Questioning

Learning to ask the right questions is an art and a critical skill. It does not matter what situation we are in or whether we are discussing technical or non-technical topics. However, many people do not know the difference between wrong and right questions. Most do not even know what a question is. At the moment, we define questions and see their purpose as gathering information and facts from which we can draw conclusions and make assumptions that will guide our decisions and thus our future course of action. However, this opinion will soon change. Apart from that, questions often serve for orientation. By this, we mean that we can get an overview based on the questions we ask, which helps us to find more information about the topic we are concerned with. Questions represent the view of the situation before we take the next step and move on our way. Metaphorically speaking, we use them to see where we want to be or can take our next step.

Especially in our field of cyber security and above all in penetration testing, we should keep the following in mind:

`The most important and most difficult thing in any situation is not the search for the right answer but the search for the right question.`

A good example is that if an answer to a task is already known, the task is no longer necessarily difficult to solve. Many people believe that searching for an answer is one of the most difficult activities that accompany them throughout their lives. However, finding the answer becomes the opposite when the question is asked correctly. It is much more challenging to ask the right questions when we do not understand the concepts or do not have any knowledge of a particular area in the first place. We have all been in a situation where we suddenly did not know what to do and could not even understand what to start with to figure out the situation.

At this point, we should choose 3 to 5 such situations from our lives and write down one question for each of them. These can be any situation. We can take difficult and obscure situations and then write down a question for them. Throughout this section, we will learn a model that will help us see the difference between the quality of the questions we were asking and the questions we needed to ask. In doing so, we will also quickly become aware of the model's effectiveness and how much it would have helped us at the time. This is the best way to judge the effectiveness based on our personal life experiences. Therefore, we should not skip this step and write down 3 to 5 situations from our lives now.

Question States

First of all, we need to solve a certain myth about questions before we continue at this point. We need to be clear about the following:

- `There are no "good" or "bad" questions. End of story.`

Let us examine the following question and clear up this myth once and for all:

- `What are "good" questions?`

Let us assume that the answer is `X`, `Y`, and `Z`. Is this question "good" or "bad"?

It does not matter and is irrelevant. "Good" or "bad" is a state we attribute to the question. What influence does this condition have on the answer? - None. The answer remains `X`, `Y`, and `Z`.

If we do something that does not affect the result, it does not matter and is therefore completely irrelevant. This is the same as asking ourselves:

- `"What happens if I jump into the water?"`

To this question, we then add the following factors:

- `"The water is cold/hot/dark/transparent."`

How does the water's condition affect the result when we jump into the water? - It does not. Apart from all the other consequences, we get wet either way. The interesting thing is that with the condition, we have even come closer to the actual situation. Because we used it to describe the state of the water, this is much closer connected than the state of the question. How would we influence the result if we set the state of the question and say that it is a "good" question? - We would not.

People use the states "good" and "bad" to describe the profit or loss they expect from the question. If people get an answer that benefits them, they classify the question as a "good" one. However, what if the question leads to a loss or, let us even say, does not help the person? Is the question bad? - Actually, not.

The state we give to the questions does not affect the answers. The state attributed to the question belongs to the answer or the result. The answer can be to some extent "good" or "bad," but not necessarily, depending on our goal and whether we are getting closer to it. If we come closer to the answer/result, moving away from the less ideal goal is good.

We can assign two states to a question; thus, we would describe it as a `rough question` or a `precise question`.

- A `rough question` would be, for example, "How can I hack X?"
- A `precise question` would be: "How can I use the server's SMB service to identify its existing user accounts?"

As we can see from these two examples, this state of precision can greatly affect the result and the answer. Nevertheless, a precise question is still not good. Because `good` or `bad` are irrelevant states, we now know that they do not influence the result or the answer.

Questions in General

We use questions in everyday life more often than we realize at first glance. On average, we ask between 3-5 questions per minute. Of course, this depends on the situation. We can experiment and set a timer for 1 minute and observe our thoughts during this period. Every time we notice that we ask ourselves something or something is unclear to us, we make a mark on a piece of paper until the timer runs out. To do this experiment, we need to take a pen and a piece of paper and set the timer. From now on, the timer should run.

Questions can be asked in many different ways. Because all questions are adapted to the circumstances, situations, and the desired goal. Questions are an essential part of the thinking process in which links are created between information nodes in our brain. Thus, it is also a fixed and unavoidable part of the learning process. Removing questions, therefore, also reduces the learning process enormously. If we do not question anything when we read content, it is like a cooking recipe without any information about how to prepare it. Because a recipe contains a big question from the ground up:

- `How do I cook the dish?`

Two main points are worked through for each recipe:

1. `ingredients`
2. `method of preparation`

Learning material content can be equated with the ingredients. The preparation method can therefore be correlated with our questions because the questions determine which step we will take next and define our approach. Finally, how the cook describes the preparation method describes when, how, and what needs to be added and processed to get closer to the finished dish. The cook or author's approach may have worked 100%, but anyone who has ever cooked from a recipe knows that a written down recipe alone will not make the dish tasty.

