Unknown

In questo word verranno inserite tutte le domande relative al prof Palmieri per la prova orale di cyber

1)

- Che cos'è l'IP spoofing?
- Se dovessi implementare anti-spoofing, come lo devo fare?
- Per proteggere la rete interna, dove devo mettere l'ACL?
- Attacchi noti di tipo spoofing

2)

- Come si combatte a un attacco SYN FLOOD?
- Cosa significa la reazione cooperativa?
- Qual è il meccanismo che si usa per propagare un filtro? (IPS, network operating center)
- In che cosa consiste il concetto di amplificazione di attacco?
- Come funziona la botnet?

3)

- Quali sono le possibili strategie per quando si tratta la realizzazione della botnet? (le varie catene di comando)
- Che cos'è un worm? e su che cosa lo differenzia a un malware?
- Qual è la strategia utilizzata dai worm che permette di conseguire risultati migliori in termini di copertura?
- Che cosa mi sai dire dei modelli matematici che descrivono l'andamento di un'epidemia? (dove spiega il concetto della diffusione dei warm) (domandato perchè un collega ha menzionato questo alla domanda precedente)
- Quali strategia viene utilizzata per combattere alla diffusione dei Worm?

4)

- Qual è la tecnica che si usa per fronteggiare mail spamming?
- Che cos'è un open relay?
- Nel momento in cui tutti bloccano gli open relay, è possibile continuare ad effettuare mail spamming?
- Su quale presupposto si basa la probabilità per la rivelazione di spam? (Teorema di bayes)
- Come funziona la tecnica SPF? (tecnica che viene utilizzata per evitare che un utente possa spammare prima che invia la mail)
- Se fossi chiamato come consulente per risolvere un problema legato alla difmmazione di una mail, come farei per vedere se è autentico o meno?

5)

- Anonimato per la mail
- Tipi di remailer
- Concetto di Perfect Forward Secrecy
- Hiddenn services per la rete Tor
- Concetto di Onion Routing
- Proxy Anonimizzatore
- VPN per l'anonimato

6)

- Resource starvation
- Slow rolis , rudy
- Tear drop
- Possibili attacchi in man in the middle sulla sessione tcp

7)

- Attacchi basati sul DNS e le possibili contromisure
- Dns seq
- Resource record
- Chi verifica che le risposte sono corrette? (resolver)
- Principali problemi del DNS (creazione della catena di attestazione)
- Visibilità del traffico DNS (DNS over HTTPS, DNS over TLS)
- Attacchi ai meccanismi di routing
- Come funziona l'EGP

8)

- Firewall di nuova e vecchia generazione
- Riconoscimento dei pacchetti
- Che cos'è il NAC
- Varie modalità (agent less….)
- Tre componenti del NAC
- Application web security (caratteristiche lato client, web based…)
- Certificati, policy….

9)

- Quali possibili minacce che lato server possono esserci
- Buffer overflow
- Come si fa ad ovviare a questo problema
- SQL injection
- Metodi per risolvere il sql injection

- Sql randomization
- Cross site scripting
- Cos'è l'infrastruttura AAA? (Menzione del radius)

10)

- Che differenza tra l'uso di un router con funzionalità di firewall e un firewall? (differenza sostanziale è che il firewall ha la conoscenza del flusso mentre il router no)
- Che differenza c'è tra un firewall che lavori in maniera trasparente e un firewall che lavora in maniera non trasparente?
- Il nat può essere implementato su un firewall trasparente?
- Che cos'è il firewalking?
- Le scansioni sono individuabili da un firewall?
- Quali sono gli elementi architetturali che possiamo trovare in un firewalking?

11)

- Differenza di IDS e IPS e delle modalità di detection (i vari approcci come Misuse e Anomaly)
- Quali sono le componenti architetturali del sistema IDS/IPS?
- Che differenza tra detection host based e detection network based?
- Quando lavoriamo in logica knoweldgebased, come funzionate le firme degli attacchi?

12)

- Cos'è la superficie di attacco, dominio di sicurezza e perimetro di sicurezza?
- Cosa differenzia un dominio di sicurezza a un altro dominio di sicurezza, a livello di visibilità? Come faccio a sapere che un dominio è più affidabile di un altro? (grado di livello di sicurezza)
- Come si implementano le ACL in modo da garantire la mutua visibilità? (mediante la clausola established)
- Parlando di politiche di sicurezza, quali sono i possibili approcci per implementarli? (le due modalità di ACL, deny all o permit all)
- Quali servizi utilizzeremo se dovessimo monitorare la sicurezza di un'azienda? (comportamento baseline)
- Che cos'è il flusso?
- Qual è il principio su cui si basa le tecniche non supervisionate?
- Come funziona il meccanismo che ti permette di classificare a livello protocollare il traffico? (tramite DPI)

13)

- Come funziona il nac?
- Asset inventor
- SIEM (log management)

14)

- Name chache amplification
- Meccanismo di firewall, differenza di un router e firewall
- Firewall trasparente può applicare filtraggio su indirizzo IP? (si sui controlli sul livello 3)
- Cosa sono il dominio di sicurezza, il perimetro e la superfice d'attacco
- SIEM

15)

- Anonimizzazione contenuti (freenet)
- Compromettere l'anonimato (attaccando TOR)
- Cookies
- Bloccare tor per limitare l'utilizzo
- Bridging nodes (non ho capito) in tor || sono nodi usati per bypassare il blocco della rete tor by Lucio

16)

- Nac (che cos'è…. Architettura…. Etc…..)
- Modalità raccolta dei dati(agent-based, scansioni sulla rete)
- Scansione della rete (cercando di non essere visibile)
- Scansione non percepita dal firewall (null scan)
- Attacchi stealth(slow loris, rudy, deeply nested xml)
- Buffer overflow

17)

- Controllo acessi
- Access list solo a livello 3? (no anche a lvl 2, per indirizzi MAC address)
- Firewall trasparenti e non (NAT)
- Perfect forward secrecy
- Chiavi usata per il perfect forward secrecy (AES, scambio di chiavi tra nodi… etc).

18)

- Filtro antispam (Il filtro bayesiano)
- Tar Pitting (tarpits)
- grayListing
- Come funziona l'anonimizzazione della mail (utilizzo remailer 0,1,2)
- Mail anonimizzata con la risposta (server di psudonimi, reply block)
- DKIM

19)

- Cos'è il nac?

- Che differenza c'è tra un sistema di managament tradizionale e ICM?
- Cosa sono i next generation firewall?

