Session Hijacking

 1

SESSION HIJACKING (lett. dirottare una sessione): una sessione attiva tra un client e un server viene "dirottata" da un intrusore che:

- Impersona il client;
- Prosegue con il server la sessione dirottata.

Spesso si accompagna con la necessita' di:

- Rendere il client inattivo.

 2

Effetti:

- bypassare la fase di autenticazione, effettuata dal reale client;
- impersonare l'identita' del client;
- sfruttare gli stessi privilegi o accedere a informazioni riservate.

Tipologie di Sessioni dirottate:

- Applicative;
- TCP.

 3

Dirottamento (Hijacking) di una Sessione TCP

```
tclient.net.52894 > tserver.com.23: S
                                    3900690:3900690(0)
tserver.com.23 > tclient.net.52894: S
                        1379776:1379776(0) ack 3900691
tclient.net.52894 > tserver.com.23: . ack 1379777

tclient.net.52894 > tserver.com.23: P
                                   3900691:3900718(27)
...
```

Cosa identifica il client rispetto il server?

- Indirizzo IP / porta del client;
- ACK del numero di sequenza del server.

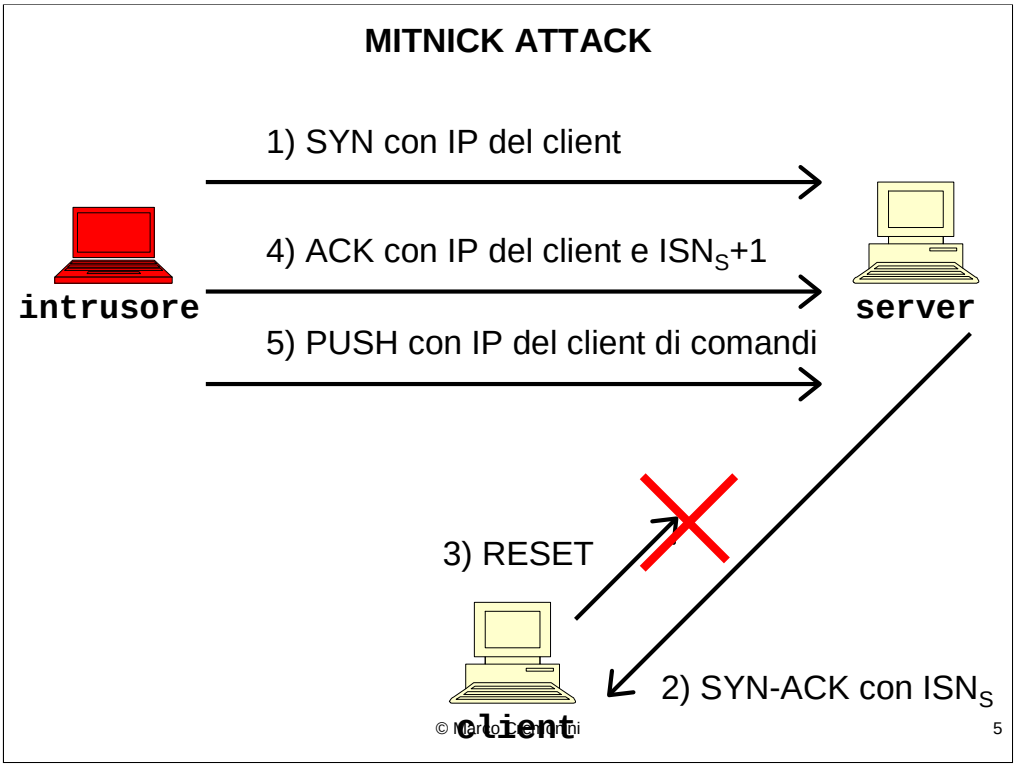
 4

Consideriamo l'handshake di una sessione TCP e in particolare che cosa identifica l'originatore della sessione stessa, al fine di valutare quali sono gli elementi critici al fine di compiere un session hijacking.

