情報ネットワーク応用 演習 2 - レポート課題

森田 蓮

2025 年 1 月 20 日

1　演習手順

1. Nmap を利用して，カメラが動作しているサービスを調べる．
2. ブルートフォース攻撃を行い管理画面の認証を突破する．
3. カメラを乗っ取り動作させることを確認する．
4. パスワードを変更してブルートフォース攻撃でパスワードが漏れないことを確認する．
5. WEB カメラから機器の乗っ取りを行う．

2　演習 2 で学んだこと

本演習で，学んだことは 3 つある．１つ目は，脆弱性がある IoT 機器は簡単に乗っ取られてしまうことを学んだ．２つ目にブルートフォース攻撃を行うことで簡単なパスワードではいとも簡単にログインを行えることも理解した．セキュリティ対策として，強固なパスワードを設定することでブルートフォース攻撃を行った際にパスワードが破れないことが確認できた．それゆえに，強固なパスワードを設定をすることを設定することが重要である．３つ目は，Nmap などのツールを利用するときは正確なコマンドとオプションへの理解が不可欠であることが理解できた．

3　感想

今回の演習では班の人数が少ないこともありとても私たちの班は自分たちの理解がしやすい演習になった．本演習では，序盤スライドの冒頭部分のコマンドの説明を見て作業しており私たちの欲しい情報が上手く出力されず時間を浪費してしまった．やはりコマンドのオプションは理解してから使うべきであると思う．わからないコマンドを利用することは非常に悪手であり説明を読んで理解するにはネットワークであるならネットワークの知識を身に着ける必要がある．セキュリティに関連するツールやコマンドを使用する際には，その動作原理や仕組みを正しく理解しておくことの重要性を痛感した．演習では，途中で知識が不足している部分を補うために，参考資料や公式ド

キュメントを確認する時間が多く必要となり，効率が悪かった．また，ブルートフォース攻撃の実行プロセスでは，実際に試行回数を重ねる中でパスワードが破られる様子を目の当たりにし，簡単なパスワードがどれほど脆弱かを実感した．特に，辞書攻撃といった手法の効果的な活用が，攻撃者にとって非常に有利な手段であると理解した．しかし自分たちのパスワードを moritaren に変えたときにブルートフォース攻撃でパスワードを表示することができなかったため，本物の攻撃者は何を使用しているのか気になった．これからの演習を通してもっと基礎知識を増やして行きたい．