-----Preambolo-----
cos'è?
questa è una compilazione delle domande infami del libro che chiede all'interrogazione, dopo l'argomento a piacere e la domanda sull'altro argomento.
Consideralo più come integrazione al file principale.
Per passare devi comunque studiare il GDPR e il darkweb anche usando quel file (quello di 48 pagine), e costituiscono l'80% della tua interrogazione, in genere chiede queste domande alla fine e se non riesci a rispondere perfettamente te ne concede un'altra, e se non rispondi neanche a questa allora ti rimanda all'appello dopo quello successivo, anche se hai portato una preparazione perfetta sul gdpr e darkweb.

a parte queste domande l'interrogazione è relativamente facile se hai studiato, visto che lui o ti dà 27-30, o ti rimanda, e i rimandati sono pochi, tipo 1/4 delle persone, e per superare queste domande ti basta una frase o 2 brevi e concise, visto che il presupposto e che hai "letto" il suo libro, e quindi ti ricordi le cose principali anche se ti scordi qualche nome.

questo file è stato compilato assistendo a circa 10 ore di interrogazione(tra gli appelli di settembre 2022 e novembre 2022) nonostante ciò credo sia al 95% completo a meno che non vengono aggiunte nuove domande(fra settembre e novembre è stata aggiunta solo quella sul ransomware a servizio) raccomando di aggiornarlo e correggere eventuali errori o mettere chiarimenti dove servono.

Ma non dicevano che era facile diritto all'informatica?
Da quanto ho capito funzionava così fino a circa l'anno scorso, però sembra che da quest'anno ha reso praticamente mandatorio leggere il libro e quelli che si sono
informati da quelli dell'anno scorso sono rimasti fregati. A sostegno della mia ipotesi il prof ha detto alla fine dell'appello di settembre " in 30 anni di insegnamento non ho mai rimandato così tante persone". Poi il libro è stato pubblicato nel 2020, esiste una edizione del 2016, ma è più piccolo.
Tutti i rimandati sono stati causati da queste domande, quindi raccomando di impararle, almeno per l'appello di gennaio 2023, poi chiedete a quelli che hanno appena fatto l'appello se questo file è obsoleto o meno.

dovresti comprare il libro?
No, a meno che non ti dispiace spendere 20 euro oppure sei molto appassionato dell'argomento.
Queste risposte sono state scritte con l'aiuto del libro(ironico), però quando ho dato l'esame non ce l'avevo, mi sono memorizzato le domande e googlato
le risposte una ad una.
Se volete comprarlo si chiama "deep web" di Emanuele Florindi, costa 20 euro edizione del 2020, non quella del 2016, se hai amazon puoi leggere gratuitamente i primi 2 capitoli.

Rischio dell' argomento a piacere
a settembre ha minacciato di togliere l'argomento a piacere per l'appello di novembre, visto che c'erano troppi rimandati, però non lo ha tolto, però a novembre lo ha minacciato di nuovo di toglierlo perché non gli piacevano quanti venivano rimandati, quindi buona fortuna per quelli di gennaio, che potrebbero non avere l'argomento a piacere.

Ci sono domande del tipo "cos'è TOR, come funziona?", "com'è strutturato internet?", "cosa fa il responsabile al trattamento?" che sono gli argomenti principali hanno risposte lunghe e dovresti studiare il file principale per saperlo, tutte le domande qui sotto hanno bisogno di una risposta breve per passare.

-----fine preambolo------

----inizio delle domande----

Hai letto il libro?
questa domanda la fa se è di pessimo umore e ha rimandato 2/3 persone di fila, ed è una domanda seria:
-se rispondi di sì ma non riesci a rispondere alle domande del libro che ti fa, allora dovrai aspettare 2 appelli prima di poterci riprovare,
-se rispondi di no, allora ti considera praticamente assente e puoi ritornare all'appello successivo. Raccomando di rispondere di Si.

Cos'è il progetto onymous?
è una operazione congiunta di decloacking condotta dall' fbi, l'europol ed altre organizzazioni nel novembre 2014 volta ad deanonimizzare e chiudere molti hidden services relativi alla vendita di beni illegali principalmente, si è conclusa con 17 arresti e 410 hidden services chiusi sequestro di 1 milione di dollari in bitcoin e 180 mila euro in contanti, oro e argento.
Come hanno fatto:
secondo quanto dichiarato dal FBI, avevano un agente sotto copertura che si è infiltrato nello staff di Silk Road, uno dei hidden service fra i più famosi, ed è riuscito ad entrare in contatto con Benthall(il capo di SR), raccogliere prove e rintracciare il server della SR,che era fuori dall'US, collaborando con la polizia locale hanno analizzato il server è recuperato molte tracce delle attività di SR.

secondo speculazioni della community di Tor invece FBI avrebbe pagato dei ricercatori per ottenere informazioni su un bug che deanonimizzava gli utenti, il bug è stato successivamente corretto.

