SEMINAR REPORT
ON

DARK WEB: A HACKER'S PERSPECTIVE

BY
Varaa Kukreti

T.Y. B.Tech. Computer Engineering,
Roll No. – 3471, Division – B
2020-2021

SEMINAR GUIDE
Prof. Saurabh Mengale

MKSSS's
Cummins College of Engineering for Women, Pune
(An Autonomous Institute Affiliated to Savitribai Phule Pune University)

CERTIFICATE

This is to certify that Ms Varaa Kukreti has satisfactorily completed the seminar on **"Dark Web: A Hacker's Perspective"** in the partial fulfilment of her term-work (Seminar) as a part of syllabus for T.Y.B.Tech. Computer Engineering for the Academic Year 2020-2021 as prescribed by MKSSS's Cummins College of Engineering for Women, Pune. (An Autonomous Institute Affiliated to Savitribai Phule Pune University)

Prof. Saurabh Mengale
Seminar Guide

Dr. Mrs. S. M. Kelkar
HOD Computer

Dr. Mrs. M. B. Khambete
Principal

MKSSS's
Cummins College of Engineering for Women, Pune
(An Autonomous Institute Affiliated to Savitribai Phule Pune University)

PLAGIARISM CERTIFICATE

This is to certify that Varaa Kukreti has satisfactorily completed the seminar report on **"Dark Web: A Hacker's Perspective"** and the data present in this report is found to be 100 % plagiarism free. This seminar report is towards the partial fulfilment of her term-work (Seminar) as a part of syllabus for T.Y.B.Tech. Computer Engineering for the Academic Year 2020-2021 as prescribed by MKSSS's College of Engineering for Women, Pune. (An Autonomous Institute Affiliated to Savitribai Phule Pune University)

Varaa Kukreti

Prof. Saurabh Mengale
Seminar Guide

ACKNOWLEDGEMENT

I would like to express my sincere thanks and gratitude to
Director Dr. Mrs. Madhuri Khambete and Dr. Mrs. S. M. Kelkar for this opportunity.
I would also like to thank Prof. Saurabh Mengale for providing me his invaluable guidance, insights and suggestions for my topic of seminar "Dark Web: A Hacker's Perspective" throughout the course of seminar.

Varaa Kukreti

Prof. Saurabh Mengale
Seminar Guide

ABSTRACT

A study which was conducted by Positive Technologies' analysts threw light on the fact that 90% of the times users of dark web forums are searching for hackers who can get them access to a particular resource or for hackers who can hack into a user's databases and download them. The research showed that 69% of the ads inquired for services for website hacking, where the main purpose was to access a particular web resource. Additionally, 4% ads corresponded to people looking for hackers to infect a web resource with malware & 3% for the ones who could delete data from a website of their choice.[3] Among various hacking services provided on the dark web there is a very high demand for hackers who can gain access to online stores as when paying for items using online transactions users enter their credit card details. Thus, there is an opportunity to inject malicious JavaScript code into the targeted websites which would enable the 'bad guys' to intercept any and all information entered by users which in turn can be used by the hacker themselves or sold to someone else on the dark web.

It is evident from the facts that dark web is a sprawling ground for hackers, not just for finding contracts but also for carrying out the deed itself. What does dark web have to offer hackers? How does internet which specially in today's pandemic struck world is helping everyone by enabling them to staying in touch with their loved ones, attending online classes or working from home become the source of something so malicious?

Table Of Contents

Contents **Page No.**

List Of Figures

Chapter 1: Introduction

To understand what dark web is we need to understand what deep web is.

1.1 What is Deep Web?

The deep web also known as hidden web are parts of the World Wide Web whose contents aren't indexed by standard web search-engines. The data in the deep web include your social media account's content, details of an individual's online banking account, data in a company's database, etc. Normal folks can't access some data on the deep web that's irrelevant to us. In simple words, the reason search engines can't return data inside the deep web to you is because there are no links to access them. For example, if I log into my email account and share the link with you, you won't be able to access my emails. The info inside deep web doesn't just show up when we search it on web. Deep web is relatively safer to access as compared to dark web.

1.2 What is Dark Web?

The dark web is a subset of the deep web that is intentionally hidden, requiring a specific browser to access i.e., Tor short for The Onion Router and is usually associated with illegal activities making it a sprawling ground for hackers, illegal traders, etc. The dark web uses The Onion Router hidden service protocol. "Tor" servers are undetectable from search engines and offer users complete anonymity which in-turn gives hackers added benefits, making it less likely to be caught while carrying out illegal activities. Dark web website publishers are anonymous as well because of the special encryption provided by the protocol. Dark web website addresses end with .onion instead of the .com, .org, etc that we encounter on a regular basis.[2][4]

Even though dark web is not completely made out of illegal activities, but is famous for the them. Some of these activities include:
1). Illegal trade- this may include, trading illegal substances like drugs, human body parts for transplants or weapons like guns which may otherwise need license.
2). Illegal services- Dark web has become a breeding ground for people who deal in child pornography, hiring hitman for murders, hiring hackers etc.

3). Leaked information- A lot of leaked information usually makes its way to dark web starting from stolen credentials for Netflix to data of multinational companies.

Hackers can use the dark web to sell stolen information or to prompt amateur users to click on malicious links which may infect their device and can cause ransomware attack or use their computer as zombies in DDoS attacks.

1.3 IP Hopping

It is important to understand IP hopping also known as IP bouncing when trying to understand why dark web is plagued by hackers. IP hopping is the practice of using one IP address for some time and then changing it to another one. IP hopping lets you avoid any bands or flags. But, if the IP you hop to is band by a website, you may not be able to do what you intended to. Hopping IP frequently can help you remain anonymous and conceal your actual location which in turn can help you browse websites which are banned in your country which is why it is very popular amongst hackers. However, a user might get banned if there are unusual changes of IP for the same user or account which is a downfall for inexperienced IP bouncers as they often forget to clear their cookies before they bounce to a new address. A prevention mechanism for this would be to use IPs in the same country.

It is better for a hacker to use IPs of different countries specially of the ones which don't have strict laws for keeping track of its citizens internet activity as it makes it even more difficult to trace any activity back to its source.

Chapter 2: History of Dark Web

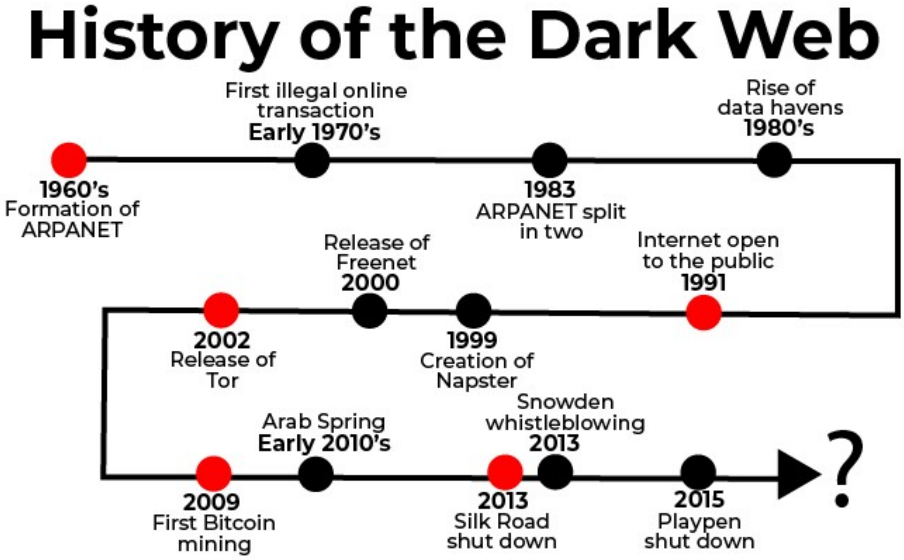

History of the Dark Web
First illegal online transaction Early 1970's
Rise of data havens 1980's
1960's Formation of ARPANET
1983 ARPANET split in two
Release of Freenet 2000
Internet open to the public 1991
2002 Release of Tor
1999 Creation of Napster
Arab Spring Early 2010's
Snowden whistleblowing 2013
2009 First Bitcoin mining
2013 Silk Road shut down
2015 Playpen shut down
?

