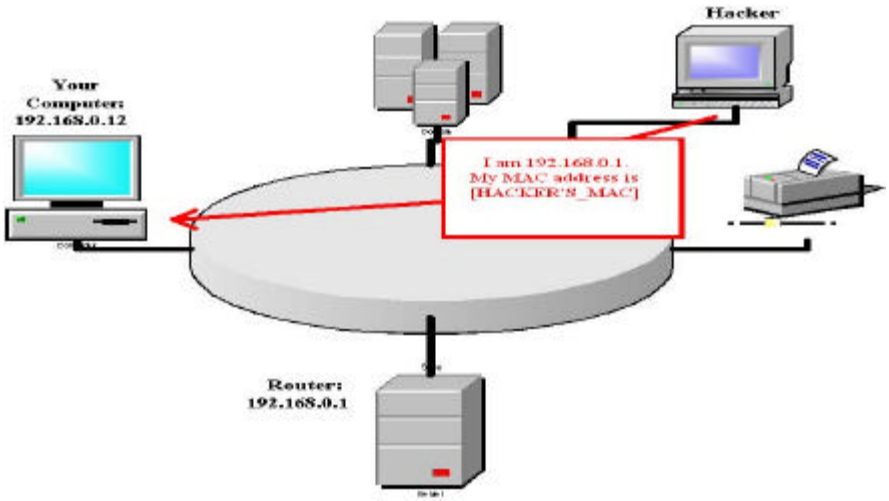
L'attacco del tipo "Man in the middle". (A cura del Dottor Antonio Guzzo – Responsabile CED – Sistemi Informativi del Comune di Praia a Mare)

La tipologia di attacco che va sotto il nome di man-in-the-middle consiste nel dirottare il traffico generato durante la comunicazione tra due host verso un terzo host (attaccante) il quale fingera' di essere l'end-point legittimo della comunicazione. Il tipico attacco man in the middle è cosi strutturato:vi è la vittima, il cattivo ed il server dhcp. La vittima fa una richiesta di IP address, a chi risponde prima gli viene assegnato un indirizzo IP e un gateway che corrisponde ad una certa interfaccia (gli diamo dei parametri nostri). Da questo punto in poi tutte le comunicazioni della vittima passano qui, io me le leggo e per non farmi accorgere di nulla le mando a chi le devo mandare, ricevo la risposta e leggo anche la risposta. Questa tipologia di attacco si chiama MAN IN THE MIDDLE e si applica a diversi contesti ed ha come caratteristica l'avere qualcosa in mezzo tenendo conto sempre che ci troviamo sempre sul layer 2 e layer 3. Qual è può essere l'obiettivo dell'attaccante? Rubare le credenziali oppure memorizzare tutto il traffico che un utente fa con un altro utente. (il cosiddetto DHCP spoofing) Adesso ritorniamo al caso precedente, la vittima fa la richiesta di ottenere l'indirizzo IP e io che sono il nemico gli rispondo per primo e gli do dei parametri miei corrispondenti ad un' interfaccia che sta sul mio portatile, da questo momento in poi l'host vittima è configurato in modo tale che tutte le sue comunicazioni passano da me che faccio da gateway, le leggo e le inoltro al vero destinatario, questo risponde e io leggo anche le risposte che poi inoltro alla vittima, in tal modo ho intercettato tutta la comunicazione e le vittime non si sono accorte di nulla. Essendo l'attaccante fisicamente in mezzo alla comunicazione delle due (o piu') vittime, riceverà pacchetti da e verso le stesse. Si dovrà preoccupare di inoltrare i pacchetti che riceve verso la corretta destinazione in modo tale che risulti trasparente ai due end-point della comunicazione. Si veda nello specifico la seguente figura:



A seconda della capacità di riuscire a monitorare solo uno o entrambi i versi della connessione l'attacco verrà chiamato man in the middle halfduplex o man in the middle full duplex. A seconda dello scenario in cui ci si trova ad operare l'attacco man in the middle assume forme diverse:

RETE LOCALE:

1) ARP poisoning; 2) DNS spoofing; 3) STP mangling.

1- ARP poisoning

Per raggiungere una destinazione all''esterno della LAN un host deve conoscere l''IP del gateway. L'host manda una ARP request per IP del gateway. Il protocollo ARP (Address Resolution

Protocol) si preoccupa di mappare i 32 bit di indirizzo IP (versione 4) in 48 bit di indirizzo ethernet. Esso genera due tipi principali di messaggi:

1) ARP request (richiesta di risoluzione indirizzo);
2) ARP reply (risposta contenente un indirizzo ethernet).

