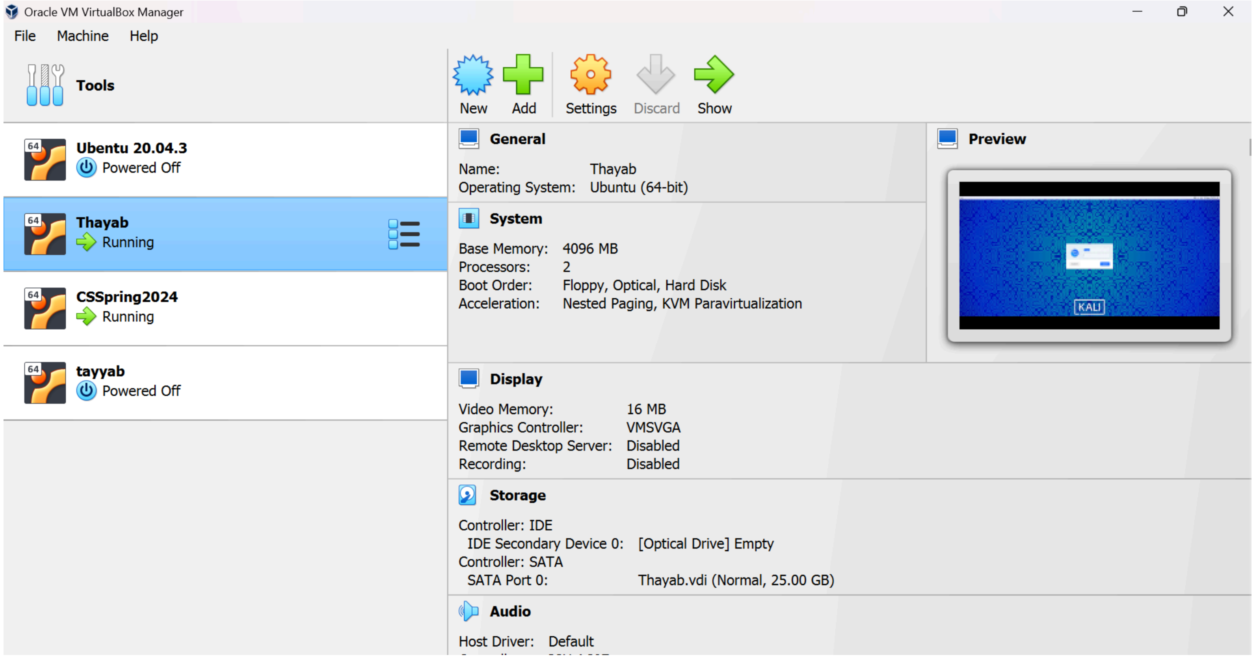
Tayyab Nadeem
21L-5830

Information Security Assignment # 1

1 Screenshot of VirtualBox after adding both VMs:



Ubuntu 20.04.3
Powered Off

Thayab
Running

CSSpring2024
Running

tayyab
Powered Off

General

Name: Thayab
Operating System: Ubuntu (64-bit)

System

Base Memory: 4096 MB
Processors: 2
Boot Order: Floppy, Optical, Hard Disk
Acceleration: Nested Paging, KVM Paravirtualization

Display

Video Memory: 16 MB
Graphics Controller: VMSVGA
Remote Desktop Server: Disabled
Recording: Disabled

