# S6000告警信息和攻击阶段关系映射

S6000告警信息和攻击链阶段关系映射：

S6000介绍：

外部网络攻击的过程可以抽象为攻击链模型，同时S6000的告警信息是对攻击的信息描述。不同的告警可以被归纳到不同的攻击步骤中去，我们将不同的告警信息和攻击链作了关系映射。因此不同的告警信息可以被定位到不同的攻击步骤上去。

如下图示例，我们整理了在攻击链中不同攻击阶段的所包含的攻击方法，以及详细的攻击告警。

【攻击链和告警映射图】

# 本体图的解释（定义）说明

在构造本体的之前，我们收集了电网的网络信息以及网络攻击的知识。通过分析，并结合已有的知识和经验，抽象出一些共有的概念、特征和关系。并将这些概念、特征和关系转换为实际构成本体（知识图谱）的元素——类、关系以及实体。为了来描述本体，我们定义了一些描述规则：

我们借鉴了统一资源描述框架（RDF）中的部分规则：椭圆被用来描述类，矩形被用来描述实体。每个类具有单个或多个属性。一方面，当两个类之间被一条有向的边连接时，这条边就代表一个属性。箭头端代表属性的作用域（range），另一端代表属性的域（domain）。RDF形式上为SPO三元组，因此属性也可以理解为谓语（关系），它定义了主语（domain）和谓语（range）之间的关系。

另一方面，类和实体之间用紫色的箭头表示。箭头一端代表实体，另一端代表实体所属的类。父类和子类之间用黄色的箭头表示，箭头一端代表子类，另一端代表父类。

根据上述规则，并基于S6000的数据知识，构建基于攻击链的知识图谱。

下图为知识图谱的本体的概览图。

【本体图片】

我们定义了如下基本类：被攻击对象，攻击者，S6000告警，行为，被攻击对象的系统组件，行为记录时刻，攻击结果，输入，位置，方法，攻击结果时刻。这些基本类作为父类会再分化为各个子类，直至化为各个实例。

以下分别为各个基本类和相关属性的解释说明：

1， 被攻击对象：电网中任何潜在被攻击的设备，可以是

1. 嵌入式设备。包括物联网中的各类传感器、智能终端以及工业控制中的PLC。
2. 服务器器。包括业务服务器。
3. 数据库。包括存储业务数据的数据库。
4. 防火墙。包括电网信息网络中的防火墙。
5. 电脑。包括信息网络中的办公电脑。
6. 通信设备。包括路由器、交换机等设备。

2，S6000告警：S6000告警的信息，这里面有网络中的可疑数据、攻击数据。

3，行为：攻击链中的可疑行为的描述，被攻击对象受害于这些行为，这些行为是S6000告警的实例。行为可以继续被细化为攻击链中特定的攻击步骤。用于将S6000告警信息和攻击链阶段关系映射起来。

4，行为记录时刻：记录了行为发生的时刻。

5，被攻击对象的系统组件：记录了被攻击对象的在受到可疑行为时的状态快照，包括了

1. 端口，包括了当前开启的端口，这些端口可能是是潜在被攻击的端口，例如445端口。
2. 网络协议，包含了被攻击对象使用的不同层网络的主要协议，这里我们例举了三个网络层的协议TCP，UDP，IP。
3. 存储设备，包含了系统中有存储功能的硬件设备。
4. 系统，包含了被攻击对象使用的操作系统的相关信息，例如版本号。
5. 进程，包含了被攻击对象的父、子进程的调用、切换情况。

当前状态属性定义了被攻击对象和被攻击对象的系统组件的关系。

“针对”属性定义了行为和被攻击对象的系统组件之间的关系，表明”行为”是针对其中的*一个或多个*状态进行了攻击。

6，位置：攻击所利用的安全漏洞在系统中被发现的位置，既可以理解为系统的薄弱点，可以分为硬件和软件两个子类。

1. 软件，包括操作系统中的文件管理系统，设备管理系统，内存管理系统等，或者是系统所运行的应用程序。
2. 硬件，包括CPU，内存，硬盘等。

被攻击对象的系统组件是位置的实例。例如，某次针对文件管理系统进行的攻击，就是一个位置实例，属于软件这个子类。

这些位置受到了攻击者生成的输入。

7，输入：攻击的输入，它驱动了攻击行为的发生。这种输入可以是

1. 邮件，可能是带有病毒附件的邮件。
2. 链接，可能是带有病毒的链接。
3. 移动存储设备的接入，可能是带有病毒程序的USB
4. 异常的访问等，例如大量机器的同时访问。

8，攻击者：攻击发起的源头，现在大部分可以被认为是IP地址。攻击者生成了输入。例如，某个IP地址生成了大量的异常访问，或者由某个IP地址发出了一封可疑邮件。

9，方法：攻击利用的方法（原理），通常为某些漏洞。方法在这里作为输入的原理，通过原理属性进行连接。方法包括的子类有：

1. 输入验证错误漏洞利用，通常发生在硬件或软件收到了畸形的输入，并且这些输入并没有被检测、隔离出来。对其继续分类有：
   1. 缓存溢出，通常由固定大小的数据结构的溢出导致。
   2. 边界情况错误，通常由在非法地址读写或系统资源耗尽造成。
   3. 畸形输入，程序接收了语法上错误的输入或者没有关联的输入，且程序缺少能力对输入进行检测和修订。
2. 逻辑漏洞利用，利用软件或硬件上的缺陷，例如竞争条。对齐继续分类有:
   1. 异常条件，由于软件模块或硬件无法处理异常条件而造成的错误。
   2. 竞争条件，在同一时间窗口存在两个操作相互竞争。
   3. 序列化错误，由非法的序列化导致。
   4. 原子性错误，有时发生在部分修改的数据结构被其他进程使用，或者原子性的数据被进程修改到一半时，进程终结了。
3. 硬件漏洞利用，利用硬件层面的漏洞，例如比特锤击，以高频率去访问一个固定地址来使附近地址的值发生改变。

10，攻击结果：攻击成功之后产生的结果，攻击者的行为导致了这些攻击结果。包括：

1. 探测，通常由信息收集或信息探测造成。
2. 拒绝服务，导致用户无法使用系统的服务，通常由于系统进入了一个不稳定的状态或者服务被没有意义的函数消耗着。
3. Root权限获取，攻击者会拥有系统的权限，导致系统被攻击者完全控制。
4. User权限获取，攻击者将会在没有权限的情况下访问系统的服务。

行为与攻击结果通过导致属性定义。

11，攻击发生时刻：记录了攻击发生的时刻。

/\*\*\*\*

三道防线：

放在位置部分？？？

电力系统三道防线是一个实体的存在。

而本体图中展现的是各个抽象出来的类，得把他们分到本体图中去。

可以将三道防线扩展到这个图上的：

被攻击对象的系统组件；

攻击结果；

被攻击对象；

S6000告警（信息）

位置

\*\*\*\*/

TDL：

排版问题A4，不要square