

NeverLAN CTF

Pcap : FTP

Value : 100 pts

Difficulty : Easy

Description : Your flag will be in the normal flag{flagGoesHere} syntax.

Attachment : It looks like someone forgot to use a secure version of ftp...

ftp.pcap

Solution :

A pcap file is given. It can be opened with Wireshark.

This time, the user is accessing files with FTP. Credentials and files are sent in clear text through the network.

First, we'll try to search the credentials of the user to see if the flag is the password.

Passwords are sent with PASS commands, with this protocol. We can search these requests in Wireshark by applying the following filter: ftp.request.command == PASS.

ftp.request.command == PASS							
No.	Time	Source	Destination	Protocol	Length	Request command	Info
11	0.001067	192.168.23.42	192.168.23.46	FTP	92	PASS	Request: PASS mozilla@example.com
36	0.020110	192.168.23.42	192.168.23.46	FTP	82	PASS	Request: PASS raspberry
105	0.000466	192.168.23.42	192.168.23.46	FTP	92	PASS	Request: PASS mozilla@example.com
129	0.020290	192.168.23.42	192.168.23.46	FTP	82	PASS	Request: PASS raspberry

It seems that this time, the flag isn't a password.

The next thing we can search are files. To search for file transfers, we can search for ftp-data in the filter. A file flag.txt was accessed:

ftp-data

No.	Time	Source	Destination	Protocol	Length	Request command	Info
85	0.000185	192.168.23.46	192.168.23.42	FTP-DA...	131		FTP Data: 65 bytes (PASV) (CWD /home/pi/)
181	0.000100	192.168.23.46	192.168.23.42	FTP-DA...	93		FTP Data: 27 bytes (PASV) (SIZE /home/pi/flag.txt)

Frame 181: 93 bytes on wire (744 bits), 93 bytes captured (744 bits)

Ethernet II, Src: Raspberr_11:47:52 (dc:a6:32:11:47:52), Dst: HengeDoc_51:6f:9e (bc:6a:2f:51:6f:9e)

Internet Protocol Version 4, Src: 192.168.23.46, Dst: 192.168.23.42

Transmission Control Protocol, Src Port: 42781, Dst Port: 56409, Seq: 1, Ack: 1, Len: 27

FTP Data (27 bytes data)

Setup frame: 168

[Setup method: PASV]

[Command: SIZE /home/pi/flag.txt]

Command frame: 170

[Current working directory: /home/pi]

Line-based text data (1 lines)

flag{sftp_OR_ftps_not_ftp}\n