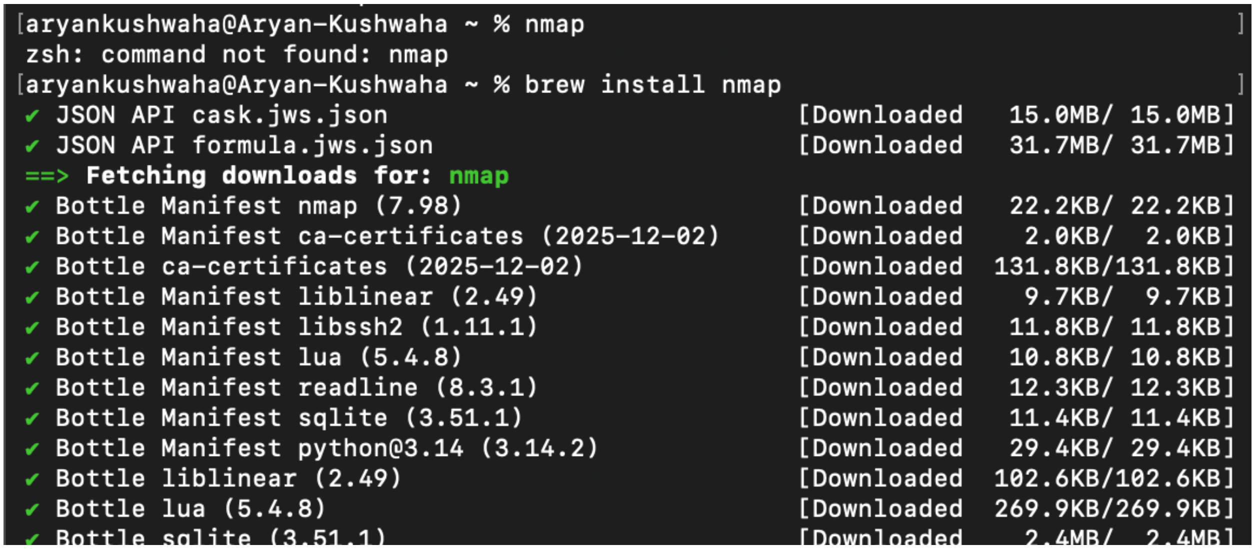
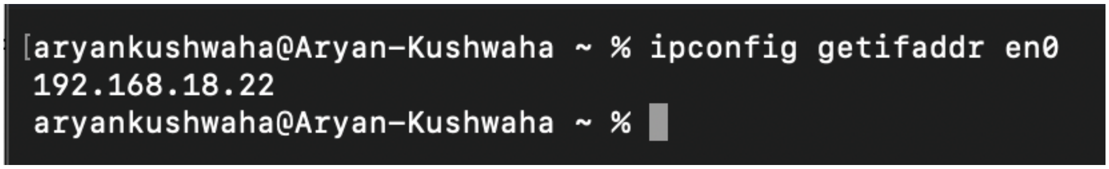
1. Nmap installation



