|  |
| --- |
| **Sofia Sackett 05/02/2020** |
| **Analysis of *Project 4 Unknown.pcap*** |
| **File Name**:  Project 4 Unknown.pcap  **File Date and Time Stamp:**  Created:2013-02-03 22:20:07 UTC  Accessed: 2020-20-04 17:39:04 UTC  **File Hash:**  MD5: 8e644a148e2e4ebc7cc2b0b6bab1abe2  SHA-256: 999950A4EF145B2D820F45479326246D68A05DC8D54183C1E5C3629CAC7A805B  **Number of Frames:**  21,757  **Source of the File:**  File retrieved from BlackBoard via Professor Robert Osgood |
| **Time Zone or Time Adjustment Factors**  All date and time stamps given in this report have been converted from their original form to a 24-hour UTC format. |
| **Statistics and Conversations**  Project 4 Unknown.pcap included four DNS requests that resolved to www.google.com (74.125.131.147), smtp.mail.yahoo.com (63.250.193.228), ssl.gstatic.com (74.125.228.79), and google.com (74.125.228.9). In total, three servers were contacted: 4.2.2.2 (DNS), 8.8.8.8 (DNS), and 172.16.253.254 (DHCP).  A screenshot of a computer  Description automatically generatedWireshark provided statistics for conversations held over UDP, TCP, and IPv4. As illustrated below, the majority of the IPv4 packets in this capture were sent between 172.16.253.129, 63.250.193.228, and 74.125.193.228.  A picture containing different, table, group, display  Description automatically generatedNext, UDP traffic occurred for the most part between 172.16.253.1 and 172.16.253.255 in terms of total bytes transmitted. In terms of packets sent, the largest amount of UDP traffic occurred between 4.2.2.2 and 172.16.253.129.  A screenshot of a social media post  Description automatically generatedWireshark also shows that the vast majority of TCP traffic in this capture occurred between 172.16.253.129 and 63.250.193.228.  Finally, the diagrams below were created in PowerPoint to represent each conversation between nodes in this capture file. Most of the traffic was centered around 172.16.253.129; however, there were also three completely isolated conversation between separate six nodes.  A screenshot of a cell phone  Description automatically generatedA close up of a map  Description automatically generated |
| **Potential Victim Details**  74.125.131.147 (www.google.com)  63.250.193.228 (smtp.mail.us.am0.yahoodns.net) |
| **Subject Details**  IP: 172.16.253.129 (Windows Dell XT)  MAC: 00:0C:29:7B:A8:DA (VMWare, Inc.) |
| **Evidence to include Frame # and Frame Date/Time Stamp**  The following evidence items are grouped by indicator. All packets were sent on 2013-02-03 and each evidence item contains the UTC timestamp and frame number.  Artifacts of Interest  Frames 57-20271 (22:21:38-22:21:51) include an email with a timestamp of June 6, 2013 9:46:41 -0400 from linux06400@yahoo.com to linux6400@yahoo.com with the subject line <Logs from “Laura”> (password: azerty/06). The email was sent with the message “You will find log file attached to this letter.” However, the actual attachments included 27 .jpg files of a Windows home screen such as the one seen below as well as 4 .png and 2 .gif files. Although none of the photos were overtly suspicious, it is worth noting that the Windows .jpg images show that the user has a folder titled “Crashplan001”.  