Monitoraggio e Network Analisys

Created	@April 17, 2023 11:34 AM
Tags	

Domini, perimetro e superficie di attacco

Un **dominio di sicurezza** è un insieme di entità/risorse da gestione come una singola zona di amministrazione legata da una politica di sicurezza comune determinata da specifiche regole di security enforcement.

Un **perimetro di sicurezza** è il confine tra un dominio di sicurezza e l'esterno.

La **superficie di attacco** di un dominio è la somma dei vari punti ("vettori di attacco") in cui un entità non autorizzata (attaccante) può tentare di inserire o estrarre dati o svolgere qualsiasi attività non autorizzata o malevola

Dominio di sicurezza

Gerarchia

A ogni dominio di sicurezza è assegnato un grado di trust (affidabilità) che ne definisce le regole di visibilità rispetto agli altri.

Un dominio con un grado di trust maggiore può avere piena visibilità su quelli di grado inferiore mentre viceversa è bloccata, a meno di eccezioni.

Architettura di base

in genere in una rete abbiamo almeno tre domini:

- Outside: tutto il mondo esterno con grado di trust 0
- Inside: l'organizzazione da proteggere all'interno con grado di trust 100
- DMZ: insieme di macchine che espongono servizi all'esterno con grado di trust 0 < x < 100

Router, firewall e sonde

Un **router** è responsabile dell'inoltro del traffico tra la rete e Internet ed è il primo punto di sbarramento o demarcazione.

Un **firewall** è un componente attivo di difesa perimetrale e serve a controllare il traffico fra due o più segmenti di rete. Però bisogno tenere conto che tutte le operazioni di ispezione/controllo/filtraggio comportano dei costi in termini di performance.

Una **sonda** garantisce la visibilità e il monitoraggio del traffico.

Osservare il traffico, Sniffing

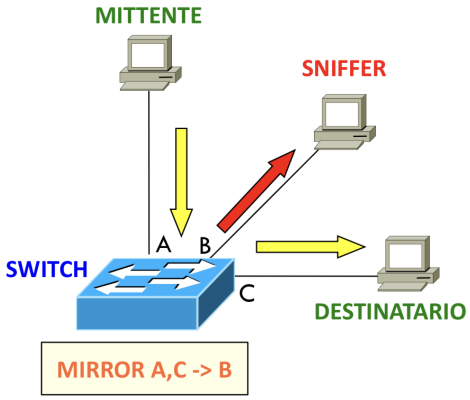
Uno sniffer è un'applicazione software che è in grado di monitorare i pacchetti a livello datalink. Queste operazioni di monitoraggio pacchetti ha un costo. Ad esempio possiamo usare il software chiamato Wireshark per ispezionare i pacchetti ma rispetto ad hardware dedicato questo software ha una capacità limitata. Infatti con strumenti semplici possiamo incorrere in perdite di pacchetti non analizzando a pieno il traffico

É possibile intercettare in chiaro le informazioni degli header di livello 2,3,4 dei pacchetti e anche dei protocolli a livello applicazione come **FTP e HTTP.**

Sniffing su reti switched

Su reti switched il traffico viene instradato in base al MAC address + la porta escludendo i dispositivi non interessati. Per questo uno sniffer è in grado di intercettare solo il traffico della macchina a cui è connesso e quello in broadcast.

Un applicazione comune è quella di impostare una porta in modalità mirroring dello switch a cui è connesso un dispositivo **sniffer** in modo da replicare tutto il traffico ricevuto nelle porte accuratamente scelte sulla porta collegata al dispositivo sniffer.