Nell'esempio:

Indirizzo IP/porta del client (tclient.net.52894);

Numero di sequenza del messaggio con l'ACK (1379777).



Pre-requisito: l'intrusore sa che tra client e server e' possibile stabilire una sessione applicativa specifica.

1) L'intrusore invia il primo pacchetto dell'handshake (SYN) con indirizzo IP del client;

2) Il server, risponde al client con il secondo pacchetto (SYN-ACK);

3) Il client, non avendo iniziato alcuna sessione con il client, dovrebbe rispondere con un RESET, ma l'operazione viene impedita (vedremo come in seguito);

4) L'intrusore risponde con l'ACK, con indirizzo IP del client e con SEQUENCE NUMBER (+1) definito dal server;

La sessione e' stabilita,

5) l'intrusore puo' inviare dati (esempio, comandi) al server.

Problema: come fa l'intrusore a rispondere (ACK) al sequence number (ISNS+1) del server se non ha mai ricevuto il pacchetto con SYN-ACK nel quale il sequence number veniva definito?

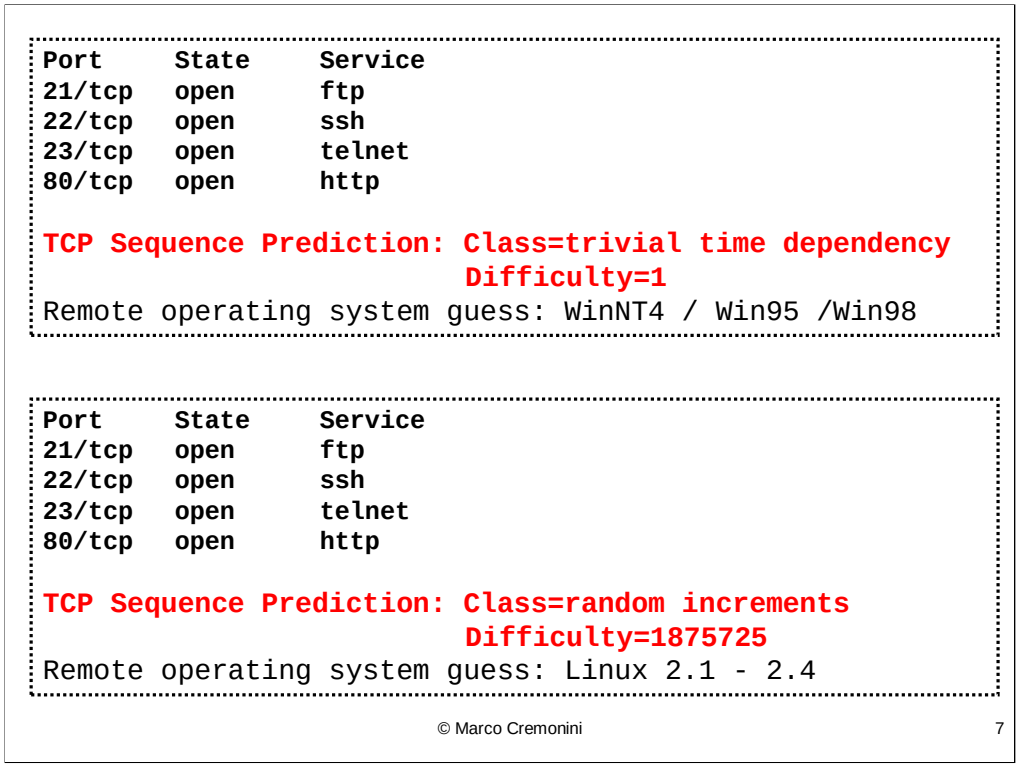
Predicibilita' dei numeri di sequenza

Problema: come fa l'intrusore a rispondere (ACK) con il sequence number (ISN_S+1) del server se non ha mai ricevuto il pacchetto con SYN-ACK nel quale il sequence number veniva definito?

