SICUREZZA DI RETE

Tutti i protocolli ed i sistemi visti finora sono applicati a sistemi e reti complesse che svolgono molteplici funzioni ed hanno varie misure che a garantire la sicurezza.

~~SICUREZZA DI UNA RETE~~ LAN: INTRODUZIONE

Oltre ai dispositivi degli utenti (client) ci sono gli apparati di rete, dei servizi sempre attivi come server locali ed altro.

Bisogna sempre garantire le 3 caratteristiche di sicurezza: Confidenzialità, integrità e disponibilità. Un attaccante può avere obbiettivi variegati:

Rubare dati, Compromettere dei sistemi o modificare dei dati, Bloccare delle attività e limitare la disponibilità di alcuni servizi.

Gli attaccanti tentano di attaccare sia gli APPARATI TECNOLOGICI a livello tecnico ma anche le PERSONE sono un obbiettivo (phishing per esempio).

L'attacco quindi viene inviato su una SUPERFICIE D'ATTACCO (insieme dei punti a cui l'attaccante ha accesso per provare a penetrare nel sistema).

Soluzioni di sicurezza che coprono tutte superfici d'attacco vanno pensate rispetto ad una in base al contesto, per proteggere i punti che si presumono più vulnerabili per gli attaccanti che potrebbero voler attaccare.

Oltre al phishing generico l'attacco alle persone può essere portato avanti da PHISHING MIRATO, disegnato per funzionare specificatamente sulla vittima (avendo qualche informazione sulla vittima e sfruttando tecniche di ~~Social~~ INGEGNERIA SOCIALE). L'unica protezione è educare le persone sul rischio e sulle pratiche da adottare per difendersi.

PRINCIPI DI SICUREZZA

Ci sono 3 principi applicabili in ogni contesto

I) DEFENSE IN DEPTH: sfruttare la sicurezza per ogni e livelli, senza ammettere che un solo livello di sicurezza basti a proteggere l'intero sistema.

II) SEPARATION AND SEGREGATION: separare le risorse in compartimenti isolati tra loro, per limitare il raggio di attacco

III) LEAST PRIVILEGE PRINCIPLE: Concedere sempre il minimo indispensabile di privilegi per eseguire un compito, sia alle persone che alla tecnologia.

In generale gli attacchi alla tecnologia si basano su: Attacchi a vulnerabilità SW, Accessi non autorizzati, Attacchi alla rete

ATTACCHI DI RETE

Gli attacchi ad una rete possono avere due bersagli:

- COMUNICAZIONE: cercare di agire sui dati in movimento, quindi sul canale di comunicazione
- SERVIZI DI RETE: si sfrutta la presenza di servizi di rete per entrare nel sistema.

Non è sempre possibile proteggere integralmente un sistema solo sfruttando i protocolli sicuri.

Un attacco condotto su una rete di un servizio tenterà di sfruttare specifiche falle dell'obiettivo quindi è impossibile descrivere genericamente l'attacco. Prima di poter fare ciò però deve affrontare una fase di studio della rete (detta NETWORK RECONNAISSANCE).

In generale questa operazione preliminare si divide in 4 fasi:

I) Scoprire l'elenco dei servizi pubblicamente disponibili, i domini DNS associati all'obiettivo, ecc. Tutte info pubbliche.

II) Controllare l'effettiva presenza e raggiungibilità degli host IP disponibili (ADDRESS SWEEPING)

III) Controllare quali porte TCP siano aperte su quegli IP (PORT SCANNING)

IV) Identificare i servizi disponibili (basandosi sulle porte) SERVICE FINGERPRINTING.

Queste operazioni non si possono evitare utilizzando dei protocolli crittografati. Dobbiamo quindi agire sulla rete per prevenire la fuga delle informazioni descritte sopra.
Si vuole per esempio evitare che attaccanti provenienti da internet possa entrare all'interno della rete locale per ispezionare la rete. Anche contro gli attaccanti interni alla LAN vanno presi provvedimenti sfruttando la segmentazione e segregazione.
Esistono varie soluzioni per affrontare questo tema specifica per livello:

- LIV. 2: VLAN
- LIV 3/4: FIREWALL
- LIV 5/6/7: DEEP PACKET INSPECTION (DPI), FIREWALL DI LIVELLO APPLICATION.

Protezione di Livello 2

Presupponiamo che l'attaccante abbia accesso alla rete locale (probabilmente ha accesso fisico alla rete) ed attacca i protocolli relativi a ethernet. Non per forza ha accesso alla rete fisica, potrebbe aver compromesso un dispositivo di rete di livello 2.

Almeno che non sia strettamente necessario le LAN devono essere separate fra loro, sia per motivi di performance che per motivi di sicurezza. Se ogni area ha la propria LAN è più facile isolare potenziali attaccanti e limitare la quantità di risorse che possono essere violate (almeno a livello 2).

Il problema è che ogni LAN richiede un router. Per ovviare a ciò si sfruttano le VLAN che consentono di separare gruppi di host fra loro anche se connessi allo stesso switch.

Al posto di queste soluzioni si potrebbe utilizzare MACSec ma è troppo nuovo e costoso da sfruttare per essere largamente diffuso oggi.