//ci sono altre operazioni di declocking citate sul libro, non dovrebbe chiederle ma in caso le metto
nel 2016 FBI ha dirottato il traffico di un sito di pedopornografia verso dei propri server sotto controllo, e hanno raccolto informazioni per 2 mesi sugli utenti, usando un programma hacker hanno raccolto informazioni come indirizzi IP ecc, e poi si sono rivolti agli ISP per identificare i computer(circa 1300-1500)
, per poi arrestare gli amministratori e i visitatori.

nel 2019 FBI arresta l'amministratore di un sito di pedopornografia grazie al tracciamento dei bitcoin, per colpa di una mala configurazione dei pagamenti stessi un agente sotto copertura ha simulato dei pagamenti per poi risalire al wallet dell'amministratore che sta in Sud Corea, identificarlo ed arrestarlo.

//penso non lo chiede a meno che non parli delle cripto
cos'è la Ring Signature?
//Monero e alcune monete lo usano
quando si effettua una transazione su una cripto valuta, per anonimizzare le transazioni si infila la chiave pubblica del tuo wallet in un gruppo con altre wallet
chiavi pubbliche, si associa al gruppo una chiave pubblica creata attraverso le chiavi pubbliche degli utenti, e con quella si convalida la transazione, così chi riceve non può sapere chi del gruppo ha inviato il denaro, ed è praticamente impossibile tracciare un il denaro visto che i gruppi sono sempre randomizzati

che caratteristiche deve avere una moneta per il browser mining?
la moneta dovrebbe essere resistente al ASIC mining(cioè mining fatto su chip specializzati solo a quel ruolo) cosi che chi usa computer normali generalistici può partecipare al mining in maniera più

equa, non esiste un HW migliore, non puoi costruirti una farm di chip specializzati facilmente, perché una farm di chip comuni avrà la stessa performance, questo evita che poche farm detengono il controllo della moneta(come nel bitcoin), ma gente comune con i propri computer possono partecipare al mining senza grossi svantaggi.

cos'è google BERT?

bert è una tecnologia google implementata nel 2019 che integra le reti neurali per comprendere meglio il linguaggio naturale e migliorare le raccomandazioni
nella barra di ricerca, non analizza le parole separatamente ma li mette in relazione, in breve un robot in grado di capire meglio il CONTESTO.

cos'è il triangolo di Zooko?

Per la scelta di nomi in un protocollo network ci sono 3 principi desiderabili
-human-meaningful, nomi facili e memorizzabili per gli utenti
-secure, il danno inflitto da un agente malizioso deve essere il minimo
-decentralizzato, si possono riattribuire i nomi correttamente senza bisogno di un autorità centrale o servizio
il Teorema di Zooko afferma che non puoi avere più di 2 di queste proprietà, .onion e bitcoin hanno le ultime 2 proprietà, i nomi dei siti o dei utenti infatti sono stringhe casuali

cosa sono i petname?

i petname sono un sistema che risolve il triangolo di zooko, immaginando di implementarlo su tor, essi associano agli indirizzi onion(difficili da ricordare) delle parole chiave (petname,facili da ricordare), però le parole chiave non portano direttamente al sito che cerchi, ma li puoi digitalizzare su una barra di ricerca apposita e un database ti lista tutti i siti associati a quelle parole parole chiave, e cerchi il sito che vuoi è human meaningful grazie ai pet name che sono parole comuni, le altre 2 proprietà sono già garantite da Tor stesso

cos'è l'autoradicalizzazione?

algoritmi automatici di youtube, facebook, instagram, google contribuiscono a questo fenomeno, se per esempio credo ad una cospirazione, ideologia politica, visione del mondo, e li cerco su queste piattaforme, dopo un periodo prolungato di uso l'algoritmo che mi raccomanda i contenuti
tende a dare impasto a me tutti i contenuti riguardanti ciò, creando praticamente una bolla di confermation bias visto che trovo solo cose che confermano la mia visione, e trovo gente che è d'accordo con me, quindi entro in una echo chamber questo è reso possibile grazie alla grande mole di informazioni che questi siti raccolgono su di noi per profilarci.
come contrastarlo? usa incognito usa browser diversi, usa vpn, usa Tor, cambia computer, cambia device, cambia motori di ricerca, virtual machine, servizi che randomizzano la tua impronta digitale(IP,che lingua usi, a che ora del giorno accedi al sito, che dispositivo usi, ecc.)

