CSCI 401

Prof. Kadri Brogi

February 7, 2020

Emranul Hakim

23467834

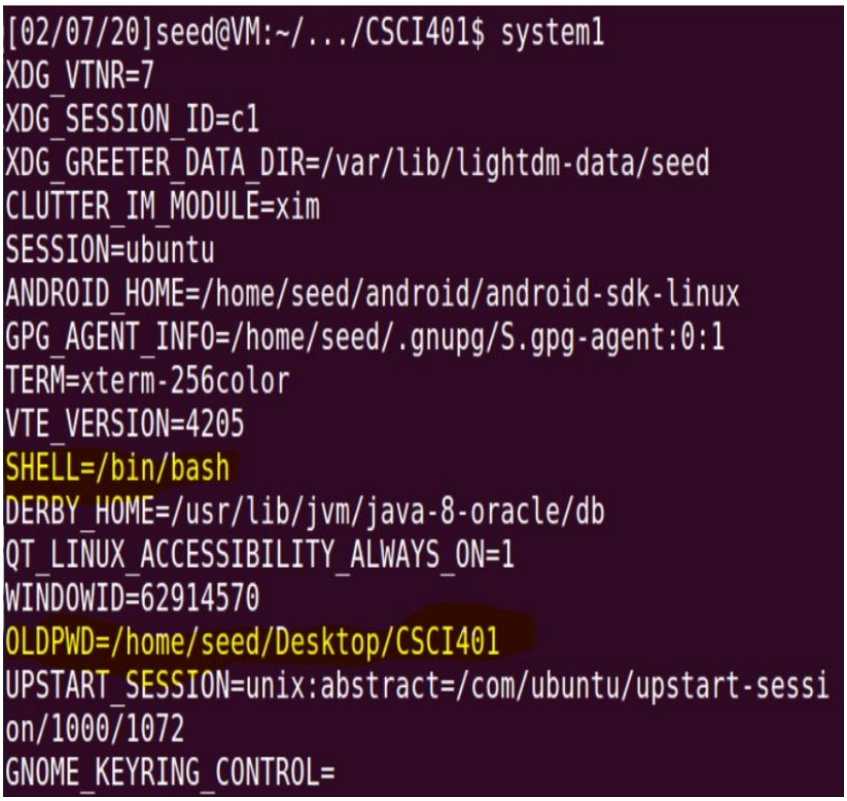
Set-UID Programs Environment Variables and Attacks.

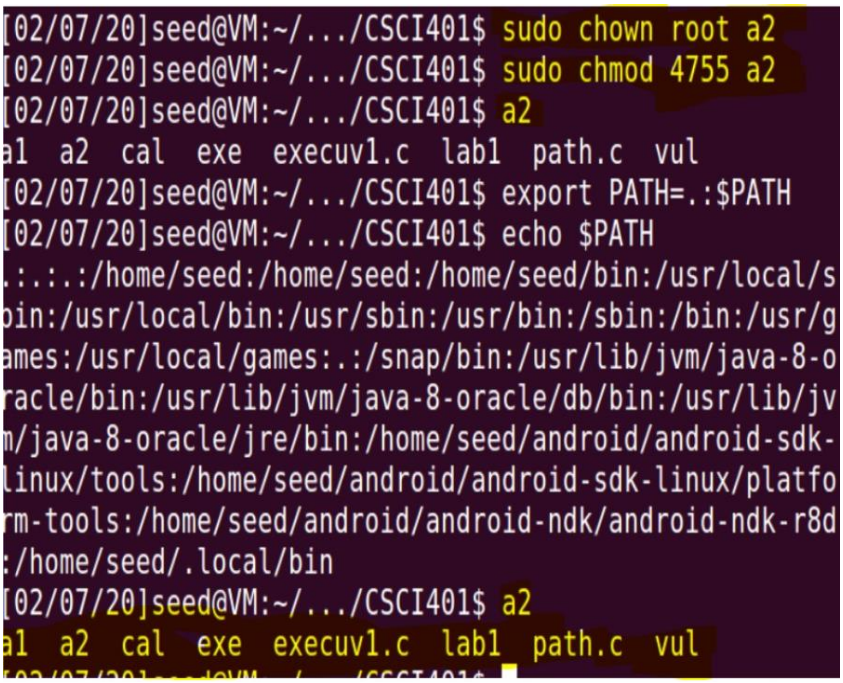
```c
#include <stdio.h>
#include <stdlib.h>

int main() {
 system("/usr/bin/env");
 return 0 ;
 }
```

```c
#include <stdio.h>
#include <stdlib.h>
extern char **environ;


int main()
{
char *argv[2];
argv[0] = "/usr/bin/env";
argv[1] = NULL;
execve("/usr/bin/env", argv, NULL);
return 0 ;
}
```


[02/07/20]seed@VM:~/.../CSCI401$ system1
XDG_VTNR=7
XDG_SESSION_ID=c1
XDG_GREETER_DATA_DIR=/var/lib/lightdm-data/seed
CLUTTER_IM_MODULE=xim
SESSION=ubuntu
ANDROID_HOME=/home/seed/android/android-sdk-linux
GPG_AGENT_INFO=/home/seed/.gnupg/S.gpg-agent:0:1
TERM=xterm-256color
VTE_VERSION=4205
SHELL=/bin/bash
DERBY_HOME=/usr/lib/jvm/java-8-oracle/db
QT_LINUX_ACCESSIBILITY_ALWAYS_ON=1
WINDOWID=62914570
OLDPWD=/home/seed/Desktop/CSCI401
UPSTART_SESSION=unix:abstract=/com/ubuntu/upstart-sessi
on/1000/1072
GNOME_KEYRING_CONTROL=



Q. Describe what environment variables are and how they affect program and system behaviors.

Ans:

Environment variable is a dynamic object on a computer that contains an editable value which can be used by one or more software programs in any operating system. It help programs know in what directory we are installing our files, storing temporary files, and where to look for user profile settings. For instance, when we run a command- *env| grep PWD* in our command prompt, it enables the child process to inherit a copy of the environmental blocks of its parent. That means we are giving the child process a privilege to access in the root.

Since the process above give us the access in the root, using environmental variable we can easily change the Set-UID of the child process and it will automatically change the Set-UID of the parent process. It clearly depicts a huge issue if the child process has more privilege than its parent process. Because it may use data from other users which make the whole system

vulnerable. However, it is not mandatory that environmental variables can be used by Set-UID, but we need to stay more vigilant about any kind of perilous situation.