System Call monitoring

The file contains following notable identifiers

- "Ts" – recorded time stamp
- pid” - process id
- "proc_name":" the name of the process
- "syscall_name" the name of the system call (read/write/execve)
- “buf :” the processc communication b

Interprocess communication sequence is given below

1. User sends a ssh session request to a the server (in our case PVM)
   The OpenSSL certificate manager is called by sshd process to validate the authenticity of the user. Traced system calls for the same here object identifiers are used with TSA policies CA certificates are loaded as well –

{"Ts":1530305425501,"buf":"#\\u000a# OpenSSL example configuration file.\\u000a# This is mostly being used for generation of certificate requests.\\u000a#\\u000a\\u000a# This definition stops the following lines choking if HOME isn't\\u000a# defined.\\u000aHOME\\u0009\\u ….

\\u000a\\u000a# We can add new OIDs in here for use by 'ca', 'req' and 'ts'.\\u000a# Add a simple OID like this:\\u000a# testoid1=1.2.3.4\\u000a# Or use config file substitution like this:\\u000a# testoid2=${testoid1}.5.6\\u000a\\u000a# Policies used by the TSA examples.\\u000atsa_policy1 = 1.2.3.4.1\\u000atsa_policy2 = 1.2.3.4.5.6\\u000atsa_policy3 = 1.2.3.4.5. .

2. RSA ,DSA,EC public ,private key pairs are loaded and verified

3. -exchange-sha256,diffie-hellman-group14-sha1\ – exchange

4. Bash and Tty communciation call

{"Ts":1530305817882,"args":["-bash"],"dtb":"0x000000001c4a6000","env":["LANG=en_US.UTF-8","USER=root","LOGNAME=root","HOME=/root","PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin","MAIL=/var/mail/root","SHELL=/bin/bash","SSH_CLIENT=10.0.13.13 60444 22","SSH_CONNECTION=10.0.13.13 60444 192.168.13.25 22","SSH_TTY=/dev/pts/0","TERM=xterm-256color","XDG_SESSION_ID=57","XDG_RUNTIME_DIR=/run/user/0"],"logtype":"sys_syscall","path":"/bin/bash","pid":2080,"proc_name":"sshd","pwd":"","rip":"0xffffffff815113a0","rsp":"0xffff88001bf7ff80","syscall_name":"stub_execve","syscall_nr":59,"uid":0,"vmid":"one-23458"

5. Memory trace for PVM

Ts":1530305817896,"buf":"MemTotal: 498176 kB\\u000aMemFree: 303096 kB\\u000aMemAvailable: 416528 kB\\u000aBuffers: 22040 kB\\u000aCached: 99444 kB\\u000aSwapCached: 0 kB\\u000aActive: 89756 kB\\u000aInactive: 58036 kB\\u000aActive(anon):   26620 kB\\u000aInactive(anon):   10068 kB\\u000aActive(file):   63136 kB\\u000aInactive(file):   47968 kB\\u000aUnevictable: 0 kB\\u000aMlocked: 0 kB\\u000aSwapTotal: 731132 kB\\u000aSwapFree: 731132 kB\\u000aDirty: 0 kB\\u000aWriteback: 0 kB\\u000aAnonPages: 26372 kB\\u000aMapped: 39484 kB\\u000aShmem: 10384

6. Switch from ssh to bash

{"Ts":1530305817916,"buf":"# /etc/profile: system-wide .profile file for the Bourne shell (sh(1))\\u000a# and Bourne compatible shells (bash(1), ksh(1), ash(1), ...).\\u000a\\u000aif [\\u0022`id -u`\\u0022 -eq 0]; then\\u000a PATH=\\u0022/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin\\u0022\\u000aelse\\u000a PATH=\\u0022/usr/local/bin:/usr/bin:/bin:/usr/local/games:/usr/games\\u0022\\u000afi\\u000aexport PATH\\u000a\\u000aif [\\u0022$PS1\\u0022]; then\\u000a if [\\u0022$BASH\\u0022] && [\\u0022$BASH\\u0022 != \\u0022/bin/sh\\u0022]; then\\u000a   # The file bash.bashrc already sets the default PS1.\\u000a   # PS1='\\u005ch:\\u005cw\\u005c$ '\\u000a   if [-f /etc/bash.bashrc]; then\\u000a   . /etc/bash.bashrc\\u000a   fi\\u000a else\\u000a   if [\\u0022`id -u`\\u0022 -eq 0]; then\\u000a PS1='# '\\u000a   else\\u000a   PS1='$ '\\u000a   fi\\u000a fi\\u000afi\\u000a\\u000aif [-d /etc/profile.d]; then\\u000a for i in /etc/profile.d/*.sh; do\\u000a   if [-r $i]; then\\u000a   . $i\\u000a   fi\\u000a done\\u000a unset i\\u000afi\\u000a","dtb":"0x000000001e0d5000","fd":3,"logtype":"sys_syscall","pid":2032,"proc_name":"sshd","pwd":"","return_value":761,"rip":"0xffffffff811a8ae0","rsp":"0xffff88001bf7ff80","size":761,"syscall_name":"SyS_read","syscall_nr":0,"uid":0,"vmid":"one-23458"}
{"Ts":1530305817927,"args":["id","-u"],"dtb":"0x000000001bda4000","env":["XDG_SESSION_ID=57","TERM=xterm-256color","SHELL=/bin/bash","SSH_CLIENT=10.0.13.13 60444 22","SSH_TTY=/dev/pts/0","USER=root","MAIL=/var/mail/root","PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin","PWD=/root","LANG=en_US.UTF-8","SHLVL=1","HOME=/root","LOGNAME=root","SSH_CONNECTION=10.0.13.13 60444 192.168.13.25 22","XDG_RUNTIME_DIR=/run/user/0","_=/usr/bin/id"],"logtype":"sys_syscall","path":"/usr/bin/id","pid":2094,"proc_name":"bas

h","pwd":"/root","rip":"0xffffffff815113a0","rsp":"0xffff88001ea4bf80","syscall_name":"stub_execve","syscall_nr":59,"uid":0,"vmid":"one-23458"}

7. Keystrokes pressed in bash (for pvm) are also detected

{"Ts":1530305817944,"buf":"","dtb":"0x000000001e0d5000","fd":3,"logtype":"sys_syscall","pid":2082,"proc_name":"bash","pwd":"/root","return_value":0,"rip":"0xffffffff811a8ae0","rsp":"0xffff88001bf7ff80","size":0,"syscall_name":"SyS_read","syscall_nr":0,"uid":0,"vmid":"one-23458"}