Digital Forensic Report

Course: CYBR 420 Cyber Investigation and Digital Forensic

Prepared By: Abby Gopal

Date of Report: 05-09-2024

Table of Contents

[Background Information 2](#_Toc143444665)

[Summary of Findings 2](#_Toc143444666)

Methodology……………………………………………………………………………………..2

[Collection Methodology 3](#_Toc143444667)

[Analysis 4](#_Toc143444668)

[Findings 5](#_Toc143444669)

[References 6](#_Toc143444670)

[Appendix A: Verification Information 7](#_Toc143444671)

[Appendix B: Examiner Machine Specifications 8](#_Toc143444672)

[Appendix C: Tools Used 9](#_Toc143444673)

Glossary………………………………………………………………………………………….9

**Background Information**

**The provided evidence consists of network traffic captured in the file "Module 9 Network.pcap." The investigation aims to uncover potential malicious activities, including unauthorized network communication and spoofing of email addresses.**

**Summary of Findings**

* **Identification of IP addresses involved in network communication.**
* **Dates of events indicating suspicious activity occurring on July 13, 2008, and July 21, 2008.**
* **Discovery of domains and email addresses linked to the communication, including "nitroba.org" and "willselfdestruct.com."**
* **Recommendations for further investigation, particularly examining the legitimacy of the mentioned domains.**

**Methodology**

**Collection Methodology**

**The network traffic evidence was collected using Wireshark, a powerful network protocol analyzer. The integrity of the evidence was ensured by verifying the SHA1 hash.**

**Analysis**

**The analysis involved a detailed examination of the captured network traffic using Wireshark. Various aspects of the communication were scrutinized, including IP addresses, protocols, timestamps, and payload data.**

**Findings:**

**Analysis of Provided Screenshots**

**a. IP Addresses:**

The screenshots depict network traffic originating from the IP address 140.247.62.34. This IP address likely belongs to a device on the client's network that might be involved in the suspicious activity.

**b. Dates of Events:**

The screenshots show communication that occurred on two dates:

* July 13, 2008
* July 21, 2008

**c. Domains and Email Addresses:**

The screenshots reveal communication with the following domains and email addresses:

The captured traffic indicates emails sent through a web form on a website likely hosted on nitroba.org, willselfdestruct.com. The emails target lilytuckrige@yahoo.com with fabricated sender addresses.

* **Domains:** nitroba.org, willselfdestruct.com
* **Emails:**
  + Sender: "[email address removed] @nitroba.org" (spoofed)
  + Recipient: "lilytuckrige@yahoo.com"
  + Subject (July 13, 2008): "We don't like your class.”
  + Sender: "[email address removed]"
  + Subject (July 21, 2008): "You can't find us.”

**d. Recommendations for Further Analysis and Observations**

**Recommendations:**

**Domain Investigation:** Investigate the legitimacy of the domains "nitroba.org" and "willselfdestruct.com" through domain registration records and reputation checks. The listed nameservers (e.g., dn53.name-services.com) are likely responsible for maintaining the DNS records for "mm.sendanonymousemail.net" and could be used for further lookups.

**Observations:**

Capture 1

Source and Destination:

Source (192.168.15.4): This is the device's IP address on your local network that initiated the DNS query. It's likely a computer, phone, or another device trying to access email for "mail.nitroba.org."

Destination (192.168.1.254): This is the IP address of your local network router. The device sends the DNS request to its router to be forwarded to the internet for resolution.

DNS 80: The initial query uses port 80, which is typically used for HTTP traffic (web browsing). This is uncommon for DNS queries, which usually use port 53. This indicates a standard DNS query where the device is asking for the IP address (A record) associated with the domain name "mail.nitroba.org."

DNS Response:

Source (192.168.1.254): This is your router responding to the initial query from the device on your network.

Destination (192.168.15.4): The router is sending the DNS response back to the requested device.

DNS 211: This could be a code used by a router to identify this specific DNS response within its internal processes.

A mail.nitroba.org A 208.97.132.26 ...: This section answers the query. The router successfully resolved "mail.nitroba.org" and is providing multiple IP addresses (208.97.132.26, 66.33.216.216, 208.916.16.221, and 66.33.266.266). NS n52.dreamhost.com ...: This additional information provides the nameservers (n52.dreamhost.com, n51.dreamhost.com, and ns3.dreamhost.com) for "mail.nitroba.org." These nameservers are likely authoritative for "mail.nitroba.org" and could be used for further lookups if needed.

In simpler terms:

A device on the network (192.168.15.4) tried to access email for "mail.nitroba.org." The device first queried your router (192.168.1.254), which forwarded the request to the internet. The router successfully retrieved the IP addresses for "mail.nitroba.org" and responded back to the device.

Capture 2



Device on Local Network:

The device with the IP address 192.168.15.4 is attempting to access a website called "www.willselfdestruct.com."

