电网项目工作总结（2020.9.12-2020.9.18）——李想

1.任务要求

> **弱口令扫描**（长期任务）

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。

2.进展情况

1. **通过资料查询与代码阅读，得到结论`IoTSeeker`不适合作为弱口令扫描工具**

   IoTSeeker为四年前GitHub项目，目前不再维护，且内置device爆破字典内容较少，测试样例不足以检测设备安全性。

2. **选择使用`hydra`工具进行弱口令扫描**

   `hydra`是著名黑客组织thc的一款开源的暴力密码破解工具,可以在线破解多种密码。

   这款暴力密码破解工具相当强大,支持几乎所有协议的在线密码破解,其密码能否被破解关键在于字典是否足够强大。

3. **在`centos`与`kali`上进行了工具安装与测试成功**

   `hydra`内置于kali中可以在集成环境中直接使用，在centos环境中安装使用也较为简单。并通过了使用测试。

4. 协助查找物联网漏洞和实用的检测工具

   查找阅读了GitHub相关物联网相关检测工具，与项目组成员讨论后得到结论成形工具较少，不易在项目上直接使用。

3.结果分析

1. centos中的hydra安装

   下载

   ```
   wget https://github.com/vanhauser-thc/thc-hydra/archive/master.zip
   ```

   安装依赖

   ```
   yum -y install gcc libssh-devel openssl-devel
   ```

   解压

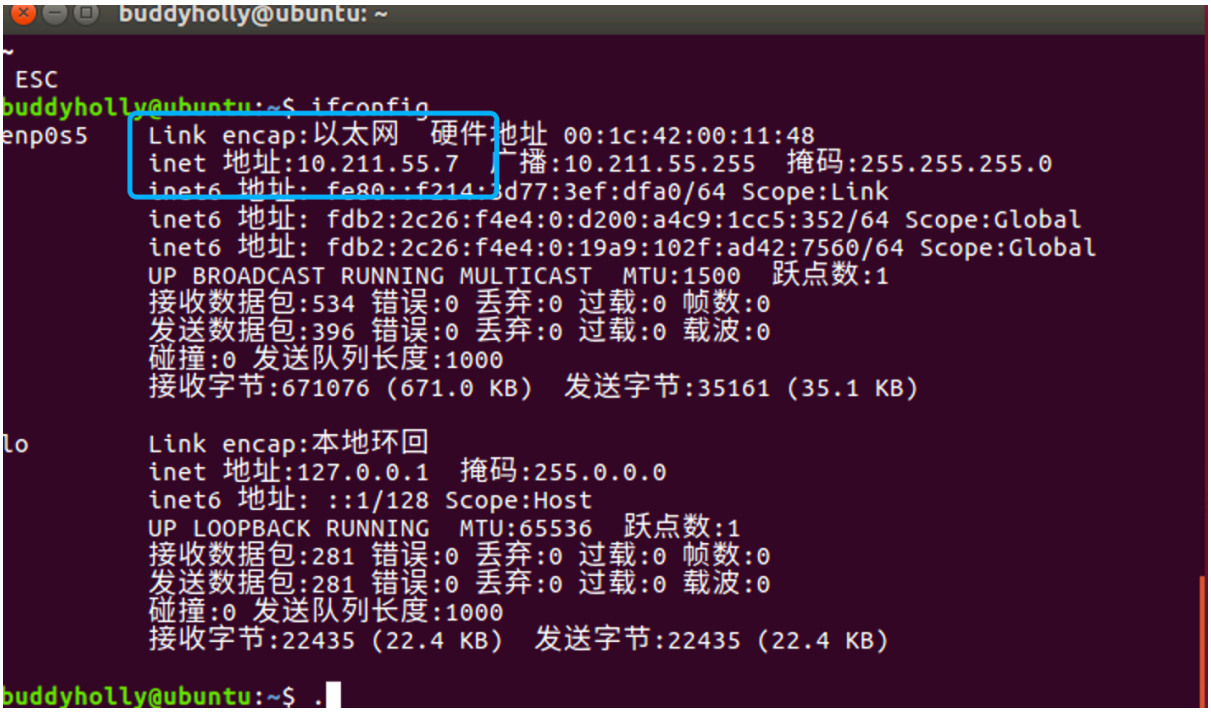
```
unzip master.zip
```

编译安装（su）

```
cd thc-hydra-master/
./configure
make && make install
```

之后即可直接使用

2. kali中的hydra使用结果

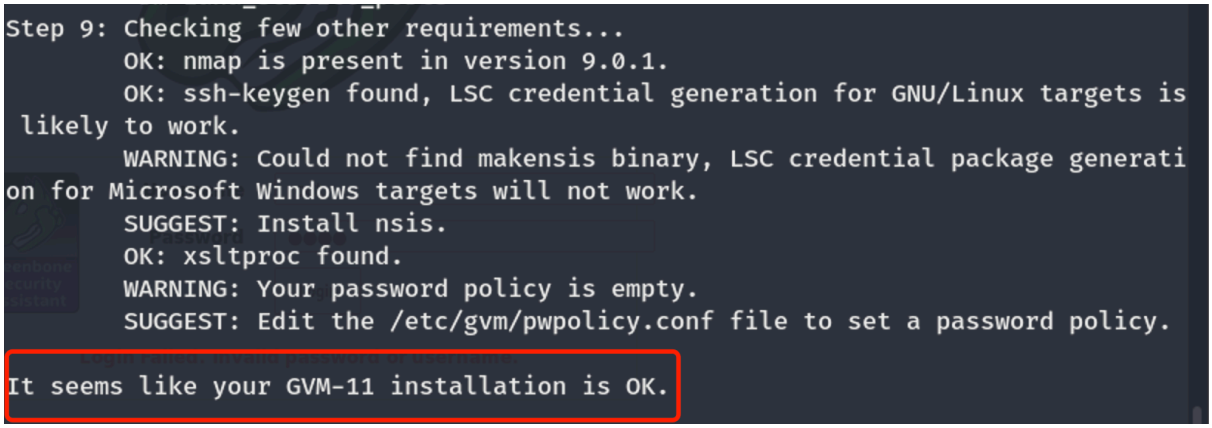



```
root@Kali-2020:~/Desktop# hydra -l buddyholly -P password.txt 10.211.55.7 ssh
Hydra v9.1 (c) 2020 by van Hauser/THC & David Maciejak - Please do not use in mi
litary or secret service organizations, or for illegal purposes (this is non-bin