A screenshot of a computer  Description automatically generated  Possible ARP Spoofing  There is also evidence of possible ARP spoofing. In frame number 5, the source IP of the packet is 172.16.253.254 and the source MAC address is 00:50:E7:50:95 (timestamp 22:20:28). However, in frame number 13 (timestamp 22:20:48), the source IP address is the same, but the source MAC address is listed as 00:50:56:EA:5C:28.  TCP Reset Flag Set [RST, ACK]   |  |  |  |  | | --- | --- | --- | --- | | Frame Number | Source IP | Destination IP | Timestamp | | 19 | 23.59.240.60 | 172.16.253.129 | 22:20:49 | | 20 | 23.59.240.60 | 172.16.253.129 | 22:20:49 | | 21742 | 172.16.253.129 | 74.125.131.147 | 22:22:40 | | 21743 | 172.16.253.129 | 74.125.131.147 | 22:22:40 | | 21744 | 172.16.253.129 | 74.125.131.147 | 22:22:40 | | 21745 | 172.16.253.129 | 74.125.131.147 | 22:22:40 | | 21746 | 172.16.253.129 | 74.125.131.147 | 22:22:40 | | 21747 | 172.16.253.129 | 74.125.131.147 | 22:22:40 | | 21748 | 172.16.253.129 | 74.125.131.147 | 22:22:40 |   TCP Retransmission   |  |  |  |  | | --- | --- | --- | --- | | Frame Number | Source IP | Destination IP | Timestamp | | 55 | 63.250.193.228 | 172.16.253.129 | 22:21:35 | | 13174 | 172.16.253.129 | 63.250.193.228 | 22:21:45 | | 14481 | 172.16.253.129 | 63.250.193.228 | 22:21:48 | | 20305 | 74.125.131.147 | 172.16.253.129 | 22:22:01 | | 20393 | 74.125.131.147 | 172.16.253.129 | 22:22:01 | | 20693 | 74.125.131.147 | 172.16.253.129 | 22:22:02 | | 20711 | 74.125.131.147 | 172.16.253.129 | 22:22:08 | | 20713 | 74.125.131.147 | 172.16.253.129 | 22:22:08 | | 20723 | 74.125.131.147 | 172.16.253.129 | 22:22:10 | | 20750 | 74.125.131.147 | 172.16.253.129 | 22:22:10 | | 20760 | 74.125.131.147 | 172.16.253.129 | 22:22:10 | | 20768 | 74.125.131.147 | 172.16.253.129 | 22:22:11 | | 20770 | 74.125.131.147 | 172.16.253.129 | 22:22:11 | | 20781 | 74.125.131.147 | 172.16.253.129 | 22:22:11 | | 20784 | 74.125.131.147 | 172.16.253.129 | 22:22:11 | | 20786 | 74.125.131.147 | 172.16.253.129 | 22:22:11 | | 20789 | 74.125.131.147 | 172.16.253.129 | 22:22:11 | | 20797 | 74.125.131.147 | 172.16.253.129 | 22:22:11 | | 20799 | 74.125.131.147 | 172.16.253.129 | 22:22:11 | | 20807 | 74.125.131.147 | 172.16.253.129 | 22:22:12 | | 20809 | 74.125.131.147 | 172.16.253.129 | 22:22:12 | | 20812 | 74.125.131.147 | 172.16.253.129 | 22:22:12 | | 20848 | 74.125.131.147 | 172.16.253.129 | 22:22:12 | | 20854 | 74.125.131.147 | 172.16.253.129 | 22:22:12 | | 20867 | 74.125.131.147 | 172.16.253.129 | 22:22:12 | | 20872 | 74.125.131.147 | 172.16.253.129 | 22:22:12 | | 20878 | 74.125.131.147 | 172.16.253.129 | 22:22:12 | | 20886 | 74.125.131.147 | 172.16.253.129 | 22:22:12 | | 20902 | 74.125.131.147 | 172.16.253.129 | 22:22:13 | | 20985 | 74.125.131.147 | 172.16.253.129 | 22:22:13 | | 21055 | 74.125.131.147 | 172.16.253.129 | 22:22:14 | | 21057 | 74.125.131.147 | 172.16.253.129 | 22:22:14 | | 21059 | 74.125.131.147 | 172.16.253.129 | 22:22:14 | | 21069 | 