# Active Recon

Target IP : 10.10.158.153

Completed : No walkth

## Web Inspect

let step = 1;

let questions = {

1 : {

'speaking' : 'alice',

'answer\_1' : 'SYN : Can you hear me Bob?',

'answer\_2' : 'FIN : Goodbye',

'answer\_3' : 'ACK : Erm... What?',

'answer' : 1

},

2 : {

'speaking' : 'bob',

'answer\_1' : 'RST : Cya Later',

'answer\_2' : 'PING : 77',

'answer\_3' : 'SYN/ACK : Yes, I can hear you!',

'answer' : 3

},

3 : {

'speaking' : 'alice',

'answer\_1' : 'FAIL : SEGMENTATION FAULT',

'answer\_2' : 'ACK : Okay Great',

'answer\_3' : 'SYN : x = 3?',

'answer' : 2

},

4 : {

'speaking' : 'alice',

'answer\_1' : 'ICMP : 99',

'answer\_2' : 'SYN : Yes, I can hear you!',

'answer\_3' : 'DATA : Cheesecake is on sale!',

'answer' : 3

},

5 : {

'speaking' : 'bob',

'answer\_1' : 'ACK : I Hear ya!',

'answer\_2' : 'REPEAT : What?',

'answer\_3' : 'RESET : Help!',

'answer' : 1

},

6 : {

'speaking' : 'alice',

'answer\_1' : 'ACK : OK',

'answer\_2' : 'FIN/ACK : I\'m all done',

'answer\_3' : 'ECHO : Retry',

'answer' : 2

},

7 : {

'speaking' : 'bob',

'answer\_1' : 'SYN : Received',

'answer\_2' : 'WIRE : Reset Connection',

'answer\_3' : 'FIN/ACK : Yeah Me Too',

'answer' : 3

},

8 : {

'speaking' : 'alice',

'answer\_1' : 'SYN : Connected',

'answer\_2' : 'ACK : Okay, Goodbye',

'answer\_3' : 'SYN/ACK : Not Received',

'answer' : 2

}

}

function answered(){

if( this.id.substr(9,100) === questions[step].speaking ) {

document.getElementsByClassName('error')[0].style.display='none';

let answer\_id = parseInt(this.id.replace('answer\_', '').replace('\_' + questions[step].speaking, ''));

if (answer\_id === questions[step].answer) {

for(let i=1;i<4;i++) {

document.getElementById('answer\_' + i + '\_' + questions[step].speaking).style.display = 'none';

}

document.getElementById('answer\_' + answer\_id + '\_' + questions[step].speaking).style.display = 'block';

document.getElementById('answer\_' + answer\_id + '\_' + questions[step].speaking).style.backgroundColor = '#b3b3b3';

document.getElementById(questions[step].speaking + '-bubble').style.opacity = '0.6';

step++;

if( step === 9 ) {

document.getElementById( 'alice-bubble' ).style.opacity='0';

document.getElementById( 'bob-bubble' ).style.opacity='0';

document.getElementsByClassName('flag\_inner')[0].innerHTML='THM{TCP\_CHATTER}';

document.getElementsByClassName('flag')[0].style.display='block';

}else {

document.getElementById(questions[step].speaking + '-bubble').style.opacity = '1';

for(let i=1;i<4;i++){

document.getElementById('answer\_' + i + '\_' + questions[step].speaking).style.backgroundColor = '#2a5a14';

document.getElementById('answer\_' + i + '\_' + questions[step].speaking).innerHTML = questions[step]['answer\_' + i];

document.getElementById('answer\_' + i + '\_' + questions[step].speaking).style.display = 'block';

}

}

} else {

document.getElementsByClassName('error')[0].style.display='block';

}

}

}

for(let i=1;i<4;i++){

document.getElementById('answer\_' + i + '\_' + questions[step].speaking ).innerHTML=questions[step]['answer\_' + i];

document.getElementById('answer\_' + i + '\_alice').addEventListener('click',answered);

document.getElementById('answer\_' + i + '\_bob').addEventListener('click',answered);

}

setTimeout(function(){

document.getElementById( questions[step].speaking + '-bubble' ).style.opacity='1';

},500);

## ping

└─$ ping 10.10.158.153

PING 10.10.158.153 (10.10.158.153) 56(84) bytes of data.

64 bytes from 10.10.158.153: icmp\_seq=1 ttl=60 time=241 ms

64 bytes from 10.10.158.153: icmp\_seq=2 ttl=60 time=264 ms

64 bytes from 10.10.158.153: icmp\_seq=3 ttl=60 time=186 ms

64 bytes from 10.10.158.153: icmp\_seq=4 ttl=60 time=162 ms

64 bytes from 10.10.158.153: icmp\_seq=5 ttl=60 time=230 ms

64 bytes from 10.10.158.153: icmp\_seq=6 ttl=60 time=253 ms

64 bytes from 10.10.158.153: icmp\_seq=7 ttl=60 time=173 ms

64 bytes from 10.10.158.153: icmp\_seq=8 ttl=60 time=196 ms

64 bytes from 10.10.158.153: icmp\_seq=9 ttl=60 time=228 ms

64 bytes from 10.10.158.153: icmp\_seq=10 ttl=60 time=255 ms

64 bytes from 10.10.158.153: icmp\_seq=11 ttl=60 time=162 ms

64 bytes from 10.10.158.153: icmp\_seq=12 ttl=60 time=185 ms

^C

--- 10.10.158.153 ping statistics ---

12 packets transmitted, 12 received, 0% packet loss, time 11014ms

rtt min/avg/max/mdev = 161.515/211.213/264.076/36.409 ms

## traceroute

└─$ traceroute 10.10.158.153

traceroute to 10.10.158.153 (10.10.158.153), 30 hops max, 60 byte packets

1 10.17.0.1 (10.17.0.1) 37.382 ms 48.910 ms 52.624 ms

2 \* \* \*

3 \* \* \*

4 \* \* \*

5 10.10.158.153 (10.10.158.153) 186.906 ms 184.948 ms 186.854 ms

## telnet

- ELNET (Teletype Network) protocol was developed in 1969 to communicate with a remote system via a command-line interface (CLI).

- telnet is 23.

- The secure alternative is SSH

- cmd didn't work some error happend, so i used nmap

server version was - 2.4.61