**MIS 6330: Cybersecurity Fundamentals**

**Individual Homework 8**

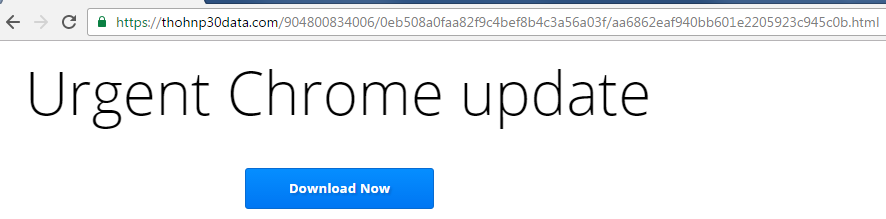
1. Solution:
   1. The destination IP address on the outer packet (not the encapsulated packet) – (b) that of the VPN gateway at the office
   2. The source address on the outer packet – (a) the ISP assigned address

The source address on the outer packet is ISP assigned address or host computer’s IP address as after encapsulating the inner packet in the outer packet, VPN software doesn’t itself send the packet to the VPN gateway.

Instead, it gives it to host computer to send it using host computer’s TCP/IP.

The destination address on the outer packet is VPN gateway as when the outer packet reaches there, the inner packet is taken out and decrypted by the VPN gateway and then sent to the destination within office network as per the destination IP address of the inner packet.

1. I have been browsing an online store, when I was suddenly redirected to the webpage shown in the screenshot below.



* It ispotentially a *Drive-by download, Cross-site scripting or Code Injection* attack due to the following reasons:
* The online store might have XSS vulnerability where they ran any script tags entered in its URL.
* The attacker could potentially create a malicious link to grab cookies by adding script tag into the URL and send it to admins. If one of the admins opened the link, the attacker would now have the admin access.
* The attacker can inject client-side script into webpages which are opened by other users.

In this case, the attacker could have added a redirection script in the online store site which redirects the user to this malicious page. Since, the user might not know that this redirection script was added by an attacker and the user might think this was an actual redirection due to some new update chrome browser had.

* This addition of malicious scripts falls under the category of *cross-site scripting* attack.

Since, *cross-site scripting* attack is a special case of *code injection* attack, this can be classified as *code injection* attack too.

* This website looks like chrome’s download link, but it is not authentic page as we can see the link is not of Google.
* In this case, an unsuspecting user might click on the *“Download Now”* button and might download a malware program that he/she didn’t intend to download.
* Also, it could happen that, the download happened automatically when the user was redirected to this malicious site.
* Both these types of attack fall under category of *Drive-by download* attack.

1. Consider the following terms: *compression virus* and *encrypted virus*.
   1. *Compression viruses* can be caught by using *integrity checks* since despite the file size will be the same as before but checksum value (or hash value) of the previously stored file and new file (with virus) will be different.

*Encrypted virus* can’t be caught by using *integrity checks* since to calculate checksum value (or hash value), the program file needs to be decrypted which can’t be done using *integrity checks*.

* 1. For *compression viruses*, I’d recommend using the *integrity checks* only since it serves the required purpose. However, *signature checks* can be added as an extra measure of security.

For *encrypted viruses*, I’d use *generic decryption* along with *signature checks or integrity checks.*

This is due to the following reasons:

By using *generic decryption*, the infected files are first decrypted. After this, it could be checked for signatures of known viruses as well as see if the original file had similar size/checksum value/hash value.

This way even if the virus is an unknown encrypted virus or a known virus inside a file, it’d be detected easily.