IS2109 Information Systems Security- IS 2109
Practical 8
Secure Web Browsing

1)

i.

Pseudo-anonymity is the appearance, but not the reality of anonymity online. It enables anonymous posting and commenting. However, administrators have access to information that can be used to ban users and keep them from returning.

ii.

Protected File Sharing can take place.
Remote Access is available.
Anonymity is maintained.
It shall bypass Blockers and Filters.
It shall improve the performance and is more affordable.

iii.

VPN stands for Virtual Private Network which shall allow you to create a secure connection to another network over the Internet. It can also be used to access region-restricted websites, shield your browsing activity from prying eyes on public Wi-Fi and more.

iv.

VPNs can be divided into three main categories as remote access, intranet-based site-to-site, and extranet-based site-to-site.
Individual users are most likely to use remote access VPNs, whereas big businesses often implement site-to-site VPNs for corporate purposes. Remote access VPNs connect the user to a secure remote server in order to access a private network. The added encryption ensures that security isn't compromised. Upon this Commercial VPN services are built. Such providers allow you to use their own network when surfing the internet. As a result, you can browse away in privacy, access content on the internet that's otherwise restricted to your regular connection, and keep your data safe from hackers and snoopers. Site-to-site VPNs is providing multiple users in various fixed locations with the ability to access each other's resources. Extranet-based is used when a connection between two separate intranets is required, but without the possibility of one accessing the other directly.

v.

A.

IPsec is a group of protocols that are used together to set up encrypted connections between devices. It helps keep data sent over public networks secure. IPsec is often used to set up VPNs, and it works by encrypting IP packets, along with authenticating the source where the packets come from. "IP" stands for "Internet Protocol" and "sec" for "secure."

B.

Internet Key Exchange is a protocol used to set up a secure, authenticated communications channel between two parties. IKE is part of the Internet Security Protocol which is responsible for negotiating security associations, which are a set of mutually agreed-upon keys and algorithms to be used by both parties trying to establish a VPN connection.

C.

In computer networking, Layer 2 Tunneling Protocol is a tunneling protocol used to support virtual private networks or as part of the delivery of services by ISPs. It uses encryption only for its own control messages, and does not provide any encryption or confidentiality of content by itself.

D.

TLS is a cryptographic protocol that provides end-to-end security of data sent between applications over the Internet. It is mostly familiar to users through its use in secure web browsing, and in particular the padlock icon that appears in web browsers when a secure session is established.

vi.

Tunnels

A VPN tunnel is an encrypted connection between the computer or mobile device and the wider internet. Since The connection is encrypted, nobody along the VPN tunnel is able to intercept, monitor, or alter your communications. When our device initiates a VPN connection, your entire network traffic passes through a secure tunnel.

Endpoints

VPN goes between a computer and a network, or a LAN and a network using two routers. Each end of the connection is an VPN "endpoint"

Sessions

VPN session is a virtual private network (VPN) extends a private network across a public network and enables users to send and receive data across shared or public networks as if their computing devices were directly connected to the private network.

vii.

Small bits of the data can be used to build a unique profile with potentially identifying information, We test for privacy issues such as DNS leaks, IP leaks, and WebRTC leaks; all of which are security flaws that could share your data with outside parties; using publicly available tools like the DNS Leak Test from Perfect Privacy, IPLeak and IPv6 Test.

We look for VPNs that offer security tools like Perfect Forward Secrecy, split tunneling, aggressive ad blockers and any unique security features. Jurisdiction and ownership transparency are also important. While user needs may vary, the ideal VPN would be located outside of those countries which participate in US intelligence sharing agreements, with an ownership structure visible for public verification.

viii.

- Stop ISP throttling
- Block Malware
- Bypass Government-mandated Censorship
- Access Online Bank Accounts from Overseas
- P2P Safely
- Use WhatsApp in China
- Secure Browsing
- Stop Unwanted Data Collection
- Unblocking YouTube
- Unblocking Netflix Regional Content
- Watch NBA
- Access Disney Plus (Disney+)

ix.

<u>Address Translation Issues</u>

With address translation, the address translation device can translate one IP address to another and, possibly, one port number to another. Mapping one IP address to another is commonly referred to as network address translation (NAT); mapping multiple IP addresses to one IP address and differentiating them by different source port numbers is commonly referred to as port address translation (PAT) or address overloading.