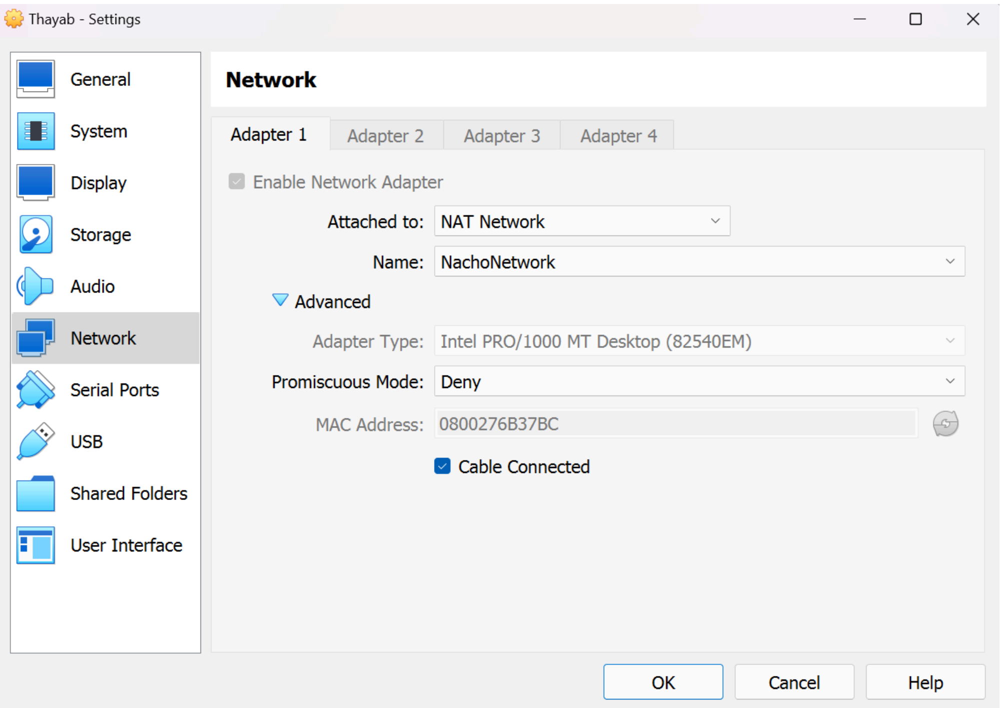
Storage

Controller: IDE
IDE Secondary Device 0: [Optical Drive] Empty
Controller: SATA
SATA Port 0: Thayab.vdi (Normal, 25.00 GB)

Audio

Host Driver: Default

After running the `sudo netdiscover` command in the VM, I checked the MAC address and compared it with the one found in the CSSpringFile.



Network

☑ Enable Network Adapter

Attached to: NAT Network

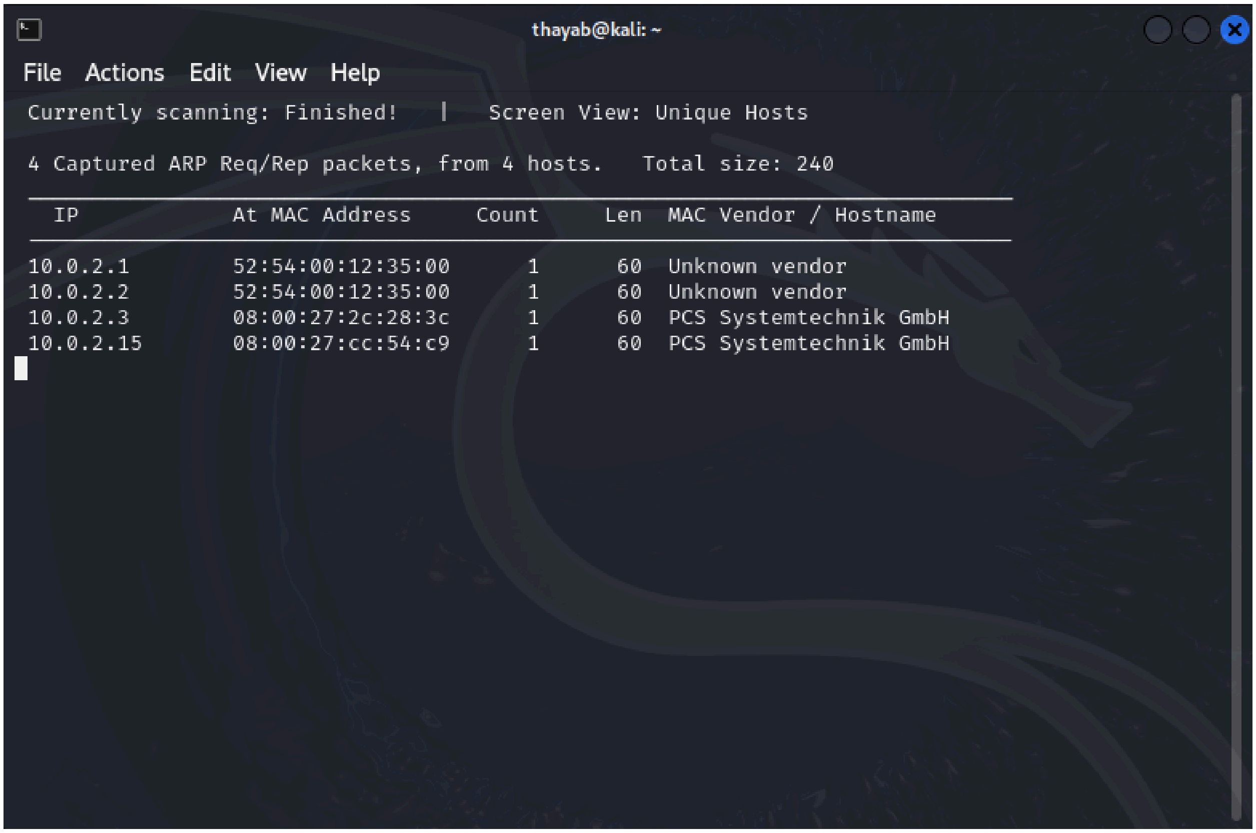
Name: NachoNetwork

Adapter Type: Intel PRO/1000 MT Desktop (82540EM)