- We must prepare and practice it, using the means at our disposal.

A professional cook typically has considerable experience and often uses special ingredients that can be very expensive, and we do not know any other use for them. Therefore, this is an essential example that copying and imitating what has been shown and explained will not always produce the desired result.

By now, the timer should have run out, and now we should add up the number of questions that came to mind while reading during this period. For comparison, at least ten questions could have been asked. If more than ten questions came up for us, all the better. The more questions we ask, the better understanding we develop of the whole picture.

To do this, let us briefly imagine the situation where we need to open a lock and follow a methodology that most people use today. The question that can be concluded from this situation is:

- How do we open the lock?

The question is unnecessary if it is a standard door lock because we have enough experience and knowledge to open the door with the appropriate key. In this case, the key is the known tool that we use to unlock or lock the door. The situation is different if we have a vault in front of us that requires a combination of numbers. What questions do we need to ask to get the answers that will allow us to find the right tools or methods and use them accordingly?

Once we know the goal (`The Goal`) to which we are attracted (`Willingness`), we can use various principles, such as the Pareto Principle or Occam's Razor, to develop our talents (`Talent`) and skills and make our decisions (`Decision Making`) to pass the obstacles that fall across our path by asking the right questions (`Questioning`).

We can all ask questions. However, not many know how to ask the right questions. Because some significant differences and influences can greatly affect the answers we want to receive. The goal of the question is one of the most important aspects that determine our approach and the question we ask. Let us look at a few things that we currently use in our everyday lives. Such goals that we have just talked about can be, for example:

- To understand the reason for an event (`past`)
- To experience something completely new and to understand the way something works (`present`)
- to predict the effect of an event (`future`)

Every question is based on three aspects with which we build our questions every day:

1. origin
2. process
3. result/goal

These questions can be of any kind and can relate to duration, reason, action/reaction, location, specification, and many others. They can be as varied as our imagination. Almost every question is based on our needs, time, type, and place.

So far, everything seems to be accurate and logical. However, it is not. At this point, a few questions arise that we need to clarify.

1. What is a question?
2. Regardless of the form, what purpose does a question serve?

The official definition of a question is as follows:

- `A question is a sentence worded or expressed to elicit information.`

This definition has two core elements: `sentence` and `information`. So what is a `sentence`?

The definition of `sentence` is as follows:

- `A sentence is a set of words that is complete in itself, typically containing a subject and predicate, conveying a statement, question, exclamation, or command, and consisting of a main clause and sometimes one or more subordinate clauses.`

Moreover, here comes the exciting part; a collision that will change many things for us.

How many words must be used to ask the shortest question?

The answer to that is `a single word`. Here are a few examples:

- "Why?"
- "How?"
- "Where?"

Is it an actual question? - Yes. Is it the shortest question or one of the most straightforward questions? - Yes.

Of course, these questions need context, like any other question, but this does not exclude the fact that these questions in this form with a single word represent a real question. Thus, the official definition of a question does not fit anymore.

Next, the definition of a question explains its purpose. Therefore, according to the definition, the purpose is to obtain or acquire `information`.

Let us, therefore, create a situation with a question to test this statement. Let us assume we see `host A` and `host B`. To do this, we can ask the following question, which we will also ask during our penetration tests:

- `How is Host A connected to Host B?`

Our goal was to obtain or acquire information with the help of the question posed. Did we obtain or acquire any information from this question? - No. Regardless of the form of the questions asked, strictly speaking, the official definition of the question also missed the point. This is an example of how we can question certain things. As we see, the effect and the surprise can make one wonder. After all, we have just discovered that the official definition does not apply to a question.

Of course, a deep discussion can be started about the question's meaning, purpose, and how it should be asked. But furthermore, here is where the question arises:

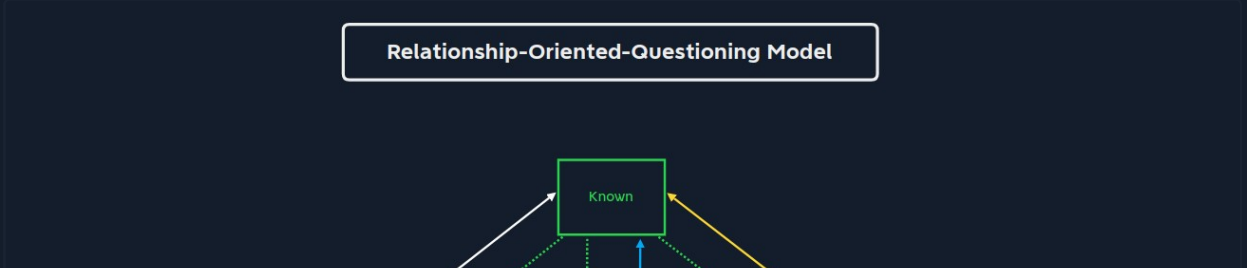
- `How should we then define a question if the official definition does not apply?`

