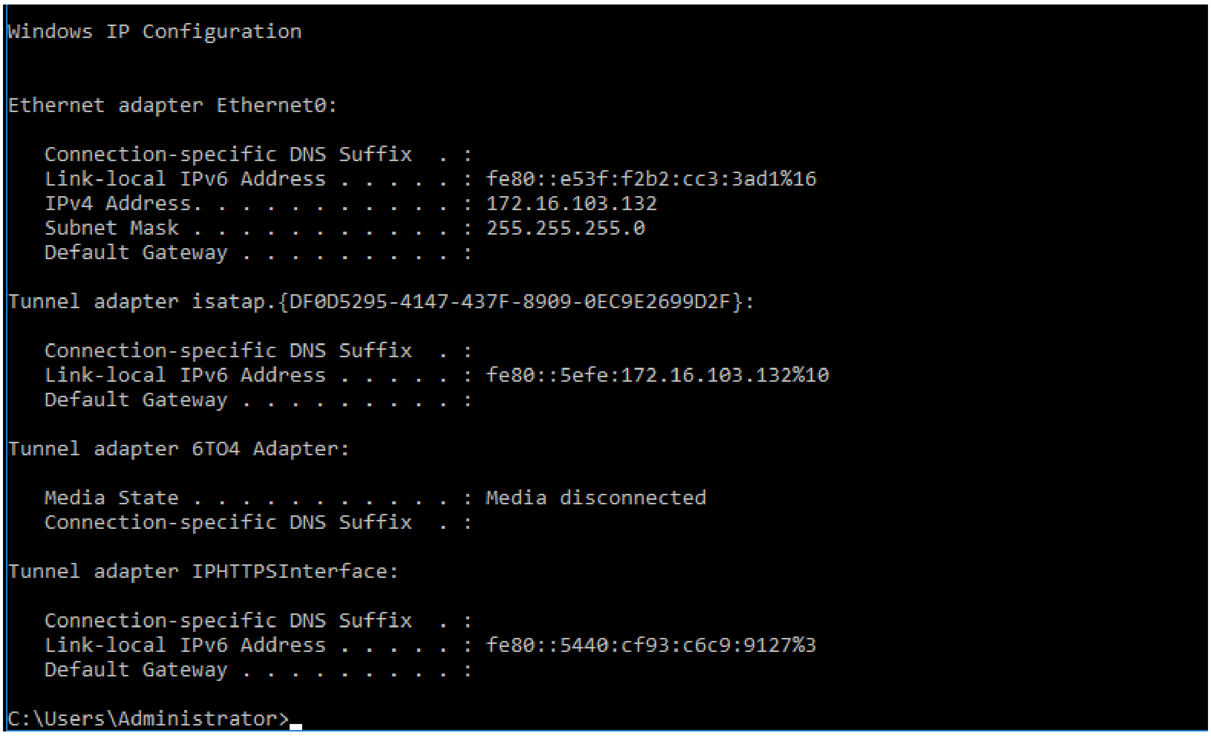
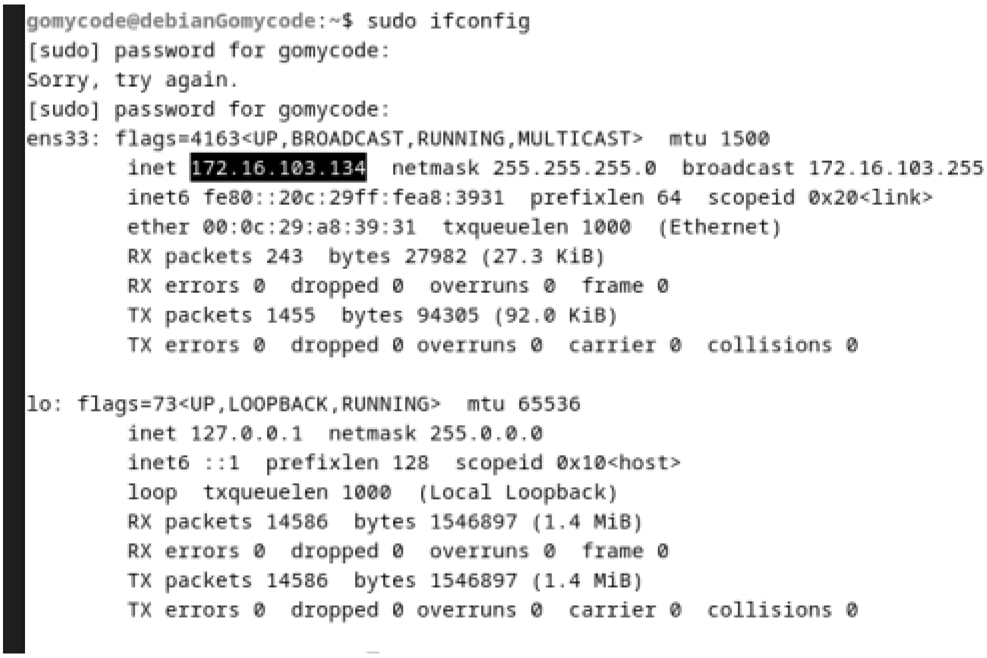
Checkpoint 2 : Networking