Promiscuous Mode: Deny

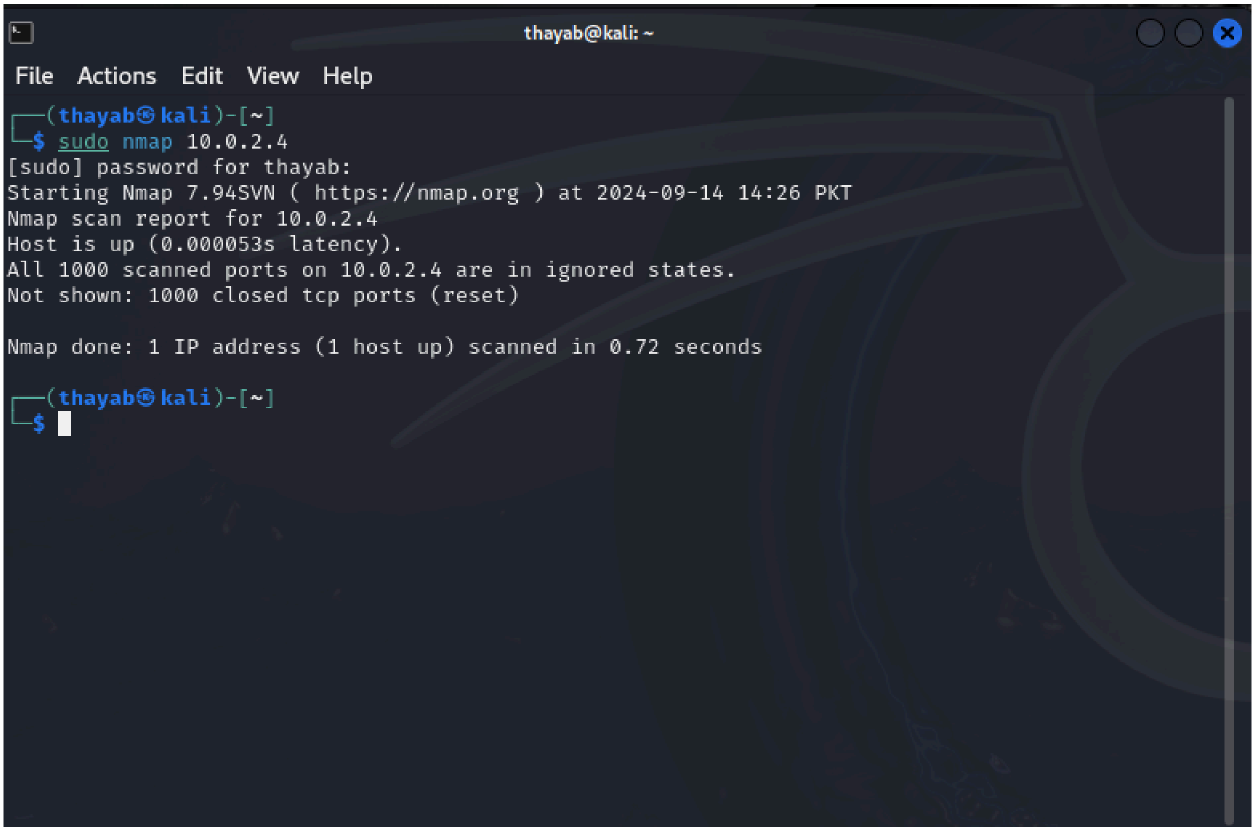
MAC Address: 0800276B37BC

☑ Cable Connected



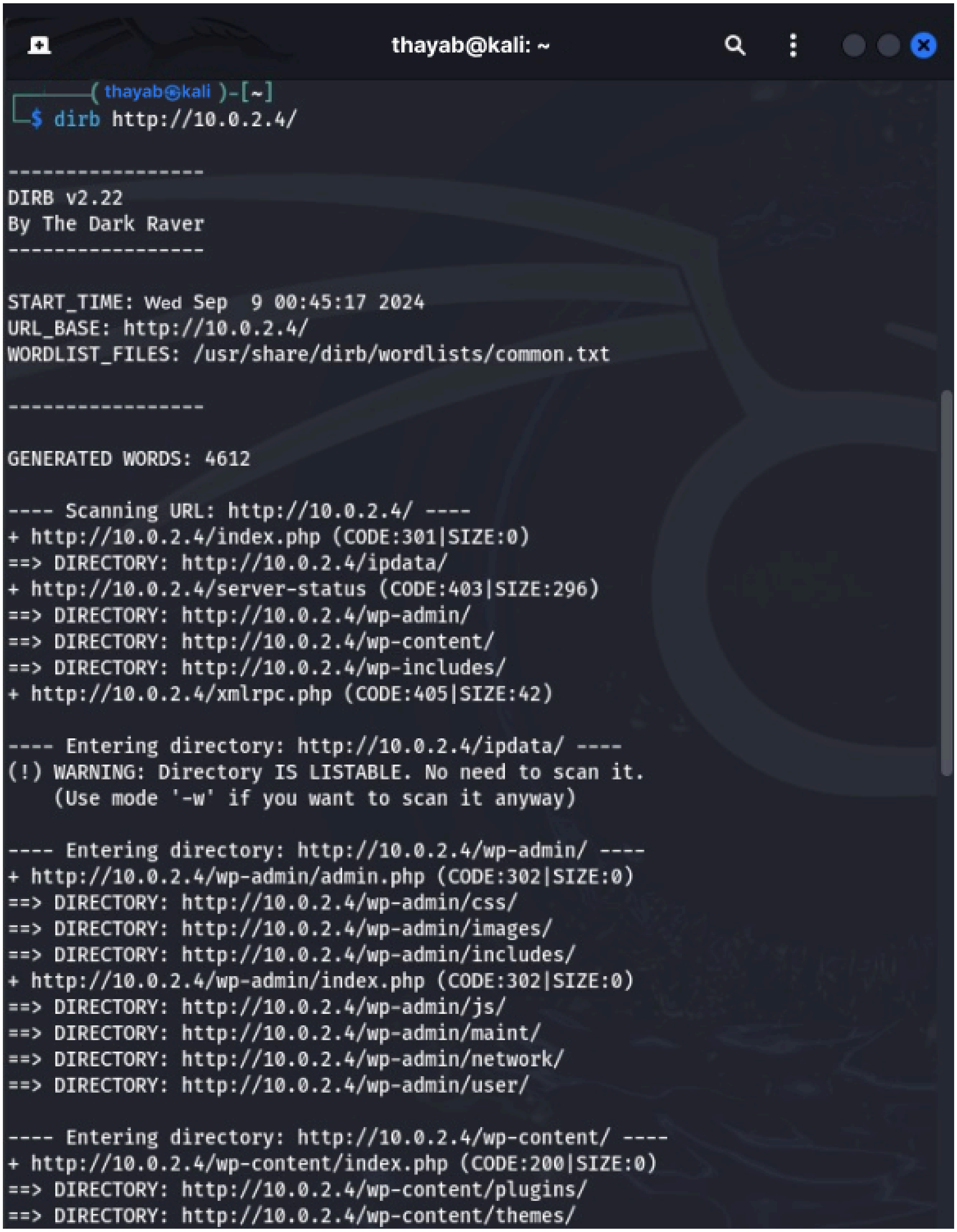
```
Currently scanning: Finished!   |   Screen View: Unique Hosts

4 Captured ARP Req/Rep packets, from 4 hosts.   Total size: 240
 _____________________________________________________________________________
  IP            At MAC Address     Count     Len  MAC Vendor / Hostname
 -----------------------------------------------------------------------------
10.0.2.1        52:54:00:12:35:00      1      60  Unknown vendor
10.0.2.2        52:54:00:12:35:00      1      60  Unknown vendor
10.0.2.3        08:00:27:2c:28:3c      1      60  PCS Systemtechnik GmbH
10.0.2.15       08:00:27:cc:54:c9      1      60  PCS Systemtechnik GmbH
```

To identify open ports and running services, utilize the `sudo nmap` command.



```
┌──(thayab㉿kali)-[~]
└─$ sudo nmap 10.0.2.4
[sudo] password for thayab:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-14 14:26 PKT
Nmap scan report for 10.0.2.4
Host is up (0.000053s latency).
All 1000 scanned ports on 10.0.2.4 are in ignored states.
Not shown: 1000 closed tcp ports (reset)

Nmap done: 1 IP address (1 host up) scanned in 0.72 seconds

┌──(thayab㉿kali)-[~]
└─$ 
```