Fig. 2.1 Timeline

2.1 ARPANET & Internet

The idea for ARPANET short for Advanced Research Projects Agency Network came from the desire to share information over huge distances without having the need to have each computer on network connected by phone connections. The ARPA, a branch of U.S. defence department, wanted a computer-based system for communication without central core, which would in turn protect against attempts by enemies to black out the entire network by simply attacking the core.

In early 1970's first illegal transaction took place where Stanford students used ARPANET accounts to indulge in a commercial transaction of marijuana with their fellow counterparts at MIT. 1983 gave us a split of ARPANET into 2 parts: the first being MILNET for military and defence agencies, and the second part was a civilian version of ARPANET which became basis for internet. Discussing ARPANET is important to know the history of dark web as at their core, both ARPANET & dark web are rooted in the same desire for a secure correspondence. Ironically, hackers take advantage of this secure correspondence to maintain anonymity. As internet popularity grew concerns regarding data storage came into picture which were answered in the form of data havens which in turn led to a growing concern for the online privacy, the same concern which was later shared by dark web users.

Coming to the 1990's also known as the decade of the Internet boom & the Dot-Com bubble. In 1991, after the release of MP3 compression formats & the Internet becoming publicly available, people began to illegally rip CD's. It didn't take long for illegally ripped music to make its way online, and later to a music sharing site called 'Napster'. As people began to come to the realization that Internet could be a one-stop shop to get anything they want, whenever they want, it was only a matter of time for more illegal transactions to start blooming to their full glory online paving a way for criminals specially hackers. Freenet even though not as popular as Tor, did help to stimulate the demand for accessing the Internet anonymously. Anonymity which was being introduced to revolt against oppression at that time lead to a playground for hackers.

2.2 Release of Tor

From 1960's till 1990's there was a growing demand for accessing any content that was desired & away from the government's prying eyes. This demand was answered by tor which was instrumental in paving the way for dark web. David Goldschlag, Mike Reed, and Paul Syverson started to find a way for routing the traffic through internet anonymously in response to growing concerns over the lack of security at the U.S. Naval Research Lab in the 90's which led to more harm than good. They planned to achieve this goal using multiple servers or network nodes called onion routers to route the internet traffic and encrypt it long the way, coining a term for their idea 'onion routing'. In an onion network, traffic is encapsulated in layers of encryption, which can be compared to layers of an onion hence the name onion routing. Each of the routers 'peels' a single layer, uncovering the data's next destination.

Tor's creators had good intentions specially when they made the platform free and modified it to address government censorships by developing a way for the internet traffic to get around government firewalls. They were motivated by the user's demands so that the people under oppressive government regimes could publish their thoughts and access restricted websites freely. But, in doing so they ran into a greater problem, the platform became complex which restricted its usage to only tech-savvy people. Though most of the dark websites came into picture to help those living under oppressive regimes, the temptation of having a place on the internet where you could browse anonymously paved way for a rise in the number of dark websites which took part in illegal activities.[5]

Tor provided a way for people to access social media, blocked websites & critical resources while protecting their identities online. So, the dark web itself wasn't the problem, it was how a person or organisation decided to utilize it. Journalists used it for good, to spread awareness to raise a voice, white hat hackers used it for good as well**,** supporting governments trying to catch terrorists dealing in firearms, but some choose to side with the criminals which were the black and grey hat hackers.

2.3 Release of Bitcoin

No one wanted to risk using credit cards or PayPal for online illegal transactions because they leave paper trails, which could potentially lead to customers being located thousands of miles away. This could defy the purpose of maintaining anonymity, but cryptocurrency came to the rescue so all the illicit activities and services like hiring hackers or selling confidential data online could be paid for. Cryptocurrency wasn't as we know it to be today until Satoshi Nakamoto "mined" the first Bitcoin which started a revolution in illegal transactions. Bitcoin wasn't the first cryptocurrency but the most famous till date as it solved the problem that other cryptocurrencies couldn't address. Bitcoin having a special accounting ledger in place forbid users from copying the money. Bitcoin helped hackers get paid online for their explicit services while maintaining anonymity which was what aggravated the desire for most of the black hat hackers and dark web became their personalised cocoon.

Chapter 3: Accessing the Dark Web

Dark web is a dangerous place to play around even for an experienced IT professional let alone a newbie. Hence, we should keep in mind certain things before we take on the task of accessing the dark web where not only professional hackers but other criminals wait for naïve users to trap them in a never-ending cycle of gloom by stealing their credentials, getting them involved in activities that are illegal or hacking into their machine and using them for activities of criminal nature without their knowledge.

3.1 Ways of Accessing the Dark Web

There are various ways of accessing the dark web, Tor is the most well know way as it provides secrecy and anonymity by passing requests through a series of specially configured computers forming a relay. The use of I2P (Invisible Internet Project), Freenet, GNUNet, FAI (Free Anonymous Internet) & ZeroNet which are other peer-to-peer networks with layered encryption led to creation of dark web. Even though till now we have mainly brought up tor in out discussion, there are multiple ways to access the dark web. Following are the means of accessing the dark web apart from Tor:

1). I2P

I2P is an anonymous network which can be used as an alternative to Tor. But, unlike Tor it can't be used to access public internet as well as .onion sites because it's a completely separate network from Tor. I2P uses its own hidden sites, 'eepsites'.[6]

- Both Tor as well as I2P have a peer-to-peer routing structure combined with layered encryption for a private and anonymous browsing experience.
- Even though there are few restrictions with accessing sites in I2P, it does have certain advantages as well, one of them being it's much faster and more reliable as compared to Tor which is a huge plus point as in hacking every second counts. This advantage over Tor exists because of the advanced peer-to-peer structure and lack of reliability on a directory to get route information.
- 1n 12P, eavesdropper can only catch inbound or outbound traffic not both due to the use of one-way tunnels which could be a disadvantage for a hacker trying to intrude in your business.

- Configuration: There are a lot of configurations which needs to be done though the router's console. After downloading and installing I2P each individual application must be configured one by one to work with it. The browser's proxy settings need to be configured as well to use the correct port.

2). Freenet

Freenet is a self-contained peer-to-peer distributed datastore network. Just like I2P it can't be used to access the public web & can only be used to access the content uploaded to the Freenet. Anything uploaded on Freenet stays there indefinitely even if you stop using it. It's still an experiment designed to resist DoS attacks & censorships. Unlike Tor and I2P you don't need a server to host the content.[6]

- Configuration: It is fairly straightforward you just need to download it, install it, and then run it. Freenet will be running through its web-based interface when you open your browser, which should be a separate browser than your usual one to help ensure anonymity.

There are 2 modes for connecting: Darknet & Opennet.

- Darknet: It allows you to specify who your friends are on the network and you only connect and share with them. This is great specially for a hacker as they can form a close-knit anonymous network made up of people they trust.
- Opennet: It automatically assigns peers on the network & uses a handful of centralized servers apart from the decentralized peer-to-peer network.

3.2 Precautions

Since along with freedom, anonymity also encourages illicit activities therefore one must take precautions while accessing the dark web. As, dark web is a hub for criminals to attract vulnerable victims and law enforcement agencies to catch criminals so you never know what the intentions are of the person or website you are interacting with. As hackers may try to infect your machine it would be advisable to take certain precautions:

1). Remove drivers for both webcam and microphone.

2). Don't use a device with your personal details which could end up in the hands of someone you'd want to protect yourself from.

