

Sicurezza delle reti & gli **Honeypots**



Relazione di Aniello Coppeto
aka
NeCoSi (necosi@autistici.org)

Data: 19 Maggio 2006
Versione: 0.1

Licenza: Gnu FDL (www.gnu.org/licenses/fdl.html#SEC1)

Prefazione

Prima di iniziare lo studio delle reti, faremo una breve introduzione teorica, attraverso le diverse tipologie di implementazione delle reti, i protocolli e concluderemo prendendo in considerazione l'uso degli Honeypot come strumento di approfondimento didattico per l'analisi delle tecniche di hacking.

Inoltre è doveroso ricordare un concetto fondamentale: "Per sicurezza si intende la riduzione del rischio".

E' inutile dunque illudersi di poter creare sistemi privi di vulnerabilità, è utile invece dividere le risorse tra: Prevenzione, Rilevazione, Reazione in modo da gestire in modo ottimale ipotetici attacchi.

Tipologie delle Reti

Rete a Stella

Al centro troviamo l' hub (o lo switch) e tutti gli host sono connessi fra loro attraverso questo hub. Nel caso in cui un cavo si guasti, solo un host verrebbe isolato. Per estendere questa rete è necessario solamente aggiungere un ulteriore hub e connettere a questo altri host.

Rete ad Anello

Tutti gli host sono connessi fra loro tramite un unico cavo circolare.

I segnali sono inviati attraverso ciascun computer che funge da ripetitore e ritrasmette il segnale potenziato al computer successivo.

Nelle reti Token Ring, a differenza di altre implementazioni per reti ad anello, un computer mal funzionante viene automaticamente escluso dall'anello consentendo agli altri di continuare a funzionare regolarmente in rete. In altri tipi di reti ad anello invece un computer che non funziona può provocare la caduta di tutta la rete.

Rete a Bus

Consiste di un singolo cavo (chiamato dorsale o segmento) che connette in modo lineare tutti i computer. I dati sono inviati a tutti i computer e dovrebbero essere accettati solo dal computer il cui indirizzo è contenuto nel segnale di origine.

Poiché un solo computer alla volta può inviare dati, maggiore è il numero di computer connessi alla rete, più saranno i computer in attesa di trasmettere dati, rallentando così le prestazioni dell'intera rete. I dati trasmessi da un computer, se non vengono interrotti, viaggiano da un capo all'altro del cavo, rimbalzano e tornano indietro impedendo ad altri computer di inviare segnali. A ciascuna estremità del cavo viene applicato quindi un componente chiamato terminatore che assorbe i dati liberi rendendo disponibile il cavo per l'invio di altri dati. Se un cavo viene tagliato o se uno dei capi viene scollegato, e quindi uno o più capi sono privi di terminatore, i dati rimbalzeranno interrompendo l'attività su tutta la rete, rendendola così inattiva.

Altri tipi di reti

Queste tre tipologie rappresentano le basi su cui poi si creano le reti più complesse, ed è il caso delle reti ad "Anello a Stella" e di "Bus a Stella".

Protocolli delle Reti

In generale, per comunicare, si usano delle regole (dette anche procedure o protocolli), e questo non vale solo nel campo informatico. Anche nel mondo reale, quando si incontra una persona e si vuol comunicare, esistono delle "regole" per una buona comunicazione/conversazione. Ad esempio se ci si conosce ci si saluta e poi si inizia a parlare mentre se non ci si conosce, prima ci si presenta (identificazione) e poi inizia la conversazione.

I protocolli di rete quindi, che descrivono il funzionamento per una corretta comunicazione tra host, vengono rappresentati da una pila protocollare e sono divisi in livelli:

Livello 1 – Fisico: Doppino, Fibra ottica, Cavo coassiale, Codifica Manchester, WiFi, ...

Livello 2 – Link: Ethernet, Lan Wireless 802.11, PPP, Token ring, ATM, ...

Livello 3 – Rete: IP (IPv4, IPv6,...)

Livello 4 – Trasporto: TCP, UDP, ...

Livello 5 – Applicazione: SMTP, Telnet, HTTP, FTP, NFS, ...

Problemi di sicurezza

I problemi di sicurezza si dividono in:

Autenticazione: AP (authentication protocol), Firma Digitale

Riservatezza: Crittografia simmetrica e/o asimmetrica

Integrità: Digest

Autenticazione

L'autenticazione può avvenire ad ogni livello della pila protocollare, ma analizzeremo rapidamente solo l'autenticazione a livello di rete (IPSec).

