# Project: Introduction to Packet Capture and Intrusion Detection/Prevention Systems

**Video Transcript:**

## [ **You are a network analyst on the fly-away team for the FBI's cybersecurity sector engagement division. You've been deployed several times to financial institutions to examine their networks after cyberattacks, ranging from intrusions and data exfiltration to distributed denial of services to their network supporting customer transaction websites.**

**A representative from the Financial Services Information Sharing and Analysis Center, FS-ISAC, met with your boss, the chief net defense liaison to the financial services sector, about recent reports of intrusions into the networks of banks and their consortium.**

**He's provided some of the details of the reports in an email. "Millions of files were compromised, and financial officials want to know who entered the networks and what happened to the information. At the same time, the FS-ISAC has seen extensive distributed denial of service disrupting the bank's networks, impacting the customer websites, and blocking millions of dollars of potential transactions," his email reads.**

**You realize that the impact from these attacks could cause the downfall of many banks and ultimately create a strain on the US economy. In the email, your chief asks you to travel to one of the banks and using your suite of network monitoring and intrusion detection tools, produce two documents—a report to the FBI and FS-ISAC that contains the information you observed on the network and a joint network defense bulletin to all the banks in the FS-ISAC consortium, recommending prevention methods and remediation against the types of malicious traffic activity that they may face or are facing.. ]**

**Project Description:**

Network traffic analysis and monitoring help distinguish legitimate traffic from malicious traffic.

Network administrators must protect networks from intrusions. This can be done using tools and techniques that use past traffic data to determine what should be allowed and what should be blocked. In the face of constantly evolving threats to networks, network administrators must ensure their intrusion detection and prevention systems are able to analyze, monitor, and even prevent these advanced threats.

In this project, you will research network intrusion and prevention systems and understand their use in a network environment. You will also use monitoring and analysis technologies in the Workspace to compile a Malicious Network Activity Report for financial institutions and a Joint Network Defense Bulletin for a financial services consortium.

The following are the deliverables for this project (2 word document files):

* **Malicious Network Activity Report**: An 8 pages double-spaced Word document with citations in APA format. The page count does not include figures, diagrams, tables, or citations.
* **Joint Network Defense Bulletin**: A one-page double-spaced document.

There are eight steps to complete the project. Begin with the workplace scenario above and continue to Step 1, “Create a Network Architecture Overview.”

# Step 1: Create a Network Architecture Overview

As part of your assignment to report on prevention methods and remediation techniques for the banking industry, you would have to travel to the various bank locations and gain access to their networks. However, you must first understand the network architecture of these banks.

Provide a network architecture overview along with diagrams. Your overview can be fictitious or based on an actual organization. The goal is to provide an understanding of the network architecture.

Describe the various data transmission components:

1. User Datagram Protocol (UDP)
2. Transmission Control Protocol/Internet Protocol (TCP/IP)
3. internet packets
4. IP address schemes
5. well-known ports and applications

Address the meaning and relevance of information, such as:

1. the sender or source that transmits a message
2. the encoder used to code messages
3. the medium or channel that carries the message
4. the decoding mechanisms used
5. the receiver or destination of the messages

Describe:

1. the intrusion detection system (IDS)
2. the intrusion prevention system (IPS)
3. the firewalls that have been established
4. the link between the operating systems, the software, and hardware components in the network, firewall, and IDS that make up the network defense implementation of the banks’ networks.

Identify:

1. how banks use firewalls
2. how banks use IDSs
3. the difference between these technologies

Include:

1. the network infrastructure information
2. the IP address schemes that will involve the IP addressing assignment model
3. the public and private addressing and address allocations
4. potential risks in setting up the IP addressing scheme

Research and read about the following:

* intrusion detection and prevention (IDS/IPS) systems
* firewalls

Identify:

1. any well-known ports and applications that are used
2. risks associated with those ports and applications being identified and possibly targeted

Add your overview to your report.

In the next step, you will identify network attacks and ways to monitor systems to prevent these attacks.

# Step 2: Identify Network Attacks

In the previous step, you provided an overview of the network architecture. In this step, you will identify possible cyberattacks such as spoofing/cache poisoning, session hijacking, and man-in-the-middle attacks.

