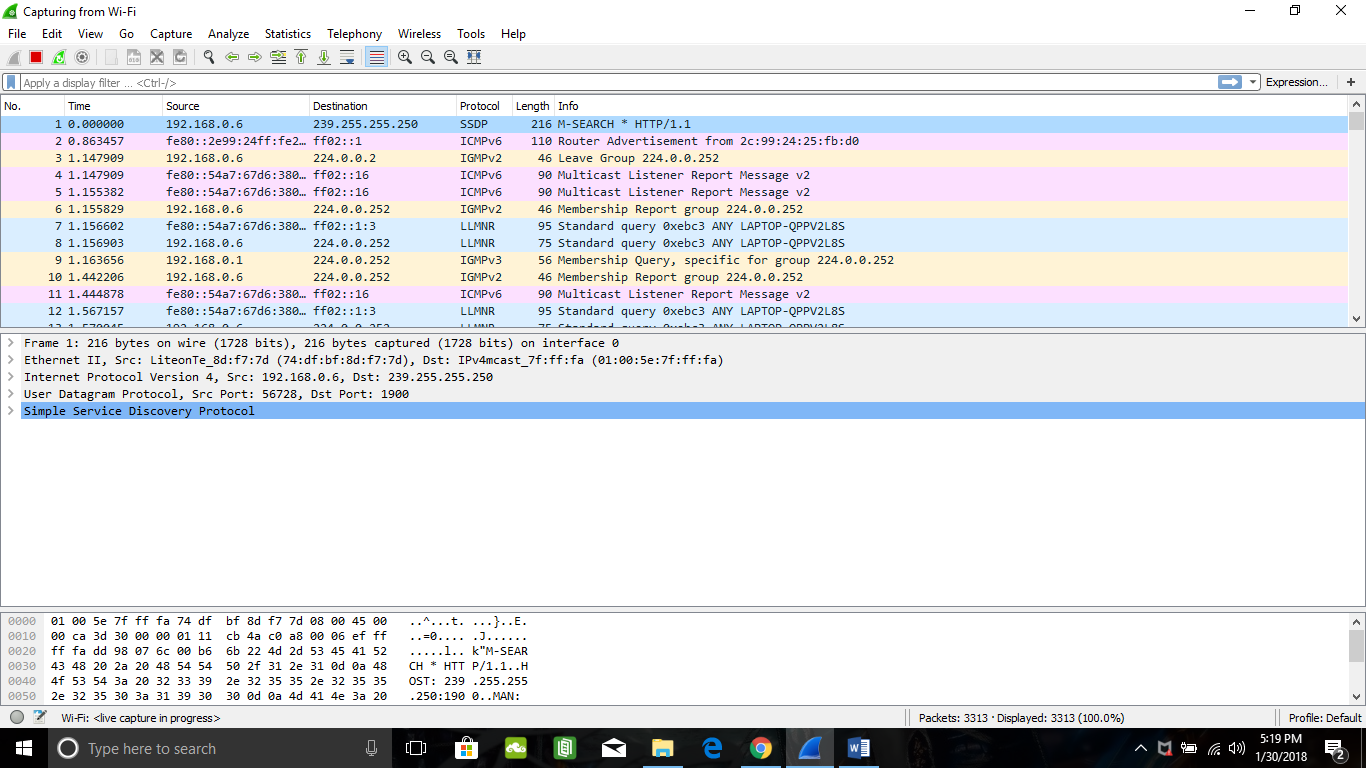
**ZAIN AHMED B00786320**

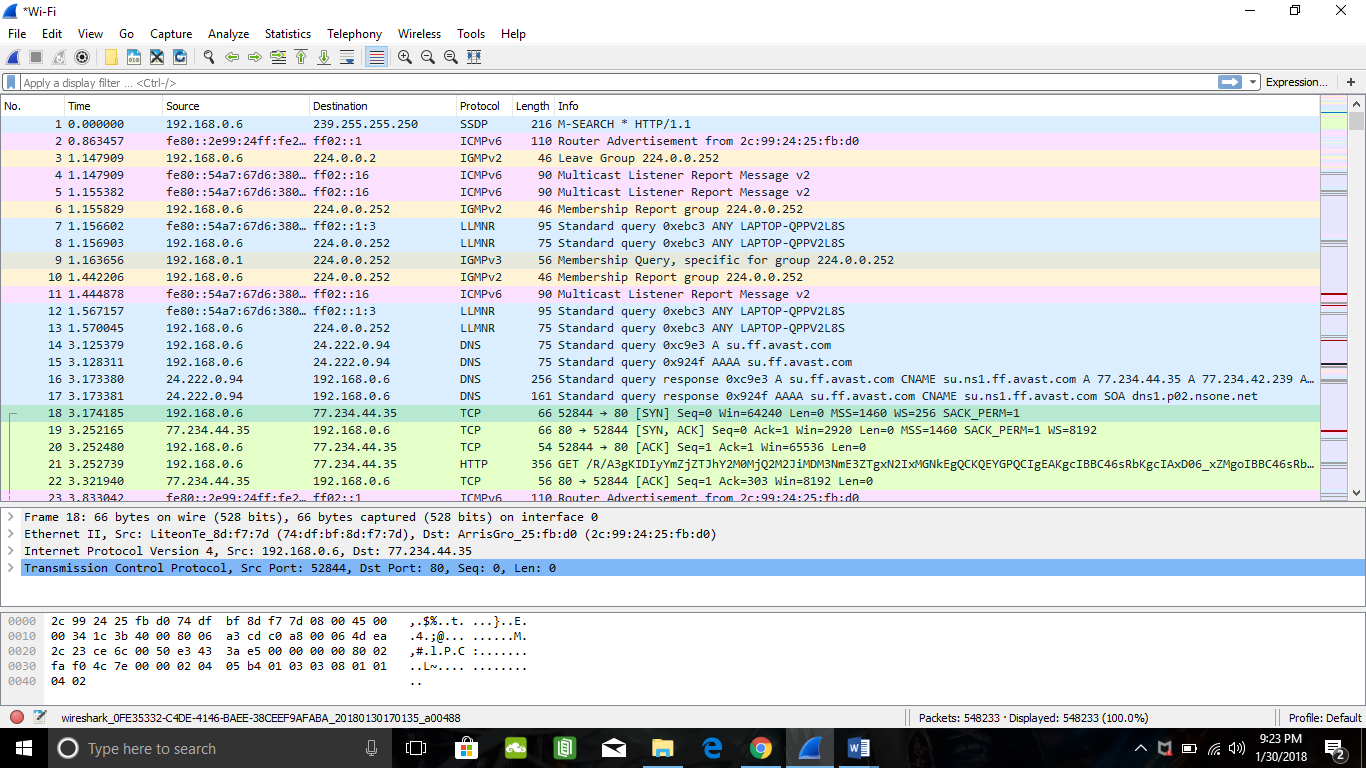
**NETWORKS SECURITY ASSIGNMENT 1**

1) WIRESHARK is used for analysing the packets in a network. The process includes accessing any URL in the browser and allowing the wireshark to start the capture.



SNAPSHOT 1: Wireshark Capture

This capture allows the user to access the details like the source address, destination address, protocols evoked, the flag, size of the packet etc.



SNAPSHOT 2: Wireshark Capture

In order to establish a connection, the Source address and the Destination is used.

**2**. **JOHN THE RIPPER**

John The Ripper is a software tool used for the purpose of cracking and testing passwords. It is an open source software which was initially developed for UNIX Operating System. It is now compatible with approximately 15 different platforms. John The Ripper is considered very effective as it performs by combining various password crackers into a single package. The key features of John The Ripper include autodetection of hast type passwords and it can be run against various encrypted password formats. [1]

**FEATURES**

John The Ripper is efficient and effective as it supports the combination of several cracking modes into a single program. It can be configured according to the desired needs and the same cracker can be used at several other places as it supports multiple platforms. John The Ripper supports the following UNIX crypt hash types:

* Traditional DES-based
* BSDI extended DES-based
* FreeBSD MD5-based
* OpenBSD Blowfish-based

John The Ripper *Pro* supports the Windows NTLM and MAC OS X 10.4+ salted SHA-1 hashes.