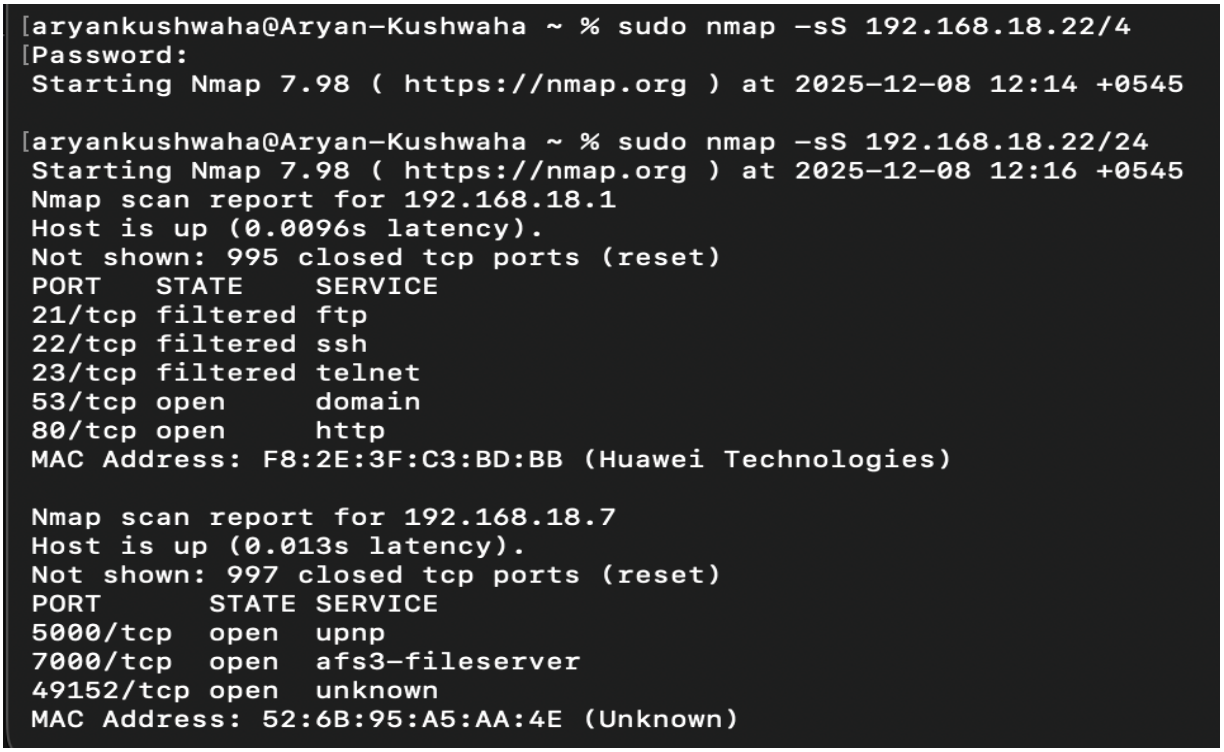
```
[aryankushwaha@Aryan-Kushwaha ~ % nmap                                                  ]
 zsh: command not found: nmap
[aryankushwaha@Aryan-Kushwaha ~ % brew install nmap                                     ]
 ✔ JSON API cask.jws.json                              [Downloaded   15.0MB/ 15.0MB]
 ✔ JSON API formula.jws.json                           [Downloaded   31.7MB/ 31.7MB]
 ==> Fetching downloads for: nmap
 ✔ Bottle Manifest nmap (7.98)                         [Downloaded   22.2KB/ 22.2KB]
 ✔ Bottle Manifest ca-certificates (2025-12-02)        [Downloaded    2.0KB/  2.0KB]
 ✔ Bottle ca-certificates (2025-12-02)                 [Downloaded  131.8KB/131.8KB]
 ✔ Bottle Manifest liblinear (2.49)                    [Downloaded    9.7KB/  9.7KB]
 ✔ Bottle Manifest libssh2 (1.11.1)                    [Downloaded   11.8KB/ 11.8KB]
 ✔ Bottle Manifest lua (5.4.8)                         [Downloaded   10.8KB/ 10.8KB]
 ✔ Bottle Manifest readline (8.3.1)                    [Downloaded   12.3KB/ 12.3KB]
 ✔ Bottle Manifest sqlite (3.51.1)                     [Downloaded   11.4KB/ 11.4KB]
 ✔ Bottle Manifest python@3.14 (3.14.2)                [Downloaded   29.4KB/ 29.4KB]
 ✔ Bottle liblinear (2.49)                             [Downloaded  102.6KB/102.6KB]
 ✔ Bottle lua (5.4.8)                                  [Downloaded  269.9KB/269.9KB]
 ✔ Bottle sqlite (3.51.1)                              [Downloaded    2.4MB/  2.4MB]
```

2. Check Local Ip address



```
[aryankushwaha@Aryan-Kushwaha ~ % ipconfig getifaddr en0
 192.168.18.22
 aryankushwaha@Aryan-Kushwaha ~ %
```

