BANCA D'ITALIA
EUROSISTEMA

ESTRATTO

3 ESPERTI PROFILO TECNICO CON ESPERIENZA NEL CAMPO DELLA CYBER INTELLIGENCE APPLICATA ALLA DIFESA PREVENTIVA, PROATTIVA E REATTIVA
(Bando del 2 dicembre 2020– Lettera B)

Testo n. 2

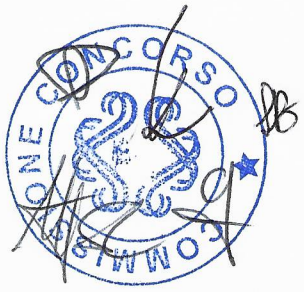
Tre quesiti su tre delle quattro materie del programma scelti tra gli otto proposti dalla Commissione (due per ogni materia del programma).

1. LA SICUREZZA DEI DATI, DEI SISTEMI E DELLE APPLICAZIONI

QUESITO N. 1A

Un'azienda ha deciso di eseguire un *penetration test* di un'applicazione già in produzione. Tale applicazione espone un servizio *web* su Internet, tratta dati riservati ed è soggetta ad alti requisiti di integrità e disponibilità.
Il candidato, con riferimento allo scenario sopra riportato:

a) progetti l'esecuzione del *penetration test*, illustrandone le fasi previste e indicando i principali strumenti che intende utilizzare;
b) indichi quali accorgimenti tecnici e organizzativi vadano considerati nelle singole fasi per minimizzare i rischi legati all'esecuzione del *test*, garantendone al tempo stesso l'efficacia;
c) proponga dei criteri per valutare la criticità delle vulnerabilità individuate e per pianificare i relativi interventi di risoluzione.



QUESITO N. 1B

Un utente segnala un'*email* al *Security Operation Center* (SOC) aziendale, in quanto ritenuta sospetta, di cui si riporta di seguito *header* e *body*:

```
Da: supporto@grandebanca.com
A: mario.rossi@grandebanca.com
Oggetto: Supporto GrandeBanca - Una nuova notifica nella tua area personale

Gentile collega,
c'è un messaggio urgente per te.

Per visualizzarlo, accedi alla tua area personale cliccando a questo link: la tua area personale

Cordialmente,
il team di supporto
```

HEADER, BODY

```
Authentication-Results: mailgw.verify;
        spf=pass smtp.mailfrom=supporto@grandebanca.tk;
        dmarc=none

Received: from [XXX.YYY.ZZZ.KKK] (smtp.grandebanca.tk [XXX.YYY.ZZZ.KKK])
        by mail.grandebanca.com (Postfix) with ESMTP id 5ACE5C0CF2
        for <mario.rossi@grandebanca.com>; Wed,  3 Feb 2021 06:39:19 +0100 (CET)
From: <supporto@grandebanca.com>
To: <mario.rossi@grandebanca.com>
Message-ID: <3741vwc61e-1@mail.grandebanca.com>
Return-Path: <supporto@grandebanca.tk>
Subject: Supporto GrandeBanca - Una nuova notifica nella tua area personale

<html>
<head><title></title></head><body>

Gentile collega,</br>
c'è un messaggio urgente per te.</br>

Per visualizzarlo, accedi alla tua area personale cliccando a questo link:
<a src="https://login.grandebanca.tk/newLogin">la tua area personale</a><br>

Cordialmente,<br>
il team di supporto.<br>

<img src=""“https://grandebanca.tk/trurl" width=""“0”"" height=""“0”"">

</body></html>
```

Il candidato, considerando che "grandebanca.com" è l'unico dominio di secondo livello registrato e gestito dall'azienda:

a) descriva le modalità di gestione della segnalazione e avanzi l'ipotesi più probabile sugli obiettivi della tecnica utilizzata;
b) individui gli *observable* di interesse, gli indicatori di compromissione (IoC) e le possibili azioni di contenimento;
c) indichi possibili contromisure tecniche e organizzative, utili a fronteggiare attacchi di questo tipo.

