# **CTF Topic:**

# **Introduction**

APT is a new generation threat that involves enemies infiltrating computer networks with an intent to be there undetected for an extended period. These criminals think tactically and strategically to incapacitate their target and walk away with sensitive information from large organizations or governments. The first one, ‘advanced,’ points to the fact that they employ intricate methods and the ‘persistent’ term suggests that they remain undercover, and they work beyond the normal time span.

Here's a more detailed breakdown on Advanced Persistent Threat (APT) :

**Sophisticated Techniques:** These intruders employ sophisticated procedures to get access to the system. These can be such stages as using unpatched software or other well-known open weaknesses, phishing emails and using malicious programs that are difficult to identify.

**Long-Term Access:** They try to maintain access inside the victims system for as long as possible and extract as much information as they can over a long period of time.

**Specific Targets:** APT groups usually target valuable companies or governmental agencies. Their goal is to steal sensitive data or a large sum of money so they perform a sophisticated attack over a long period of time.

**Continuous Monitoring :** Due to their long stay in the victim's system they have a constant monitoring in place to ensure they can elongate their stay, they create several backdoors to re-enter the network if they get kicked.

**High Risk:** Defending against apt is really hard and requires constant monitoring and different preventive measures in place, they are really destructive and cause the collapse of a whole company if used properly.

# **Let's Begin The Challenge**

# **Question**

**Flag 1 :** What do APT’s create to re-enter the network if they get kicked ?

**Answer :** Backdoor

**Flag 2 :** What kind of Techniques do APT groups use ?

**Answer :** Sophisticated

**Flag 3 :** Do small scale companies get targeted ?

**Answer :** No