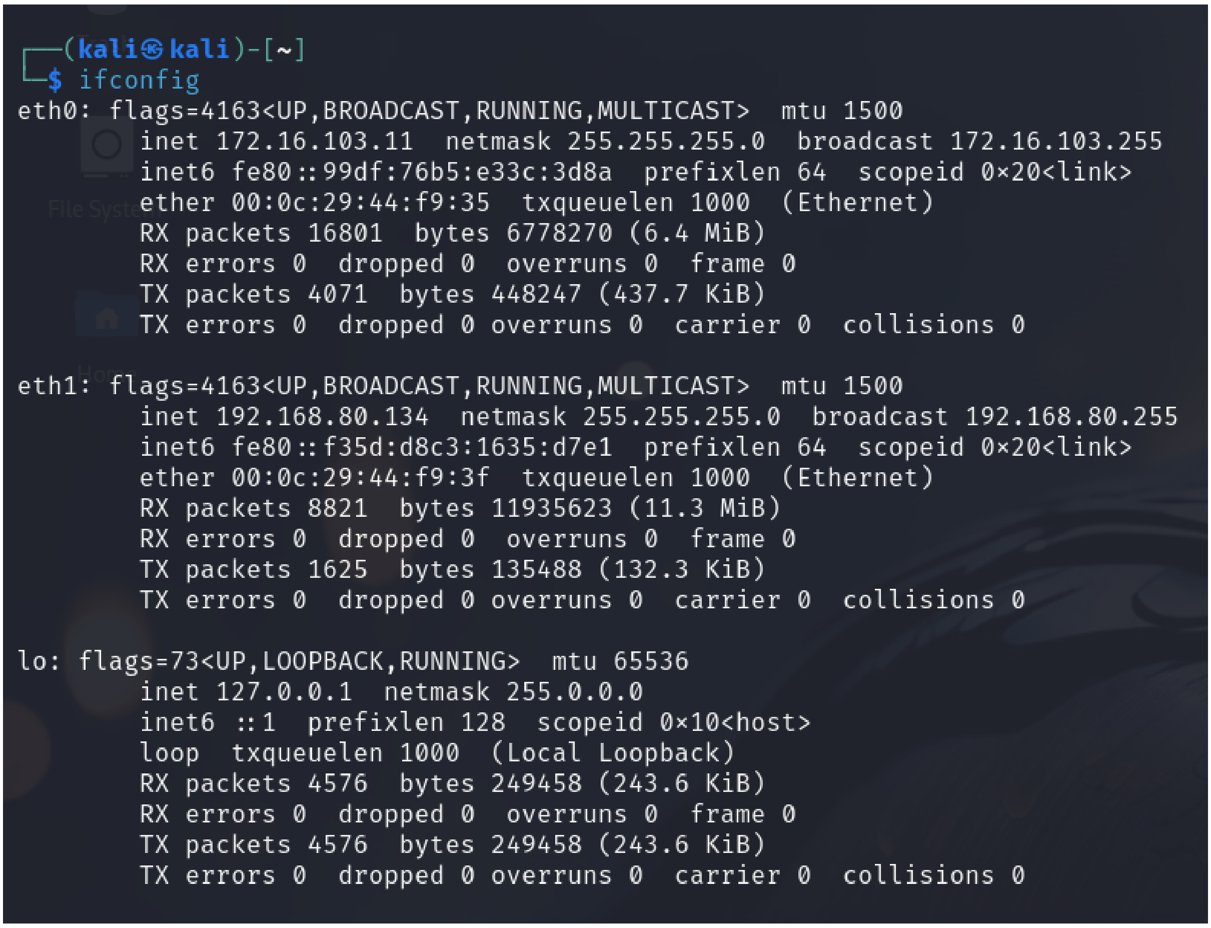
First step you will use the following tools to identify the different IP address of the kali linux , windows and debian OS:



```
Windows IP Configuration


Ethernet adapter Ethernet0:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::e53f:f2b2:cc3:3ad1%16
   IPv4 Address. . . . . . . . . . . : 172.16.103.132
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :

Tunnel adapter isatap.{DF0D5295-4147-437F-8909-0EC9E2699D2F}:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::5efe:172.16.103.132%10
   Default Gateway . . . . . . . . . :

Tunnel adapter 6TO4 Adapter:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Tunnel adapter IPHTTPSInterface:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::5440:cf93:c6c9:9127%3
   Default Gateway . . . . . . . . . :

C:\Users\Administrator>_
```

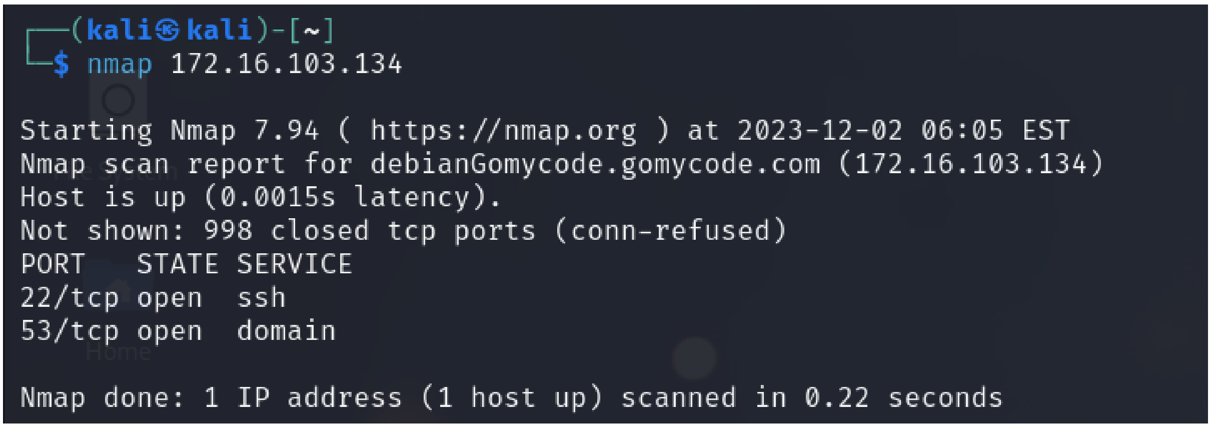


```
gomycode@debianGomycode:~$ sudo ifconfig
[sudo] password for gomycode:
Sorry, try again.
[sudo] password for gomycode:
ens33: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 172.16.103.134  netmask 255.255.255.0  broadcast 172.16.103.255
        inet6 fe80::20c:29ff:fea8:3931  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:a8:39:31  txqueuelen 1000  (Ethernet)
        RX packets 243  bytes 27982 (27.3 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 1455  bytes 94305 (92.0 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 14586  bytes 1546897 (1.4 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 14586  bytes 1546897 (1.4 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

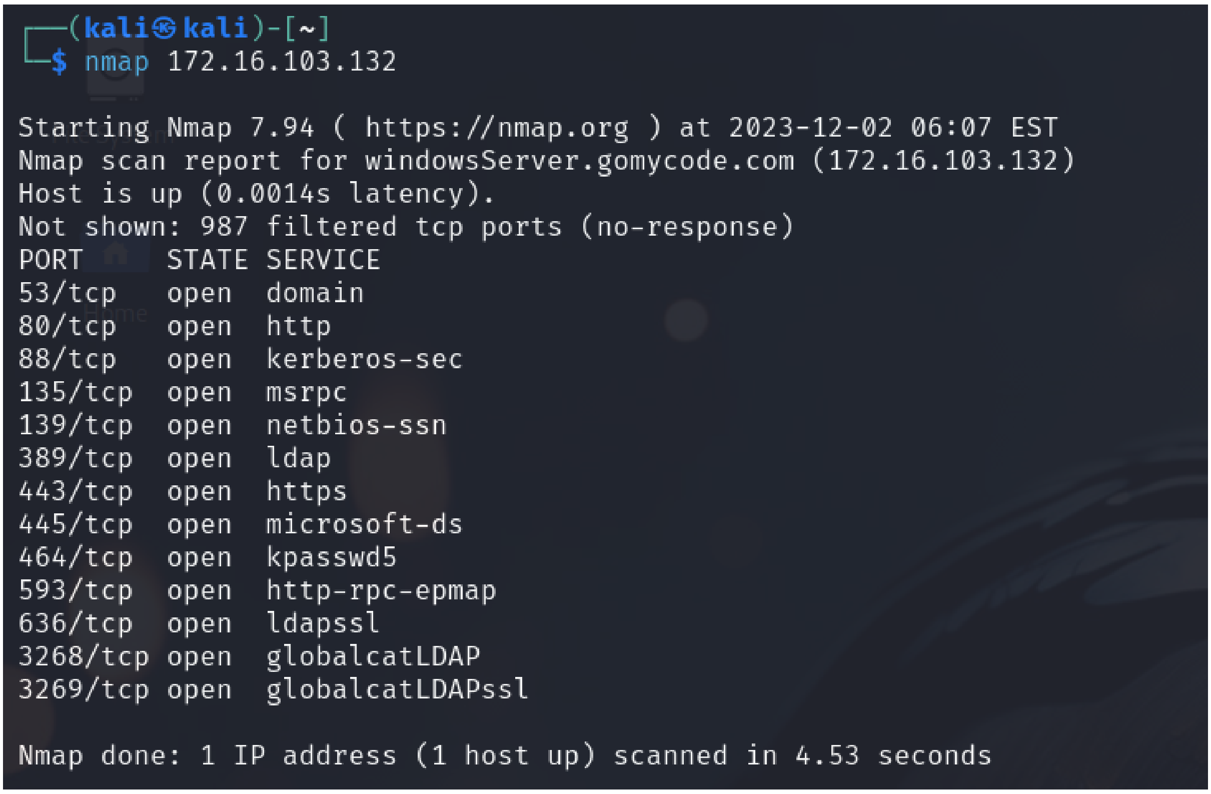