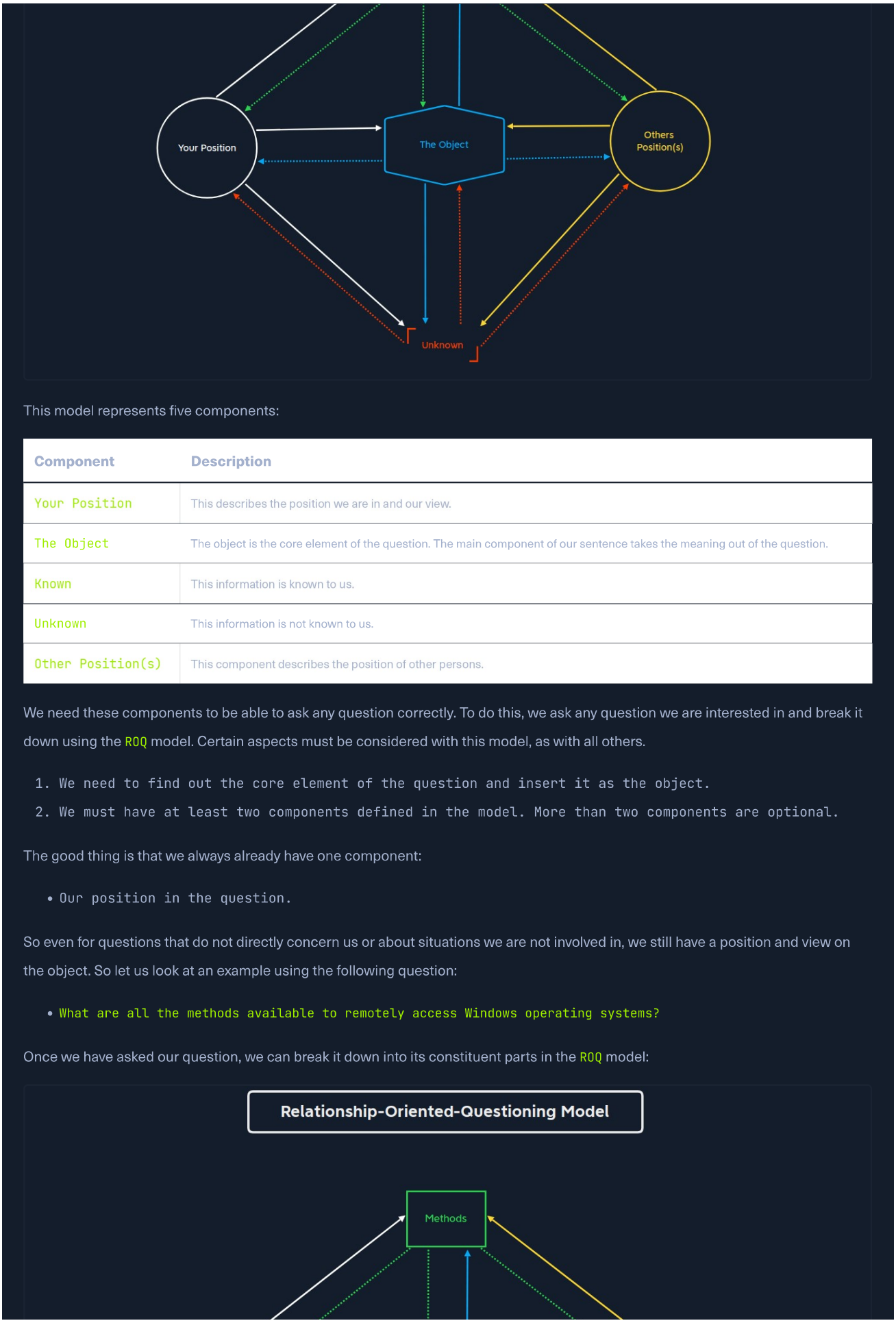
Here we see the global scale when the goal has been set incorrectly.

What goal could we set for ourselves if the previous goal "to obtain information" can be constantly missed?

Relationship-Oriented-Questioning Model

To do this, we must consider what our questions have in common. All our questions have a commonality: the `relationship` between the individual components. So let us take a quick look at a model we have developed, which we call the `Relationship-Oriented-Questioning Model` (`ROQ`), and see how it looks and works.





This model represents five components:

Component	Description
`Your Position`	This describes the position we are in and our view.
`The Object`	The object is the core element of the question. The main component of our sentence takes the meaning out of the question.
`Known`	This information is known to us.
`Unknown`	This information is not known to us.
`Other Position(s)`	This component describes the position of other persons.

