Possible Questions

Does 2FA stop mitm attacks and if not why?

Answer:

No, Since the attacker places themselves between the user and the server they are trying to authenticate on, the attacker can intercept the users credentials and 2FA-code and authenticate as them regardless.

What does the Cyber kill chain depict?

Answer:

Phases of a cyber attack

What kind of information is shared on Mitre ATT&CK?

Answer:

Known threat actors and the techniques and tacktics they are known to use aswell as procedure examples and some mitigation methods

What does yara do?

Answer:

It scans files for patterns that are know to be used in malware. These patterns are conditions described in yara rules.

What does the following Yara Rule do?

```
rule Wild_rule
{
 meta:
   description = "yet_another_redundant_description"
 strings:
   $hex = { FF ?? ?2 A0 }
 condition:
   $hex
}
```

Answer:

Return any files that contains the mentioned hexcode, with the questionmarks beeing wildcards that can be any byte value.