

Network Challenges:

Here, they provided a PCAPNG file named “captured.pcapng”. Then they asked some questions.

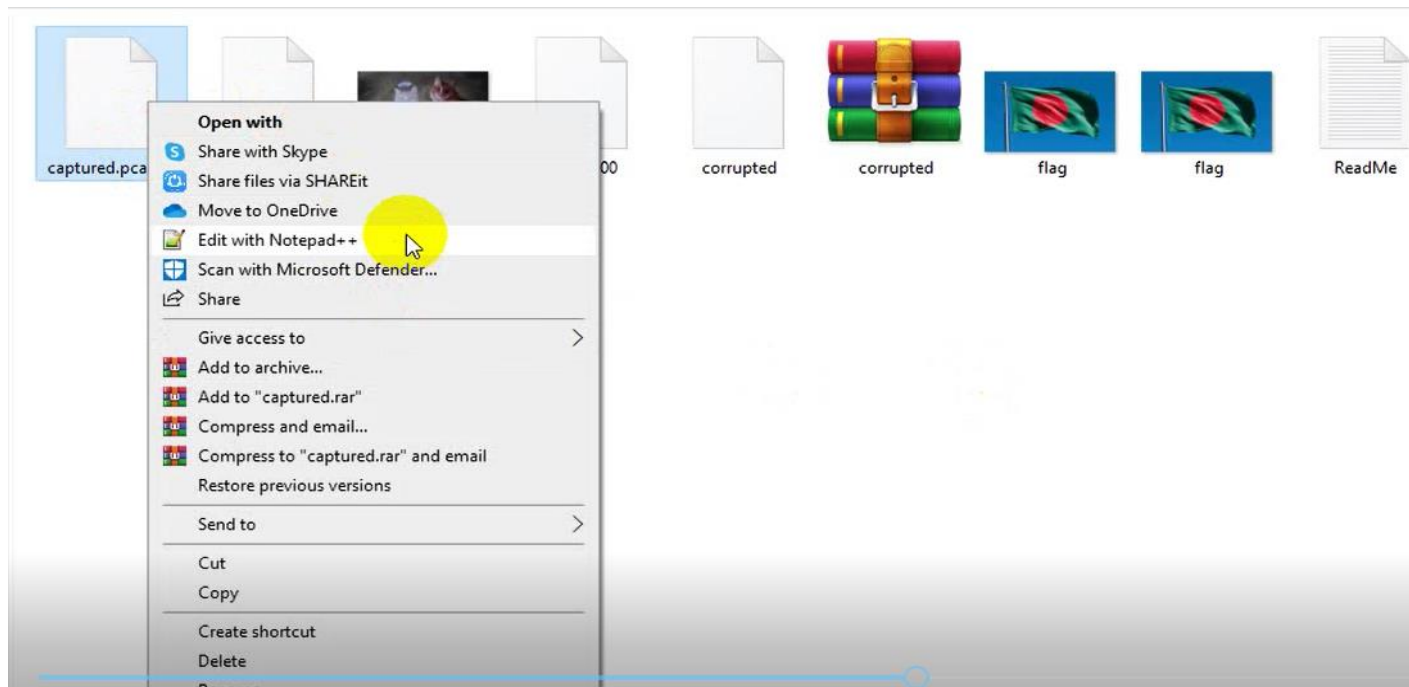
Question No: 01

Which tools attacker used to find vulnerability?

Solution:

Step-01: I downloaded that **PCAPNG** file at first.

Step-02: Opened it with **Notepad++**.



Step-03: Then pressed **Ctrl+F** and opened the search option. Then I read the question again.

