IIUC

আন্তর্জাতিক ইসলামী বিশ্ববিদ্যালয় চট্টগ্রাম

الجامعة الإسلامية العالمية شيتاغونغ

International Islamic University Chittagong

Department of Computer Science and Engineering

M.Sc in Computer Science and Engineering

Assignment 2

Packet Sniffing using Wireshark

submitted to

Mohammad Zainal Abedin

Assistant Professor

by

Yuvraj Das (MC223101)

1. Introduction:

This report presents an analysis of packet sniffing activities conducted using Wireshark, a widely used network protocol analyzer. The objective of this assignment was to gain practical experience in packet sniffing techniques and to understand the implications of unauthorized network traffic interception.

2. Methodology:

The packet sniffing activity was conducted using Wireshark, installed on a Windows operating system. Wireshark was configured to capture network traffic on the local network interface. The following steps were followed:

1. Installation: Wireshark was downloaded and installed on the Windows system from the official website (https://www.wireshark.org/).

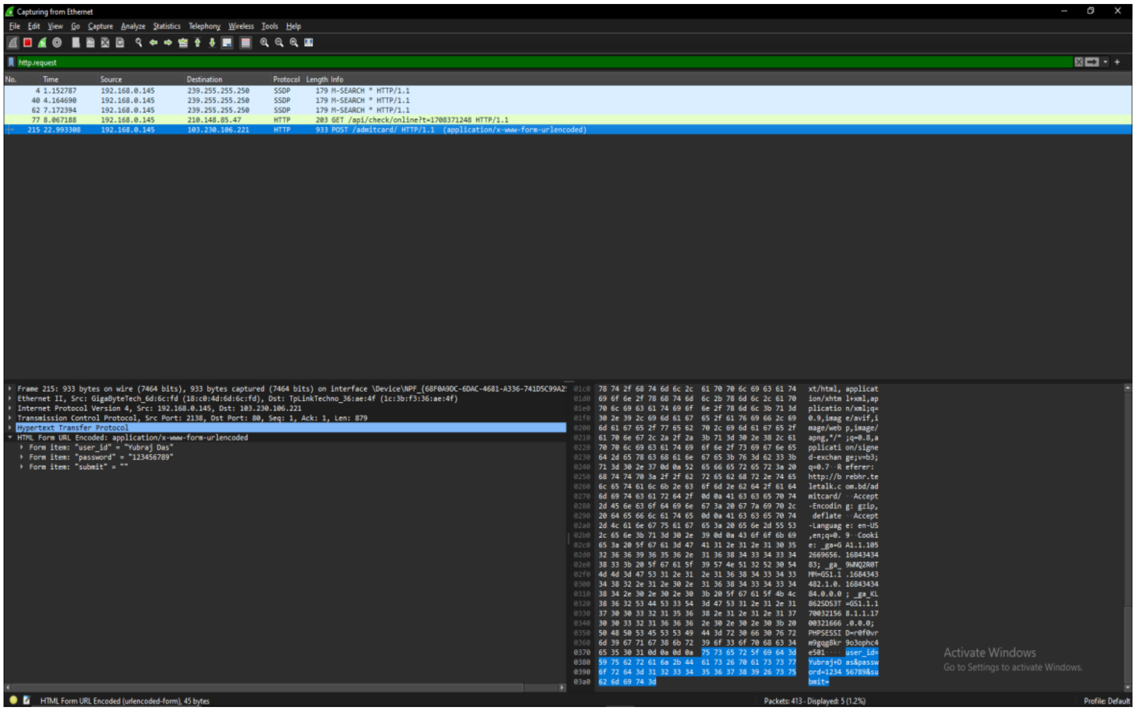
2. Capture Setup: The network interface to be monitored was selected within Wireshark's interface. In this case, the Ethernet adapter connected to the local network was chosen.

