Cybersecurity, Gamified

Solve a series of cybersecurity-related tasks in order to get your well-deserved flag!

Solution

The challenge is a webpage hosting a game written in Inform 7. For those who are not familiar with the language, a simple search on a web browser will reveal a series of commands that can be helpful in order to play it (as will the `HINTS`, `HELP` or `HINT` commands do, redirecting the player to `VERBS`).

Room 1 - the Internet

The player finds themselves in the Internet, their way blocked by a firewall, and with an Outgoing Packet as company.

This prompts the player to *look* at those things:

- Examining the firewall (`x firewall`, short for `examine firewall`) suggests that the player should find a way to avoid it.
- Examining the packet will reveal some fields of its header (they are random every time), for instance:
  - srcIP: "169.84.122.116";
  - dstIP: "40.18.150.70";
  - srcPort: 42635;
  - dstPort: 4559;
  - SEQ: 5315;
  - ACK: 5763;
  - payload: "We demand rigidly defined areas of doubt and uncertainty!".

Furthermore, if the player looks at themselves, their own fields are revealed:

- srcIP: "0.0.0.0";
- dstIP: "0.0.0.0";
- srcPort: 0;
- dstPort: 0;
- SEQ: 0;
- ACK: 0;
- payload: "For instance, on the planet Earth, man had always assumed that he was more intelligent than dolphins because he had achieved so much - the wheel, New York, wars and so on - whilst all the dolphins had ever done was muck about in the water having a good time. But conversely, the dolphins had always believed that they were far more intelligent than man - for precisely the same reasons.".

Which have nothing to do with those of the packet they just sniffed! Indeed, trying to enter the firewall without changing anything will have the player dropped by the firewall and they will end up in the Afterlife.

The objective here is therefore mimicking the other side of the conversation in order to bypass the firewall, thus completing a **TCP hijacking** attack.

The `VERBS` command shows the correct syntax to use in order to change the player's header fields (it is sufficient to swap all src/dst IPs and src/dst Ports, then the SEQ will be the ACK of the Outgoing Packet and the ACK will be the SEQ of the Outgoing Packet + the number of characters in the payload):

```
srcIP "40.18.150.70"
dstIP "169.84.122.116"
dstPort 42635
srcPort 4559
SEQ 5763
ACK 5372
```

Now the player can simply enter the firewall (`enter firewall` or `go firewall`), and the firewall will accept them.

Room 2 - the Switch

The player is now in the Switch, where 7 interfaces are open and a NIDS/IPS completes some random tasks. A packet exits a random interface and enters `Fa0/7`.

Observing the situation for some turns (`z` will have the player waste a turn waiting, but nearly any command will do the trick) makes it clear that the only correct interface from which to enter the Switch (as every packet goes there) is `Fa0/7`.

Therefore, `enter Fa0/7` will have the player successfully enter the Switch.

Room 3 - the Second Firewall

Again, the player faces a firewall and a NIDS. It is said that no packet comes out, however many packets enter it.

Packet 42 arrives and knocks on port 1337. Another packet arrives and looks at the firewall.

If reading that the action involved is *knocking* was not enough on its own to reveal the objective of this room, waiting for some turns will show other packets arriving and knocking on the exact same ports and then, after they have completed the sequence, being taken by the NIDS inside the firewall.

It is now clear that the player has to perform **port knocking**, with the sequence being the same one they have witnessed the other packets using.

```
knock 1337
knock 0
knock 42
knock 73
knock 101
knock 404
knock 418
knock 666
```

Knocking on port 666 will then trigger the completion of the room.

Room 4 - the Mail Room

The player is now in the Mail Room, their way out blocked by a locked door, where they are sitting behind a counter next to two creatures called Alice and Bob (who the player is prompted to think are keeping a *secret* from them) and in front of a series of objects:

- A piece of parchment the two have exchanged, which upon examination (`x parchment`) will reveal the following: *"[...] p = 11, g = 2"*
- A blue letter from Alice (`x blue letter` will reveal *The top of the blue letter reads: "To: Bob, From: Alice", and the content is a simple number: "8".*)
- A red letter from Bob (`x red letter` will reveal *The top of the red letter reads: "To: Alice, From: Bob", and the content is a simple number: "10".*)
- Two pinpads, one blue and one red, waiting for the player to type digits on them

An extra hint on what to do can be found by examining the player (`x me`), which will print the following: *You are dressed in a strange, yellow tunic with a gigantic blue "DH - Express Key Exchange" embroidered on the front.*

The point here is then breaking a simple **Diffie-Hellman** key exchange with very small numbers by typing the correct secrets on the pinpads.

We can try to bruteforce the secrets:

$$Alice: 2^1 \mod 11 = 1, 2^2 \mod 11 = 4, 2^3 \mod 11 = 8 \rightarrow \text{her secret is } 3$$

$$Bob: 2^1 \mod 11 = 2, 2^2 \mod 11 = 4, 2^3 \mod 11 = 8, 2^4 \mod 11 = 5, 2^5 \mod 11 = 10 \rightarrow \text{his secret is } 5$$

The color of the pinpad suggests which one is for whom, and typing the following commands will do the trick:

```
type 3 on blue pinpad
type 5 on red pinpad
```

Solving both pinpads will make everything disappear and spawn a key on the counter. Taking the key and entering the door (unlocking and opening it will be done implicitly by Inform, however the player can do every step if they so wish) will solve the room:

```
take key
enter crimson door
```

Room 5 - the Bedroom

Once the player is in the Bedroom, they can finally read the flag that is sitting on the ground (`x flag` or `read flag`)!

Flag: *KSUS{Pls_K4fk4_n0w_wr1t3_4_n0v3l_4b0ut_m3_4s_w3ll}*