We need these components to be able to ask any question correctly. To do this, we ask any question we are interested in and break it down using the `ROQ` model. Certain aspects must be considered with this model, as with all others.

1. `We need to find out the core element of the question and insert it as the object.`
2. `We must have at least two components defined in the model. More than two components are optional.`

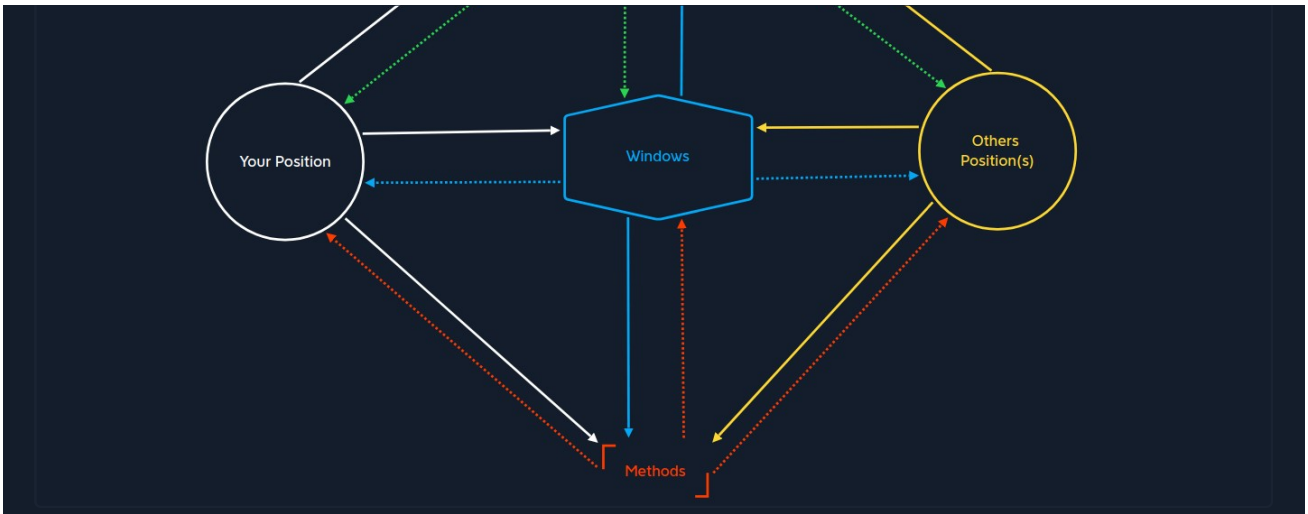
The good thing is that we always already have one component:

- `Our position in the question.`

So even for questions that do not directly concern us or about situations we are not involved in, we still have a position and view on the object. So let us look at an example using the following question:

- `What are all the methods available to remotely access Windows operating systems?`

Once we have asked our question, we can break it down into its constituent parts in the `ROQ` model:



Component	Question Part	Description
`Your Position`		Our position where we are situated.
`The Object`	Windows	The Object is the core element of the question. The main component of our sentence takes the meaning out of the question.
`Known`	Methods	This information is known to us.
`Unknown`	Methods	This information is not known to us.
`Other Position(s)`		This component describes the position of other persons.

Based on the parts assigned to the components, we now have to define in which relationship they act among each other. In the graphic, we see solid and dashed lines.

- `Solid line: Connection - How is X connected to Y?`
- `Dashed line: Affection - How does Y influence the state of component X?`

Connecting the Components

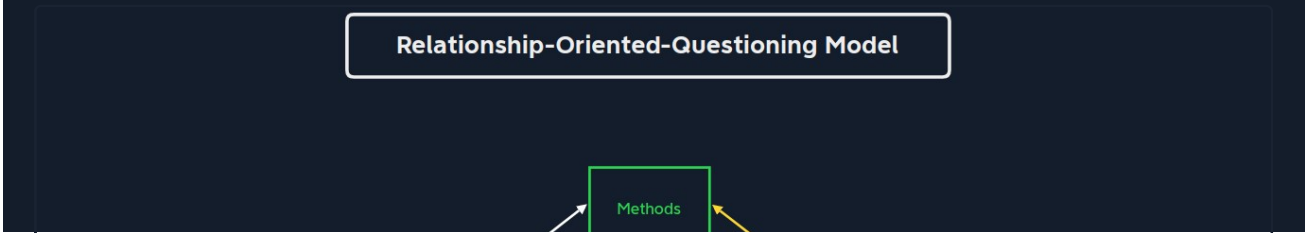
With this, we can go through the individual relationships and establish them between the individual components. It is recommended to always start with the object, which in this case is the Windows operating system. First, we need to establish and understand our position on the object.