```
┌──(kali㉿kali)-[~]
└─$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 172.16.103.11  netmask 255.255.255.0  broadcast 172.16.103.255
        inet6 fe80::99df:76b5:e33c:3d8a  prefixlen 64  scopeid 0×20<link>
        ether 00:0c:29:44:f9:35  txqueuelen 1000  (Ethernet)
        RX packets 16801  bytes 6778270 (6.4 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 4071  bytes 448247 (437.7 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

eth1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.80.134  netmask 255.255.255.0  broadcast 192.168.80.255
        inet6 fe80::f35d:d8c3:1635:d7e1  prefixlen 64  scopeid 0×20<link>
        ether 00:0c:29:44:f9:3f  txqueuelen 1000  (Ethernet)
        RX packets 8821  bytes 11935623 (11.3 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 1625  bytes 135488 (132.3 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0×10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 4576  bytes 249458 (243.6 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 4576  bytes 249458 (243.6 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

Using nmap identify the different ports running on The different machines

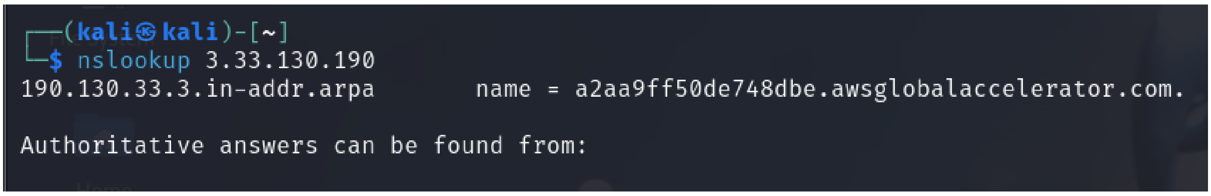


```
┌──(kali㉿kali)-[~]
└─$ nmap 172.16.103.134

Starting Nmap 7.94 ( https://nmap.org ) at 2023-12-02 06:05 EST
Nmap scan report for debianGomycode.gomycode.com (172.16.103.134)
Host is up (0.0015s latency).
Not shown: 998 closed tcp ports (conn-refused)
PORT    STATE SERVICE
22/tcp open  ssh
53/tcp open  domain

Nmap done: 1 IP address (1 host up) scanned in 0.22 seconds
```



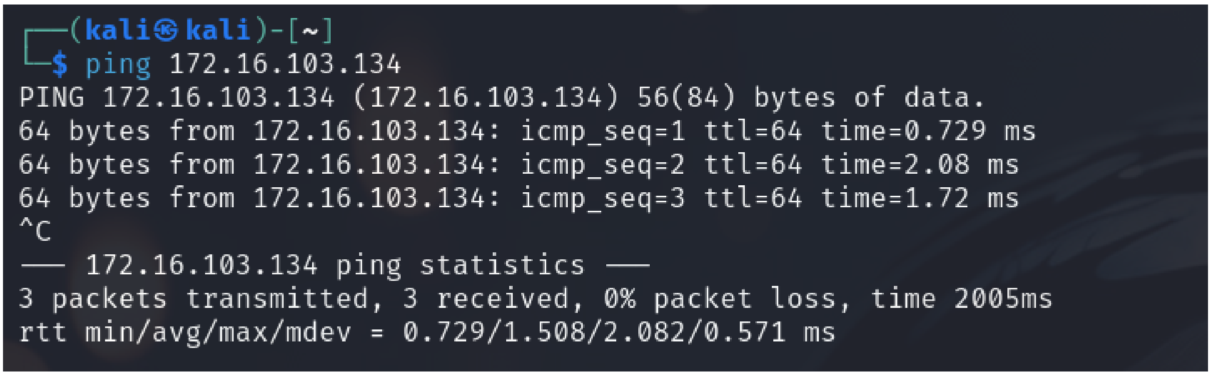
```
┌──(kali㉿kali)-[~]
└─$ nmap 172.16.103.132

Starting Nmap 7.94 ( https://nmap.org ) at 2023-12-02 06:07 EST
Nmap scan report for windowsServer.gomycode.com (172.16.103.132)
Host is up (0.0014s latency).
Not shown: 987 filtered tcp ports (no-response)
PORT     STATE SERVICE
53/tcp   open  domain
80/tcp   open  http
88/tcp   open  kerberos-sec
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
389/tcp  open  ldap
443/tcp  open  https
445/tcp  open  microsoft-ds
464/tcp  open  kpasswd5
593/tcp  open  http-rpc-epmap
636/tcp  open  ldapssl
3268/tcp open  globalcatLDAP
3269/tcp open  globalcatLDAPssl

Nmap done: 1 IP address (1 host up) scanned in 4.53 seconds
```