Riservatezza

La crittografia è uno strumento usato per "proteggere" i dati da osservatori non "autorizzati". Ci sono diverse tecniche per implementare i concetti di crittografia. Crittografia simmetrica e crittografia asimmetrica sono le tecniche maggiormente usate oggi, anche per alcune comunicazioni in internet. La fusione fra questi diversi tipi di crittografia oggi vengono largamente usati grazie alla loro stabilità e alla loro flessibilità. Sono basati su seri modelli matematici e oggi rappresentano la miglior soluzione al problema della riservatezza. Inoltre una tecnica innovativa è rappresentata dalla crittografia quantistica, nata e sviluppata da fisici/matematici/informatici soprattutto europei al fine di contrastare le intercettazioni maggiormente svolte dagli USA attraverso il sistema di spionaggio denominato Echelon. Questa tecnica si basa fondamentalmente sul concetto di quanto, concetto generalizzato e rappresentato come se fosse una particella descritta dalla meccanica quantistica. La crittografia quantistica è stata sviluppata per mettere a nudo il problema delle intercettazioni, essa infatti è in grado di determinare se un messaggio è stato intercettato attraverso lo studio della variazione del quanto.

Integrità

Per assicurarsi che il messaggio non sia "corrotto", cioè per verificare che non siano state apportate modifiche (volontarie o involontarie) ai dati, si usano degli algoritmi conosciuti come funzioni hash. Un digest rappresenta l' "impronta digitale" del messaggio.

Esistono diverse funzioni per calcolare il digest di un messaggio, ma l'algoritmo più usato e considerato maggiormente sicuro attualmente è SHA-1, Secure Hash Algorithm, che rappresenta lo standard federale usato negli USA.

Attacchi e contromisure

Gli attacchi possono avvenire in tutti gli strati della pila protocollare che abbiamo precedentemente illustrato, ma spesso viene considerato solamente lo strato applicativo.

Prima di ogni attacco viene effettuato un **Mapping**, cioè vengono raccolte il maggior numero di informazioni riguardo l' host considerato target. Per questo scopo vengono usati i *port scanner*, ma non è da sottovalutare l'uso dell'*ingegneria sociale* cioè l'arte del prendere informazioni facendo leva direttamente sulla superficialità delle persone (telefonate, fax, email,...).

Come abbiamo visto, in alcune tipologie di rete i dati passano su tutti gli host della rete, ma automaticamente il proprio host preleva le informazioni a lui destinate scartando gli altri dati. Possiamo però configurare, entrando in *modalità promiscua*, la nostra macchina per non scartare nessuna informazione: questa tecnica è chiamata **Packet sniffing** e per attuarla spesso si usano software classificati *sniffer*. Chiaramente sniffare dati crittografati è molto meno utile di sniffare dati in chiaro.

Essendo il livello di rete gestito dal Sistema Operativo, se noi avessimo i privilegi di root (o Administrator per gli ambienti Windows) potremmo costringere la nostra macchina a porre un indirizzo IP arbitrario nel campo Source Address di un datagram (particolare sezione contenuta in ogni messaggio mandato in rete). Questa tecnica è chiamata **IP Spoofing** e viene spesso arginata introducendo nella rete dei *router* specializzati che effettuano il *filtraggio in ingresso* [RFC 2827] e controllano se l' IP è valido in base al range di IP disponibili su quella particolare interfaccia di rete.

La struttura del protocollo di trasporto TCP (usato largamente in internet) è divisa in pacchetti di tipo SYN e ACK. Un pacchetto SYN dichiara di voler effettuare una connessione ed un pacchetto ACK dichiara che la connessione è stata accettata. Inviando ad un server molte richieste di connessione, quindi molti pacchetti di tipo SYN, ed usando IP diversi tra loro sfruttando l'IP Spoofing, metteremo in atto un attacco di tipo DoS (**Denial of Service**), conosciuto come **SYN flooding** che saturerà la memoria del server.

Molto usato tra gli attacchi Dos è anche lo **smurf**, che consiste nel mandare richieste a molti host utilizzando

L' IP della vittima, in modo che tutti gli host interrogati rispondano alla vittima con messaggi di tipo ICMP echo-replay saturandogli la connessione.

L'evoluzione degli attacchi Dos è rappresentata dai DDos (**Distributed Denial of Services**). Questa tipologia di attacchi consiste nell'uso, da parte dell'attaccante di una rete di macchine *zombie* (cioè macchine che svolgono attività comandate da remoto). In questo modo un attaccante ha a sua disposizione diversi host da cui poter lanciare diversi tipi di DoS rendendo quasi inutile la difesa da parte della vittima. Essendo difficile per un firewall capire quali richieste sono legittime e quali invece appartengono ad un utente malizioso, in attacchi di questo genere è spesso richiesto l'intervento umano per mettere in "quarantena" le macchine zombie.

