

CSCE 4555/5555 – Computer Forensics

Participation Activity 04 Assignment

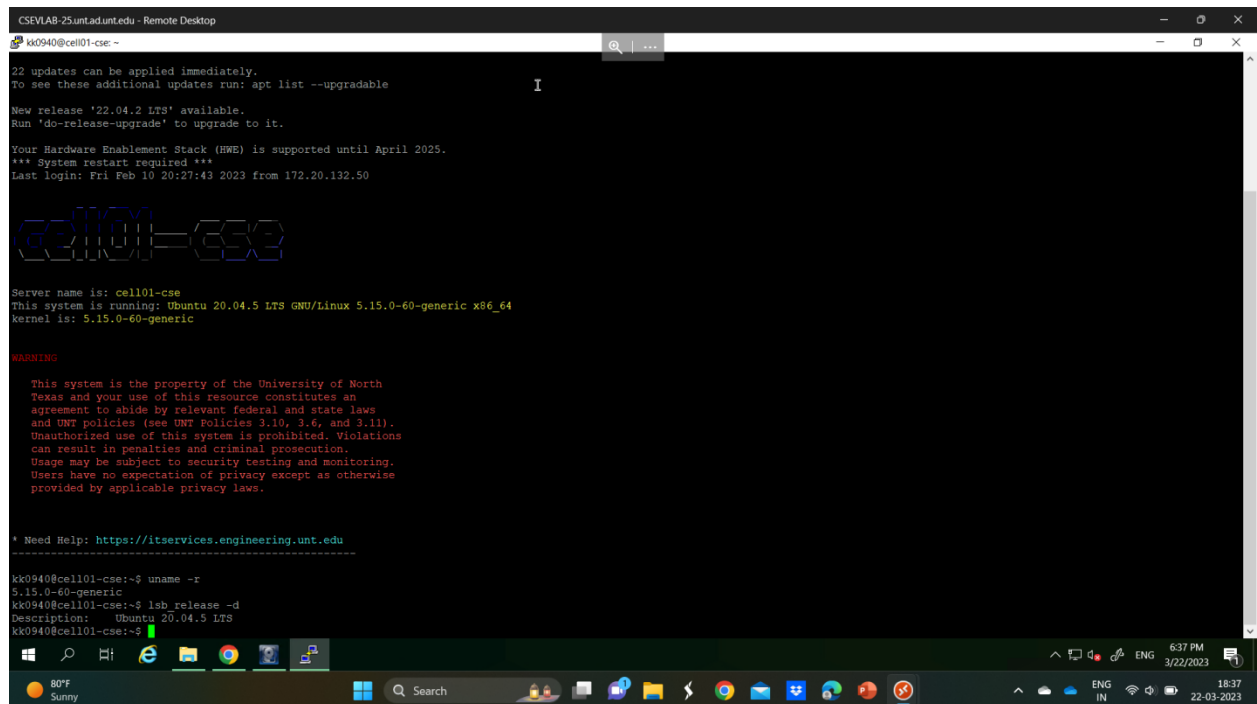
Linux System

Student ID:11647576

Linux Device and Account Information

We want to obtain some general information about our Linux CELL Servers computer.

1. Use PuTTY to login to one of our CELL machines (i.e., cell01 – cell06).
2. Enter **uname -r** to display the OS kernel version.
 - a. What is the Kernel Version of this CSE Linux Server? 5.15.0-60-generic



```
CSEVLAB-25.untad.unt.edu - Remote Desktop
k00940@cell01-cse: ~
22 updates can be applied immediately.
To see these additional updates run: apt list --upgradable
New release '22.04.2 LTS' available.
Run 'do-release-upgrade' to upgrade to it.
Your Hardware Enablement Stack (HWE) is supported until April 2025.
*** System restart required ***
Last login: Fri Feb 10 20:27:43 2023 from 172.20.132.50

cell01-cse

Server name is: cell01-cse
This system is running: Ubuntu 20.04.5 LTS GNU/Linux 5.15.0-60-generic x86_64
kernel is: 5.15.0-60-generic

WARNING

This system is the property of the University of North
Texas and your use of this resource constitutes an
agreement to abide by relevant federal and state laws
and UNT policies (see UNT Policies 3-10, 3-6, and 3-11).
Unauthorized use of this system is prohibited. Violations
can result in penalties and criminal prosecution.
Usage may be subject to security testing and monitoring.
Users have no expectation of privacy except as otherwise
provided by applicable privacy laws.

* Need Help: https://itservices.engineering.unt.edu

k00940@cell01-cse:~$ uname -r
5.15.0-60-generic
k00940@cell01-cse:~$ lsb_release -d
Description:    Ubuntu 20.04.5 LTS
k00940@cell01-cse:~$
```

