UNIVERSITA' DI CATANIA

RELAZIONE SUL CHALLENGE DEDICATO ALLA GESTIONE DEI CERTIFICATI

ORESTE DELITALA - W82000025

1. Introduzione

L'obiettivo del seguente challenge è incentrato sullo studio della gestione dei certificati di root da parte dei sistemi operativi Fedora e Windows 7 utilizzando i browser nativi del sistema operativo stesso.

Il challenge è diviso in 4 punti principali:

- spiegare come visualizzare i certificati nei due browser.
- verificare se sono gli stessi e come sono fatti.
- costruire un certificato di root ad hoc ed importarlo nei browser, dimostrando la procedura di import, specie in termini di interazione con l'uomo.
- costruire una sessione malevola basata su quei certificati di root.

2. Visualizzare i certificati nei due browser

I browser nativi nei due sistemi operativi sono, Internet Explorer su Windows 7 e Mozilla Firefox su Fedora.

Le procedure per visualizzare i certificati dei browser sono molto simili sui due browser esaminati. Nel primo, cioè Internet Explorer su Windows 7, la procedura per visualizzare consiste nel selezionare il menù delle impostazioni del browser, cliccare su "Opzioni Internet" e selezionare il menù "contenuto", dentro troveremo un pulsante "certificati" e cliccandoci entreremo dentro il gestore dei certificati per Internet Explorer.

Le voci che troveremo nel gestore dei Certificati interessanti al fine del nostro challenge sono:

- Autorità di certificazione intermedie: contiene tutti i certificati intermedi per la risoluzione della catena dei certificati, dove non faranno parte i nostri certificati radice.
- Autorità di certificazione radice attendibile: contiene tutti i certificati radice che saranno considerati attendibili nella risoluzione della catena di certificati.

Nel secondo browser, Mozilla Firefox su Fedora, la procedura per la visualizzazione dei certificati consiste nel aprire il menù del browser e cliccare su "Preferenze", che aprirà una finestra che selezionando "avanzate" ed in seguito "certificati" visualizziamo il pulsante "mostra certificati".

Le voci che troveremo nel gestore dei Certificati interessanti al fine del nostro challenge sono:

- Server: contiene tutti i certificati intermedi per la risoluzione della catena dei certificati, dove non faranno parte i nostri certificati radice.
- Autorità: contiene tutti i certificati radice che saranno considerati attendibili nella risoluzione della catena di certificati.

3. Verificare se sono gli stessi e come sono fatti

Adesso si possono esaminare i Certificati visualizzati nel punto precedente, e possiamo subito notare che la quantità dei certificati nei due browser è differente.
Internet Explorer su Windows 7 contiene circa 45 certificati, invece Mozilla Firefox su Fedora contiene circa 170 certificati. Valutare quale condizione è migliore dell'altra è relativo, perché una quantità maggiore di certificate potrebbe risolvere più catene di fiducia dei certificati e quindi fornire un servizio più user-friendly, però bisogna vedere come gestisce questi certificati in caso di scadenza o di certificato compromesso.

Per visualizzare il contenuto del Certificato su Internet Explorer basta cliccare sul certificato da noi interessato e cliccare sul pulsante in basso "visualizza", si aprirà una finestra contenenti le informazioni del certificato, e su "dettagli" possiamo vedere tutto il contenuto del certificato.

Per visualizzare il contenuto del Certificato su Mozilla Firefox basta come per Explorer selezionare il Certificato e cliccare su "visualizza" e su "dettagli" abbiamo tutte le informazioni sul certificato.

4. Costruire un certificato di root ad hoc ed importarlo

Per costruire un certificato di root ad hoc ho utilizzato OPENSSL sulla macchina Fedora, che permette di costruire certificati auto firmati oppure firmati da altri certificati di root.

Il comando di OPENSSL per costruire un certificato auto-firmato, per poi essere caricato come certificato di root, è il seguente:

openssl req -new -x509 -nodes -days 3650 -newkey rsa:2048 -keyout ./my-ca.key -out ./my-ca.crt

dove:

- req sta per richiesta
- -new nuovo certificato
- -x509 lo standard utilizzato per il certificato.
- -nodes non codifica con des la kiava privata
- -days 3650 fissa la durata in giorni del certificato
- -newkey rsa:2048 richiesta di una nuova chiave a 2048 bit con codifica rsa
- -keyout ./my-ca.key dove viene salvata la chiave privata
- -out ./my-ca.crt dove viene salvato il certificato costruito

Lanciando il comando chiederà delle informazioni per la costruzione del Certificato, noi andremo a settare "Common Name" con il nome della nostra CA Root.