Le risposte sono memorizzate nella ARP CACHE, in modo da limitare il traffico arp sulla rete. Questa tipologia di attacco presenta alcuni problemi come il fatto che il protocollo è stateless mentre le ARP reply sono memorizzate in cache anche se non erano state sollecitate (incrementa prestazioni ma penalizza la sicurezza). Inoltre esso sfrutta il comportamento stateless del protocollo. Se l'attaccante invia una ARP reply (spoofata) verso un host, questo la memorizzerà nella propria arp cache. Le entries della cache sono provviste di timeout, quindi l'attaccante deve periodicamente "rinfrescarla". Un'entry non e' aggiornata se non era già presente nella cache. L'arp poisoning è aggirabile tramite un ICMP spoofato. E' molto utile per sniffare su reti connesse tramite switch che opera a livello 2 ed e' ignaro dei cambiamenti delle associazioni nelle arp cache degli host vittime. L'arp poisoning lascia delle tracce infatti le ARP cache delle vittime contengono il mac address dell'attaccante per cui se lo switch non e' provvisto di port-security o se si e' su HUB, l'attaccante può spoofare il suo mac address.

CONTROMISURE

Per evitare un attacco man in the middle di tipo arp poisoning è possibile effettuare le seguenti azioni:

1) un passive monitoring (mediante un tool arpwatch);
2) un active monitoring (mediante un tool ettercap);
3) un IDS (Intrusion Detection System) che rilevano ma non evitano;
4) ARP entries statiche;
5) un Secure-ARP (in development)

2 DNS spoofing

Il Domain Name System si occupa di trasformare i nomi simbolici degli host in indirizzi IP utilizzabili dal kernel. Il protocollo in realtà è molto più complesso, ma l'obiettivo è quello della trattazione delle funzionalità che ci servono per l'attacco. L'unico campo del pacchetto UDP (porta 53) che ci interessa e' l'ID per cui risulta necessario intercettare le richieste e memorizzare il campo ID. Successivamente si passa a forgiare una falsa risposta con il giusto ID e si spedisce al client che ha effettuato la richiesta. Infine si passa ad intercettare eventuali reverse query (PTR). In questo caso l'attaccante può fungere da proxy per il server e rispondere in modo corretto a tutti i servizi che il client si aspetta di trovare sul server. Il DNS spoofing lascia delle tracce infatti usando un risolutore di indirizzi diverso, ci si può accorgere della differenza di risposte. L'indirizzo IP dell'attaccante è presente all'interno delle risposte DNS.

CONTROMISURE

Per evitare un attacco man in the middle di tipo dns spoofing è possibile effettuare le seguenti azioni:

1) individuare risposte multiple (IDS);
2) usare lmhost o host file per risoluzioni statiche;
3) DNSSEC (questa è una risoluzione criptata).

3 STP mangling

Non è un vero e proprio attacco man in the middle e permette solo di ricevere traffico "unmanaged". Si forgiano BPDU con priorità molto alta (fingendoci per la nuova root). Gli switch ricostruiranno l'albero per adattarsi alla nostra presenza e cercheranno di saturare le tabelle dello switch. A tale proposito interviene il protocollo di spanning tree (802.1d) che è un protocollo di layer 2 appositamente progettato per evitare "loop" di pacchetti dove siano presenti percorsi ridondati. I pacchetti con MAC sorgente non presente nelle tabelle dello switch, sono forwardati su tutte le porte. Questo potrebbe portare a loop di forwarding. Per evitare loop nella topologia della rete, gli switch si costruiscono un albero di copertura (spanning tree) attraverso lo scambio di BPDU (bridge protocol data unit). Si viene a generare l'elezione di un "root switch". Per ogni

switch si designano le porte attraverso le quali si raggiunge la root e quelle verso i suoi discendenti dell'albero (designated port). Ogni pacchetto contiene una priorità che sarà utilizzata per l'elezione della root. La priorità e' rappresentata da un numero formato da 2 byte con in aggiunta il mac address dello switch (minore e' questo numero maggiore e' la priorita'). Le BPDU sono continuamente scambiate per rilevare cambiamenti nella rete. Questa tipologia di attacco lascia come traccia il Mac address dell'attaccante che e' presente nello stato dello switch.