3. Capture Filtering: Filters were applied within Wireshark to focus on specific types of network traffic, such as HTTP, HTTPS, or DNS, depending on the objectives of the analysis.

4. Packet Capture: Network traffic was captured by initiating a packet capture session within Wireshark. The capture session was allowed to run for a specific duration to collect sufficient data for analysis.

5. Analysis: Captured packets were analyzed to identify various network protocols, source and destination IP addresses, ports, and any sensitive information transmitted in plaintext.

3. Practical:


Capturing from Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http.request
Activate Windows
Go to Settings to activate Windows.

```
No.   Time        Source          Destination       Protocol Length Info
    4 1.152787    192.168.0.145   239.255.255.250   SSDP      179 M-SEARCH * HTTP/1.1
   40 4.164690    192.168.0.145   239.255.255.250   SSDP      179 M-SEARCH * HTTP/1.1
   62 7.172394    192.168.0.145   239.255.255.250   SSDP      179 M-SEARCH * HTTP/1.1
   77 8.067188    192.168.0.145   210.148.85.47     HTTP      203 GET /api/check/online?t=1708371248 HTTP/1.1
  215 22.993308   192.168.0.145   103.230.106.221   HTTP      933 POST /admitcard/ HTTP/1.1  (application/x-www-form-urlencoded)
```

```
Frame 215: 933 bytes on wire (7464 bits), 933 bytes captured (7464 bits) on interface \Device\NPF_{68F0A9DC-6DAC-4681-A336-741D5C99A2
Ethernet II, Src: GigaByteTech_6d:6c:fd (18:c0:4d:6d:6c:fd), Dst: TpLinkTechno_36:ae:4f (1c:3b:f3:36:ae:4f)
Internet Protocol Version 4, Src: 192.168.0.145, Dst: 103.230.106.221
Transmission Control Protocol, Src Port: 2138, Dst Port: 80, Seq: 1, Ack: 1, Len: 879
Hypertext Transfer Protocol
HTML Form URL Encoded: application/x-www-form-urlencoded
    Form item: "user_id" = "Yubraj Das"
    Form item: "password" = "123456789"
    Form item: "submit" = ""
```

```
01c0  78 74 2f 68 74 6d 6c 2c  61 70 70 6c 69 63 61 74   xt/html, applicat
01d0  69 6f 6e 2f 78 68 74 6d  6c 2b 78 6d 6c 2c 61 70   ion/xhtm l+xml,ap
01e0  70 6c 69 63 61 74 69 6f  6e 2f 78 6d 6c 3b 71 3d   plicatio n/xml;q=
01f0  30 2e 39 2c 69 6d 61 67  65 2f 61 76 69 66 2c 69   0.9,imag e/avif,i
0200  6d 61 67 65 2f 77 65 62  70 2c 69 6d 61 67 65 2f   mage/web p,image/
0210  61 70 6e 67 2c 2a 2f 2a  3b 71 3d 30 2e 38 2c 61   apng,*/* ;q=0.8,a
0220  70 70 6c 69 63 61 74 69  6f 6e 2f 73 69 67 6e 65   pplicati on/signe
0230  64 2d 65 78 63 68 61 6e  67 65 3b 76 3d 62 33 3b   d-exchan ge;v=b3;
0240  71 3d 30 2e 37 0d 0a 52  65 66 65 72 65 72 3a 20   q=0.7··R eferer: 
0250  68 74 74 70 3a 2f 2f 62  72 65 62 68 72 2e 74 65   http://b rebhr.te
0260  6c 65 74 61 6c 6b 2e 63  6f 6d 2e 62 64 2f 61 64   letalk.c om.bd/ad
0270  6d 69 74 63 61 72 64 2f  0d 0a 41 63 63 65 70 74   mitcard/ ··Accept
0280  2d 45 6e 63 6f 64 69 6e  67 3a 20 67 7a 69 70 2c   -Encodin g: gzip,
0290  20 64 65 66 6c 61 74 65  0d 0a 41 63 63 65 70 74    deflate ··Accept
02a0  2d 4c 61 6e 67 75 61 67  65 3a 20 65 6e 2d 55 53   -Languag e: en-US
02b0  2c 65 6e 3b 71 3d 30 2e  39 0d 0a 43 6f 6f 6b 69   ,en;q=0. 9··Cooki
02c0  65 3a 20 5f 67 61 3d 47  41 31 2e 31 2e 31 30 35   e: _ga=G A1.1.105
02d0  32 36 36 39 36 35 36 2e  31 36 38 34 33 34 33 34   2669656. 16843434
02e0  38 33 3b 20 5f 67 61 5f  39 57 4e 51 32 52 30 54   83; _ga_ 9WNQ2R0T
02f0  4d 4d 3d 47 53 31 2e 31  2e 31 36 38 34 33 34 33   MM=GS1.1 .1684343
0300  34 38 32 2e 31 2e 30 2e  31 36 38 34 33 34 33 34   482.1.0. 16843434
0310  38 34 2e 30 2e 30 2e 30  3b 20 5f 67 61 5f 4b 4c   84.0.0.0 ; _ga_KL
0320  38 36 32 53 44 53 33 54  3d 47 53 31 2e 31 2e 31   862SDS3T =GS1.1.1
0330  37 30 30 33 32 31 35 36  38 2e 31 2e 31 2e 31 37   70032156 8.1.1.17
0340  30 30 33 32 31 36 36 36  2e 30 2e 30 2e 30 3b 20   00321666 .0.0.0; 
0350  50 48 50 53 45 53 53 49  44 3d 72 30 66 30 76 72   PHPSESSI D=r0f0vr
0360  6d 39 67 71 67 38 6b 72  39 6f 33 6f 70 68 63 34   m9gqg8kr 9o3ophc4
0370  65 35 30 31 0d 0a 0d 0a  75 73 65 72 5f 69 64 3d   e501···· user_id=
0380  59 75 62 72 61 6a 2b 44  61 73 26 70 61 73 73 77   Yubraj+D as&passw
0390  6f 72 64 3d 31 32 33 34  35 36 37 38 39 26 73 75   ord=1234 56789&su
03a0  62 6d 69 74 3d                                     bmit=
```

```
HTML Form URL Encoded (urlencoded-form), 45 bytes          Packets: 413 · Displayed: 5 (1.2%)          Profile: Default
```