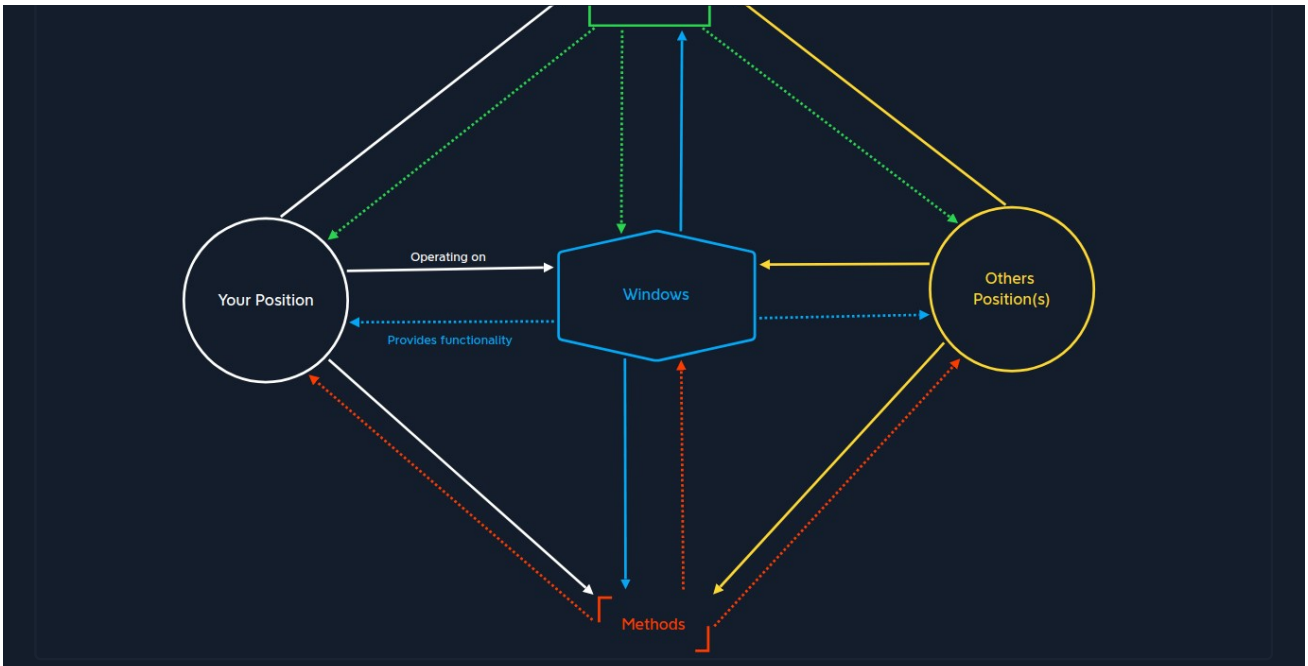
- `What is the purpose for us to use Windows?`

Mainly we use the operating system to use its functions to solve our tasks. We describe this as `Operating on`.

- `How does Windows influence our state in our position?`

Windows is the most used operating system in the world and has the most compatibility and many user-friendly functions. Therefore, we can also summarize this and call it `Provides functionality`.





Now we can connect the relations between Windows and the methods we know.

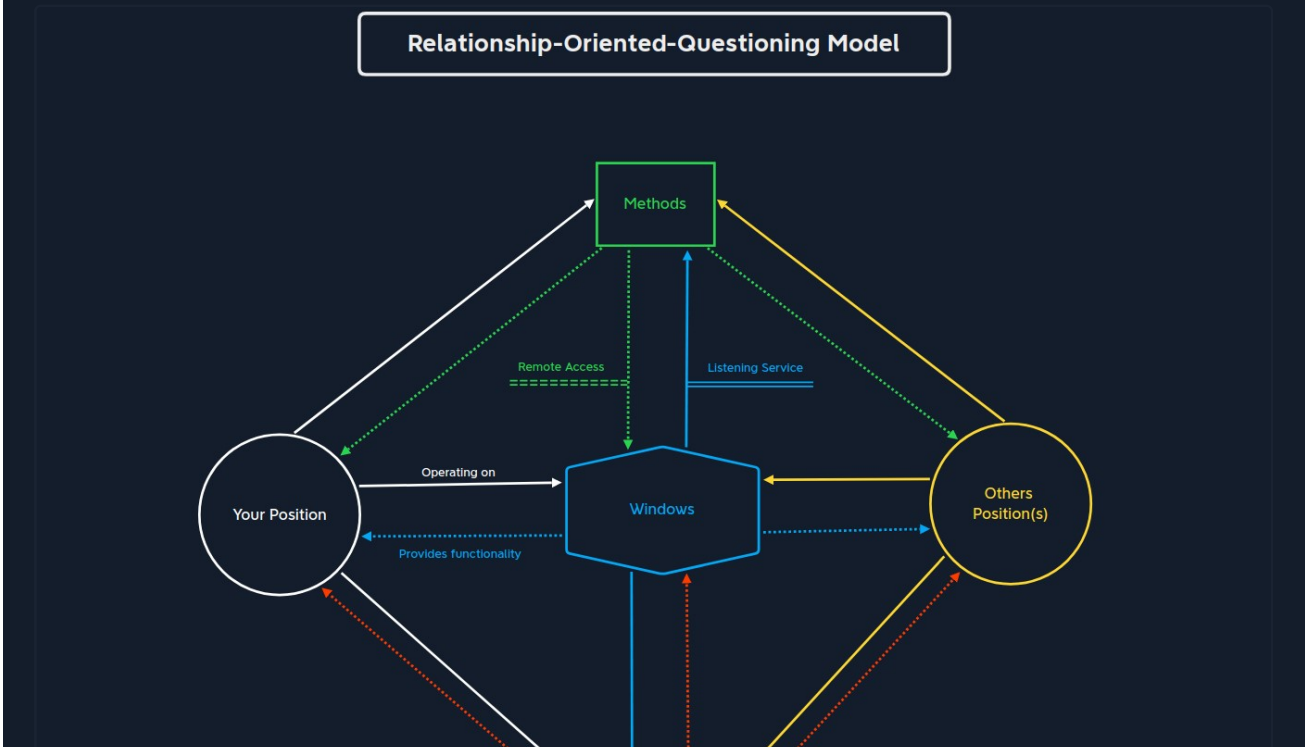
- `What must Windows do or offer to be managed by remote access methods?`