20)

- Che vantaggio offre il proxy anonimizzatore? E quando si utilizza?
- Le chiavi sono asimmetriche o simmetriche? (perfect forward secrecy)
- Cosa sono i bridge routes?

21)

- Template architetturali per la sicurezza
- Che cos'è il siem?
- Che cos'è il sistema sandboxing?
- Che cos'è un worm?

22)

- Che differenza c'è tra IDS e IPS? In che modo vanno a integrarsi con i firewall di nuova generazione?
- Quali sono le componenti architetturali di un sistema IDS/IPS?
- Cosa differenzia un sistema host-based e network-based?
- Che differenza c'è tra souzione knowedge-based e anomaly-based?
- Come funziona nello specifico l'anomaly-based?

23)

- Architettura della reazione comunicativa ai DoS
- Come vengono comunicati le regole di filtraggio? (mediante il protocollo BGP)

24)

- Cos'è e come funziona il DDoS?
- Che cos'è l'IRC?
- Qual'è l'architettura più robusta nel contesto di DDoS?(P2P)
- Come funziona l'effetto di amplificazione?
- Che cos'è il backscattering?

Successivamente, verranno divise anche per argomenti, per una perfetta divisione

Per ogni studente, deve esserci uno spazio di differenza

Osso

Risposte:

1)

- Che cos'è l'IP spoofing?
  - *E' una tecnica che utilizza un pacchetto IP nel quale viene falsificato l'indirizzo IP del mittente. Nell'header di un pacchetto IP si trova uno specifico campo, il source address, il cui valore indica l'indirizzo IP del mittente, modificando questo campo si può far credere che un pacchetto sia stato inviato da una macchina diversa*
- Se dovessi implementare anti-spoofing, come lo devo fare?
  - *Tramite l'utilizzo delle ACL. Quindi bisognerebbe bloccare gli indirizzi IP uscenti dalla propria rete che non appartengono al proprio intervallo di IP noti. Per combatterlo a livello globale bisognerebbe che tutti applicano questa regola, purtroppo, però, pochi lo applicano. Per esempio si potrebbe creare una ACL che permetta in uscita le connessioni tcp e un numero di servizi TCP verso l'interno limitato. Oppure di consentire in ingresso solo il traffico che ha avuto inizio dall'interno*
- Per proteggere la rete interna, dove devo mettere l'ACL?
  - *Le ACL si inseriscono nel punto più vicino alle entità da proteggere, così da definire le dimensioni del nostro dominio di sicurezza. Le ACL standard devono essere posizionate quanto più vicino alla destinazione, mentre quelle estese più vicino possibile alla sorgente.*
- Attacchi noti di tipo spoofing
  - *DHCP Spoofing: il protocollo DHCP è utilizzato per l'assegnazione dinamica per la rete (IP, DNS etc..). Non prevedendo nessun tipo di autenticazione ed essendo completamente stateless, è molto debole dal punto di vista della sicurezza. L'attaccante, per esempio, potrebbe agire in logica man in the middle assegnando il proprio indirizzo IP come DNS così che tutte le richieste vadano a lui dirottando le richieste su siti con lo scopo di rubare tutte le informazioni possibili (DNS spoofing). (da verificare o aggiungere robe) (IRD Spoofing, Email Spoofing)*

2)

- Come si combatte a un attacco SYN FLOOD?
  - In questi casi la soluzione migliore è il filtraggio in banda in cui devono essere bloccate tutte le sessioni SYN lasciando passare solo le sessioni già established (Committed Access Rate). Purtroppo, ciò non basta perché grandi SYN flood diventano comunque impossibili da gestire, ed alcuni provider come Prolexic e CloudFlare offrono una soluzione che limita l'effetto di questi attacchi: essa è basata su una rete di proxy in logica reverse che fanno da intermediari per stabilire le connessioni TCP e per inviare al sito solo le connessioni che passano in stato established
- Cosa significa la reazione cooperativa?
  - *Con l'aumento del traffico degli attacchi si ha sempre più bisogno di una cooperazione cooperativa di tutte le difese. Questo significa che c'è una "reazione networkcentrica" (o reazione coordinata o mitigazione dinamica). Questo significa che non solo i firewall, IPS o router si oppongo all'attacco ma è l'intera rete che in maniera cooperativa reagisce implementando a ciascun livello delle opportune attività in grado di bloccare l'attacco*
- Qual'è il meccanismo che si usa per propagare un filtro? (IPS, network operating center)
  -

- In che cosa consiste il concetto di amplificazione di attacco?
    - *Si basano sull'amplificazione di un attacco DOS sfruttando elementi dei rete non configurati correttamente. Quindi a questi tipi di attacco nascono i broadcast amplification attack e i DNS amplification attack. Il primo ha l'obiettivo di superare la capacità dell'host sfruttando il meccanismo di amplificazione che non sia limitata a una singola macchina ma dalla potenza di attacco dell'aggregazione di tutte le macchine. Si chiama broadcast proprio perché i pacchetti che contengono le informazioni per iniziare l'attacco sono inviato in broadcast su tutte le macchine che sono coinvolte nell'attacco(i pacchetti in broadcast vengono bloccati dal router quando vengono ricevuti da remoto, quindi non sono più utili). Per il secondo ,invece, il bot invia una query al DNS con indirizzo sorgente spoofato con quello della vittima. Quindi utilizzando anche la tecnica della riflessione, all'host arriveranno tantissimi pacchetti con grandi dimensioni causando un DOS. (per risolverlo: applicando una policy che impedisce di rispondere a domande UDP DNS).*
    - *L'ultimo è il Memcache amplification: si basa sul servizio di memcached che consente il caching distribuito open source utilizzando le porte TCP e UDP 11211. Il bot attaccante invia un messaggio all'host causando una risposta con un fattore elevatissimo avente come destinazione l'host vittima. (per bloccarlo: packet capture con protocllo UDP, porca 11211 e numero pacchetti >10)*
- Come funziona la botnet?
    - *Il bot è un agent che fornisce all'attante un meccanismo di controllo su di esso che attraverso il worm si propaga e si vanno a creare rti di macchine controllabili attraverso la logica command & control. Questo significa che i bot sono controllati da server intermedi che fungono da protettore al botmaster per impartire gli ordini ai bot stessi. I comandi possono essere diretti o indiretti permettendo all'attaccante di poter fare ciò che vuole con le macchine. I meccanismi per il controllo possono essere molteplici come IRC(server sotto controllo del botmaster che impartisce gli ordini a un altro server) oppure http (i bot effettuano richieste http al fine di interpretare le risposte ottenute come comandi da eseguire.*

3)

