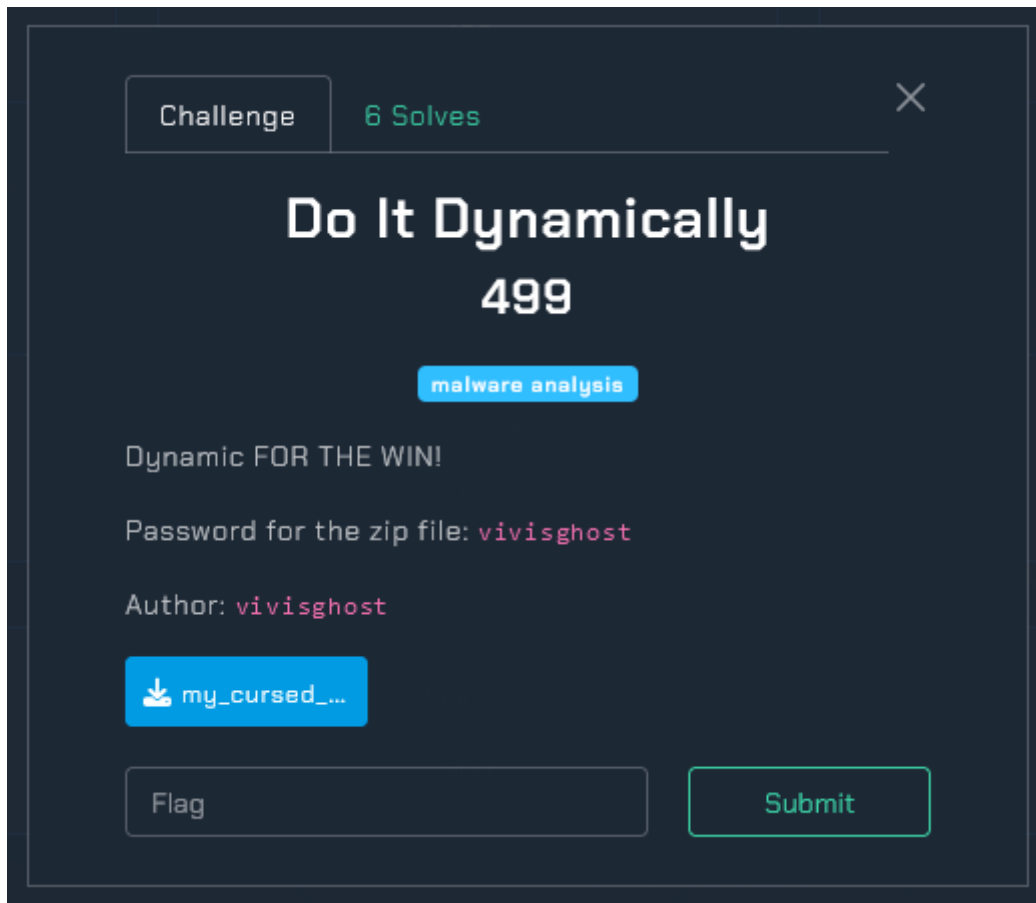


# Do It Dynamically Walkthrough



The goal of this challenge is to teach players how to monitor network traffic while dynamically analyzing malware. The executable comprises three stages:

1. **Ping the IP 10.0.0.6 and wait for response**
2. **If response send question**
3. **If answer correct, send the flag**

To solve this we can set up a listener on this IP by either changing the host machine's IP or configuring an internal network.

If a response is received, the executable prints a fake flag in its execution directory and sends a query to port 1234 on the same IP.

