BANCA D'ITALIA
EUROSISTEMA

CONCORSO 4 ESPERTI - PROFILO TECNICO CON ESPERIENZA NEL CAMPO DELLA *CYBER SECURITY* O DELLA *CYBER INTELLIGENCE* APPLICATE ALLA DIFESA PREVENTIVA, PROATTIVA O REATTIVA

(lettera B del bando del 20 novembre 2023)

Testo n. 1

LA SICUREZZA DELLE ARCHITETTURE INFORMATICHE

QUESITO N. 1

A. Si illustri la fase di *handshake* del protocollo TLS; si descriva, con l'eventuale ausilio di un esempio pratico, la tipologia di attacco *downgrade* applicata al protocollo TLS.

B. Alcune organizzazioni, il cui numero è variabile nel tempo, hanno la necessità di scambiarsi vicendevolmente tramite internet, a cadenza temporale non nota a priori, file di ingenti dimensioni (10^4–10^6 megabyte ciascuno) contenenti dati riservati. Ciascun file può essere di volta in volta destinato a una o più di queste organizzazioni, non necessariamente a tutte. Le organizzazioni stabiliscono di conservare tali dati esclusivamente in forma cifrata.

   Si descrivano le caratteristiche principali di una soluzione tecnica che soddisfi i suddetti requisiti; si discutano le problematiche relative alla gestione del ciclo di vita delle chiavi crittografiche.

C. Si discutano i problemi di sicurezza posti dallo sviluppo del *quantum computing* nei confronti degli algoritmi crittografici basati su chiave asimmetrica e su chiave simmetrica oggi in uso.

QUESITO N. 2

A. Si illustrino i principali rischi da trattare nello sviluppo di applicazioni web con riferimento a quanto contenuto nell'OWASP Top 10.

B. Si consideri un'applicazione web che utilizza cookie per scambiare con i client dati strutturati sotto forma di oggetti serializzati; si discutano, anche con esempi, i rischi introdotti da tale pratica.

C. Si consideri un'applicazione web che può ricevere all'interno di ogni richiesta HTTP `GET` un cookie del tipo `TrackNum=ju784bh5utt87l`. In risposta a questo cookie il codice lato server esegue la query `SELECT TrackNum FROM TrackedUsers WHERE TrackNum = 'ju784bh5utt87l'`. Se e solo se la query restituisce almeno un record l'applicazione aggiunge alla pagina il testo "`Bentornato!`".

   Ipotizzando che il database contenga una tabella `Users` con campi `Username` e `Password`, si illustri come un attaccante potrebbe sfruttare la query per estrarre la password dell'utente con username "`Administrator`".

LE VERIFICHE DI SICUREZZA E LA CYBER DEFENCE

QUESITO N. 3

A. Dopo aver sinteticamente descritto le principali fasi in cui è tipicamente articolato il processo di gestione degli incidenti di sicurezza, si illustrino in dettaglio le caratteristiche della fase di eradicazione; si descrivano inoltre gli indicatori di performance (*Key Performance Indicator*, KPI) che possono essere utilizzati per valutare l'andamento del processo in termini di efficacia ed efficienza.

B. Durante l'investigazione di un incidente di sicurezza, gli analisti di un SOC aziendale hanno rilevato sulla piattaforma di *Security Information and Event Management* (SIEM) eventi relativi a numerose richieste di *Ticket Granting Service* (TGS) effettuate, nell'arco di pochi minuti, dall'*host* 10.100.8.123 per diversi *Service Principal Names* (SPN); di seguito è riportato un evento della specie:

```
Event 4769

A Kerberos service ticket was requested.

Account Information:
       Account Name: Joe@ExampleDOMAIN
       Account Domain: ExampleDOMAIN
       Logon GUID: {9133E569-7424-C429-9FD3-C2E9DACCB7DD5}

Service Information:
       Service Name: SQL-SVC-1
       Service ID: ExampleDOMAIN\SQL-SVC-1

Network Information:
       Client Address: ::ffff:10.100.8.123
       Client Port: 62793

Additional Information:
       Ticket Options: 0x40810000
       Ticket Encryption Type: 0x17
       Failure Code: 0x0
       Transited Services: -
```

1. si discuta il motivo per cui tali eventi possano essere ritenuti sospetti, specificando quale tecnica di attacco potrebbe averli generati; si indichino le possibili misure per il rilevamento di attacchi di questo tipo e si descriva una possibile regola di correlazione per la loro individuazione tramite una piattaforma SIEM;
2. si illustri sinteticamente il ruolo delle tecniche di *cyber deception* nel contrasto delle minacce *cyber* e si discuta con un esempio pratico come queste possano essere utilizzate per contrastare la tipologia di attacco individuata al punto precedente.

