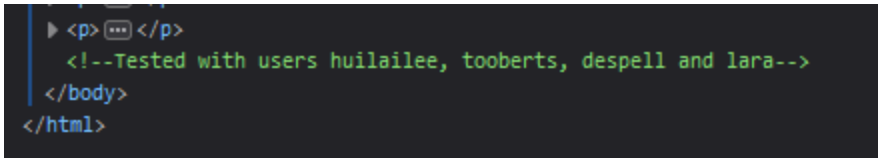
Vulnerability		Severity ▼
Missing 'Secure' Cookie Attribute (HTTP)		6.4 (Medium)
Missing 'Secure' Cookie Attribute (HTTP)		6.4 (Medium)
SSL/TLS: Certificate Expired		5.0 (Medium)
SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection		4.3 (Medium)
TCP Timestamps Information Disclosure		2.6 (Low)
ICMP Timestamp Reply Information Disclosure		2.1 (Low)

(Applied filter: apply_overrides=0 levels=hml rows=100 min_qod=70 first=1 sort-reverse=severity)

Nothing too fancy here maybe needs more investigation

Lab3 Info gathered and Lab2 reflection

Facts -
We know there is an image on ctf.wpk.tpu.fi that has some a base64 comment from exiftool and one file embedded in it from steghide
We know the webserver on host3 has basic http auth which can be brute forced using the combinations of usernames from ctf.wpk.tpu.fi nginx page and the finnish song names Kisu, Sisu, Visu, Misu,
The topsecretfile.txt had some more info
But there are still different usernames from the comments here



Thoughts
Maybe used somewhere else hmm
We know theres FTP running and also ssh on port 2222 which means theres more to discover still. First try after http auth would be to see if reused credentials.
Could also think about box usernames enumeration.
Also didnt use a lot of nmap script just rolled with -sC so maybe theres something to find there although i think not.

Overall lab went okay feel like i have all the info needed but the attack surface feels quite distributed, dont know which server to actually target. Host 3 is priority for now.