- Quali sono le possibili strategie per quando si tratta la realizzazione della botnet? (le varie catene di comando)
    - *I meccanismi per il controllo possono essere molteplici come IRC(server sotto controllo del botmaster che impartisce gli ordini a un altro server sul quale vengono letti i comandi dai bot) oppure http (i bot effettuano richieste http al fine di interpretare le risposte ottenute come comandi da eseguire).*
      Altri tipi di controllo remoto è il Covert Channell: Cioè creare dei canali invisibili basati su versioni modificare del protocollo IRC.
      P2P: Non c'è un single point o failure, ma i comandi vengono distribuiti in logica p2p che entrano nella comunicazione. E' la più efficiente in assoluto poiché essendo decentralizzata è molto difficile individuare il meccanismo di controllo remoto. (contromisure: antivirus)

- Che cos'è un worm? e su che cosa lo differenzia a un malware?
    - *Un worm ha una proprietà che è autoreplicante. Questa la distingue per esempio da un malware che è un software che ha lo scopo di provocare danneggiamenti o malfunzionamenti al dispositivo. Il worm viene lanciato in seguito a un'azione ed ha la Capacità di autoreplicarsi autonomamente sfruttando le vulnerabilità sconosciute (0-day) .*

Una volta arrivato al massimo della sua replicazione può lanciare attacchi DoS con logiche di tipo botnet.

- Qual'è la strategia utilizzata dai worm che permette di conseguire risultati migliori in termini di copertura?
    - *I warms possono essere classificati in diversi modi: Scanning worms e non scanning worms. Il primo permette di cercare in maniera automatica le potenziali vittime attraverso una scansione degli indirizzi IP scelti in maniera casuale. Il secondo, invece, costruisce delle liste sulla base delle informazioni che cambiano in base alle macchine compromesse come il Routing di una rete. In questo caso è meglio il secondo in quanto si possono conoscere delle informazioni importanti sulla macchina e sfruttarne le vulnerabilità. (indeciso se spiegare anche le strategie di infezione, pg 105 della dispensa, non pdf)—Scansioni localizzate, topologiche, basate su hitlist---*

- Che cosa mi sai dire dei modelli matematici che descrivono l'andamento di un'epidemia? (dove spiega il concetto della diffusione dei warm) (domandato perchè un collega ha menzionato questo alla domanda precedente)
    - *Il più noto è il modello SI (suscettibili/infettati). Questo modello tiene conto di eventuali macchine che dopo essere infettate acquisiscono magari l'immunità attraverso operazioni di patching. Però questo lavora su una logica continua, mentre a noi interessa un modello discreto. Il più famoso è modello AAWP(Analytical active worm propagation model). Questo modello permette di conoscere il risultato di un'infezione in un tempo preciso permettendo di conoscere la probabilità che un host sia infettato. Le principali differenze sono che per esempio il SI assumono un tempo di infezione pari a 0, mentre questo non è possibile poiché i warm prima si diffondono in maniera esponenziale e poi iniziano ad assestarmi magari dovuto a congestione di rete o a spazio di indirizzamento.*
- Quali strategia viene utilizzata per combattere alla diffusione dei Warm?
    - *Non esistono metodi efficaci di difesa, l'unica contromisura è individurare le vulnerabilità ed effettuale il patching delle applicazioni e sistemi operativi e tenere aggiornati l'antivirus.*

4)

- Qual è la tecnica che si usa per fronteggiare mail spamming?
    - *Ce ne sono diverse:*
        - *Black & white listening e RBL: si verificano gli header dei messaggi. Ogni volta che si riceve una mail il server consulta una lista di indirizzi che contiene una lista di mittenti validi(white) ed una lista di mittenti non sicuri(black). In realtà è possibile anche affidarsi a società terze che gestiscono un database aggiornato chiamato RBL (real time blocking list)*
        - *Filti di contenuti come: filtro bayesano—E' un meccanismo basato su analisi probabilistica, che caratterizzano uno spam. Il concetto è che permette di definire alcuni eventi che caratterizzano uno spam. Essa così di permettere di costruire le cosiddette reti bayesane, che permettono di definire come alcuni eventi sono dipendenti dagli eventi passati e ciò che si può aspettare da un evento futuro. Quindi i messaggi vengono ispezionati ed analizzati e viene costruita una base di conoscenza sulla base di essi come parole e simboli.*

    - *Sender policy framework(SPF): risolve I problemi di sicurezza dell'SMTP in quanto chiunque può impersonare chiunque di impersonare qualsiasi indirizzo email. Questo meccanismo invece effettua un check su chi ha avuto il permesso di inviare la mail da un determinato dominio e lo blocca nel caso di dominio non autorizzato.*
    - *DKIM: Esso autentifica la mail in modo da prevenire lo spoofing. Infatti questo meccanismo permette di verificare il domnio di provenienza del messaggio in mariera tale da accertarsi sulla veridicità del mittente. Il DKIM permette di associare il proprio indirizzo con una firma digitale sulla quale viene verificata da una chiave pubblica. L'unico modo per comunicare è il DNS.*

- Che cos'è un open relay?
    - *Per tentare di camuffare l'header, gli spammer si affidano a un server terzo chiamato per l'appunto Relayer. Questo comunica tramite un protocollo SMTP e quindi non essendo previsto di autenticazione, può inviare qualsiasi messaggio senza alcun problema. Per impedire l'invio, è necessario far autenticatore il mittente oppure la disconnessione*
- Nel momento in cui tutti bloccano gli open relay, è possibile continuare ad effettuare mail spamming?
    - *Si, utilizzando un worm che innesca una botnet all'interno di queste macchine per esegue un enorme invio di messaggi connettendosi direttamente alla porta 25 degli host di destinazione.*
- Su quale presupposto si basa la probabilità per la rivelazione di spam? (Teorema di bayes)
    - *Filtri di contenuti come: filtro bayesano—E' un meccanismo basato su analisi probabilistica, che caratterizzano uno spam. Il concetto è che permette di definire alcuni eventi che caratterizzano uno spam. Essa così di permettere di costruire le cosiddette reti bayesane, che permettono di definire come alcuni eventi sono dipendenti dagli eventi passati e ciò che si può aspettare da un evento futuro. Quindi i messaggi vengono ispezionati ed analizzati e viene costruita una base di conoscenza sulla base di essi come parole e simboli.*
- Come funziona la tecnica SPF? (tecnica che viene utilizzata per evitare che un utente possa spammare prima che invia la mail)
    - *risolve I problemi di sicurezza dell'SMTP in quanto chiunque può impersonare chiunque di impersonare qualsiasi indirizzo email. Questo meccanismo invece effettua un check su chi ha avuto il permesso di inviare la mail da un determinato dominio e lo blocca nel caso di dominio non autorizzato.*
- Se fossi chiamato come consulente per risolvere un problema legato alla diffammazione di una mail, come farei per vedere se è autentico o meno?
    - *Esso autentifica la mail in modo da prevenire lo spoofing. Infatti questo meccanismo permette di verificare il dominio di provenienza del messaggio in maniera tale da accertarsi sulla veridicità del mittente. Il DKIM permette di associare il proprio indirizzo con una firma digitale sulla quale viene verificata da una chiave pubblica. L'unico modo per comunicare è il DNS.*