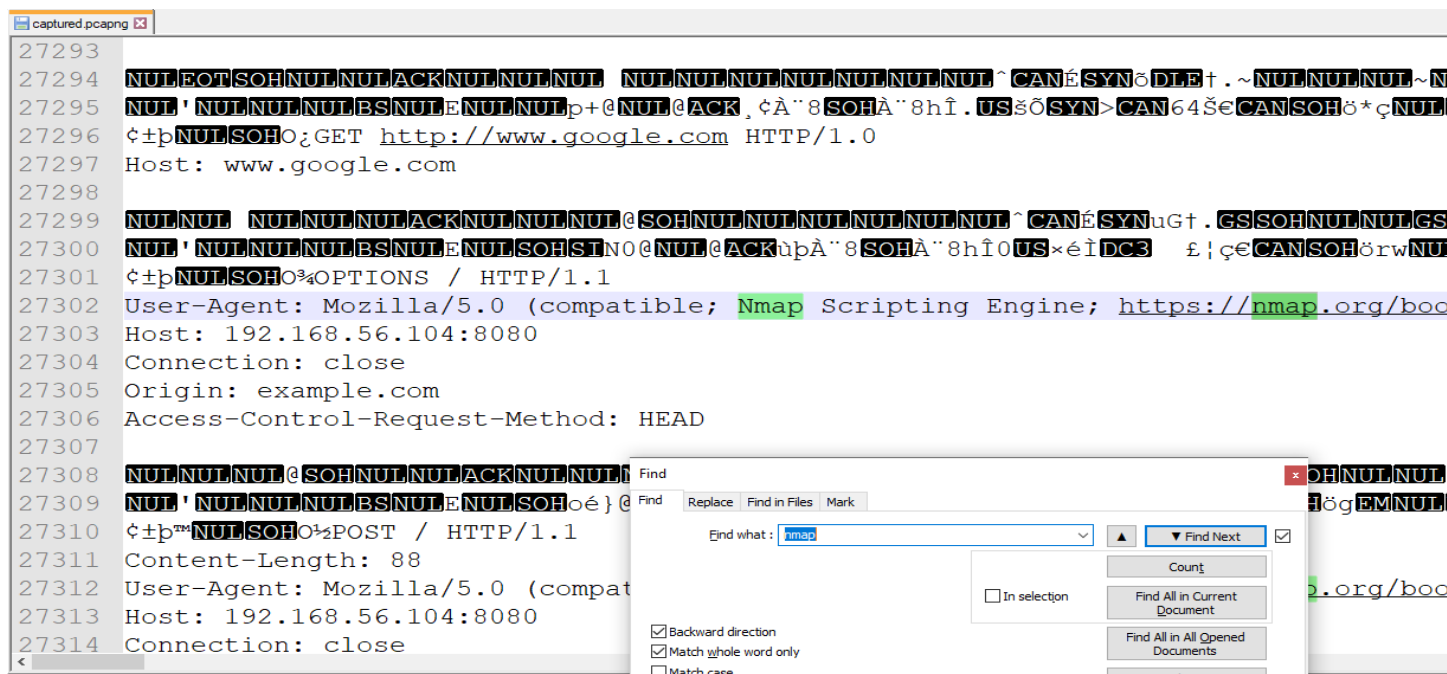
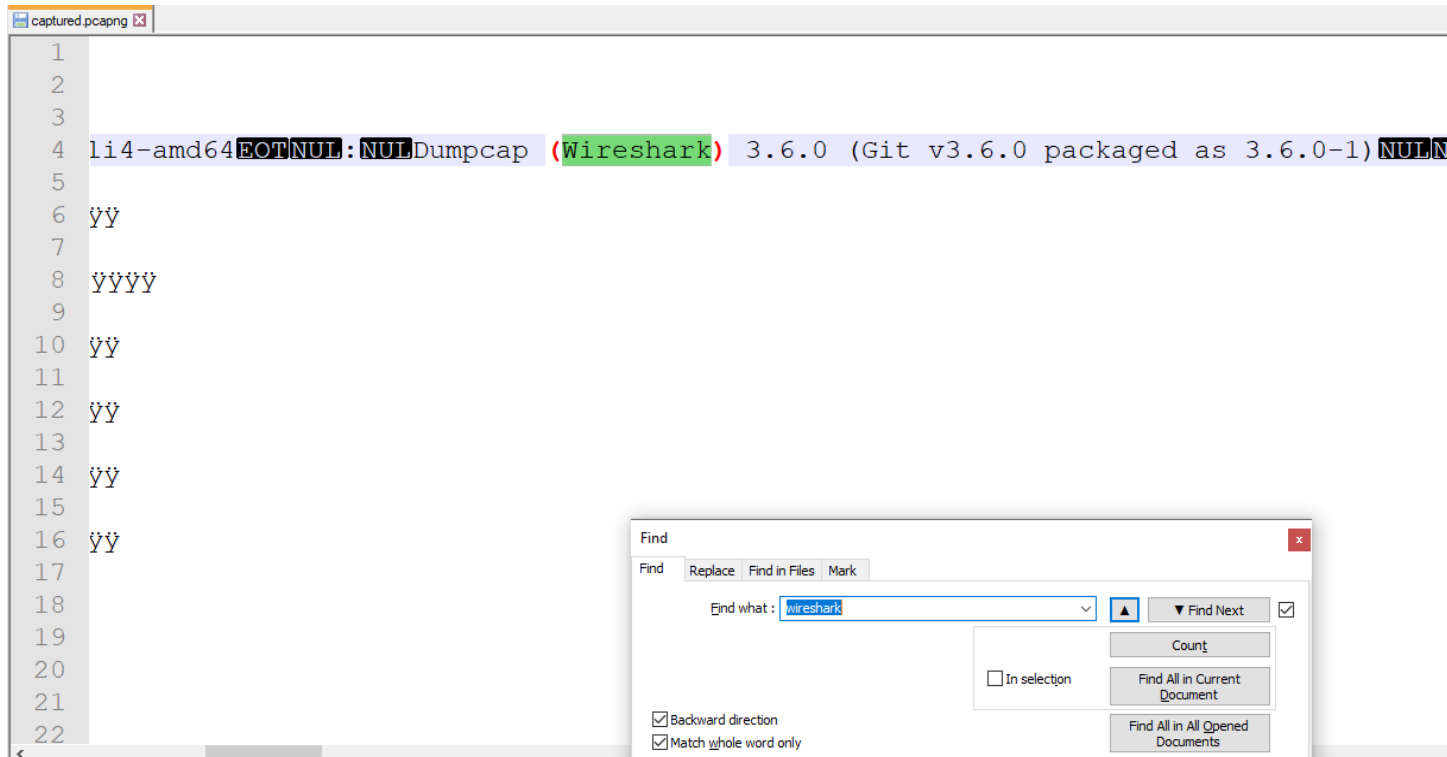
As they asked for tool's name so I