Provide techniques for monitoring these attacks using knowledge acquired in the previous step. Review the following resources to gain a better understanding of these particular cyberattacks:

* Session hijacking: spoofing/cache poisoning attacks
* Man-in-the-middle attacks

One way to monitor and learn about malicious activities on a network is to create honeypots.

Propose a honeypot environment to lure hackers to the network and include the following in your proposal:

1. Describe a honeypot.
2. Explain how a honeypot environment is set up.
3. Explain the security and protection mechanisms a bank would need for a honeypot.
4. Discuss some network traffic indicators that will tell you that your honeypot trap is working.

Include this information in your final report. However, do not include this information in the bulletin to prevent hackers from being alerted about these defenses.

Then, continue to the next step, where you will identify false negatives and positives.

# Step 3: Identify False Positives and False Negatives

You just identified possible information security attacks. Now, identify the risks to network traffic analysis and remediation. Review the resources on false positives and false negatives and discuss the following:

1. Identify what are false positives and false negatives.
2. How are false positives and false negatives determined?
3. How are false positives and false negatives tested?
4. Which is riskier to the health of the network, a false positive or a false negative?

Describe your analysis about testing for false negatives and false positives using tools such as IDSs and firewalls, and include this as recommendations for the banks in your public service Joint Network Defense Bulletin.

Discuss the concept of performing statistical analysis of false positives and false negatives.

Explain how banks can reduce these issues.

Research possible ways to reduce these events and include this information as recommendations in the Malicious Network Activity Report.

Network intrusion analysis is often done with a tool such as Snort. Snort is a free and open-source intrusion detection/prevention system program. It is used for detecting and preventing malicious traffic and attacks on networks, analysis, and education. Such identification can be used to design signatures for the IDS, as well as to program the IDS to block this known bad traffic.

Network traffic analysis is often done using tools such as Wireshark. Wireshark is a free and open-source packet analyzer. It is used for network troubleshooting, analysis, software and communications protocol development and education. Cybersecurity professionals must know how to perform network forensics analysis.

In the next step, you will analyze network traffic (LAB).

# Step 4: Analyze Network Traffic (LAB) This part is for an online LAB no need to do anything for this part. Continue to the next step.

This Lab is about analyzing network traffic, conducting network forensics analysis, identifying malicious network addresses, developing proposed rules to prevent against known malicious sites and testing for these signatures.

# Step 5: Determine Sensitivity of Your Analysis

In the previous step, you completed network analysis. In this step, you will determine which information to include in which document.

Information appropriate for internal consumption may not be appropriate for public consumption. The Joint Network Defense Bulletin may alert criminals of the network defense strategy. Therefore, be careful about what you include in this bulletin.

Once you have assessed the sensitivity of the information, include appropriate information in your Malicious Network Activity Report.

Then, include appropriate information in the Joint Network Defense Bulletin in a way that educates the financial services consortium of the threat and the mitigating activities necessary to protect against that threat.

# Step 6: Explain Other Detection Tools and Techniques

In the previous step, you included appropriate information in the proper document. In this step, perform independent research and briefly discuss what other tools and techniques may be used to detect these signatures.

Provide enough detail so that a bank network administrator could follow your explanation to deploy your system in production. Include this information in the Joint Network Defense Bulletin.

Next, move to the next step, where you will organize and complete your report.

# Step 7: Complete Malicious Network Activity Report

Now that you have gathered all the data for your **Malicious Network Activity Report** word document, it is time to organize your report. The following is a suggested outline:

1. Introduction: Describe the banking institution and the issue you will be examining.
2. Overview of the Network Architecture
3. Network Attacks
4. Network Traffic Analysis and Results
5. Other Detection Tools and Techniques
6. Recommended Remediation Strategies

You are now ready for the last piece of this project, the Joint Network Defense Bulletin.

# Step 8: Create the Joint Network Defense Bulletin

In this step, you will create the **Joint Network Defense Bulletin** word document. Compile the information you have gathered, taking care to eliminate any sensitive bank-specific information. The Joint Network Defense Bulletin is an educational document for the financial services consortium. This bulletin should be addressed to the FBI chief and the FS-ISAC representative.

The following are the deliverables for this project:

* **Malicious Network Activity Report**: An 8 pages double-spaced Word document with citations in APA format. The page count does not include figures, diagrams, tables, or citations.
* **Joint Network Defense Bulletin**: A one-page double-spaced document.

**End of Project**