LETTERKENNY INSTITUTE OF TECHNOLOGY

ASSIGNMENT COVER SHEET

Lecturer’s Name: Danny Mc Fadden

Assessment Title: Addressing Digital forensics of modern networks

Work to be submitted to: Danny Mc Fadden

Date for submission of work: Sunday 24/04/2022

Place and time for submitting work:

To be completed by the Student

Student’s Name: Stephen Duffy

Class: CSDF

Subject/Module: Advanced Digital Forensics 2

Word Count (where applicable):

I confirm that the work submitted has been produced solely through my own efforts.

Student’s signature: Stephen Duffy Date: 22 – 04 - 2022

|  |
| --- |
| **Notes:**  **Penalties:** The total marks available for an assessment is reduced by 15% for work submitted up to one week late. The total marks available are reduced by 30% for work up to two weeks late. Assessment work received more than two weeks late will receive a mark of zero. [Incidents of alleged plagiarism and cheating are dealt with in accordance with the Institute’s Assessment Regulations.]  **Plagiarism:** Presenting the ideas etc. of someone else without proper acknowledgement (see section L1 paragraph 8).  **Cheating:** The use of unauthorised material in a test, exam etc., unauthorised access to test matter, unauthorised collusion, dishonest behaviour in respect of assessments, and deliberate plagiarism (see section L1 paragraph 8).  **Continuous Assessment:** For students repeating an examination, marks awarded for continuous assessment, shall normally be carried forward from the original examination to the repeat examination. |
|  |

Addressing Digital Forensics of Modern Networks

Topic: Wireshark or other packet capture devices use and roles within networks

Introduction / Methodology

**Logo, company name

Description automatically generated**

Wireshark is a packet sniffer tool/analyzer, we use Wireshark as a way of sniffing out these packets because packets are important and we want to see them in as much detail as possible, these packets are captured on a local network in real time and then stored to be analyzed. Although Wireshark isn’t the only software that does this, it has competitors such as Auvik and SolarWinds Network packet sniffer, but Wireshark is by far the more popular and best of the three.

Wireshark is really helpful with it’s different set of tools, graphing software, and ability to separate information. You can find out information about sequences, ports, IP addresses and protocols with just a click of a button.

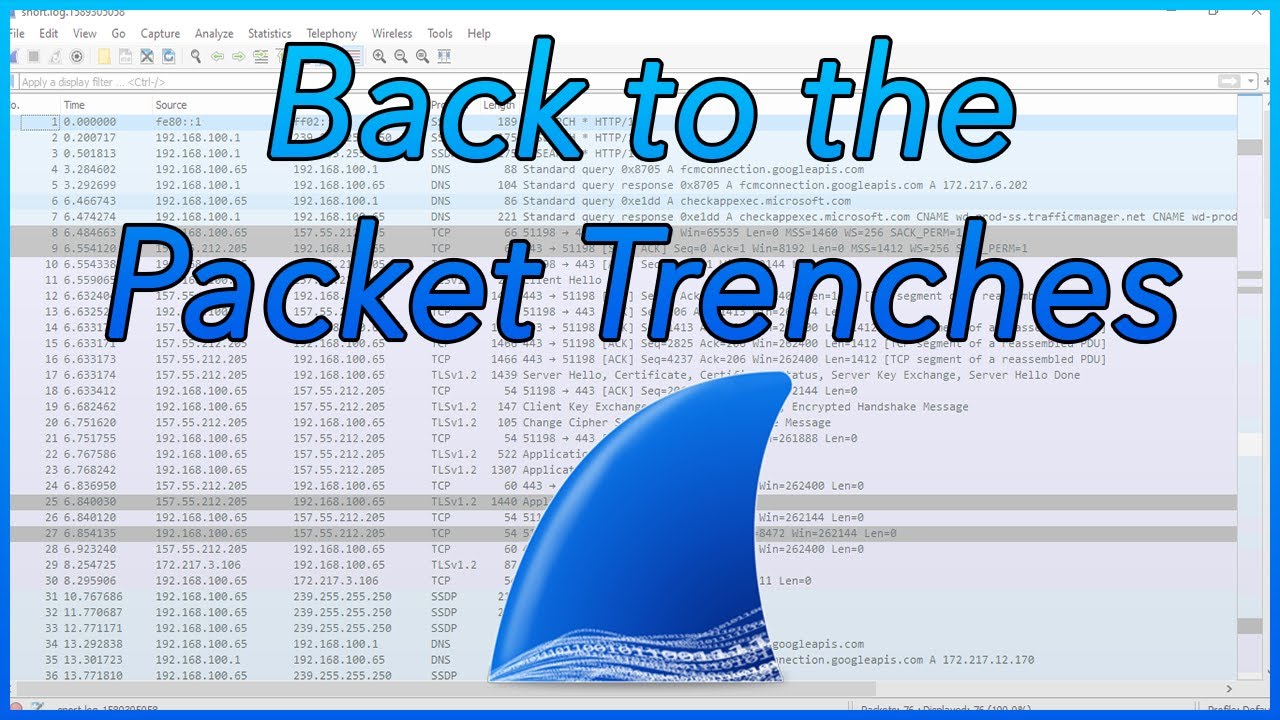
Wireshark is a great tool for simple network analyzing or troubleshooting potential issues on your network because it lets you sieve through information and use different types of filters to filter, capture and inspect the different types of packets being sent and received through your network, Wireshark can also be used to find malicious traffic and hacking possibilities in your home or work environment.