CONTROMISURE

Per evitare un attacco man in the middle di tipo stp mangling è possibile effettuare le seguenti azioni:

1) Disabilitare STP sulle VLAN prive di loop (sconsigliato da CISCO);
2) Root Guard (se l'apparato lo supporta) impedisce che determinate porte diventino "root port", oppure disabilitare l'STP su queste porte;
3) Settare le porte connesse a workstations come "portfast", e attivare BPDU Guard su queste porte (se l'apparato lo supporta). Il portfast da solo NON e' sufficiente.

DA RETE LOCALE A REMOTO (attraverso un gateway):
1) ARP poisoning; 2) DNS spoofing; 3) DHCP spoofing; 4) ICMP redirection; 5) IRDP spoofing; 6) route mangling.

1 ARP poisoning

E' un attacco simile all'attacco locale. Il gateway è un host locale, quindi può essere poisonato come qualsiasi altro host. In presenza di "proxy arp" gli host remoti sono considerati locali. Per raggiungere una destinazione all'esterno della LAN un host deve conoscere l'IP del gateway. L'host manda una ARP request per l'IP del gateway.

CONTROMISURE

Per evitare un attacco man in the middle di tipo arp poisoning è possibile effettuare un entry statica del gateway su tutti gli host.

2 DNS spoofing;

Il DNS spoofing si verifica nel momento in cui intercettando una richiesta (broadcast) dhcp è possibile rispondere prima del vero server. In questo modo possiamo modificare i parametri di Default gateway e DNS Default gateway assegnando l'indirizzo IP dell'attaccante come default gateway per cui tutto il traffico verso l'esterno della lan passerà da esso. Le richieste saranno per host non locali, verso DNS non locali. La tecnica è identica a quella utilizzata per gli host locali. Consente infine di abilitare il flag "autoritative" per evitare richieste iterative.

Contromisure

Per evitare un attacco man in the middle di tipo dns spoofing è possibile effettuare le seguenti azioni:

1) individuare risposte multiple (IDS);
2) usare lmhost o host file per risoluzioni statiche;
3) DNSSEC (risoluzione criptata)

3 DHCP spoofing

Con il DNS spoofing assegnando l'indirizzo IP dell'attaccante come DNS, tutte le richieste di risoluzione dei nomi verranno fatte a lui e sarà quindi in grado di portare un attacco simile a quello visto in precedenza (DNS spoofing). Non e' necessario un tool apposito ma basterà configurare la macchina attaccante come DHCP server, installando ad esempio dhcpd. Questa tipologia di attacco lascia come traccia l'indirizzo IP dell'attaccante nelle configurazioni del client.

CONTROMISURE

Per evitare un attacco man in the middle di tipo DHCP spoofing la migliore contromisura è l'attenzione dell'utente che si vedrà probabilmente arrivare più di una risposta dhcp e potrà controllare "manualmente" alla ricerca di strane o inaspettate configurazioni assegnate.

4 ICMP redirection

L'ICMP (Internet Control Message Protocol) è un protocollo di servizio di livello 3 che si occupa ti trasmettere informazioni relative a malfunzionamenti, variazioni e prestazioni di una (o diverse) reti di calcolatori. I suoi messaggi sono ben definiti e numerati (8 bit) vengono chiamati "comandi ICMP" Il più famoso dei comandi di ICMP, è il numero 0/8, ECHO, solitamente noto come "PING". Tra gli altri comandi disponibile, uno in particolare attira la nostra attenzione: ICMP Redirect . Serve a consentire ad un router la segnalazione di una via piu breve verso il destinatario di un pacchetto in modo che l'host lo invii tramite la strada piu breve, migliorando le performance della rete. Esaminiamo solo il comando REDIRECT del protocollo ICMP. Il comando redirect serve ad avvisare un host che esiste una rotta più breve per la destinazione richiesta e questa rotta passa per il gateway indicato nel pacchetto ICMP. Quindi risulta necessario forgiare un ICMP redirect spoofando la sorgente dello stesso come se fossimo il gateway originale e con destinazione della redirezione l'host attaccante. E' necessario sniffare il pacchetto originario poichè nel REDIRECT ne devono essere inclusi 64 bit più l'header IP (non sempre necessario, a seconda del sistema operativo). I pacchetti di tipo REDIRECT vengono presi in considerazione dagli host a seconda del loro sistema operativo: Windows 9x accetta i REDIRECT di default e aggiunge un'entry (di tipo host) nelle sue tabelle di routing. Linux accetta di default i REDIRECT in alcune distribuzioni. Le rotte aggiunte sono comunque temporanee

Questa tipologia di attacco lascia come traccia l'indirizzo IP dell'attaccante che è presente nelle rotte dell'host ed è possibile spoofarlo e far comunque arrivare a lui i pacchetti rispondendo alle ARP request per l'indirizzo.