3). Before accessing dark web use your own VPN even though Tor has its own VPN and encryption.[1]

3.3 Risks of Getting Infected by Malware

There is a high probability that your device may get infected with viruses and malware while on dark web making your device a tool for hacktivists or hackers to carry out their deeds which may land you in trouble because of your machine being involved. According to an article by Motherboard a person surfing on the dark web could be exposed to the following programs:
Vawtrack: gains access to user's financial accounts.
Skynet: used to steal bitcoins or make the user's device a zombie for a DDoS attack.
Niospy: Can record audio or video, steal documentation and capture keystrokes.[1]

3.4 Keep in Mind

1). Ask why?
Try to follow your instincts. If someone is being too friendly, ask why? Question their every move and yours as well. Social engineering attacks become especially easy when on dark web, cause even though you may think anonymity gives you protection, it also gives protection to a hacker.
2). Hide yourself.
Anonymity may protect you to some extent but don't let your ignorant attitude get you into trouble. Using your real name, accounts, or passwords that you've used before can lead hackers straight to your real self.
3). Avoid using personal credit card.
Remember why cryptocurrency came into the picture. If you used your actual credit card or bank account details it can be traced back to you, or your credentials could be stolen when you enter it on a website. If there is no choice other than to use your financial account details, enter your bank account details on websites with https:// where s stands for secure socket layer.
4). Don't download
Downloading anything on dark web can be an open invitation to hackers to inject your machine with trojans, viruses, worms, spywares, ransomwares and what not. Don't click on suspicious links too. Think before you act & don't give into your impulses.

Chapter 4: Tor

Tor is the most popular means for us to communicate anonymously on the dark web. It directs Internet traffic through a volunteer overlay network, having more than six thousand relays which help conceal a user's usage and location from anyone conducting network surveillance or traffic analysis. Tor makes it difficult to trace the Internet activity of a user but it's not impossible.

4.1 Maintaining Secrecy:

- When using Tor, a node in the relay just knows about the IP address from which the request came from and IP address to where it's going to forward the request to, this in turn makes it difficult to trace back the IP of the source.
- By keeping some of the entry or bridge relays a secret, users can avoid Internet censorships that depend on blocking public Tor relays.
- Anyone eavesdropping can't identify both the source and the destination as the IP address of the sender & receiver are not both in cleartext.
- Furthermore, to the receiver or website it seems as though the last Tor node also known as the exit node is the source of the communication instead of the actual sender.

4.2 Implementation

Onion routing is implemented in the application layer. Nested like the layers of an onion there is encryption of the communication protocol stack. Tor is primarily written mostly in C, along with Python, JavaScript, and several other programming languages. It had 505,034 lines of code in May 2019.

4.3 Nyx Status Monitor

It is a command-line status monitor which was written in Python for Tor. This provides real time statistics for:

- Resource Usage: Memory Usage, Bandwidth & CPU.
- General Relaying Information: Fingerprint, Nickname & Flags
- Connections Correlated Against Tor's Consensus Data: IP, Connection Types, Relay Details

- Tor's configuration file called torrc.

4.4 Tor's Weaknesses

Tor doesn't attempt to protect against traffic monitoring at the boundaries of Tor network i.e., when the traffic enters or leaves the Tor network, just like all low-latency anonymity networks. Tor can't protect you against traffic confirmation which is also called end-to-end correlation but can save you from analysis of traffic.[7]

1). Consensus Blocking: Tor being a decentralized system, relies on a consensus mechanism to update its current operating parameters periodically, which are network parameters like exit guards, how much traffic can a node handle & which nodes are good/bad relays. Directory authority nodes whose IP addresses are hard coded into each Tor client vote on the current network parameters for deciding the consensus.

2). Eavesdropping: Autonomous System (AS) & Exit node

- Autonomous System eavesdropping: An AS exists on both sides i.e., from client to entry relay and from exit relay to the destination and hence can correlate and analyse the traffic, potentially discovering which client is communicating with which destination.
- Exit node eavesdropping: As Tor can't encrypt traffic from the exit node to the destination hence any traffic that doesn't use end-to-end encryption is not secure.

3). Traffic-analysis attack: passive & active.

- Passive: In this method, the hacker may look for those features on one side of the network which he/she extracted from the traffic on the other side of the network.
- Active: The hacker can alter the timings, of packets, of a flow according to a particular pattern & can look for it on the other side of the network and hence can break the anonymity of the user.

4). Tor exit node block: Few websites can offer reduce functionalities to Tor user or can block IP of Tor exit nodes.

5). Bad apple attack: One method of attack can depend on taking control over the exit node

6). Sniper attack: It can be compared to DoS attack, here we fill the queues of exit node till it runs out of memory restricting it from serving genuine clients. By, doing this to several exit nodes the hacker can degrade network and increase the chances of the target using an exit node controlled by the hacker.

7). Relay early traffic confirmation attack: The node in onion service directory which is attacking can change the header of cells being relayed and can tag them as 'relay' or 'relay early' to encode extra information and send them back to the requesting user. If the user's guard node is a part of attacking relays, then they might be able to get the IP address of the user apart from the onion service information.

Chapter 5: VPN

A VPN or Virtual Private Network allows users to encrypt all of their internet traffic traveling from and to their device and route it through a server in a location of the user's choice.

5.1 VPN & Tor

- VPN and Tor are quite similar differing in that fact that Tor emphasizes anonymity and VPN, privacy.
- Using Tor along with VPN adds a layer of security and anonymity which gives added protection to users, be it a gullible person trying to surf the dark web the first time or a hacker trying to conceal his/her identity.
- Due to all the nodes that your traffic passes through in Tor network even if you add a fast VPN still the process will be slower but it's better to be safe than slow.

Let's discuss 2 methods to use VPN with Tor, even though both have their advantages and disadvantages for naïve users and hackers still they both are superior to not using VPN at all.

5.2 Tor over VPN

Tor over VPN is the most commonly used method where you connect to your VPN and then use Tor browser. All your internet traffic first passes through your VPN server and then bounces though various nodes in the Tor relay ending up in its final destination.[6]

- This is helpful if you don't trust your ISP as your ISP will only see the encrypted VPN traffic and won't know that you're surfing on Tor. This is especially useful for hackers as they want to conceal their identity and it's important for their ISP to not know what they're up to.
- Even though VPN provider can't really see what exactly you're doing on Tor as your traffic is encrypted internally by Tor itself this method still requires the user to trust their VPN provider as they can see that you're using Tor & may also keep metadata logs. In this case a logless VPN which doesn't store session or traffic logs is highly preferable. Traffic logs which store the content

of your internet traffic like websites you visited and search queries are a bigger concern as compared to session logs which contain metadata like your IP address when you logged into your VPN or how much data was transferred, but neither are good.

- Tor over VPN does have one disadvantage for normal users as it doesn't protect you from malicious exit nodes which is the final node in the relay, but this disadvantage is actually an advantage for hackers as they can get intercept the data here. Exit nodes can decrypt your traffic and hence steal your personal information or inject malicious code. Nodes are volunteer machines and not all of them are there to provide a helping hand.
- Some nodes are blocked by websites that don't trust them and if such node is your exit node, then you won't be able to access that particular website.

NordVPN operates specialised servers that provide a built-in Tor over VPN functionality by automatically routing your internet traffic through the TOR network. You don't need to use Tor browser for this but other browsers might pass identifying information through the network which could compromise your anonymity. Alternatively, there is IPVanish who claims to be the world's number one VPN for Tor.

A hacker would most likely prefer this method, as it keeps them hidden from the ISP and hackers can tamper with your machine and data when casual users use this method due to malicious exit nodes.

5.3 VPN over Tor

The other method is VPN over Tor which is less popular as it is advised against by the official Tor project. The internet traffic in this case first passes through the Tor network and then through the VPN which means VPN provider can't see your real IP address.[6]

- VPN will protect you from harmful exit nodes which is good for most users, not for hackers trying to get into such user's system. AirVPN & BolehVPN offer this service but are not known for their high speed.