using nslookup try to identify the FQND of the following IP : 3.33.130.190



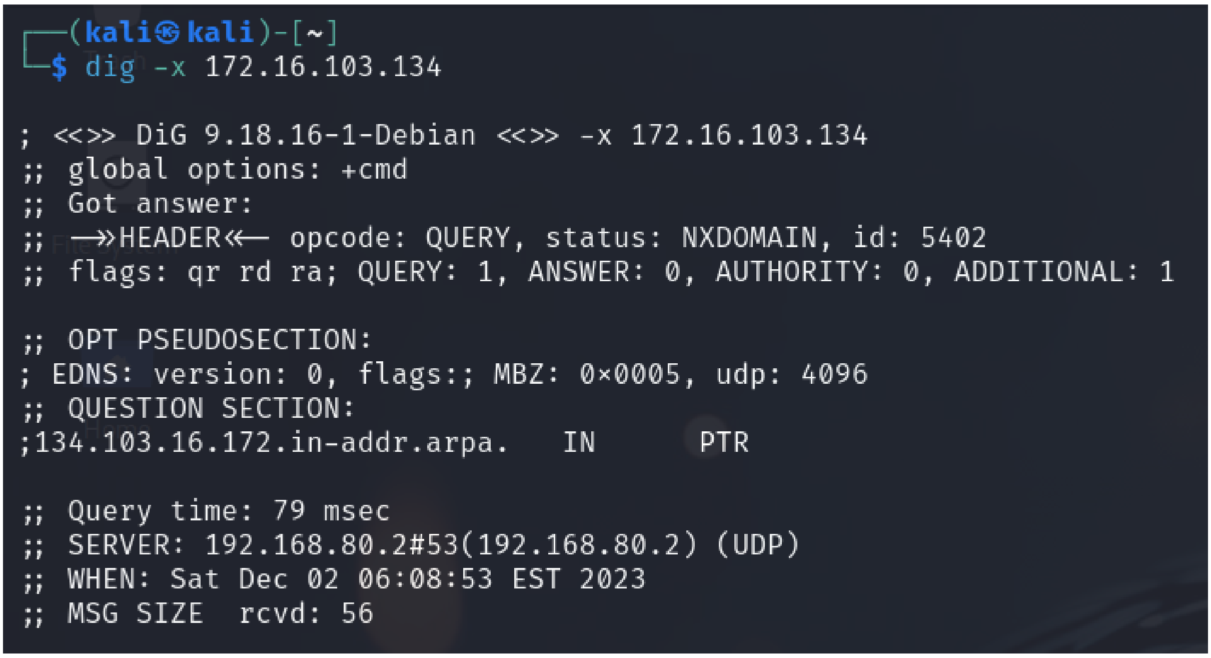
```
┌──(kali㉿kali)-[~]
└─$ nslookup 3.33.130.190
190.130.33.3.in-addr.arpa       name = a2aa9ff50de748dbe.awsglobalaccelerator.com.

Authoritative answers can be found from:
```

verify the communication with the following ip : 172.16.103.134 (use ping)



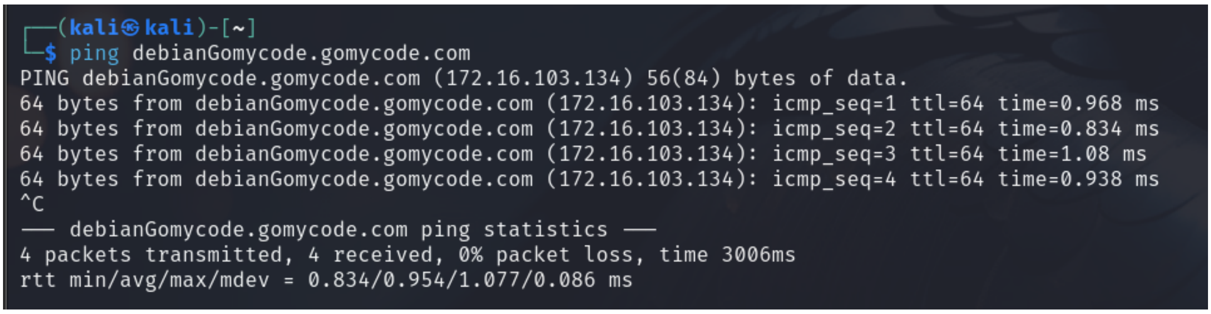
```
┌──(kali㉿kali)-[~]
└─$ ping 172.16.103.134
PING 172.16.103.134 (172.16.103.134) 56(84) bytes of data.
64 bytes from 172.16.103.134: icmp_seq=1 ttl=64 time=0.729 ms
64 bytes from 172.16.103.134: icmp_seq=2 ttl=64 time=2.08 ms
64 bytes from 172.16.103.134: icmp_seq=3 ttl=64 time=1.72 ms
^C
--- 172.16.103.134 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2005ms
rtt min/avg/max/mdev = 0.729/1.508/2.082/0.571 ms
```

let’s try to identify it’s FQND : use dig



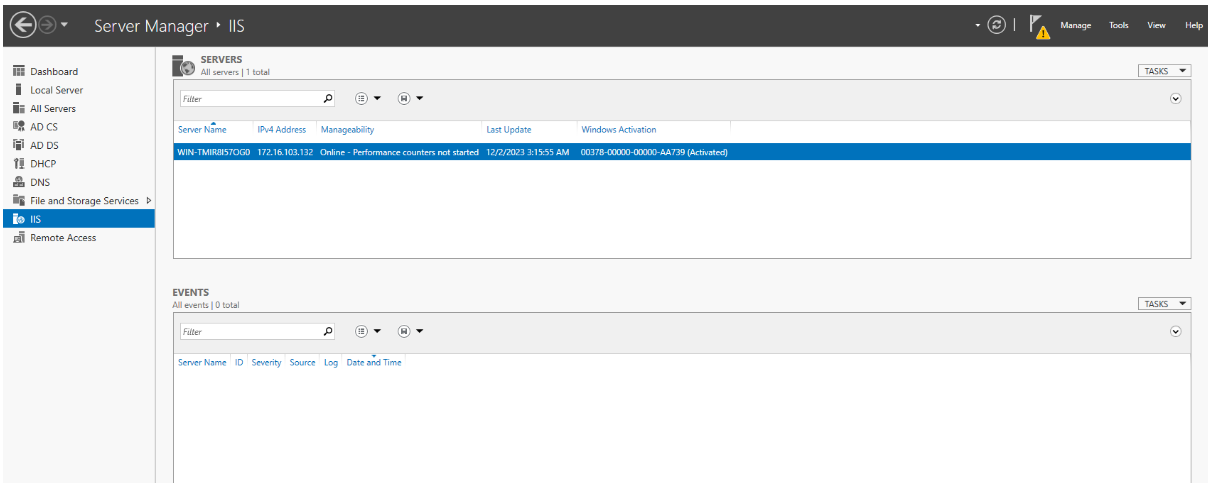
```
┌──(kali㉿kali)-[~]
└─$ dig -x 172.16.103.134

; <<>> DiG 9.18.16-1-Debian <<>> -x 172.16.103.134
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NXDOMAIN, id: 5402
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; MBZ: 0×0005, udp: 4096
;; QUESTION SECTION:
;134.103.16.172.in-addr.arpa.   IN      PTR

;; Query time: 79 msec
;; SERVER: 192.168.80.2#53(192.168.80.2) (UDP)
;; WHEN: Sat Dec 02 06:08:53 EST 2023
;; MSG SIZE  rcvd: 56
```

let’s re-verify by pinging : debianGomycode.gomycode.com



```
┌──(kali㉿kali)-[~]
└─$ ping debianGomycode.gomycode.com
PING debianGomycode.gomycode.com (172.16.103.134) 56(84) bytes of data.
64 bytes from debianGomycode.gomycode.com (172.16.103.134): icmp_seq=1 ttl=64 time=0.968 ms
64 bytes from debianGomycode.gomycode.com (172.16.103.134): icmp_seq=2 ttl=64 time=0.834 ms
64 bytes from debianGomycode.gomycode.com (172.16.103.134): icmp_seq=3 ttl=64 time=1.08 ms
64 bytes from debianGomycode.gomycode.com (172.16.103.134): icmp_seq=4 ttl=64 time=0.938 ms
^C
── debianGomycode.gomycode.com ping statistics ──
4 packets transmitted, 4 received, 0% packet loss, time 3006ms
rtt min/avg/max/mdev = 0.834/0.954/1.077/0.086 ms
```

on the windows server make sure that the IIS is running:



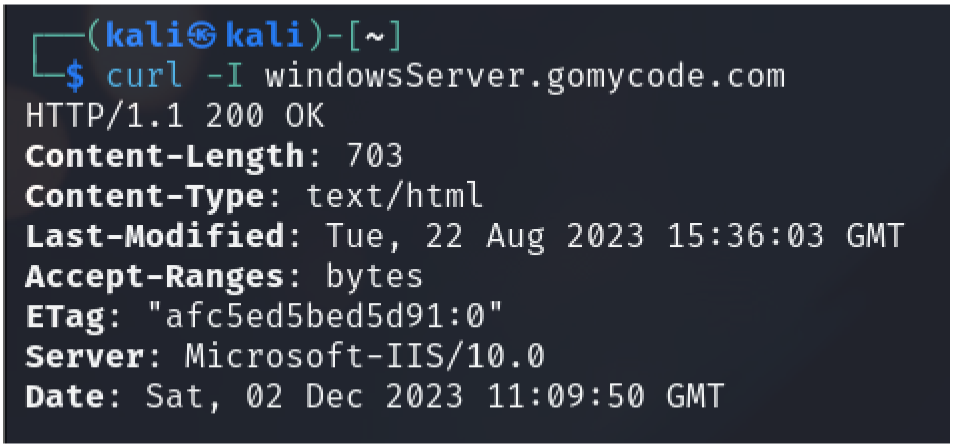
SERVERS
All servers | 1 total

Server Name	IPv4 Address	Manageability	Last Update	Windows Activation
WIN-TMIR8I57OG0	172.16.103.132	Online - Performance counters not started	12/2/2023 3:15:55 AM	00378-00000-00000-AA739 (Activated)

EVENTS
All events | 0 total

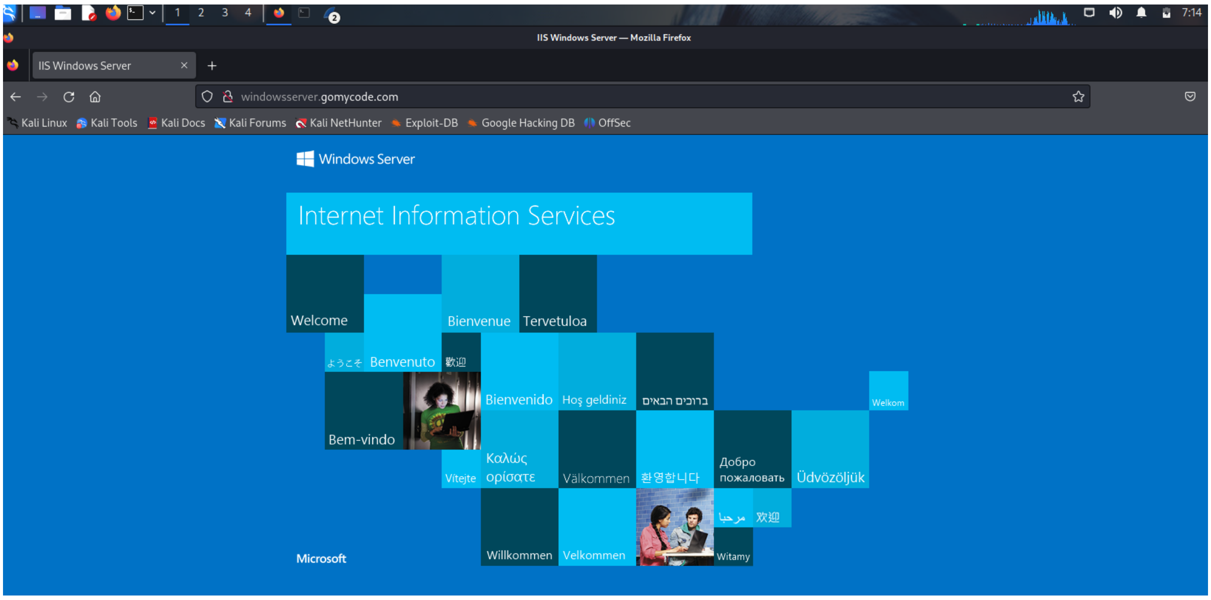
Server Name	ID	Severity	Source	Log	Date and Time

On the kali linux machine run : curl -I windowsServer.gomycode.com and identify the server running is should be (Microsoft IIS/10.0)

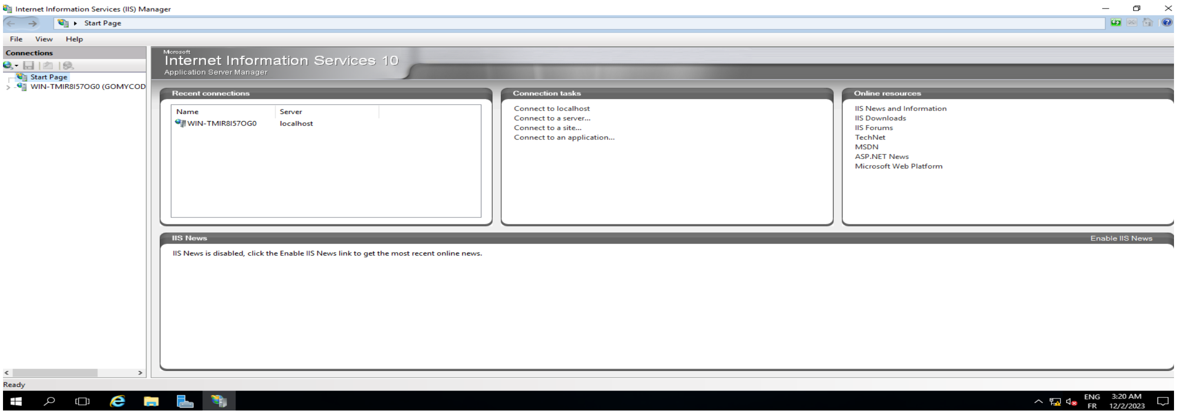


```
┌──(kali㉿kali)-[~]
└─$ curl -I windowsServer.gomycode.com
HTTP/1.1 200 OK
Content-Length: 703
Content-Type: text/html
Last-Modified: Tue, 22 Aug 2023 15:36:03 GMT
Accept-Ranges: bytes
ETag: "afc5ed5bed5d91:0"
Server: Microsoft-IIS/10.0
Date: Sat, 02 Dec 2023 11:09:50 GMT
```

on kali linux machine open firefox and try to visit windowsServer.gomycode.com. Can you access the windows website ? (right answer YES)