Esempio di codice

Si entra nello switch in modalità configurazione: conf t

#monitor session 1 source interface fa0/2 : imposto una porta come sorgente da sniffare

#monitor session 1 source interface fa0/1 - 3: imposto un range di porte sorgenti dai sniffare

#monitor session 1 destination interface fa0/4: imposto la porta di destinazione

Per analizzare il traffico usiamo tcpdump che via terminale ci consente di monitorare i pacchetti. Un esempio di codice per usare tcpdump è: *tcpdump -i eth0 port 21*

Sniffing senza port mirroring

In assenza di uno switch capace di fare port mirroring si può:

- Utilizzo di un ripetitore/hub, ma questa soluzione è molto vecchia e non si usa più (bande limitate);
- Utilizzare un TAP hardware (Traffic Access Port);
- Dirottamento del traffico attraverso attacchi (ARP Poisoning)

Traffic access Port

Consiste in una particolare sonda hardware dedicata. Questo dispositivo fa una copia del traffico su una tratta (molti di questi dispositivi non richiedono alimentazione elettrica) e permette di avere una grande visibilità del traffico di rete oltre a verificare se ci sono degli errori sulla tratta di interesse. Quando si fa il

tapping bisogna fare in modo che chi è intercettato non se ne deve accorgere; un tapping può essere rilevato mediante tecniche riflettometriche, utilizzate soprattutto nei cavi in fibra ottica.

ARP Poisoning

Il protocollo ARP (Address Resolution Protocol) si occupa di mappare i 32 bit di IPv4 in 48 bit di indirizzo MAC.

Ci sono 2 tipi di messaggi:

- ARP request (richiesta di risoluzione di un IP address)
- ARP reply (richiesta di risoluzione di un MAC address)

Questo attacco sfrutta il comportamento stateless del protocollo, ovvero che non ha uno stato e non si ricorda delle vecchie richieste ma solo dell'ultima. Quindi un attaccante deve fare varie richieste nel tempo perché i dati sono conservati in una cache e sono provviste di timeout.

Esempio pratico

Per intercettare una comunicazione bilaterale occorre spoofare in entrambi le direzioni quindi abbiamo bisogno di lanciare 2 volte il programma:

#./arpspoof -i eth0 -t 10.0.0.1 10.0.0.2

#./arpspoof -i eth0 -t 10.0.0.2 10.0.0.1

con il primo dica a 10.0.0.1 che sono 10.0.0.2 e con il secondo il contrario

---

Strumenti di monitoraggio

Per monitorare tutti i pacchetti che passano sulla rete si usano dei software per l'analisi real time.

Uno **sniffer** è uno strumento hardware o software che sfruttando il promiscuous mode cattura e consente l'analisi di tutti i pacchetti che transitano su un pezzo di rete.

Un esempio sono **tcpdump** che si usa tramite CLI o **Wireshark** che ha una GUI.

Tramite questi 2 software possiamo filtrare il traffico in base ai parametri che ci interessano andando a introdurre espressioni apposite che ci consentono di andare a monitorare quello che più ci interessa.

Ntop è uno strumento di monitoraggio della rete che fornisce una panoramica dettagliata del traffico di rete. Ntop può essere utilizzato per raccogliere informazioni sulla quantità di traffico, la banda utilizzata, i protocolli utilizzati e le applicazioni che generano traffico. Inoltre, Ntop può essere utilizzato per identificare le fonti e le destinazioni del traffico di rete, nonché per rilevare eventuali anomalie o attività sospette. Ntop è uno strumento utile per la sicurezza informatica in quanto consente di monitorare e analizzare il traffico di rete in tempo reale, individuando eventuali minacce alla sicurezza.

Sniffing su dispositivi di rete

La funzionalità di debugging può essere usata per vedere i pacchetti in transito, una buona pratica è di usare il debug delle ACL usando gli internal buffer e non la console. Tuttavia è necessario controllare il carico di della CPU che comportano queste operazioni.

```
R2(config)#access-list 155 permit icmp any any
R2(config)#do debug ip packet detail 155
IP packet debugging is on (detailed) for access list 155
R2(config)#
*Mar 1 01:17:16.039: IP: tableid=0, s=10.1.1.1 (FastEthernet0/0), d=2.2.2.2
(Loopback0), routed via RIB
*Mar 1 01:17:16.043: IP: s=10.1.1.1 (FastEthernet0/0), d=2.2.2.2, len 100, rcvd 4
*Mar 1 01:17:16.047: ICMP type=8, code=0
*Mar 1 01:17:16.047: IP: tableid=0, s=2.2.2.2 (local), d=10.1.1.1
(FastEthernet0/0), routed via FIB
*Mar 1 01:17:16.051: IP: s=2.2.2.2 (local), d=10.1.1.1 (FastEthernet0/0), len 100,
sending
*Mar 1 01:17:16.055: ICMP type=0, code=0
*Mar 1 01:17:16.095: IP: tableid=0, s=10.1.1.1 (FastEthernet0/0), d=2.2.2.2
(Loopback0), routed via RIB
```

Network monitoring

Le architetture per il network monitoring sono strutturate in accordo a un modello Manager-Agent.

