TU Wien
Institut für Rechnergestützte Automation
Forschungsgruppe Industrial Software
Arbeitsgruppe ESSE
http://security.inso.tuwien.ac.at/

Abgabedokument Lab1

Security for Systems Engineering

183.637 - SS 2013

10.5.2013

Gruppe 48

Name	**MatrNr.**	**Emailaddresse**
Patrick Fleck	1025484	e1025484@student.tuwien.ac.at
Klaus Behrens	0927376	e0927376@student.tuwien.ac.at
Matthias Pernerstorfer	0929329	e0929329@student.tuwien.ac.at
Martin Winklmüller	1025742	e1025742@student.tuwien.ac.at
David Mihola	9902433	e9902433@student.tuwien.ac.at

Inhaltsverzeichnis

1 Lab1a

1.1 Hinweise

Hinweise:

- Setzen sie alle Variablen nach *FOR STUDENTS* in der .tex File
- Ersetzen sie die Platzhalter für ihre Namen und MatNr.
- Löschen sie diese Sektion über Hinweise und die folgenden Beispiel-Kapitel
- Achten sie auf geforderte Formate und Anforderungen an die Dateinamen

1.2 Zugang zu Tomcat

Den Zugang zum Tomcat-Server erhält man sehr leicht - zumindest unter Linux. Alle Arbeiten wurden unter Linux durchgeführt. Für den Zugang ist es notwendig, sich via SSH auf den ESSE-Server zu verbinden, allerdings mit Port Forwarding auf den angegebenen Tomcat-Server:
ssh -p 12345 MATRNR@sela.inso.tuwien.ac.at -L 2222:192.168.20.100:20
Dies hat zur Folge, dass der Port 2222 nun auf den Port des Tomcat-Servers geforwarded wird und es somit ein leichtes ist mittels http://localhost:2222 die Homepage auf dem Server einzusehen.

1.3 Walter's Private Key

Nun war es die Aufgabe sich einen SSH-Zugang mit dem User 'walter' zu verschaffen. Hierfür gibt es 2 Möglichkeiten, sich via SSH zu authentifizieren: 1) Plain-Text Passwort und 2) Private-Key und Public-Key Methode
Natürlich ist es sehr unwahrscheinlich, dass jemand sein Passwort als Plain-Text irgendwo auf einem Server abspeichert. Deshalb fokusieren wir uns im folgenden auf die 2. Möglichkeit.
Unter Linux-Systemen gibt es hierfür einen Ordner .ssh im Home-Verzeichnis des Users. Im Falle von David Mihola würde dieser unter /home/David/.ssh zu finden sein. Hier liegt nun eine Datei id_rsa, die im Normalfall den Private Key des Users, der den SSH-Zugang anfordert beinhaltet.
Nun sollte es doch für 'walter' genauso sein. Das heißt wir suchen nach dem Ordner /home/walter/.ssh. Dieser ist aber natürlich am Server geschützt und kann nicht einfach durch

eintippen in Plain-Text in die Adresse des Servers angesurft werden. Jedoch hat der hier verwendete Tomcat-Server eine Schwachstelle. Mittels Directory-Traversal kann der Server ausgetricktst werden und der Ordner eingesehen werden. Hier die Adresse der zu untersuchenden Datei:
http://localhost:2222/
Directory-Traversal führt hier eine Umwandlung von Plain-Characters in Sonderzeichen ein, wodurch der Server nun die Datei auch anzeigt. Die Sonderzeichen sind spezielle URI-Zeichenfolgen, die vom Server in Plain-Text umgewandelt werden. Damit kann man etwaige Schutzmechanismen des Tomcat-Servers umgehen.

