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。

c：ミラーポートを使用せずにパケットを取得する方法として、ネットワークタップを使用する方法がある。ネットワークタップは、ネットワーク上を流れるトラフィックをレイヤ 1 レベルで分岐して取り出す装置である。

d：同一セグメント内の PC を探索する目的でブロードキャストで送信されるリクエストであるから、該当するのは ARP（Address Resolution Protocol）である。

e：ワームのインディケータ情報など、サイバー攻撃活動を記述する標準的な仕様として、STIX（Structured Threat Information eXpression）がある。STIX は、サイバー攻撃活動(Campaigns)、攻撃者(Threat_Actors)、攻撃手口(TTPs)、検知指標(Indicators)、観測事象(Observables)、インシデント(Incidents)、対処措置(Courses_Of_Action)、攻撃対象(Exploit_Targets)の 8 つの情報群から構成されている。

■設問２

［試験センターによる解答例］

(1) SYN＋ACK（7 字）

(2) (a) パケットが NSM センサの監視対象外であるため（22 字）
(b) 同一 IP アドレスへのスキャン回数は少ないから（22 字）

(1) TCP では、次のようなフラグの組合せによる 3 回のパケットのやり取り（3 ウェイハンドシェイク）によって接続を確立する。

① SYN　　接続要求
② SYN+ACK　正常応答（接続可能）
③ ACK　　接続確立

ポートスキャンに対する正常な応答とは、②の SYN+ACK である。

(2) (a) 図 1 にあるように、NSM センサは L3SW に接続されているため、L3SW を経由するパケットを監視対象としている。感染した PC と同一セグメント内でのポートスキャンであればパケットが L3SW を通過しないため、NSM センサの監視対象となり、宛

先 IP アドレス別の件数として集計されない。

(b) 図3下部の説明にあるように、(b)のスキャンは、IPアドレス範囲の最後までスキャンが完了した場合、スキャンを終了する。したがって、同一の IP アドレスへのスキャン回数は少なく、宛先 IP アドレス別の件数の上位には登場しないと考えられる。

■設問3

［試験センターによる解答例］

(1) PC101, PC133, PC277, PC301, PC321, PC340

(2) イ、オ、カ

(1) 表1で、445/TCP ポートをスキャンしてる PC のホスト名を表2で確認すると、次のようになる。

14:25:02 の時点で 192.68.0.32 をリースされていた PC のホスト名：PC321
14:26:45 の時点で 192.68.0.8 をリースされていた PC のホスト名：PC101
14:27:18 の時点で 192.68.0.44 をリースされていた PC のホスト名：PC277
16:51:50 の時点で 192.68.0.12 をリースされていた PC のホスト名：PC101
17:31:22 の時点で 192.68.0.44 をリースされていた PC のホスト名：PC133
17:31:23 の時点で 192.68.0.32 をリースされていた PC のホスト名：PC340
17:31:25 の時点で 192.68.0.12 をリースされていた PC のホスト名：PC101
17:31:25 の時点で 192.68.0.8 をリースされていた PC のホスト名：PC301

上記のホスト名から重複分を除き、昇順に並べると、PC101, PC133, PC277, PC301, PC321, PC340 である。

(2) 上記のように、感染した PC の送信元 IP アドレスは 192.68.0.8, 192.68.0.12, 192.68.0.32, 192.68.0.44 の4つであるが、これらのうち、複数の PC によって使われた IP アドレスは、192.68.0.8, 192.68.0.32, 192.68.0.44 の3つである。

■設問４

［試験センターによる解答例］

(1)・セキュリティ修正プログラムが適用されていること（23 字）
・マルウェア定義ファイルが更新されていること（21 字）
・PC がマルウェアに感染していないこと（18 字）
※上記より 2 つ。

(2) VLAN を使い、PC 間の通信を禁止する。(20 字)

(1) 問題文にあるように、ワーム V の感染が広がった原因は、IP アドレスが 192.168.0.32 の PC を社外に持ち出して公衆無線 LAN に接続した際に、セキュリティ修正プログラムが未適用で、かつ、マルウェア対策ソフトのマルウェア定義ファイルが更新されていない状態であったためと考えられる。したがって、PC を持ち帰った際に接続可否を判断するためにチェックすべき内容としては、セキュリティ修正プログラムが適用されていること、マルウェア定義ファイルが更新されていること、が挙げられるほか、PC がマルウェアに感染していないことをチェックすることも必要である。

(2) 問題文に「L3SW 及び L2SW は、VLAN をサポートしている機器であるが、G 社では VLAN の設定はしていない」とあり、これが解答のヒントになる。同じ L2SW に接続された PC 同士のワーム感染を防ぐには、使われていなかった VLAN の機能を使い、PC 間の通信を禁止するのが有効である。

＜問３＞　ソフトウェアの脆弱性対策

■設問１

［試験センターによる解答例］

NTP による時刻同期（10 字）

FW やサーバの時刻を整合させる方法としては、NTP（Network Time Protocol）を用いるのが一般的である。

■設問２

［試験センターによる解答例］

a：CVSS

基本評価基準、現状評価基準、環境評価基準の三つの基準で脆弱性の深刻さを評価するシステムは、CVSS（Common Vulnerability Scoring System：共通脆弱性評価システム）である。CVSS は、IT 製品の脆弱性に対するオープンで汎用的な評価手法であり、ベンダに依存しない共通の評価方法を提供している。CVSS で用いる三つの基準は次の通り。