4. Findings:

The packet sniffing activity revealed the following findings:

Network Traffic Analysis: Wireshark captured various types of network traffic, including HTTP, HTTPS, DNS, FTP, and SMTP, among others.

Plaintext Data Transmission: Some network protocols, such as HTTP, transmitted data in plaintext, making sensitive information vulnerable to interception. For example, login credentials, session tokens, and website content were observed in plaintext within HTTP traffic.

Encrypted Data Transmission: Encrypted protocols like HTTPS and SSH appeared as encrypted data streams within Wireshark, indicating secure communication channels that protect data confidentiality.

5. Recommendations:

Based on the findings, the following recommendations are proposed to mitigate the risks associated with packet sniffing:

Encryption Implementation: Employ strong encryption protocols (e.g., TLS/SSL) for securing sensitive data transmission over the network to prevent interception of plaintext data.

Network Segmentation: Implement network segmentation to isolate sensitive data traffic from non-sensitive traffic, limiting the exposure of sensitive information to potential packet sniffing attacks.

Traffic Monitoring: Continuously monitor network traffic using intrusion detection systems (IDS) and intrusion prevention systems (IPS) to detect and mitigate unauthorized packet sniffing activities in real-time.

6. Conclusion:

In conclusion, the packet sniffing activity using Wireshark provided valuable insights into network traffic patterns and vulnerabilities associated with plaintext data transmission. By understanding the risks and implementing appropriate security measures, organizations can enhance the confidentiality and integrity of their network communications.