​

南京科讯次元信息科技有限公司 四月工作汇总

​

\*本月主要工作地点为江苏省公安厅、据点、会战地点、公司 涉及项目：特侦云平台2.0版本 项目进展：已完成第一轮迭代，交付用户进行测试，收集问题中 一、 本周总体工作情况

本周客户其他业务较为繁忙，使用我们的产品不是很频繁，提出的问题较少。

下周将会开始新的会战，预计使用频率会有较大提升。

二、详细工作情况

1、第一周

1. 本周进行了一次版本升级，在此次版本升级中，更新了如下内容

1）上线python2.7、phpstudy两款软件

2）去掉linux前缀

3）虚拟机详情页名称不显示

4）硬盘可选项减少

5）大文件回传问题

6）windwos禁用445端口

7）云主机禁用声卡

8）输入法全部改为谷歌输入法

9）创建虚拟机界面分为简单页面和高级页面

10）公私网选择后显示ip

11）远程连接卡顿问题给出解决方案

1. 返回公司参与公司保密室建设
2. 收集问题如下

1）快到期的任务需要做出提醒，已修复 ​

2）公网ip需要尽快增加，需要给出增加完成的日期，已修复 ​

3）与拓建方面魅影的对接需要有进度反馈，已修复 ​

4）外网虚拟机修改密码时提示检测信息失败，已修复

2、第二周

1. 本周收集问题如下

1）虚拟机缺少显卡，不支持安卓开发，需要添加显卡，暂未添加 ​

2）临时虚拟机要有一个方便的创建方法，暂未修复

3）公网ip需要尽快增加，已经增加完成，已修复 ​

4）与拓建方面魅影的对接已经准备完成，已升级

1. 本周列表新增武器，正在制作中

1）ANGRY IP SCANNER 通过对IP和端口进行扫描来找到进入系统的方案

2）CAIN & ABEL针对Microsoft操作系统的口令恢复和网络嗅探测试工具 ​

3）ETTERCAP 欺骗工具，支持linux和windows，可以创建和发送伪造的包 ​

4）JOHN THE RIPPER 快速进行密码破解的工具

5）Nessus 系统漏洞分析与扫描工具

6）THC-Hydra 暴力破解密码的工具

7）Netcat 像瑞士军刀一样有许多功能的测试功率

8）Wifiphisher 伪造恶意接入点的工具，可以针对wifi网络发起自动化网络钓鱼攻击 ​

9）CEM（CrackMapExec） 一款后漏洞利用工具，可以帮助自动化大型活动目录网络安全评估任务 ​

10）Impacket 一个python类库，可以从0开始构造数据包，或者从原始数据中解析包

11）PowerSploit 在评估过程中使用的一系列模块的集合

12）Luckystrike 一款恶意excel和word文档生成工具

13）BeEF 浏览器漏洞利用框架，利用客户端攻击方法，评估目标环境的工具

14）Immunity Debugger 分析恶意软件和逆向工程二进制文件的工具

15）SetLists 一份列表集，包含用户名、口令、常见数据模式、模糊测试载荷、shell等

1. 协助其他人员进行服务器的安装与调试

3、第三周

1. 协助安装服务器
2. 修改软件安装包语言，全部增加英文选项
3. 更新windows系统补丁
4. 武器库版本升级完成
5. 本周进行了系统升级，内容如下
   * 

Windows8名字统一改为Windows8.1，并添加操作系统子版本号

* + 系统全部改为官方纯净版
  + 已解决大文件完全传不回来的问题
  + 操作系统版本号具体到子版本号
  + 新增任务审核记录查询功能。即，内网任务审核后通过和不通过任务都有记录
  + 云主机远程桌面输入法全部改为谷歌输入法
  + 新增F盘用于文件夹和文件回传，C、D盘供用户使用，解决C盘容量不足的问题
  + 外网登录超时时间延长为30分钟
  + 创建云主机时部分软件支持多国语言
  + 创建云主机时自动安装的软件语言已改为英文

4、第四周

1. 查看更新后内网状态，目前内网运行稳定，内网任务审核记录功能状态正常
2. 准备公司项目的验收，制备验收用数据、创建验收用虚拟机、模拟数据回传、默认任务整套流程，参加公司项目验收的会议，向专家领导讲解系统的使用方法以及功能，项目在验收中响应良好，各个功能模块显示效果正常，使用正常，无任何不良反馈
3. 上周问题汇总如下，已经反馈回公司 1）云主机生成模板开始时需要有提示:创建模板时间较长，请耐心等待，预计创建时间最长可达20分钟 2）云主机升级配置时，新增硬盘可以提供一个挂载新硬盘的方式，既不需要我们直接帮忙扩容，而是仅挂载硬盘，由用户自己进入硬盘管理器进行磁盘扩容 3）云主机在系统升级后会有windows.old文件夹占用c盘空间，建议删除windows.old文件
4. 前往机房新增硬盘，修改服务器间连接方式，未对系统产生影响

三、遗留问题

1. 仍然未收到新的武器工具包，新的武器包制作可能延后，已开始对旧的武器安装包的改造
2. *魅影上线后稳定性仍需进一步测试*
3. 正在进一步收集问题