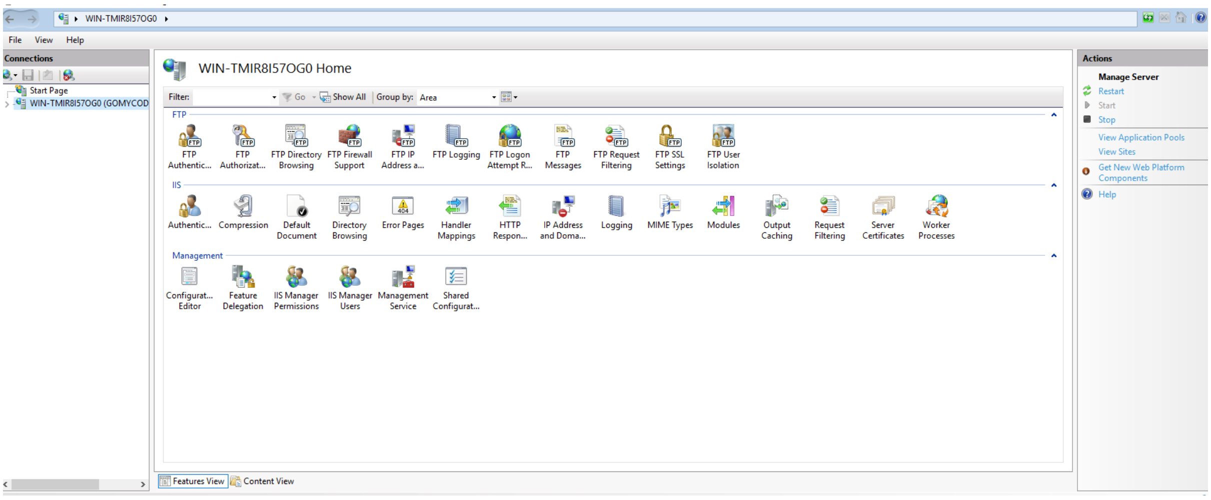
on the windows server go to tools -> internet information service (IIS).



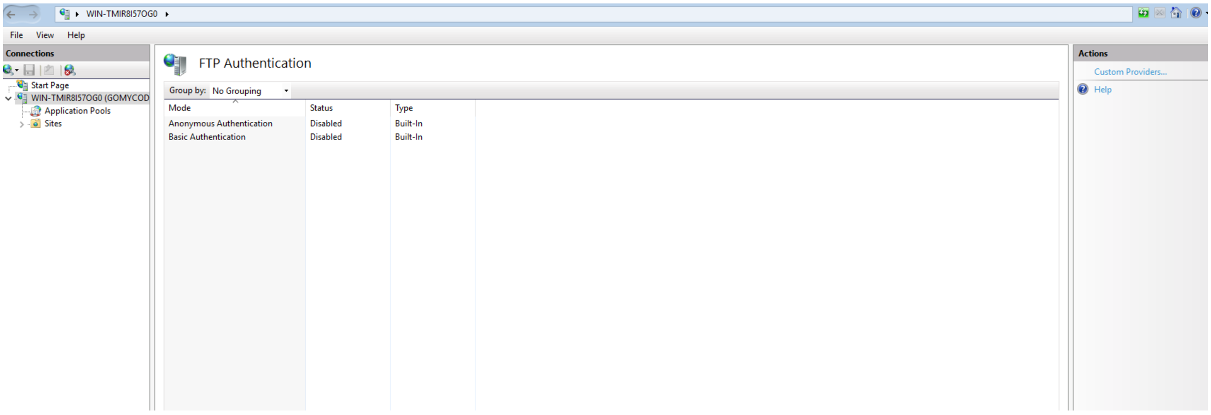
Name	Server
WIN-TMIR8I57OG0	localhost

IIS News is disabled, click the Enable IIS News link to get the most recent online news.

click on the server name

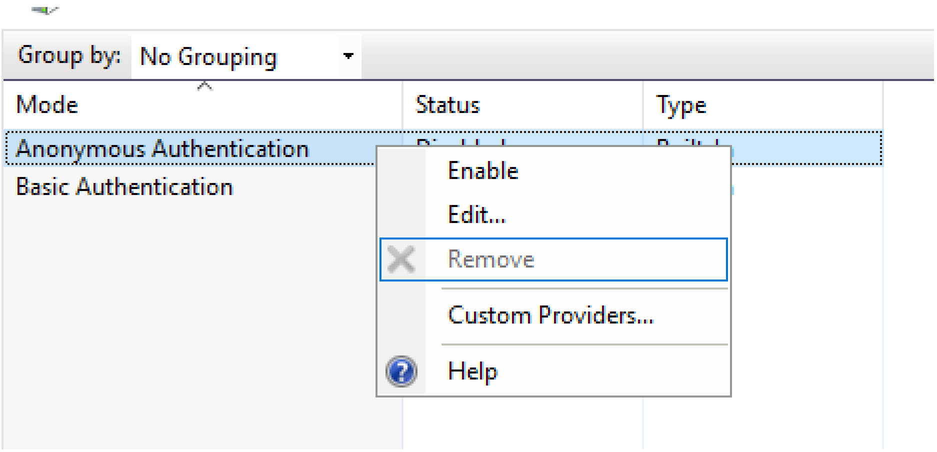


on the IIS section under ftp section click on : authentication



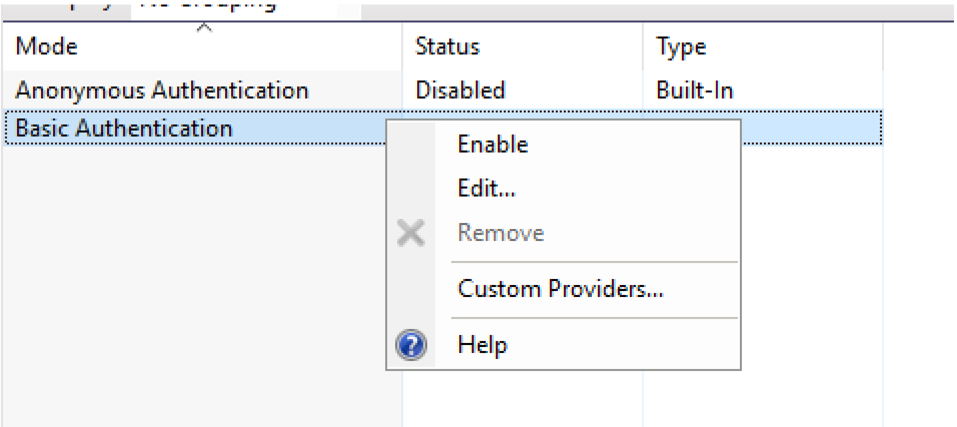
Mode	Status	Type
Anonymous Authentication	Disabled	Built-In
Basic Authentication	Disabled	Built-In

right click on Anonymous Authentication and choose disable



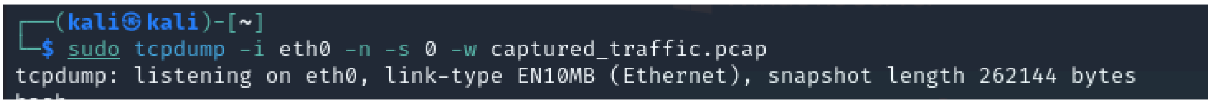
Mode	Status	Type
Anonymous Authentication		
Basic Authentication		