tecnodiscriminazione

quando le intelligenze neurali o programmi discriminano categorie di utenti per ragioni, le banche per esempio non danno prestiti a utenti che hanno indice di affidabilità basso, oppure giornali mostrano articoli solo a persone di una certa ideologia/etnia, in breve si formano nuove minoranze che vengono filtrati automaticamente dagli algoritmi, oppure anche da umani che però hanno usato questi algoritmi per raccogliere
le informazioni

java anon proxy

è un servizio di proxy sviluppata da una università tedesca che permette di ottenere anonimato revocabile, è un semplice e gratuito programma java scaricabile che ti permette di poter scegliere da

una lista quali server chiamati "mixers" che vorresti usare e il programma li usa come intermediari per anonimizzare la tua connessione, è sicuro grazie al fatto che gli intermediari non registrano la tua attività, e la tua connessione viene mascherata dal fatto che altri usano lo stesso "mixer", ogni mixer non conosce l'identità di chi la usa visto che la connessione passa per molti di questi ed è criptata.
JAP ha perso fiducia degli utenti perché se la magistratura lo chiede, possono forzare i mixer a tenere log di utenti criminali, poi è pure circolata la voce che il programma JAP avesse anche uno spyware, qualche riga di codice che diminuiva l'anonimato.
nonostante ciò JAP è comunque uno dei programmi più sicuri per l'anonimato se non commetti crimini.

che tipi di servizi ci sono nel dark web?
vendita di armi
vendita di carte di credito rubate o contraffatte
Servizi di contraffazione, riciclaggio o lavaggio di denaro
vendita di prodotti contraffatti o rubati
assumere killer
assumere hackers
contenuti pedopornografici
redroom(stanze della tortura in diretta streaming)

come funziona la compravendita nel darkweb?
generalmente si usano criptovalute(perché il denaro reale è tracciabile dalla polizia).
come fai a fidarti di un venditore anonimo? esistono i forum di discussione o anche siti con recensioni, per assicurarti che la merce arriva si possono usare "escrow services", cioé intermediari fidati da entrambe le parti dove puoi pagare a lui, il commerciante viene informato del pagamento, invia la merce, il cliente riceve la merce e conferma all'intermediario, l'intermediario rilascia i soldi al commerciante

quali sono i 2 modi con cui vengono venduti le armi nel DW?
//in realtà sono 3, ma ne chiede sempre 2 per poi aggiungere una domanda extra tipo"in realtà ho mentito, c'è ne una terza, mi sapresti dire qual è?", perché il suo
//libro è strutturato così
ci sono 2 modi di vendere armi nel dark market:
-forum sulla manutenzione e manuali d'uso delle armi
-vendita di armi, munizioni, pezzi di ricambio, accessori
della seconda categoria ecco i tipi delle armi vendute:
-armi nuove di origine legale,a volte mai registrate quindi intracciabili
-armi usate che possono essere legali o illegali a seconda della provenienza
-armi usate per atti criminosi e potrebbero essere già registrate nei database della polizia
qual è il terzo modo?
terzo modo: armi improvvisate, fra queste rientrano istruzioni su come costruire esplosivi artigianali usando materiali facilmente reperibili, e vengono usati nei
attentati terroristici

tipi di hacking venduti
-hackers a noleggio
se paghi l'hacker può andare a violare account, creare ransomware personalizzati, ddos, anche violare registri scolastici per modificare voti
-servizi di hacking
questi ti aiutano a fare hacking, sono organizzazioni che offrono siti dove mettere i virus, oppure reti di computer compromessi per fare il ddos oppure inviare spam

-programmi hack
sono programmi, offerti a volte gratis, che ti aiutano a fare hack, tipo compilatori per creare virus, indovinare password, intercettare il traffico di una connessione
-manuali e guide
sono pagine informatiche che contengono guide per diventare un hacker, oppure per imparare la cyber security, contengono tecniche, procedure, vulnerabilità.
Fra vulnerabilità esistono quelli chiamati 0-day exploit che sono delle vulnerabilità che non sono state ancora corrette(letterlmante 0 giorni sono passati da quando lo sviluppatore l'ha scoperto)
-forum di discussione fra hackers
hackers discutono fra di loro per scambiarsi informazioni o pianificare qualcosa
-hacktivism
domanda a parte, vedi sotto

cos'è hacktivism?