5)

- Anonimato per la mail
    - *Il protocollo SMTP è noto per essere insicuro. Tutte le funzioni di relay SMTP sono svolte da un daemon che aspetta le connessioni sulla porta 25 per inviare la posta in uscita e/o inn ingresso. Su questa fragilità, si basa il concetto di mail spoofing: ovvero falsificare l'email*

inserendo un falso mittente così da raggiungere il destinatario. Per anonimizzare la mail, viene utilizzata la rete freenet. Infatti, grazie all'uso di un meccanismo, chiamato remailing, è possibile anonimizzare gli header attraverso di essi. In sostanza questi remailer vanno a riscrivere gli header per non far individuare il mittente.

- Tipi di remailer
  - *Ci sono 4 tipi di remailer:*
    - *Tipo 0: "Penet": Meno sicuri, che ricevono posta opportunamente formattata e tolgono le informazioni relative al mittente.*
    - *Tipo 1: "CyberPunk": Vengono usati in catene di remailer di almeno 3 elementi. Per garantire che non venga intercettato, i messaggi vengono crittografati.*
    - *Tipo2: "Mixmaster": per evitare attacchi di tipo statistico, i pacchetti vengono frammentati e resi della stessa dimensione e successivamente inviati con delay casuali e mandati in coda.*
    - *Tipo3: "Mixminion": non utilizzano più il protocollo SMTP, ma utilizzano il protocollo SSL fra vari server attraverso una struttura di Reply Block. Le chiavi, vengono gestite automaticamente grazie alla rete P2P.*
- Concetto di Perfect Forward Secrecy
  - *Per garantire un buon grado di sicurezza nella rete TOR, viene utilizzato il meccanismo di forward secrecy, questa permette di utilizzare il TLS nelle comunicazioni tra i nodi, garantendo l'integrità dei dati scambiati implementando anche dei meccanismi di controllo della congestione e servizi proxy. Quindi tutte le connessioni, dal nodo di entrata fino a quello di uscita, sono cifrate.*
- Hiddenn services per la rete Tor
  - *Usando la rete TOR è possibile ospitare dei server in modo che la loro localizzazione si sconosciuta e quindi non conosce né l'indirizzo IP né il nome mappato sul DNS. Ai servizi nascoti, è possibile accedere solamente se .onion (quindi primo livello). Per rendere disponibile un hidden service, deve costruire il cosidetto "service descriptor" che serve a rendere disponibile il servizio al mondo attraverso l'utilizzo di una chiave privata e successivamente inviato ad un server pubblico di lookup (che la funzione di un DNS) usando sempre un circuito tor.*
- Concetto di Onion Routing
  - *E' una tecnica di traffico basato sulla struttura in logica overlay basato sulla creazione di circuiti virtuali cifrati. Il concetto base è che i pacchetti ed to end vengono incapsulati in logica telescopica in modo che ogni instradamento avviene attraversando un certo numero di nodi, dove ognuno di essi aggiunge o elimina un layer di cifratura specifico.*
- Proxy Anonimizzatore
  - *Utilizza un proxy a cascata tale che il pacchetto venga inviato ad un altro proxy casuale che conosce solamente il nodo precedente e il nodo successivo. In questo modo, l'ultimo livello di proxy ha la visione del contenuto*
- VPN per l'anonimato
  - *Le VPN non garantiscono l'anonimato, ma garantisce solamente una sicurezza in più in quanto va a rimappare solamente il nostro indirizzo IP. Quindi, dal punto di vista dell'identificazione tramite indirizzo siamo anonimi ma in realtà non lo siamo perché se c'è una compromissione all'interno della VPN, saremo completamente esposti. Inoltre, a differenza di TOR, non viene implementato nessuno offuscamento o altro.*

6)

- Resource starvation
    - *E' un tipo di attacco non volumetrico, basato sul generare flussi di dimensioni limitate e difficilmente percepibili da un sistema automatico di rilevamento. Questi flussi sono realizzati in modo da saturare la capacità delle risorse di un server in modo tale da sfruttare delle vulnerabilità di livello protocollare o generare pacchetti malformati.*
- Slowlolis , rudy
    - *Slow lolis: è un tipo di attacco low rate basato sul protocollo http dove si cerca di mantenere le connessioni aperte il più a lungo possibile, facendo in modoc he le connessioni saturano completamente le capacità della macchina per la gestione delle connessioni simultanee. Quindi ad ogni richiesta get, vengono aggiunti tag in modo tale da non terminare mai la richiesta*
    - Rudy: *tale attacco si basa sullo stesso criterio di slow loris con la differenza che viene effettuato una richiesta Post contenente un form. L'attacante quindi manda tale richiesta post al server in cui quest'ultimo si aspetta di ricevere un pacchetto ugualmente grande. Fatto questo, l'attacante manda un byte alla volta in modo da mantenere quanto più aperto possibile la connessione, tenendo attenzione del time out. Le contromisure da applicare in tale contesto è la definizione del timeout facendo si che il valore sia minore rispetto a quello definito all'attaccante oppure applicare i controlli sul form*.
    - LOIC: *Software utilizzato per generare grande quantità di richieste verso un sistema target, effettuando una iscrizione ad una botnet volontaria. Il tool effettua delle chiamate get verso un server con path randomizzati in modo tale da dare errore 404*
- Tear drop: *tale attacco sfrutta la sovrapposizione dei frammenti di un pacchetto IP mandato in modalità UDP tramite gli offset. Definendo un offset in modo tale che esso* sia *sovrapposta con un frammento già presente porta così in tilt la macchina*.
- Possibili attacchi in man in the middle sulla sessione tcp: *L'attacco si chiama TCP session hijackiing. L'attaccante prevede i sequence number dei pacchetti, rispettando ovviamente le sequenze corrette del RCP. L'attaccante quindi si inserisce e riesce ad effettuare un dirottamento della connessione in modo da poter sniffare tutti i dati presenti nel pacchetto. Per impedire ciò, sarebbe ottimale che i seguence number vengano generati in maniera randomica e non basati sul clock locale.*

