**CIS 4391 Homeworks – Spring 2020**

**NOTE:** In order to receive credit for these homeworks, it is necessary to correctly complete each step as listed below. With each homework you submit,

* **print out the report pages required in the instructions**
* **print out the matching homework descriptions page,**
* **showing that you have checked off each of the required items**.
**NOTE:** These homeworks are preferably to be completed on your own network-connected computer connected to broadband service.

**ETHICS Responsibility Statement DUE 1/15/2020**

**As a group, research and craft a statement describing lawful and ethical practice of information security. List your names, sign, and submit.**

**TEAMS Participation Statement DUE 1/15/2020**

**As a group, develop a statement describing fair, equitable and effective procedures for working as a team. Include shared workload, meeting processes, response to communications, etc. List your names, sign, and submit.**

**HW1 .** **Generate a Windows “Security Center” report.** **DUE 1/20/2020**

1. **Win 10** - Control Panel - Security and Maintenance - Security - you have to click on 'Security' to expand that section, so you can see that firewall and anti-virus are active. On my current setup with UTRGV there is a further link ‘View in Windows Security’. If that is present, click on that to see the actual information, and use those screens for your printouts. You must demonstrate that BOTH virus protection and firewall protection are working and present.

**Print Report part 1 – If you have no warnings, then your hw is complete. Otherwise, continue:**

1. If Windows gives you any warnings, follow the instructions to make sure your computer is properly protected. For example, you may be running your own firewall instead of Windows firewall, which is OK – Get the screenshot showing that Windows firewall is off, plus a shot of the firewall you’re running instead, from your security application software. (If your computer shows that Windows firewall is off, but you \*don’t\* have another firewall, then turn Windows firewall ON!)

**Print Report part 2**, showing that all components are present and functioning.

1. Label each page, including title (copy/paste from above), and your name on each sheet. Number your sheets using "X of Y" format: "1 of 2", "2 of 2", etc. **Staple in order and turn in hard copy**.

**HW2. Ports Self-Scan – Due 1/22/2020**
1) Navigate to the ShieldsUP tool in <http://www.grc.com/intro.htm> , 'Services' tab, 'ShieldsUp!'

2) Read the “If you are new” box, then click ‘Proceed’

3) Run the File Sharing scan and read the report.
3) **Print scan results as page 1**
4) Run the Common Ports scan and read the report.
5) **Print scan results as page 2**
6) Run the All Service Ports scan
7) **Print scan results as page 3, plus:** For 3 warnings (red), **Write your own mini-report-3 paragraphs**.

For each warning:
 a) Identify port #, associated service (click directly on the red square for information)
 b) Identify vulnerability or security problem for that port
 c) Identify a potential attack against that port/service

**If your scan comes back all green, go back to the Common Ports scan, and click on three numbers that look interesting to use in your written mini-report**.

Your completed hw includes **three scans**, and your own written **mini-report**.

**HW3. Malicious Software Removal Scan – Due 1/27/2020**
o Navigate to Microsoft Download Center: <https://www.microsoft.com/en-us/download/details.aspx?id=9905>

o Download the “malicious software removal tool” IN MICROSOFT SITE ONLY. There are different versions, one of which is for 64-bit systems (x64); select the one appropriate for your system. This time mine was Windows-KB890830-x64-V5.78.exe, but the exact name and version # may change.
o Click link, go to software download page. Microsoft will suggest some extra things to download; I always click 'No Thanks'.
o Download software - Make sure it's correct for your system OS version and bus (32-bit or 64-bit)

o Run the tool using ‘Quick Scan’
o **\*While the tool is running**\*, hit <Print Screen> key to capture an image of it in action
o **Print the screenshot image as page 1**
o When tool is finished, use Print-Screen again to capture image of overall results.
o Click on “View detailed results”, use Print-Screen to capture image of the top of this list
You need NOT scroll down to print **all** the results – just the first 16 is OK.
o **Print the screenshot image of “View detailed results” as page 2**

**HW4. Windows Updates Information Due Feb 3

1. COMPLETE THIS HOMEWORK ON A NON-UTRGV PC.**

**2. In an administrator account logon, go to the Start button on lower left, click the gear symbol to access ‘Settings’, click on ‘Update & Security’, then click on ‘Windows Update’.**

**\*\*\*NOTE\*\*\* Do not click on the ‘Check for Updates’ button unless you are prepared to actually update at this time.**

**3. Click on ‘View Update History’. You will see a reverse chronological list of your installed updates of all kinds. SCREENSHOT AND PRINT this view (viewed in full screen, you should be able to see about 8 updates). HIGHLIGHT OR CIRCLE THE SECURITY UPDATES.**

**4. Open the Control Panel. In Category View, click on ‘Programs’. In the center pane, under the heading ‘Programs and Features’, click on ‘View installed updates’.**