3. Enter **lsb_release -d** to display the current OS version.
 - b. What is the Kernel Release of this CSE Linux Server? Ubuntu 20.04.5 LTS

CSCE 4555/5555 – Computer Forensics

```
CSEVLAB-25untad.unt.edu - Remote Desktop
k00940@cell01-cse:~$ uname -r
5.15.0-60-generic
k00940@cell01-cse:~$ lsb_release -d
Description: Ubuntu 20.04.5 LTS
k00940@cell01-cse:~$ lscpu
Architecture:          x86_64
CPU op-mode(s):        32-bit, 64-bit
Byte Order:            Little Endian
Address sizes:          43 bits physical, 48 bits virtual
CPU(s):                2
On-line CPU(s) list:   0,1
Thread(s) per core:    1
Core(s) per socket:    1
Socket(s):             2
NUMA node(s):          1
Vendor ID:              GenuineIntel
CPU family:            65
Model:                 85
Model name:             Intel(R) Xeon(R) Gold 6140 CPU @ 2.30GHz
Stepping:              4
CPU MHz:               2294.609
BogoMIPS:              4589.21
Hypervisor vendor:     VMware
Virtualization type:    full
L1d cache:             64 KiB
L1i cache:             64 KiB
L2 cache:              2 MiB
L3 cache:              49.5 MiB
NUMA node0 CPU(s):    0,1
Vulnerability Itlb multihit: KVM: Mitigation: VMX unsupported
Vulnerability L1tf:        Mitigation: PTE Inversion
Vulnerability Mds:        Mitigation: Clear CPU buffers; SMT Host state unknown
Vulnerability Meltdown:   Mitigation: PTI
Vulnerability Mmio stale data: Mitigation: Clear CPU buffers; SMT Host state unknown
Vulnerability Retbleed:   Mitigation: IBRS
Vulnerability Spec store bypass: Mitigation: Speculative Store Bypass disabled via prctl and seccomp
Vulnerability Spectre v1: Mitigation: usercopy/swapgs barriers and __user pointer sanitization
Vulnerability Spectre v2: Mitigation: IBRS, IBPB conditional, RSB filling, PBSRB-eIBRS Not affected
Vulnerability Srbds:      Not affected
Vulnerability Tsx async abort: Not affected
Flags:                    fpu vme de pse tsc msr pae mce cx8 apic sep mtrr pge mca cmov pat pse36 clflush mmx fxsr sse sse2 ss syscall nx pdpe1gb rdtscp lm constant tsc arch_perfmon
nopl xtopology tsc_reliable nonstop_tsc cpuid tsc_known_freq pni pclmulqdq ssse3 fma cx16 pcid sse4_1 sse4_2 x2apic movbe popcnt tsc_deadline_timer aes xsave
e avx f16c rdrand hypervisor lahf_lm ahm 3dnowprefetch invpcid_single pti ssbd ibrs ibpb stibp fsgsbase tsc_adjust bmi1 avx2 smep bmi2 invpcid avx512f avx51
2dq rdseed adx smap clflushopt clwb avx512cd avx512bw avx512vl xsaveopt xsavec xsavec_arat pkus ospke md_clear flush_l1d arch_capabilities

k00940@cell01-cse:~$
```