7)

- Attacchi basati sul DNS e le possibili contromisure
    - I DNS sono importanrti perchè permettono di mappare i nomi agli indirizzi IP. Il DNS ha una debolezza, per renderlo più efficiente, vengono utilizzate delle cache locali e sono completamente stateless.
        - *Chache poisoning: L'attaccante inserisce all'interno della cache delle entry fraduolente facendo si che l'host vittima venga redirezionato all'host attaccante. In questo caso, l'attacco avviene in questo modo: manda una query al DNS locale dicendo di applicare la risoluzione del dominio IP di un sito web malevolo in modo. Da qui il sito web malevolo oltre a mandare delle informazioni relativa al proprio raggiungimento, inserisce delle informazioni aggiuntive quali: la redirezione all'host*

attaccante ogniqualvolta l'host vittima richiede una risoluzione di un determinato web. In questo modo, viene così inserita l'entry fraudolenta nel dns locale.
    - *Response spoofing: L'attaccante invia al DNS sia una query di risoluzione che una query di risposta. Così, l'attaccante invia tantissime query di risposta al DNS tale da sovrascrivere all'interno della cache locale del DNS l'host malevolo. Quindi quando un host richiede una risoluzione, esso viene redirizionato all'host attaccante.*
- DNS secure:
    - *E' una serie di specifiche che garantiscono sicurezza e affidabilità. In sostanza, permette di autenticare l'effettiva origine dei dati e che i dati siano effettivamente integri. Per confermare se la risposta sia valida, o meno, vene utilizzato il DNSSeq che introdice tre nuovi tipi di Resource Record…(prossima domanda)*
- Resource record
    - Ha 3 nuovi tipi di record che permettono di aumentare la sicurezza degli stessi grazie al resolver…..
        - *RRSIG: firma del resurce record con una chiave privata della zona*
        - *DNSKEY: chiave pubblica della zona, firmata dalla chiava privata della zona del padre per prevedere la logica di gerarchia delle chiavi*
        - *DS: fornisce la possibilità di trustare la prossima zona figlia del prossimo client DNS*
- Chi verifica che le risposte sono corrette? (resolver)
    - *Il resolver nel determinare l'autenticità di una risposta, controlla innanzitutto la firma presente nella risposta prendendo in riferimento la chiave pubblica del DNS finale (DNSKey).*
- Principali problemi del DNS (creazione della catena di attestazione): *A causa del fatto che i dati DNS sono esposti quindi non sottoposti ai meccanismi di cifratura, è possibile svolgere un'attività chiama monitoraggio pervasivo in cui l'attaccante intercetta e analizza i pacchetti catturati a livello DNS avente come conseguenza la costruzione di un fingerprinting dell'utente vittima.*
- Visibilità del traffico DNS (DNS over HTTPS, DNS over TLS)—DNS Embedded nel broswer
    - *Questo meccanismo mira a crittografare le query e le risposte del DNS tramite TLS. Questo, utilizzandop un handashake assicura che all'interno della sessione non ci siano problemi in quanto crittografata. Questo ovviamente porta a diverse problematiche, poiché per consentire la crittografia, viene effettuato un uso intensivo della memoria per i resolver che lavorano in logica ricorsiva*
    - *E' basato sul protocollo https, poiché esso si basa direttamente in risposte in JSON o formato standard DNS. Utilizzando direttamente questa architettura, c'è un notevole incremento delle prestazioni e la sicurezza è fornita direttamente dal protocollo HTTPS.*
    - *DNS embedded: integra all'interno del broswer le funzionalità dei DNS migliorando in modo significativo le prestazioni*
- Attacchi ai meccanismi di routing: *ci sono vari attacchi che possono essere effettuati nell'ambito del protocollo BGP con conseguenze disastrose come la rredirezione dei pacchetti verso una blach hole, iniezione dei netblock falsi rendendo inacessibile siti web, redirezione dei pacchetti verso un centro di intercettazione oppure un attacco DDoS verso un'AS vittima. Gli attacchi sono: as path padding in cui consiste nel rendere meno attraente un determinato percorso cossichè il protocllo BGP scelga un altro percorso, riduzione del percorso in cui consiste nel rendere più attraente un percorso con lo scopo di attiare il traffico in maniera fraudolenta , blocco degli annunci BGP, creazione di loop all'interno dell'AS.*
- Come funziona l'EGP: *viene utilizzato per mantenere tutto il traffico che transita tra i vari AS nella global Internet. Infatti qualsiasi cosa annunciata tramite BGP si propaga in tutto il mondo. E' importante poihcè un attacco al BGP può creare instabilità nel routing globale creando dei black hole*

8)

- Firewall di nuova e vecchia generazione
    - *Deve integrare ovviamente tutte le caratteristiche di un firewall tradizionale integrandole con le caratteristiche di intrusion detection. Deve integrarsi con sistemi di monitoraggio esterni come un NAC e con sistemi che siano in grado di monitorare il traffico ed individuare eventuali minacce. Inoltre, deve poter bloccare in tempo reale le minacce garantendo protezione in tutte le fasi d'attacco*
- Riconoscimento dei pacchetti
    - *Il deep packet inspection può essere applicato in ambo figure con la differenza che nei firewall di nuova generazione viene applicato fino a livello applicativo consentendo quindi di riconoscere che tipo di applicazione sta utilizzando una determinata persona. Mentre con i firewall di vecchia generazione viene applicato fino a livello trasporto consentendo solo di poter riconoscere i flussi di pacchetti.*
- Che cos'è il NAC
    - *Viene utilizzato per effettuare controllo degli accessi nel contesto di una rete. L'obiettivo è quello di controllare la sicurezza degli endpoint facendo in modo che sulla rete ci siano macchine che sono compatibili con la politica di sicurezza prestabilita, se così non fosse verrebbero messe in una situazione di quarantena.*
- Varie modalità (agent less….)
    - Esistono due modi per acquisire le informazioni riguardanti le macchine: Agent based o agent less.
        - *Agent based: raccolta dei dati fatta in maniera collaborativa, quindi che la macchina accede alla rete e installa un agente di controllo*
        - *Agent less: In questo caso, vengono utilizzate delle tecniche esterne per verificare da remoto le caratteristiche di sicurezza del dispositivo*
- Tre componenti del NAC
    - *I tre componenti del NAC sono*
        - *Access Requestors: sono le macchine finali che devono connettersi alla rete.*
        - *Policy Enforcement Point: comprende vari network enforcement point che garantiscono e controllano l'accesso alla rete e quisti possono essere per esempio switch, routers…..*
        - *Policy Decision Point: Ricevendo tutte le informazioni da tutti i componenti precedenti, esso li raccoglie e li compatta inviandoli al PEP che devide se ammerre o meno il dispositivo che deve accedere alla rete.*
- Application web security (caratteristiche lato client, web based…)
    - *Lato client abbiamo il web browser. La prima si intende che si connette a un web service attraverso un software il quale può installare malware, keyloggers…. Mentre le web based sono tutte le applicazioni che girano lato server che possono essere soggetti ad attacchi di tipo xss o sql injection*
- Certificati, policy….
    - *Le tecnologie utilizzare per proteggere i servizi web based sono orientati dall'utilizzo di certificati digitali, tecniche di crittografia simmetrica per rendere più sicuro possibile l'autenticazione del client.*