基本評価基準（Base Metrics）
脆弱性そのものの特性を評価する基準。機密性、完全性、可用性に対する影響を評価し、CVSS 基本値（Base Score）を算出する。

現状評価基準（Temporal Metrics）
脆弱性の現状の深刻度を評価する基準。攻撃コードの出現有無や対策情報が利用可能であるかといった基準で評価し、CVSS 現状値（Temporal Score）を算出する。

環境評価基準（Environmental Metrics）
製品利用者の利用環境も含め、最終的な脆弱性の深刻度を評価する基準。攻撃による被害の大きさや対象製品の使用状況といった基準で評価し、 CVSS 環境値（Environmental Score）を算出する。

■設問３

［試験センターによる解答例］

E サーバをネットワークから切り離して、待機サーバを公開する。（30 字）

問題文より、E サーバが攻撃を受けていることは明らかである。このような状況で被害拡大を防止するためにとるべき措置としては、E サーバをネットワークから切り離すことである。続いて、こうした事態に備えて準備してある待機サーバを接続し、公開する必要がある。

■設問 4

［試験センターによる解答例］

① 調査すべき機器：外部メールサーバ又はログ管理サーバ（17 字）
調査すべき内容：外部メールサーバからサイト Z への接続の有無を確認する。（27 字）

② 調査すべき機器：E サーバ又はログ管理サーバ（13 字）
調査すべき内容:外部メールサーバへの SSH コマンドの接続の有無を確認する。(29 字)

③ 調査すべき機器：FW1 又はログ管理サーバ（12 字）
調査すべき内容：サイト Z と HTTP を使用した通信を確認する。（22 字）

※①、②又は③の組合せとする。

図 3 にあるように、スクリプト U は次のような振舞いをする。

・AP1，及び AP1 を動作させるのに必要な複数のライブラリをサイト Z から HTTP を使ってダウンロードし、AP1 を実行する。
・コマンド履歴から SSH コマンドの接続先 IP アドレスをすべて抽出する。
・IP アドレスが抽出された場合は、IP アドレスで示される各機器に対し、SSH コマンドで接続を試行し、成功するとその機器上でスクリプト U を実行する。

また、表 1 にはログ管理サーバについて次のような説明がある。

・B 社情報システム中の全 FW 及び全サーバのログを syslog で受信し保存する。
・FW1 及び FW2 のログには、通信の通過や遮断に関する記録がある。
・各サーバのログには、OS 上で実行される SSH などのコマンド履歴、アプリケーションやミドルウェアのイベント記録がある。
・Web サーバ及びプロキシサーバのログには、送信元及び宛先の IP アドレス、HTTP リクエストの内容、データ転送量などが含まれている。
・ログ保全機能があり、それによって、保存したログが改ざんされていないことを証明できる。

E サーバのコマンド履歴に外部メールサーバの IP アドレスが含まれていた場合には、次のような事象が発生する可能性がある。

(1) E サーバに感染を感染したスクリプト U が、外部メールサーバに対し、SSH コマンドで接続を試行する。
(2) 外部メールサーバに感染したスクリプト U が、FW1 経由してサイト Z に接続し、HTTP を使って AP1，及び AP1 を動作させるのに必要な複数のライブラリをダウンロードする。

上記の発生状況について調査する対象としては、まず(1)については、E サーバ又はログ管理サーバを対象として、外部メールサーバへの SSH コマンドの接続の有無を確認すべきである。続いて(2)については、外部メールサーバ又はログ管理サーバを対象として、外部メールサーバからサイト Z への接続の有無を確認すべきである。また、FW1 のログには通信の通過や遮断に関する記録があるので、(2)については、FW1 又はログ管理サーバを対象として、サイト Z との間で HTTP を使用した通信についても確認すべきである。

■設問５

［試験センターによる解答例］

(1) b：攻撃（2 字）

(2) インターネットからの HTTPS 通信を復号する機能（24 字）

(3) c：外部 DNS サーバ
　　d：CNAME

(1) WAF をモニタリングモードで導入した場合し、アラートが通知された際に検知した通信について確認することであり、その場合には E サーバの停止が必要となるのであるから、該当するのは「攻撃」である。

(2) 通販システム利用者の通信プロトコルは HTTPS であり、E サーバとの通信は全て暗号化されている。そのため、L2SW と E サーバとの間に設置されるハードウェア型 WAF には、インターネットからの HTTPS 通信を復号する機能が必要である。

(3) c：E サーバへのアクセス経路をクラウド型 WAF 経由に変えるには、E サーバへのアクセス要求があった際に、クラウド型 WAF の IP アドレスに名前解決するように外部

DNS サーバの設定を変更する必要がある。

d：ホスト名の別名を記述する DNS サーバのリソースレコードは「CNAME」である。