A service must allow remote access over the Internet or network. We know for sure `WinRM`, `Remote Desktop`, and a few more. (If not, it does not matter. We will learn about these in other modules). Otherwise, we would not be able to access it remotely. We call this connection `Listening Service`.

Next, the following question comes up:

- `How do the remote access methods affect Windows and thus change the state of Windows? What do these methods provide us with?`

Here the answer and the purpose are already in the description - these allow `Remote Access`.



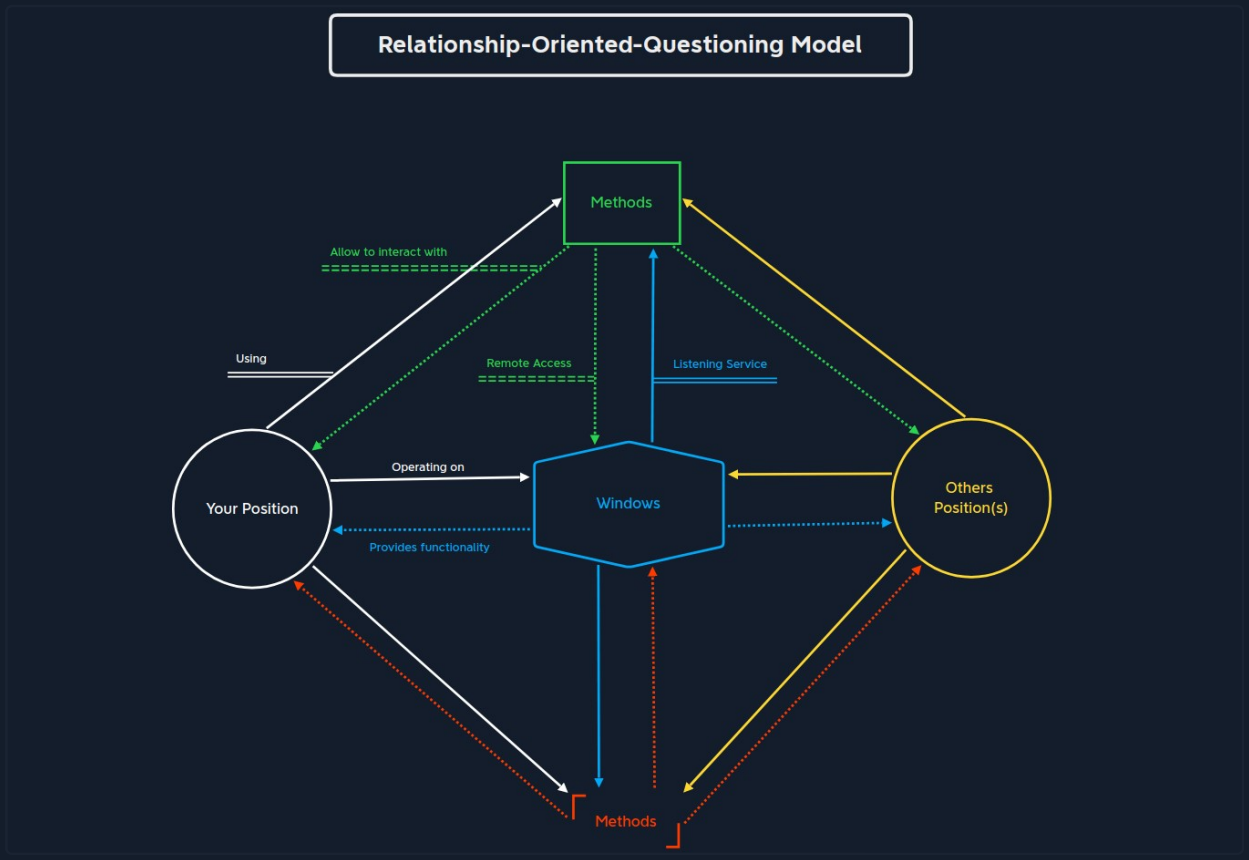
Now let us look at what we know about the known remote access methods.