Most of the traditional crackers use a Crypt-style routine. But, such Crypt API could not handle the algorithms like Bitslice DES. Such algorithms require a more powerful interface like the one used in John The Ripper. Therefore, it holds an extraordinary advantage over the traditional crackers.

John The Ripper can be used by the hackers for harmful purposes such as gaining an unauthorized access to a system, cracking passwords for illegal use, stealing money and identity theft.

A network security specialist can utilize this software to recover a forgotten password or gain access in to a system for which the permission has been granted. John The Ripper offers two modes to provide the best results. One of the modes uses the Dictionary Attack which can be used by the network security specialist to crack the passwords that are relevant to the dictionary wordlists. The other mode uses the Brute force attack. In this attack the network specialist can crack the passwords that might be unavailable in the dictionary wordlist. [1]

**3**. A Distributed Denial Of Service (DDoS) is a type of attack in which the audience or the user is refrained from accessing a service or information. It is the most common type of cyber-attack which is carried out by diverting a huge amount of traffic to the server of the online service which is being attacked. The victims of these attacks comprise of banks, large organizations, news channels and various other online service providers.

RIO OLYMPICS DDoS ATTACK 2016

Rio Olympics faced a DDoS attack in 2016. Previously such Olympics were carried out by a DDoS-hire-for service called the LizardStresser. In 2016, LizardStresser used the Internet Of Things botnet along with several other botnets to initiate an attack on the Olympics. Such attack would affect a huge audience considering how big the event was. The attack was launched by diverting extremely huge amount of traffic to the Olympic association servers by an IP protocol called the Generic Routing Encapsulation. The attack was a UDP reflection/amplification attack and thus the UDP was targeted. The defenders tend to make a mistake of assuming that UDP is being used by the attackers instead of TCP. [2]

The victims of this attack were the millions of people watching the Olympics on their Televisions or other electronical devices that required online services. The attack was planned to create a chaos worldwide and deplete the image and quality of the Olympic associations that were responsible for providing the live telecast of the Olympics to the millions of people worldwide.

DEFENDING OF THE ATTACK

The attack was a UDP reflection/amplification attack. A high volume of traffic was diverted to the UDP associated servers to fool the defenders that UDP is being used for the attack instead of TCP, but the defending team had analyzed the possibilities of such an attack and were prepared for such an outcome. The defending team was not fooled by this move of the attackers. The team had gathered information and took effective countermeasures to defend the attack and were able to maintain a proper network infrastructure. The defending team was able to pull these mitigating services and provide an uninterrupted telecast to the people worldwide. [2]

**4 (a)** Frame on Token Ring1 – FTP message from S to D.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| S | R11 | S | D | 49500 | 20 | DATA |

**(b)** Frame on FDDI – FTP message from S to D.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| R14 | R21 | S | D | 49500 | 20 | DATA |

**(c)** Frame on Token Ring 2 – FTP message from S to D

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| R22 | R34 | S | D | 49500 | 20 | DATA |

**(d)** Frame on Ethernet – FTP message from S to D.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| R31 | d | S | D | 49500 | 20 | DATA |

**(e)** Frame on Token Ring 1 – FTP message from D to S.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| R11 | S | D | S | 20 | 49500 | DATA |

**(f)** Frame on FDDI – FTP message from D to S

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| R21 | R14 | D | S | 20 | 49500 | DATA |

**(g)** Frame on Token Ring 2 – FTP message from D to S

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| R34 | R22 | D | S | 20 | 49500 | DATA |

**(h)** Frame on FDDI – SSH message from S to D

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| R14 | R21 | S | D | 52000 | 22 | DATA |

**(i)** Frame on Token Ring 2 – SSH message from S to D.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| R22 | R34 | S | D | 52000 | 22 | DATA |

**(j)** Frame on Ethernet – SSH message from S to D

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| R31 | d | S | D | 52000 | 22 | DATA |

**(k)** Frame on Token Ring 1 – SSH message from D to S

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| R11 | S | D | S | 22 | 52000 | DATA |

**(l)** Frame on FDDI – SSH message from D to S.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| R21 | R14 | D | S | 22 | 52000 | DATA |