平成 30 年度 秋期 情報処理安全確保支援士

＜午後Ⅰ解答・解説＞

＜問１＞　ソフトウェア開発

■設問１

［試験センターによる解答例］

(1) a：キ
　　b：カ
　　c：ウ
　　d：ア

(2) あ：㋒

(3) shell コードが DEP で実行禁止にされているスタック領域にあるから（34 字）

(1) a：スタック領域は、プログラム内でサブルーチンを呼び出す際に、その戻り位置であるリターンアドレスを格納するほか、サブルーチン内で定義された変数の格納など、一時的に使用されるデータを格納する用途に使われる。スタックバッファオーバフローは、スタック領域に確保された変数に、サイズを超えたデータを格納することで、リターンアドレスを書き換え、不正な shell コード等を実行する攻撃である。

b：DEP（Data Execution Prevention）を回避する手法として、「Return-to-libc」と呼ばれるバッファオーバフロー攻撃がある。Return-to-libc では、攻撃者はメモリ上にロードされた libc 共有ライブラリ内の特定の関数を呼び出すようにリターンアドレスと引数を書き換えることにより攻撃を成立させる。この攻撃はスタック領域のコードを実行するわけではないため、DEP が実装されていたとしても防ぐことができない。

c：図 2 で Vuln が格納されていることからわかるように、テキスト領域である。

d：上記のように、該当するのは Return-to-libc 攻撃である。

(2) 図 2 を見ると、メモリアドレスは下に行くほど低位となっていることがわかる。した

がって、shell コードの開始アドレスは㋐である。なお、通常プログラムや初期データなどをメモリに格納する場合には低位のアドレスから使われていくが、スタック領域では、逆に高位のアドレスから順に使われる。これは、スタック領域にするデータの数が増えることによって、メモリに格納されたプログラムやデータを破壊してしまうのを防ぐためである。

(3) DEP は、データ領域に格納されたデータをプログラムとして実行するのを禁止する機能である。この機能により、スタック領域に格納されたデータをプログラムとして実行することができなくなるため、攻撃は成功しない。

■設問２

［試験センターによる解答例］

(1) e：canary
　　f：ASLR

(2) g：strcpy

(1) e：表 1 の SSP の概要にあるように、この方式では canary と呼ばれる値を利用してスタックバッファオーバフローの有無を確認する。関数を呼び出す際にベースポインタレジスタ保存値より下位に canary（″カナリア値″とも呼ばれる）を挿入しておき、canary が上書きされた場合に攻撃と判断する。

f：表 1 の概要にあるように、プログラムの実行時に、データ領域。ヒープ領域、スタック領域及びライブラリをランダムにマップすることで、ライブラリ関数等のアドレス推定を困難にさせる OS の技術として、ASLR がある。ただし、ASLR はテキスト領域にある実行可能なコードを用いる攻撃に対しては効果がない。

(2) g：プログラム Vuln で使われているライブラリ関数で、バッファオーバフローを引き起こす可能性があるのは、strcpy である。

■設問 3

［試験センターによる解答例］

(1) 行番号：16 行目
排除できない理由：ポインタを使って直接メモリ操作しているから（21 字）

(2) 問題：メモリ破壊攻撃を防げないこと（14 字）
開発環境：SSP を適用できないコンパイラを利用する開発環境（24 字）

(1) 表 1 の概要にあるように、Automatic Fortification は、脆弱なライブラリ関数をコンパイル時に安全な関数に置換する技術であるが、同機能を使用したとしても、ポインタを使って直接メモリ操作を行っている場合には、バッファオーバフローの原因を排除することができない。これに該当する処理は、16 行目である。

(2) SSP は、コンパイラを用いてスタックバッファオーバフロー脆弱性を悪用した攻撃を防ぐ対策技術であるため、コンパイラに依存している。したがって、SSP を適用できない開発環境でコンパイルした場合には同機能は有効とはならず、メモリ破壊攻撃を防ぐことはできない。

＜問２＞　セキュリティインシデント対応

■設問 1

［試験センターによる解答例］

a：ウ
b：ス
c：セ
d：エ
e：コ

a：1Gbps の全二重であるから、1Gbps ×2 で、最大 2Gbps となる。

b：IEEE 802.1Q では、VLAN タグを用いて VLAN を構成する。