- `What is the purpose of remote access methods?`

The purpose is to be able to manage Windows in different ways remotely. So all we do with it is to use it. So, therefore, we call this connection `Using`.

- `How do the different remote access methods that we know affect us?`

Apart from the different services these methods are designed for, they all have one thing in common. They allow us to interact with Windows. Therefore we call this connection `Allow to interact with`.



Since we already know some remote access methods, we know how they are connected to Windows. Before Windows can be accessed remotely, the corresponding service must be running.

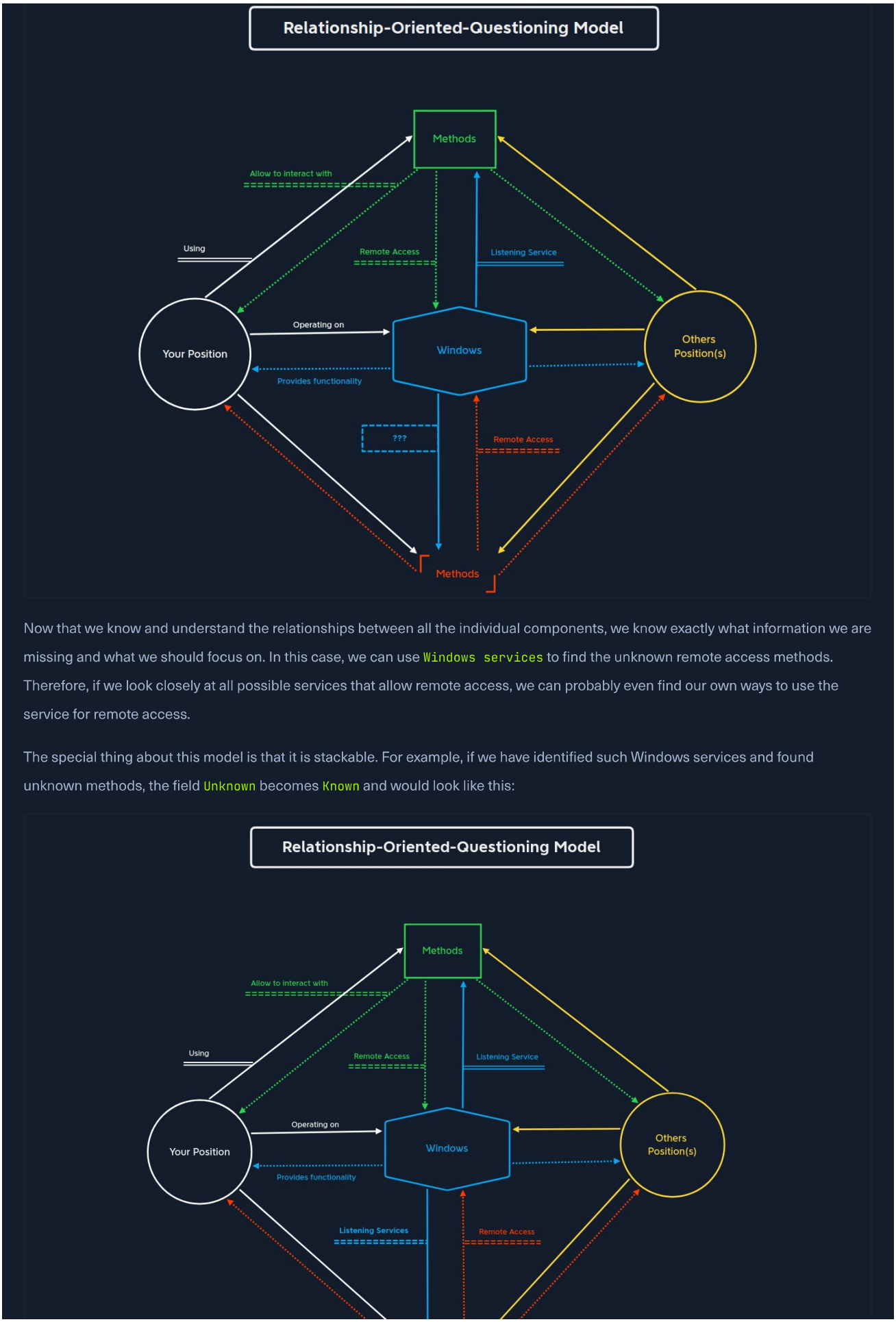
- `Which services must Windows have running to use methods unknown to us?`

We can not know this because the methods are unknown to us. Therefore we name it like this: `???`

Now the same question arises again.