Now packets are a formatted unit of data that is passed through a network. A packet consists of information and user data and can hold so much information in just a small size of 64kb. In Wireshark we can find packets anywhere, packets have a huge importance in a network, they’re basic units of communication used over a TCP or IP network.

When a packet is sent it is basically broke down and then divided into segments and takes its route over the internet and once they arrive at their destination the packets reconstruct into the original file by the TCP layer at the receiving end.

The majority of packets that will be on your network will be layer 4 protocols such ass TCP and UDP.

Wireshark can be used to intercept and analyze encrypted TLS Traffic; symmetric keys are stored in the browser and with the right administrator permissions and knowledge you can take these session keys and load them into Wireshark to examine unencrypted web traffic.



Wireshark in security

To use Wireshark in a cybersecurity role you got to know what is normal and abnormal, while Wireshark is a protocol analyzer and packet sniffer it can be quite useful when it comes down to narrowing malicious traffic once a red flag has been spotted in your network.

To give you a rough idea of what Wireshark is capable of and how some people who work in cybersecurity use Wireshark I’m going to show you a Qakbot infection with Cobalt Strike and VNC Activity that occurred a few weeks ago on the 14/03/2022 Not only will this show you how Wireshark is used but it’ll show you how a daily consumer can be targeted through something as simple as Email and get infected by malicious malware. I believe the average consumer who uses a computer for anything business related should have basic skills for Wireshark.

So, A few weeks ago SANS ISC InfoSec decided to test the capabilities of Wireshark and decided to see if Wireshark could detect Qakbots generated traffic once a windows computer is infected.

Diagram

Description automatically generated with low confidence

They infected a vulnerable windows host with QBot malware through an email with a download link and 17 hours later infected traffic host for cobalt strike and VNC was detected, cobalt strike and VNC are commonly used Malware for going after gov orgs and big businesses so that is why it is used for this test, Like Cobalt Strike, VNC allows a remote connection to the infected computer/network.

DLL files for Qbot have tags in the code to differentiate the distribution channel, now this is very important as this is what you’d be looking for inside of Wireshark as it alters inside of the web traffic.

Once the vulnerability was downloaded and executed it created 3 OCX files on the local disk and started sending Qbot TCP C2 traffic between the botnet and infected user, Once you run a Wireshark scan and filter out the tcp packets you can actually see the infected windows host botnet ID and the public ip address off the infected windows host

After the initial 17 hours of infection cobalt strike traffic starts tcp streams for VNC traffic. After the streams started Qbot made a change to the registry.

Graphical user interface, application, table

Description automatically generated with medium confidence

So just by using Wireshark we were able to:

Detect unusual activity

Detect Qakbot on the machine

Find the DLL files

See C2 Activity

See Cobalt Strike Activity

See VNC Activity

Discover the Botnet ID and public IP address

And find the TCP streams for VNC Traffic

Conclusion:

So in short, Wireshark is a free, safe and Open-Source Packet analyzer used for Education, Troubleshooting, Software, Communications protocol Development

It is a very productive and efficient software in what it is made to do which is sniff out packets, find out where they’re going and where they’re coming from and then analyzing those packets.

Wireshark is very widely used in business and cybersecurity today as it helps us detect all kinds of infections and malicious traffic such as Qakbot, Emotet and Astaroth which all occur quite often in malspam / malicious emails - <https://twitter.com/Unit42_Intel/status/1483960736502136832>

Which can be all detected with the help of Wireshark.

Wireshark’s role in networks is to filter out the bad and keep the good and is one of the best if not the best for troubleshooting issues on your network.

References:

<https://twitter.com/Unit42_Intel/status/1483960736502136832>

<https://www.educba.com/what-is-wireshark/>

<https://www.youtube.com/watch?v=Lb-PJl9u3z8>

<https://www.youtube.com/watch?v=z8MnyxGGqNQ>

<https://www.youtube.com/watch?v=3t1BNAavrlQ&t>

<https://www.malware-traffic-analysis.net> <https://www.techtarget.com/searchnetworking/definition/packet>

<https://www.comptia.org/content/articles/what-is-wireshark-and-how-to-use-it>

<https://www.csoonline.com/article/3305805/what-is-wireshark-what-this-essential-troubleshooting-tool-does-and-how-to-use-it.html>

<https://www.howtogeek.com/104278/how-to-use-wireshark-to-capture-filter-and-inspect-packets/>