è l'uso di hacking per sostenere un attivismo sociale o politico, generalmente senza lucro come principale obbiettivo per esempio un sito viene buttato giù perché impopolare da un gruppo di persone, oppure recentemente anonymous hackera i siti russi per favorire l'ucraina

cos'è il Netstrike?

si immagini una protesta fisica, in piazza dove la gente si raduna e blocca le strade per farsi notare, il netstrike, una forma di hacktivismo, è molta gente che si collega un sito bersaglio nello stesso momento per rallentare il sito e rallentare o bloccare totalmente il traffico(ddos praticamente)
//prof potrebbe chiede anche della storia di omega e 94 se è di pessimo umore
hactivism è stato coniato da omega nel 96(ma il libro dice 94). Omega è un membro del gruppo hacker CULT OF DEAD COW,
//non dovrebbe chiedere esempi

Com'è l'hacktivism oggi?

I gruppi hacker in genere usano Tor e dibattono nei forum quali bersagli colpire, usando ddos e defacement(rovinare l'aspetto di un sito cambiando il nome per
esempio, dopo averlo hackerato)

tipi di contenuti pedopornografici trovabili nel dark web

-forum dove i pedofili raccontano esperienze e si scambiano consigli, tutto testo
-siti dove si pubblicano i contenuti pedopornografici(immagini o video), potrebbe essere venduto o barattato con altri contenuti pedopornografici
-siti dedicati al turismo sessuale o prostituzione minorile.

cos'è una redroom?

siti dove vengono streamati persone che vengono torturate, a pagamento o gratuitamente e se paghi abbastanza potresti diventare "master" e assumere il controllo della
stanza, puoi dettare ordini direttamente ai torturatori, a volte permettendo pure di uccidere il torturato.

differenza fra cyberwar e cyber terrorismo.

entrambi usano strumenti informatici per fare guerra, la prima ha bersagli militari(intercettare comunicazioni fra soldati, sabotare sistemi missilistici),
la seconda invece mira a bersagli civili(centrali elettriche, semafori, database dei ospedali)
il cyberterrorismo ha il vantaggio che paesi sottosviluppati hanno meno da perdere (perché non hanno infrastrutture sviluppate) contro i paesi del primo mondo.
il paradosso è che le nazioni più sviluppate e ricche sono più vulnerabili agli attachi di cyberterrorismo.

Come si usa il darkweb per il terrorismo:

3 modi:
-informazione(diffondi l'esistenza del tuo gruppo terrorista)
-propaganda(convinci la gente ad aderire al tuo ideale)
-reclutamento(recluti soldati)
cosa ha portato di nuovo il darkweb rispetto a prima per i terroristi?
hai una diffusione più larga visto che puoi diffondere tanti volantini virtuali, anonimato, il reclutatore si espone a 0 rischio visto che non deve incontrare nessuno faccia a faccia, ci sono corsi di addestramenti militari online su come fabbricare e usare armi.
poi il dark web offre comunicazioni sicure, anche attraverso la stenografia(vedi wikipedia) si cripta il messaggio in un file audio o immagine, li si pubblica apertamente in un forum, e solo chi appartiene allo stesso gruppo terrorista può trovare il messaggio attraverso codici/programmi

cos'è l'albo pretorio online?

// copia incollata dal sito del comune di Milano
L'Albo Pretorio online è uno spazio informatico, accessibile senza formalità,
nel quale sono pubblicati i documenti relativi ad atti e provvedimenti che,
in base alla normativa vigente o per scelta delle singole amministrazioni pubbliche,
devono essere resi potenzialmente conoscibili a chiunque.

La cosa importante da ricordare è che fa parte del deep web per motivi giuridici, documenti personali che non devono essere indicizzati dai motori di ricerca

quali sono i tipi di proxy

-trasparent proxy: sono proxy senza configurazione che vengono messi dall'ISP per poter regolare e migliorare la navigazione
generalmente non fanno niente e servono per raccogliere dati
-anonymous proxy
aggiungono qualche header, non mettono l'IP del client, oppure mettono IP diversi, modificando l'header continuamente
-highly anonymous proxy
non modificano gli header e non trasmettono l'IP
-proxy CGI
sono siti web che ti permettono di navigare senza modificare il tuo browser
-I2P proxy
Catene di server e proxy

ramsomware as service

//l'ha chiesto ma sul libro non è molto chiaro a cosa si riferisce di preciso
il ramsomware è un particolare virus che cripta i contenuti di un computer infetto, per poi promettere di dare la chiave per la decriptazione in cambio di un riscatto
(in genere criptovalute) altrimenti il computer avrà praticamente perso i suoi contenuti permanentemente.
Dal darkweb puoi assumere hacker che possono compiere ransomware, oppure scaricarti programmi appositi per farlo.