**5. The window that opens next is called ‘Installed Updates’; the heading in the center pane is ‘Uninstall an update’. \*\*\*DO NOT UNINSTALL ANY UPDATES\*\*\*.**

 **SCREENSHOT AND PRINT this window. HIGHLIGHT OR CIRCLE THE SECURITY UPDATES.**

**6. The Security Updates for Microsoft Windows have version numbers. Last year I received update KB4480966, installed on 1/11/2019. Find your latest security update for Windows, copy the update number. Microsoft provides a support webpage online for each release. The URL is:**[**http://support.microsoft.com/help/##**](http://support.microsoft.com/help/)**, where ## is the digits from your update.
My support page was thus** [**http://support.microsoft.com/help/4480966**](http://support.microsoft.com/help/4480966)

**7. Go to the support page for your latest security update for Windows. SCREENSHOT AND PRINT this page.**

**MARK AND LABEL:**

1. **The release date**
2. **The OS build number**
3. **The Operating System version (mine is Windows 10, version 1803)**

**HW 5 Software Applications Updates Due February 10**

1. **Go to** [**https://www.kcsoftwares.com/?sumo**](https://www.kcsoftwares.com/?sumo)
2. **You should be on the page for their free software update monitor software. Download and install the utility. NOTE: When I install, I nearly always UNCHECK the box for ‘Quick Launch’, which preloads the program into RAM at startup. **
3. **Once installed it will appear in your ‘All programs’ list as a plain folder called ‘KC Softwares’, with the program ‘SUMo’ in that folder. Click the program to start it. You will see the basic window with all functions.**

****

**The first time I ran it the ‘wizard’ opened. Close the wizard.**

****

**Click on the ‘Check’ button which you see highlighted in blue outline in the SUMo image above.
SUMo will go through all your applications and try to figure out if you have the latest version or not. This may take a few minutes. You can see in the image on the last line of the report, that it is giving me a minor warning about Firefox.**

**SCREENSHOT AND PRINT your results.**

**SUMo will probably list your programs from top to bottom in what it considers the most critical to the least critical. I have clicked on the ‘Product’ column heading to list mine in ascending alphabetical order.**

**If NONE of your programs are out of date, then you are done, and please accept my hearty congratulations, because 100% up to date is rare.**

1. **If you DO have programs that need updating, MARK AND LABEL a program you intend to update, with the version number you currently have either highlighted or circled. For example, my copy of Firefox was out of date with version 72.0.1.**

**At this point, the free version of SUMo does not help: although there is a ‘Get Update’ button at the top, and you also have various options when you right-click on the file, SUMo will mostly just tell you to buy SUMo Pro.**

**Instead, go to the original maker’s website, and update your application.**

**For my result above, I went to mozilla.org to get the latest copy of Firefox.**

**NOTE: In general, you should try to always obtain your software copies ONLY from the original maker, or a trusted supplier. My only two trusted suppliers right now that are not the original makers are UTRGV, and download.com**

1. **Once your update is finished, run SUMo ‘Check’ again. The output webpage with results now shows that the latest version of Firefox is 72.0.2, and I have a green checkmark indicating that this is the newest version SUMo knows about.**

**SCREENSHOT AND PRINT your follow-up results. MARK AND LABEL your printout to indicate the same program – it should now have a green checkmark. Highlight the version number, which should be different from your first printout.**

**HW6. Data Execution Prevention - Due Feb 10**

* Turn ON Data Execution Prevention. This option is located at:

Control Panel (view by icons) - System - Advanced System Settings (on left) -

In System Properties pop-up, select Advanced tab - Peformance area 'Settings' button -

Data Execution tab.

* Turn on DEP "for all programs and services except those I select". Screen capture showing that this option is selected and **PRINT.**
* Use the "Add…" button to add an exception for a program. Screen capture and **PRINT** to show the new exception.
	+ **NOTE – You will need to find a 32-bit .exe to do this part with.** If you have an older computer, you shouldn't hit any snags.
	+ If you're running a 64-bit machine, then you need to look for your 32-bit applications [left as an exercise for the student, to find where they are].
	+ You don't have to do Notepad.exe specifically, just choose something that works, add the exception, and get your screenshot.
* Remove the exception, Apply, OK, and Close.