2. LA GESTIONE DEI DATI, DELLE INFORMAZIONI E DELLA CONOSCENZA

QUESITO N. 2A

Il CERT del gruppo Grande Banca S.p.A. riceve una segnalazione relativa all'*email* di seguito riportata:

> ***Data e ora ricezione:*** *martedì 16 marzo 2021, ore 7:45*
> ***Da:*** *APTXX@protonmail.com*
> ***A:*** *email@grandebanca.com*
> ***Oggetto:*** *Attacco DDoS*
>
> *Siamo APTXX e abbiamo scelto la vostra organizzazione come bersaglio del nostro prossimo attacco DDoS. Se non sai chi siamo, prova a cercare "APTXX" su Internet…*
> *La vostra rete subirà un attacco DDoS a partire dal prossimo venerdì; questo non è uno scherzo e per provarlo inizieremo subito un attacco dimostrativo di 30 minuti contro l'indirizzo IP del vostro sito web.*
> *Non ci sono contromisure per questo attacco poiché avrà un volume di 10 Tbps!*
> *Come fermarlo? Ci asterremo dall'attaccare i vostri server in cambio di un piccolo compenso, al momento pari a 10 Bitcoin (BTC).*
> *È un piccolo prezzo per voi, soprattutto rispetto agli impatti che deriverebbero dal nostro attacco. Ne vale la pena? A voi la scelta!*
> *Nota: il pagamento va effettuato entro venerdì; ti stiamo dando il tempo di acquistare Bitcoin, se non li hai già.*
> *L'importo del riscatto aumenterà di 10 Bitcoin per ogni giorno di ritardo nel pagamento.*
> *Si prega di inviare la somma al seguente indirizzo Bitcoin: XYZ1234567890KJH.*

Il candidato, nell'ipotesi che APTXX sia un nome utilizzato per identificare un noto *advanced persistent threat* (APT) statuale e che altre organizzazioni operanti nello stesso settore abbiano informato il CERT di aver ricevuto *email* simili, seguite effettivamente da un attacco DDoS dimostrativo:

a) esprima, sulla base delle informazioni disponibili, una valutazione del grado di pericolosità della minaccia in questione;
b) descriva le azioni da intraprendere per la pronta rilevazione dell'attacco minacciato;
c) illustri i presidi di sicurezza strutturali e contingenti che è possibile adottare per il contrasto della minaccia in questione.

QUESITO N. 2B

Il CERT di una infrastruttura critica nazionale ha consolidato l'attivazione di diversi flussi informativi: due provenienti da fornitori commerciali di *threat intelligence*, due provenienti da *information sharing* con controparti qualificate e uno da un *Information Sharing and Analysis Center* (ISAC) settoriale. Questa condizione determina un elevato flusso informativo in ingresso che richiede lo sviluppo di un processo utile alla gestione efficace ed efficiente dei dati e delle informazioni ricevute.
Il candidato, con riferimento allo scenario sopra riportato:

a) individui e descriva le principali fasi del processo di *triage* da applicare alle informazioni ricevute dal CERT;
b) descriva i principali parametri utilizzabili per la valorizzazione e la prioritizzazione delle informazioni acquisite.

3. LA CYBER THREAT INTELLIGENCE

QUESITO N. 3A

a) Il candidato descriva le fasi previste da una metodologia di analisi strutturata per l'individuazione e la valutazione di ipotesi concorrenti, come ad esempio l'*Analysis of Competing Hypotheses* (ACH) di Heuer;
b) considerando le seguenti ipotesi:
   - H1 - intrusione ascrivibile a un attacco mirato;
   - H2 - intrusione non facente parte di un attacco mirato;
   - H3 - non è avvenuta alcuna intrusione, trattasi di un falso positivo;
   - H4 - non è avvenuta alcuna intrusione, trattasi di *malware* inoculato intenzionalmente da un *insider*;