74.125.131.147 | 172.16.253.129 | 22:22:17 | | 21081 | 74.125.131.147 | 172.16.253.129 | 22:22:17 | | 21088 | 74.125.131.147 | 172.16.253.129 | 22:22:17 | | 21102 | 74.125.131.147 | 172.16.253.129 | 22:22:18 | | 21112 | 74.125.131.147 | 172.16.253.129 | 22:22:18 | | 21120 | 74.125.131.147 | 172.16.253.129 | 22:22:18 | | 21122 | 74.125.131.147 | 172.16.253.129 | 22:22:18 | | 21142 | 74.125.131.147 | 172.16.253.129 | 22:22:19 | | 21152 | 74.125.131.147 | 172.16.253.129 | 22:22:20 | | 21166 | 74.125.131.147 | 172.16.253.129 | 22:22:20 | | 21182 | 74.125.131.147 | 172.16.253.129 | 22:22:20 | | 21192 | 74.125.131.147 | 172.16.253.129 | 22:22:20 | | 21202 | 74.125.131.147 | 172.16.253.129 | 22:22:20 | | 21228 | 74.125.131.147 | 172.16.253.129 | 22:22:21 | | 21236 | 74.125.131.147 | 172.16.253.129 | 22:22:21 | | 21238 | 74.125.131.147 | 172.16.253.129 | 22:22:21 | | 21249 | 74.125.131.147 | 172.16.253.129 | 22:22:22 | | 21305 | 74.125.131.147 | 172.16.253.129 | 22:22:23 | | 21307 | 74.125.131.147 | 172.16.253.129 | 22:22:23 | | 21317 | 74.125.131.147 | 172.16.253.129 | 22:22:29 | | 21325 | 74.125.131.147 | 172.16.253.129 | 22:22:29 | | 21327 | 74.125.131.147 | 172.16.253.129 | 22:22:29 | | 21340 | 74.125.131.147 | 172.16.253.129 | 22:22:30 | | 21344 | 74.125.131.147 | 172.16.253.129 | 22:22:30 | | 21352 | 74.125.131.147 | 172.16.253.129 | 22:22:30 | | 21366 | 74.125.131.147 | 172.16.253.129 | 22:22:30 | | 21372 | 74.125.131.147 | 172.16.253.129 | 22:22:30 | | 21380 | 74.125.131.147 | 172.16.253.129 | 22:22:30 | | 21382 | 74.125.131.147 | 172.16.253.129 | 22:22:30 | | 21392 | 74.125.131.147 | 172.16.253.129 | 22:22:31 | | 21404 | 74.125.131.147 | 172.16.253.129 | 22:22:31 | | 21410 | 74.125.131.147 | 172.16.253.129 | 22:22:31 | | 21498 | 74.125.131.147 | 172.16.253.129 | 22:22:31 | | 21521 | 74.125.131.147 | 172.16.253.129 | 22:22:31 | | 21523 | 74.125.131.147 | 172.16.253.129 | 22:22:31 | | 21531 | 74.125.131.147 | 172.16.253.129 | 22:22:32 | | 21533 | 74.125.131.147 | 172.16.253.129 | 22:22:32 | | 21577 | 74.125.131.147 | 172.16.253.129 | 22:22:32 | | 21583 | 74.125.131.147 | 172.16.253.129 | 22:22:32 | | 21591 | 74.125.131.147 | 172.16.253.129 | 22:22:32 | | 21593 | 74.125.131.147 | 172.16.253.129 | 22:22:32 | | 21607 | 74.125.131.147 | 172.16.253.129 | 22:22:34 | | 21617 | 74.125.131.147 | 172.16.253.129 | 22:22:34 | | 21623 | 74.125.131.147 | 172.16.253.129 | 22:22:34 | | 21636 | 74.125.131.147 | 172.16.253.129 | 22:22:34 | | 21642 | 74.125.131.147 | 172.16.253.129 | 22:22:34 | | 21648 | 74.125.131.147 | 172.16.253.129 | 22:22:35 | | 21662 | 74.125.131.147 | 172.16.253.129 | 22:22:35 | | 21672 | 74.125.131.147 | 172.16.253.129 | 22:22:35 | | 21676 | 74.125.131.147 | 172.16.253.129 | 22:22:35 | | 21678 | 74.125.131.147 | 172.16.253.129 | 22:22:35 | | 21688 | 74.125.131.147 | 172.16.253.129 | 22:22:35 | | 21738 | 74.125.131.147 | 172.16.253.129 | 22:22:36 | | 21740 | 74.125.131.147 | 172.16.253.129 | 22:22:36 |   TCP Window Update   |  |  |  |  | | --- | --- | --- | --- | | Frame Number | Source IP | Destination IP | Timestamp | | 20392 | 172.16.253.129 | 74.125.131.147 | 22:22:01 | | 20395 | 172.16.253.129 | 74.125.131.147 | 22:22:01 | | 20454 | 172.16.253.129 | 74.125.131.147 | 22:22:01 | | 20462 | 172.16.253.129 | 74.125.131.147 | 22:22:01 | | 20595 | 172.16.253.129 | 74.125.131.147 | 22:22:02 | | 20596 | 172.16.253.129 | 74.125.131.147 | 22:22:02 | | 20604 | 172.16.253.129 | 74.125.131.147 | 22:22:02 | | 20616 | 172.16.253.129 | 74.125.131.147 | 22:22:02 | | 20617 | 172.16.253.129 | 74.125.131.147 | 22:22:02 | | 20835 | 172.16.253.129 | 74.125.131.147 | 22:22:12 | | 20836 | 172.16.253.129 | 74.125.131.147 | 22:22:12 | | 20922 | 172.16.253.129 | 74.125.131.147 | 22:22:13 | | 20927 | 172.16.253.129 | 74.125.131.147 | 22:22:13 | | 20983 | 172.16.253.129 | 74.125.131.147 | 22:22:13 | | 20984 | 172.16.253.129 | 74.125.131.147 | 22:22:13 | | 21041 | 172.16.253.129 | 74.125.131.147 | 22:22:14 | | 21042 | 172.16.253.129 | 74.125.131.147 | 22:22:14 | | 21303 | 172.16.253.129 | 74.125.131.147 | 22:22:23 | | 21455 | 172.16.253.129 | 74.125.131.147 | 22:22:31 | | 21483 | 172.16.253.129 | 74.125.131.147 | 22:22:31 | | 21500 | 172.16.253.129 | 74.125.131.147 | 22:22:31 | | 21501 | 172.16.253.129 | 74.125.131.147 | 22:22:31 | | 21576 | 172.16.253.129 | 74.125.131.147 | 22:22:32 | | 21579 | 172.16.253.129 | 74.125.131.147 | 22:22:32 |   Wireshark’s TCP Window Full Notifications   |  |  |  |  | | --- | --- | --- | --- | | Frame Number | Source IP | Destination IP | Timestamp | | 555 | 172.16.253.129 | 63.250.193.228 | 22:21:39 | | 561 | 172.16.253.129 | 63.250.193.228 | 22:21:39 | | 568 | 172.16.253.129 | 63.250.193.228 | 22:21:39 | | 20450 | 74.125.131.147 | 172.16.253.129 | 22:22:01 | | 20458 | 74.125.131.147 | 172.16.253.129 | 22:22:01 | | 20506 | 74.125.131.147 | 172.16.253.129 | 22:22:01 | | 20600 | 74.125.131.147 | 172.16.253.129 | 22:22:02 | | 21479 | 74.125.131.147 | 172.16.253.129 | 22:22:31 |   TCP ZeroWindow   |  |  |  |  | | --- | --- | --- | --- | | Frame Number | Source IP | Destination IP | Timestamp | | 558 | 63.250.193.228 | 172.16.253.129 | 22:21:39 | | 563 | 63.250.193.228 | 172.16.253.129 | 22:21:39 | | 572 | 63.250.193.228 | 172.16.253.129 | 22:21:39 | | 20451 | 172.16.253.129 | 74.125.131.147 | 22:22:01 | | 20459 | 172.16.253.129 | 74.125.131.147 | 22:22:01 | | 20507 | 172.16.253.129 | 74.125.131.147 | 22:22:01 | | 20601 | 172.16.253.129 | 74.125.131.147 | 22:22:02 | | 21480 | 172.16.253.129 | 74.125.131.147 | 22:22:31 |   TCP ZeroWindowProbe   |  |  |  |  | | --- | --- | --- | --- | | Frame Number | Source IP | Destination IP | Timestamp | | 20452 | 74.125.131.147 | 172.16.253.129 | 22:22:01 | | 20460 | 74.125.131.147 | 172.16.253.129 | 22:22:01 | | 20508 | 74.125.131.147 | 172.16.253.129 | 22:22:01 | | 20519 | 74.125.131.147 | 172.16.253.129 | 22:22:01 | | 20592 | 74.125.131.147 | 172.16.253.129 | 22:22:01 | | 20602 | 74.125.131.147 | 172.16.253.129 | 22:22:02 | | 21481 | 74.125.131.147 | 172.16.253.129 | 22:22:31 |   TCP Duplicate ACK   |  |  |  |  | | --- | --- | --- | --- | | Frame Number | Source IP | Destination IP | Timestamp | | 740 | 63.250.193.228 | 172.16.253.129 | 22:21:39 | | 13177 | 63.250.193.228 | 172.16.253.129 | 22:21:45 | | 14485 | 63.250.193.228 | 172.16.253.129 | 22:21:48 |   TCP ZeroWindowProbeAck and TCP ZeroWindow   |  |  |  |  | | --- | --- | --- | --- | | Frame Number | Source IP | Destination IP | Timestamp | | 20453 | 172.16.253.129 | 74.125.131.147 | 22:22:01 | | 20461 | 172.16.253.129 | 74.125.131.147 | 22:22:01 | | 20509 | 172.16.253.129 | 74.125.131.147 | 22:22:01 | | 20520 | 172.16.253.129 | 74.125.131.147 | 22:22:01 | | 20593 | 172.16.253.129 | 74.125.131.147 | 22:22:01 | | 20603 | 172.16.253.129 | 74.125.131.147 | 22:22:02 | | 21482 | 172.16.253.129 | 74.125.131.147 | 22:22:31 | |
| **Conclusion**  For the most part, this capture file can be described with two main conversations. The first is a TCP and HTTP conversation between the 172.16.253.129 and 74.125.131.147 (www.google.com). Within this traffic, 74.125.131.147 sent many TCP zero window probes to 172.16.253.129, which means that 172.16.253.129 had reduced its window size to zero, effectively telling 74.125.131.147 that the receive buffer was full and to stop sending data. In return, 172.16.253.129 acknowledged the zero window probes from 74.125.131.147, sent even more zero window packets, and had to eventually update its window size in order to receive more data from 74.125.131.147. As a result of this data backup, 74.125.131.147 sent 172.16.253.129 a massive number of TCP retransmissions. Finally, 172.16.253.129 sent 74.125.131.147 a fair number of packets with the TCP flag RST, meaning that it wanted to abruptly end the connection and no longer receive data from 74.125.131.147.  Next, the TCP and SMTP conversation between 63.250.193.228 (yahoodns.net) and 172.16.253.129 also involved window full messages, zero window warnings, and retransmissions. However, in this case 172.16.253.147 was on the receiving end. 63.250.193.228 also sent a few TCP packets with duplicate ACKs to 172.16.253.129, possibly meaning that 172.16.253.129 was using them for fast retransmissions of out-of-order packets. It is also worth noting the one-sidedness of this conversation; while both sent approximately 10,000 packets, 63.250.193.228 sent only 611 KB, but it received over 10 MB from 172.16.253.129.  One unexplained connection is that between 172.16.253.129 and 23.59.240.60, which belongs to Akamai Technologies in Cambridge, MA. The only record of the traffic between these two IPs is 23.59.240.60’s abrupt ending of the TCP session with two consecutive TCP RST packets.  Finally, there also exists the potential that 172.16.253.129 is using ARP spoofing to hide or alter the MAC address. From frame number 5 to frame 13, the MAC address of 172.16.253.129 changed from 00:50:E7:50:95 to 00:50:56:EA:5C:28.  While this network capture did not yield an obvious attack between any nodes on the network, there is potential that 172.16.253.129 is performing reconnaissance for an attack solely based on the slightly antagonistic nature of its network connections with www.google.com and yahoodns.net as well as the potential that 172.16.253.129 is hiding its true MAC address. |