Funziona cosi:

- La funzione di management interfaccia l’applicazione
- L’agente di management interfaccia l’oggetto da monitorare
- Un agente di monitoraggio può aggregare più funzioni associate a oggetti multipli

Polling e event reporting

In un modello Manager-Agent, il *polling* consiste in una richiesta periodica di informazioni da parte del manager all'agente. Il manager fa una richiesta all'agent per ottenere informazioni sullo stato dell'oggetto di cui l'agente è responsabile.

L'*event reporting* invece, è un metodo in cui l'agent notifica il manager di un evento o di un cambiamento di stato. In questo caso, l'agent invia una notifica al manager solo quando si verifica un evento o un cambiamento di stato, senza che il manager debba richiedere continuamente lo stato dell'oggetto.

Entrambi i metodi hanno vantaggi e svantaggi:

- Il polling può essere più efficiente in termini di utilizzo della larghezza di banda, ma richiede una maggiore elaborazione del manager per elaborare e analizzare le informazioni ricevute.
- L'event reporting può essere meno efficiente in termini di utilizzo della larghezza di banda, ma riduce il carico di elaborazione del manager, in quanto il manager riceve solo le notifiche degli eventi che si verificano.

Osservazione del traffico via SNMP

L'*Simple Network Management Protocol* (SNMP) è un protocollo di rete utilizzato per gestire e monitorare dispositivi di rete come router, switch e firewall. SNMP consente ai manager di rete di monitorare le prestazioni dei dispositivi di rete e di raccogliere informazioni sul traffico di rete.

SNMP utilizza un modello di dati gerarchico, con una struttura ad albero di oggetti gestiti.

L'osservazione del traffico di rete tramite SNMP può essere effettuata utilizzando una varietà di strumenti di monitoraggio di rete, come ad esempio Nagios, MRTG o Cacti. Questi strumenti utilizzano SNMP per accedere ai dati di gestione dei dispositivi di rete e raccogliere informazioni sul traffico di rete.

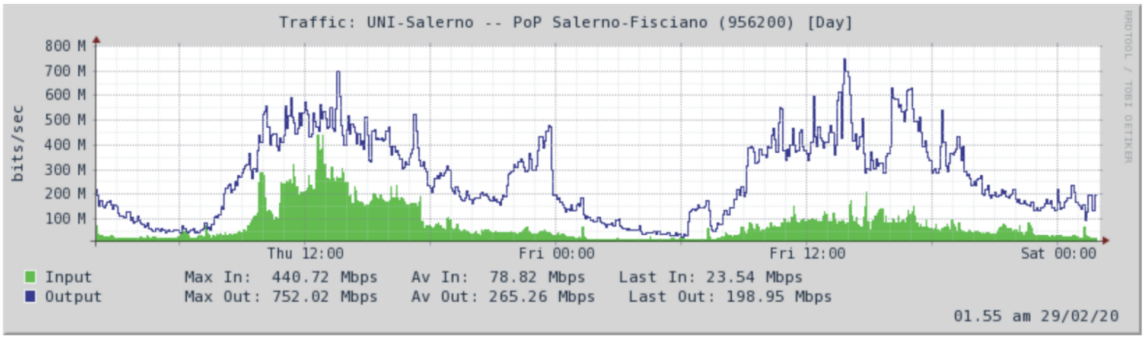
Per utilizzare SNMP per l'osservazione del traffico di rete, è necessario configurare i dispositivi di rete per supportare SNMP e abilitare il monitoraggio del traffico di rete. Questo può essere fatto utilizzando le impostazioni di configurazione del dispositivo di rete o utilizzando gli strumenti di gestione di rete.