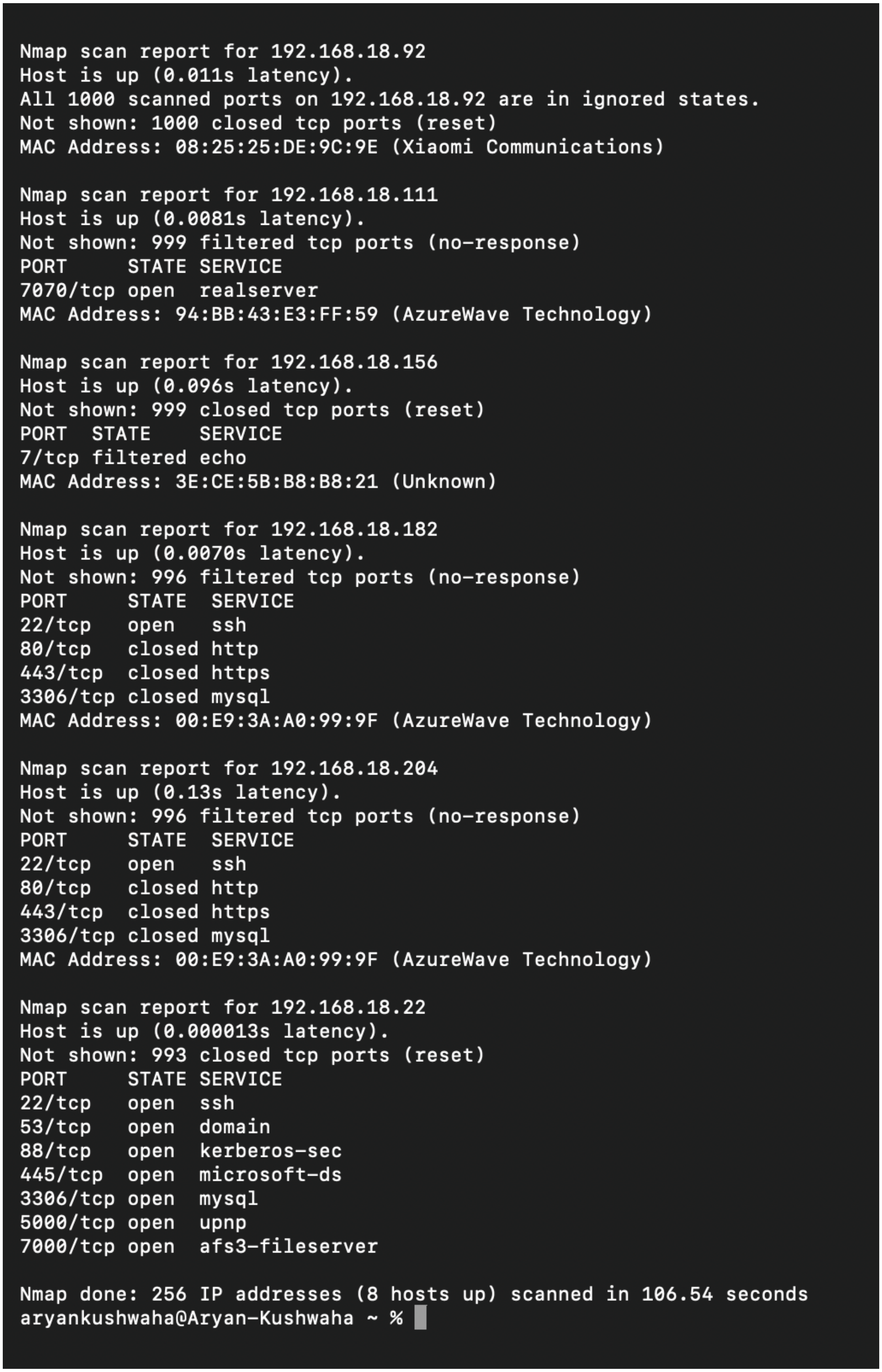
3. Nmap scans Wi-Fi network.



```
[aryankushwaha@Aryan-Kushwaha ~ % sudo nmap -sS 192.168.18.22/4
[Password:
 Starting Nmap 7.98 ( https://nmap.org ) at 2025-12-08 12:14 +0545

[aryankushwaha@Aryan-Kushwaha ~ % sudo nmap -sS 192.168.18.22/24
 Starting Nmap 7.98 ( https://nmap.org ) at 2025-12-08 12:16 +0545
 Nmap scan report for 192.168.18.1
 Host is up (0.0096s latency).
 Not shown: 995 closed tcp ports (reset)
 PORT    STATE    SERVICE
 21/tcp  filtered ftp
 22/tcp  filtered ssh
 23/tcp  filtered telnet
 53/tcp  open     domain
 80/tcp  open     http
 MAC Address: F8:2E:3F:C3:BD:BB (Huawei Technologies)

 Nmap scan report for 192.168.18.7
 Host is up (0.013s latency).
 Not shown: 997 closed tcp ports (reset)
 PORT      STATE SERVICE
 5000/tcp  open  upnp
 7000/tcp  open  afs3-fileserver
 49152/tcp open  unknown
 MAC Address: 52:6B:95:A5:AA:4E (Unknown)
```



```
Nmap scan report for 192.168.18.92
Host is up (0.011s latency).
All 1000 scanned ports on 192.168.18.92 are in ignored states.
Not shown: 1000 closed tcp ports (reset)
MAC Address: 08:25:25:DE:9C:9E (Xiaomi Communications)

Nmap scan report for 192.168.18.111
Host is up (0.0081s latency).
Not shown: 999 filtered tcp ports (no-response)
PORT     STATE SERVICE
7070/tcp open  realserver
MAC Address: 94:BB:43:E3:FF:59 (AzureWave Technology)

Nmap scan report for 192.168.18.156
Host is up (0.096s latency).
Not shown: 999 closed tcp ports (reset)
PORT  STATE    SERVICE
7/tcp filtered echo
MAC Address: 3E:CE:5B:B8:B8:21 (Unknown)

Nmap scan report for 192.168.18.182
Host is up (0.0070s latency).
Not shown: 996 filtered tcp ports (no-response)
PORT     STATE  SERVICE
22/tcp   open   ssh
80/tcp   closed http
443/tcp  closed https
3306/tcp closed mysql
MAC Address: 00:E9:3A:A0:99:9F (AzureWave Technology)

Nmap scan report for 192.168.18.204
Host is up (0.13s latency).
Not shown: 996 filtered tcp ports (no-response)
PORT     STATE  SERVICE
22/tcp   open   ssh
80/tcp   closed http
443/tcp  closed https
3306/tcp closed mysql
MAC Address: 00:E9:3A:A0:99:9F (AzureWave Technology)

Nmap scan report for 192.168.18.22
Host is up (0.000013s latency).
Not shown: 993 closed tcp ports (reset)
PORT     STATE SERVICE
22/tcp   open  ssh
53/tcp   open  domain
88/tcp   open  kerberos-sec
445/tcp  open  microsoft-ds
3306/tcp open  mysql
5000/tcp open  upnp
7000/tcp open  afs3-fileserver

Nmap done: 256 IP addresses (8 hosts up) scanned in 106.54 seconds
aryankushwaha@Aryan-Kushwaha ~ %
```