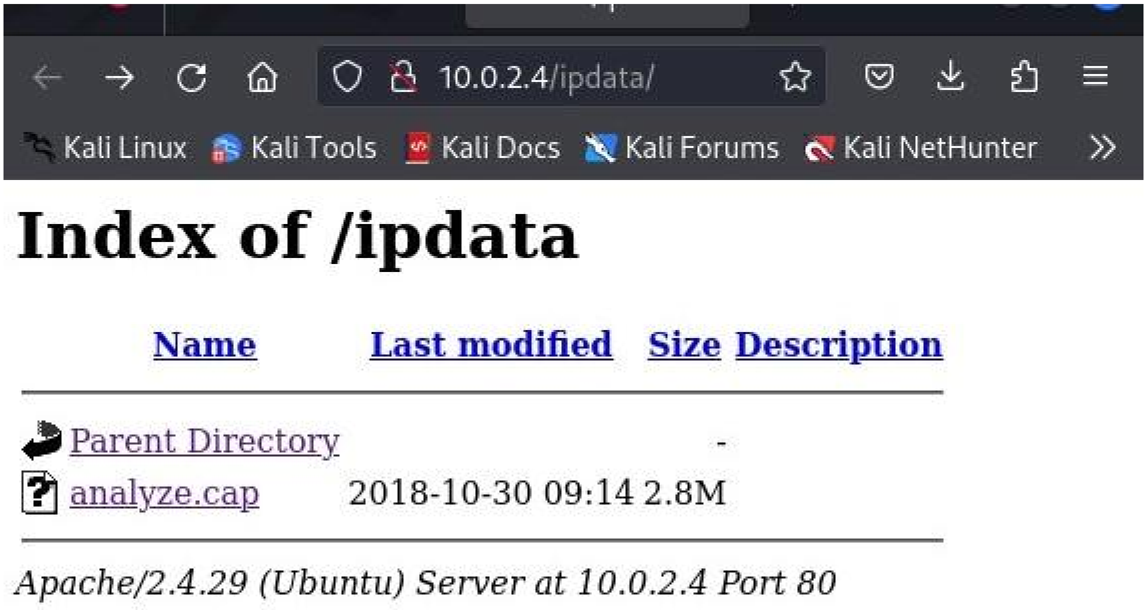
Utilizing Dirb for dictionary-based enumeration



```
┌──(thayab㉿kali)-[~]
└─$ dirb http://10.0.2.4/

-----------------
DIRB v2.22
By The Dark Raver
-----------------

START_TIME: Wed Sep  9 00:45:17 2024
URL_BASE: http://10.0.2.4/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

-----------------

GENERATED WORDS: 4612

---- Scanning URL: http://10.0.2.4/ ----
+ http://10.0.2.4/index.php (CODE:301|SIZE:0)
==> DIRECTORY: http://10.0.2.4/ipdata/
+ http://10.0.2.4/server-status (CODE:403|SIZE:296)
==> DIRECTORY: http://10.0.2.4/wp-admin/
==> DIRECTORY: http://10.0.2.4/wp-content/
==> DIRECTORY: http://10.0.2.4/wp-includes/
+ http://10.0.2.4/xmlrpc.php (CODE:405|SIZE:42)

---- Entering directory: http://10.0.2.4/ipdata/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://10.0.2.4/wp-admin/ ----
+ http://10.0.2.4/wp-admin/admin.php (CODE:302|SIZE:0)
==> DIRECTORY: http://10.0.2.4/wp-admin/css/
==> DIRECTORY: http://10.0.2.4/wp-admin/images/
==> DIRECTORY: http://10.0.2.4/wp-admin/includes/
+ http://10.0.2.4/wp-admin/index.php (CODE:302|SIZE:0)
==> DIRECTORY: http://10.0.2.4/wp-admin/js/
==> DIRECTORY: http://10.0.2.4/wp-admin/maint/
==> DIRECTORY: http://10.0.2.4/wp-admin/network/
==> DIRECTORY: http://10.0.2.4/wp-admin/user/

---- Entering directory: http://10.0.2.4/wp-content/ ----
+ http://10.0.2.4/wp-content/index.php (CODE:200|SIZE:0)
==> DIRECTORY: http://10.0.2.4/wp-content/plugins/
==> DIRECTORY: http://10.0.2.4/wp-content/themes/
```

.

Once completed, the first file saved is the ipdata file. When I clicked on it, it opened a new web page.