4. Enter **lscpu** to display system information about the CSE Linux Server.

c. How many CPUs does the CELL Linux Server? 2

```
CSEVLAB-25untad.unt.edu - Remote Desktop
k00940@cell01-cse:~$ uname -r
5.15.0-60-generic
k00940@cell01-cse:~$ lsb_release -d
Description: Ubuntu 20.04.5 LTS
k00940@cell01-cse:~$ lscpu
Architecture:          x86_64
CPU op-mode(s):        32-bit, 64-bit
Byte Order:            Little Endian
Address sizes:          43 bits physical, 48 bits virtual
CPU(s):                2
On-line CPU(s) list:   0,1
Thread(s) per core:    1
Core(s) per socket:    1
Socket(s):             2
NUMA node(s):          1
Vendor ID:              GenuineIntel
CPU family:            65
Model:                 85
Model name:             Intel(R) Xeon(R) Gold 6140 CPU @ 2.30GHz
Stepping:              4
CPU MHz:               2294.609
BogoMIPS:              4589.21
Hypervisor vendor:     VMware
Virtualization type:    full
L1d cache:             64 KiB
L1i cache:             64 KiB
L2 cache:              2 MiB
L3 cache:              49.5 MiB
NUMA node0 CPU(s):    0,1
Vulnerability Itlb multihit: KVM: Mitigation: VMX unsupported
Vulnerability L1tf:        Mitigation: PTE Inversion
Vulnerability Mds:        Mitigation: Clear CPU buffers; SMT Host state unknown
Vulnerability Meltdown:   Mitigation: PTI
Vulnerability Mmio stale data: Mitigation: Clear CPU buffers; SMT Host state unknown
Vulnerability Retbleed:   Mitigation: IBRS
Vulnerability Spec store bypass: Mitigation: Speculative Store Bypass disabled via prctl and seccomp
Vulnerability Spectre v1: Mitigation: usercopy/swapgs barriers and __user pointer sanitization
Vulnerability Spectre v2: Mitigation: IBRS, IBPB conditional, RSB filling, PBSRB-eIBRS Not affected
Vulnerability Srbds:      Not affected
Vulnerability Tsx async abort: Not affected
Flags:                    fpu vme de pse tsc msr pae mce cx8 apic sep mtrr pge mca cmov pat pse36 clflush mmx fxsr sse sse2 ss syscall nx pdpe1gb rdtscp lm constant tsc arch_perfmon
nopl xtopology tsc_reliable nonstop_tsc cpuid tsc_known_freq pni pclmulqdq ssse3 fma cx16 pcid sse4_1 sse4_2 x2apic movbe popcnt tsc_deadline_timer aes xsave
e avx f16c rdrand hypervisor lahf_lm ahm 3dnowprefetch invpcid_single pti ssbd ibrs ibpb stibp fsgsbase tsc_adjust bmi1 avx2 smep bmi2 invpcid avx512f avx51
2dq rdseed adx smap clflushopt clwb avx512cd avx512bw avx512vl xsaveopt xsavec xsavec_arat pkus ospke md_clear flush_l1d arch_capabilities

k00940@cell01-cse:~$
```

d. What is the Model Name of the processor for all CPUs? Intel (R) Xeon (R) Gold 6140 CPU @ 2.30GHZ

CSCE 4555/5555 – Computer Forensics

```
CSEVLAB-25untad.unt.edu - Remote Desktop
kk0940@cell101-cse:~$ uname -r
5.15.0-60-generic
kk0940@cell101-cse:~$ lsb_release -d
Description: Ubuntu 20.04.5 LTS
kk0940@cell101-cse:~$ lscpu
Architecture:          x86_64
CPU op-mode(s):        32-bit, 64-bit
Byte Order:             Little Endian
Address sizes:          43 bits physical, 48 bits virtual
CPU(s):                 2
On-line CPU(s) list:    0,1
Thread(s) per core:     1
Core(s) per socket:     1
Socket(s):              2
NUMA node(s):           1
Vendor ID:              GenuineIntel
CPU family:             65
Model:                  85
Model name:             Intel(R) Xeon(R) Gold 6140 CPU @ 2.30GHz
Stepping:               4
CPU MHz:                2294.609
BogoMIPS:               4589.21
Hypervisor vendor:      VMware
Virtualization type:    full
L1d cache:              64 KiB
L1i cache:              64 KiB
L2 cache:               2 MiB
L3 cache:               49.5 MiB
NUMA node0 CPU(s):      0,1
Vulnerability Itlb multihit: KVM: Mitigation: VMX unsupported
Vulnerability L1tf:        Mitigation: PTE Inversion
Vulnerability Mds:         Mitigation: Clear CPU buffers; SMT Host state unknown
Vulnerability Meltdown:    Mitigation: PTI
Vulnerability Mmio stale data: Mitigation: Clear CPU buffers; SMT Host state unknown
Vulnerability Retbleed:    Mitigation: IBRS
Vulnerability Spec store bypass: Mitigation: Speculative Store Bypass disabled via prctl and seccomp
Vulnerability Spectre v1:  Mitigation: usercopy/swapgs barriers and __user pointer sanitization
Vulnerability Spectre v2:  Mitigation: IBRS, IBPB conditional, RSB filling, PBSRB-eIBRS Not affected
Vulnerability Srbds:       Not affected
Vulnerability Tsx async abort: Not affected
Flags:                     fpu vme de pse tsc msr pae mce cx8 apic sep mtrr pge mca cmov pat pse36 clflush mmx fxsr sse sse2 ss syscall nx pdpe1gb rdtscp lm constant tsc arch_perfmon
nopl xtopology tsc_reliable nonstop_tsc cpuid tsc_known_freq pni pclmulqdq ssse3 fma cx16 pcid sse4_1 sse4_2 x2apic movbe popcnt tsc_deadline_timer aes xsave
e avx f16c rdrand hypervisor lahf_lm abm 3dnowprefetch invpcid_single pti ssbd ibrs ibpb stibp fsgsbase tsc_adjust bmi1 avx2 smep bmi2 invpcid avx512f avx51
2dq rdseed adx smap clflushopt clwb avx512cd avx512bw avx512vl xsaveopt xsavec xsavec_arat pkus ospke md_clear flush_lld arch_capabilities
```

5. Use the **lsblk** command with various options to find the following information about the hard drive.

e. How many partitions does the **sda** hard drive have?