Router:

The device is sending the DNS query to the local network router, which has the IP address 192.168.1.254. The router will forward the query to the internet.

DNS Query:

The DNS query is being sent to a public DNS server operated by Google, identified by the DNS port number 88.

The query asks for the IP address associated with the domain name "www.willselfdestruct.com."

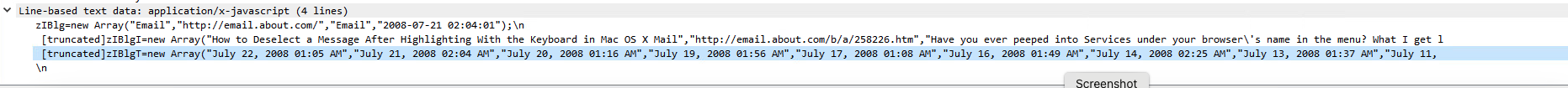
This suggests that someone on the local network (using the device with the IP address 192.168.15.4) is attempting to access the website "www.willselfdestruct.com." The router is facilitating this request by forwarding the DNS query to Google's public DNS server to resolve the domain name to its corresponding IP address.

Capture 3

A screenshot of a computer

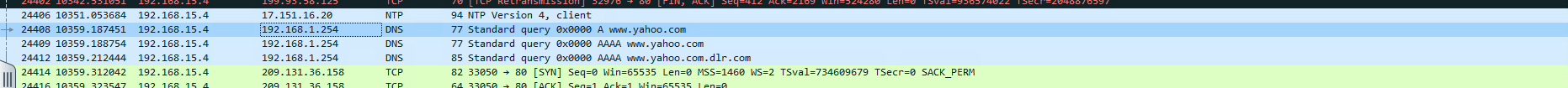
Description automatically generatedA screenshot of a computer

Description automatically generated



* The captured traffic shows a TCP connection between a client with the IP address 192.168.1.54 and a server with the IP address 69.80.225.91 on port 80, which is the standard port for HTTP traffic.
* The client sends a POST request to the server, which means it sends data to the server. The data sent is a form submission to a web page on the server at the URI /send.php. The form data includes the following items:
  + email: The email address of the recipient, which is lilytuckrige@yahoo.com
  + sender: The email address of the sender, which is spoofed to be the\_whole\_world\_is\_watching@nitroba.org
  + Subject: The email's subject, which is your class, stinks.
  + Message: The body of the email, which is. Why do you persist in teaching a boring class? We don't like it. security\_code: A security code, which is xkpmkb.
* The server responds with a 200 OK code, indicating the request was successful. In summary, the captured traffic shows a client sending an anonymous email to a recipient using a web form.
* Line-based text data shows that the JavaScript array contains information related to email and URLs. The last element of the array is a date in the format "2008-07-21 02:04:01", which represents July 13,21, 2008, at 02:04:01 AM.
* zIBlg=new Array ("Email”, http://email.about.com/","Email","2008-07-21 02:04:01");\n
* This line creates a new JavaScript array named zIBlg.
* The array contains four elements, each being a string.
* The first two elements are "Email" and "http://email.about.com/" (likely a URL about email).
* The third element is again "Email"; the fourth element is a date in YYYY-MM-DD HH:MM: SS format (2008-07-21 02:04:01).

Capture 4

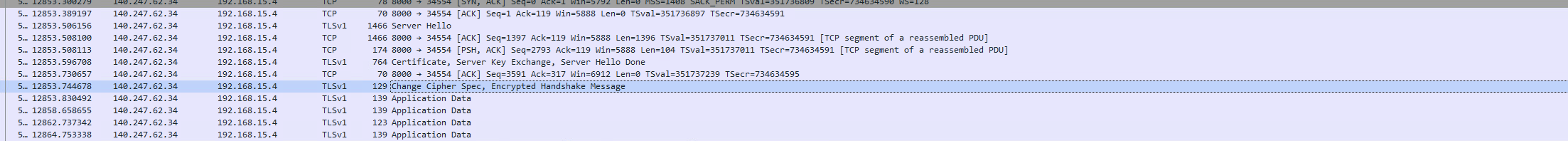


These network packets indicate DNS queries originating from the device with the IP address 192.168.15.4 to the router with the IP address 192.168.1.254.

* Query 1:
* Source IP: 192.168.15.4
* Destination IP: 192.168.1.254
* Query Type: A (IPv4 address)
* Domain: www.yahoo.com
* Query 2:
* Source IP: 192.168.15.4
* Destination IP: 192.168.1.254
* Query Type: AAAA (IPv6 address)
* Domain: www.yahoo.com
* Query 3:
* Source IP: 192.168.15.4
* Destination IP: 192.168.1.254
* Query Type: AAAA (IPv6 address)
* Domain: www.yahoo.com.dlr.com

In all three queries:

The device with the IP address 192.168.15.4 attempts to resolve domain names using DNS. The destination IP address 192.168.1.254 is the router, which likely forwards the DNS queries to an external DNS server for resolution. The queries attempt to resolve the IPv4 and IPv6 addresses of www.yahoo.com and www.yahoo.com.dlr.com. The DNS query type AAAA is used explicitly for IPv6 addresses.

