Activity Overview

In this activity, you will analyze DNS and ICMP traffic in transit using data from a network protocol analyzer tool. You will identify which network protocol was utilized in assessment of the cybersecurity incident.

In the internet layer of the TCP/IP model, the IP formats data packets into IP datagrams. The information provided in the datagram of an IP packet can provide security analysts with insight into suspicious data packets in transit.

Knowing how to identify potentially malicious traffic on a network can help cybersecurity analysts assess security risks on a network and reinforce network security.

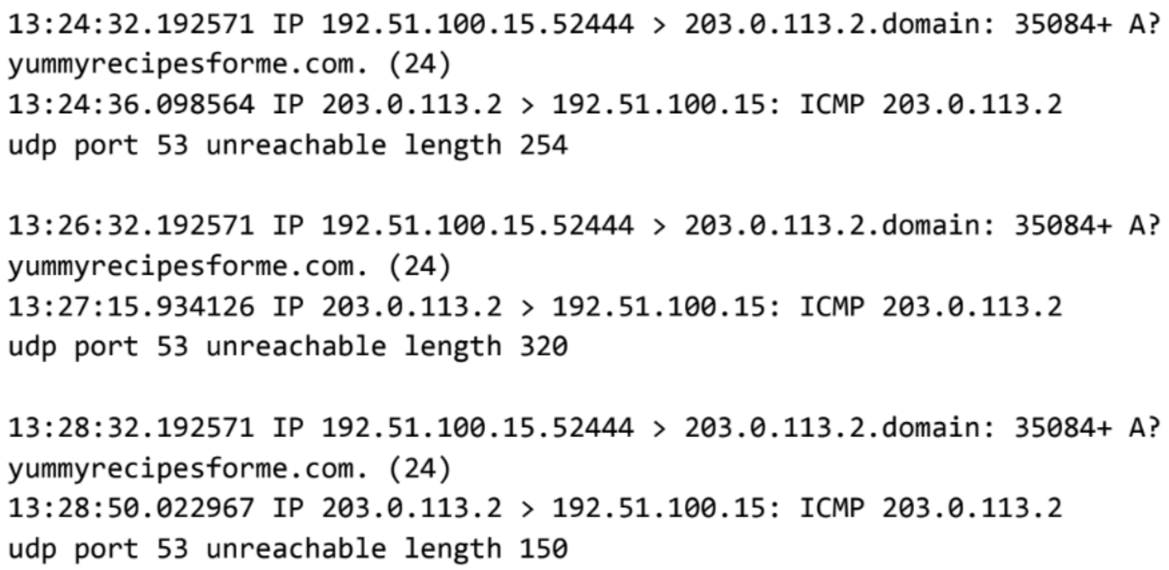
Be sure to complete this activity before moving on. The next course item will provide you with a completed exemplar to compare to your own work.

Scenario

Review the scenario below. Then complete the step-by-step instructions.

You are a cybersecurity analyst working at a company that specializes in providing IT services for clients. Several customers of clients reported that they were not able to access the client company website www.yummyrecipesforme.com, and saw the error “destination port unreachable” after waiting for the page to load.

You are tasked with analyzing the situation and determining which network protocol was affected during this incident. To start, you attempt to visit the website and you also receive the error “destination port unreachable.” To troubleshoot the issue, you load your network analyzer tool, tcpdump, and attempt to load the webpage again. To load the webpage, your browser sends a query to a DNS server via the UDP protocol to retrieve the IP address for the website's domain name; this is part of the DNS protocol. Your browser then uses this IP address as the destination IP for sending an HTTPS request to the web server to display the webpage The analyzer shows that when you send UDP packets to the DNS server, you receive ICMP packets containing the error message: “udp port 53 unreachable.”



```
13:24:32.192571 IP 192.51.100.15.52444 > 203.0.113.2.domain: 35084+ A?
yummyrecipesforme.com. (24)
13:24:36.098564 IP 203.0.113.2 > 192.51.100.15: ICMP 203.0.113.2
udp port 53 unreachable length 254

13:26:32.192571 IP 192.51.100.15.52444 > 203.0.113.2.domain: 35084+ A?
yummyrecipesforme.com. (24)
13:27:15.934126 IP 203.0.113.2 > 192.51.100.15: ICMP 203.0.113.2
udp port 53 unreachable length 320

13:28:32.192571 IP 192.51.100.15.52444 > 203.0.113.2.domain: 35084+ A?
yummyrecipesforme.com. (24)
13:28:50.022967 IP 203.0.113.2 > 192.51.100.15: ICMP 203.0.113.2
udp port 53 unreachable length 150
```

