**CSE 523S System Security**

**Studio 1: Getting to know our systems**

Security work often requires system knowledge. In this studio, we will create a reference sheet we can use when working on future studios and homework assignments. Provide the appropriate Linux shell command(s) for each desired task below (i.e., the command-line interface command, NOT a graphical user interface procedure). Please do your best to answer as many as possible on your own, but note that you may also ask for help in class or on Piazza if you get stuck.

There are no restrictions on resources that can be used to answer questions. This studio will be graded for completeness rather than correctness.

The “Windows” column is optional.

|  |  |  |  |
| --- | --- | --- | --- |
| **#** | **How do I...** | **… in Linux?** | **… in Windows?** |
| 1 | List directory contents? | ls  dirs | dir |
| 2 | Find my machine name? | hostname  hostnamectl | hostname |
| 3 | Start an admin console session? | sudo bash  sudo -i  su [user] | Right click on powershell or cmd run by administrator |
| 4 | Find which processes use the most CPU or memory? | top (use P or M to sort)  htop (should install) | Use task manager |
| 5 | Stop/Kill a process? | kill -9 [process pid] pkill -9 [process name]  killall -9 [process name] | Use task manager  taskkill |
| 6 | Find out how much disk space is free? | df -h  du -sh [directory]  lsblk | Enter computer and see |
| 7 | Find out who is logged in? | who, whoami, users, w  last | Use task manager user page |
| 8 | Find a log of recent logins and login attempts? | last, lastb  last -i [username] | Event Viewer & check login events |
| 9 | Find my IP and MAC addresses? | ifconfig | ipconfig |
| 10 | Examine my OS name and version? | lsb\_release -a | systeminfo |
| 11 | Find kernel version? | uname -r | systeminfo |
| 12 | Examine which programs run at system boot time? | systemctl list-unit-files --type=service (enabled) | taskschd.msc |
| 13 | Stop a program from running at system boot time? | systemctl disable [service\_name] | Task Manager -> startup -> disable  Taskchd.msc |
| 14 | Find the list of trusted certificates installed on my system? | ls /etc/ssl/certs |  |
| 15 | Remove a trusted certificate from my system? | sudo rm /etc/ssl/certs/[certificate-file].pem |  |
| 16 | Compile my program? | gcc, | Mingwin gcc |
| 17 | Display an object file? | objdump  readelf |  |
| 18 | Start gdb? | gdb [program] | N/A |
| 19 | (within gdb): Set a breakpoint? | break [function name]  break [file]:[line] | N/A |
| 20 | (within gdb): Show registers information? | info register [register name]  info all-registers | N/A |
| 21 | (within gdb): Present stack values? | bt or backtrace | N/A |
| 22 | (within gdb): Read stack content (explain in words)? | Frame [m] |  |
| 23 | Examine the program structure without the source file (explain in words)? | file + readelf or objdump + nm + gdb |  |
| 24 | List all open network connections? | netstat -at  ss -tunlp  lsof |  |
| 25 | Find the process responsible for each open network connection? | ss -tunlp  netstat -tunlp  lsof |  |
| 26 | Find the binary executable responsible for each open network connection? | lsof  ls -l /proc/[PID]/exe |  |
| 27 | Reset my network interface? | ifconfig down/up |  |
| 28 | Find my default IP gateway? | ip route show default  netstat -rn |  |
| 29 | Find my default name server? | cat /etc/resolv.conf  resolvectl status |  |
| 30 | Examine contents of the ARP cache? | arp -a ip neigh |  |
| 31 | Add an entry to the ARP cache? | arp -s [ip] [mac]  ip neigh add |  |
| 32 | Examine contents of the DNS cache? | dig @localhost [domain] |  |
| 33 | Make a local DNS query respond with an IP of my choosing? | dnsmasq  bind |  |
| 34 | Open my favorite command-line editor? | vi, vim |  |
| 35 | Bring the most recent suspended job to the foreground? | jobs  fg |  |
| 36 | List and resume stopped jobs in the background? | jobs  bg |  |
| 37 | List files opened by processes? | lsof |  |