1.4 SSH-Zugang via User 'Walter'

Wie bekommt man nun einen SSH-Zugang mit einem fremden Private Key? Wie oben beschrieben, gibt es für jeden User den Ordner .ssh mit den Private Keys für SSH-Zugängen. Es muss nun möglich sein, sich einen Zugang zum User 'walter' zu verschaffen, indem man sich als dieser ausgibt. Dazu wird einfach im Ordner /home/David/.ssh eine Datei namens id_rsa erstellt (falls diese noch nicht existiert). Danach wird der gefundene Schlüssel von 'walter' hineinkopiert und die Datei gespeichert. Nun ist es nocht notwendig mittels 'chmod 600 id_rsa' den Zugriffsschutz des Keys auf Permission 600 umzustellen. Andernfalls wird der Server die Verbindung verweigern, da der Key nicht ausreichend geschützt ist. Das Port-Forwarding über die SSH-Verbindung zum ESSE-Institut sollte nun noch vorhanden sein. Da wir ja über den Port 2222 direkt auf den Tomcat-Server zugreifen können, ist es nun möglich sich mittels 'ssh -p 2222 walter@localhost' mit dem Benutzer 'walter' einzuloggen. Dies funktioniert aus folgendem Grund:
Der Server speichert (im .ssh-Ordner) zusätzlich noch den Public-Key jedes Users. Wird nun eine Verbindung angefordert, so muss der User, der dies durchführt, einen Private-Key in seinem .ssh-Ordner besitzen, der zu einem Public-Key am Server passt. Wir haben uns den Private-Key von 'walter' in unseren eigenen .ssh-Ordner kopiert und der Server glaubt nun, wir seien auch dieser User.

2 Ueberschrift 2

2.1 Sub-Ueberschrift 1

Lorem ipsum dolor sit amet, consetetur sadipscing elitr, sed diam nonumy eirmod tempor invidunt ut labore et dolore magna aliquyam erat, sed diam voluptua.

2.2 Sub-Ueberschrift 2

Lorem ipsum dolor sit amet, consetetur sadipscing elitr, sed diam nonumy eirmod tempor invidunt ut labore et dolore magna aliquyam erat, sed diam voluptua. At vero eos et

accusam et justo duo dolores et ea rebum.

2.3 Sub-Ueberschrift 3

Lorem ipsum dolor sit amet, consetetur sadipscing elitr, sed diam nonumy eirmod tempor invidunt ut labore et dolore magna aliquyam erat, sed diam voluptua.

3 Beispiele

3.1 Source Code formatieren

Es folgen einige Beispiele wie Sourcecode in diesem Dokument formatiert und referenziert werden kann (siehe Listing ?? auf Seite ?? und siehe Listing ?? auf Seite ??).

Ebenso können kurzer Code oder kurze Befehle direkt in der Zeile in einem `lstinline Block` mit typengleicher Schrift formatiert werden.

```
/*
 * Just an example C-file.
 */

#include <stdio.h>

int global_variable = 1;
#ifdef DEBUG
int another_global_variable = 1;
#endif

/*
 * Some comment
 */
int main(void)
{
  temp_variable = 4711;
  another_variable = 0815;

  printf("foo bar baz %02d", temp_variable);

  return 1;
}
```

Listing 1: Example C/C++ file

```
#!/bin/bash
echo "Bash version ${BASH_VERSION}..."
for i in {0..10..2}
  do
     echo "Welcome $i times"
 done
```

```
8 echo "some very very very very very very very very very ↵
     very very very very very very very very very very ↵
     long string"

10 exit 0;
```

Listing 2: Example bash script

3.2 Bilder

Es folgen einige Beispiele wie Bilder in diesem Dokument eingefuegt werden koennen (siehe Abbildung ?? auf Seite ??).

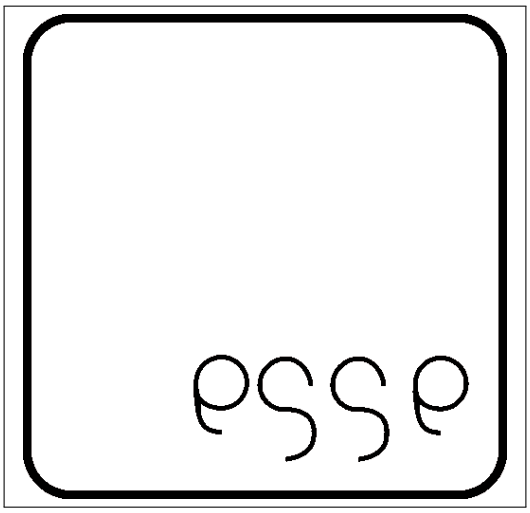

Abbildung 1: ESSE Logo