3

```
CSEVLAB-25untad.unt.edu - Remote Desktop
kk0940@cell101-cse:~$ lsblk
NAME MAJ:MIN RM SIZE RO TYPE MOUNTPOINT
sda 8:0 0 250G 0 disk
├─sda1 8:1 0 512M 0 part /boot/efi
├─sda2 8:2 0 1K 0 part
└─sda5 8:5 0 249.5G 0 part /
sr0 11:0 1 1024M 0 rom
```

f. Which **sda** partition contains the boot block?

Sda1

g. For each of the partitions found in e., identify the file system (be sure to list each partition and its associated file system). If you are not able to find the file system for

CSCE 4555/5555 – Computer Forensics

all of the partitions, you may use the `fsck -N` command with the specific partition to obtain this information.

Vfat,ext2,ext4

```
CSEVLAB-25.untad.unt.edu - Remote Desktop
kk0940@cell01-cse:~$ cat /etc/passwd
Steppling: 4
CPU MHz: 2294.609
BogoMIPS: 4589.21
Hypervisor vendor: VMware
Virtualization type: full
L1d cache: 64 KiB
L1i cache: 64 KiB
L2 cache: 2 MiB
L3 cache: 49.5 MiB
NUMA node0 CPU(s): 0,1
Vulnerability Itlb multihit: KVM: Mitigation: VMX unsupported
Vulnerability Itlb: Mitigation: PTE Inversion
Vulnerability Mds: Mitigation: Clear CPU buffers; SMT Host state unknown
Vulnerability Meltdown: Mitigation: PTI
Vulnerability Mmio stale data: Mitigation: Clear CPU buffers; SMT Host state unknown
Vulnerability Retbleed: Mitigation: IBRS
Vulnerability Spec store bypass: Mitigation: Speculative Store Bypass disabled via prctl and seccomp
Vulnerability Spectre v1: Mitigation: usercopy/swapgs barriers and __user pointer sanitization
Vulnerability Spectre v2: Mitigation: IBRS, IBPB conditional, RSB filling, PBRSB-eIBRS Not affected
Vulnerability Srbds: Not affected
Vulnerability Tsx async abort: Not affected
Flags: fpu vme de pse tsc mtr pae mce cx8 apic sep mtrr pge mca cmov pat pse36 clflush mmx fxsr sse sse2 ss syscall nx pdpe1gb rdtscp lm constant_tsc arch_perfmon
nopl xtopology tsc_reliable nonstop_tsc cpuid tsc_known_freq pni pclmulqdq ssse3 fma cx16 pcid sse4_1 sse4_2 x2apic movbe popcnt tsc_deadline_timer aes xsave
e_ux fl6c rdrand hypervisor lahf_lm abm 3dnowprefetch invpcid_single pti ssbd ihps stibp fsgsbase tsc_adjust bml avx2 smep bml2 invpcid avx512f avx51
2dq rdseed adx smap clflushopt clwb avx512cd avx512bw avx512vl xsaveopt xsavec xsavec arat pku ospke md_clear flush_lld arch_capabilities

kk0940@cell01-cse:~$ lsblk
NAME MAJ:MIN RM SIZE RO TYPE MOUNTPOINT
sda 8:0 0 250G 0 disk
├─sda1 8:1 0 512M 0 part /boot/efi
├─sda2 8:2 0 1K 0 part
└─sda5 8:5 0 249.5G 0 part /
sr0 11:0 1 1024M 0 rom

kk0940@cell01-cse:~$ fsck -N /dev/sda
fsck from util-linux 2.34
[/usr/sbin/fsck.ext2 (1) -- /dev/sda] fsck.ext2 /dev/sda
kk0940@cell01-cse:~$ fsck -N /dev/sda1
fsck from util-linux 2.34
[/usr/sbin/fsck.vfat (1) -- /boot/efi] fsck.vfat /dev/sda1
kk0940@cell01-cse:~$ fsck -N /dev/sda2
fsck from util-linux 2.34
[/usr/sbin/fsck.ext2 (1) -- /dev/sda2] fsck.ext2 /dev/sda2
kk0940@cell01-cse:~$ fsck -N /dev/sda5
fsck from util-linux 2.34
[/usr/sbin/fsck.ext4 (1) -- /dev/sda5] fsck.ext4 /dev/sda5
kk0940@cell01-cse:~$
```

You are to submit this document with your answers to the **Participation Activity 4** dropbox on Canvas by the due date and time. **No late submissions will be accepted.**