QUESITO N. 4

A. Si descrivano le finalità e le caratteristiche dell'attività di *threat hunting*, illustrandone le differenze rispetto all'attività di monitoraggio *real time* degli eventi di sicurezza.

B. Si descrivano le metodologie e gli strumenti utilizzabili per l'analisi statica e dinamica del software malevolo al fine di estrarre indicatori di compromissione (*Indicator of Compromise*, IoC), evidenziando vantaggi e svantaggi dei due approcci; si illustrino, infine, le caratteristiche di un software malevolo che possono impedirne o renderne meno efficace e più complessa l'analisi statica e/o dinamica.

C. Si discutano le problematiche del monitoraggio dei c.d. "*Living-Off-the-Land Binaries*" (LOLBins); si illustrino in particolare possibili strategie per rilevarne l'utilizzo a fini malevoli e per mitigare i relativi rischi.

LA CYBER THREAT INTELLIGENCE E L'INFORMATION SHARING

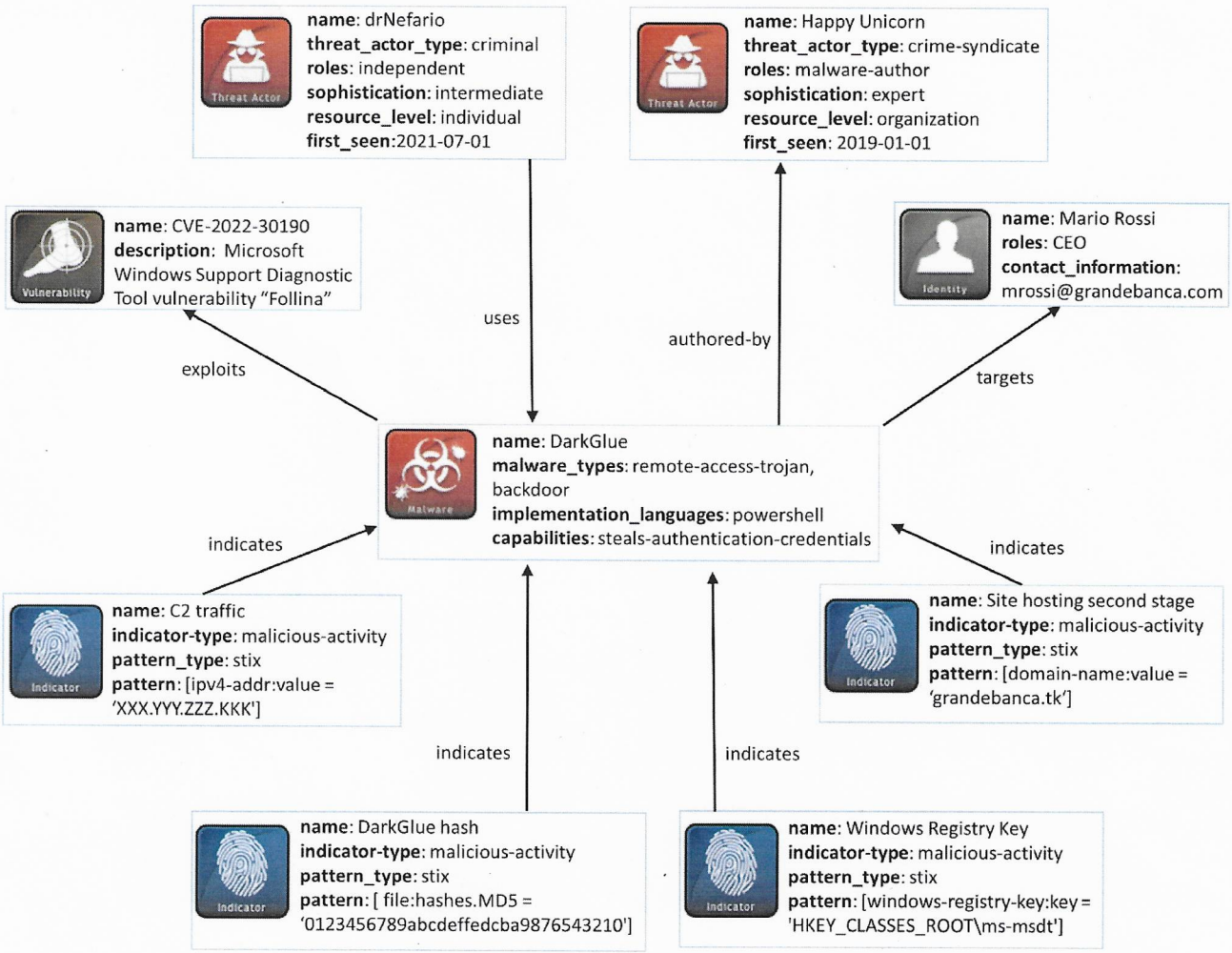
QUESITO N. 5

L'*information sharing* tratta lo scambio volontario tra controparti fidate di dati, informazioni e intelligence relativi a eventi o incidenti *cyber*.