In the tcpdump log, you find the following information:

1. The first two lines of the log file show the initial outgoing request from your computer to the DNS server requesting the IP address of yummyrecipesforme.com. This request is sent in a UDP packet.
2. The third and fourth lines of the log show the response to your UDP packet. In this case, the ICMP 203.0.113.2 line is the start of the error message indicating that the UDP packet was undeliverable to port 53 of the DNS server.
3. In front of each request and response, you find timestamps that indicate when the incident happened. In the log, this is the first sequence of numbers displayed: 13:24:32.192571. This means the time is 1:24 p.m., 32.192571 seconds.
4. After the timestamps, you will find the source and destination IP addresses. In the first line, where the UDP packet travels from your browser to the DNS server, this information is displayed as: 192.51.100.15 > 203.0.113.2.domain. The IP address to the left of the greater than (>) symbol is the source address, which in this example is your computer's IP address. The IP address to the right of the greater than (>) symbol is the destination IP address. In this case, it is the IP address for the DNS server: 203.0.113.2.domain. For the ICMP error response, the source address is 203.0.113.2 and the destination is your computers IP address 192.51.100.15.
5. After the source and destination IP addresses, there can be a number of additional details like the protocol, port number of the source, and flags. In the first line of the error log, the query identification number appears as: 35084. The plus sign after the query identification number indicates there are flags associated with the UDP message. The "A?" indicates a flag associated with the DNS request for an A record, where an A record maps a domain name to an IP address. The third line displays the protocol of the response message to the browser: "ICMP," which is followed by an ICMP error message.
6. The error message, "udp port 53 unreachable" is mentioned in the last line. Port 53 is a port for DNS service. The word "unreachable" in the message indicates the UDP message

requesting an IP address for the domain "www.yummyrecipesforme.com" did not go through to the DNS server because no service was listening on the receiving DNS port.

7. The remaining lines in the log indicate that ICMP packets were sent two more times, but the same delivery error was received both times.

Now that you have captured data packets using a network analyzer tool, it is your job to identify which network protocol and service were impacted by this incident. Then, you will need to write a follow-up report.

As an analyst, you can inspect network traffic and network data to determine what is causing network-related issues during cybersecurity incidents. Later in this course, you will demonstrate how to manage and resolve incidents. For now, you only need to analyze the situation.

This event, in the meantime, is being handled by security engineers after you and other analysts have reported the issue to your direct supervisor.

Step-By-Step Instructions

Follow the instructions and answer the question below to complete the activity. Then, go to the next course item to compare your work to a completed exemplar.

Step 1: Access the template

To use the template for this course item, click the link below and select *Use Template*.

Use the sentence starters and prompts provided in the template to support your thinking and ensure that you include all relevant details about the incident.

Link to template:

- Cybersecurity incident report template

Step 1: Access the template

To use the template for this course item, click the link below and select *Use Template*.

Use the sentence starters and prompts provided in the template to support your thinking and ensure that you include all relevant details about the incident.

Link to template:

- Cybersecurity incident report template

Step 2: Access supporting materials

The following supporting materials will help you complete this activity. Keep them open as you proceed to the next steps.

To use the supporting materials for this course item, click the following links and select *Use Template*.

Link to supporting materials:

- Example of a Cybersecurity Incident Report

Step 3: Provide a summary of the problem found in the tcpdump log

After analyzing the data presented to you from the tcpdump log, identify trends in the data. Assess which protocol is producing the error message from the DNS server for the yummyrecipesforme.com website. Recall that one of the ports that is displayed repeatedly is port 53, commonly used for DNS. In your analysis:

- Include a brief summary of the tcpdump log analysis and identify which protocols were used for the network traffic.
- Provide a few details about what was indicated in the log.
- Interpret the issues found in the log.

Record your responses in part one of the cybersecurity incident report.

Step 4: Explain your analysis of the data and provide one solution to implement

Now that you've inspected the traffic log and identified trends in the traffic, describe why the error messages appeared on the log. Use your answer in the previous step and the scenario to identify the reason behind the ICMP error messages. The error messages indicate that there is an issue with a specific port. What do the different protocols involved in the log reveal about the incident? In your response:

- State when the problem was first reported.
- Provide the scenario, events, and symptoms identified when the event was first reported.
- Explain the current status of the issue.
- Describe the information discovered while investigating the issue up to this point.
- List the next steps in troubleshooting and resolving the issue.
- Provide the suspected root cause of the problem.

Record your responses in part two of the cybersecurity incident report.

Pro tip: Save the template

Finally, be sure to save a blank copy of the template you used to complete this activity. You can use it for further practice or in your professional projects. These templates will help you work through your thought processes and demonstrate your experience to potential employers.

