CSCI 4174/CSCI 6708 NETWORK SECURITY: ASSIGNMENT NO. 1
Date Given: Sunday, January 21, 2018
Date Due: Saturday, February 3, 2018, 11.55 PM
Submission: On Brightspace (dal.ca/brightspace)

NOTES:

1. It is very important that you use the network tools that you download only for collecting information about your own machine or a self-contained private network. Never use any of the tools for unethical purposes. It may result in your account being suspended and further actions being taken.
2. All references must be properly cited in your answers. Use IEEE or ACM reference styles (https://www.ieee.org/documents/ieeecitationref.pdf) (https://www.cs.ucy.ac.cy/~chryssis/specs/ACM-refguide.pdf) . Points will be deducted for improper citations and citations in incorrect formats.
3. Keep in mind that just because you cite references, you must not "cut-and-paste" from these or other sources. The write-up must be properly paraphrased and referenced.
4. **Late Penalty Policy**: 10% per day on the mark earned on the assignment. For instance, if your score on the assignment is 8/10 and it is one day late, the score will be reduced to 7.2/10. Assignments that are five days past due will not be accepted.
5. **Submission**: Convert your documents into pdf. Submit ONE zip file containing the answers to all questions on Brightspace.

Exercise 1 (Experimentation): Information gathering is an important step in a hacker's attempt to launch an attack. A number of network administration tools can be used for this purpose. One such tool that we discussed in class is Wireshark.

a) Download Wireshark (http://www.wireshark.org/download.html) and understand its features.
b) Connect to a website such as http://www.google.ca and use Wireshark to sniff the packets. Get the screen dump of the Wireshark capture.
c) Using the screen dump, describe in detail all the steps that your browser goes through when you connect to the web site. You should describe which protocols are invoked (e.g., TCP, ARP, DNS, etc.), their parameters (e.g., port numbers, addresses), and the network entities (e.g., DNS server, default gateway/router).

Note: Clear your machine's arp tables before clicking on the web page link, use information from ipconfig/ifconfig, route, etc.
Length of the report: Approximately 2 pages including the screen snapshot and description, single line spacing, 11-point font size.

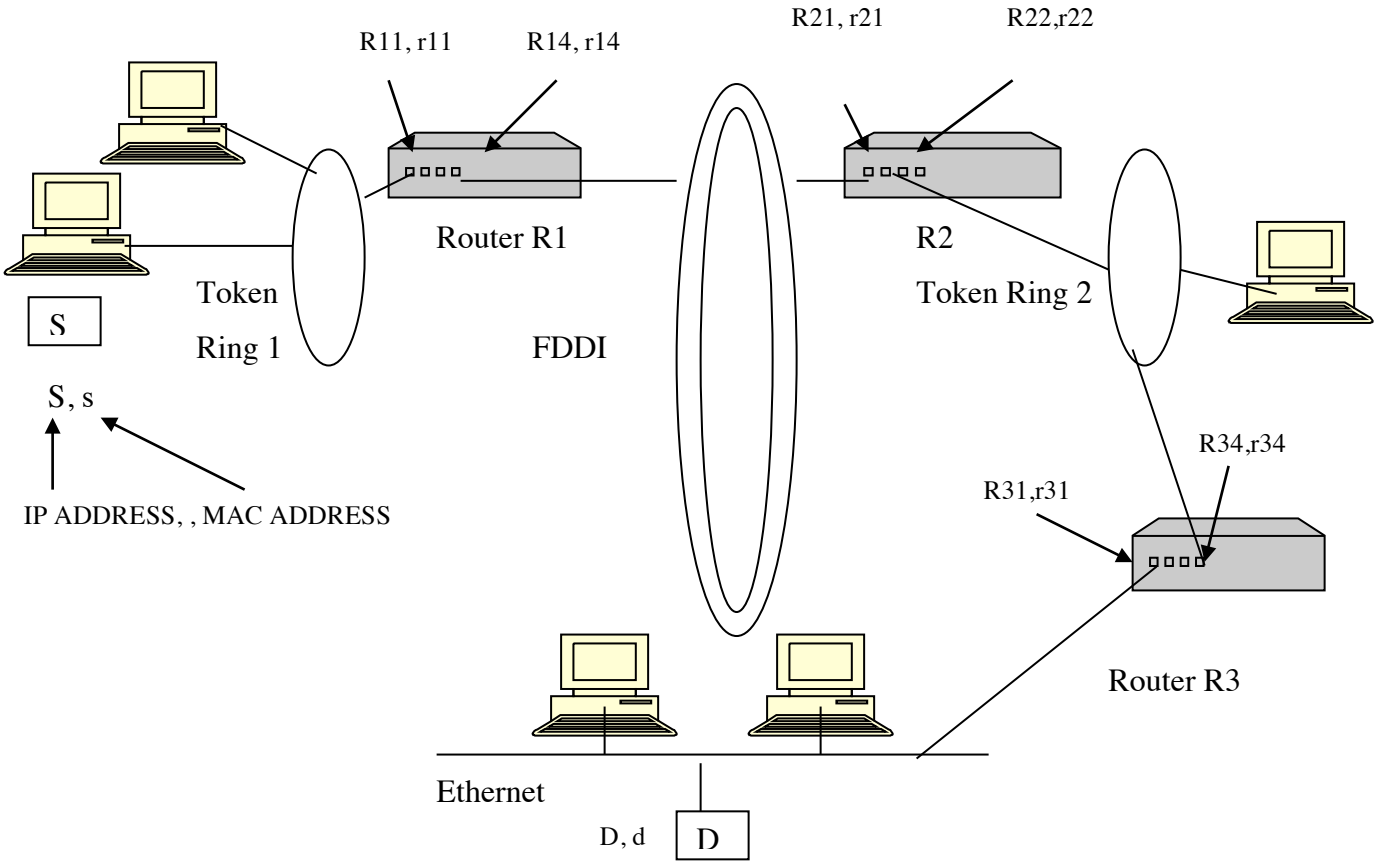
Exercise 2 (Exploratory): www.sectools.org offers a rich catalogue of network security tools, including their classification, ratings, links to the tool's website and reviews. Visit the website and pick one network security tool. Conduct a thorough exploration of the tool and write a report summarizing the tool. In your report, describe the tool's features, what it provides, and how it works. Also outline how it is useful to a network security specialist and how it may be used for harmful purposes by a hacker.
Length of the report: Approximately 1 page, single line spacing, 11-point font size.