Per importare il nostro certificato auto-firmato come certificato di root, dobbiamo per entrambi i browser aprire il gestionale dei certificati come descritto nel punto 2 della relazione, dopo nel caso

di Internet Explorer andare a selezionare la voce di menù “Autorità di certificazione radice attendibile” e clicchiamo sul pulsante “Importa”, seguire la procedura di importazione ed in fine il certificato costruito precedentemente sarà nella lista dei certificati di root.

Un'altra modalità di importazione del certificato è aprire il certificato auto-firmato, seguire la procedura di importazione, ed al momento della richiesta di selezione dell’archivio dei certificato vado a selezionare “Autorità di certificazione radice attendibile”, che corrisponde alla lista dei certificati di root.

Nel caso di importazione su Mozilla Firefox entriamo nel gestionale dei certificati, selezioniamo la voce di menù “Autorità” e si clicca su “importa” e si seleziona il certificato auto-firmato costruito precedentemente.

Le considerazioni in termini di interazione con l'uomo sull’importazione di un certificato sono:

- Il browser viene eseguito con i permessi di root del sistema su cui viene eseguito
- Un utente senza permessi di amministratore del sistema può importare un certificato radice.

5. Costruire una sessione malevola basata su certificati di root ad hoc

Per costruire una sessione malevola basata sul certificato radice generato nel punto 4 bisogna utilizzare un server virtuale, nel caso del challenge ho usato “xampp” come server virtuale su Windows 7.

Ci serve un certificato firmato dal certificato di root ad hoc precedentemente generato nel punto 4 ed installarlo nel server virtuale xampp.

Per costruire il certificato per il server virtuale lanciamo il seguente comando openssl che costruire una richiesta di certificato da far firmare in seguito dalla CA di root:

openssl req -new -nodes -newkey rsa:2048 -keyout ./my-site.key -out ./my-site.csr

dove:

- req sta per richiesta
- -new nuovo certificato
- -nodes non codifica con des la kiava privata
- -newkey rsa:2048 richiesta di una nuova chiave a 2048 bit con codifica rsa
- -keyout ./my-site.key dove viene salvata la chiave privata
- -out ./my-site.csr dove viene salvata la richiesta di certificato

Adesso prendiamo la richiesta di certificato e la facciamo firmare dalla CA di root costruita nel punto 4.

Lanciamo il seguente comando:

openssl x509 -req -in ./my-site.csr -out ./my-site.crt -sha1 -CA ./my-ca.crt -CAkey ./my-ca.key -CAcreateserial -days 3600

Dove:

- x509 lo standard utilizzato per il certificato.
- -req sta per richiesta
- -in ./my-site.csr indica il file di input cioè la richiesta del certificato
- -out ./my-site.crt dove viene salvato il certificato costruito dalla CA root
- -sha1 l'algoritmo di hashing utilizzato
- -CA ./my-ca.crt seleziono la CA che firma il certificato
- -CAkey ./my-ca.key la chiave private del CA che firma
- -CAcreateserial la CA crea un seriale
- -days 3600 fissa la durata in giorni del certificato

Lanciando il comando chiederà delle informazioni per la costruzione del Certificato, noi andremo a settare "Common Name" con il nome del nostro server, cioè il dominio, nel nostro caso "localhost".

Adesso si va a settare il certificato del server appena generato all'interno del Server Virtuale xampp:

- Inserisco il file my-site.crt su /xampp/apache/conf/ssl.crt/
- Inserisco il file my-site.csr su /xampp/apache/conf/ssl.csr/
- Inserisco il file my-site.key su /xampp/apache/conf/ssl.key/
- Modifico il file httpd-ssl.conf su /xampp/apache/conf/extra/ inserendo le seguenti righe:
    - SSLCertificateFile "conf/ssl.crt/my-site.crt"
    - SSLCertificateKeyFile "conf/ssl.key/my-site.key"
    - SSLCACertificatePath "conf/ssl.crt/"
    - SSLCACertificateFile "conf/ssl.crt/my-site.crt"

Il server virtuale adesso configurato è pronto per essere utilizzato, apro l'applicazione Internet Explorer e digito l'indirizzo "https://localhost" e vedremo che il lucchetto di sicurezza del browser sarà chiuso indicando il sito attendibile in quando si è risolta la risoluzione della catena dei certificati.

6. Conclusioni

Dal challenge svolto in laboratorio si è evinto che la questione dei certificati è cruciale, e la scelta di assegnare i permessi di amministratore al browser da delle vulnerabilità al sistema, in quanto permette ad un utente non amministratore di installare un Certificato come Certificato di Root.