Una volta configurato il dispositivo di rete per supportare SNMP e il monitoraggio del traffico di rete, è possibile utilizzare gli strumenti di monitoraggio di rete per visualizzare i dati di traffico di rete in tempo reale e analizzare i dati storici per identificare i modelli di traffico e le tendenze.

Le statistiche SNMP vengono collezionate in automatico e ogni 5 minuti vengono letti i contatori e salvati su un file di log (1 logfile x interfaccia).

Avremo quindi una rappresentazione grafica del Throughput e una Loadmap che ci premette di visualizzare il livello di carico degli uplink di tutti gli apparati di rete.

Link name	Use	BW	Side A	Side B	Target options
UNI-Salerno -- PoP Salerno-Fisciano	access	10,00 Gbps	UNI-Salerno 193.204.219.202	PoP Salerno-Fisciano rx1.sa.garr.net (MX480) irb.200 193.204.219.201	



Identificazione attacco

É facile riconoscere attacchi volumetrici identificando soglie anormali che sono molto diversi da un comportamento normale. Questa attività può essere facilmente automatizzata attraverso funzioni di monitoraggio tramite MRTG o CACTI che generano allarmi (mail, sms …) al superamento di specifiche soglie di traffico pre-impostate.

Però questo tipo di analisi va sempre legata al contesto tenendo conto anche di event straordinari o particolari che possono verificarsi in maniera lecita.

Osservazione traffico via Netflow

Il *Netflow* è un protocollo di rete sviluppato da Cisco che consente di raccogliere informazioni sul traffico di rete in tempo reale. Il protocollo Netflow viene utilizzato per raccogliere informazioni sul traffico di rete, come l'indirizzo IP di origine e di destinazione, il tipo di protocollo utilizzato e la quantità di dati trasmessi. Queste informazioni possono essere utilizzate per la gestione della rete, il monitoraggio delle prestazioni e la sicurezza della rete.

Il Netflow funziona in modo simile allo SNMP, ma invece di raccogliere informazioni sulla gestione dei dispositivi di rete, raccoglie informazioni sul traffico di rete. Il Netflow viene utilizzato principalmente per il monitoraggio della rete e l'identificazione di problemi di congestione della rete.

L'osservazione del traffico di rete tramite Netflow può essere effettuata utilizzando una varietà di strumenti di monitoraggio di rete, come ad esempio PRTG Network Monitor, SolarWinds NetFlow Traffic Analyzer o ManageEngine NetFlow Analyzer. Questi strumenti utilizzano il protocollo Netflow per accedere ai dati di traffico dei dispositivi di rete e raccogliere informazioni sul traffico di rete in tempo reale.

Per utilizzare il Netflow per l'osservazione del traffico di rete, è necessario configurare i dispositivi di rete per supportare il protocollo Netflow e abilitare il monitoraggio del traffico di rete tramite Netflow. Questo può essere fatto utilizzando le impostazioni di configurazione del dispositivo di rete o utilizzando gli strumenti di gestione di rete.

Una volta configurato il dispositivo di rete per supportare il protocollo Netflow e il monitoraggio del traffico di rete tramite Netflow, è possibile utilizzare gli strumenti di monitoraggio di rete per visualizzare i dati di traffico di rete in tempo reale e analizzare i dati storici per identificare i modelli di traffico e le tendenze.

Le informazioni raccolte dal Netflow possono essere utilizzate per identificare i dispositivi di rete che stanno generando il maggior quantitativo di traffico, i protocolli di rete che stanno generando il maggior quantitativo di traffico e le applicazioni di rete che stanno generando il maggior quantitativo di traffico.

L'utilizzo del Netflow può essere utile per l'identificazione di attacchi alla rete, come ad esempio gli attacchi DDoS (Distributed Denial of Service). Il Netflow può essere utilizzato per identificare gli indirizzi IP di origine degli attacchi e le porte utilizzate dagli attaccanti, consentendo ai gestori di rete di bloccare il traffico di rete malevolo e proteggere la rete.

In conclusione, l'utilizzo del protocollo Netflow per l'osservazione del traffico di rete può essere molto utile per la gestione della rete, il monitoraggio delle prestazioni e la sicurezza della rete.

(Da controllare)