Exercise 3 (Exploratory): Distributed DoS (DDoS) is the second most common type of cyber-attacks, next only to malware. Surf the web and write a report on ONE DDoS attack that occurred in 2016. What techniques were used to launch the attack? Who was the victim? What was the vulnerability in the victim that led to the success of this attack? What are some of the remedial measures, if any, that have been taken after the attack?
Length of the report: Approximately 1 page, single line spacing, 11-point font size.

Exercise 4 (Conceptual): The following figure depicts an internetwork. The IP and the MAC addresses of the significant interfaces are shown. An FTP connection is set up from S to D (S is the client and D is the server) and a SSH connection is set up from D to S (D is the client and S is the server). Write the formats of the following message entities, showing the port addresses, IP addresses and MAC addresses using the format:

Source MAC address	Destination MAC address	Source IP address	Destination IP address	Source port address	Destination port address

d) Frame on Token Ring1 – FTP message from S to D.
e) Frame on FDDI – FTP message from S to D.
f) Frame on Token Ring 2 – FTP message from S to D.
g) Frame on Ethernet – FTP message from S to D.
h) Frame on Token Ring 1 – FTP message from D to S.
i) Frame on FDDI – FTP message from D to S.
j) Frame on Token Ring 2 – FTP message from D to S.
k) Frame on FDDI – SSH message from S to D.
l) Frame on Token Ring 2 – SSH message from S to D.
m) Frame on Ethernet – SSH message from S to D.
n) Frame on Token Ring 1 – SSH message from D to S.
o) Frame on FDDI – SSH message from D to S.



Exercise 5 (Conceptual): We discussed five generic intrusion types, namely, interruption, interception, modification, fabrication and invasion. In addition, we outlined the seven security goals as confidentiality, integrity, authentication, non-repudiation, access control and availability. For each of the following scenarios, identify the most likely intrusion or set of intrusions. Also identify which security goal or set of goals have been violated. Give a short justification.

The answer for the first scenario has been given (in red font). Follow a similar procedure for the remaining scenarios.

Scenario	Intrusion(s)	Security Goal(s) violated	Justification
Bob crashes Alice's computer system by sending a flood of packets	Interruption	Availability	This is a classic case of a DoS attack and hence falls under the category of interruption. Alice's computer is unavailable for her use and hence the security goal violated is Availability.
Alice copies Bob's assignment by eavesdropping on traffic from his machine.			
Bob copies Alice's assignment by accessing her hard drive.			
Alice changes the amount on Bob's cheque when it is being transmitted.			
Bob sends a property deed to the Registrar in the name of Alice by forging Alice's signature.			
Alice spoof's Bob's IP address to gain access to his office server.			
Bob installs malware on Alice's computer.			
Bob obtains Alice's credit card information online and has the credit card company replace it with another card bearing a different account number.			
Alice has a fake third party authenticate her server as legitimate.			