right click on the Basic Authentication and choose enable



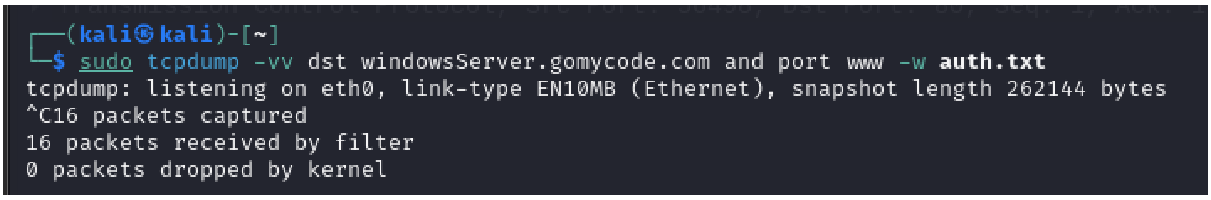
Mode	Status	Type
Anonymous Authentication	Disabled	Built-In
Basic Authentication		

run the following command to sniff the network



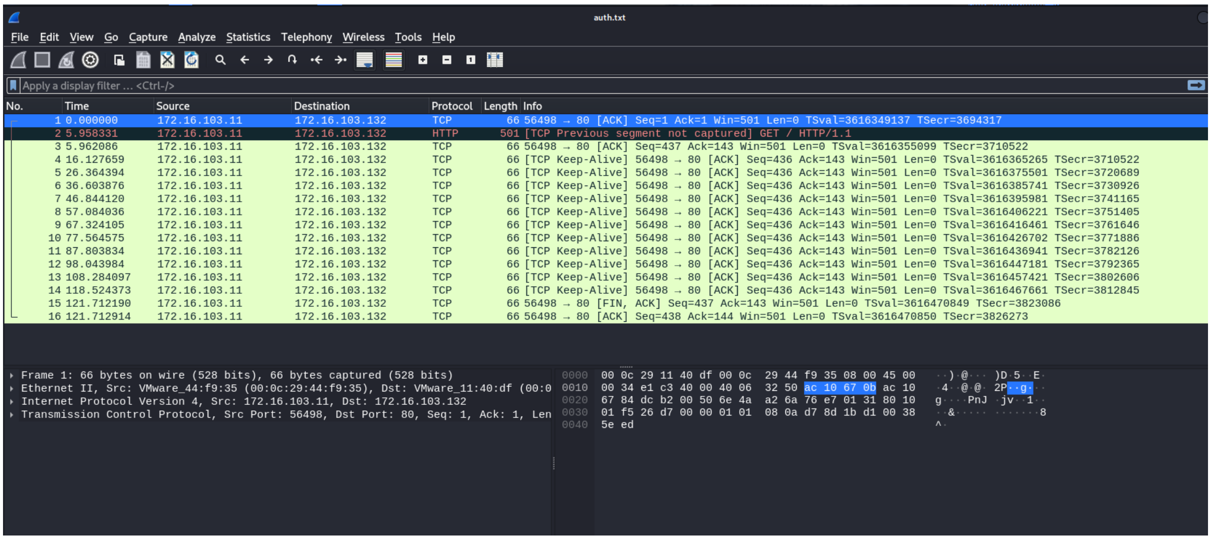
```
┌──(kali㉿kali)-[~]
└─$ sudo tcpdump -i eth0 -n -s 0 -w captured_traffic.pcap
tcpdump: listening on eth0, link-type EN10MB (Ethernet), snapshot length 262144 bytes
```

sudo tcpdump -vv dst windowsServer.gomycode.com and port www -w auth.txt



```
┌──(kali㉿kali)-[~]
└─$ sudo tcpdump -vv dst windowsServer.gomycode.com and port www -w auth.txt
tcpdump: listening on eth0, link-type EN10MB (Ethernet), snapshot length 262144 bytes
^C16 packets captured
16 packets received by filter
0 packets dropped by kernel
```

- **reload the website and try to login using the following credentials (username and password are wrong) : admin / password**
- **do it many times than stop the tcpdump command using CTRL+C**
- **launch wireshark auth.txt**