9)

- Quali possibili minacce che lato server possono esserci
    - *sono tutte le applicazioni che girano lato server che possono essere soggetti ad attacchi di tipo xss, sql injection e buffer overflow*
- Buffer overflow
    - *E' un tipo di attacco molto sofisticato poiché sfrutta una vulnerabilità di una specifica applicazione. Infatti si parla di questa tecnica quando una stringa in input è più grande del buffer che dovrà contenere. Questo comporta un superamento della soglia che finisce per sovrascrivere porzioni di memoria destinate ad altre applicazioni. Andando a riscrivere quelle porzioni, siccome siamo nello logica di uno stack, il return address non punterà più al codice originale, ma a quello malevolo. Ovviamente questo succede solamente quanto c'è allocazione dinamica della memoria.*
- Come si fa ad ovviare a questo problema
    - *Si utilizza un meccanismo che si chiama INSTRUCTION set Randomization. In sostanza attraverso una chiave di codifica, viene creato un unico insieme di istruzioni randomizzate dove le istruzioni saranno eseguite in un ambiente virtualizzato così che l'attaccante non può attaccare la macchina poiché non conosce la key*
- SQL injection
    - *E' un tecnica utilizzata per inserire codice malevolo all'interno delle query SQL con l'obiettivo di recuperare dati, eliminare o modificare il DB. Questa tecnica sfrutta query non strutturate correttamente, parametri non controllati, query senza vincoli oppure una gestione non corretta del tipo*
- Metodi per risolvere il sql injection
    - *Per risolvere questi problemi, basta utilizzare due tecniche: SQL parametrizzato oppure SQL randomization. Per il primo che utilizza delle query già parametrizzate utilizzando un statement specifico, mentre per il secondo…..(continua dopo)*
- Sql randomization
    - *E' la soluzione più efficace in quanto si introduce un proxy che effettua una de randomizzazione delle query e successivamente inviarle al DB in chiaro. Per randomizzare le istruzioni vengono utilizzate delle chiavi che per poterle utilizzare, l'ataccante dovrebbe o saperlo a priori oppure effettuare un attacco bruteforce.*
- Cross site scripting
    - E' una vulnerabilità chge affligge siti web malevoli che sono in esecuzione nel browser dell'utente. Esitono due tipi di tipologie:
        - *Reflected(non persistente): sono più comuni, e sono usati quando c'è una form e non c'è bisogno da parte del server di verificare la correttezza dei dati. Infatti, la url risultante in una pagina malevola contiene al suo interno uno script che viene automaticamente iniettato nel browser web cercando di rubare cookie o altre informazioni al proprio interno.*
        - *Persistente: E' lo scripting più devastante e si verifica quando i dati forniti dall'utente vengono salvati sul server, quindi visualizzati in modo permanente nelle pagine degli utenti durante la normale navigazione. In sostanza viene eseguito senza che l'utente se ne accorga quando su una qualsiasi pagina senza che l'utente venga indirizzata o clicca du qualche bottone.*
- Cos'è l'infrastruttura AAA? (Menzione del radius)
    - *E' un insieme di protocolli usati per la gestione degli accessi a una rete informatica. Gli accesso vengono divisi nelle fase di autenticazione, autorizzazione e accounting. Inoltre, tiene traccia dei comportamenti delle persone per stimare l'uso di risorse e le abitudini di un*

determinato utente, così da capire tempestivamente in caso di diversa "abitudine" di identificare eventuali problemi di sicurezza. Radius è un protocollo è utilizzato per dare l'accesso alla rete a determinati utenti previa autenticazione.

10)

- Che differenza c'è tra l'uso di un router con funzionalità di firewall e un firewall? (differenza sostanziale è che il firewall ha la conoscenza del flusso mentre il router no)
    - I filtraggi sui router possono mettere controlli degli accessi, ma sono completamente stateless. Infatti, a differenza di un firewall vero e proprio, esso non ha conoscenza del flusso e quindi non può sapere effettivamente se quel flusso è legittimo o meno. Infatti il firewall, grazie alle entry nella sua tabella, riesce a capire se quel flusso è sospetto o meno.

Che differenza c'è tra un firewall che lavora in maniera trasparente e un firewall che lavora in maniera non trasparente?

- Il firewall può lavorare in due modi, trasparente o meno.
    - Non trasparente: è un dispositivo di livello 3, il suo compito è segmentare reti diverse su base degli indirizzi IP, effettuando controlli di sicurezza applicando le opportune politiche. Quindi in sostanza ha diverse subnet per ogni interfaccia
    - Trasparente: significa che lavora solamente a livello 2 ed è completamente trasparente nella rete. Cioè quindi è perfettamente visibile nella rete e individuabile.In sostanza, ha la stessa subnet per ogni interfaccia che dispone.
- Il nat può essere implementato su un firewall trasparente?
    - No, poiché avendo sempre lo stessa subnet non può essere compatibile con esso. Infatti il NAT viene utilizzato per la traduzione e modifica degli indirizzi IP per poi essere instradati nella propria rete
- Che cos'è il firewalking? <u>(Non ho ben capito la domanda)</u>
    - E' un'attività di scansione molto sofisticata che permette di capire quali sono le misure di protezione che devono essere applicate a difesa della nostra struttura. Infatti esso è molto utile poiché grazie ad esso possono essere costruite delle ACL ad hoc, oppure risolvere altri problemi individuati. Quindi permette una visione generale del sistema di protezione
- Le scansioni sono individuabili da un firewall?
    - *Dipende dal tipo di scansione che viene utilizzata: per esempio per il TCP syn scan l'IDS se ne accorge, mentre per esempio per le NULL scan è impossibile. In sostanza sono individuabili tutte le scansioni che necessitano il three way handshaking, mentre chi utilizza scansioni tramite flag non sono individuabili.*
        - *TCP port scanning: in questo attacco viene aperta una connessione three way handshaking per verificare se la porta è aperta grazie ad un SYN iniziale inviato dall'attante. Dopodichè, la connessione viene immediatamente chiusa dopo aver ricevuto l'ACK viene inviato un FIN per chiudere la connessione.*
        - *Scan non indiduabili: Null scan, fin scan, xtras scan:*
            - *Fin scan: sono scansioni che invia pacchetti FIN direttamente a una porta, se la porta è aperta il FIN viene ignorato mentre se è chiusa viene riecevuto un RST.*