IPSec

Queste poche tecniche di cui abbiamo parlato, sono attuabili a causa di problemi di sicurezza a partire dallo strato di rete fino allo strato di applicazione. Se riuscissimo a garantire una maggiore sicurezza allo strato di rete, questo si estenderebbe automaticamente (a causa della natura gerarchica della pila protocollare) a tutti gli strati successivi. Per questo motivo è stato progettato **IPSec** [RFC 2401 e RFC 2411] che rappresenta una suite di protocolli che dovrebbero garantire la sicurezza a livello di rete. In breve vi basta sapere che IPSec usa la crittografia per garantire la riservatezza dei dati e l'autenticazione a partire dal livello di rete, ma essendo di nuova generazione, IPSec non è supportato da tutti gli host, ed inoltre a sua volta è affetto da alcune vulnerabilità, difficili da sfruttare, ma già evidenziate da alcuni studi di ricerca.

WiFi

Abbiamo detto precedentemente che le vulnerabilità esistono a tutti i livelli: analizziamo ora una vulnerabilità a livello fisico, il WiFi (**IEEE 802.11**). In moltissimi casi, le reti wifi non terminano lì dove dovrebbero terminare, esse si estendono oltre gli appartamenti/edifici interessati che in molti casi non sono isolati. Questo comporta una vulnerabilità sul piano fisico dato che è possibile "agganciarsi" a quella rete con estrema semplicità, sfruttando un' antenna direzionale ad esempio puntata verso l'edificio stesso.

A questo scenario poco rassicurante poi, dobbiamo aggiungere che circa l' 85% delle reti wireless non utilizza il protocollo WEP (**Wired Equivalent Privacy**) che si occupa attraverso la crittografia di "isolare" la rete ad un livello protocollare superiore. Inoltre per il restante 15% che usa il WEP è importante ricordare che questo protocollo di sicurezza ha serie vulnerabilità e permette di essere compromesso nel giro di alcuni minuti (15-30 min.). Per questo motivo è stato sviluppato il protocollo WPA (**Wi-Fi Protected Access**), che stato creato proprio per risolvere i problemi di scarsa sicurezza del WEP. Ma pochissimi attualmente lo usano.

Dunque, munendosi di un pc portatile ed una periferica IEEE 802.11 (scheda wireless) si possono trovare in giro per le città moltissimi punti di accesso ad internet anonimi e gratuiti.

Honeypot

Potremmo continuare ancora per molto elencando vulnerabilità e contromisure, ma non credo sia questo il posto adatto per questo genere di lavoro, in internet si trova moltissima documentazione.

Il campo della sicurezza è un campo in continua evoluzione, ogni giorno si scoprono nuove vulnerabilità ed ogni giorno vengono proposte nuove soluzioni.

Esiste un solo modo per tener traccia in tempi brevissimi delle nuove ed effettive tecniche di hacking di cui però pochissimi ne parlano: gli Honeypot.

Gli utenti sono da sempre considerati prede di hacker e cracker, ma con gli Honeypot possiamo capovolgere questa regola diventando noi utenti cacciatori di hacker.

Un po' come se i pesci si munissero di "strumenti" per pescare gli uomini.

L' Honeypot è un'idea, e come tale può essere implementato a seconda di ciò voi lo stiate pensando. L'idea di base però è che esso venga attaccato e compromesso...proprio in questo risiede il suo valore intrinseco.

Chiaramente esistono delle soluzioni "preconfezionate", ma per coltivare questo aspetto vi rimando alla documentazione dei software che potete trovare facilmente tramite il vostro motore di ricerca preferito.

Esistono due tipologie di honeypot:quelli di **produzione** e quelli di **ricerca**.

Gli honeypot di produzione sono strumenti che rappresentano una "difesa" mentre gli honeypot di ricerca,sono raccoglitori di informazioni sulla comunità blackhat.

Gli honeypot di produzione difendono i sistemi informatici spesso aziendali. Il loro compito infatti è quello di

rallentare l'attacco ai sistemi importanti e sensibili dell'azienda. La loro implementazione resta comunque poco diversa dagli honeypot di ricerca.

Un'ulteriore differenza per classificare gli honeypot è il loro **grado di interazione**. Per grado di interazione intendiamo le azioni che permettiamo a priori di svolgere ad un attaccante. Maggiore sarà il livello di interazione, maggiori saranno le informazioni che possiamo ricavare, e proporzionalmente maggiore sarà anche il tempo di rallentamento dell'attaccante.