**HW7. Hands-On Project – Network Connections Due Feb 12**

**NOTE: This is \*very\* detailed work, cross-matching information by hand. Read through carefully and make sure you understand each piece before creating your report and submitting.**

* Open one browser window, navigate to some favorite website—which one does not matter.
* Open a DOS window [OR, a Powershell window], type ‘netstat –ano’ (Don’t forget the space and the hyphen)
Make sure your DOS window is open long enough to show all entries; screen capture that image (of the DOS window results only, not the whole Desktop) and **Print. \*\*\*Make sure you get all the DOS entries, there may be a lot\*\*\*.**
* Look at the ‘State’ column and notice which entries are Listening or Established—these entries are open ports on your system. The port # is the last part of the “Local Address”.
* Look at the PID column to see which Process ID #’s are associated with each entry.
* Open Task Manager
	+ Click on the Details Tab.
	Combine this information:
	In your Word document, **create a table** of **four** columns listing the following:
	# of the **port** that is in State either “LISTENING” or “ESTABLISHED” (from netstat)

IMPORTANT: Do **NOT** use a line for which the ‘Foreign Address’ is

 **0.0.0.0**

 Or

 **127.0.0.1**

These are basic addresses just for internal and LAN housekeeping purposes. You want a true external address out there on the Internet. Scroll down to find some.
**Process ID** (from netstat) that is on that port (Task Manager)
**Name** (from Task Manager) that is executing on that PID (Task Manager)
**User Name** (from Task Manager) that is using that Process (Task Manager)

* You only need to report on the Ports that are LISTENING or ESTABLISHED. Focus on the ones which are to external servers. If you have more than 10, you can stop there.
* **Print** your Table of reported ports and processes, hand in **all** Printouts.

**HW 8 – Firewalls – DUE Feb 17 2020**

1. FOR WIN7 / WIN 10 –
	1. Open Control Panel - Windows Firewall to open the “Windows Firewall” box.
	2. Click on 'Turn Windows [or Windows Defender] Firewall on or off'
		1. **Screen capture and print** the image of the window (Windows Firewall ON)
	3. EXTRA CREDIT: If you are running a third-party firewall such as Comodo or ZoneAlarm, open the interface for that tool and demonstrate that it is on and working, then **Screen capture and print that screen** instead.
	4. Go back to Windows Firewall home (Ctl Panel – Windows [Defender] Firewall)
	5. Click on 'Allow a program or feature through Windows firewall'
	6. . **Screen capture and Print** the image of this “Allow Programs” window view. You may have a scroll bar; it is impossible to show all of a long list of exceptions at once, so just stay scrolled to the top and print what is visible.
	7. Click the "Allow another program” [Allow an app or feature] link. In the pop-up which appears, Click 'browse' to find "Notepad.exe" (C:, Windows, System32). Click 'Open' in the Browse pop-up to put Notepad in the Add list.
	8. In the "Add a Program" pop-up, make sure Notepad is highlighted. Click "Add".
	9. In the "Allowed Programs" window, scroll down far enough to make sure Notepad is visible. **Screen capture and print** the new image of the box. **Highlight the line with the Notepad exception on your printout.**
	10. With the Notepad line still selected, click 'Remove' to remove this exception.
	NOTE: In updated Windows Firewall, I have to go to “Advance Settings”, “Inbound Rules”, find the Notepad rules there, and right-click on each one to be able to delete it.

10 Points extra credit for doing this homework successfully in Comodo firewall instead of Windows.

**HW9. Logon Events Auditing Project – Due Feb 17 2020**

* Start WinXP Pro, either native, or **in your virtual machine**
* Go to Control Panel – Administrative Tools
* Double-click the “Local Security Policy” icon
* In the left pane, click the + next to “Local Policies” to expand it
* In the left pane, click “Audit Policy”
* In the right pane, look for “Audit account logon events”
* Double-click this entry to open the properties pop-up, and check the boxes next to both "Success" and “Failure”. Click "Apply" and "OK
* Repeat the procedure for "Audit logon events"
* Do a **SCREEN CAPTURE AND PRINT** to show the “Local Security Settings” window with the Security Setting for "Audit Account Logon Events" and "Audit Logon Events" **highlighted**, showing that the logon Success and Failure events will be audited.
* Close the "Local Security Settings", Administrative Tools and Ctl Panel windows
* Stay booted up, but Log Off.
* Do a couple of wrong logons on purpose, using non-existent account names. Then logon correctly.
* Go to Ctl Panel, Administrative Tools, Computer Management, System Tools, Event Viewer, Security. **HIGHLIGHT** THE ENTRIES REPRESENTING YOUR FAILED AND SUCCESSFUL LOGON. **Screen Capture, Print.**