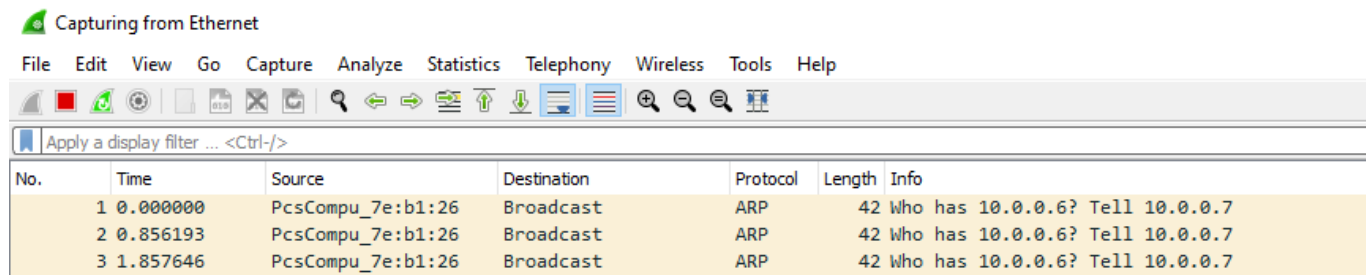
Correctly answering the query prompts the executable to send the real flag to port 1337 on the same IP.

## Solve with 2 machines on internal network

## The Cursed executable

```
(kali㉿kali)-[~/Desktop/cursed_exe]
$ file my_cursed_executable.exe
my_cursed_executable.exe: PE32+ executable (console) x86-64, for MS Windows, 19 sections
```

Running the executable with Wireshark shows the exe network traffic.



Capturing from Ethernet

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	PcsCompu_7e:b1:26	Broadcast	ARP	42	Who has 10.0.0.6? Tell 10.0.0.7
2	0.856193	PcsCompu_7e:b1:26	Broadcast	ARP	42	Who has 10.0.0.6? Tell 10.0.0.7
3	1.857646	PcsCompu_7e:b1:26	Broadcast	ARP	42	Who has 10.0.0.6? Tell 10.0.0.7

Virus total shows evidence of the ping too.

---

**Process and service actions** ⓘ

---

**Processes Created**

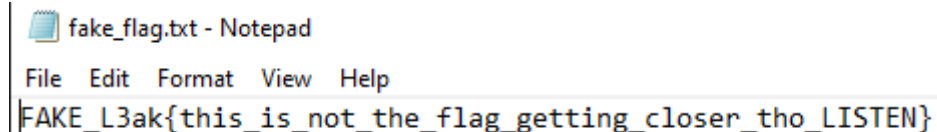
- 📁 "C:\Users\<USER>\AppData\Local\Temp\my\_cursed\_executable.exe"
- 📁 C:\Windows\system32\WerFault.exe -u -p 4328 -s 528
- 📁 C:\Windows\system32\cmd.exe /c ping -n 1 -w 1000 10.0.0.6 > NUL
- 📁 ping -n 1 -w 1000 10.0.0.6

Now I connect a second VM to the network with IP 10.0.0.6 and run the executable again.

When the executable receives a ping response it will

1. Print a fake/hint flag to the same directory as the exe was ran.
2. and try to reach out to port 1234.

Fake flag encourages player to actively listen



```
fake_flag.txt - Notepad
File Edit Format View Help
FAKE_L3ak{this_is_not_the_flag_getting_closer_tho_LISTEN}
```


Wireshark shows fails if a listener is not set up on port 1234.

21	13.581037	10.0.0.7	10.0.0.6	TCP	66	49685 → 1234 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
22	13.581453	10.0.0.6	10.0.0.7	TCP	60	1234 → 49685 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
23	14.111366	10.0.0.7	10.0.0.6	TCP	66	[TCP Retransmission] 49685 → 1234 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 S...
24	14.112448	10.0.0.6	10.0.0.7	TCP	60	1234 → 49685 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
25	14.342826	PcsCompu_21:b1:d0	Broadcast	ARP	60	Who has 10.0.2.2? Tell 10.0.2.15
26	14.626129	10.0.0.7	10.0.0.6	TCP	66	[TCP Retransmission] 49685 → 1234 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 S...
27	14.627011	10.0.0.6	10.0.0.7	TCP	60	1234 → 49685 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
28	15.157333	10.0.0.7	10.0.0.6	TCP	66	[TCP Retransmission] 49685 → 1234 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 S...
29	15.157792	10.0.0.6	10.0.0.7	TCP	60	1234 → 49685 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
30	15.367228	PcsCompu_21:b1:d0	Broadcast	ARP	60	Who has 10.0.2.2? Tell 10.0.2.15
31	15.658194	10.0.0.7	10.0.0.6	TCP	66	[TCP Retransmission] 49685 → 1234 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 S...
32	15.658851	10.0.0.6	10.0.0.7	TCP	60	1234 → 49685 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0

