**张平：总体负责、WEBUI**

**马林威:** **（系统扫描)**

系统扫描是指对设备开放的服务端口发送扫描报文，以判断服务程序、版本、引用库、服务实现漏洞等，典型的如对WEB网站的扫描。主要使用工具OpenVas，并考虑以此工具作为框架调用其他扫描工具。

1. 将已经安装了openvas11(gvm11?)的kali2020，分享给大家，给出分享链接；（9月12日）

1. 熟悉openvas的命令行及响应的格式，包括不局限于：（9月13-9月19）  
   1）扫描目标的管理（增删改查）；  
   2）扫描任务的管理  
   3）扫描计划  
   4）扫描状态  
   5）报告生成

6）漏洞库更新

1. 对openvas的管理协议进行熟悉，(老版本的协议为omp，新版本的协议名字？），尤其是命令执行以后的xml格式的响应。

**张琪：(网络扫描和设备扫描）**

网络扫描是指对指定IP地址发送各类网络报文，根据应答情况判断设备网络是否可达、开放哪些服务端口、协议栈版本等，给出相关报告。

1. 从马林威那里获得安装了openvas的kali2020虚拟机；
2. 网络扫描工具nmap(不局限于nmap,可以找其它的扫描工具）的使用;
3. 设备扫描的方案

**李想：（弱口令扫描）**

弱口令扫描是指对设备的telnet、SSH、WEB服务的账户进行登录尝试，以判断设备是否存在账户口令安全性不够的风险。

1）参考工具如IoTSeeker等；

2）如果没有合适的弱口令扫描工具的话，也可以考虑自己编写；

3）后面再了解是否可以在openvas中调用此种扫描工具，就以往了解的情况看，openvas有对其它第三方扫描工具的调用，比如ncrack，nikto等。