ding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2020-09-14 18:57:
44
[WARNING] Many SSH configurations limit the number of parallel tasks, it is reco
mmended to reduce the tasks: use -t 4
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip wa
iting)) from a previous session found, to prevent overwriting, ./hydra.restore

[DATA] max 16 tasks per 1 server, overall 16 tasks, 101 login tries (l:1/p:101),
 ~7 tries per task
[DATA] attacking ssh://10.211.55.7:22/
[22][ssh] host: 10.211.55.7   login: buddyholly   password: lion45655
1 of 1 target successfully completed, 1 valid password found
[WARNING] Writing restore file because 6 final worker threads did not complete u
ntil end.
[ERROR] 6 targets did not resolve or could not be connected
[ERROR] 0 target did not complete
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2020-09-14 18:58:
37
```

可以看到已经成功探测局域网中开设`ssh`服务的账户密码（通过自生成字典）。

3. openvas安装测试

   安装成功但是账户无法登陆，待解决



4.下一步计划

1. 需要成功**配置`openvas`账户**，运行`openvas`框架。
2. 确定是否可以**在`openvas`中调用`hydra`**，若可集成尝试将`hydra`模块集成在`openvas`环境当中。

附

> hydra用法简记：https://leex0.top/2020/09/14/hydra%E7%94%A8%E6%B3%95%E7%AE%80%E8%AE%B0/