If a listener is setup the player receives a question.

```
(kali㉿kali)-[~]  
$ nc -nvlp 1234  
listening on [any] 1234 ...  
connect to [10.0.0.6] from (UNKNOWN) [10.0.0.7] 49688  
Who is the author of this challenge?(lowercase)vivisghost
```

Below shows the output of the executable if the correct answer is entered. Another hint to set up a second listener on port 1337 is also given.

 C:\Users\Blue\Desktop\my\_cursed\_executable.exe

```
Received response. Prepare to initiate sequence.  
Validating Response.....(really installing malware)... Lulz jk  
Correct response received: vivisghost made this.  
They say people with 1337 listening skills can hold 2 conversations at once, idk tho...
```

Using the same idea for port 1337 gives the flag

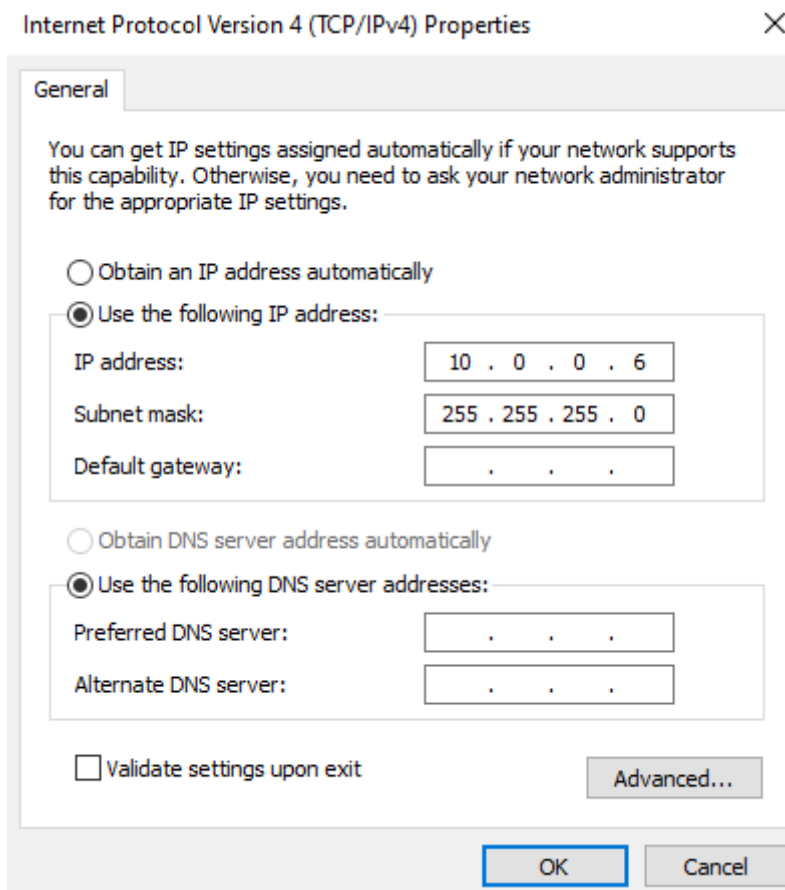
```
(kali㉿kali)-[~]  
$ nc -nvlp 1337  
listening on [any] 1337 ...  
connect to [10.0.0.6] from (UNKNOWN) [10.0.0.7] 49691  
L3AK{L34rN_2_L1573N_2_6H0575}
```