- One big disadvantage is that your ISP will know you're using Tor which is a huge concern, especially for a hacker.
- In this case too it's better to go for a logless VPN. It is highly unlikely, but possible in this case to be the victim of an end-to-end timing attack.

Weighing both options, VPN over Tor can be considered more secure because it maintains anonymity throughout the process assuming you don't use your credit card details for payment and opt for bitcoins to maintain anonymity. VPN over Tor would be a safer option for a casual user who just wants to surf the dark web as the possibility of attack and ways through which you could fall prey to a notorious hacker is less, but you using this technique could be bad news for a hacker.

Chapter 6: Case Study

6.1 Red Room

Even though Red Room is not a hacker specific but a crime specific topic, but it is very important to address when talking about dark web. We have discussed how dark web is a hub for criminals, what techniques are used and what are the advantages and disadvantages but here is an actual example of what criminals can get to if given the power of anonymity. Red Room is considered to be a myth by many, but I'll let you decide for yourself.

Red Rooms are places on the dark web used to hide illegal activities online while showcasing them at the same time. This is where people can pay in cryptocurrency to watch 'live videos' of rape, torture murder & even worse.

- Users pay thousands for access to these dark clips online which could be a potential hunting ground for white hat hackers working for government to track down paedophiles, murderers & rapists.
- Tor can't be used to access these videos or hosts these rooms as being slow Tor can't support live-streamed videos

To access such gory videos viewers, send their mail ID to the website's owner using which the website owner sends them a link on which viewer may pay charges using mostly bitcoins. In return, the user gets password and either a live video where the viewer just watches or else the viewer demands actions of torture or death to be performed by a masked person on a victim. More torture demands more money.

One episode linked to Red Room is of paedophile Peter Scully who would entice impoverished kids with money back to his house and later drugged the vulnerable youngsters to make clips of him torturing and raping them for selling them for up to $10,000 per view for an international paedophile ring. One such video was where he made 2 little girls dig up their own graves.

There are 2 noteworthy cases one was of ISIS saying they would behead a Turkish soldier live on a specified date and time and the other case is 'Daisy's Destruction' in which Scully was involved, which is one of the most horrific case of child abuse. While there are some sites that don't advertise themselves as Red Rooms, but may actually be. Most of the sites that make outlandish claims are just out there to rob people's money, or to deceive them.

6.2 Silk Road:

It an online black market mainly known for trading in illegal goods and services. It was the first ever modern dark web market which was operated as Tor hidden service. Over 100,000 users could browse securely and anonymously without traffic monitoring.

1). Trial:
The FBI shut Silk Road down in October 2013 and arrested Ross Ulbricht as being site's founder **'**Dread Pirate Roberts' but Silk Road 2.0 was back in November 2013 which was yet again shutdown in November 2014 as a part of 'Operation Onymous'. Ulbricht was sentenced to life in prison without possibility of parole and was indicted with several charges including money laundering, computer hacking, and attempting to kill 6 people.[8]
2). Worth:
The FBI seized 26,000 bitcoins initially which was worth $ 3.6 million at that time. Again, in October 2013, 144,000 bitcoins worth $ 28.5 million was seized by the FBI which belonged to Ulbricht. U.S. Government seized more than $ 1 billion worth of bitcoins in connection to Silk Road in November 2020.
3). Silk Road thriving:
Introduction of cryptocurrency & ecommerce markets led to demand in data privacy which led to increase in regulations and laws which in turn led to increase in tools maintain anonymity to protect user's personally identifiable information but these tools further increased illegal criminal activities online including hacking.

- Accessible only using Tor, which obfuscates IP addresses of users so buyers and sellers conducted trade without fear of being caught.

- Another thing which leads to Silk Road thriving so well was the feedback of buyers which weeded out fraudulent sellers, which promoted confidence of buyers on the online platform.
- Due to transparency of Bitcoin Transactions, dark wallets were invented which encrypted and masked the transactions, adding a layer of privacy.

Chapter 7: Conclusion

'Rent-A-Hacker' is a website on the dark web, seemed to be managed by a single hacker who explained that he specialised in illegal hacking services and offered to 'destroy some business or a person's life'. This is one out of thousands of hackers on the dark web offering their services in exchange for money.

We have seen how black hat hackers can take advantage of technology and techniques on the dark web but white hat hackers can also use the same techniques to track down criminals or trap them using sites where criminals take part in illegal activities. The technology is the same, it's about how we decide to use it.

As, we are depending more on the internet more cybercrimes take place. As technology for protecting us online advances so does the technology to breach our privacy and data. Being mindful of every move you make is very important when browsing on the dark web as you may fall prey to social engineering attacks, malware attacks, data breaches, frauds, etc.

It's important to know the dark web through a hacker's eyes so that you can protect yourself & others from attacks, as when you can think like an attacker and know the points of attack so you can better defend yourself accordingly for those probable attacks. It is easy to be a black hat hacker and trap people by finding a single loop hole out of many to exploit but it's more difficult to know all the loop holes and protect them all. That's the difference between attackers and protectors, both are hackers so their knowledge base is the same but their intentions distinguish them.

Now that I've given knowledge of probable points that could be exploited and advantages for hackers on the dark web, how you decide to use this information will determine which side you lie on.

Appendix A

FAQs

Q1) Why Is Tor slow?

Ans. As your traffic is being routed through multiple volunteers before arriving at the destination this leads to Tor being slow.

Q2) Why do hackers want my data?

Ans. While each piece of data is only worth a few dollars but when resold this adds up to a huge amount, accounting for data stolen from thousands of people.

Q3). Is the dark web illegal?

Ans. No, dark web in itself isn't illegal but most of the activities that it fosters are, as criminals can remain anonymous which further fuels their fire for crime.

Q4). Do I need to be certified to be a hacker?

Ans. Depends, hacking is a talent not a certification so to be called a hacker you just need to know how to hack. But, to work as an 'ethical' hacker in a company or government usually you need to have an ethical hacking certification like CEH.

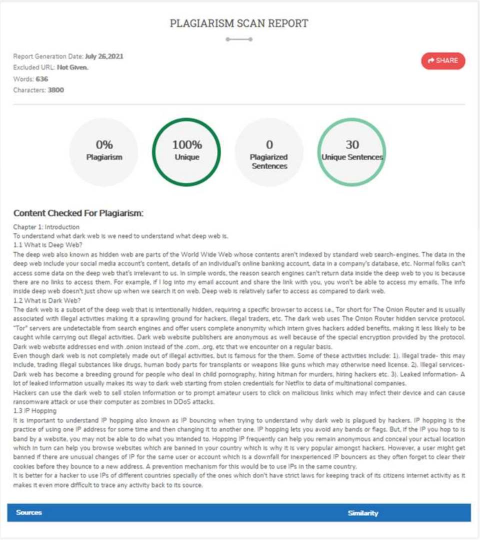
Q5). How can I join hacking communities on the dark web?

Ans. There are multiple hacking communities like Mazafaka, Trojanforge, dark0de, etc. But, most of them are closed to public and you need to request an invitation to join the discussion. Approach the ones which specialise in the domain of hacking you want.