1. Port 21 - FTP (Filtered)

- **Description:** File Transfer Protocol for file sharing.
- **Vulnerabilities:** FTP transmits data (including passwords) in plaintext; susceptible to sniffing, brute force, and anonymous access risks.
- **Prevention:** Use **SFTP/FTPS** (encrypted alternatives), strong passwords, disable anonymous login, and firewall to limit access.

---

2. Port 22 - SSH (Open)

- **Description:** Secure Shell for encrypted remote login.
- **Vulnerabilities:** Weak passwords, outdated SSH versions, and brute force attacks.
- **Prevention:** Use **key-based authentication**, disable root login, limit allowed IPs via firewall, and keep SSH updated.

---

3. Port 23 - Telnet (Filtered)

- **Description:** Unencrypted remote login protocol (deprecated).
- **Vulnerabilities:** Sends data in plaintext, easily intercepted.
- **Prevention:** Avoid using Telnet; use **SSH** instead. Block Telnet ports via firewall.

---

4. Port 53 - DNS (Open)

- **Description:** Domain Name System for hostname resolution.
- **Vulnerabilities:** DNS cache poisoning, amplification DDoS attacks.
- **Prevention:** Use DNSSEC, restrict recursive queries, and secure DNS servers.

---

5. Port 80 - HTTP (Open/Closed)

- **Description:** Unencrypted web traffic.
- **Vulnerabilities:** Data sniffing, injection attacks if the web app is vulnerable.
- **Prevention:** Use **HTTPS** (TLS), keep web applications updated, and use web application firewalls.

---

6. Port 443 - HTTPS (Closed)

- **Description:** Secure web traffic with TLS encryption.
- **Vulnerabilities:** Misconfiguration, outdated TLS versions.
- **Prevention:** Use strong TLS configurations and keep certificates updated.

---

7. Port 3306 - MySQL (Open/Closed)

- **Description:** MySQL database server.
- **Vulnerabilities:** Default or weak passwords, SQL injection.
- **Prevention:** Restrict access to MySQL port, use strong passwords, update database software, and apply application-level protections.

---

8. Port 5000 - UPnP (Open)

- **Description:** Universal Plug and Play for automatic device discovery.
- **Vulnerabilities:** Can expose devices to remote attacks or unauthorized control.
- **Prevention:** Disable UPnP if not needed or restrict it within trusted networks.