- ❖ *XmasTree: Prevede l'invio di un pacchetto con i bit FIN, UTG e push attivati alla porta target. Come risposta dovrebbe ricevere un RST con tutte le porte chiuse.*
- ❖ *Null scan: viene inviato un pacchetto con tutti i flag disattivati, il sistema obiettivo dovrebbe rispondere con un RST con norte chiuse.*

- Quali sono gli elementi architetturali che possiamo trovare in un firewalking?

11)

- Differenza di IDS e IPS e delle modalità di detection (i vari approcci come Misuse e Anomaly)
  - Differenza: Un IDS è un intrusion detection system, mentre un IPS è intrusion detection system. L'IPS permette di risolvere gli attacchi in maniera dinamica, mentre un IDS rileva gli attacchi in corso. Quindi, un IPS è una sorta di estensione di un IDS in quanto si basa su di esso per rilevare l'attacco per poi applicare determinate contromisure per risolverlo.
    - Nella logica Misuse: gli IDS e IPS devono lavorare sulla logica di una conoscenza pregressa attraverso dei pattern che si chiamano signature(firme). Quindi è basato sulla costruzione di database di conoscenza che viene utilizzato per fare matching sulla base della sua conoscenza. La decisione viene presa attraverso un grafo decisionale che determinano se c'è una intrusione o meno grazie a un database di pattern di attacchi noti.
      - ❖ Sistemi basati su specifiche: definiscono il comportamento del sitema, quindi se c'è un traffico insolito esso viene segnalato e identificato
      - ❖ Sul comportamento: Lavora grazie all'AI. Infatti riescono a costruire un tipo di nuovo attacco in grado di riconoscere le deviazioni di di attacchi rispetto all'originale.
    - Anomaly: Essendo i misuse dei pattern "statici" , quando c'è un attacco con il quale non c'è modo di riconoscerli, questi approcci si chiamano anomaly based. Infatti questo approccio si basa molto sul machine learning e ai vari modelli di addestramento. Prima però viene definito un comportamento di "normalità" del sistema e successivamente in base alle violazioni che vanno al di fuori del modello stesso.
- Quali sono le componenti architetturali del sistema IDS/IPS?
  - Hanno un motore di packet ispection, estraendo i dati tramite l'audit data processor che li estrae traendone le caratteristiche e li invia a un motore di detection che effettua il matching con i modelli e sulla base di questo vengono generati opportuni alarms e azioni.
- Che differenza c'è tra detection host based e detection network based?
  - Host based: sono strutturate in modo da effettuare monitorano e analisi a livello di sistema operativo per riconoscere delle specifiche delle attività ostili di istruzione generate da un malware sta infestato la macchina
  - Network Based: analizzano il traffico di rete per identificare intrusioni permettendo di analizzare una rete completa come ad esempio delle informazioni sul traffico.

- Quando lavoriamo in logica knowledge based, come funzionate le firme degli attacchi?
    - Si usano pattern di attacchi ben conosciuti, quindi si basa sulla conoscenza pregressa . Nella logica Misuse: gli IDS e IPS devono lavorare sulla logica di una conoscenza pregressa attraverso dei pattern che si chiamano signature(firme). Quindi è basato sulla costruzione di database di conoscenza che viene utilizzato per fare matching sulla base della sua conoscenza. La decisione viene presa attraverso un grafo decisionale che determinano se c'è una intrusione o meno grazie a un database di pattern di attacchi noti.
        - ❖ Sistemi basati su specifiche: definiscono il comportamento del sitema, quindi se c'è un traffico insolito esso viene segnalato e identificato
        - ❖ Sul comportamento: Lavora grazie all'AI. Infatti riescono a costruire un tipo di nuovo attacco in grado di riconoscere le deviazioni di di attacchi rispetto all'originale.

12)

- Cos'è la superficie di attacco, dominio di sicurezza e perimetro di sicurezza?
    - Superficie d'attacco: è la somma di diversi punti in cui un'entità non è autorizzata a svolgere attività
    - Dominio di sicurezza: è un insieme di risorse che devono essere gestite tramite una politica comune di gestione
    - Perimetro di sicurezza: è il confine protetto tra il lato esterno e il latro interno di un dominio di sicurezza
- Cosa differenzia un dominio di sicurezza a un altro dominio di sicurezza, a livello di visibilità? Come faccio a sapere che un dominio è più affidabile di un altro? (grado di livello di sicurezza)
    - Tramite il trust degree: infatti esso ne definisce le regole di visibilità rispetto agli altri. Quindi un grado di dominio con affidabilità maggiore può avere piena visibilità sulle sottostanti
- Come si implementano le ACL in modo da garantire la mutua visibilità? (mediante la clausola established)
    - Permette di poter scartare tutte le connessioni che non hanno completato il threeway handshaking
- Parlando di politiche di sicurezza, quali sono i possibili approcci per implementarli? (le due modalità di ACL, deny all o permit all)
    - Deny all, rifiuto tutto tranne le mie regole
    - Accetto tutto tranne le mie regole
- Quali servizi utilizzeremo se dovessimo monitorare la sicurezza di un'azienda? (comportamento baseline)
    - Sicuramente capire come il sistema si comporta normalmente (quindi approccio misuse), per poi capirne i punti deboli ed effettivamente applicare le regole necessarie per aumentare la sicurezza
- Che cos'è il flusso?
    - E' un insieme di pacchetti che sono caratterizzati da una stessa origine e la stessa porta di destinazione con magari lo stesso protocollo.
- Qual è il principio su cui si basa le mutue tecniche non supervisionate?
    - Non si ha nessun campione preclassificato, non c'è categorizzazione degli elementi da cui poter imparare. Il sistema deve essere in grado di costruire un dataset dividendo in cluster i dati, dalle quali creare delle sottocategorie per sviluppare eventuali anomalie.