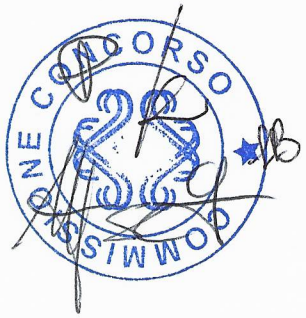
   e lo scenario descritto di seguito

> Una società che si occupa di vendite al dettaglio, facente parte di una *holding* multi-nazionale, riceve da una controparte esterna un indicatore di compromissione (IoC) descritto come il server di comando e controllo (C2) utilizzato dal *malware* XYZ che prende di mira i sistemi PoS (*point of sale*) per il furto di dati relativi alle carte di credito.
> Di seguito gli elementi accertati dalle analisi condotte sui *log* di rete sui sistemi:
> - un unico tentativo di risoluzione DNS del nome del *server* C2 in questione proveniente da un sistema PoS;
> - il PoS in questione è risultato essere infetto dal *malware* XYZ;
> - il *malware* XYZ non ha effettuato alcuna altra azione sul PoS infetto;
> - il *malware* XYZ non è riuscito a stabilire una connessione con il *server* C2;
> - non sono stati sottratti dati attraverso la rete.
>
> L'unico dipendente autorizzato ad accedere al PoS in questione è Mario Rossi che è in buoni rapporti con la società.

il candidato applichi la metodologia descritta al punto a) per ordinare le ipotesi in ordine decrescente di probabilità.

QUESITO N. 3B

Il candidato:
a) illustri le fasi, le modalità e le conseguenze di un attacco *cyber* riconducibile a un'operazione di *cyber warfare* condotta con finalità di sabotaggio;
b) specifichi le tattiche, le tecniche e le procedure adottate nello scenario precedentemente descritto.



4. IL CONTESTO ORGANIZZATIVO E NORMATIVO

QUESITO N. 4A

Un gruppo finanziario è stato recentemente oggetto di un attacco *cyber* che ha portato alla sottrazione di informazioni riservate.
A seguito di questo evento, la Direzione ha chiesto alla funzione informatica interna di eseguire un *security assessment* per misurare la reale capacità di prevenire, rilevare, rispondere e resistere ad attacchi *cyber*, al fine di individuare possibili punti di miglioramento. Al riguardo, si osserva che sono già attivi in azienda processi di *incident response*, *vulnerability and patch management* (supportato da strumenti automatici per la validazione delle vulnerabilità eliminate), e *penetration test* periodici.
Il candidato:

a) proponga e motivi alla Direzione il ricorso a un *red team test*, evidenziandone le finalità e i principali vantaggi e svantaggi rispetto a quanto già in essere;
b) illustri, riferendosi eventualmente a *framework* esistenti, le fasi del *test* proposto, descrivendo i principali ruoli previsti, i rischi legati alla sua esecuzione e le possibili misure per mitigarli.

QUESITO N. 4B

La Direttiva europea 2016/1148 *Network and Information Security* (NIS), recepita dal *corpus* normativo sul perimetro di sicurezza nazionale cibernetica, specifica che i cosiddetti Operatori di Servizi Essenziali (OSE) notifichino alla competente autorità nazionale incidenti che abbiano un impatto rilevante sulla continuità operativa di un servizio.
Il candidato:

a) illustri un possibile processo per la notifica tempestiva degli incidenti rilevanti all'autorità nazionale, così come previsto dalla Direttiva NIS;
b) descriva come l'Italia ha recepito la Direttiva NIS con particolare riferimento alla strutturazione del sistema di notifica degli incidenti rilevanti da parte delle infrastrutture critiche nazionali informatizzate.

PROVA IN LINGUA INGLESE

Due to the Covid-19 pandemic, schools have been closed for most of this and part of the previous school year, and online learning has become the norm. Consider the short and long-term consequences.