---

9. Port 7000 - AFS3 Fileserver (Open)

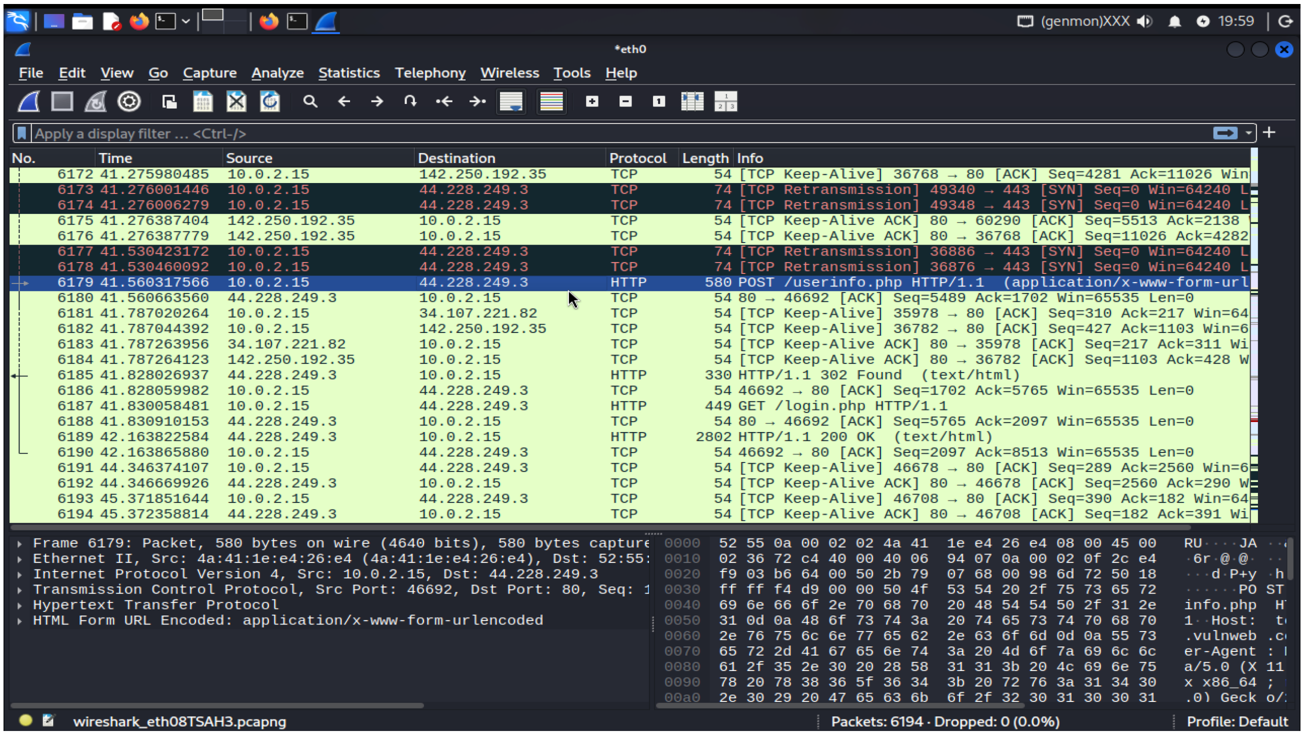
- **Description:** Part of Andrew File System (distributed file system).
- **Vulnerabilities:** Uncommon, but misconfigurations can expose files.
- **Prevention:** Restrict access to trusted users, disable if unused.

---

10. Port 445 - Microsoft-DS (Open)

- **Description:** Microsoft Directory Services for file sharing and network browsing.
- **Vulnerabilities:** Exploited by ransomware (e.g., WannaCry), SMB vulnerabilities.
- **Prevention:** Block port 445 from the internet, keep Windows updated, disable SMBv1.

