1 Introduction

Unix-like Artifacts Collector (UAC) is a script that can be used to gather information from a Unix machine under investigation, making use of built-in tools. UAC supports AIX, BSD, Linux, MacOS and Solaris and requires administrative rights to run successfully. To tamper evidence as little as possible, it is strongly recommended to run the script from a **USB stick** or a **network share** that can be mounted from the target machine. The output of the UAC script should be saved on the same partition from which UAC was run. The size of this output can be several hundreds of MB; hence it is important to choose a partition with enough free space.

2 Preparation (on separate machine)

1. Obtain UAC. This tool can be downloaded for free from the official GitHub repository https://github.com/tclahr/uac
2. Depending on whether target machine has a physical USB port or not, either:
   a. Unzip file on USB stick.
   b. Unzip file on network share that can be mounted on target machine.

3 Information capture (on target Unix machine)

1. Mount the network share where UAC was unzipped or connect USB stick to target machine.
2. Open terminal and gain root privileges, depending on Linux distribution, this can be done either by running a command:
   `$ sudo su`
   on distributions using sudo (e.g. Ubuntu), or
   `$ su -`
   on other distributions (e.g. Debian, CentOS, RHEL)
3. Navigate to the folder where UAC was unzipped.
4. Run command[1]:

   ```
   # ./uac -p full <DESTINATION FOLDER>
   ```

5. When the script finishes, two files are created inside the destination folder. The output file whose name has the format a folder whose name has the format uac-<hostname>-<OS>-YYYYMMDDHHMMSS.tar.gz and another file with a similar name containing the MD5 hash of the output file.
6. Encrypt created archive with complex password (16 characters, mixed case letters, numbers, and special symbols):

   ```
   # gpg --symmetric --cipher-algo AES256 <hostname>.tar.gz
   ```

   This output file with *.gpg extension is ready to be sent to IBM Security X-Force IR.
7. Use method approved within your organization to securely erase UAC output folder and unencrypted tar.gz archive.

Note: On an average Linux system, the UAC script can take up to 60 minutes to complete. On other Unix systems, it can take up to several hours to complete depending on filesystem size and network shares.

Note: in case the script is unable to detect the UNIX version it is running on, it might be necessary to force it by specifying it explicitly with parameter -o. The syntax is as follows:

```
-o OPERATING_SYSTEM Where OS is:

 aix: Used to collect AIX artifacts.
 android: Used to collect Android artifacts.
 freebsd: Used to collect freeBSD artifacts.
 linux: Used to collect Linux artifacts.
 macos: Used to collect macOS artifacts.
 netbsd: Used to collect netBSD artifacts.
 netscaler: Used to collect Netscaler
artifacts.
 openbsd: Used to collect OpenBSD artifacts.
 solaris: Used to collect Solaris artifacts.

Ex.: ./uac -p full -o macos <DESTINATION
FOLDER>
```

4 Delivering files to IBM Security X-Force IR

1. Compressed, encrypted archive is ready for delivery to IBM Security X-Force IR team via agreed method of delivery.
2. Share complex password used to for encryption with IBM Security X-Force IR team using different

[1] https://tclahr.github.io/uac-docs/#command-line-options

communication channel then used to share forensic image.