Operating Systems Security – Assignment 1

Version 1.0.1 – 2015/2016

Institute for Computing and Information Sciences,
Radboud University Nijmegen, The Netherlands.

1 Manage custom PAM authentication rules

Pre-requisite: Setup (virtualized) Kali Linux operating system

- Download, install and configure the Kali Linux VMWare image, see website[1]
- Add a few (test) users to the system.

Objectives

Play around with the Pluggable Authentication Modules (PAM) in the Kali Linux system.

a) For each of the PAM control values (required, requisite, optional, sufficient), give an example of a PAM rule using it, which is actually useful in some context. Explain the context where the rule should be used and what the rule accomplishes.
b) Create the text file `/tmp/users` and specify on each line a valid username; you have to specify at least one user.
In this exercise, limit yourself to only adjust the rules in the sshd PAM module configuration file (`/etc/pam.d/sshd`).
Use the `pam_listfile` module[2] and try to achieve the following sshd login configurations for the users listed in `/tmp/users`:
   i) Lockout remote password logins for the specified users.
   ii) Disable remote public key logins for specified users.
   iii) Bypass authentication and allow remote user logins without a valid password or authorized public key.

   Hand in your solution for each of the previous rules and point out why you applied the corresponding control value. If you were not able to compose a PAM directive that restricts/allows one or more of the previous rules, explain briefly why you think this is not possible.

   Note: For some background knowledge about PAM, please refer to the following websites [3][4]

2 Become familiar with the Metasploit Framework

Pre-requisite: Download and setup a vulnerable system

- Download and setup Metasploitable[5], which is an intentionally vulnerable Linux virtual machine. Note, **never** expose this VM to an untrusted network (e.g. set

[1] http://www.offensive-security.com/kali-linux-vmware-arm-image-download/
[2] http://www.linux-pam.org/Linux-PAM-html/sag-pam_listfile.html
[3] http://www.linux-pam.org/Linux-PAM-html/Linux-PAM_SAG.html
[4] https://www.netbsd.org/docs/guide/en/chap-pam.html
[5] http://sourceforge.net/projects/metasploitable/

it up behind a router / NAT / Host-only configuration). For now, setup Metasploitable and Kali using NAT and make sure that your VM's have a different IP address and that you are able to `ping` the Metasploitable VM from your Kali VM.

– Download in Kali Linux the Nessus "home" edition from Tenable network security[6] and register for an activation code on their website[7]. Install the Nessus Debian package:
```
# dpkg -i Nessus-6.5.3-debian6_amd64.deb
```
And start Nessus with:
```
# /etc/init.d/nessusd start
```
Register your software by entering the activation code that you received by e-mail:
```
# /opt/nessus/sbin/nessuscli fetch --register xxxx-xxxx-xxxx-xxxx
```
Start Iceweasel, a free version of Firefox, (or download another browser) and open the local Nessus web-interface:
```
https://localhost:8834
```

Objectives

Create a new profile, that defines a full system scan and use Nessus to scan the Metasploitable 2 system. You will find in this system at least 9 problems which are identified by Nessus as "critical". Some of those problems are trivial to exploit (like logging into a service with username "admin" and password "admin"). Some other problems require some more effort, but are efficiently exploitable with Metasploit.

a) Exploit at least one buffer-overflow vulnerability and at least one other non-trivial vulnerability with Metasploit. Note that not all buffer-overflow vulnerabilities are explicitly called "buffer-overflow vulnerability" by Nessus. For each of the attacks give a brief summary what actions you performed and which (additional) sources you have used to exploit the system. Of course, if you want to play more with Metasploit, feel free to keep exploiting more vulnerabilities.

Some practical examples are explained on the following websites[8][9][10]

[6] http://www.tenable.com/products/nessus/select-your-operating-system
[7] http://www.tenable.com/register
[8] http://www.securitytube.net/video/5489
[9] http://www.securitytube.net/video/6432
[10] https://community.rapid7.com/docs/DOC-1875