- Come funziona il meccanismo che ti permette di classificare a livello protocollare il traffico? (tramite DPI)

13)

- Come funziona il nac?
    - *Viene utilizzato per effettuare controllo degli accessi nel contesto di una rete. L'obiettivo è quello di controllare la sicurezza degli endpoint facendo in modo che sulla rete ci siano macchine che sono compatibili con la politica di sicurezza prestabilita, se così non fosse verrebbero messe in una situazione di quarantena.*
- Asset inventor
    - Permette di classificare i dati in base un inventario, quindi per esempio sulla natura dati oppure sull'origine degli stessi
- SIEM (log management)
    - E' il sistema più sofisticato dei log management, permette di combinare diverse funzioni di informazioni ed eventi permettendo di capire se memorizzare i log di lunga data per permetterne un'analisi e reporting di tali dati successiva. Inoltre, ha la capacità di effettuare una correlazione di eventi che si sono susseguiti

14)

- Memcache amplification
    - *il Memcache amplification: si basa sul servizio di memcached che consente il caching distribuito open source utilizzando le porte TCP e UDP 11211. Il bot attaccante invia un messaggio all'host causando una risposta con un fattore elevatissimo avente come destinazione l'host vittima. (per bloccarlo: packet capture con protocllo UDP, porca 11211 e numero pacchetti >10)*
- Meccanismo di firewall, differenza di un router e firewall
    - Già fatta

- Firewall trasparente può applicare filtraggio su indirizzo IP? (si sui controlli sul livello 3)
    - Firewall non trasparente
- Cosa sono il dominio di sicurezza, il perimetro e la superfice d'attacco
    - Già fatto
- SIEM
    - Già fatta

15)

- Anonimizzazione contenuti (freenet)
    - E' una rete che eroga servizi in forma anonima a livello di contenuti. Quindi chi pubblica un determinato contenuto è anonimo. In questo modo c'è la resistenza ad attacchi volti a censurarli. Inoltre, essendo la pubblicazione anonima è sicura anche sotto l'aspetto legale.

Infatti, essendo completamente anonimo, il proprietario del nodo non può essere a conoscenza di ciò che viene pubblicato, assicurandolo. Inoltre, non è possibile eliminare un contenuto, neanche dall'autore. Ma è fatto tutto automaticamente dai vari nodi, se il contenuto non viene visualizzato dopo X tempo, esso viene eliminato.

- Compromettere l'anonimato (attaccando TOR)
    - In questo caso, la rete TOR ha dei punti deboli come il nodo in ingresso e il nodo di uscita. Quindi mettendo insieme delle correlazioni di traffico, è possibile capire il pattern di traffico e comprometterne l'anonimato. Infatti, esistono due tipi di attacchi di questo tipo: temporale e sulla dimensione dei pacchetti. Sul primo l'attaccante monitora il traffico sull'entry guard e sull'exit node per cercare di intercettare i pacchetti. Sul secondo invece prende in considerazione la dimensione dei pacchetti e il numero di pacchetti scambiati. In questo modo, è possibile correlare i due nodi.
    - Mixing di traffico, quindi cercare di cambiare l'andamento del flusso per diversificare la sorgente e la destinazione
- Cookies
- Bloccare tor per limitare l'utilizzo
    - L'unico modo per bloccarlo è mediante l'uso di bridge.
- Bridging nodes (non ho capito) <u>in tor || sono nodi usati per bypassare il blocco della rete tor by Lucio</u>
    - L'uso di questi bridge non è suffiente in quanto l'attaccante può effettuare un DPI per andare a classificare il traffico riconoscendo il pattern protocollare di tor

16)

- Nac (che cos'è…. Architettura…. Etc…..)
- Modalità raccolta dei dati(agent-based, scansioni sulla rete)
- Scansione della rete (cercando di non essere visibile)
- Scansione non percepita dal firewall (null scan)
- Attacchi stealth(slow loris, rudy, deeply nested xml)
- Buffer overflow

17)

- Controllo accessi
- Access list solo a livello 3? (no anche a lvl 2, per indirizzi IP o MAC address)
- Firewall trasparenti e non (NAT)
- Perfect forward secrecy
- Chiavi usata per il perfect forward secrecy (AES, scambio di chiavi tra nodi… etc).

18)

- Filtro antispam (Il filtro bayesiano)
    - Già fatto
- Tar Pitting (tarpits)

    - Si sfrutta questa caratteristica per rallentare l'invio di email quando si inviano email in modo non umano, quindi quando c'è un invio troppo veloce delle stesse
- grayListing
    - Quando un utente invia un messaggio a un determinato destinario ma esso non è disponibile, invia un messaggio a ritroso verso il mittente. Nel caso dello spammer, non esegue un altro invio in quanto esso deve inviare velocemente le email e quindi non ne effettuano un nuovo invio. Quando il server intermedio per la prima volta riceve un determinato messaggio, viene generata un tupla che contiene l'ip, il sender e il messaggio stesso inviando un messaggio verso il mittente. Se c'è un reinoltro del server, allora la tupla viene rimossa dalla lista. Tale meccanismo si basa sul fatto che gli spammer non eseguono mai un secondo invio.
- Come funziona l'anonimizzazione della mail (utilizzo remailer 0,1,2)
    - Fatto già
- Mail anonimizzata con la risposta (server di psudonimi, reply block)
    - Già fatto
- DKIM
    - Questa key viene utilizzata per permettere l'utilizzo di una chiave che autentica il messaggio in modo tale da accertare l'autenticità del mittente. La firma certifica che il messaggio inviato sia autentico e non modificato. Inoltre non è visibile all'utente in quanto vengono verificate dal provider.

IMPORTANTE!

DISCLAIMER

Il materiale contenuto nel drive è stato raccolto e richiesto tramite autorizzazione ai ragazzi frequentanti il corso di studi di Informatica dell'Università degli Studi di Salerno.

Gli appunti e gli esercizi nascono da un uso e consumo degli autori che li hanno creati e risistemati, per tanto non ci assumiamo la responsabilità di eventuali mancanze o difetti all'interno del materiale pubblicato.

Il materiale sarà modificato aggiungendo il logo dell'associazione, in tal caso questo possa recare problemi ad alcuni autori di materiale pubblicato, tale persona può contattarci in privato ed elimineremo o modificheremo il materiale in base alle sue preferenze.

Ringraziamo eventuali segnalazioni di errori così da poter modificare e fornire il miglior materiale possibile a supporto degli studenti.

Associazione CoScienze