平成 31 年度 春期 情報処理安全確保支援士

＜午後Ⅱ解答・解説＞

＜問 1＞　マルウェア感染と対策

●設問 1

［試験センターによる解答例］

a：FW1
b：プロキシサーバ

a：プロキシサーバからインターネット上の C&C サーバへの通信が行われていたことを確認するには、インターネットとの境界にある FW1 のログを確認する必要がある。

b：問題文に「プロキシサーバでは、各機器からのすべてのアクセスについて、アクセスログを取得している」とあるように、インターネット上の C&C サーバとの HTTP over TLS 通信を開始した端末を特定するためには、プロキシサーバのログを確認する必要がある。

●設問 2

［試験センターによる解答例］

内容：削除されたファイルの内容（12 字）
手段：空きセクタの情報からファイルを復元する。（20 字）

今回のインシデントではマルウェアによる外部への情報流出の可能性が疑われるが、こうしたケースでは、マルウェアによって流出させたファイルが削除されていることが多い。そのため、HDD からその痕跡を探すには、ファイル単位ではなく、すべてのセクタをコピーして調査する必要がある。ファイルが削除された場合、HDD には空きセクタとして記録されているため、そこから削除されたファイルを復元できる可能性がある。

●設問 3

［試験センターによる解答例］

(1) MAC アドレスが平文の状態で送信されるから（21 字）

(2) 端末の無線 LAN ポートの MAC アドレスを、総務部の W-AP に登録済みの MAC アドレスに変更する。（48 字）

(1) WPA2 によって無線 LAN の通信内容は暗号化されるが、MAC アドレスについては暗号化されず、平文のまま送信されている。そのため、無線 LAN の通信が傍受されると、B さんが利用しているタブレット PC の MAC アドレスを攻撃者が知ることができてしまう。

(2) 前述のように、MAC アドレスを傍受することにより、攻撃者は総務部の W-AP に登録されている MAC アドレスを知ることができる。MAC アドレスは詐称することが可能であるため、攻撃者は端末の無線 LAN ポートの MAC アドレスを、総務部の W-AP に登録済みの MAC アドレスに変更することにより、不正に接続できたと考えられる。

●設問 4

［試験センターによる解答例］

(1) IP ヘッダ部及び TCP ヘッダ部は、同一のバイト列であることが多いこと（34 字）

(2) c：同一の暗号ブロック（9 字）
d：平文ブロック（6 字）
e：カウンタ値を暗号化した値（12 字）

(1) TCP/IP のパケットにおいて、IP ヘッダ部には送信元 IP アドレスや送信先 IP アドレス、TCP ヘッダ部には送信元ポート番号や送信先ポート番号などが格納されるため、同一端末間においては、異なるパケットであっても同一のバイト列であることが多い。そのため TCP/IP パケットをヘッダも含めて平文ブロックに分割すると、同一の平文ブロックが繰り返して現れることが想定される。

(2)

c：ECB（Electronic Code Book）モードは、暗号ブロック間の関連性はなく、単に平文をブロックごとに区切り、暗号化する方式である。そのため、TCP/IP パケット全体を ECB モードで暗号化した場合には、同一の暗号ブロックが繰り返して現れることになる。

d、e：図 3 の CTR（Counter）モードにあるように、CTR モードでは、平文ブロックとカウンタ値を暗号化した値の排他的論理和である。CTR モードでは、初期カウンタ値の再利用の強制によって、同一のカウンタ値を暗号化した値を使用して異なるパケットの暗号文を作成してしまう可能性がある。したがって、［ d ］には「平文ブロック」、［ e ］には「カウンタ値を暗号化した値」が入る。

●設問 5

［試験センターによる解答例］

(1) f：読み取る（4 字）

(2) g：カ
h：オ

(3) ・攻撃者が用意した W-AP に接続し、情報を送信する。（25 字）
・内部メールサーバを利用して攻撃者にメールを送信する。（26 字）

(1) HTTP 通信の場合、パケットは平文のため、プロキシサーバで内容を読み取ることができるが、HTTPS 通信で社内 PC と Web サーバの間で TLS セッションが成立して暗号通信路が確立した後は、プロキシサーバでは内容を読み取ることはできない。

(2) URL の構成する要素であり、解答群でこれに該当するのは「パス」と「ホスト」である。HTTPS 通信の場合は、プロキシサーバで URL のパス部を読み取ることはできず、ブラックリストに登録できるのはホスト部とポート番号部だけである。したがって、［ g ］にはカ、［ h ］にはオが入る。

(3) マルウェアが窃取した情報を社内 PC から社外に送信する経路として、FW1 を経由した HTTPS 以外の経路が問われている。まず考えられる経路として、メールがある。表 1 の

FW1 のルールと表 2 の FW2 のルールを見ると、内部 IP から内部メールサーバ、外部メールサーバを経由してインターネットにメールを送信することが可能であることがわかる。また、これとは別な経路として、攻撃者が設置した W-AP に接続し、そこから社外に情報を送信することも考えられる。

●設問 6

［試験センターによる解答例］

(1) i：信頼する CA のディジタル証明書（15 字）

(2) j：クライアント証明書の提示が必要な外部 Web サーバにアクセスする。（32 字）

(3) k：FW1 の製造元によって安全性が確認されていない CA が発行したサーバ証明書を使用した外部 Web サーバにアクセスする。（57 字）

(1) 図 4 にあるように、社内 PC は FW1 との間で TLS セッションを確立するので、FW1 が発行した自己署名証明書を社内 PC のブラウザに正規な証明書として認識させる必要がある。そのため、事前準備として、FW1 の自己署名証明書を信頼する CA のディジタル証明書としてすべての社内 PC に登録しておく。

(2) 表 5 の制約の原因に「FW1 は、社内 PC がもっているクライアント証明書に対応した秘密鍵を利用することができない」とあることから、クライアント証明書の提示が必要な外部 Web サーバへのアクセスであることがわかる。問題文にあるように、この制約を回避するには、FW1 の HTTPS 復号機能の例外リストに該当する外部 Web サーバを追加する必要がある。

(3) 表 5 の制約の原因に「FW1 の製造元によって安全性が確認された CA のディジタル証明書だけが、信頼されたルート CA のディジタル証明書としてインストールされている」とあることから、これ以外の証明書を必要とする通信であることがわかる。具体的には、FW1 の製造元によって安全性が確認されていない CA が発行したサーバ証明書を使用した外部 Web サーバへのアクセスが該当する。