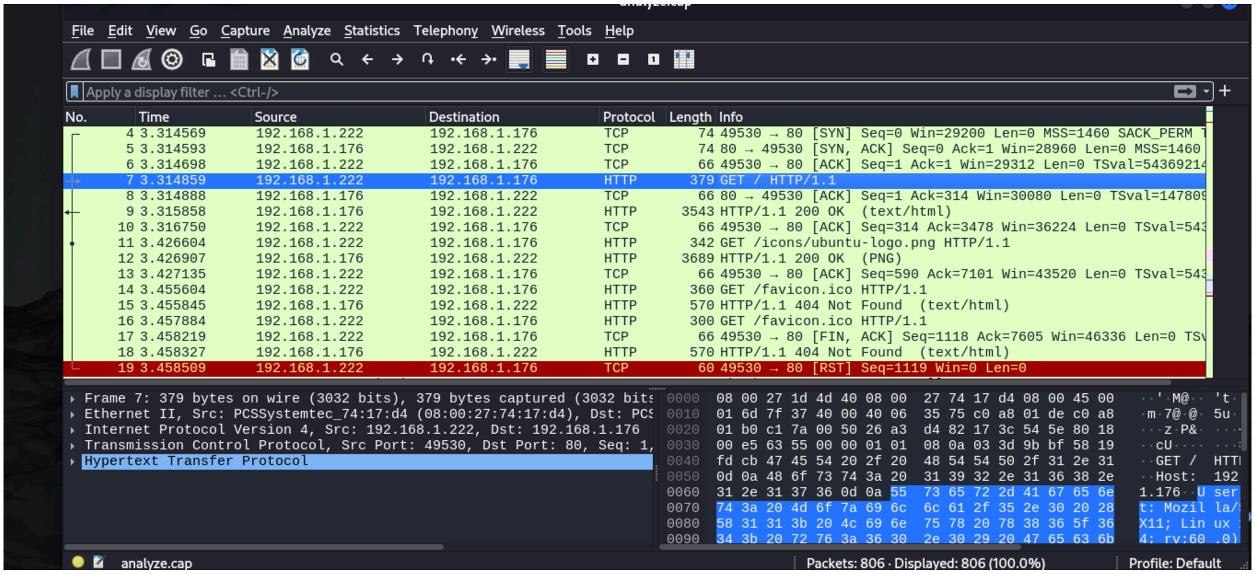


Index of /ipdata

Name	Last modified	Size	Description
Parent Directory		-	
analyze.cap	2018-10-30 09:14	2.8M	

Apache/2.4.29 (Ubuntu) Server at 10.0.2.4 Port 80

I discovered a file named ‘analyze.cap’ here, which I downloaded and opened in Wireshark. It contained a directory of all the packets associated with this website.