CONTROMISURE

Per evitare un attacco man in the middle di tipo ICMP redirection è possibile disabilitare i REDIRECT ma così facendo ci potrebbero essere dei cali di prestazioni nella rete (i pacchetti fanno più HOP). In una rete con un gateway solo è possibile ignorare le "ICMP Redirect" senza incorrere in un calo di prestazioni.

5 IRDP Spoofing

Questo tipo di attacco consente di forgiare degli "advertisment" annunciandoci come router e settando i campi "livello di preferenza" e "lifetime" al massimo valore consentito. Nei sistemi operativi Windows a seconda della versione utilizza l'IRDP (ad esempio in Windows 9x accetta IRDP) mentre Windows NT usa IRDP al boot, Windows 2000 ignora IRDP e Linux ignora IRDP. Si può rendere l'attacco più efficace forgiando degli ICMP Host Unreachable impersonando l'attuale router di default. IRDP (ICMP Router Discovery Protocol) è un protocollo basato su ICMP, utilizzato per l'assegnazione automatica agli host di un gateway (router). Ci sono due tipi di messaggi previsti dal protocollo:"Router Advertisements" e "Router Solicitations". Periodicamente, ogni router manda in multicast degli advertisment per annunciare il suo indirizzo IP. Ogni advertisment contiene un "livello di preferenza" e un campo "lifetime". Nel caso un host riceva più advertisment da diverse sorgenti, si dovrebbe scegliere quello con il livello più elevato. Il "lifetime" sta ad indicare il tempo per cui l'host deve conservare quella rotta. Questa tipologia di attacco lascia come traccia l'indirizzo IP dell'attaccante che e' presente nelle rotte dell'host ed e' possibile spoofarlo e far comunque arrivare a noi i pacchetti rispondendo alle ARP request per l'indirizzo spoofato.

Contromisure

Per evitare un attacco man in the middle di tipo IRDP spoofing è possibile disabilitare IRDP sugli hosts se il sistema operativo lo permette.

6– ROUTE mangling

Nel caso in cui un router ha più rotte possibili per una stessa destinazione, sceglie quella col "peso" maggiore. Il peso viene determinato in base a vari fattori come le metriche proposte dai vari protocolli di routing, e il tipo di protocollo stesso che ha proposto la rotta. Più il protocollo è "fidato", maggiore sarà il peso delle rotte che propone. Le rotte statiche hanno generalmente un "grosso" peso. Nel caso in cui un router ha più rotte possibili per una stessa destinazione, sceglie quella col "peso" maggiore. Il peso viene determinato in base a vari fattori come le metriche proposte dai vari protocolli di routing, e il tipo di protocollo stesso che ha proposto la rotta. Più il protocollo e' "fidato", maggiore sarà il peso delle rotte che propone. Le rotte statiche hanno generalmente un "grosso" peso. Forgiare dei pacchetti per gateway annunciandoci come router con un'ottima metrica per un determinato host (o classe o subnet). Specificare una netmask grande per "battere" rotte di peso maggiore. Quando l'host manderà dei pacchetti per l'host per cui l'attaccante si e' annunciato come rotta preferenziale, questi arriveranno a gateway. Gateway sarà convinto che il modo più veloce per raggiungere quell'host e' attraverso l'attaccante. Gateway manderà ad host degli ICMP redirect dicendogli di usare l'attaccante come gateway per i pacchetti successivi. Il problema a questo punto e' trovare un modo per far arrivare i pacchetti al legittimo destinatario. Gateway, infatti, e' convinto di poter raggiungere l'host attraverso l'attaccante. Questa tipologia di attacco lascia come traccia l'indirizzo IP dell'attaccante nelle tabelle del router che sono comunque temporanee. E' possibile spoofarlo come nei casi precedenti.