Appendix B

Plagiarism Report of Small SEO Tools

Chapter 1



PLAGIARISM SCAN REPORT

Report Generation Date: **July 26,2021**
Excluded URL: **Not Given.**
Words: **636**
Characters: **3800**

SHARE

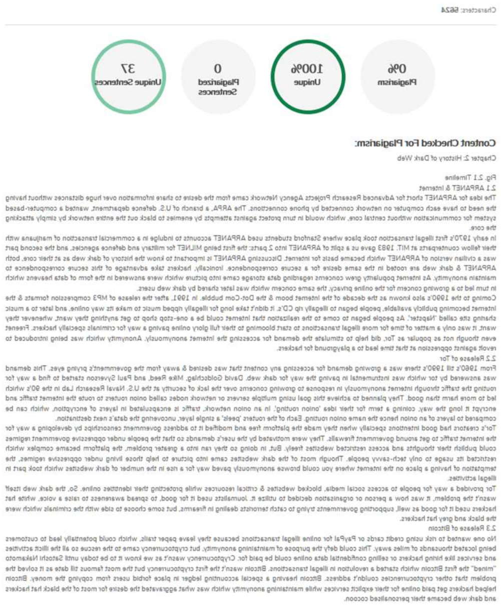
0% Plagiarism
100% Unique
0 Plagiarized Sentences
30 Unique Sentences

Content Checked For Plagiarism:

Chapter 1: Introduction
To understand what dark web is we need to understand what deep web is.
1.1 What is Deep Web?
The deep web also known as hidden web are parts of the World Wide Web whose contents aren't indexed by standard web search-engines. The data in the deep web include your social media account's content, details of an individual's online banking account, data in a company's database, etc. Normal folks can't access some data on the deep web that's irrelevant to us. In simple words, the reason search engines can't return data inside the deep web to you is because there are no links to access them. For example, if I log into my email account and share the link with you, you won't be able to access my emails. The info inside deep web doesn't just show up when we search it on web. Deep web is relatively safer to access as compared to dark web.
1.2 What is Dark Web?
The dark web is a subset of the deep web that is intentionally hidden, requiring a specific browser to access i.e., Tor short for The Onion Router and is usually associated with illegal activities making it a sprawling ground for hackers, illegal traders, etc. The dark web uses The Onion Router hidden service protocol. "Tor" servers are undetectable from search engines and offer users complete anonymity which intern gives hackers added benefits, making it less likely to be caught while carrying out illegal activities. Dark web website publishers are anonymous as well because of the special encryption provided by the protocol. Dark web website addresses end with .onion instead of the .com, .org, etc that we encounter on a regular basis.
Even though dark web is not completely made out of illegal activities, but is famous for the them. Some of these activities include: 1). Illegal trade- this may include, trading illegal substances like drugs, human body parts for transplants or weapons like guns which may otherwise need license. 2). Illegal services- Dark web has become a breeding ground for people who deal in child pornography, hiring hitman for murders, hiring hackers etc. 3). Leaked information- A lot of leaked information usually makes its way to dark web starting from stolen credentials for Netflix to data of multinational companies.
Hackers can use the dark web to sell stolen information or to prompt amateur users to click on malicious links which may infect their device and can cause ransomware attack or use their computer as zombies in DDoS attacks.
1.3 IP Hopping
It is important to understand IP hopping also known as IP bouncing when trying to understand why dark web is plagued by hackers. IP hopping is the practice of using one IP address for some time and then changing it to another one. IP hopping lets you avoid any bands or flags. But, if the IP you hop to is band by a website, you may not be able to do what you intended to. Hopping IP frequently can help you remain anonymous and conceal your actual location which in turn can help you browse websites which are banned in your country which is why it is very popular amongst hackers. However, a user might get banned if there are unusual changes of IP for the same user or account which is a downfall for inexperienced IP bouncers as they often forget to clear their cookies before they bounce to a new address. A prevention mechanism for this would be to use IPs in the same country.
It is better for a hacker to use IPs of different countries specially of the ones which don't have strict laws for keeping track of its citizens internet activity as it makes it even more difficult to trace any activity back to its source.

Sources	Similarity

Chapter 2



Characters: 5624

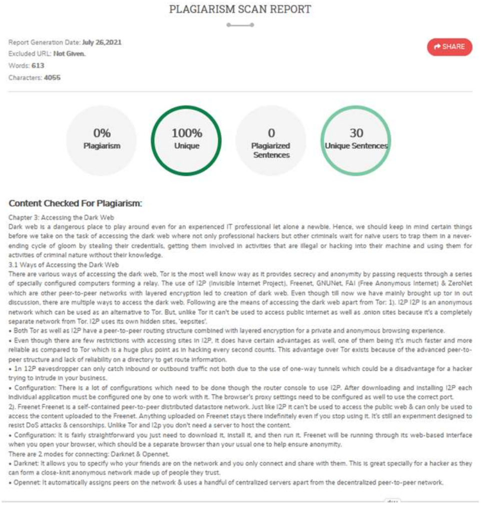
0% Plagiarism
100% Unique
0 Plagiarized Sentences
37 Unique Sentences

Content Checked For Plagiarism:

Chapter 2: History of Dark Web

Fig. 2.1 Timeline
2.1 ARPANET & Internet
The idea for ARPANET short for Advanced Research Projects Agency Network came from the desire to share information over huge distances without having the need to have each computer on network connected by phone connections. The ARPA, a branch of U.S. defence department, wanted a computer-based system for communication without central core, which would in turn protect against attempts by enemies to black out the entire network by simply attacking the core.
In early 1970's first illegal transaction took place where Stanford students used ARPANET accounts to indulge in a commercial transaction of marijuana with their fellow counterparts at MIT. 1983 gave us a split of ARPANET into 2 parts: the first being MILNET for military and defence agencies, and the second part was a civilian version of ARPANET which became basis for internet. Discussing ARPANET is important to know the history of dark web as at their core, both ARPANET & dark web are rooted in the same desire for a secure correspondence. Ironically, hackers take advantage of this secure correspondence to maintain anonymity. As internet popularity grew concerns regarding data storage came into picture which were answered in the form of data heavens which in turn led to a growing concern for the online privacy, the same concern which was later shared by dark web users.
Coming to the 1990's also known as the decade of the internet boom & the Dot-Com bubble. In 1991, after the release of MP3 compression formats & the internet becoming publicly available, people began to illegally rip CD's. It didn't take long for illegally ripped music to make its way online, and later to a music sharing site called 'Napster'. As people began to come to the realization that internet could be a one-stop shop to get anything they want, whenever they want, it was only a matter of time for more illegal transactions to start blooming to their full glory online paving a way for criminals specially hackers. Freenet even though not as popular as Tor, did help to stimulate the demand for accessing the internet anonymously. Anonymity which was being introduced to revolt against oppression at that time lead to a playground for hackers.
2.2 Release of Tor
From 1960's till 1990's there was a growing demand for accessing any content that was desired & away from the government's prying eyes. This demand was answered by tor which was instrumental in paving the way for dark web. David Goldschlag, Mike Reed, and Paul Syverson started to find a way for routing the traffic through internet anonymously in response to growing concerns over the lack of securty at the U.S. Naval Research Lab in the 90's which led to more harm than good. They planned to achieve this goal using multiple servers or network nodes called onion routers to route the internet traffic and encrypt it long the way, coining a term for their idea 'onion routing'. In an onion network, traffic is encapsulated in layers of encryption, which can be compared to layers of an onion hence the name onion routing. Each of the routers 'peels' a single layer, uncovering the data's next destination.
Tor's creators had good intentions specially when they made the platform free and modified it to address government censorships by developing a way for the internet traffic to get around government firewalls. They were motivated by the user's demands so that the people under oppressive government regimes could publish their thoughts and access restricted websites freely. But, in doing so they ran into a greater problem, the platform became complex which restricted its usage to only tech-savvy people. Though most of the dark websites came into picture to help those living under oppressive regimes, the temptation of having a place on the internet where you could browse anonymously paved way for a rise in the number of dark websites which took part in illegal activities.
Tor provided a way for people to access social media, blocked websites & critical resources while protecting their identities online. So, the dark web itself wasn't the problem, it was how a person or organisation decided to utilize it. Journalists used it for good, to spread awareness to raise a voice, white hat hackers used it for good as well, supporting governments trying to catch terrorists dealing in firearms, but some choose to side with the criminals which were the black and grey hat hackers.
2.3 Release of Bitcoin
No one wanted to risk using credit cards or PayPal for online illegal transactions because they leave paper trails, which could potentially lead to customers being located thousands of miles away. This could defy the purpose of maintaining anonymity, but cryptocurrency came to the rescue so all the illicit activities and services like hiring hackers or selling confidential data online could be paid for. Cryptocurrency wasn't as we know it to be today until Satoshi Nakamoto "mined" the first Bitcoin which started a revolution in illegal transactions. Bitcoin wasn't the first cryptocurrency but the most famous till date as it solved the problem that other cryptocurrencies couldn't address. Bitcoin heaving a special accounting ledger in place forbid users from copying the money. Bitcoin helped hackers get paid online for their explicit services while maintaining anonymity which was what aggravated the desire for most of the black hat hackers and dark web became their personalised cocoon.