4. Capturing Data Packets WireShark

- 

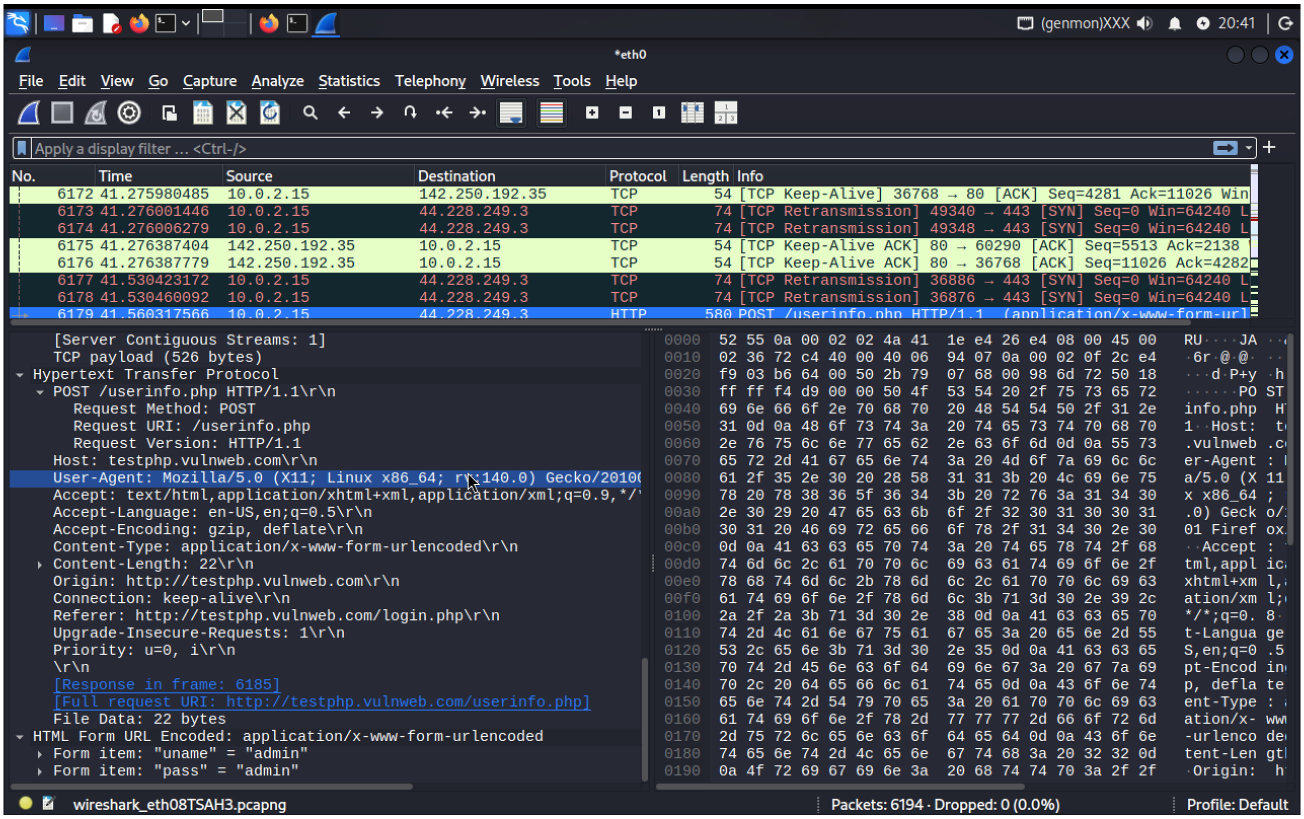
(genmon)XXX
19:59
*eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>

```
No.     Time         Source          Destination     Protocol Length Info
   6172 41.275980485 10.0.2.15       142.250.192.35  TCP        54 [TCP Keep-Alive] 36768 → 80 [ACK] Seq=4281 Ack=11026 Win
   6173 41.276001446 10.0.2.15       44.228.249.3    TCP        74 [TCP Retransmission] 49340 → 443 [SYN] Seq=0 Win=64240 L
   6174 41.276006279 10.0.2.15       44.228.249.3    TCP        74 [TCP Retransmission] 49348 → 443 [SYN] Seq=0 Win=64240 L
   6175 41.276387404 142.250.192.35  10.0.2.15       TCP        54 [TCP Keep-Alive ACK] 80 → 60290 [ACK] Seq=5513 Ack=2138
   6176 41.276387779 142.250.192.35  10.0.2.15       TCP        54 [TCP Keep-Alive ACK] 80 → 36768 [ACK] Seq=11026 Ack=4282
   6177 41.530423172 10.0.2.15       44.228.249.3    TCP        74 [TCP Retransmission] 36886 → 443 [SYN] Seq=0 Win=64240 L
   6178 41.530460092 10.0.2.15       44.228.249.3    TCP        74 [TCP Retransmission] 36876 → 443 [SYN] Seq=0 Win=64240 L
   6179 41.560317566 10.0.2.15       44.228.249.3    HTTP      580 POST /userinfo.php HTTP/1.1  (application/x-www-form-url
   6180 41.560663560 44.228.249.3    10.0.2.15       TCP        54 80 → 46692 [ACK] Seq=5489 Ack=1702 Win=65535 Len=0
   6181 41.787020264 10.0.2.15       34.107.221.82   TCP        54 [TCP Keep-Alive] 35978 → 80 [ACK] Seq=310 Ack=217 Win=64
   6182 41.787044392 10.0.2.15       142.250.192.35  TCP        54 [TCP Keep-Alive] 36782 → 80 [ACK] Seq=427 Ack=1103 Win=6
   6183 41.787263956 34.107.221.82   10.0.2.15       TCP        54 [TCP Keep-Alive ACK] 80 → 35978 [ACK] Seq=217 Ack=311 Wi
   6184 41.787264123 142.250.192.35  10.0.2.15       TCP        54 [TCP Keep-Alive ACK] 80 → 36782 [ACK] Seq=1103 Ack=428 W
   6185 41.828026937 44.228.249.3    10.0.2.15       HTTP      330 HTTP/1.1 302 Found  (text/html)
   6186 41.828059982 10.0.2.15       44.228.249.3    TCP        54 46692 → 80 [ACK] Seq=1702 Ack=5765 Win=65535 Len=0