A. Si introduca la tematica dello scambio di informazioni sensibili; si illustri quindi lo standard *Traffic Light Protocol* (TLP) per la definizione del livello di circolarità delle informazioni scambiate.

B. Si descrivano le modalità per modellare e rappresentare informazioni di *Cyber Threat Intelligence* (CTI), con riferimento allo standard STIX o equivalenti.

C. Si consideri il seguente diagramma STIX:



1. si fornisca una descrizione dello scenario rappresentato;
2. si individuino gli elementi che è possibile estrapolare ai fini della loro condivisione con una controparte fidata esterna;
3. assumendo che non si intenda diffondere informazioni relative al contesto interno all'organizzazione, si proponga il livello di circolarità da associare a ciascun elemento da condividere, motivando la risposta.

QUESITO N. 6

Nell'ambito delle attività di contrasto preventivo e proattivo della minaccia *cyber*, il CERT di una grande banca commerciale intende potenziare le proprie capacità di rilevazione di infrastrutture e di attività riconducibili alla predisposizione di attacchi *cyber* contro la banca stessa o i suoi clienti.

Nel contesto di tale scenario:

A. si descrivano le attività di monitoraggio del *surface*, *deep* e *dark web* che il CERT può svolgere, facendo anche riferimento a servizi e strumenti utilizzabili per tale finalità;

B. si discuta la problematica relativa all'esposizione involontaria di informazioni riguardanti le attività di monitoraggio intraprese dal CERT; si illustrino quindi i meccanismi da utilizzare per garantire un'adeguata OPSEC (*operations security*);

C. si descrivano le azioni di contrasto che la banca potrebbe eseguire sulle infrastrutture rilevate.

PROFILI ORGANIZZATIVI, METODOLOGICI E NORMATIVI

QUESITO N. 7

A. Si illustrino le finalità e l'ambito di applicazione materiale e territoriale del Regolamento UE/2016/679 (c.d. "GDPR").

B. InvoiceU, società con sede legale in uno Stato membro dell'UE, offre un servizio di fatturazione elettronica internazionale e interoperabile. Il servizio è erogato in modalità Software-as-a-Service (SaaS) ed è a sua volta basato su un'infrastruttura cloud offerta da un soggetto terzo (*cloud service provider*, CSP), con *data center* localizzati in paesi UE ed extra-UE. StartUp è una società con sede legale in Italia, cliente di InvoiceU per il servizio di fatturazione elettronica.

   Si illustrino i presidi di sicurezza tecnici e organizzativi che le società InvoiceU e StartUp potrebbero adottare per mitigare il rischio di *data breach*.

C. InvoiceU subisce un *data breach* che coinvolge dati personali riferibili a clienti di StartUp.

   Si illustrino sinteticamente le attività di segnalazione che, ai sensi del GDPR, ciascuna società coinvolta (InvoiceU, StartUp e il CSP) potrebbe ritenere opportuno o essere obbligata ad avviare dopo essere venuta a conoscenza del *data breach*.

QUESITO N. 8

A. Si illustrino le caratteristiche principali dei test di resilienza operativa digitale previsti dal Regolamento UE/2022/2554 (c.d. "DORA") e le diverse tipologie di entità del sistema finanziario interessate.

B. La Direttiva UE/2022/2557 (c.d. "CER") e la Direttiva UE/2022/2555 (c.d. "NIS2") fanno parte di un pacchetto legislativo volto a incrementare i livelli di *cyber resilience* e *cyber security* nell'Unione europea.

   Si discutano:

   1. finalità e caratteristiche delle due Direttive;
   2. le principali differenze tra la Direttiva NIS2 rispetto alla precedente Direttiva UE/2016/1148 (c.d. "NIS"), con particolare riferimento alle tipologie di soggetti interessati.

PROVA IN LINGUA INGLESE

The spread of fake news and the increase of misinformation found online is a concern for many. What measures can be taken to promote media literacy and ensure that individuals have access to accurate and reliable information?