Chapter 3a



PLAGIARISM SCAN REPORT

Report Generation Date: **July 26,2021**
Excluded URL: **Not Given.**
Words: **613**
Characters: **4055**

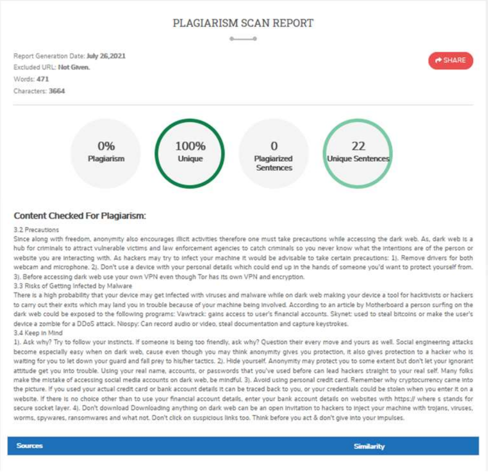
SHARE

0% Plagiarism
100% Unique
0 Plagiarized Sentences
30 Unique Sentences

Content Checked For Plagiarism:

Chapter 3: Accessing the Dark Web
Dark web is a dangerous place to play around even for an experienced IT professional let alone a newbie. Hence, we should keep in mind certain things before we take on the task of accessing the dark web where not only professional hackers but other criminals wait for naive users to trap them in a never-ending cycle of gloom by stealing their credentials, getting them involved in activities that are illegal or hacking into their machine and using them for activities of criminal nature without their knowledge.
3.1 Ways of Accessing the Dark Web
There are various ways of accessing the dark web. Tor is the most well know way as it provides secrecy and anonymity by passing requests through a series of specially configured computers forming a relay. The use of I2P (Invisible Internet Project), Freenet, GNUNet, FAI (Free Anonymous Internet) & ZeroNet which are other peer-to-peer networks with layered encryption led to creation of dark web. Even though till now we have mainly brought up tor in out discussion, there are multiple ways to access the dark web. Following are the means of accessing the dark web apart from Tor: 1). I2P I2P is an anonymous network which can be used as an alternative to Tor. But, unlike Tor it can't be used to access public internet as well as .onion sites because it's a completely separate network from Tor. I2P uses its own hidden sites, 'eepsites'.
• Both Tor as well as I2P have a peer-to-peer routing structure combined with layered encryption for a private and anonymous browsing experience.
• Even though there are few restrictions with accessing sites in I2P, it does have certain advantages as well, one of them being it's much faster and more reliable as compared to Tor which is a huge plus point as in hacking every second counts. This advantage over Tor exists because of the advanced peer-to-peer structure and lack of reliability on a directory to get route information.
• 1n 12P eavesdropper can only catch inbound or outbound traffic not both due to the use of one-way tunnels which could be a disadvantage for a hacker trying to intrude in your business.
• Configuration: There is a lot of configurations which need to be done though the router console to use I2P. After downloading and installing I2P each individual application must be configured one by one to work with it. The browser's proxy settings need to be configured as well to use the correct port.
2). Freenet Freenet is a self-contained peer-to-peer distributed datastore network. Just like I2P it can't be used to access the public web & can only be used to access the content uploaded to the Freenet. Anything uploaded on Freenet stays there indefinitely even if you stop using it. It's still an experiment designed to resist DoS attacks & censorships. Unlike Tor and I2p you don't need a server to host the content.
• Configuration: It is fairly straightforward you just need to download it, install it, and then run it. Freenet will be running through its web-based interface when you open your browser, which should be a separate browser than your usual one to help ensure anonymity.
There are 2 modes for connecting: Darknet & Opennet.
• Darknet: It allows you to specify who your friends are on the network and you only connect and share with them. This is great specially for a hacker as they can form a close-knit anonymous network made up of people they trust.
• Opennet: It automatically assigns peers on the network & uses a handful of centralized servers apart from the decentralized peer-to-peer network.

Chapter 3b



PLAGIARISM SCAN REPORT

Report Generation Date: **July 26,2021**
Excluded URL: **Not Given.**
Words: **471**
Characters: **3664**

SHARE

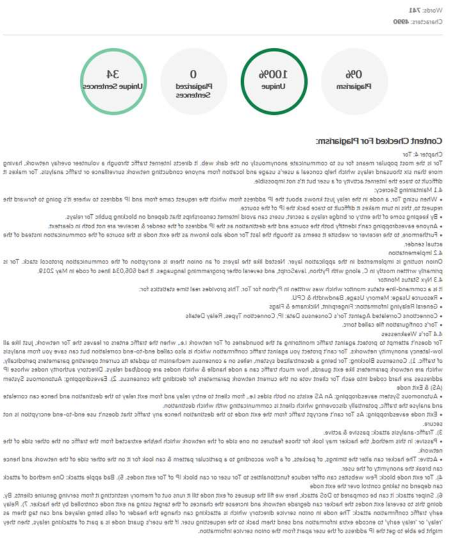
0% Plagiarism
100% Unique
0 Plagiarized Sentences
22 Unique Sentences

Content Checked For Plagiarism:

3.2 Precautions
Since along with freedom, anonymity also encourages illicit activities therefore one must take precautions while accessing the dark web. As, dark web is a hub for criminals to attract vulnerable victims and law enforcement agencies to catch criminals so you never know what the intentions are of the person or website you are interacting with. As hackers may try to infect your machine it would be advisable to take certain precautions: 1). Remove drivers for both webcam and microphone. 2). Don't use a device with your personal details which could end up in the hands of someone you'd want to protect yourself from. 3). Before accessing dark web use your own VPN even though Tor has its own VPN and encryption.
3.3 Risks of Getting Infected by Malware
There is a high probability that your device may get infected with viruses and malware while on dark web making your device a tool for hacktivists or hackers to carry out their exits which may land you in trouble because of your machine being involved. According to an article by Motherboard a person surfing on the dark web could be exposed to the following programs: Vawtrack: gains access to user's financial accounts. Skynet: used to steal bitcoins or make the user's device a zombie for a DDoS attack. Niospy: Can record audio or video, steal documentation and capture keystrokes.
3.4 Keep in Mind
1). Ask why? Try to follow your instincts. If someone is being too friendly, ask why? Question their every move and yours as well. Social engineering attacks become especially easy when on dark web, cause even though you may think anonymity gives you protection, it also gives protection to a hacker who is waiting for you to let down your guard and fall prey to his/her tactics. 2). Hide yourself. Anonymity may protect you to some extent but don't let your ignorant attitude get you into trouble. Using your real name, accounts, or passwords that you've used before can lead hackers straight to your real self. Many folks make the mistake of accessing social media accounts on dark web, be mindful. 3). Avoid using personal credit card. Remember why cryptocurrency came into the picture. If you used your actual credit card or bank account details it can be traced back to you, or your credentials could be stolen when you enter it on a website. If there is no choice other than to use your financial account details, enter your bank account details on websites with https:// where s stands for secure socket layer. 4). Don't download Downloading anything on dark web can be an open invitation to hackers to inject your machine with trojans, viruses, worms, spywares, ransomwares and what not. Don't click on suspicious links too. Think before you act & don't give into your impulses.