L'honeypot è dunque uno strumento di rete in attesa di essere attaccato. Tutto il **traffico** diretto verso di lui ha il solo fine di comprometterlo. Tutto il traffico generato da lui invece è la conferma che è stato compromesso!

Per capire meglio il vantaggio di un honeypot, potrebbe risultare utile sottolineare la differenza con i normali sistemi di controllo di intrusioni (**IDS**). A differenza degli Intrusion Detection System infatti, che possono essere sovraccaricati da finti allarmi, un honeypot raccoglie sempre con un'elevata determinazione gli attacchi effettivi.

Abbiamo affermato precedentemente che la sicurezza è divisa in 3 aspetti: Prevenzione, Rilevazione, Reazione.

Dal punto della **prevenzione** gli honeypot sono poco utili infatti la loro utilità sta proprio nell'essere attaccati.

Dal punto della **rilevazione** invece è molto utile. Come abbiamo detto, per rilevare un attacco spesso si usano sistemi IDS, ma questi sono affetti da *false negative* e *false positive* e per questo motivo consultare i log e risalire ad un attacco risulta difficile. L'honeypot essendo dedicato solamente agli attacchi, avrà log di dimensioni minori e quindi più utili per la rilevazione dell'attacco.

Dal punto di vista di **reazione**, che è strettamente legato alla rilevazione, l'honeypot è utile perché semplifica la ricostruzione dell'attacco proprio attraverso **log** più precisi e maggiormente descrittivi. Inoltre per reagire ad un attacco spesso c'è bisogno di **scollegare** la macchina dalla rete, per lavorare in locale, ma questa procedura sui sistemi di produzione non è praticabile. Avendo un honeypot a disposizione invece questa procedura può essere svolta senza ripercussioni sulla produzione. Questo concetto è fondamentale quando si lavora nell'ambito aziendale.

E' risaputo che per proteggersi da una minaccia, bisogna prima conoscerla. Cosa c'è quindi di più utile di un honeypot di ricerca?

The Honeynet Project (<http://project.honeynet.org>) è uno dei più grandi progetti che studia aspetti di sicurezza sfruttando honeypot. Questo progetto raccoglie ogni giorno solo 1-5 Mb di dati. Queste informazioni sono solitamente di grande valore, perché mostrano cosa fa un hacker una volta entrato nel sistema.

Honeypot visto da un Hacker

I primi honeypot hanno permesso lo studio delle pratiche della stragrande maggioranza degli hacker perché questi ignoravano la loro esistenza. Ma con la nascita di questi strumenti, gli hacker hanno iniziato a chiedersi come è possibile sapere se il sistema target è o meno un honeypot.

Studiando ed analizzando questo problema sono emersi i seguenti punti che potrebbero insospettire un hacker:

1. il traffico in ingresso ed in uscita su un server target è praticamente assente
2. l'area di memoria in cui è in esecuzione il sistema operativo non appartiene ad un range di indirizzi di memoria riservati al **Kernel Space**, ma si trova in **User Space**
3. i processi ed i log residenti sulla macchina sono scarni e poco reali

Aspetti legali

Parlando di honeypot ci si imbatte in spesso in due aspetti legali: **intrappolamento e privacy**. Vedremo brevemente questi due argomenti. Per prima cosa vediamo la definizione legale di intrappolamento:

Una persona è 'intrappolata' quando è indotta o persuasa da chi rappresenta la legge o da un suo agente a commettere un crimine non premeditato.

Essendo noi dei privati, non si conforma un illecito.

Nel caso del diritto di privacy, questo non è attuabile nel caso di computer rubati o macchine violate. Per questo motivo, anche se l'hacker dal nostro pc compromesso effettua senza espresse autorizzazioni connessioni ad esempio IRC per comunicare, le sue conversazioni non possono essere considerate protette dalla privacy in quanto è lui stesso ad aver violato la nostra "proprietà privata" ponendosi quindi contro la

legge che protegge oggetti privati e nel caso di computer, anche la loro privacy.

Riferimenti

[Sicurezza in informatica] di C. Pfleeger e S. Pfleeger

[Internet e Reti di Calcolatori] di Kurose Ross

[Honeypots] di Lance Spitzner

Indice generale

Prefazione.....	2
Tipologie delle Reti.....	2
Protocolli delle Reti.....	2
Problemi di sicurezza.....	3
Attacchi e contromisure.....	3
IPSec.....	4
WiFi.....	4
Honeypot.....	4
Honeypot visto da un Hacker.....	5
Aspetti legali.....	5
Riferimenti.....	6