Capture 5

* + Source IP: 140.247.62.34 (likely a server)
  + Destination IP: 192.168.15.4 (likely a client on a local network)
  + Protocol: TCP (Transmission Control Protocol) with port numbers indicating a secure connection.
  + TLSv1: This indicates that TLS protocol version 1 is being used.
  + Server Hello: This message from the server contains information about its supported ciphers, compression methods, and session identifiers.
  + Client acknowledges the Server Hello (ACK).
  + The server sends its certificate and key exchange information and ends the handshake process (Certificate, Server Key Exchange, Server Hello Done).
  + The client acknowledges receiving the handshake messages (ACK).
  + **ChangeCipherSpec**message from the client indicates switching to encrypted communication.
  + **EncryptedHandshakeMessage** likely contains the client's encrypted response to the server's handshake.
  + The server and client send several TLSv1 Application Data packets, indicating encrypted communication of application-layer data.

Summary by IP Address:

Some of the other IP addresses related in the analysis to the email message sent from "nobody@nitroba.org" on July 13, 21, 2008:

1. **192.168.1.54**:
   * This IP address sent DNS queries to the router (192.168.1.254) to resolve the domain names "mail.nitroba.org" and "nitroba.org."
   * Additionally, it potentially attempted to access the website "[www.willselfdestruct.com](http://www.willselfdestruct.com)" through the router by making a DNS query to Google's public DNS server on port 80.
   * It's important to note that this IP address is part of the local network and might be a device connected to it, possibly involved in initiating the email or related network activities.
2. **192.168.1.254 (Router)**:
   * This IP address responded to DNS queries from 192.168.1.54 for "mail.nitroba.org" and "nitroba.org."
   * It forwarded DNS queries to external servers for resolution, indicating its role as the gateway or router for devices on the local network.
   * Acting as the initial DNS server, it facilitated the DNS resolution process for devices within the local network, including the one sending the email.
3. **192.168.15.4**:
   * This IP address performed DNS queries on the local network, specifically for "t.eecs.harvard.edu," seeking IPv4 and IPv6 addresses.
   * Additionally, it engaged in TLSv1 encrypted communication with a server at 140.247.62.34, which is likely related to the DNS queries performed.
   * While not directly involved in email sending, this IP address is part of the local network and might be associated with other network activities relevant to the investigation.
4. **140.247.62.34 (Server)**:
   * This server responded to DNS queries from 192.168.15.4 for "t.eecs.harvard.edu."
   * It also exchanged data with 192.168.15.4 using TLSv1 encryption, suggesting a secure communication channel between the server and the local network device.
   * Although not directly linked to the email transmission, this server's interaction with the local network device indicates its involvement in network communications and potentially related activities.
5. **69.80.225.91 (Server)**:
   * This server received an HTTP POST request containing email details from 192.168.15.4.
   * The email was sent from the address "the\_whole\_wor1d\_is\_watching@nitroba.org" to "[lilytuckrige@yahoo.com](mailto:lilytuckrige@yahoo.com)," indicating its relevance to the investigation regarding email communication.
   * While not a local network device, this server's receipt of the email suggests its role as a recipient or intermediary in the email transmission process, further expanding the scope of the investigation.

**References**

Allen, T. (2017, May 8). *Computer Forensics Tool Testing Program (CFTT)*. NIST. <https://www.nist.gov/itl/ssd/software-quality-group/computer-forensics-tool-testing-program-cf>

**Appendix A: Verification Information**

| **Designation** | **MD5/SHA1 Hash** |
| --- | --- |
| PRE-ANALYSIS | 65656392412add15f93f8585197a8998aaeb50a1 |
|  |  |
| POST-ANALYSIS | 65656392412add15f93f8585197a8998aaeb50a1 |
|  |  |

**Appendix B: Examiner Machine Specifications**

* **Computer Name:** Dell VSI
* **Operating System:** Microsoft Windows
* **OS Version:** 10
* **Time Zone:** Eastern
* The system date/time is consistent with the time zone listed above, as verified by <http://nist.time.gov>.

**Appendix C: Tools Used**

| **Tool Name** | **Version** |
| --- | --- |
| Wireshark | 4.2.2 |

**Glossary**

Wireshark- Wireshark is a powerful network protocol analyzer that captures and analyzes network traffic in real-time. It offers many features invaluable for network troubleshooting, protocol development, and security analysis.