   6187 41.830058481 10.0.2.15       44.228.249.3    HTTP      449 GET /login.php HTTP/1.1
   6188 41.830910153 44.228.249.3    10.0.2.15       TCP        54 80 → 46692 [ACK] Seq=5765 Ack=2097 Win=65535 Len=0
   6189 42.163822584 44.228.249.3    10.0.2.15       HTTP     2802 HTTP/1.1 200 OK  (text/html)
   6190 42.163865880 10.0.2.15       44.228.249.3    TCP        54 46692 → 80 [ACK] Seq=2097 Ack=8513 Win=65535 Len=0
   6191 44.346374107 10.0.2.15       44.228.249.3    TCP        54 [TCP Keep-Alive] 46678 → 80 [ACK] Seq=289 Ack=2560 Win=6
   6192 44.346669926 44.228.249.3    10.0.2.15       TCP        54 [TCP Keep-Alive ACK] 80 → 46678 [ACK] Seq=2560 Ack=290 W
   6193 45.371851644 10.0.2.15       44.228.249.3    TCP        54 [TCP Keep-Alive] 46708 → 80 [ACK] Seq=390 Ack=182 Win=64
   6194 45.372358814 44.228.249.3    10.0.2.15       TCP        54 [TCP Keep-Alive ACK] 80 → 46708 [ACK] Seq=182 Ack=391 Wi
```

```
› Frame 6179: Packet, 580 bytes on wire (4640 bits), 580 bytes capture
› Ethernet II, Src: 4a:41:1e:e4:26:e4 (4a:41:1e:e4:26:e4), Dst: 52:55:
› Internet Protocol Version 4, Src: 10.0.2.15, Dst: 44.228.249.3
› Transmission Control Protocol, Src Port: 46692, Dst Port: 80, Seq: 1
› Hypertext Transfer Protocol
› HTML Form URL Encoded: application/x-www-form-urlencoded
```

```
0000  52 55 0a 00 02 02 4a 41  1e e4 26 e4 08 00 45 00   RU····JA ··&···E·
0010  02 36 72 c4 40 00 40 06  94 07 0a 00 02 0f 2c e4   ·6r·@·@· ······,·
0020  f9 03 b6 64 00 50 2b 79  07 68 00 98 6d 72 50 18   ···d·P+y ·h··mrP·
0030  ff ff f4 d9 00 00 50 4f  53 54 20 2f 75 73 65 72   ······PO ST /user
0040  69 6e 66 6f 2e 70 68 70  20 48 54 54 50 2f 31 2e   info.php  HTTP/1.
0050  31 0d 0a 48 6f 73 74 3a  20 74 65 73 74 70 68 70   1··Host:  testphp
0060  2e 76 75 6c 6e 77 65 62  2e 63 6f 6d 0d 0a 55 73   .vulnweb .com··Us
0070  65 72 2d 41 67 65 6e 74  3a 20 4d 6f 7a 69 6c 6c   er-Agent : Mozill
0080  61 2f 35 2e 30 20 28 58  31 31 3b 20 4c 69 6e 75   a/5.0 (X 11; Linu
0090  78 20 78 38 36 5f 36 34  3b 20 72 76 3a 31 34 30   x x86_64 ; rv:140
00a0  2e 30 29 20 47 65 63 6b  6f 2f 32 30 31 30 30 31   .0) Geck o/201001
```