Sources	Similarity

Chapter 4



Words: **741**

Characters: **4990**

Content Checked For Plagiarism:

Chapter 4: Tor

Tor is the most popular means for us to communicate anonymously on the dark web. It directs internet traffic through a volunteer overlay network, having more than six thousand relays which help conceal a user's usage and location from anyone conducting network surveillance or traffic analysis. Tor makes it difficult to trace the internet activity of a user but it's not impossible.

4.1 Maintaining Secrecy:

- When using Tor, a node in the relay just knows about the IP address from which the request came from and IP address to where it's going to forward the request to, this in turn makes it difficult to trace back the IP of the source.
- By keeping some of the entry or bridge relays a secret, users can avoid internet censorships that depend on blocking public Tor relays.
- Anyone eavesdropping can't identify both the source and the destination as the IP address of the sender & receiver are not both in cleartext.
- Furthermore, to the receiver or website it seems as though the last Tor node also known as the exit node is the source of the communication instead of the actual sender.

4.2 Implementation

Onion routing is implemented in the application layer. Nested like the layers of an onion there is encryption of the communication protocol stack. Tor is primarily written mostly in C, along with Python, JavaScript, and several other programming languages. It had 505,034 lines of code in May 2019.

4.3 Nyx Status Monitor

It is a command-line status monitor which was written in Python for Tor. This provides real time statistics for:

- Resource Usage: Memory Usage, Bandwidth & CPU.
- General Relaying Information: Fingerprint, Nickname & Flags
- Connections Correlated Against Tor's Consensus Data: IP, Connection Types, Relay Details
- Tor's configuration file called torrc.

4.4 Tor's Weaknesses

Tor doesn't attempt to protect against traffic monitoring at the boundaries of Tor network i.e., when the traffic enters or leaves the Tor network, just like all low-latency anonymity networks. Tor can't protect you against traffic confirmation which is also called end-to-end correlation but can save you from analysis of traffic. 1). Consensus Blocking: Tor being a decentralized system, relies on a consensus mechanism to update its current operating parameters periodically, which are network parameters like exit guards, how much traffic can a node handle & which nodes are good\bad relays. Directory authority nodes whose IP addresses are hard coded into each Tor client vote on the current network parameters for deciding the consensus. 2). Eavesdropping: Autonomous System (AS) & Exit node

- Autonomous System eavesdropping: An AS exists on both sides i.e., from client to entry relay and from exit relay to the destination and hence can correlate and analyse the traffic, potentially discovering which client is communicating with which destination.
- Exit node eavesdropping: As Tor can't encrypt traffic from the exit node to the destination hence any traffic that doesn't use end-to-end encryption is not secure.

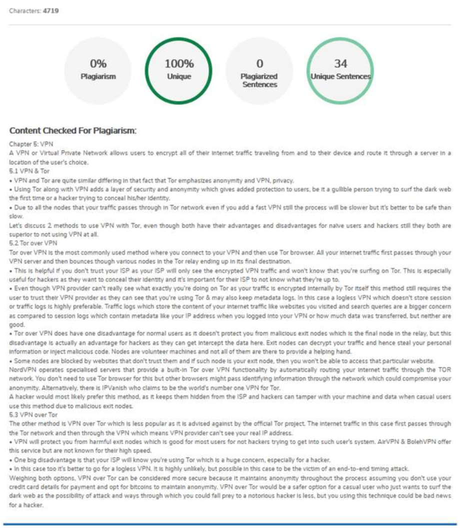
3). Traffic-analysis attack: passive & active.

- Passive: In this method, the hacker may look for those features on one side of the network which he/she extracted from the traffic on the other side of the network.
- Active: The hacker can alter the timings, of packets, of a flow according to a particular pattern & can look for it on the other side of the network and hence can break the anonymity of the user.

4). Tor exit node block: Few websites can offer reduce functionalities to Tor user or can block IP of Tor exit nodes. 5). Bad apple attack: One method of attack can depend on taking control over the exit node

6). Sniper attack: It can be compared to DoS attack, here we fill the queues of exit node till it runs out of memory restricting it from serving genuine clients. By, doing this to several exit nodes the hacker can degrade network and increase the chances of the target using an exit node controlled by the hacker. 7). Relay early traffic confirmation attack: The node in onion service directory which is attacking can change the header of cells being relayed and can tag them as 'relay' or 'relay early' to encode extra information and send them back to the requesting user. If the user's guard node is a part of attacking relays, then they might be able to get the IP address of the user apart from the onion service information.

Chapter 5



Characters: **4719**

Content Checked For Plagiarism:

Chapter 5: VPN

A VPN or Virtual Private Network allows users to encrypt all of their internet traffic traveling from and to their device and route it through a server in a location of the user's choice.

5.1 VPN & Tor

- VPN and Tor are quite similar differing in that fact that Tor emphasizes anonymity and VPN, privacy.
- Using Tor along with VPN adds a layer of security and anonymity which gives added protection to users, be it a gullible person trying to surf the dark web the first time or a hacker trying to conceal his/her identity.
- Due to all the nodes that your traffic passes through in Tor network even if you add a fast VPN still the process will be slower but it's better to be safe than slow.

Let's discuss 2 methods to use VPN with Tor, even though both have their advantages and disadvantages for naive users and hackers still they both are superior to not using VPN at all.

5.2 Tor over VPN

Tor over VPN is the most commonly used method where you connect to your VPN and then use Tor browser. All your internet traffic first passes through your VPN server and then bounces though various nodes in the Tor relay ending up in its final destination.

- This is helpful if you don't trust your ISP as your ISP will only see the encrypted VPN traffic and won't know that you're surfing on Tor. This is especially useful for hackers as they want to conceal their identity and it's important for their ISP to not know what they're up to.
- Even though VPN provider can't really see what exactly you're doing on Tor as your traffic is encrypted internally by Tor itself this method still requires the user to trust their VPN provider as they can see that you're using Tor & may also keep metadata logs. In this case a logless VPN which doesn't store session or traffic logs is highly preferable. Traffic logs which store the content of your internet traffic like websites you visited and search queries are a bigger concern as compared to session logs which contain metadata like your IP address when you logged into your VPN or how much data was transferred, but neither are good.
- Tor over VPN does have one disadvantage for normal users as it doesn't protect you from malicious exit nodes which is the final node in the relay, but this disadvantage is actually an advantage for hackers as they can get intercept the data here. Exit nodes can decrypt your traffic and hence steal your personal information or inject malicious code. Nodes are volunteer machines and not all of them are there to provide a helping hand.
- Some nodes are blocked by websites that don't trust them and if such node is your exit node, then you won't be able to access that particular website.

NordVPN operates specialised servers that provide a built-in Tor over VPN functionality by automatically routing your internet traffic through the TOR network. You don't need to use Tor browser for this but other browsers might pass identifying information through the network which could compromise your anonymity. Alternatively, there is IPVanish who claims to be the world's number one VPN for Tor.

A hacker would most likely prefer this method, as it keeps them hidden from the ISP and hackers can tamper with your machine and data when casual users use this method due to malicious exit nodes.

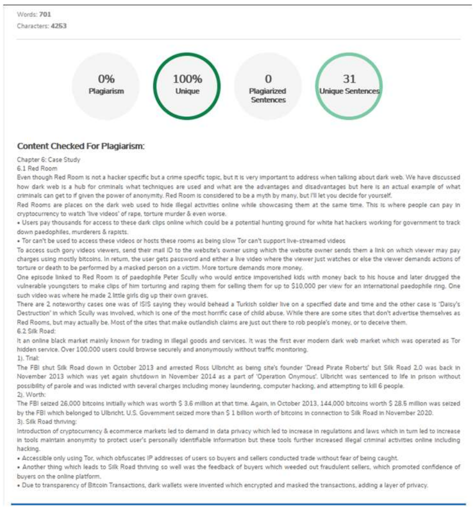
5.3 VPN over Tor

The other method is VPN over Tor which is less popular as it is advised against by the official Tor project. The internet traffic in this case first passes through the Tor network and then through the VPN which means VPN provider can't see your real IP address.