Contromisure

Per evitare un attacco man in the middle di tipo ROUTE mangling è possibile effettuare le seguenti azioni:

1) Disabilitare i protocolli di routing dinamico che sono inutili in uno scenario di questo tipo;
2) Mettere delle ACL esplicite sull'interfaccia interna del router che blocchino gli "update" indesiderati;
3) Abilitare l'autenticazione MD5 nei protocolli che la supportano;

REMOTO:
1) DNS poisoning; 2) traffic tunnelling; 3) route mangling

1 – DNS poisoning

Quando il DNS riceve una richiesta ci possono essere 3 possibilità. Il DNS è "autoritativo" per il dominio a cui il nome richiesto appartiene. (risposta autoritativa). Il DNS non e' "autoritativo" per il dominio richiesto ma ha nella cache la coppia <nome simbolico, indirizzo IP> in seguito ad una precedente richiesta (la cosiddetta risposta non autoritativa). Si verificano in questo caso tre tipologie di attacco:

ATTACCO DEL PRIMO TIPO

L'attacco ha come fine quello di mettere nella cache del DNS una coppia <indirizzo IP, nome simbolico>. Successivamente si effettua una richiesta al DNS vittima. Si spoofa la risposta che dovrebbe arrivare dal DNS autoritativo (i pacchetti sono di tipo UDP). Infine nella risposta forgiata dobbiamo inserire l'ID corretto della transazione iniziata dal DNS vittima (brute force, semi-blind guessing)

ATTACCO DEL SECONDO TIPO

Sfrutta la "feature" del dynamic update di alcuni DNS. Infatti inviando richieste di tipo "update" è possibile aggiungere o eliminare alcune entries per cui il DNS e' autoritativo

ATTACCO DEL TERZO TIPO

Abusare del sistema di assegnazione dei domini (ad esempio richiedendo uno spostamento di dominio a Network Solutions Inc.).

Questa tipologia di attacco lascia delle tracce. Come nel caso del DNS spoofing, gli host manderanno tutti i pacchetti della connessione verso l'indirizzo IP della macchina attaccante. Il DNS conserverà traccia di tale IP per tutto il tempo di latenza dell'entry nella cache.

Contromisure

Per evitare un attacco man in the middle di tipo DNS poisoning è possibile effettuare le seguenti azioni:

1)Usare DNS con generazione casuale dei transaction ID (Bind v9);

2) DNSSec (implementato in Bind v9) permette la firma digitale dei dati. Ovviamente anche il resolver deve supportare questa estensione;

3) Evitare di rendere pubblico il DNS che si utilizza "in casa" per la risoluzione di nomi non appartenenti alla propria zona;

4) Eliminare il dynamic update o rendere pubblico un semplice forwarder che inoltra le richieste ad un altro name server con questa feature, non raggiungibile dall'esterno;

2 Traffic tunnelling

Quando parliamo di traffic tunnelling faremo riferimento ai router CiscoIOS e al metodo di incapsulamento IP su GRE. Un tunnel e' instaurato tra due "end point" detti tunnel broker. Su ognuno dei due endpoint, il tunnel e' associato ad un'interfaccia virtuale con un suo indirizzo (ad esempio Tunnel0), che deve essere legata ad un'interfaccia reale (ad esempio Serial0). Ogni volta che il router deve inoltrare un pacchetto IP che ha come "next hop" un indirizzo che cade nella subnet dell'IP address dell'interfaccia di tunnel, il pacchetto viene incapsulato e spedito all'altro endpoint. Questa tipologia di attacco lascia come traccia più evidente la riconfigurazione del router.

Contromisure

Per evitare un attacco man in the middle di tipo traffic tunneling è possibile effettuare le seguenti azioni:

1) Password forti sul router per l'accesso a qualsiasi livello;

2) Disabilitare o proteggere con community forti l'accesso in scrittura via snmp.

3 – Route mangling

L'attacco mira a dirottare il traffico tra le vittime A e B e consente di raccogliere informazioni dall'attaccante verso A e verso B.

Dal punto di vista del routing internet è divisa in Autonomous System (AS) connessi tra loro attraverso le backbone. Si adottano differenti politiche all'interno dell'AS e all'esterno. Gli AS sono identificati dal loro Border Gateway quando i pacchetti viaggiano sul backbone.

Contromisure

La contromisura più efficace e' senza dubbio abilitare un'autenticazione forte nei protocolli che la supportano ma è anche importante disabilitare i protocolli di routine dinamici.