Homework 3

CIS 4930 / CIS 5930
Offensive Computer Security (OCS2014)
Spring 2014

Due January 31th, 2014, by *MIDNIGHT*
Worth: 100 points

Electronic turn in (Turn in via email to TA. Email address is raiaan@cs.fsu.edu)
The email must be titled in the following format:
"[OCS2014] hw3 <your last name>". (where <your last name> is your last name)
Example: [OCS2014] hw3 redwood

The following questions pertain to general linux systems. When in doubt, refer to Debian or Ubuntu implementations.

1) [10 points] What is the purpose of:
a) the /etc/passwd file?
b) the /etc/shadow file?
c) the setuid bit?
d) chroot?

2) [10 points] Explain the differences between the commands "ls -l" and "lsattr".

3) [5 points] Android is a linux based operating system. The android app store features many apps that when installed request access to all sorts of information, sometimes information that seems completely irrelevant to the program. Explain the general problem with android apps through the least privilege principle.

4) [5 points] Compare access control lists to the standard unix permissions model.

5) [10 points] Compare ruid and euid. Explain an example how they may not be equal.

6) [10 points] List two entirely different ways that an attacker might clean his/her tracks when attacking a unix based system. State the required level of access for each approach. Explain your answers.

7) [20 points] Intelligent Platform Management Interface (IPMI) Questions. Read https://jhalderm.com/pub/papers/ipmi-woot13.pdf. Answer the following:

A. What are the author's main findings, and the impact of these findings?
B. What countermeasures / practices do the authors suggest?
C. [10 points] Explain 3 of the vulnerabilities did the researchers find? What impacts did they have?

8) [25 points] Here's a scenario, which is going to take some googling / research: You've been hired to do incident response/investigation at a local small coffee shop, and the believe that their webserver has been hacked when the boss was out of town, as the website has been defaced with various rantings and graffiti from disapproving coffee-"fascists".

They also believe that the attacker used their own wifi (WEP encryption) at the coffee shop to do it, so it occurred within their network firewall. They also believe that the attacker used SQL injection (we'll cover this later) to hack into the admin console for their custom content management system (a undergraduate student designed it for them), for the purpose of uploading a webshell. They found the webshell (which was called bkdoor.php), and also found some interesting entries in the logs for the URL's that were served to the attacker using the bkdoor.php:

- www.coffeshop.com/include/bkdoor.php?cmd=cat ../../../../../../etc/passwd
- www.coffeshop.com/include/bkdoor.php?cmd=cat ../../../../../../etc/shadow
- www.coffeshop.com/include/bkdoor.php?cmd=cat ../../../../../../etc/hosts.equiv
- www.coffeshop.com/include/bkdoor.php?cmd=cat ../../../../../../root/.rhosts

The employees explain that the webserver's apache http daemon (tomcat6) was implemented using the least permissions principle, with tomcat6 under its own user account and does not have access to the shadow file (which is pretty impressive for a bunch of art students). But they do not understand how the attacker managed to get root, as the password hashes were not in the /etc/passwd file, and not accessible to the user account running the apache daemon (tomcat6). Also they don't understand the request for /root/.rhosts as the attacker couldn't have viewed it under the tomcat6 account (which did not have root access).

The logs show no sign of the attacker trying to brute force the root password on the webserver. Lastly the boss's Debian computer (which upon inspection has not been patched in forever) seems to have been hacked as well, and the attacker seems to have got root access on it as well.

The employees provide you with the /etc/passwd, /etc/hosts.equiv, and /root/.rhosts file on the webserv (but not the /etc/shadow file)

1. The contents of the /etc/hosts.equiv file and the /root/.rhosts file contain only the IP address for the boss's computer
2. The contents of the /etc/passwd file are:

root:x:0:0:root:/root:/bin/bash daemon:x:1:1:daemon:/usr/sbin:/bin/sh bin:x:2:2:bin:/bin:/bin/sh sys:x:3:3:sys:/dev:/bin/sh sync:x:4:65534:sync:/bin:/bin/sync games:x:5:60:games:/usr/games:/bin/sh man:x:6:12:man:/var/cache/man:/bin/sh lp:x:7:7:lp:/var/spool/lpd:/bin/sh mail:x:8:8:mail:/var/mail:/bin/sh news:x:9:9:news:/var/spool/news:/bin/sh uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh proxy:x:13:13:proxy:/bin:/bin/sh www-data:x:33:33:www-data:/var/www:/bin/sh backup:x:34:34:backup:/var/backups:/bin/sh list:x:38:38:Mailing List Manager:/var/list:/bin/sh irc:x:39:39:ircd:/var/run/ircd:/bin/sh gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/bin/sh	nobody:x:65534:65534:nobody:/nonexistent:/bin/sh libuuid:x:100:101::/var/lib/libuuid:/bin/sh syslog:x:101:102::/home/syslog:/bin/false klog:x:102:103::/home/klog:/bin/false mysql:x:103:105:MySQL Server,,,:/var/lib/mysql:/bin/false landscape:x:104:122::/var/lib/landscape:/bin/false sshd:x:105:65534::/var/run/sshd:/usr/sbin/nologin postgres:x:106:109:PostgreSQL administrator,,,:/var/lib/postgresql:/bin/bash messagebus:x:107:114::/var/run/dbus:/bin/false tomcat6:x:108:115::/usr/share/tomcat6:/bin/false user:x:1000:1000:user,,,:/home/user:/bin/bash polkituser:x:109:118:PolicyKit,,,:/var/run/PolicyKit:/bin/false haldaemon:x:110:119:Hardware abstraction layer,,,:/var/run/hald:/bin/false pulse:x:111:120:PulseAudio daemon,,,:/var/run/pulse:/bin/false postfix:x:112:123::/var/spool/postfix:/bin/false

A. [15 points] Explain a possible attack scenario for this situation. Start with (or even before!) the wifi hacking. Explain in a manner that non-computer-science students might understand.

B. [5 points] Draw or provide a diagram for the attack chain for your answer in part A. Provide as many technical details as you like here.

C. [5 points] Provide the coffee shop some advice to prevent this in the future.

9) **[10 points]** Feedback (Be honest. It is free points)

A. [5 points] Are you struggling with anything in the class so far? If so what?

B. [5 points] How have the homeworks been so far (useful feedback for me involves difficulty / time discussion)?