wireshark_eth08TSAH3.pcapng
Packets: 6194 · Dropped: 0 (0.0%)
Profile: Default



(genmon)XXX
20:41
*eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>

```
No.     Time         Source          Destination     Protocol Length Info
   6172 41.275980485 10.0.2.15       142.250.192.35  TCP        54 [TCP Keep-Alive] 36768 → 80 [ACK] Seq=4281 Ack=11026 Win
   6173 41.276001446 10.0.2.15       44.228.249.3    TCP        74 [TCP Retransmission] 49340 → 443 [SYN] Seq=0 Win=64240 L
   6174 41.276006279 10.0.2.15       44.228.249.3    TCP        74 [TCP Retransmission] 49348 → 443 [SYN] Seq=0 Win=64240 L
   6175 41.276387404 142.250.192.35  10.0.2.15       TCP        54 [TCP Keep-Alive ACK] 80 → 60290 [ACK] Seq=5513 Ack=2138
   6176 41.276387779 142.250.192.35  10.0.2.15       TCP        54 [TCP Keep-Alive ACK] 80 → 36768 [ACK] Seq=11026 Ack=4282
   6177 41.530423172 10.0.2.15       44.228.249.3    TCP        74 [TCP Retransmission] 36886 → 443 [SYN] Seq=0 Win=64240 L
   6178 41.530460092 10.0.2.15       44.228.249.3    TCP        74 [TCP Retransmission] 36876 → 443 [SYN] Seq=0 Win=64240 L
   6179 41.560317566 10.0.2.15       44.228.249.3    HTTP      580 POST /userinfo.php HTTP/1.1  (application/x-www-form-url
```

```
    [Server Contiguous Streams: 1]
    TCP payload (526 bytes)
⌄ Hypertext Transfer Protocol
  ⌄ POST /userinfo.php HTTP/1.1\r\n
      Request Method: POST
      Request URI: /userinfo.php
      Request Version: HTTP/1.1
    Host: testphp.vulnweb.com\r\n
    User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:140.0) Gecko/20100
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*
    Accept-Language: en-US,en;q=0.5\r\n
    Accept-Encoding: gzip, deflate\r\n
    Content-Type: application/x-www-form-urlencoded\r\n
  › Content-Length: 22\r\n
    Origin: http://testphp.vulnweb.com\r\n
    Connection: keep-alive\r\n
    Referer: http://testphp.vulnweb.com/login.php\r\n
    Upgrade-Insecure-Requests: 1\r\n
    Priority: u=0, i\r\n
    \r\n
    [Response in frame: 6185]
    [Full request URI: http://testphp.vulnweb.com/userinfo.php]
    File Data: 22 bytes
⌄ HTML Form URL Encoded: application/x-www-form-urlencoded
  › Form item: "uname" = "admin"
  › Form item: "pass" = "admin"
```

```
0000  52 55 0a 00 02 02 4a 41  1e e4 26 e4 08 00 45 00   RU····JA ··&···E·
0010  02 36 72 c4 40 00 40 06  94 07 0a 00 02 0f 2c e4   ·6r·@·@· ······,·
0020  f9 03 b6 64 00 50 2b 79  07 68 00 98 6d 72 50 18   ···d·P+y ·h··mrP·
0030  ff ff f4 d9 00 00 50 4f  53 54 20 2f 75 73 65 72   ······PO ST /user
0040  69 6e 66 6f 2e 70 68 70  20 48 54 54 50 2f 31 2e   info.php  HTTP/1.
0050  31 0d 0a 48 6f 73 74 3a  20 74 65 73 74 70 68 70   1··Host:  testphp
0060  2e 76 75 6c 6e 77 65 62  2e 63 6f 6d 0d 0a 55 73   .vulnweb .com··Us
0070  65 72 2d 41 67 65 6e 74  3a 20 4d 6f 7a 69 6c 6c   er-Agent : Mozill
0080  61 2f 35 2e 30 20 28 58  31 31 3b 20 4c 69 6e 75   a/5.0 (X 11; Linu
0090  78 20 78 38 36 5f 36 34  3b 20 72 76 3a 31 34 30   x x86_64 ; rv:140
00a0  2e 30 29 20 47 65 63 6b  6f 2f 32 30 31 30 30 31   .0) Geck o/201001
00b0  30 31 20 46 69 72 65 66  6f 78 2f 31 34 30 2e 30   01 Firef ox/140.0
00c0  0d 0a 41 63 63 65 70 74  3a 20 74 65 78 74 2f 68   ··Accept : text/h
00d0  74 6d 6c 2c 61 70 70 6c  69 63 61 74 69 6f 6e 2f   tml,appl ication/
00e0  78 68 74 6d 6c 2b 78 6d  6c 2c 61 70 70 6c 69 63   xhtml+xm l,applic
00f0  61 74 69 6f 6e 2f 78 6d  6c 3b 71 3d 30 2e 39 2c   ation/xm l;q=0.9,
0100  2a 2f 2a 3b 71 3d 30 2e  38 0d 0a 41 63 63 65 70   */*;q=0. 8··Accep
0110  74 2d 4c 61 6e 67 75 61  67 65 3a 20 65 6e 2d 55   t-Langua ge: en-U
0120  53 2c 65 6e 3b 71 3d 30  2e 35 0d 0a 41 63 63 65   S,en;q=0 .5··Acce
0130  70 74 2d 45 6e 63 6f 64  69 6e 67 3a 20 67 7a 69   pt-Encod ing: gzi
0140  70 2c 20 64 65 66 6c 61  74 65 0d 0a 43 6f 6e 74   p, defla te··Cont
0150  65 6e 74 2d 54 79 70 65  3a 20 61 70 70 6c 69 63   ent-Type : applic
0160  61 74 69 6f 6e 2f 78 2d  77 77 77 2d 66 6f 72 6d   ation/x- www-form
0170  2d 75 72 6c 65 6e 63 6f  64 65 64 0d 0a 43 6f 6e   -urlenco ded··Con
0180  74 65 6e 74 2d 4c 65 6e  67 74 68 3a 20 32 32 0d   tent-Len gth: 22·
0190  0a 4f 72 69 67 69 6e 3a  20 68 74 74 70 3a 2f 2f   ·Origin:  http://
```

wireshark_eth08TSAH3.pcapng
Packets: 6194 · Dropped: 0 (0.0%)
Profile: Default