## On One Machine

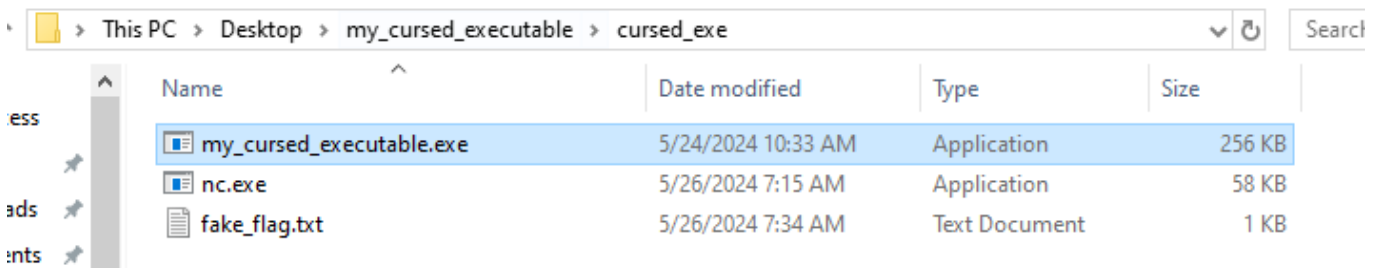
The above solve involves 2 machines on an internal network. This could have been done with a single machine as well.

Bring nc.exe to the machine, change machine IP to 10.0.0.6.

Network Ethernet Settings -> Change adaptor options -> Ethernet -> Properties -> Internet Protocol Version 4 (TCP/IPv4) -> Properties



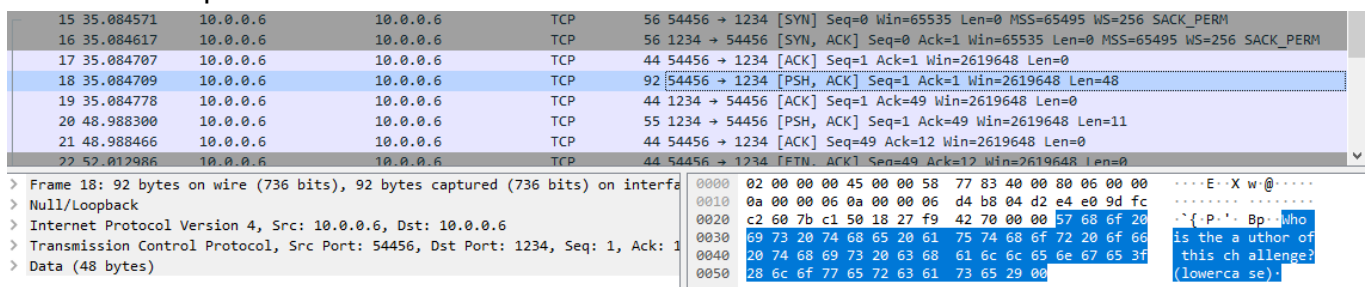
Confirm settings and run executable. We can see ping worked as fake/hint flag was printed.



Set up nc connections and run again.

```
PS C:\Users\Blue\Desktop\my_cursed_executable\cursed_exe> .\nc.exe -l -p 1234
Who is the author of this challenge?(lowercase) vivisghost
```

Can also see plaintext traffic in wireshark.



```
PS C:\Users\Blue\Desktop\my_cursed_executable\cursed_exe> .\nc.exe -l -p 1337
L3AK{L34rN_2_L1573N_2_6H0575}
```

Again in wireshark.

Wireshark interface showing a network capture. The packet list displays several TCP packets. The selected packet (No. 29) is a TCP packet from 10.0.0.6 to 10.0.0.6, Seq=1, Ack=1, Win=2619648, Len=29. The packet details pane shows the Internet Protocol Version 4 and Transmission Control Protocol headers. The packet bytes pane shows the raw data, which is the netcat command output: L3AK{L34rN\_2\_L1573N\_2\_6H0575}.

## Conclusion

Understanding how to monitor and interact with network traffic during malware analysis is crucial for cybersecurity professionals. This challenge demonstrates techniques that can be applied to identify and communicate with malicious beacons. By setting up listeners and responding to malware queries, analysts can uncover command and control (C2) infrastructure, gather intelligence on threat actor behavior, and develop effective countermeasures.