What to Include in Your Response

Be sure to address the following items in your completed activity:

- Provide a summary of the problem found in the tcpdump log
- Explain your analysis of the data and provide one possible cause of the incident

Activity Overview

In this activity, you will consider a scenario involving a customer of the company that you work for who experiences a security issue when accessing the company's website. You will identify the likely cause of the service interruption. Then, you will explain how the attack occurred and the negative impact it had on the website.

In this course, you have learned about several common network attacks. You have learned their names, how they are carried out, and the characteristics of each attack from the perspective of the target. Understanding how attacks impact a network will help you troubleshoot issues on your organization's network. It will also help you take steps to mitigate damage and protect a network from future attacks. To review attacks, visit Identify: Network Attacks

Be sure to complete this activity before moving on. The next course item will provide you with a completed exemplar to compare to your own work.

Scenario

Review the following scenario. Then complete the step-by-step instructions.

You work as a security analyst for a travel agency that advertises sales and promotions on the company's website. The employees of the company regularly access the company's sales webpage to search for vacation packages their customers might like.

One afternoon, you receive an automated alert from your monitoring system indicating a problem with the web server. You attempt to visit the company's website, but you receive a connection timeout error message in your browser.

You use a packet sniffer to capture data packets in transit to and from the web server. You notice a large number of TCP SYN requests coming from an unfamiliar IP address. The web server appears to be overwhelmed by the volume of incoming traffic and is losing its ability to respond to the abnormally large number of SYN requests. You suspect the server is under attack by a malicious actor.

You take the server offline temporarily so that the machine can recover and return to a normal operating status. You also configure the company's firewall to block the IP address that was sending the abnormal number of SYN requests. You know that your IP blocking solution won't last long, as an attacker can spoof other IP addresses to get around this block. You need to alert your manager about this problem quickly and discuss the next steps to stop this attacker and prevent this problem from happening again. You will need to be prepared to tell your boss about the type of attack you discovered and how it was affecting the web server and employees.

Step-By-Step Instructions

Follow the instructions and answer the question to complete the activity. Then, go to the next course item to compare your work to a completed exemplar.

Step 1: Access the template

To use the template for this course item, click the link below and select *Use Template*.

Link to template: [Cybersecurity incident report]

Pro Tip: Save the template

You can save a blank copy of the template you used to complete this activity for further practice or in your professional projects. These templates will help you work through your thought processes and demonstrate your experience to potential employers.

What to Include in Your Response

Be sure to address the following in your completed activity:

- The name of the network intrusion attack
- A description of how the attack negatively impacts network performance

Follow the instructions and answer the question to complete the activity. Then, go to the next course item to compare your work to a completed exemplar.

Step 1: Access the template

To use the template for this course item, click the link below and select *Use Template*.

Link to template: [Cybersecurity incident report]

The following supporting materials will help you complete this activity. Keep them open as you proceed to the next steps.

To use the supporting materials for this course item, click the following links and select *Use Template*.

Links to supporting materials:

- Wireshark TCP/HTTP log
- How to read a Wireshark TCP/HTTP log

Reflect on the types of network intrusion attacks that you have learned about in this course so far. As a security analyst, identifying the type of network attack based on the incident is the first step to managing the attack and preventing similar attacks in the future.

Here are some questions to consider when determining what type of attack occurred:

- What do you currently understand about network attacks?
- Which type of attack would likely result in the symptoms described in the scenario?
- What is the difference between a denial of service (DoS) and distributed denial of service (DDoS)?
- Why is the website taking a long time to load and reporting a connection timeout error?

Review the Wireshark reading from step 2 and try to identify patterns in the logged network traffic. Analyze the patterns to determine which type of network attack occurred. Write your analysis in section one of the Cybersecurity incident report template provided.

Review the Wireshark reading from step 2, then write your analysis in section two of the Cybersecurity incident report template provided.

When writing your report, discuss the network devices and activities that are involved in the interruption. Include the following information in your explanation:

- Describe the attack. What are the main symptoms or characteristics of this specific type of attack?
- Explain how it affected the organization's network. How does this specific network attack affect the website and how it functions?
- Describe the potential consequences of this attack and how it negatively affects the organization.
- *Optional:* Suggest potential ways to secure the network so this attack can be prevented in the future.

Pro Tip: Save the template

You can save a blank copy of the template you used to complete this activity for further practice or in your professional projects. These templates will help you work through your thought processes and demonstrate your experience to potential employers.

What to Include in Your Response

Be sure to address the following in your completed activity:

- The name of the network intrusion attack
- A description of how the attack negatively impacts network performance