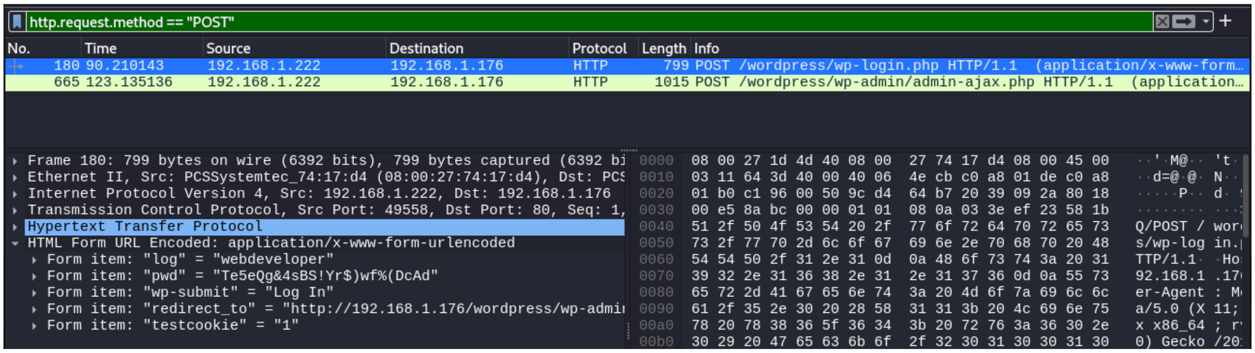
```
No.   Time        Source          Destination     Protocol Length Info
    4 3.314569    192.168.1.222   192.168.1.176   TCP        74 49530 → 80 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM T
    5 3.314593    192.168.1.176   192.168.1.222   TCP        74 80 → 49530 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1460
    6 3.314698    192.168.1.222   192.168.1.176   TCP        66 49530 → 80 [ACK] Seq=1 Ack=1 Win=29312 Len=0 TSval=54369214
    7 3.314859    192.168.1.222   192.168.1.176   HTTP      379 GET / HTTP/1.1
    8 3.314888    192.168.1.176   192.168.1.222   TCP        66 80 → 49530 [ACK] Seq=1 Ack=314 Win=30080 Len=0 TSval=147809
    9 3.315858    192.168.1.176   192.168.1.222   HTTP     3543 HTTP/1.1 200 OK  (text/html)
   10 3.316750    192.168.1.222   192.168.1.176   TCP        66 49530 → 80 [ACK] Seq=314 Ack=3478 Win=36224 Len=0 TSval=543
   11 3.426604    192.168.1.222   192.168.1.176   HTTP      342 GET /icons/ubuntu-logo.png HTTP/1.1
   12 3.426907    192.168.1.176   192.168.1.222   HTTP     3689 HTTP/1.1 200 OK  (PNG)
   13 3.427135    192.168.1.222   192.168.1.176   TCP        66 49530 → 80 [ACK] Seq=590 Ack=7101 Win=43520 Len=0 TSval=543
   14 3.455604    192.168.1.222   192.168.1.176   HTTP      360 GET /favicon.ico HTTP/1.1
   15 3.455845    192.168.1.176   192.168.1.222   HTTP      570 HTTP/1.1 404 Not Found  (text/html)
   16 3.457884    192.168.1.222   192.168.1.176   HTTP      300 GET /favicon.ico HTTP/1.1
   17 3.458219    192.168.1.222   192.168.1.176   TCP        66 49530 → 80 [FIN, ACK] Seq=1118 Ack=7605 Win=46336 Len=0 TSv
   18 3.458327    192.168.1.176   192.168.1.222   HTTP      570 HTTP/1.1 404 Not Found  (text/html)
   19 3.458509    192.168.1.222   192.168.1.176   TCP        60 49530 → 80 [RST] Seq=1119 Win=0 Len=0
```

```
› Frame 7: 379 bytes on wire (3032 bits), 379 bytes captured (3032 bits
› Ethernet II, Src: PCSSystemtec_74:17:d4 (08:00:27:74:17:d4), Dst: PCS
› Internet Protocol Version 4, Src: 192.168.1.222, Dst: 192.168.1.176
› Transmission Control Protocol, Src Port: 49530, Dst Port: 80, Seq: 1,
› Hypertext Transfer Protocol
```

```
0000  08 00 27 1d 4d 40 08 00  27 74 17 d4 08 00 45 00   ··'·M@··  't··
0010  01 6d 7f 37 40 00 40 06  35 75 c0 a8 01 de c0 a8   ·m·7@·@·  5u··
0020  01 b0 c1 7a 00 50 26 a3  d4 82 17 3c 54 5e 80 18   ···z·P&·  ····
0030  00 e5 63 55 00 00 01 01  08 0a 03 3d 9b bf 58 19   ··cU····  ···:
0040  fd cb 47 45 54 20 2f 20  48 54 54 50 2f 31 2e 31   ··GET /   HTTI
0050  0d 0a 48 6f 73 74 3a 20  31 39 32 2e 31 36 38 2e   ··Host:   192
0060  31 2e 31 37 36 0d 0a 55  73 65 72 2d 41 67 65 6e   1.176··U ser
0070  74 3a 20 4d 6f 7a 69 6c  6c 61 2f 35 2e 30 20 28   t: Mozil la/
0080  58 31 31 3b 20 4c 69 6e  75 78 20 78 38 36 5f 36   X11; Lin ux
0090  34 3b 20 72 76 3a 36 30  2e 30 29 20 47 65 63 6b   4: rv:60 .0)
```

analyze.cap   Packets: 806 · Displayed: 806 (100.0%)   Profile: Default

I added a filter on POST requests, which are used to login. From there I found the username and password