Sequence Number: 32-bit, differente per ogni nuova sessione --> pacchetti di sessioni differenti DEVONO avere SN diversi.

Implementazione dipendente dalla versione del sistema operativo.

 6

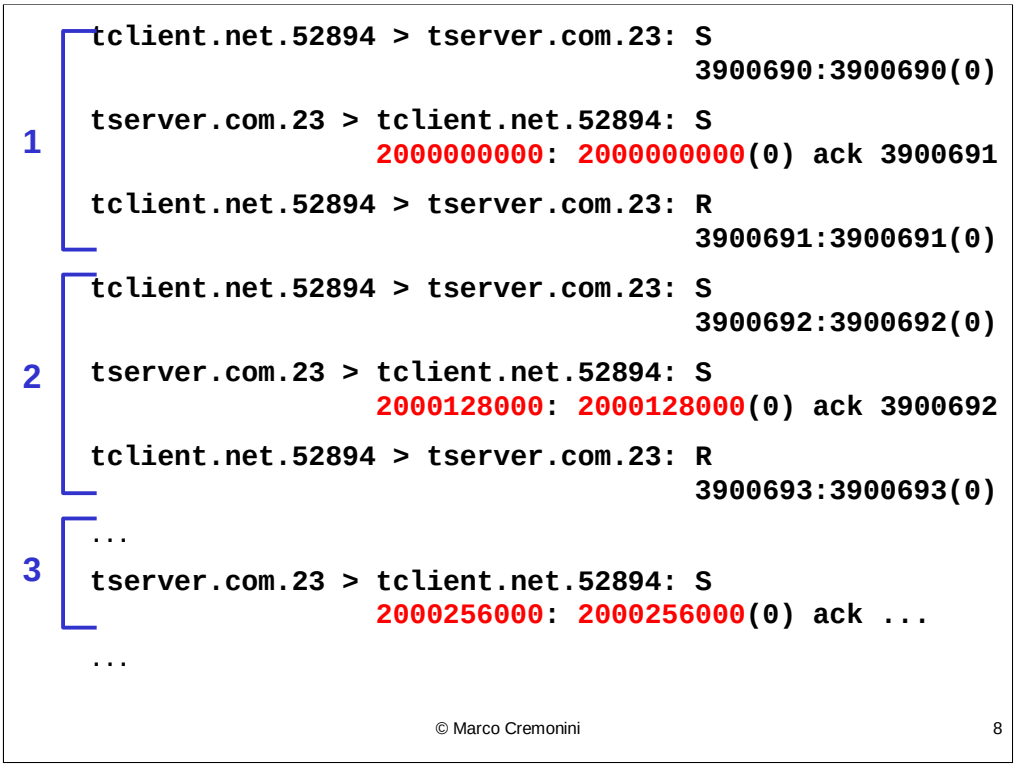


Con l'uso di scanner (es. Nmap) o altri tool disponibili liberamente (sia open source, freeware che commerciali) e' possibile verificare il tipo di sistema operativo remoto (con ottime possibilita' di individuazione).

La conoscenza del sistema operativo indica anche il tipo di implementazione del generatore di numeri di sequenza.

In allcuni casi puo' essere molto semplice (incrementi fissi a intervalli temporali regolari), in altri puo' essere estremamente difficile.

Esistono poi tool specializzati per la predizione dei numeri di sequenza e per facilitare un session hijacking.



Provando molte connessioni successive e' possibile ricavare un elenco di numeri di sequenza da analizzare per verificare se sono predicibili.

Nell'esempio, vediamo che, banalmente, il SN viene incrementato di 128000 => molto facile da predire.