- VPN will protect you from harmful exit nodes which is good for most users for not hackers trying to get into such user's system. AirVPN & BolehVPN offer this service but are not known for their high speed.
- One big disadvantage is that your ISP will know you're using Tor which is a huge concern, especially for a hacker.
- In this case too it's better to go for a logless VPN. It is highly unlikely, but possible in this case to be the victim of an end-to-end timing attack.

Weighing both options, VPN over Tor can be considered more secure because it maintains anonymity throughout the process assuming you don't use your credit card details for payment and opt for bitcoins to maintain anonymity. VPN over Tor would be a safer option for a casual user who just wants to surf the dark web as the possibility of attack and ways through which you could fall prey to a notorious hacker is less, but you using this technique could be bad news for a hacker.

Chapter 6



Words: **701**

Characters: **4253**

Content Checked For Plagiarism:

Chapter 6: Case Study

6.1 Red Room

Even though Red Room is not a hacker specific but a crime specific topic, but it is very important to address when talking about dark web. We have discussed how dark web is a hub for criminals what techniques are used and what are the advantages and disadvantages but here is an actual example of what criminals can get to if given the power of anonymity. Red Room is considered to be a myth by many, but I'll let you decide for yourself.

Red Rooms are places on the dark web used to hide illegal activities online while showcasing them at the same time. This is where people can pay in cryptocurrency to watch 'live videos' of rape, torture murder & even worse.

- Users pay thousands for access to these dark clips online which could be a potential hunting ground for white hat hackers working for government to track down paedophiles, murderers & rapists.
- Tor can't be used to access these videos or hosts these rooms as being slow Tor can't support live-streamed videos

To access such gory videos viewers, send their mail ID to the website's owner using which the website owner sends them a link on which viewer may pay charges using mostly bitcoins. In return, the user gets password and either a live video where the viewer just watches or else the viewer demands actions of torture or death to be performed by a masked person on a victim. More torture demands more money.

One episode linked to Red Room is of paedophile Peter Scully who would entice impoverished kids with money back to his house and later drugged the vulnerable youngsters to make clips of him torturing and raping them for selling them for up to $10,000 per view for an international paedophile ring. One such video was where he made 2 little girls dig up their own graves.

There are 2 noteworthy cases one was of ISIS saying they would behead a Turkish soldier live on a specified date and time and the other case is 'Daisy's Destruction' in which Scully was involved, which is one of the most horrific case of child abuse. While there are some sites that don't advertise themselves as Red Rooms, but may actually be. Most of the sites that make outlandish claims are just out there to rob people's money, or to deceive them.

6.2 Silk Road:

It an online black market mainly known for trading in illegal goods and services. It was the first ever modern dark web market which was operated as Tor hidden service. Over 100,000 users could browse securely and anonymously without traffic monitoring.

1). Trial:

The FBI shut Silk Road down in October 2013 and arrested Ross Ulbricht as being site's founder 'Dread Pirate Roberts' but Silk Road 2.0 was back in November 2013 which was yet again shutdown in November 2014 as a part of 'Operation Onymous'. Ulbricht was sentenced to life in prison without possibility of parole and was indicted with several charges including money laundering, computer hacking, and attempting to kill 6 people.

2). Worth:

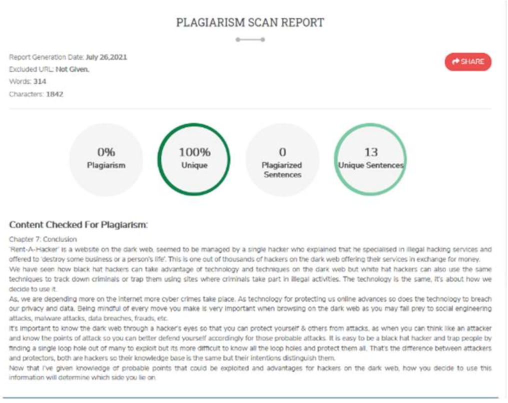
The FBI seized 26,000 bitcoins initially which was worth $ 3.6 million at that time. Again, in October 2013, 144,000 bitcoins worth $ 28.5 million was seized by the FBI which belonged to Ulbricht. U.S. Government seized more than $ 1 billion worth of bitcoins in connection to Silk Road in November 2020.

3). Silk Road thriving:

Introduction of cryptocurrency & ecommerce markets led to demand in data privacy which led to increase in regulations and laws which in turn led to increase in tools maintain anonymity to protect user's personally identifiable information but these tools further increased illegal criminal activities online including hacking.

- Accessible only using Tor, which obfuscates IP addresses of users so buyers and sellers conducted trade without fear of being caught.
- Another thing which leads to Silk Road thriving so well was the feedback of buyers which weeded out fraudulent sellers, which promoted confidence of buyers on the online platform.
- Due to transparency of Bitcoin Transactions, dark wallets were invented which encrypted and masked the transactions, adding a layer of privacy.

Chapter 7



PLAGIARISM SCAN REPORT

Report Generation Date: **July 26,2021**

Excluded URL: **Not Given.**

Words: **314**

Characters: **1842**

Content Checked For Plagiarism:

Chapter 7: Conclusion

'Rent-A-Hacker' is a website on the dark web, seemed to be managed by a single hacker who explained that he specialised in illegal hacking services and offered to 'destroy some business or a person's life'. This is one out of thousands of hackers on the dark web offering their services in exchange for money.

We have seen how black hat hackers can take advantage of technology and techniques on the dark web but white hat hackers can also use the same techniques to track down criminals or trap them using sites where criminals take part in illegal activities. The technology is the same, it's about how we decide to use it.

As, we are depending more on the internet more cyber crimes take place. As technology for protecting us online advances so does the technology to breach our privacy and data. Being mindful of every move you make is very important when browsing on the dark web as you may fall prey to social engineering attacks, malware attacks, data breaches, frauds, etc.

It's important to know the dark web through a hacker's eyes so that you can protect yourself & others from attacks, as when you can think like an attacker and know the points of attack so you can better defend yourself accordingly for those probable attacks. It is easy to be a black hat hacker and trap people by finding a single loop hole out of many to exploit but its more difficult to know all the loop holes and protect them all. That's the difference between attackers and protectors, both are hackers so their knowledge base is the same but their intentions distinguish them.

Now that I've given knowledge of probable points that could be exploited and advantages for hackers on the dark web, how you decide to use this information will determine which side you lie on.

References

IEEE Papers

[1] A Dark Web Story In-Depth Research and Study Conducted on the Dark Web based on Forensic Computing and Security in Malaysia. (2017) Mohammed Farook Bin Rafiuddin, Hamza Minhas, Prethpal Singh Dhubb
[2] Evolution of Dark Web Threat Analysis and Detection: A systematic Approach. (2020) Saiba Nazah, Shamsul Huda, Jemal Abawajy, Mohammad Mehedi Hassan

WEB Resources

[3] Dark Web Analysis Shows high demand for Hackers
https://www.helpnetsecurity.com/2021/02/10/dark-web-analysis-shows-high-demand-for-hackers/
[4] Deep Web & Dark Web
https://us.norton.com/internetsecurity-how-to-how-can-i-access-the-deep-web.html
[5] History of Dark Web
https://www.soscanhelp.com/blog/history-of-the-dark-web
[6] VPN &Tor
https://www.comparitech.com/blog/vpn-privacy/access-dark-web-safely-vpn/
[7] Tor
https://en.wikipedia.org/wiki/Tor_(network)
[8] Silk Road
https://en.wikipedia.org/wiki/Silk_Road_(marketplace)