|  |  |
| --- | --- |
| Python  Project 1  IDS Documentation | Aaron Legg  PYTWO1 |

Contents

[1.Project overview 2](#_Toc187933344)

[2.Features 2](#_Toc187933345)

[3.Installation 2](#_Toc187933346)

[4.Usage 3](#_Toc187933347)

[5.Code Explanation 3](#_Toc187933348)

[6.Project 5](#_Toc187933349)

[7.Conclusion 5](#_Toc187933350)

# 1.Project overview

The purpose of the Intrusion Detection System (IDS) is to identify possible security risks by continuously monitoring and analysing network traffic. Pattern matching is used to find suspicious activity, including known malicious URLs or phrases, unsafe instructions, and unencrypted HTTP traffic.

# 2.Features

 Monitors TCP traffic in real-time.

 Detects unencrypted HTTP traffic.

 Identifies malicious patterns in payloads, such as :

* Suspicious URLs.
* Keywords related to unauthorized access or malicious scripts.
* Dangerous system commands.

 Logs detected threats with detailed timestamps and packet summaries for further analysis.

# 3.Installation

 Install Python (version 3.6 or later).

 Install the required libraries :

>pip install scapy

# 4.Usage

Run the script:

1. Start cmd in administrator
2. Navigate to the file where Packet\_Sniffer.py is. (ex: cd "C:\Users\aaron\Desktop\LGK\PYTWO1\PROJECT 1")
3. Run the program (>python Packet\_Sniffer.py)

* If no network interface is specified, the program will display a list of available interfaces. Enter the name of the desired interface when prompted.
* The IDS will analyse the network traffic in real time. Detected threats will be displayed on the terminal and logged into the file threat\_log.txt.
* Press Ctrl+C to stop the program.

# 5.Code Explanation

Imports and configuration:

 Imports : The script uses scapy for packet sniffing, re for pattern matching, and logging for storing threat logs.

 Logging **Setup** : Logs are stored in threat\_log.txt with timestamps and detailed messages.

Suspicious Patterns:

The suspi\_patterns dictionary contains predefined patterns to identify:

* **URLs**: Known malicious domains and websites.
* **Keywords**: Indicators of malicious activity (e.g., password, <script>, or patterns resembling credit card numbers).
* **Commands**: Dangerous shell commands (e.g., rm -rf, sudo, and wget).

Detection Functions:

detect\_http\_traffic(packet)

This function examines the Host header in the packet payload to look for unencrypted HTTP traffic. It logs a warning against unencrypted browsing if the server does not use HTTPS.

detect\_suspicious\_packet(packet)

 Searches for matches within the payload based on the predefined patterns in suspi\_patterns.

 Logs and prints details of any detected suspicious activity, including the category, pattern, and packet summary.

 Calls detect\_http\_traffic(packet) to check for unencrypted HTTP connections.

Sniffing function:

sniff\_packets(interface=None)

This function starts sniffing packets on a specified network interface:

* Displays a list of available interfaces if none is provided.
* Uses Scapy’s sniff() method to capture packets filtered by the tcp protocol.
* Processes each packet using the detect\_suspicious\_packet() function.

Main Function:

The script calls sniff\_packets() to start running. Network interfaces can be specified by users or chosen from the list that is shown.

# 6.Project

I think the project was a success. I have managed to create this IDS with all the functionalities I needed and wanted. It is working well and one of the main features I wanted, was respected. This feature is the ease of use. It is a simple command to use in the command prompt on your PC.

I have encountered a few issues during that project which are time and debugging.

I think I should have planned my project earlier that what I did. For the debugging part I think it is normal to have trouble with debugging bug I would say it was my biggest loss of time.

# 7.Conclusion

An effective method of continuously monitoring network traffic for possible threats is offered by this intrusion detection system. The intrusion detection system (IDS) improves network security by detecting threats including malicious payloads and unencrypted HTTP traffic by using Scapy for packet analysis and predefined patterns for threat identification. The system is a useful tool for network managers and security experts due to its ease of use and expandability.