入侵路径：10.10.32.70

- 1.tomcat弱口令
- 2.上传war包
- 3.获得webshell
  - 3.1 搜索：翻资料Account.rec0（foxmail缓存文件），dir /s
    - FoxmailPasswordDecryptor工具解密
      - 获取foxmail邮箱账号密码
        - 成功登录邮箱
          - 获得工资条
  - 3.2 搜索：翻资料*.doc、*.pdf、*.xls、*.ppt，dir /s
    - 个人画像（包括：本人图片、手机号、身份证图片、毕业证图片等）
- 4.上传木马
- 5.viper上线
- 6.uac提权
- 7.获得system权限
  - 7.1 进程注入：可以x86注入到x64位进程
  - 7.2 创建自守护Session，可能被杀
  - 7.3 加载Powershell插件
    - 执行powershell命令：powershell_execute $PSVersionTable
  - 7.4 获取浏览器信息
    - 7.4.1 浏览器保存密码Login Data
      - 可能存在域账户登录密码
      - ...
    - 7.4.2 浏览器历史记录History
    - 7.4.3 浏览器收藏书签Bookmarks
      - 编写url.bat脚本，自动批量打开url链接
      - 可能存在收藏的密码表
      - ...
    - 7.4.4 浏览器cookie
  - 7.5 开启WDigest开关
    - 获取windows内存密码
      - 获得mhaibo域用户和密码
        - kali：尝试hopac漏洞攻击域控
  - 7.6 添加后门
    - 7.6.1 添加计划任务："Daily Check"
      - 进入cmd
        - （1）查看计划任务
        - （2）修改计划任务：每一分钟执行一次
        - （3）终止计划任务
        - （4）运行计划任务
        - （5）修改计划任务：指定日期指定时间运行
    - 7.6.2 添加管理员账户：just
      - just账户远程桌面登录
        - 上传everything工具
        - 查看mhaibo：Desktop路径
          - 发现并查看"远程"文件夹
            - 发现FinalShell3.0.10管理工具
              - 找文件：/finalshell/conn/，获取保存的密码
                - 找解密代码：FnalShellDecodPass.java
                  - 解密，获得ssh密码：
*10.10.6.165
*10.10.6.168
*10.10.15.100
10.10.93.12
10.88.17.9
                    - 发现密码规律
                      - fscan存活探测：10.10.1.1/16网段
                        - 制作目标表：ip.txt
                          - 制作密码表：pass.txt
                            - fscan批量ssh探测
                              - 获得10.10网段下的27台服务器root权限
10.10.10.35
10.10.10.37
10.10.110.13
10.10.13.105
10.10.13.106
10.10.14.100
10.10.14.101
10.10.14.105
10.10.14.109
10.10.14.112
10.10.14.147
10.10.14.24
10.10.15.124
10.10.15.151
10.10.15.160
10.10.15.162
10.10.15.179
10.10.15.24
10.10.15.27
10.10.15.28
10.10.6.181
10.10.6.182
10.10.6.30
10.10.6.32
10.10.93.12
10.10.93.110
10.10.93.112
  - 7.7 迁移cobaltstrike
    - cobaltstrike上线
      - （1）进程注入
      - （2）远程VNC(桌面监控)
      - （3）激活Guest账户并加入管理员组
        - Guest远程桌面登录，用户名：MIHAIBO-PC\Guest 密码：空（直接回车）
      - （4）获取sshell凭证
        - 获得"10.88.17.9"的权限，ssh账户和密码
          - 添加公钥后门
            - 免密登录
              - 查看known_hosts文件
                - 利用sshell获得的凭证，尝试登录known_hosts文件里的主机
                  - ssh成功登录
10.88.17.8
10.88.17.53
10.88.17.55
                    - 利用获取的密码fscan批量ssh探测Known_hosts文件里的主机
                      - 获得2台服务器root权限
*10.10.13.56
*10.10.14.115
                    - 利用获取的密码fscan批量ssh探测10.88.17.0/24网段
                      - 获得10.88网段下的25台服务器root权限
10.88.17.7
10.88.17.8
10.88.17.9
10.88.17.13
10.88.17.14
10.88.17.23
10.88.17.25
10.88.17.27
10.88.17.28
10.88.17.29
10.88.17.30
10.88.17.31
10.88.17.32
10.88.17.33
10.88.17.34
10.88.17.35
10.88.17.36
10.88.17.37
10.88.17.38
10.88.17.39
10.88.17.40
10.88.17.45
10.88.17.53
10.88.17.55
10.88.17.61