randomly put some known tool's name (**kismet, nikto, wireshark, nmap...**) and searched it in that file.

And I found 2 tools name, one is **wireshark** and another is **nmap**.

Step-04: I put **IIUC{wireshark}** (as it was the flag format) in the flag submission box at first. but it was incorrect.

Step-05: Then I tried with **IIUC{nmap}** and It was the correct flag.



Question No: 02

Which port is running vulnerable service?

Solution:

Step-01: When I solved the first question, I got a host IP address and a port, that is **8080**.

Step-02: So I put that port in the flag submission box following the flag format: **IIUC{8080}** and it was the correct flag.

27293
27294 NULÉOT|SOHNULNULACKNULNULNUL NULNULNULNULNULNULNUL ^CANÉSYNöDLE+.~NULNULNUL~NUL
27295 NUL'NULNULNULBSNULENULNULp+@NUL@ACK,çÀ`8SOHÀ`8hîf.USšÖSYN>CAN64ŠeCANSOHö*çNUL
27296 ç+pNULSOHO¿GET http://www.google.com HTTP/1.0
27297 Host: www.google.com
27298
27299 NULNUL NULNULNULACKNULNULNUL@SOHNULNULNULNULNULNUL ^CANÉSYNuGt.GSSOHNULNULGS
27300 NUL'NULNULNULBSNULENULSOHSTIN0@NUL@ACKùpÀ`8(SOHÀ`8hîf0US×éìDC3 ε|ç€CANSOHörwNUL
27301 ç+pNULSOHO%OPTIONS / HTTP/1.1
27302 User-Agent: Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/boo
27303 Host: 192.168.56.104:8080
27304 Connection: close
27305 Origin: example.com
27306 Access-Control-Request-Method: HEAD
27307
27308 NULNULNUL@SOHNULNULACKNULNULNUL SOHNULNULNULNULNULNUL ^CANÉSYNI|+.}SOHNULNUL
27309 NUL'NULNULNULBSNULENULSOHoé}|CNULESOHQñ8SOHÀ`8hî4USCANÚ+æâ!â€CANSOHögEMNUL
27310 ç+pNULSOHO%POST / HTTP/1.1
27311 Content-Length: 88
27312 User-Agent: Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/boo
27313 Host: 192.168.56.104:8080
27314 Connection: close

Question No: 04

What is the root flag?