Firewall Issues

VPNs have issues with traveling through stateful filtering firewalls. A stateful firewall keeps track of the state of a connection, allowing only returning traffic for outbound connections, by default. The stateful function is based on keeping track of sessions between devices. In most cases, this only includes TCP and UDP sessions. That is because it is very easy to track TCP and UDP sessions by examining the source and destination IP addresses, and the source and destination port numbers of these values change, the change indicates a different connection.

x.

Step 1: Checking to see which version of Ubuntu you have

Since there are 32 bit and 64 bit flavors of VPN Softwares available, the first thing you'll want to do before getting started is checking to see which version of Ubuntu you're currently using. To do this, first open the Terminal through either Ubuntu Dash or Ctrl+Alt+T shortcut. Once the Terminal is opened, enter the following command:

$ lscpu

Step 2: Updating System Apt Cache and Packages

Next we want to update our system's apt cache and packages to the latest versions so that no issues arise during installation. This can be done by running the following commands:

$ sudo apt-get update
$ sudo apt-get upgrade

Step 3: Installation of OpenVPN

In most Linux distros, OpenVPN is already installed. But it is better to verify this beforehand. Enter the following command to do this:

$ sudo apt-get install openvpn

Step 4: Installation of Network Manager Packages

The easiest way to set up and install VPN in Linux is through the Network Manager. It basically is a mandatory package that allows us to import and use the OpenVPN Config files. Installation of this package can be done by the following commands:

$ sudo apt install network-manager-open vpn network-manager-openvpn-gnome

Step 5: Download the OpenVPN Configurations

Now you have to select your VPN service that you'll be using to set up VPN on your Linux distro. It is important to note that you have to select the OpenVPN configuration files of your VPN service for the set up. To get your OpenVPN configurations, you have to sign in to your VPN account and check in the Linux support or OpenVPN support slot (different for all VPN Services).

Step 6: Setting up the VPN

Now finally we will be using the Network Manager to set up our VPN Connection

2.

i.

The dark web refers to encrypted online content that is not indexed by conventional search engines. The dark web is a part of the deep web, which just refers to websites that do not appear on search engines.

ii.

Deep web is usually used for legit purposes that require anonymity but dark web is sometimes used for illegal activities.
To access Deep web, you require a password, encryption whereas to access dark web you require Tor project or a similar browser.
Both deep and Dark web are hidden and not shown to conventional search engines.
Deep web is larger than the Surface web on the other hand Dark web size is unmeasurable.

iii.

Onion routing is a technique for anonymous communication over a computer network. In an onion network, messages are encapsulated in layers of encryption, analogous to layers of an onion.
The encrypted data is transmitted through a series of network nodes called onion routers, each of which "peels" away a single layer, uncovering the data's next destination.

iv.

The hidden service is a site you visit or a service you use that uses Tor technology to stay secure and, if the owner wishes, anonymous.

v.

Tor directs internet traffic through a network of thousands of relays, many of which are set up and maintained by volunteers.
Messages are encapsulated in layers of encryption, comparable to the layers of an onion. Inside the Tor network are. onion sites, or 'hidden services'.
Tor facilitates anonymized browsing by allowing traffic to pass onto or through the network through nodes that only know the immediately preceding and following node in a relay.
The source and destination of messages is obscured by encryption.

vi.

TOR	VPN
● Comparatively slow ● Only PC compatible ● High Encryption ● Completely Free ● Allow anonymous accessing to web ● Can use to access dark web	● Faster than Tor ● All the devices compatible(Android, windows) ● Good Encryption ● Need to pay to use a fast, good VPN ● Cookies will create ● Cannot use to access dark web

vii.

- Speed of the Tor browser is very low since data is routed through multiple relays, each with varying bandwidth.
- Using Tor browsers can lead to legal trouble.
- Many web services are blocked from accessing Tor browser.
- Does not have compatibility with all the devices. (PC version only available)

References

https://clario.co/blog/vpn-tunnel/
https://www.google.com/search?q=what+is+vpn+endpoint&oq=What+is+VPN+endpoint&aqs=chrome.0.0i457j0i22i30.8972j0j7&sourceid=chrome&ie=UTF-8
https://www.webhostingsecretrevealed.net/blog/security/how-a-vpn-can-be-useful/
https://www.guru99.com/deep-web-vs-dark-web.html
https://wire19.com/differences-between-tor-browser-and-vpn/
https://en.wikipedia.org/wiki/Onion_routing

Group 07

Name	Index Number
R.M.D.K.B. Rajakaruna	18020641
W.H.M. Gunathilaka	18020275
S. Maayura	18020461
T. Athavan	18020097
T. Thushanthan	18020844