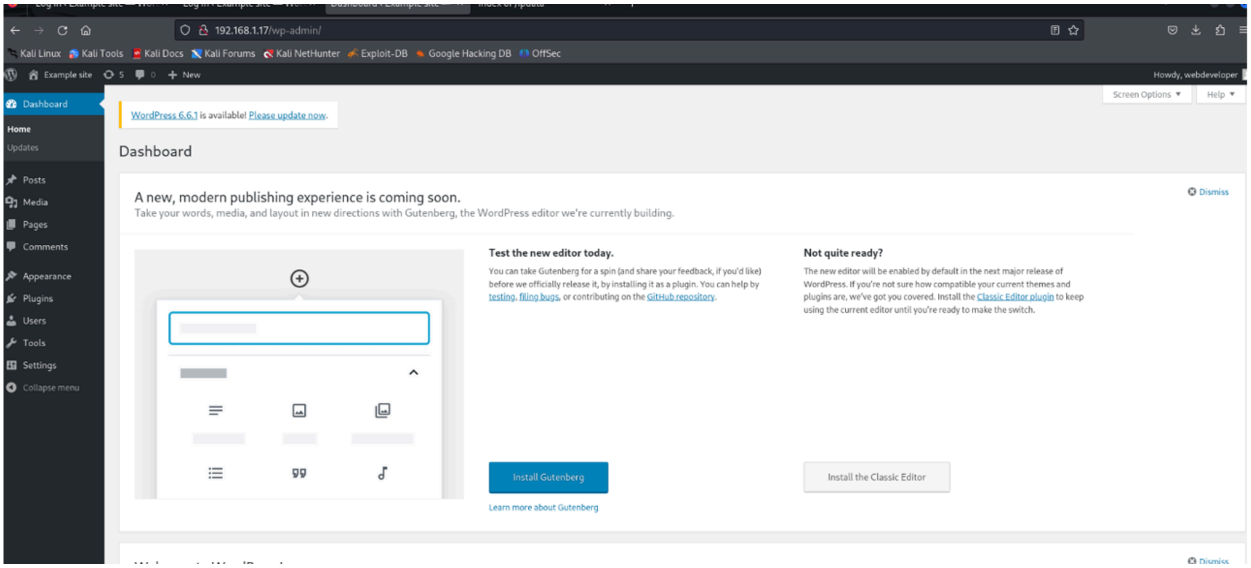
http.request.method == "POST"

```
No.   Time          Source          Destination     Protocol Length Info
  180 90.210143     192.168.1.222   192.168.1.176   HTTP      799 POST /wordpress/wp-login.php HTTP/1.1  (application/x-www-form…
  665 123.135136    192.168.1.222   192.168.1.176   HTTP     1015 POST /wordpress/wp-admin/admin-ajax.php HTTP/1.1  (application…
```

```
› Frame 180: 799 bytes on wire (6392 bits), 799 bytes captured (6392 bi
› Ethernet II, Src: PCSSystemtec_74:17:d4 (08:00:27:74:17:d4), Dst: PCS
› Internet Protocol Version 4, Src: 192.168.1.222, Dst: 192.168.1.176
› Transmission Control Protocol, Src Port: 49558, Dst Port: 80, Seq: 1,
› Hypertext Transfer Protocol
⌄ HTML Form URL Encoded: application/x-www-form-urlencoded
  › Form item: "log" = "webdeveloper"
  › Form item: "pwd" = "Te5eQg&4sBS!Yr$)wf%(DcAd"
  › Form item: "wp-submit" = "Log In"
  › Form item: "redirect_to" = "http://192.168.1.176/wordpress/wp-admi
  › Form item: "testcookie" = "1"
```

```
0000  08 00 27 1d 4d 40 08 00  27 74 17 d4 08 00 45 00   ··'·M@··  't··
0010  03 11 64 3d 40 00 40 06  4e cb c0 a8 01 de c0 a8   ··d=@·@·  N···
0020  01 b0 c1 96 00 50 9c d4  64 b7 20 39 09 2a 80 18   ·····P··  d·
0030  00 e5 8a bc 00 00 01 01  08 0a 03 3e ef 23 58 1b   ········  ···:
0040  51 2f 50 4f 53 54 20 2f  77 6f 72 64 70 72 65 73   Q/POST /  wor
0050  73 2f 77 70 2d 6c 6f 67  69 6e 2e 70 68 70 20 48   s/wp-log  in.
0060  54 54 50 2f 31 2e 31 0d  0a 48 6f 73 74 3a 20 31   TTP/1.1·  ·Ho
0070  39 32 2e 31 36 38 2e 31  2e 31 37 36 0d 0a 55 73   92.168.1  .17
0080  65 72 2d 41 67 65 6e 74  3a 20 4d 6f 7a 69 6c 6c   er-Agent  : M
0090  61 2f 35 2e 30 20 28 58  31 31 3b 20 4c 69 6e 75   a/5.0 (X  11;
00a0  78 20 78 38 36 5f 36 34  3b 20 72 76 3a 36 30 2e   x x86_64  ; r
00b0  30 29 20 47 65 63 6b 6f  2f 32 30 31 30 30 31 30   0) Gecko  /20
```

Then used the provided username and password to log into the website, and it was successful.



WordPress 6.6.1 is available! Please update now.

Dashboard

A new, modern publishing experience is coming soon.

Take your words, media, and layout in new directions with Gutenberg, the WordPress editor we're currently building.

Test the new editor today.

You can take Gutenberg for a spin (and share your feedback, if you'd like) before we officially release it, by installing it as a plugin. You can help by testing, filing bugs, or contributing on the GitHub repository.

Not quite ready?

The new editor will be enabled by default in the next major release of WordPress. If you're not sure how compatible your current themes and plugins are, we've got you covered. Install the Classic Editor plugin to keep using the current editor until you're ready to make the switch.