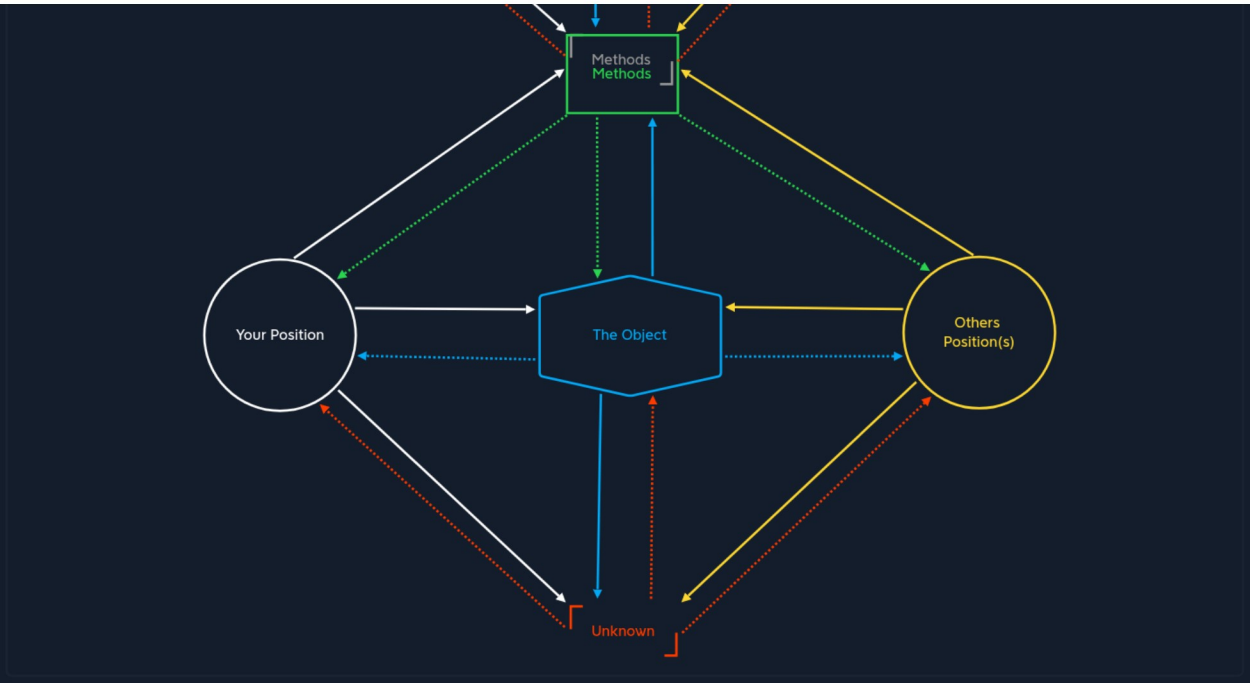
- `How do the remote access methods affect Windows and thus change the state of Windows? What do these methods offer us?`

The different methods offer different ways to access Windows. Because the purpose of the methods, in this case, has not changed. Therefore we call it again: `Remote Access`.



Now that we know and understand the relationships between all the individual components, we know exactly what information we are missing and what we should focus on. In this case, we can use `Windows services` to find the unknown remote access methods. Therefore, if we look closely at all possible services that allow remote access, we can probably even find our own ways to use the service for remote access.

The special thing about this model is that it is stackable. For example, if we have identified such Windows services and found unknown methods, the field `Unknown` becomes `Known` and would look like this:



Practice

The model may be unusual at first, and from experience, I can say that many people have difficulties in the beginning to apply this model. You will be using this model subconsciously after practicing five to ten times. You will not have to think about it much, and you will see the difference in a very short time when you have practiced this model. In fact, with these few practice sessions, you will internalize this model so much that you will even begin to use it automatically during conversations. This is the recipe that I have given you, and now you must learn to prepare the dish yourself.

Now take the 3 to 5 questions from the situations we had to write down at the beginning of this section and apply this model. You will be amazed at the conclusions you will come to.

However, this model has one special feature. If applying this model to your question is unsuccessful, you will have to rephrase it and make it more precise. Because this feature of the `ROQ` model will not allow us to ask questions to which there is no clear answer.

Now, let us settle one last question.

- `So, what is the right question?`

`A right question is a precise question that allows us to establish the relationships between the components, to understand them, and to take us one step further to the required answer.`

Previous Next Mark Complete & Next

Learning Dependencies

- Way Of Learning
- Learning Efficiency
- Learning Types
- The Brain
- The Will
- The Goal
- Decision Making

Learning Overview

- Documentation
- Organization

The Process

- Focus
- Attention
- Comfort
- Obstacles
- Questioning
- Handling Frustration
- Learning Progress

My Workstation

OFFLINE

Start Instance

1 / 1 spawns left