**HW10. Packet Sniffing, Due Feb 19, 2019**

□ NOTE: If you are doing this homework on the lab computers you may skip the next four steps. If you are doing it on your own computer (recommended), you may do the next steps for EITHER or BOTH of your Ethernet and Wireless NIC’s. The main requirement here is to be able to capture packets.
□ On the Internet, go to <http://www.download.com> and download the Wireshark installer. Install it.
□ Wireshark’s installer should notice if you don’t have WinPcap, and ask to install it. If not, then go to <http://www.download.com/> and download the WinPcap installer. Install it.
□ On your own computer, open Control Panel – System – Hardware tab – Device Manager. In the list of devices, click the ‘plus’ box next to ‘Network Adapters’. Use the headings which appear to identify the precise brand and model of your wireless network adapter.
□ Double-click on the wireless adapter – Driver tab, in order to view the driver version you are using. On the Internet, navigate to your NIC manufacturer’s website and check for the latest driver. If there is a newer one than you are using, download it and install it. NOTE: Notice that in the Device Manager view of your NIC, you can roll back your driver later if you wish to the previous version you were using.
□ **Now you are ready to capture data packets**. Connect to the Internet, open a DOS window and run ipconfig /all, **Screen capture and print your output.** You will want to know your current IP address so that you can use it in your packet inspections.
□ Start the Wireshark program. Click on Capture menu – Interfaces. In the pop-up you will likely see several options. Look for the entry for the device you are currently using for Internet access, either Ethernet or wireless adapter. NOTE: Avoid websites with streaming content during this homework. Click the ‘Start’ button on the right to begin capturing packets.
□ Navigate [http://www.raymondville-chronicle.com/](http://www.raymondville-chronicle.com/%20) You should see a lot of packets arriving in Wireshark.
□ NOTE: If you fail to capture any packets, check to see that you have selected the right NIC. If you still have no packets, click the 4th icon from the left (with the tiny red circle with ‘X’) to stop the current capture. Click ‘OK’ on the popup. Click Capture menu – Options, and make sure that the box labeled ‘Capture packets in promiscuous mode’ is NOT checked (your NIC driver may or may not support this mode.) Click ‘Start’ at the bottom right. You should now be able to capture packets arriving at your NIC.
□ In the far upper left corner of the Raymondville Chronicle website, click “Login”. In the form which appears, type ‘JOHNSMITH’ for the Member ID, and ‘MYSECRETPASSWORD’ for the password. Click the ‘Log in’ button.
□ Raymondville-Chronicle.com will come back with a message saying that the password you entered was not recognized. Go back to your Wireshark window and stop the packet capture. (Capture menu – Stop, or click the 4th icon from the left).
□ In Wireshark, make sure your scroll bar is at the top of the packets listing pane. Click Edit menu – Find Packet. In the pop-up window, select the radio button ‘String’ under the By: heading. In the Filter field, type ‘JOHNSMITH’ (without the quotes—just as you entered it for the web form). Click the ‘Find’ button. [Another way to do this is to search for the packet whose ‘Info’ entry on the right starts with the text ‘POST’].
□ In the top pane containing the chronological list of packets captured, the packet you were searching for will be selected. Use the mouse to click and drag to open up the center pane of the display, if necessary. Click on the +- boxes on the left of each item to open and close that item, and see the information it provides. The last item should be labeled ‘Line-based text data’. Click on that label. Click on the + to open that item, and click on the label.
□ As you do, you will see that part of the packet content highlighted in the bottom pane. In both the middle and bottom panes you should be able to read, in clear text, not only your Member ID ‘JOHNSMITH’, but also “MYSECRETPASSWORD’, sent over the Internet unencoded. **Screen capture and print the Wireshark output as it now appears. Use a highlighter to highlight the ID and password text, or a colored pen to circle them, in both panes**.
□ In the top pane, look at the ‘Source’ and ‘Destination’ columns to figure the IP address from which Raymondville-Chronicle.com was sending you packets. Write down this number.
□ Click Analyze menu – Display Filters. Click the ‘+’ button on the left to add a new filter. The ‘Filter string’ input field is highlighted pink. Type ‘ip.addr == ‘ (without the quotes, and use a double equals sign), followed by the IP address you discovered in the previous step. In the ‘Filter name’ input field, type ‘Raymondville-Chronicle.com’. **Screen capture and print the image of the ‘Display Filter’ box, showing your entry.** Click ‘OK’ to apply the filter.
□ The top pane now shows ONLY packets for which the Raymondville-Chronicle.com IP address is either the source or the destination. In the top pane, click on the word ‘Source’ to sort on that column. Each click will toggle a sort Ascending or Descending. Sort that column Descending, so that the list of packets begins with all the packets for which Raymondville-Chronicle.com was the Source. **Screen capture and print (entire screen)**. Click ‘Clear’ near the top of the screen to remove the filter.
□ In the Wireshark interface, click Statistics menu – IPv4 address…(near the bottom of the drop-down list. Choose "All addresses". The pop-up box that results shows all the IP addresses contacted during your session, with some simple statistics. If the whole list is not showing, click to the left of “All addresses” to expand the entry and show all the entries. **Screen capture and print the image of the pop-up box showing all your statistics**.