ATTACCHI MITM A RETI LAN E POSSIBILI DIFESE

Le reti LAN moderne sono sempre organizzate a stella con centri stella rappresentati da SWITCHES.

Gli switches separano i DOMINI DI COLLISIONE poiché inoltra i messaggi UNICAST solo al destinatario voluto. Lo switch però inoltra a tutti i messaggi BROADCAST, quindi mantiene unico il DOMINIO DI BROADCAST, in particolare per il protocollo di discovery ARP. Questa è una limitazione intrinseca del protocollo ETH ed è una vulnerabilità.

Considerando di essere connessi ad 1 porta dello switch, un attaccante può fare diverse cose:

- ARP SPOOFING: Consente di attaccare un'altro host della rete
- PORT STEALING: attacco allo switch direttamente
- DHCP POISONING: Permette di attaccare il protocollo DHCP se nella rete è presente un server DHCP

ARP SPOOFING

L'attaccante vuole condizionare il protocollo ARP per alterare le tabelle contenute nello switch. In questo modo l'associazione IP - MAC viene alterata e di conseguenza lo switch inoltra i pacchetti verso gli host sbagliati. Per esempio l'attaccante potrebbe redirigere verso di se tutto il traffico diretto ad un altro host della rete. La prima fase consiste in un flood di ARP request per scovare tutti gli IP connessi alla rete lan (connessi allo switch).

Si procede poi a fare un PING per confermare che gli host sono raggiungibili. In fine invia una serie di ARP response per associare ogni IP al proprio MAC address, falsificando la tabella ARP dello switch. Lo switch quindi attacca funziona normalmente. Un tool apposito o un amministratore di rete può rilevare l'attacco perché anche gli host hanno la tabella ARP che sarà popolata di informazioni sbagliate.

Se gli host sono statici (server) si può popolare manualmente la tabella ARP per disattivare ARP su tali host, eliminando la base su cui si svolge l'attacco. A volte questo attacco provoca un DENIAL OF SERVICE perché a causa del traffico lo switch va in crash.

SEPARAZIONE RETE LIV. 2 : VLAN

Le VLAN consentono di separare il dominio di broadcast degli host connessi ad uno stesso switch, creando di fatto due reti di livello 2 distinte. I pacchetti fra host di livello 2 quindi devono passare tramite router (quindi liv. 3).

Sui router è possibile applicare regole di segregazione, ovvero limitare la capacità e le modalità di interazione fra reti diverse (per esempio tramite firewall).

SEGREGAZIONE LIV. 3 e 4: FIREWALL

Un firewall è un componente (SW o HW) della rete che permette di definire regole sulle interazioni consentite fra reti e fra host su reti diverse.

I firewall servono ad attuare la SEGREGAZIONE DELLE RETI.
I firewall vanno sempre configurati per funzionare in base al contesto della rete. È necessario che il firewall stesso sia fortemente sicuro perché potrebbe essere vittima di attacco ed inoltre deve essere ben POSIZIONATO CORRETTAMENTE nella rete per poter garantire una sicurezza efficace.

ACCESS CONTROL LIST (ACL): lista che definisce cosa può il traffico consentito e quello non consentito, basandosi su regole esplicite e implicite. Le regole implicite possono essere APPLY ALL / DENY ALL che è il trattamento di default, ovvero che non venga esplicitamente permesso/negato, applicato ad ogni pacchetto.
I firewall possono essere installati su dispositivi ad-hoc, su host o su router. Nel caso dei router il firewall agisce come segregazione del traffico su varie reti.

Un firewall installato su un router il dispositivo si può chiamare ~~in vari modi a seconda delle funzioni~~ SCREENING ROUTER.

PROXY FIREWALL: analizza molto approfondita di connessioni, pacchetti ecc. di un certo protocollo applicativo

STEALTH FIREWALL: analizza il traffico all'interno della rete e decide le regole di traffico senza da rendere evidente la presenza del ~~stesso~~ firewall stesso.

SCREENING ROUTER: implementa la segregazione e blocca il traffico non autorizzato dall'esterno. Effettua analisi più veloci e meno accurate.

Solitamente questi firewall si usano tutti insieme per il concetto di defense in depth.

Il proxy firewall oltre a filtrare ed analizzare i liv. 3 e 4 analizza anche il livello applicativo e pertanto deve anche eseguire l'applicazione stessa. Quindi stabiliscono loro stessi una connessione con i due capi della comunicazione per agire come mediatore.
Per poter analizzare il traffico cifrato (ad esempio TLS) è necessario che il proxy firewall agisca come MITM per aprire il traffico stabilendo una connessione con l'host ed un'altra col server.

BASTION HOST: estensione dell'architettura screening router. Prevede l'introduzione di un proxy firewall (detto bastion host) che deve analizzare tutto il traffico da/a la rete sicura (LAN) e la rete NON SICURA (tipicamente internet).

DE-MILITARIZED ZONE (DMZ): porzione della rete intermedia tra la rete sicura e quella non sicura. Tutti gli host della DMZ non hanno bisogno di passare dal bastion host.
Questa topologia non limita il traffico tra host interni.

SCREENED-SUBNET: ~~Nessuno~~ Gli host sono sulla rete fidata chiusa da uno screening router mentre i servizi di rete sono in una DMZ. Si aggiungono quindi screening router per regolare gli host tra loro