Solution:

Step-01: For the root flag, I searched with the flag format directly as **"IIUC "**and I got a flag which is down to the **"root/flag.txt"** line. The Flag is **IIUC{D0N7_U53_Kn0wN_VuLn3r4BiL17y}**.

Step-02: I just copied the whole flag and pasted it into the flag submission box and it was correct.

```
captured pcapng x
30159 NUL'NULNULNULBSNUL'yøDC4BSNULENULNULT>~@NUL@ACK-:À`8hÀ`8SOH±#DC1\EìðAÛI´ýeCAN
30160 NULSTXCEMç¶i°VBoxGuestAdditions.iso
30161 flag.txt
30162 NULNUL,,NULNULNULACKNULNULNULdNULNULNULNULNULNULNULO CANÉSYNéšø-BNULNULNULBNUL
30163 NUL'NULNULNULBSNULENULNUL4¶P@NUL@ACK'¹À`8SOHÀ`8hDC1\±#ÛI´ýEìðaeDLESOHpR`NULNU
30164 ç¶i»NULSTXCEMNULNULdNULNULNULACKNULNULNULhNULNULNULNULNULNULO CANÉSYN-OëGF
30165 NUL'NULNULNUL+Ý`NULNULNULNULDLE:yþeNULNULNULNULNULNULBSNUL'yþNULNULNULySTXNU
30166 NUL'NULNULNULNULNULhNULNULNULACKNULNULNULxNULNULNULNULNULNULO CANÉSYNeI,zU
30167 NUL'NULNULNULBSNULENULNULG¶Q@NUL@ACK'¥À`8SOHÀ`8hDC1\±#ÛI´ýEìðaeCANSOHP¼'NULNU
30168 ç·"%NULSTXCEMcat /root/flag.txt
30169 NULNULNULxNULNULNULACKNULNULNUL~NULNULNULNULNULNULNULO CANÉSYNDc2î;zèNULNULNU
30170 NUL'NULNULNULBSNUL'yøDC4BSNULENULNULW>°@NUL@ACK-6À`8hÀ`8SOH±#DC1\EìðAUipDLEEÇ
30171 NULSTXiç·"%IIUC{D0N7_U53_Kn0wN_VuLn3r4BiL17y}
30172 NULNULNUL~NULNULNULACKNULNULNULdNULNULNULNULNULNULO CANÉSYNc<žBNULNULNULBN
30173 NUL'NULNULNULBSNULENULNUL4¶R@NUL@ACK'·À`8SOHÀ`8hDC1\±#ÛipDLEEïð„eDLESOHPDC2SN
30174 ç·"%ŠNULSTXiNULNULdNULNULNULAC Find
30175 NUL'NULNULNULBSNULENULNUL>¶S@ Find Replace Find in Files Mark
30176 ç·E]NULSTXi¶pass root Find what : IIUC ▲ ▼ Find Next ☑
30177 lNULNULNULACKNULNULNULdNULNUL In selection Count
30178 NUL'NULNULNULBSNUL'yøDC4BSNUL Find All in Current Document
30179 NULSTX³Mç·E]NULNULdNULNULNULA Find All in All Opened Documents
30180 NUL'NULNULNULBSNULENULNUL9¶T@
```

Question No: 06

How many packed captured on this file?

Solution:

Step-01: At first, I opened the file of Question No:01 with **Wireshark**.

Step-02: Then clicked at **Statistics > Capture File Properties**. At the bottom, of **Capture File Properties**, I got some informations of that file including the count of **Packets Captured**.

Step-03: I entered the number into the flag format like this: **IIUC{14695}** and it was a correct flag.

Statistics			
Measurement	Captured	Displayed	Marked
Packets	14695	14695 (100.0%)	—
Time span, s	756.029	756.029	—
Average pps	19.4	19.4	—
Average packet size, B	49	49	—
Bytes	727130	727130 (100.0%)	0
Average bytes/s	961	961	—
Average bits/s	7694	7694	—

Made By:

Omar Hasnain Mahmud