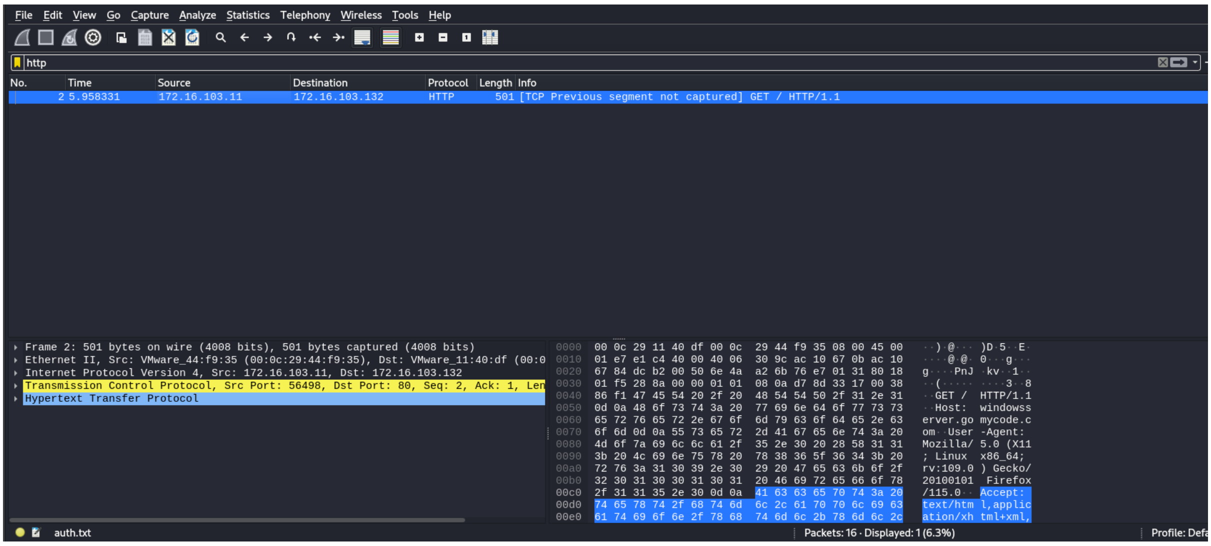


auth.txt
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>

```
No.   Time        Source          Destination      Protocol Length Info
    1 0.000000    172.16.103.11   172.16.103.132   TCP        66 56498 → 80 [ACK] Seq=1 Ack=1 Win=501 Len=0 TSval=3616349137 TSecr=3694317
    2 5.958331    172.16.103.11   172.16.103.132   HTTP      501 [TCP Previous segment not captured] GET / HTTP/1.1
    3 5.962086    172.16.103.11   172.16.103.132   TCP        66 56498 → 80 [ACK] Seq=437 Ack=143 Win=501 Len=0 TSval=3616355099 TSecr=3710522
    4 16.127659   172.16.103.11   172.16.103.132   TCP        66 [TCP Keep-Alive] 56498 → 80 [ACK] Seq=436 Ack=143 Win=501 Len=0 TSval=3616365265 TSecr=3710522
    5 26.364394   172.16.103.11   172.16.103.132   TCP        66 [TCP Keep-Alive] 56498 → 80 [ACK] Seq=436 Ack=143 Win=501 Len=0 TSval=3616375501 TSecr=3720689
    6 36.603876   172.16.103.11   172.16.103.132   TCP        66 [TCP Keep-Alive] 56498 → 80 [ACK] Seq=436 Ack=143 Win=501 Len=0 TSval=3616385741 TSecr=3730926
    7 46.844120   172.16.103.11   172.16.103.132   TCP        66 [TCP Keep-Alive] 56498 → 80 [ACK] Seq=436 Ack=143 Win=501 Len=0 TSval=3616395981 TSecr=3741165
    8 57.084036   172.16.103.11   172.16.103.132   TCP        66 [TCP Keep-Alive] 56498 → 80 [ACK] Seq=436 Ack=143 Win=501 Len=0 TSval=3616406221 TSecr=3751405
    9 67.324105   172.16.103.11   172.16.103.132   TCP        66 [TCP Keep-Alive] 56498 → 80 [ACK] Seq=436 Ack=143 Win=501 Len=0 TSval=3616416461 TSecr=3761646
   10 77.564575   172.16.103.11   172.16.103.132   TCP        66 [TCP Keep-Alive] 56498 → 80 [ACK] Seq=436 Ack=143 Win=501 Len=0 TSval=3616426702 TSecr=3771886
   11 87.803834   172.16.103.11   172.16.103.132   TCP        66 [TCP Keep-Alive] 56498 → 80 [ACK] Seq=436 Ack=143 Win=501 Len=0 TSval=3616436941 TSecr=3782126
   12 98.043984   172.16.103.11   172.16.103.132   TCP        66 [TCP Keep-Alive] 56498 → 80 [ACK] Seq=436 Ack=143 Win=501 Len=0 TSval=3616447181 TSecr=3792365
   13 108.284097  172.16.103.11   172.16.103.132   TCP        66 [TCP Keep-Alive] 56498 → 80 [ACK] Seq=436 Ack=143 Win=501 Len=0 TSval=3616457421 TSecr=3802606
   14 118.524373  172.16.103.11   172.16.103.132   TCP        66 [TCP Keep-Alive] 56498 → 80 [ACK] Seq=436 Ack=143 Win=501 Len=0 TSval=3616467661 TSecr=3812845
   15 121.712190  172.16.103.11   172.16.103.132   TCP        66 56498 → 80 [FIN, ACK] Seq=437 Ack=143 Win=501 Len=0 TSval=3616470849 TSecr=3823086
   16 121.712914  172.16.103.11   172.16.103.132   TCP        66 56498 → 80 [ACK] Seq=438 Ack=144 Win=501 Len=0 TSval=3616470850 TSecr=3826273
```

```
› Frame 1: 66 bytes on wire (528 bits), 66 bytes captured (528 bits)
› Ethernet II, Src: VMware_44:f9:35 (00:0c:29:44:f9:35), Dst: VMware_11:40:df (00:0
› Internet Protocol Version 4, Src: 172.16.103.11, Dst: 172.16.103.132
› Transmission Control Protocol, Src Port: 56498, Dst Port: 80, Seq: 1, Ack: 1, Len
```

```
0000  00 0c 29 11 40 df 00 0c  29 44 f9 35 08 00 45 00   ··)·@···)D·5··E·
0010  00 34 e1 c3 40 00 40 06  32 50 ac 10 67 0b ac 10   ·4··@·@·2P··g···
0020  67 84 dc b2 00 50 6e 4a  a2 6a 76 e7 01 31 80 10   g····PnJ·jv··1··
0030  01 f5 26 d7 00 00 01 01  08 0a d7 8d 1b d1 00 38   ··&·········8
0040  5e ed                                              ^·
```



File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
http
```

```
No.     Time          Source            Destination       Protocol  Length  Info
      2 5.958331      172.16.103.11     172.16.103.132    HTTP        501   [TCP Previous segment not captured] GET / HTTP/1.1
```

```
› Frame 2: 501 bytes on wire (4008 bits), 501 bytes captured (4008 bits)
› Ethernet II, Src: VMware_44:f9:35 (00:0c:29:44:f9:35), Dst: VMware_11:40:df (00:0
› Internet Protocol Version 4, Src: 172.16.103.11, Dst: 172.16.103.132
› Transmission Control Protocol, Src Port: 56498, Dst Port: 80, Seq: 2, Ack: 1, Len
› Hypertext Transfer Protocol
```

```
0000  00 0c 29 11 40 df 00 0c  29 44 f9 35 08 00 45 00   ··)·@···  )D·5··E·
0010  01 e7 e1 c4 40 00 40 06  30 9c ac 10 67 0b ac 10   ····@·@·  0···g···
0020  67 84 dc b2 00 50 6e 4a  a2 6b 76 e7 01 31 80 18   g····PnJ  ·kv··1··
0030  01 f5 28 8a 00 00 01 01  08 0a d7 8d 33 17 00 38   ··(·····  ····3··8
0040  86 f1 47 45 54 20 2f 20  48 54 54 50 2f 31 2e 31   ··GET /   HTTP/1.1
0050  0d 0a 48 6f 73 74 3a 20  77 69 6e 64 6f 77 73 73   ··Host:   windowss
0060  65 72 76 65 72 2e 67 6f  6d 79 63 6f 64 65 2e 63   erver.go  mycode.c
0070  6f 6d 0d 0a 55 73 65 72  2d 41 67 65 6e 74 3a 20   om··User  -Agent: 
0080  4d 6f 7a 69 6c 6c 61 2f  35 2e 30 20 28 58 31 31   Mozilla/  5.0 (X11
0090  3b 20 4c 69 6e 75 78 20  78 38 36 5f 36 34 3b 20   ; Linux   x86_64; 
00a0  72 76 3a 31 30 39 2e 30  29 20 47 65 63 6b 6f 2f   rv:109.0  ) Gecko/
00b0  32 30 31 30 30 31 30 31  20 46 69 72 65 66 6f 78   20100101   Firefox
00c0  2f 31 31 35 2e 30 0d 0a  41 63 63 65 70 74 3a 20   /115.0··  Accept: 
00d0  74 65 78 74 2f 68 74 6d  6c 2c 61 70 70 6c 69 63   text/htm  l,applic
00e0  61 74 69 6f 6e 2f 78 68  74 6d 6c 2b 78 6d 6c 2c   ation/xh  tml+xml,
```

auth.txt | Packets: 16 · Displayed: 1 (6.3%) | Profile: Defa