**Midterm Exam**

**NOVA**

**Spring 2021**

Please answer below questions based on class lessons. This exam is open book, open notes but you may not work with others in the classroom. Your answers to the questions should be your own, do not copy and paste from the web. Once complete, submit on canvas.

1. What is the dark web? (5 Points)

The dark web is part of the internet that is not indexed by search engines. The dark web also needs a specialized browser and search engine to be able to access.

1. What are three lessons learned from the FBI Guide to Dark Web Investigations article? (5 Points)

Three lessons that I learned from the FBI Guide to the Dark Web Investigations article are:

- That passively collecting information is not typically considered illegal.

- to have a rule of engagement if entangled with legal repercussions.

- involve the legal team in preparation and planning to find any legal issues that could arise.

1. How is the dark web different from the surface web? Provide three examples. (5 Points)

Three ways the dark web is different are:

-The surface web does not require a special browser or search engine to access it unlike the dark web that does.

- To access the dark web the user needs to take precautions to reach near anonymity, unlike on the surface web which is considered generally much safer to use.

-The dark web does not track the user as easily as it is done on the surface web. It will be near impossible to track the user on the dark web like the user is tracked on surface web.

1. What are five unique lessons learned from “Beware The Predator” readings? How do they relate to dark web research? (20 Points)

Five lessons that I learned from Beware the Predator readings are:

-to avoid using foreign antivirus

-use separate credit cards for different thing, for example a card for groceries, a card for gas, etc. This will prevent someone to see the use’s habits or schedule if they are able to access a history of a single card and any other purchase that was not made by the user will stick out if it is stolen.

-Have a go bag ready for emergencies in any place that the user frequents

- create a “trap” to know if someone looked through the traveler’s belonging in a hotel

-have clothes and other necessary things to put on if there is an emergency and need to evacuate the hotel.

1. What are the top three encrypted communications applications you have read about in the class? Describe how each relate to the dark web and how they are different from each other. (15 Points)

- onion messenger: an online chat service on the dark web

- telegrass: an online instant messaging service like telegram. This was used in Israel to sell drugs.

-EncroChat: another instant messaging service. It is being investigated for selling illegal substances over it.

All these encrypted communication applications are used by sellers and buyers selling illegal substances and other things over them. They probably start contact over the dark web and move over to these communication channels for easier contact. The difference with the onion messenger is an android app that uses the tor network with full encryption. The telegrass application was an encrypted messaging application like the onion messenger and EncroChat. The main use was to deliver cannabis in Israel. EncroChat would sell cellular services to hide the owner’s identity, location and anything else that could be used in a law enforcement investigation.

1. What are the three darknet diaries podcast you have listened to? What are they about? Provide a brief description, episode number and title. (7 Points)

- Episode 77: Olympic Destroyer- The hacking of the South Korean Olympics that was carried out by Russia. It was hard to figure it out since the Russian Hackers were trying to blame it on North Korea with the code signatures.

-Episode 81: The Vendor- A college student was selling drugs and explaining how he was doing. He ended selling on the dark web. He used a used a virtual machine, with many ways to prevent being caught.

- Episode 83: NSA Cryptologist- Markus Carey and Jeff Man explained how they got into the NSA and stories of what they did while in the NSA and deployed for the NSA.

1. Name three things listed under General Course Information section of the class canvas site. Provide a brief explanation for each. (5 Points)

– 90% of the internet is hidden and those who want anonymity use the deep, dark web

- required materials include dark web diaries podcast, Beware the Predator by Warren Holster, and RF Threat Intel Podcast

- the class will have a few guest speakers throughout the semester

1. What are VPNs? What do they offer the user? Provide a screenshot of a successful VPN connection based on class lessons. (5 Points)



A VPN is a virtual private network that provides anonymity on a public network.

1. Describe the Tor network and provide two examples of Tor Hops. (10 Points)

The Tor network uses a minimum of 5 hops to help provide near anonymity. These hops are jumps like a VPN would make, but does a minimum of three random hops before hopping off onto the server of the website the user is trying to access. So if the user’s IP is 192.234.100.244 inside the US, the hops can land in Switzerland, then Lithuania, and Ukraine, then land on the webpage they were trying to reach like McDonalds.

1. What is ZeroNet and how does it differ from Tor? (10 Points)

ZeroNet is different from Tor because it does not provide hops as a default and everything is downloaded onto the user’s machine so there is no need to connect to the internet.

1. What does VPN provide the user? (5 Points)

A VPN provides a user private network, making it harder to trace where the user is and helps bypass any restrictions on the network as well as providing a more secure measure for exchanging data.

1. What is one thing you learned from guest speaker Bianca? (3 Points)

One thing I learned from Bianca is that the C.I.A. Triade is used a lot more in the professional settings than I thought.

1. What are two lessons learned from guest speaker Warren? (5 Points)

Two things that I had learned from Mr. Holster is that:

* I am constantly being monitored with my advertising ID on my mobile device.
* That I have no privacy from the devices I have and from using the internet.

Resources:

<https://www.bankinfosecurity.com/blogs/encrypted-chat-apps-arent-replacing-darknet-markets-p-2949>

<https://play.google.com/store/apps/details?id=com.onionsearchengine.onionmessenger&hl=en_US&gl=US>