Hijacking

```
spoofed.login > tserver.com.23: S
                          3900690:3900690(0)

????????? (il SYN-ACK non viene ricevuto) ??????????

spoofed.login > tserver.com.23: ack
                       2000384000:2000384000(0) ack
```

Se il numero di sequenza contenuto nel ACK e' quello che il server si aspetta, allora la sessione rimane attiva per uno scambio di dati, altrimenti verra' resettata dal server.

 9

Comandi

```
mitnick.login > x-terminal.shell: P 0:2(2) ack 1
mitnick.login > x-terminal.shell: P 2:7(5) ack 1
mitnick.login > x-terminal.shell: P 7:32(25) ack 1

mitnick.login > x-terminal.shell: F 32:32(0) ack 1
```

Comando utilizzato :

rsh x-terminal "echo + + >>/.rhosts"

 10

La traccia mostra l'invio di dati dall'intrusore al server compromesso (x-terminal).

I dati, nel caso di Mitnik, contenevano il comando rsh x-terminal "echo + + >>/.rhosts" che fa si che x-terminal accetti connessioni (con permessi di root) da qualunque computer utilizzando il login remoto.

Come venne isolato il reale client

```
mitnick2.600 > client.login: S 3900690:3900690(0)
mitnick2.601 > client.login: S 3900690:3900690(0)
mitnick2.602 > client.login: S 3900690:3900690(0)
mitnick2.603 > client.login: S 3900690:3900690(0)
mitnick2.604 > client.login: S 3900690:3900690(0)
mitnick2.605 > client.login: S 3900690:3900690(0)
...
```

SYN Flooding: tipologia di denial-of-service, nel caso di Mitnik un pacchetto ogni decimo di secondo.

 11

CRITICITA' EMERSE

- **Scanning e Fingerprinting;**
- **IP Spoofing;**
- **Numeri di Sequenza Predicibili;**
- **SYN Flooding;**
- **Modifica ad un file critico (.rhosts) non rilevata;**
- **Servizi insicuri (rlogin)**

 12

Ad oggi, tutte le tecniche utilizzate sono ancora pienamente efficaci ed utilizzate.

Scanning e Fingerprinting: necessita' di monitoraggio per riconoscere attivita' sospetta di acquisizione di informazioni.

IP Spoofing: INGRESS ed EGRESS filtering permetterebbero di ridurre drasticamente l'uso di indirizzi IP fasulli. Raramente vengono implementati.

La predicibilita' dei numeri di sequenza e' diminuita, anche se i tool sviluppati sono stati resi piu' efficaci. Molto spesso sarebbe necessaria l'installazione di patch rilasciate dai produttori di sistemi operativi che pero' gli utenti non installano.

SYN Flooding: I sistemi sono diventati piu' resistenti, ma le tecniche per denial-of-service si sono evolute notevolmente.

La possibilita' di rilevare modifiche a file di sistema critici e' possibile con l'uso di tool appositi che eseguono questi controlli. Forte carico di gestione, analisi di log. Spesso non ci sono le persone da assegnare a questo compito.

Nonostante esistano servizi piu' sicuri comunemente disponibile, la norma continua ad essere quella di utilizzare i servizi tradizionali, efficienti ma non sicuri.

CONTROMISURE

- **Comunicazioni crittate (es. SSL);**
- **Protocolli sicuri (es. SSH);**
- **Limitare i tipi di connessione (FIREWALL);**
- **Limitare la possibilita' di accessi remoti;**
- **Metodi di autenticazione forti (?? meno efficaci)**

 13

Perche' i metodi di autenticazione possono non essere efficaci per evitare il session hijacking? Vedere caso dei cookies al termine della presentazione delle vulnerabilita'.

Analizziamo ora quali tecniche vengono oggi in realta' utilizzate.

Si verifica dai dati resi pubblici che I modi per realizzare intrusioni oggi sono molto diversi da quelli di Mitnik.

In particolare, sono piu' semplici, non e' necessario oggi, nella media, l'utilizzo di strategie di attacco cosi' complesse.