DNS キャッシュポイズニングを題材とした情報セキュリティ教材の開発

小松なごみ† 浦山 康洋†
†高知工業高等専門学校　ソーシャルデザイン工学科

1．はじめに

ISC2 Cybersecurity workforce study 2023 の報告によると，日本のセキュリティ人材は約 11 万人が不足している[1]．総務省が発表している令和 5 年版情報通信白書においても日本のセキュリティ人材は質的にも量的にも依然不足していると指摘されており[2],セキュリティ人材の育成が急務となっている．

本稿では情報システムに対する攻撃の一つである DNS キャッシュポイズニングに着目し，本攻撃を容易に体験できる実験環境とその手順・解説書を作成する．作成した成果物をまとめることで，セキュリティ人材育成の一助となれるような学習教材の完成を目指す．

2. DNS キャッシュポイズニング

DNS キャッシュポイズニングとは，DNS サーバへ偽の情報を流し込むことで，DNS の利用者を不正なサイトへ誘導する攻撃である．DNS キャッシュポイズニングが発生する流れを以下に示す（図 1 参照）．

① 一般ユーザがキャッシュ DNS へ名前解決を依頼する DNS メッセージを送信する．
② キャッシュ DNS が①のメッセージを受信し，当該メッセージを権威 DNS に転送する．
③ 攻撃者は権威 DNS の応答パケットを偽装し，キャッシュ DNS に向けて送信する．キャッシュ DNS はこの偽装パケットを正規の応答と誤認してしまい，当該情報をキャッシュとして一定期間保管する．
④ キャッシュ DNS は③の偽情報を①の応答としてユーザに転送する．
⑤ 一般ユーザがキャッシュ DNS から偽情報を受け取ってしまい，攻撃者の用意した偽サイト，または悪質なサイトへ誘導されてしまう．

3. 演習環境の構築

3.1. DNS サーバ

2 台の RaspberryPi（小型 PC)に，DNS サーバソフトである BIND9 をインストールし,それぞれを権威 DNS，キャッシュ DNS として動作するよう設定を行った．また，DNS キャッシュポイズニングの成功確率を上げるために，両 DNS に対して以下の設定を施した．

■送信元ポートの固定（キャッシュ DNS）

図 1 中②において，キャッシュ DNS が権威 DNS へメッセージ転送を行う際は，ポートランダマイゼーション機能によって送信元ポートがランダムに決定される．DNS ではこの送信元ポートを正規の応答であるかの判断材料としているため，本機能を OFF にしポートを固定することで攻撃の成功確率を上げた．

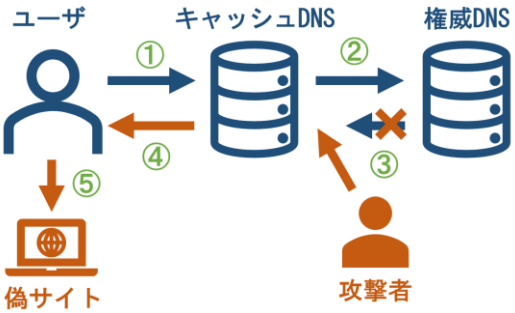

図 1　攻撃の全体図

■EDNS の無効化（キャッシュ DNS）

BIND9 では DNSSEC(DNS Security Extensions)というセキュリティツールがデフォルトで設定されている．DNSSEC では応答パケットが正しいものであるか検証が行われるため，本機能を一時的に無効化した．

■ネットワーク遅延の設定（権威 DNS）

権威 DNS の応答に遅延を設定し，権威 DNS からの応答がキャッシュ DNS まで到達する時間を延長した．これにより,偽装応答が割り込む時間を確保した．

3.2. 攻撃用プログラム

本稿では，DNS キャッシュポイズニングを実行するためのプログラムを Python 言語で記述した．具体的には，Python で用意されている Scapy ライブラリを用いて偽装応答を生成・送信するプログラムを作成した．ここで，DNS の通信ではトランザクション ID という 16bit の識別子が用意されており，DNS はこの ID を使って応答が正しいものであるかを確認していることに注意する．今回作成したプログラムにはトランザクション ID を変更しながら偽装応答を送信し続ける機能を実装しており，偽装応答を 1 秒間に約 6,000 件送信できることを確認した．

4．まとめと今後の予定

本稿では DNS キャッシュポイズニングを題材とした学習教材の作成状況について報告した．今後は演習手順書を作成し実際に模擬演習を行うことで，学習教材としての有用性を評価する予定である．

参考文献

[1] International Information System Security Certification Consortium (ISC2), https://www.isc2.org/research
[2] 総務省，″令和5年版情報通信白書（PDF版），″ https://www.soumu.go.jp/johotsusintokei/whitepaper/ja/r05/pdf/index.html