CCSI460 Final Forensic Lab Report

Investigator’s Name: Matt Ferry

Date of Investigation: 9/23/13

Lab Number and Title: Homework Week 4: FTP Pcap

Summary of Findings:

The site that was visited was ftp.microsoft.com at IP address 10.11.177.42 from IP address 64.4.30.34 with the username: anonymous and password secret@devryu.net on Jun 14, 2012 15:16:48.

Details of Investigation:

Examine the FTP.pcap file to locate the requested information.

* Date and time of transactions
* Protocol used to communicate with server
* All IPs utilized
* Username of connection
* Password of connection
* Site visited

9/23/13

 12:15 PM – Launched wireshark

 12:18 PM – Updated wireshark

 12:23 PM – Begin packet analyzing, pulling all Source and Destination IPs as requested.

1:00 PM – Finished pulling information out of the pcap file.

1:15 PM – Importing excel spreadsheet.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Packet No** | **Source:** | **Destination:** | **Protocol:** | **Time** |
| 1 | 64.4.30.34 | 10.11.177.42 | FTP |  Jun 14, 2012 15:16:48.280468000 |
| 2 | 64.4.30.34 | 10.11.177.42 | FTP |  Jun 14, 2012 15:16:48.850482000 |
| 3 | 64.4.30.34 | 10.11.177.42 | FTP |  Jun 14, 2012 15:16:49.645524000 |
| 4 | 10.11.177.42 | 64.4.30.34 | FTP |  Jun 14, 2012 15:16:50.942813000  |
| 5 | 64.4.30.34 | 10.11.177.42 | FTP |  Jun 14, 2012 15:16:51.125442000  |
| 6 | 64.4.30.34 | 10.11.177.42 | FTP |  Jun 14, 2012 15:16:54.336623000 |
| 7 | 10.11.177.42 | 64.4.30.34 | FTP |  Jun 14, 2012 15:16:57.474372000  |
| 8 | 64.4.30.34 | 10.11.177.42 | FTP |  Jun 14, 2012 15:16:57.603812000  |
| 9 | 64.4.30.34 | 10.11.177.42 | FTP |  Jun 14, 2012 15:16:57.605813000  |
| 10 | 10.11.177.42 | 64.4.30.34 | FTP |  Jun 14, 2012 15:16:59.855000000  |
| 11 | 10.11.177.42 | 64.4.30.34 | FTP |  Jun 14, 2012 15:17:00.191051000  |
| 12 | 64.4.30.34 | 10.11.177.42 | FTP |  Jun 14, 2012 15:17:00.427972000  |
| 13 | 10.11.177.42 | 64.4.30.34 | FTP |  Jun 14, 2012 15:17:00.430525000  |
| 14 | 10.11.177.42 | 64.4.30.34 | FTP |  Jun 14, 2012 15:17:01.441257000  |
| 15 | 64.4.30.34 | 10.11.177.42 | FTP |  Jun 14, 2012 15:17:01.441459000 |
| 16 | 64.4.30.34 | 10.11.177.42 | FTP |  Jun 14, 2012 15:17:01.743048000 |
| 17 | 64.4.30.34 | 10.11.177.42 | FTP |  Jun 14, 2012 15:17:04.635385000  |
| 18 | 10.11.177.42 | 64.4.30.34 | FTP |  Jun 14, 2012 15:17:10.435088000  |
| 19 | 64.4.30.34 | 10.11.177.42 | FTP |  Jun 14, 2012 15:17:10.795567000  |
| 20 | 10.11.177.42 | 64.4.30.34 | FTP |  Jun 14, 2012 15:17:13.493989000  |

|  |  |
| --- | --- |
| User:  | anonymous |
| Password | secret@devryu.net |
| Site:  | ftp.microsoft.com |