Networking

FTP - authentication

Download
Open with wire shark
follow TCP stream

Flag = cdts3500

TELNET - authentication

same as First challenge

Flag = user

ETHERNET - frame

https://hpd.gasmi.net/

decode the ethernet fram in this website
and check the http section for the authentication

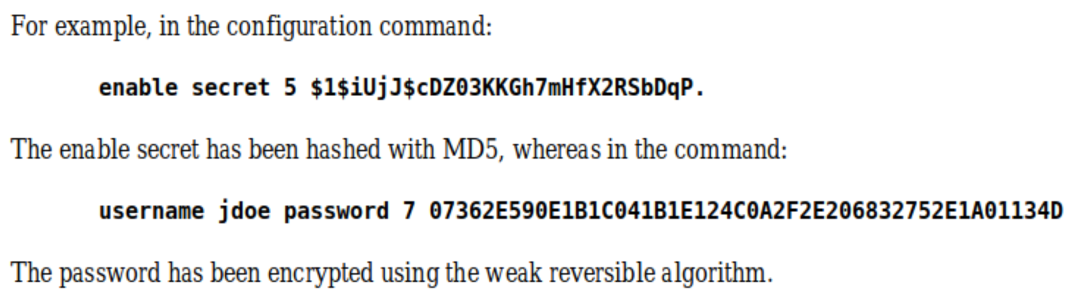
Flag = confi:dential

Twitter authentication

Open with wireshark
check the authorization
Decode with burp base 64
Flag = password

CISCO - password

this is from the reference given



For example, in the configuration command:

```
enable secret 5 $1$iUjJ$cDZ03KKGh7mHfX2RSbDqP.
```

The enable secret has been hashed with MD5, whereas in the command:

```
username jdoe password 7 07362E590E1B1C041B1E124C0A2F2E206832752E1A01134D
```

The password has been encrypted using the weak reversible algorithm.

we can decrypt level 7 passwords so lets do this
http://x.almx.cc/cisco-type7-cracker.html

hub password = 025017705B3907344E --> 6sK0_hub
admin password = 6sK0_admin

we find a pattern

Flag = 6sK0_enable

CISCO - password

check the packets with wireshark

you will find the host sending ICMP ping requests with increasing ttl
he gets ttl exceeded until he reaches 13 then he recieves a response

Flag = 13

DNS - zone transfert

```
nslookup challenge01.root-me.org
```

we get the ip 212.129.38.224
now we do dns zone transfer

```
dig [@server] [-p port#][name]
dig @212.129.38.224 -p 54011 axfr ch11.challenge01.root-me.org
```

Output:

```
; <<>> DiG 9.11.5-P4-5.1+b1-Debian <<>> @212.129.38.224 -p 54011 axfr
ch11.challenge01.root-me.org
; (1 server found)
;; global options: +cmd
ch11.challenge01.root-me.org. 604800 IN        SOA   ch11.challenge01.root-me.org.
root.ch11.challenge01.root-me.org. 2 604800 86400 2419200 604800
ch11.challenge01.root-me.org. 604800 IN        TXT   "DNS transfer secret key :
CBkFRwfNMMtRjHY"
ch11.challenge01.root-me.org. 604800 IN        NS    ch11.challenge01.root-me.org.
ch11.challenge01.root-me.org. 604800 IN        A     127.0.0.1
challenge01.ch11.challenge01.root-me.org. 604800 IN A 192.168.27.101
ch11.challenge01.root-me.org. 604800 IN        SOA   ch11.challenge01.root-me.org.
root.ch11.challenge01.root-me.org. 2 604800 86400 2419200 604800
;; Query time: 77 msec
;; SERVER: 212.129.38.224#54011(212.129.38.224)
;; WHEN: Sat Feb 29 06:55:00 EST 2020
;; XFR size: 6 records (messages 1, bytes 246)
```

SIP - authentication

```
apt install sipcrack
sipcrack -w /usr/share/wordlists/rockyou.txt ch4.txt
```

press 2 --> 1234

Flag = 1234